Forensic Science International: Digital Investigation 45 (2023) 301541

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

IoT forensic analysis: A family of experiments with Amazon Echo devices

Scott Lorenz [a], Stanley Stinehour [a], Anitha Chennamaneni [b, *], Abdul B. Subhani [a], Damiano Torre [b]

[a] Centex Technologies, 501 N 4th St, Killeen, 76541, TX, USA
[b] Department of Computer Information Systems, Texas A&M University Central Texas, 1001 Leadership Pl, Killeen, 76549, TX, USA

ARTICLE INFO

Article history:
Received 16 September 2022
Received in revised form
30 January 2023
Accepted 26 March 2023
Available online xxx

Keywords:
Forensics analysis
Internet of things
Amazon echo
Experiments

ABSTRACT

Criminal Investigations involving digital devices often focus on the analysis of mobile phones, tablets, and computers associated with the suspect or the victim. The connection of IoT devices to criminal investigations may not always be considered or understood by professionals handling the crime scene. The language, experience, and understanding needed to articulate the appropriate causes required to include IoT devices in search warrant affidavits are not always known or available to case agents overseeing the evidence-gathering portion of the investigation. For this reason, we introduce a novel methodology that shows how to locate and identify IoT device owner account information, device specifications and configurations, and the location of user activity on the device. We use this methodology to carry out a family of eight experiments on IoT devices that can assist law enforcement professionals in the construction of search warrant affidavits with information that will help satisfy the legal requirement to show evidence of a crime is likely contained on IoT devices. In this paper, we focus on Amazon Echo Show IoT devices and the legal justification for seizing and examining the devices, methods of extraction, and location of user-related artifacts on IoT device hardware. Overall, the implications of our study offer law enforcement professionals specific, practical instructions on how to deal with Amazon IoT devices involved in a crime scene. The analysis of data related to these devices is presented through practical demonstrations of these devices in action.

1. Introduction

For the typical law enforcement officer or agency, understanding what digital devices should be seized at a crime scene and providing that legal justification is of paramount importance. Mobile phones and computers are frequent targets for seizure at crime scenes, but Internet of Things (IoT) devices (Goulart et al., 2022) (i.e., connected appliances, smart home security systems, autonomous farming equipment, wearable health monitors, smart factory equipment, wireless inventory trackers, etc.) can be overlooked or not considered for lack of specific information needed to justify their seizure. The identification of the location of IoT data is often listed as one of the biggest challenges for investigators (Chi et al., 2018) because evidence related to IoT can be varied across all devices. There is a lack of training, software, education, and needed improvements to tools with most improvement needed in data acquisition and device disassembly (Wu et al., 2019). In addition, the novelty of the IoT devices can create inefficient forensic investigations leading to the inadmissibility of evidence Gómez et al. (2019). Some specific information about IoT devices is needed by law enforcement, pre-seizure, for legal justification to remove the device from the scene of a crime. When IoT devices are seized, investigators need to know how to exploit the devices, extract the data, parse the data, and understand what data is likely stored on the device. Often investigators have no guidance or standardized method to collect evidence from an IoT device in a forensically sound manner (Stoyanova et al., 2020). There is a need for more forensically sound methods when investigators analyze IoT devices (Hadgkiss et al., 2019). Examination and analysis of data stored on IoT devices can be challenging for many reasons: (i) there is no universal standard to collect, examine and analyze data from IoT

* Corresponding author.
E-mail addresses: slorenz@centextech.com (S. Lorenz), stanley@centextech.com (S. Stinehour), anitha.chennameneni@tamuct.edu (A. Chennamaneni), asubhani@centextech.com (A.B. Subhani), damiano.torre@tamuct.edu (D. Torre).

https://doi.org/10.1016/j.fsidi.2023.301541
2666-2817/© 2023 Elsevier Ltd. All rights reserved.

devices (Karabiyik and Akkaya, 2019); (ii) IoT devices have no common interfaces (Meffert et al., 2017); (iii) the diversity of IoT devices compared to mobile devices (Li et al., 2019); (iv) the lack of familiarity of the investigators with IoT devices (Li et al., 2019); (v) there is no a forensically solid method or reliable tool to gather evidence from IoT devices (Alenezi et al., 2019); (vi) IoT devices generate a huge amount of diverse data (Yaqoob et al., 2019); each IoT manufacture uses different hardware and operating systems (Chung et al., 2017; Stoyanova et al., 2020). It is clear that without some knowledge of what IoT devices can contain, it is difficult for crime scene investigators to articulate the justification for the seizure of the device in a search warrant affidavit. This can create a legal issue of meeting the requirement that the place to be searched likely contains evidence of a crime and thus difficulty describing the things to be seized as prescribed by the Fourth Amendment to the U.S. Constitution. The U.S. Department of Justice (DoJ, 2009) discusses the importance of describing things to be seized with particularity as required by the Fourth Amendment. The warrant must describe the things to be seized with sufficient precise language and the description of things to be seized should be limited to the scope of the probable cause established in the warrant.

The analysis of digital devices has rapidly become a large part of many criminal investigations. Many papers focus on privacy as it relates to IoT devices (Nieto et al., 2018). It is equally important that law enforcement professionals have access to research that can assist in making the connection between digital data on IoT devices and legal procedure as it relates to the justification for the seizure and search of IoT devices. Multiple studies (Nieto et al., 2018; Chi et al., 2018; Alenezi et al., 2019; Servida and Casey, 2019; Li et al., 2019; Chung et al., 2017) can be found in the literature about the need for forensic tools and methods to collect and analyze IoT devices. We describe these papers in detail in section 7 as part of the related work. All those papers pointed out the need for information on specific IoT device hardware and real-world scenarios.

Although many IoT devices are limited in their ability or design to store content or contraband, mere evidence and metadata can be valuable sources of evidence in criminal investigations. Nevertheless, the vast majority of IoT devices do not store any metadata (Stoyanova et al., 2020). There are several categories of importance when respondents were asked about the evidence on IoT devices (Wu et al., 2019) such as behavioral patterns of users, timelines of events, and metadata. Most IoT devices do not store any kind of metadata or temporal information, e.g. modified, accessed, and created time, correlation between pieces of evidence gathered from various IoT devices is nigh on impossible (Pawlaszczyk1 et al., 2019). Newer IoT devices are not supported by the existing forensics tools, making the data extraction process even more challenging. Therefore, advances in Digital Forensics are now more difficult to achieve than in the early years of the discipline (Stoyanova et al., 2020). IoT devices always connected to the Internet produce evidentiary data but how to acquire forensically relevant data and how to analyze it from different IoT devices without a common interface, internal storage or standard protocols is a challenge (Meffert et al., 2017).

With this being said, there is a need to identify and classify data stored on IoT hardware to be introduced in future projects (Chung et al., 2017). For crime scene investigators, there is a lack of detailed information on how to exploit specific IoT hardware for the purpose of forensic investigations and thus a lack of information about what data IoT devices store. IoT devices can generate personal data which can be stored in various locations including the IoT hardware. This information can be an important part of criminal investigations. The universe of IoT devices is vast and growing but the understanding, training, and experience needed by law enforcement to seize and examine IoT devices are lacking. The main object of this research is to provide to the Forensics community, law enforcement, and related professionals, specific information about what data can be stored on Amazon IoT devices (i.e., Amazon Echo), how to access and parse that information, and how the information relates to user activity and thus potentially to a crime. A recent study carried out by Orr and Sánchez (2018) showed how Amazon Echo does possess data of evidentiary value. Difficulty in examining Amazon hardware due to changes in hardware configuration resulting in lack of public information on device pinouts needed to extract data via In-System-Programming(ISP) (Pawlaszczyk1 et al., 2019). There is a need for scenario-based analysis and device-specific based analysis which can include a reconstruction of crime scenes and events (Li et al., 2019). With this research, it is our intention to provide specific examples of data located on Amazon IoT device hardware and demonstrations of how that data was created and stored on these devices through scenarios designed to seed the specific IoT devices through typical user activity. Although this paper is designed to be a technical paper on exploiting digital data on Amazon IoT devices, it is impossible to discuss the relevance of digital data without defining and discussing the relationship between digital data and legal procedure. It is necessary to understand the requirements and constraints of legal procedure as it relates to the description, seizure, and analysis of IoT devices. Clearly stated, without knowledge related to specific IoT devices and what digital data they can store, law enforcement will not be able to articulate probable cause linking an IoT device to a specific crime or provide a magistrate with facts demonstrating the IoT device can store evidence.

The main goal of this paper is to determine what could be gleaned from Amazon IoT device hardware alone, with the assumption that it is the only evidence the forensic examiner possessed at the time of the analysis. Amazon devices are considered great sources of evidence but their analysis did not include an examination of the Echo hardware (Chung et al., 2017). This research provides a practical approach and guide for law enforcement agencies when encountering Amazon IoT devices at crime scenes or during criminal investigations. We describe the results of a family of experiments that provide law enforcement with the necessary information and tools to seize and handle Amazon IoT hardware from beginning to end.

We provide the following main contributions:

- A methodology that shows how to locate and identify device owner account information, device specifications, and configurations, and the location of user activity on the device which can contain mere evidence and contraband is also provided;
- A four-step process to carry out experiments on IoT devices that can assist law enforcement professionals in the construction of search warrant affidavits with information that will help satisfy the legal requirement to show evidence of a crime is likely contained on the IoT device.
- The results of eight experiments carried out on IoT Amazon devices. Those results are meant to provide law enforcement with specific, practical instructions on how to extract data from Amazon IoT devices;
- A background analysis of IoT device forensics discussing the reasons for seizing digital evidence and the types of digital evidence.
- A complete example of the device diagram that will help law enforcement personnel to understand how evidence is stored on the IoT hardware by everyday interactions with the device.

The rest of this paper is structured as follows. Section 2 provides background information. Section 3 describes the methodology we apply in this research. We present the IoT devices involved in this study in section 4. This is followed by the description of the experimental setup in section 5. A preliminary discussion with the main findings of the experiments carried out is provided in section 6. In section 7 we provide a brief discussion on related work. Section 8 discusses limitations and provides directions for future works. Finally, section 9 draws the conclusions.

2. Background

In this section, we briefly describe what could be, in the context of IoT devices forensics, (i) the causes of seizing digital evidence, (ii) the types of digital evidence, and (iii) the differences between metadata and content.

2.1. Seizure of digital evidence

Traditional digital forensics investigations can involve the seizure of digital evidence at crime scenes in which voluntary participation of citizens is not required (Nieto et al., 2018). That lack of voluntary participation means law enforcement will need the warrant to seize and search the IoT device. Presence at a crime scene, alone, does not satisfy the probable cause requirement to seize or search a digital device. A legal seizure of a device requires the search warrant affiant to justify the taking of another's property based on probable cause that links the IoT device to a crime (Novak, 2020). Like the arrest of a person, the justification to seize an item must be present before the seizure occurs. This is a fundamental concept that requires law enforcement professionals to go beyond the proximity of an IoT device at a crime scene in their articulation for probable cause to seize an item. The United States Department of Justice (DoJ, 2009) describes the facts needed to establish probable cause to search computers or electronic media. These facts include probable cause to believe that the media contains or is contraband, evidence of a crime, fruits of crime, or an instrumentality of a crime (DoJ, 2009). The problem law enforcement investigators face at crime scenes when identifying the presence of an IoT device, is a lack of prior knowledge, experience, training, and detailed research to assist them in drafting a search warrant affidavit justifying the seizure of the particular IoT device. The nature of digital evidence complicates seizing it with a warrant and there is a need for law enforcement to update warrants over time (Bair, 2017). After establishing probable cause to believe a crime was committed, a search warrant affidavit must also articulate the likelihood that evidence of that crime will be present in the particular place to be searched or on the particular thing to be seized. That part of the Fourth Amendment frequently referred to as the “particularity requirement” requires that the particular place to be searched and the thing or things to be seized must be described with as much detail as possible. These fundamental principles mandated in the Fourth Amendment apply to the digital world even though the Fourth Amendment was written long before digital devices were imagined. Digital evidence to be used in a trial must be obtained with probable cause supporting the search and seizure of the evidence. Failing to justify the seizure of the device can result in the evidence being inadmissible in court (Novak, 2020). Probable cause necessary to search a digital device must articulate that the item likely contains evidence of a crime or the fruits of a crime (DoJ, 2009). With few exceptions, e.g., contraband or fruits of a crime, seizing and searching digital evidence require the same probable cause but are two separate events. Seizing digital hardware, which includes IoT devices, as evidence can be done if there is probable cause to believe the device is reasonably likely to contain evidence of a crime. Probable causes related to the information stored on a computer should identify the information, in particular, by focusing on the content of the relevant files rather than on the storage devices which may happen to contain them (DoJ, 2009). This same concept applies to digital information on IoT devices. The approval for the seizure of an IoT device should come in advance of the seizure itself in the form of a search warrant after a judge has been presented with probable cause that the IoT device likely contains evidence of a crime. The actual search or analysis of the IoT hardware seized occurs later. Under Federal law and most State laws, a search warrant for digital evidence is considered executed when the device is seized by the law enforcement agency executing that search warrant. The time limitation on the execution of the warrant is satisfied if the IoT device is seized within the jurisdiction's time constraints set out by law. The U.S. Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (DoJ, 2009) distinguishes the seizure of seized digital media from the later forensic examination as codified in the Federal Rules of Criminal Procedure 41(e) (2) (A) and (B). The Texas Code of Criminal Procedure Chapter 18.07(c)[1] also has a provision distinguishing the seizure of the device as the execution of a search warrant, from the analysis of the device contents after the seizure.

2.2. Types of digital evidence of IoT devices

The definition of IoT devices and digital evidence is important when conducting investigations involving IoT devices. Describing what type of digital evidence is being sought and where the digital evidence is stored is critical for legal justification of IoT device seizure. Experience, training, and research generated by someone other than the affiant in the application of a search warrant may be used to provide further details needed to justify the seizure of the IoT device. A basic definition of digital data is the 1's and 0's located on an electronic device. Unless someone uses an IoT device to beat someone over the head, the IoT device was purchased with the fruits of a crime, the IoT device is stolen, or the IoT device is modified so that it meets the definition of a criminal instrument, the seizure of an IoT device is typically related to the data stored on the IoT device. Digital evidence is inherently different than physical evidence and thus creates a unique set of search and seizure complications (Novak, 2020). At least a fundamental understanding of what type of data is capable and likely to be stored on an IoT device is necessary for a search warrant affiant to particularly describe the likelihood the data is related to the crime being investigated. Without knowing what type of data is or can be stored on an IoT device, it is impossible to legally seize an IoT device, as evidence, at a crime scene. It is the burden of the government agent seizing an IoT device to describe how the item is evidence of a crime or contains evidence of a crime. When considering the seizure of an IoT device at a crime scene, law enforcement must be able to show that evidence of a crime is likely to be located on that “particular” device and provide some details and facts based on the totality of the circumstances connecting that device to a crime. The U.S. Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (DoJ, 2009) emphasizes this requirement in their guidance to “particularly describe” the place to be searched and the persons or things to be seized as explicitly required in the language of the Fourth Amendment to the United States Constitution. This requirement is sometimes overlooked or left out of search warrant affidavits when seizing digital evidence because the information may not be known by the law enforcement professional processing the crime scene.

[1] https://statutes.capitol.texas.gov/Docs/CR/htm/CR.18.htm.

Even if this requirement is known and understood by the law enforcement professional processing the crime scene, there may be a lack of information regarding the content of IoT devices and thus evidence may be left behind. Probable cause to seize an IoT device must describe the device hardware and the information capable of being stored on the device hardware. This is a point clearly made by the U.S. Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (DoJ, 2009): If a digital device hardware is contraband, evidence, fruits, or instrumentalities of crime, the warrant should describe the hardware itself. If the probable cause relates only to information, however, the warrant should describe the information to be seized, and then request the authority to seize the information in whatever form it may be stored (whether electronic or not). It is necessary for law enforcement to understand the difference between mere evidence and contraband and how those terms are applied to digital evidence to link an IoT device to a particular crime. Mere evidence and contraband are terms that are also associated with "metadata" and "content" in the digital world. A relevant consideration regarding the seizure of an IoT device by a law enforcement agency is if the IoT device can contain content, mere evidence, contraband, and metadata or if the IoT device itself is contraband or/and instrument of a crime:

- **Contraband:** a digital device can be contraband either because the digital device is a repository of data that is contraband (such as child pornography) or because the computer is stolen property;
- **Evidence of a crime:** a digital device can be a repository of data that is evidence of a crime—such as a spreadsheet showing illegal drug transactions, a letter used in an ongoing fraud, or log files showing IP addresses assigned to the digital device and websites accessed.
- **Instrument of a crime:** a digital device can be an instrument of a crime—for example, the digital device was used as a tool to hack into websites, distribute copyrighted videos, or produce illegal pornography (DoJ, 2009).

The U.S. Department of Justice (DoJ, 2009) suggests devising a search strategy before drafting an affidavit for a warrant for a digital device in which a consideration is made as to the likely role the digital device played in the offense being investigated.

2.2.1. *Contraband*

The definition of contraband is a thing that is illegal to possess. Contraband can include items in the digital and physical world and some contraband can exist in both. The U.S. Department of Justice in their Citizen's Guide to U.S. Federal Law on Child Pornography describes child pornography as contraband, not protected by the First Amendment, and illegal to possess (DoJ, 2020). A digital image depicting child pornography is contraband. Child pornography can exist as evidence in the digital and physical world and is contraband in either. Viewing child pornography as an abuse of a Smart TV and thus it may be considered part of a digital forensic investigation (Boztas et al., 2015). Methamphetamine can exist in the physical world where it is contraband, but it cannot exist as contraband in the digital world. Although photographs of methamphetamine may be evidence of a crime, they are not illegal to possess and therefore may be considered mere evidence.

2.2.2. *Evidence of a crime*

The definition of mere evidence of a crime is something that is evidence of a crime but is not illegal to possess. The aforementioned photographs of methamphetamine can be mere evidence of a crime. The U.S. Department of Justice (DoJ, 2009) in discussing the history of the Privacy Protection Act distinguished "mere evidence" of crime and "contraband, instrumentalities, or fruits of a crime". Evidence that someone researched or downloaded child pornography can be mere evidence of a crime while the actual images of child pornography are contraband. Thus, digital devices can contain mere evidence or contraband, though some devices may only contain one or the other. The distinction between the two as it pertains to IoT devices is more than just an academic consideration. The likelihood that an IoT device can contain contraband or just mere evidence can affect the legal procedure involving the seizure and examination of the device. Understanding what type of evidence is stored on an IoT device can be crucial in meeting the legal requirements to seize and examine the device. Depending on the statute, a search warrant for contraband versus mere evidence can place restrictions or requirements on the type of judge or magistrate who can issue the search warrant. In their Warrants Manual, the Texas County and District Attorneys Association distinguishes between warrant affidavits requesting permission to search for contraband versus mere evidence. Although any magistrate may issue a warrant searching for contraband, warrants for mere evidence, an "item or substance not inherently illegal", fall under more stringent guidelines. Under these guidelines warrants for mere evidence generally can not be issued by magistrates who are not licensed attorneys and not from courts of record (Bechham et al., 2018).

2.3. *Metadata and content*

Merriam-Webster defines metadata as "data that provides information about other data.[2]" The term "metadata" as it is commonly used in referring to digital privacy and digital forensics means the same thing. When discussing evidence on digital devices, the data which is described by metadata is referred to as "content". Metadata as defined cannot be considered contraband, but it can be evidence of a crime and thus is considered "mere evidence" for purposes of search warrant affidavits. Metadata has a legal distinction from content in that content of communication generally has more privacy protection than metadata. In discussing Pen Registers and Trap and Trace Devices defined in Title 18 of the United State Code, the U.S. Department of Justice (DoJ, 2009) distinguishes metadata from content stating "In general, the Pen/Trap statute regulates the collection of addressing and other non-content information for wire and electronic communications. Title III regulates the collection of the actual content of wire and electronic communications". The older definition of metadata, referring to traditional phone conversations, makes a clear distinction between metadata and content. However, when applied to modern mobile devices and the Internet of Things, metadata taken in mass can be much more revealing and impactful from an evidentiary point of view. Ferguson (2015) distinguishes metadata from content referring to metadata as "telephone contacts" but not the "telephone content" in describing old-fashioned pen registers used to log a subscriber's phone call activity. However, Ferguson points out that contacts and content become blurred with IoT devices in which the metadata can "reveal personal information just like content." Ferguson refers to IoT as the "internet of metadata" creating data trails that creates maps of a person's lives.

3. Methodology

In determining our methodology, we not only considered previous and current research, but we also decided to carry out this

[2] https://www.merriam-webster.com/dictionary/metadata.

case study from a typical investigative scenario perspective which is most frequently encountered by law enforcement in criminal investigations.

Fig. 1 shows the following six-step methodology that we used to carry out this research:

1. **Select IoT devices:** we select the Amazon IoT devices used in this research.
2. **Provide ID information of IoT devices:** we provide a detailed description and examples of identifying (ID) information and user data stored on the IoT devices.
3. **Verify ID information via FCC:** we used the grantee code, composed by five characters, in order to identify their devices in advance of release.
4. **Identify types of evidences:** we define and categorize the type of evidence which can be stored on Amazon IoT hardware including mere evidence and contraband; metadata and content, allowing law enforcement to justify the seizure of the IoT hardware at crime scenes.
5. **Extract data from IoT devices:** we show how to locate, identify, and parse evidence by searching the physical dump of the IoT device storage.
6. **Describe how to identify relevant data:** we describe in detail the Echo Show devices hardware and file structure identifying where data and evidence are stored.

In section 4, we introduce the Amazon IoT devices involved in this study, section 5 shows the experimental setup, and in section 6 we present the results of a family of experiments where we extract and parse digital data and evidence from a set of Amazon devices.

3.1. Select IoT devices

As stated before, we use Amazon Echo Show devices to carry out our experiments. These devices are listed under Smart Displays on the Amazon website under Amazon Echo & Alexa Devices. Amazon categorizes its devices with a “device family” designation. Amazon devices under the “Knight” family of devices are IoT devices with a touchscreen for viewing and user interaction. Although there are several devices in this category that support the Alexa Application, we focused on devices manufactured by Amazon. These devices are sold under the retail name of Amazon Echo Show.[3] Amazon tablets were not selected for this study as they do not fit the definition of an IoT device. Amazon tablets function also without an internet connection and are equipped with a battery. Amazon IoT devices with a screen do not function without an Internet connection and do not have a battery. We also selected another Amazon IoT device with a screen – the Echo Spot which also uses eMMC storage. In our analysis of Amazon devices, we also tested other Amazon IoT devices for comparison including other Amazon Echo devices without a screen and several Amazon Fire TV Sticks, and the Amazon Fire TV Cube. These devices have eMMC storage that is discussed in our detailed diagrams along with in-system-programming (ISP) pinouts.

3.2. Provide ID information of IoT devices

At the writing of this paper, there are seven Echo Show devices currently sold. The seven Echo Show devices released all have 8 GB eMMC storage and are not encrypted by default when sold. All are running Fire OS based on the Android operating system. Amazon's use of pseudo-Limited Liability Companies (LLCs) makes researching their devices in advance of release challenging unless examiners have the FCC ID number provided or have the actual device in which the FCC ID number is displayed on the outside. An LLC is the usual method of mining the FCC database based on manufacturer or other information, which remains consistent across other OEM's device registration submissions, but does not work with Amazon devices. If we do not have the device in our lab or obtain the FCC ID from another source, it is challenging to comb the FCC database for new Amazon devices on the horizon. For years Amazon has engaged in the practice of using a different LLC for each new device in registering their equipment with the FCC. That new LLC also includes different contact information and addresses to ensure nothing is the same from device to device. The name “Amazon” is not listed on any of the filing paperwork, even after all the confidentiality requests have expired. This can be frustrating for examiners or researchers looking ahead, before receiving the device in their lab, for internal photos to see what tear-down challenges are to be faced, what hardware the devices are using, or potential ISP locations.

3.3. Verify ID information via FCC

There is a common pattern with Amazon devices in that the Grantee Code is 5 characters starting with 2A***. A dash separates the Grantee Code from the Product Code which is four numbers on Amazon devices. Internal and external photographs for Amazon devices are often delayed for public release via the FCC by confidentiality letters submitted by the filing LLC. The external model number (the number visible on the outside of the device) eventually appears on some documentation when the confidentiality requests expire. The FCC filing for the Echo Show 8 was made by Teachey-1625 LLC. The LLC, its address, and all other information associated with Teachey-1625 LLC, have no visible connection to Amazon until it becomes obvious that the device is an Amazon product.

3.4. Identify types of evidences

In terms of the location of evidence on an IoT device, probable cause generally means “likely” to contain evidence. For this paper, while the presence of evidence on an IoT device might be possible, we characterize the presence of evidence on an IoT device under the metric of “likely” or not. This determination is normally made based on how the device performs under normal, intended usage as designed by Amazon, and specific facts known by law enforcement at a crime scene in connection with the seizure of that particular IoT device. Evidence on IoT devices can vary depending on the type (i.e., family) of Amazon devices. As an example, it is not likely that an Amazon Echo Flex would contain contraband but could contain “mere evidence”. The Echo Flex is a smart speaker but is not designed to store photographs. The Amazon Echo Dot (2nd Generation) is not “likely” to store contraband (photographs). It has a 4 GB eMMC storage and using a flasher box and ISP, it is possible to use the device to store contraband by writing information, including photos, to the storage. But the device has no display and is not configured to store photos under normal operating circumstances. The Echo Dot can contain mere evidence but is not likely to contain contraband under normal operating conditions.

3.4.1. After-the-fact hardware analysis

For crime scene investigations, this type of “after the fact” analysis of information extracted from the IoT hardware does not suffer from the legal, practical, and technical limitations of real-time analysis of IoT devices which also does not see into the past. It is not limited by the requirement to have usernames and

[3] https://www.amazon.com/echo-show-10/dp/B07VHZ41L8.

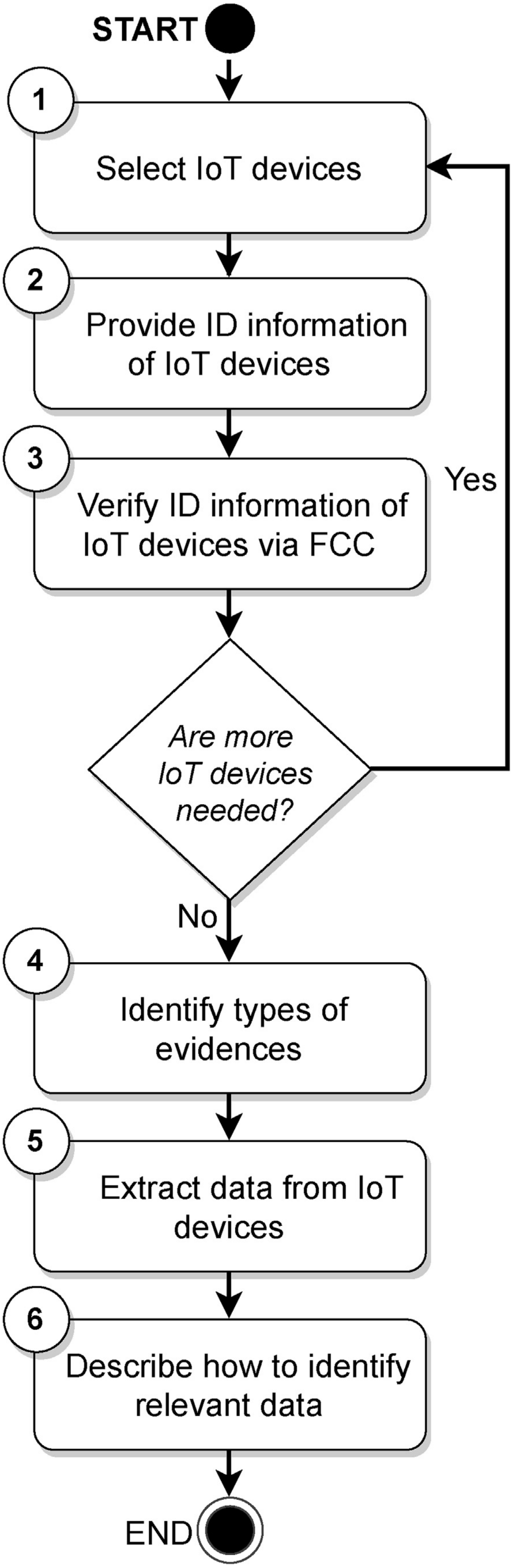

START
1
Select IoT devices
2
Provide ID information of IoT devices
3
Verify ID information of IoT devices via FCC
Are more IoT devices needed?
Yes
No
4
Identify types of evidences
5
Extract data from IoT devices
6
Describe how to identify relevant data
END

Fig. 1. Methodology.

passcodes for analyzing the data stored on the Amazon website. Electronic devices collected as evidence are usually collected after the fact – after the crime has been committed. Much of the previous research on IoT devices involves real-time analysis of network traffic but, according to Servida and Casey (2019), it is usually not possible to retroactively collect network traffic from an IoT device during a criminal investigation. A search warrant for the IoT device hardware can be executed without requiring that Amazon searches data stored in the cloud. The IoT device and its data can be preserved immediately when law enforcement occupies the crime scene. At the writing of this paper, we do know if detailed log information like touch events is stored by Amazon. Knowing what information is likely stored on Amazon IoT devices will help provide the information needed to justify the seizure of the device at the crime scene. This does not diminish previous studies or the need to understand how IoT devices perform and operate in real time. During device seeding, we could immediately view what information was stored on the Amazon site via Amazon's API. Chung et al. (2017) provides an appendix of unofficial APIs in their paper which allows the viewing of data stored in the Amazon cloud. This was extremely beneficial when seeding our test devices and in our analysis of the IoT hardware and the search for artifacts. There is a limitation that will often restrict law enforcement from making immediate use of this information. Access to this data is restricted as it requires the user's login and password to view it. This did not present a problem for our test devices attached to our accounts but under normal circumstances, law enforcement would not have immediate access to this information. Even with the user account and login information, a search warrant would be necessary to access the data or consent from a cooperating account owner.

3.4.2. *Cloud-side forensics*

Cloud extractions "after the fact" can also require additional, separate legal justification which may not be covered in the original search warrant affidavit to examine the IoT devices seized at the crime scene. In some cases, the recovery of deleted data may only be possible on the IoT device. Chung et al. (2017) note the difficulty in recovering deleted data in the cloud as a limitation of forensic analysis. In many criminal investigations, probable cause to search the cloud is obtained after the analysis of the digital device or hardware seized at the scene of the crime. In some cases, where legally permissible, tokens needed to access cloud-related data are obtained by analyzing the hardware seized at the scene.

3.4.3. *Real-time data analysis*

In addition to legal restrictions, real-time interception and examination of data can also be technically challenging. In particular, user credentials can represent a practical limitation of cloud-side forensics along with confirming that most data transfers were encrypted (Chung et al., 2017), and encrypted data transfers could represent also a challenge to forensics investigation of IoT devices (Servida and Casey, 2019). Real-time interception of data as it is created does not represent law enforcement actions in most criminal investigations. Justification for real-time interceptions is legally challenging, most often restricted to exigent circumstances for crimes still in progress, or long-term investigations related to specific criminal activity after obtaining monitoring warrants in furtherance of an ongoing investigation. In both of those scenarios, an after-the-fact collection and analysis of the IoT hardware are still necessary at some point. The after-the-fact examination of IoT hardware is most likely the first step in most criminal investigations when processing crime scenes.

3.5. Extract data from IoT devices

Amazon devices are not encrypted by default and most use an embedded Multi-Media Controller (eMMC) for non-volatile storage. Many Android-based devices have used eMMC storage for over a decade and this storage is still widely used today. This type of flash storage integrates flash memory and controller onto a single chip (Afonin and Katalov, 2016). Because the controller is built into the chip there is no need for the processor on the device to be involved in the extraction of data. Access to the data on eMMC storage can be accomplished while the device is powered off. Data can be obtained from non-functioning and severely damaged devices which utilize eMMC storage. Direct access to the eMMC can be accomplished by removing the eMMC storage to access the necessary connection points on the eMMC's ball grid array (BGA) or by accessing these same points on the eMMC without removing it using in-system-programming (ISP). The process of ISP allows for the connection of a software interface to the eMMC without removing it from the printed circuit board (PCB) as with chip-off (Reiber, 2019). ISP requires device-specific information to connect a software interface to specific locations on the PCB which lead to specific locations on the BGA of the eMMC. This device-specific information is colloquially referred to as a pinout. The pinout for a particular device can be unique for that specific model of IoT device or any device using eMMC storage. The pinout is a map that identifies specific locations on the PCB which correspond to specific locations on the eMMC's BGA pads. The BGA pads are not directly accessible while the eMMC is still mounted on the PCB. The minimum locations needed for ISP include Data0, Command, Clock, Ground, and Voltage to power the eMMC. The process of ISP has also been referred to as eMMC five-wire method by Boztas et al. (2015) in their research into extracting data from the eMMC chip on a smart TV. Creating pinouts for devices is typically done by using the chip-off method to remove the eMMC from an exemplar (a test device). The test device must be an identical model to the device being examined. With training, experience, and the proper tools it is sometimes possible to pin out a device being examined without removing the eMMC or destroying a test device. This process can be challenging and time-consuming and thus forensic examiners, including law enforcement, share pinouts with others in the forensic community through listservs and other forums. For ISP, a thin wire is typically used to make individual connections to specific points on the PCB for powering and communication with the eMMC. This is usually accomplished by soldering although there are solder-free solutions available. The ISP process can involve connecting more than five wires or less depending on how many data lines are located and utilized and whether the eMMC is powered via USB through the software interface in which connecting wires for power or ground may not be necessary for successful communication and extraction of data. Removing the eMMC is generally a destructive process with very few planned exceptions and is discussed in section 3.6.1. This removal of the eMMC from the PCB is a process referred to as chip-off and can involve using heat to remove the chip or a milling process to cut through or grind away the PCB to reach the underside of the eMMC. As Reiber (2019) describes, chip-off is destructive and generally, the device will not function after this procedure. Once the eMMC is removed it can be read by having access to the pads on the chip's BGA which allow communication with the controller and the transfer of data. The eMMC requires power for the extraction but powering the chip without booting the phone does not change the data stored on the eMMC as described by Reiber (2019). This makes extracting data directly from eMMC storage the most forensically sound method of obtaining data from these devices. Reiber (2019) described the benefit of a direct read of the eMMC via chip-off: The examiner can create a full binary file of the device memory flash without limitations typically imposed by a device microprocessor. This physical collection method would conform to a bit-by-bit representation of the entire device's physical store and equates to a traditional hard drive collection. The Echo Show devices and the Echo Spot all use eMMC storage and are not encrypted by default, making chip-off or ISP the best option to obtain a physical image of the storage. According to Reiber (2019) there is currently no available tools to access Alexa-based devices "via noninvasive means" but JTAG, ISP, and Chip-off allow access to the data. This means that device disassembly will be necessary to extract the data from the eMMC storage on Echo Show devices. Boztas et al. (2015) consider chip-off the most forensically sound method to copy data as no data is changed during the process. ISP is not destructive if done properly and, like chip-off, does not require the device to boot or even be in working order to access the data. Extraction of data via ISP will yield the same result as chip-off of the same device as long as the system does not power on while applying power to the eMMC storage. In this instance, a hash analysis of the two images taken from the same device — one image extracted via chip-off and one image extracted via ISP — will yield the same hash result.

3.6. Describe how to identify relevant data

The data stored on the eMMC storage of the Amazon Echo Show devices and the Echo Spot is not encrypted by default. There is no option to encrypt the data via the menus on the Echo Show devices. That means ISP and chip-off are options for these devices for purposes of conducting a forensic exam. These two options also provide the most forensically sound method of extracting data and allow a full physical dump of the storage without booting the device. For purposes of testing and demonstration for this paper, we used both ISP and chip-off in testing these devices. The purpose of this research project and paper is to provide forensic examiners with multiple options for accessing evidence of Amazon Echo show devices if more than one is available. This allows examiners to determine best practices for their agency or organization. Best practices can vary depending on the law enforcement agency or organization. Sometimes the circumstances in which the device was obtained can restrict the possible methods of extraction — e.g., the device was obtained via consent with the expectation of return in functioning order. Some agencies may be restricted by policy from forensic procedures deemed destructive or risky. Some examiners may have training in chip-off procedure but not ISP or vice versa. It may be necessary to inform judges, prosecutors, or private clients of methods before approval for examination is given.

3.6.1. Chip-off and reinstalling of eMMC storage on Echo Show devices

Examiners frequently use the word "destructive" to describe forensic processes or procedures that render a digital device damaged or non-functioning after the procedure is performed. Chip-off is generally considered a destructive process, whether using the milling process or hot air. The removal of the eMMC storage from the logic board renders the device inoperable. During this research, we used hot air to remove the eMMC from all the Echo Show devices. This allowed us to pin out the devices for ISP locations so future extractions could be done without removing the eMMC. For purposes of testing and economy, we reinstalled the eMMC storage on some Show devices so we could continue lab testing - using the devices for our research. With this procedure, chip-off is not a destructive process so long as the eMMC is not damaged during removal, cleanup, re-balling, and reinstalling. Reinstalling device storage is not a typical procedure performed by forensic examiners, but the procedure allowed us to continue using and testing the device while also documenting the time and temperature needed for hot air removal. Most Amazon devices with eMMC storage are relatively easy to chip off and reinstall with hot air. There is usually no epoxy on or under the eMMC and thus removal with hot air at a relatively low temperature for a short duration of time is possible and simple with experience.

3.6.2. In-system-programming (ISP) of Echo Show devices

In-System Programming (ISP) is most often not a "destructive" process or procedure. The exception to that general assumption is that the device is not damaged during the tear-down process, the soldering to ISP locations, or the reassembly of the device after extracting the data. The likelihood of damage occurring during any of those activities is dependent on the experience of the examiner and the design of some devices which can make some or all those steps challenging and difficult. We were able to pin out and successfully use ISP to extract data from all the Echo Show devices. Diagrams and tear-down video guides are available for each device and procedure including tear-down and the ISP procedure. We used the Z3X Easy JTAG Pro Plus[4] flasher box for our extractions via ISP, but other flasher boxes are just as reliable at performing the same function.

3.6.3. Modification of Echo Show devices for repeated ISP laboratory tests

During our repeated seeding and testing we wanted to be able to have quick access to data and specific files stored on the Echo Show devices across multiple tests for the economy of time. To avoid repeated tear-downs and reassembly of the devices for ISP extractions, we installed a permanent method for accessing the device via an external quick-connect method. We soldered permanent wires to the ISP locations inside the device and routed the wires to the outside for quick, solderless attachment to the flasher box adaptor. The wires were enameled 32AWG and we attached color-coded male breadboard jumper connectors for plugging into a Z3X Easy JTAG Pro Plus flasher box adaptor. We used a permanent connection of ISP wires extended to the outside used this method to permanently connect an ISP adaptor, commonly used with the Z3X flasher box, to the Echo Show 5 to serve the same purpose. These modifications allowed us to seed a device with a singular activity, like sending a message or setting an alarm, and immediately retrieve specific files for quick analysis via ISP without any device disassembly or soldering. If properly installed, these modifications do not interfere with the normal operation of the device. Connection to the device via ISP is still accomplished while the device is in the off-state. Whether only retrieving specific files or a complete physical dump via ISP, the procedure is forensically sound and does not alter the performance of the device or the data stored on the device. If the ISP locations are not connected to the Z3X flasher box, the Echo Show device powers on and work normally when the power supply is connected. If the wires are connected to the Z3X box when plugging in the power adapter to the Show device, the device will not boot but instead is appropriately powered for an ISP connection and extraction. This method was not used on the Echo Show 10 (3rd Generation) running two eMMC storage chips.

4. Amazon IoT devices

All the Amazon Echo Show devices have a screen. The Show devices are identified as the Knight Family of devices by Amazon. They have no battery and thus are not running if not plugged into AC power. They all come with an AC power adaptor which is useful during some ISP procedures. In seizing the device, make sure to include the power adapter for ISP or manual inspection of the device by powering it on after a physical dump. There are two unique "model" numbers associated with each Echo Show device and these devices are sometimes identified on listserves by either or both. The identifying model number on the outside of the device is what our lab refers to as the external model number as it contains letters and numbers. This external model number is not found when searching any part of the physical dump. The other model name has no numbers and is not found anywhere on the outside of the device but is found in several locations of the physical dump, including the build.prop as ro.product.model = . It is used to identify the device in some communication with the Amazon cloud. The external model number is also found in the FCC filings on the internal and external photos and various other PDFs on the FCC website. This external model number is located next to the FCC ID number displayed on the outside, the bottom of the Echo Show devices. The digital serial number is unique to each individual device, even of the same model, and is also displayed on the bottom of all the Echo Show devices except the Echo Show 1st Generation which displays the external model number and FCC ID but no serial number. See Table 1 for identifying each device. The complete list of ISP diagrams and tear-down videos of the Amazon devices involved in this study is publicly available on Zenodo (Lorenz et al., 2022).

4.1. Amazon Echo Show functionality

Reviews for Amazon Show devices have pointed out that the Echo Show is just an Echo smart speaker with a screen (Gil, 2017). The Show devices still rely heavily on voice interactivity, but the screen does allow the user to access the settings menus, swipe through news and weather, and navigate through menus retrieved via voice commands, like Prime Video. We were able to send messages on Echo Show devices using the touchscreen keyboard or voice. You can also use the touchscreen to surf the internet including scrolling through search hits and typing web addresses or search terms into your choice of browsers – either Silk or Firefox. The screen means the user can view the result of their web searches instead of being restricted to having them read aloud by Alexa on Amazon devices with no screen. For the tests we ran for this research, we used the screen and voice commands, independently and combined, for interaction with the device. All the Show devices have 8 GB eMMC storage which allows the storage of user-created photos saved to Amazon photos. We viewed the additional functionality created by the screen from a forensic examiner's point of view and is one of the reasons we decided to focus on this family of devices in this research. The addition of the touchscreen means that this device is easily capable of storing both contraband and mere evidence – content and metadata. The addition of the touchscreen to Echo Show devices has important implications for forensic examiners detailed in this initial paper and distinguishes the Show family of devices from other Amazon IoT devices which have no screen. There is evidence in the form of metadata which can be located on the Show devices but will not be found on other Amazon devices without a screen.

In this section, we present the tear-down and ISP of the Echo Show devices we used in our experiments. For those who are experienced with using ISP, Table 1 provides all the information needed to extract the seven models of the Echo Show and the Echo Spot. A link to a detailed diagram of each device is available with tear-down steps, ISP locations, and flasher box settings. There is also a tear-down video guide for each device which covers each step of the tear-down process and ISP procedure. The tear-down of devices to access ISP locations can sometimes be the most

[4] https://easy-jtag.com/.

challenging part of the ISP procedure. Heat shields can sometimes be tough to remove without damaging the device. Having a video to view in advance can help reveal some of the traps which may not be recognized or easily visible when disassembling the device for the first time. Disassembly of some of the Echo Show devices can be time-consuming and difficult.

4.2. Amazon Echo Show (1st generation)

The Echo Show 1st Generation was released in June of 2017 and was the first Echo device with a screen (Weinberger, 2017). It is referred to as the Echo Show or the Echo Show 1st Generation. The product name found in the build.prop (ro.product.name =) is knight. Thus, each Echo show device is part of the Knight family of Amazon devices. Tear-down of the Echo Show 1st Generation is the most challenging and labor-intensive of all the Show devices. We make that statement even while considering that there is no exposed CLK on the Echo Show 2nd Generation and ISP of that device required surgery on the logic board. The tear-down of the Echo Show 1st Generation to access ISP locations rates as challenging and labor intensive even when compared to most phones and tablets we have examined using ISP. Heat is required to remove the digitizer which is necessary to access screws for the tear-down. There are some pitfalls including ribbon cables in awkward positions which make tear-down and especially reassembly frustrating and almost a two-person job in some steps. There are two heavily armored heat shields that must be removed to access ISP locations. We were able to ISP this device and reassemble it with full functionality for further testing. There are several methods for removing heavily armored heatshields which are soldered to the board. The difficulty of this task is sometimes overlooked by examiners who may not have had much experience with ISP. In the tear-down video guides of the Echo show 1st Generation, we elected to cut away part of the heat shield to expose ISP locations. This may not be the best or the easiest method to access the ISP points and some examiners may opt to remove the heatshield completely via hot air or careful prying as we do with some devices. Some devices can have overheating issues when reassembled and used if significant portions or all the heat shields are removed. Since this device was to be continually used for testing, we elected to leave most of the heat shields in place.

4.3. Amazon Echo Spot

The Amazon Echo Spot was included in our research as it is the only other Amazon IoT device with a screen. The Echo Spot is not part of the Knight family as is the Echo Show device. The Echo Spot is part of the Rook family but is the only device in that family. Tear-down of the Echo Spot is challenging as there are many different steps and some hidden secrets that make tear-down without damaging the device difficult. We have created a clear tear-down video for the Echo Spot that reveals these hidden issues. The logic board is sandwiched between parts of the inner frame and it is necessary to remove it to access the ISP locations.

4.4. Amazon Echo Show (2nd generation)

The Echo Show 2nd Generation is also referred to as the Echo Show 10. It has the largest screen of the Echo Show devices and excellent sound quality. While the Echo Show (2nd Gen) tear-down is not as difficult as the Echo Show 1st Generation, it still has its challenges that do not exist on the Echo Show 5 and Echo Show 8. It was released in October 2018 and runs the same processor as the Echo Show 1st Generation. The Tear-down of this device does not require heat and is much easier that the Echo Show 1st Generation.

Table 1
Amazon IoT devices with a screen.

RETAIL NAME	Echo Show (1st Gen)	Echo Spot	Echo Show (2nd Gen)	Echo Show 5	Echo Show 8	Echo Show 10 (3rd Gen)	Echo Show 10 (3rd Gen)	Echo Show 5 (2nd Gen)	Echo Show 8 (2nd Gen)
Release Price	$229.99	$129.99	$199.99	$79.99	$109.99	$249	$249	$84.99	$129.99
Diagram	YES	YES	YES	YES	YES	YES	YES	YES	YES
Video Tear-down	YES	YES	YES	YES	YES	YES	YES	YES	YES
FCCID	2AETL-0725	2ALBE-0301	2ANZL-2474	2ARIV-2425	2ARO5-7879	2AUPE-8959	2AUPE-8959	2AXW2-3476	2AWTZ-8462
External Model #	MW46WB	VN94DQ	DW84JL	H23K37	C7H6N3	T4E4AT	T4E4AT	C76N8S	A8H3N2
Internal model	AEOKN	AEORK	AEOBP	AEOCH	AEOCW	AEOTA	AEOTA	AEOCN	AEOAT
Screen	7”	2.5” Circular	10.1” HD	5.5”	8”	10.1” HD	10.1” HD	5.5”	8”
Released	June 2017	Sept 2017	Oct 2018	June 2019	Nov 2019	February 2021	February 2021	June 2021	June 2021
Processor	Intel Atom x5 Z8350	MediaTek MT8163V	Intel Atom x5 Z8350	MediaTek MT8163V	MediaTek MT8163V	MediaTek 8183V	MediaTek MT8512 AZ1	MediaTek MT8163V	MediaTek MT8183V
Storage	8 GB eMMC	8 GB eMMC	8 GB eMMC	8 GB eMMC	8 GB eMMC	8 GB eMMC	4 GB eMMC	8 GB eMMC	8 GB eMMC
Encrypted	**NO**	**NO**	**NO**	**NO**	**NO**	**NO**	**NO**	**NO**	**NO**
Extraction Type	physical	physical	physical	physical	physical	physical	physical	physical	physical
Extraction Method	ISP	ISP	*ISP (surgery)	ISP	ISP	ISP	ISP	ISP	ISP
Device Family	KNIGHT	ROOK	KNIGHT	KNIGHT	KNIGHT	KNIGHT	KNIGHT	KNIGHT	KNIGHT
Device Type	A1NL4BVLQ4L3N3	A10A33FOX2NUBK	AWZZ5CVHX2CD	A4ZP7ZC4PI6TO	A1Z88NGR2BK6A2	AIPK7MM90V7TB	AIPK7MM90V7TB	A1XWJRHALS1REP	A15996VY63BQ2D
OS	5.1.1	5.1.1	5.1.1	7.1.2	7.1.2	9	7.1.2	9	9
Internal name	knight	rook	bishop	checkers	crown	theia	mopac	cronos	athena
ro.build.id=	LVY48F	LVY48F	LVY48F	NS6541	NS6541	PS7542	NS6542	NS6547	PS7547

Heat shields are easily removed as they are only snapped onto heat shield frames and come off with a fingernail. The one hitch is that there is no exposed CLK which is needed for an ISP connection. All other ISP locations are faceup when tearing the device down to the logic board. Youn et al. (2021) conducted research on the Echo Show (2nd Generation) and extracted data from the hardware of the Echo Show by using the chip-off method to extract data from the eMMC storage. Youn et al. (2021) also conducted experiments based on a hypothetical case and examined data from a mobile device and the cloud related to the use of the Echo Show 2nd Generation. They were able to recover logs from the hardware of the Echo Show related to user interactions with the IoT device. This log data was consistent with our observations and results across the entire family of Echo Show devices we tested. We still wanted to provide ISP access to Echo Show (2nd Generation) as a non-destructive alternative to chip-off for examiners. Understanding how the eMMC and processor are connected under the top layer of the logic board and a lot of experience with board surgery on many other devices helped with this endeavor. We have provided a method to expose the CLK line using a technique that does not damage the functionality of the device and allows for a sTable ISP connection as shown in Fig. 2.

The technique requires the careful removal of the top layer of circuit board material to expose the traces on the layer underneath to access the CLK line for ISP. Removing the heat shield frame next to the eMMC storage removes the ground plane. Then using a soldering iron, the composite material can be carved away revealing the CLK line. The entire process is demonstrated in the tear-down video for the Echo Show (2nd Generation). So, while we still refer to this technique as non-destructive using our previous definition of destructive, it is still challenging and can be destructive if not done properly because it requires some precision work and soldering. A detailed diagram is provided and the entire procedure for tear-down, exposing the CLK line, and ISP extraction is provided for review. The device still functions normally for our lab tests after this procedure and has been in constant use for months after surgery.

4.5. Amazon Echo show 5

The Echo Show 5 is so named because it has a 5-inch screen. Even though it was manufactured in June of 2019 it is not considered the next generation of the original Echo Show 1st and 2nd Generation. It is merely a small, cheaper alternative to the two original Show devices. It runs 8 GB eMMC storage but runs a MediaTek processor with a much less robust sound system. Tear-down of this device is much easier than the 1st and 2nd generations and ISP locations are easily identifiable pads, but the design of the device does require the logic board to be flipped to access the ISP pads. Soldering is much easier compared to the 1st and 2nd generations.

4.6. Amazon Echo Show 8

The Echo Show 8 is also not considered a continuation of 1st and 2nd generation of Show devices and is just referred to as the Echo Show 8. It was released in November of 2019 and has an 8-inch screen and much better sound than the Echo Show 5 due to the larger size and more robust speakers. The tear-down of the Echo Show 8 is somewhat like the Echo Show 5 and it has the exact same ISP pinout pads as the Echo Show 5. The ISP pads on Show 8 are even labeled the same as Show 5. But there are significant differences in the tear-down and preparation for ISP.

4.7. Amazon Echo Show 10 (3rd generation)

The newest Echo Show is named the Echo Show 10 (3rd Gen) and thus a continuation of the 1st and 2nd Generation but with significant design differences and hardware. Press releases for the device appeared in early to mid-2020. The device was available for pre-order and shipped in late February 2021. The device is priced at $249 and has 13 MP camera and a screen designed to turn and pan the room or follow the user while they interact with the device. Amazon and MediaTek have partnered for the development a processor installed on this device with use of a MediaTek main processor and a second Amazon AZ1 Neural Edge processor (Faulkner, 2020). Most of the speech recognition will be done on

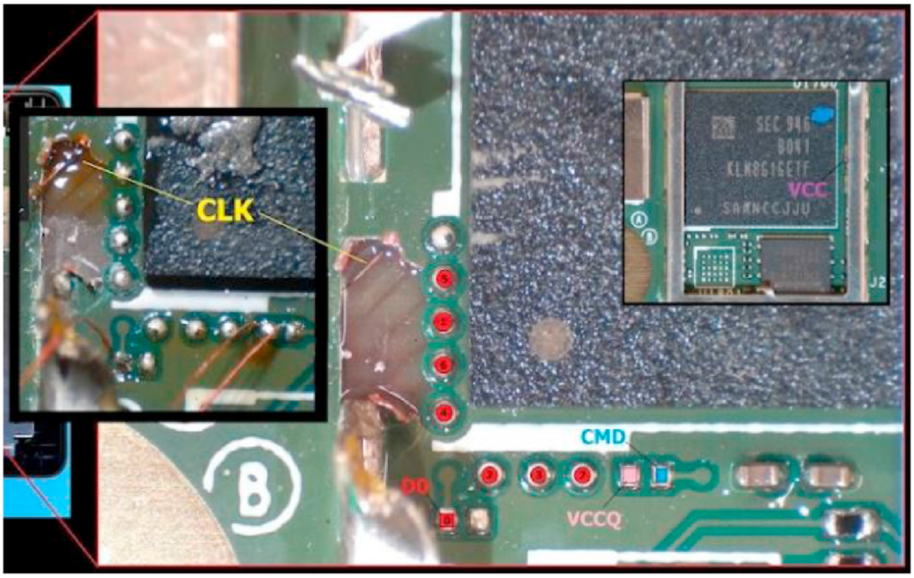


Fig. 2. ISP of echo show 2nd generation.

this new Echo Show 10 instead of streamed to the Amazon site and processed. Amazon's press release states that the device was designed with privacy in mind with audio and vision "all processed locally and securely on device …" (Amazon, 2020). Our analysis of the Echo Show 10 (3rd Generation) identified two separate MediaTek processors and two eMMC storage chips. After significant teardown, pinning, seeding, and testing this device we were able to determine the effect of Amazon's new AZ1 processor related to storage of metadata and content. We have a complete diagram of the logic board available detailing two ISP pinouts – one for each eMMC storage. Fig. 3 shows the hardware and ISP locations for the Echo Show 10 (3rd Generation), and Table 2 describes the location of data also for the Echo Show 10 (3rd Generation). This 3rd Generation Echo Show boots and functions using a MediaTek MT8183V processor connected to 16 GB LPDRAM and 8 GB eMMC storage. There is a separate MediaTek MT8512BAAV processor which contains Amazon's new AZ1 Neural Edge processor which is connected to 8 GB LPDDR4 Ram and a 4 GB eMMC storage. The new AZ1 processor and its connected 4 GB eMMC storage perform a separate function from the primary booting and standard operations of the MT8183V and its connected 8 GB eMMC. These processors run independently and came installed with different versions of Amazon's Fire OS. We were able to determine that Amazon's use of the MT8512 with the AZ1 Neural processor appears to perform as stated in their press releases. Thus, with more processing being done "locally" with the more advanced AZ1 processor, some user data was stored on its connected 4 GB eMMC.

4.7.1. Additional content stored on the 4 GB eMMC

The privacy to which Amazon refers means less user data is pushed to the cloud for analysis and more data recognition and learning performed with the AZ1 processor. This means that the 4 GB eMMC now contains user content needed for this processing to occur quickly and locally. This user content is not present on previous versions of the Echo Show or on the 8 GB eMMC on this same device. Thus, an analysis of both eMMC storage chips is beneficial for obtaining metadata and user content on this latest device. In the initial analysis we were able to locate actual names of contacts on the 4 GB eMMC and the actual content of lists we created during seeding. The addition of new Alexa Skills also means more user data is being stored on the 8 GB eMMC, including email addresses and content. Through a series of tests and configurations we were able to boot this device and add metadata and content to the 8 GB eMMC storage while freezing out the functioning of the AZ1 processor and its connected 4 GB storage. With each test, a full physical image was obtained from both the 8 GB eMMC and the 4 GB eMMC using ISP pinouts we identified. With our configuration we locked out the 4 GB eMMC so that the hash value remained consistent across each seeding test while we changed and added content to the 8 GB eMMC during normal user interaction. This was accomplished by shorting the AZ1 and the 4 GB eMMC's CMD line to ground, which caused the AZ1 and 4 GB eMMC to become unresponsive, or frozen, thus keeping any data from being modified on the 4 GB eMMC storage. The device did not need the AZ1 or its attached storage to boot or perform, like other previous models of the Echo Show devices. This demonstrated that the device is capable of booting, functioning, storing metadata and content on the 8 GB eMMC without changing 1 bit of information on the 4 GB eMMC – with our modifications. Without our modification, the AZ1 and 4 GB eMMC perform the more advanced functions of identifying audio and video and rely on gathering and storing some user content on the 4 GB eMMC to improve this process and the user experience.

4.7.2. Seeding files with specific user data

We identified several files on the 4 GB eMMC which were storing user content we created during our testing of the Echo Show 10 (3rd Generation). Once we identified these locations, we were able to consistently add user content to these locations by creating named list and adding specific items to this list. We used several different scenarios which could be related to criminal investigations to include a list titled "Making Meth". Specific words and instructions were added to this list which do not appear on the 8 GB eMMC and did not exist in these specific files before we added them to our lists.

After each seeding of the Echo Show 10 (3rd Generation) we used the ISP method to extract a full physical image of the 8 GB eMMC and the 4 GB eMMC. User content and metadata can be found on both chips, but some data is unique to each chip. We created 17 separate lists under one of our user accounts using

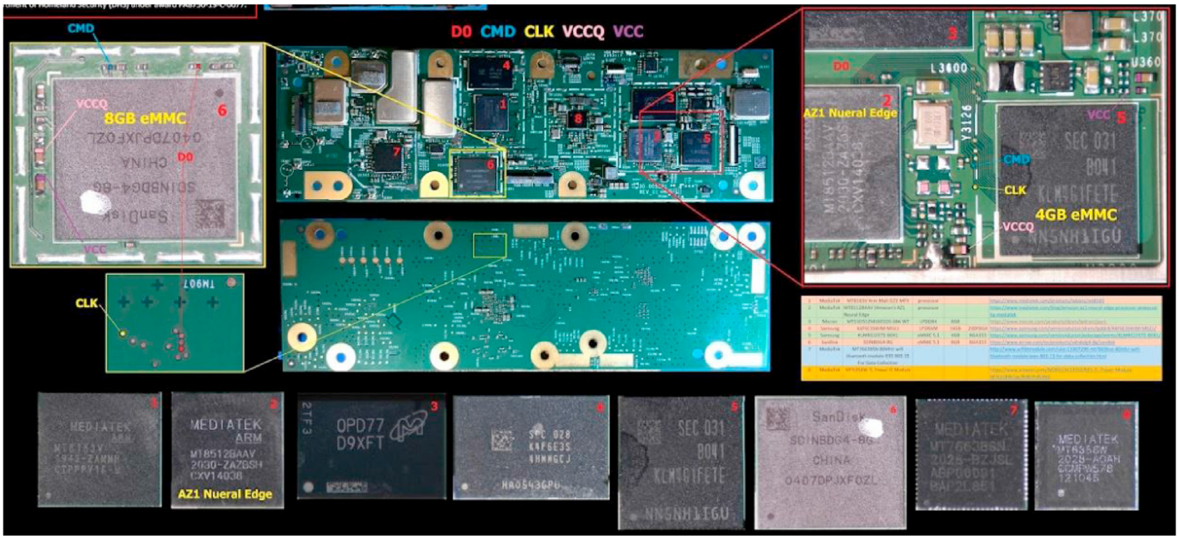


Fig. 3. Hardware and ISP locations for the Echo Show 10 (3rd Generation).

Table 2
Location of data on Echo Show 10 (3rd Generation).

Content and Metadata	MT8183V 8 GB eMMC	MT8512/Amazon AZ1 4 GB eMMC
Logs documenting date and time user interacts with the device.	✓	×
Internet search history.	✓	×
Email content.	✓	×
Screenshots, user photos.	✓	×
User created lists and items on each list.	×	✓
List of Smart Devices under user account.	✓	✓
Content of reminders.	✓	✓
Alarms.db.	✓	×
Phone call times and number called.	✓	×

different Amazon devices. We also added items to these lists using the Alexa App using an iPhone. We discovered the names of each list we created and the items on each list in one file on our Echo Show 10 (3rd Generation) test devices. We were able to determine that user content generated under our account would appear on the 4 GB eMMC in the following location:

```
data\alexahybrid\files\AmModel\nlu-person-
alized.OFFLINE.en-US.7.125\vocab.syms
```

These tests demonstrated that the newest of the Echo Show devices with the AZ1 processor stored user content created on other IoT and devices with the Alexa app. With previous Echo devices we were only able to find content and metadata on the Echo device which was used to create the data. As an example, we added words like “methocarbamol” to our Pharmacy list. Prior to our seeding, we extracted physical images from the 8 GB and 4 GB eMMC. We used ENCASE to process the images and conduct keyword searches. Prior to seeding, we only found one hit for “methocarbamol” on the 4 GB eMMC in a master word list (asr_data\words.txt) that is approximately 32 MB in size and appears to contain just about any word you can find in a dictionary or on the Internet. There were no other hits on the 4 GB eMMC or the 8 GB eMMC. After creating our Pharmacy list which included “methocarbamol” as an item, we found three (3) hits for methocarbamol, with two new hits - one in each of the following files:

- 4 GB data\alexahybrid\files\AmModel\nlu-personalized.OFFLINE.en-US.7.125\vocab.syms (8.3 KB file size)
- 4 GB data\alexahybrid\files\AmModel\spectrum-nlu-personalized.df194f18e6422fd00f35df7f2a8b1917.en-US.7.123\vocab.syms (7.1 KB file size)

We were able to find the name of each of the 17 lists we created and every word of each separate line of our lists inside these vocab.syms files. The vocab.syms files also contained names of contacts from email accounts tied to our Amazon account along with the “friendlyname” of our Amazon devices which was our unique inventory number from Amazon devices in our lab, e.g. “A815 Amazon Echo Show 10”. The names of the lists and items on the lists created by the user were only stored in the vocab.syms files on the 4 GB eMMC.

4.7.3. *Alexa’s attempt to become familiar with the user*

Our hypothesis that the vocab.syms file represents Alexa’s attempt to become familiar with the user is based on our tests and Amazon’s own statements about the purpose and abilities of the AZ1 processor, which is privacy and speed due to more processing on the device and less processing in the cloud. The device and Alexa are faster and more responsive, having a personalized list of words, related to the user, stored on the 4 GB eMMC and connected to the AZ1 processor. This file did not exist at unboxing with our ISP analysis, and it grows with user interactions and only contains personal contacts, and words, which can be modified over time. Lists not created on our test device were also found in the vocab.syms files, indicating Alexa uses data created on other devices and locations related to the same user account. We surmised this file is related to audio, specifically items of the list being read aloud by Alexa at the request of the user, e.g., “Alexa, read me my pharmacy list.” Items from the pharmacy list did not appear in the vocab.syms file until we requested Alexa read the list aloud. There may be exceptions to this as we found names of contacts from our associated email account which appeared in this vocab.syms file even though we had not requested all emails or contacts to be read aloud.

4.8. *Echo Show 5 (2nd generation)*

The Echo Show 5 (2nd generation) has the same logic board and ISP pinout as the first generation of the Echo Show 5. Considering the minor differences in the tear-down of the devices, we created only one tear-down video guide for both generations of the Echo Show 5. On the other hand, we created a separate ISP diagram for the Echo Show 5 2nd generation because it has different specs (e.g. FCC ID, model #,internal model, etc.) compared to the 1st generation.

4.9. *Echo Show 8 (2nd generation)*

The Echo Show 8 (2nd Generation) has a similar tear-down process to the first-generation version but has a different logic board and pinout. We created a separate tear-down video and diagram for this device.

4.10. *Example of tear-down video guides and diagrams*

In this subsection, we describe how to use tear-down videos guides and diagrams. The tear-down video guides and diagrams are designed to provide a visual reference and a step-by-step guide for forensic examiners and practitioners. We created a diagram and a video for each device covered in this paper. The diagrams are designed to provide a comprehensive overview of the entire process involved in extracting data from the IoT device. This process starts with the orderly disassembly of the device to access the logic board and expose the locations needed to connect to the device for In-System-Programming (see Fig. 4).

The diagram will also include a magnified photograph with each point necessary for ISP connection clearly marked (see Fig. 5). The video of each procedure shows the step-by-step process from disassembly to soldering for ISP connection and is a very helpful

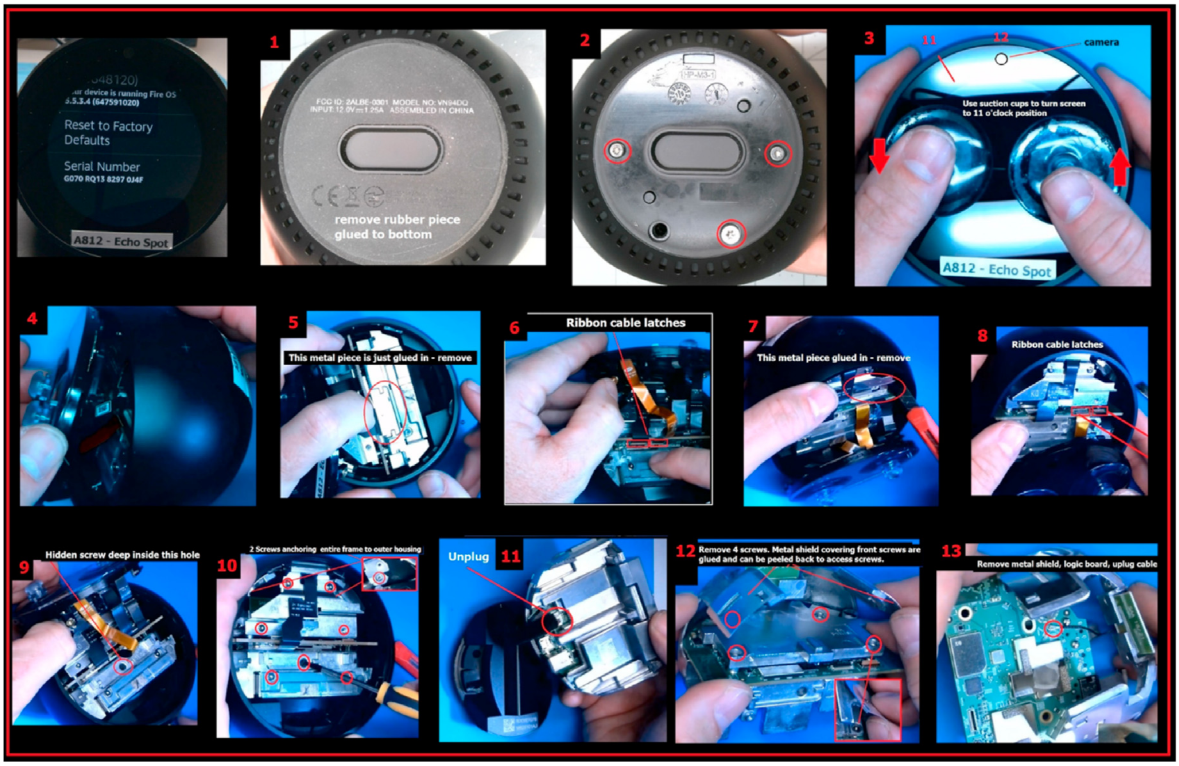

548120)
ur device is running Fire OS
5.5.3.4 (647591020)
Reset to Factory Defaults
Serial Number
G070 RQ13 8297 0J4F
A812 - Echo Spot
1
FCC ID: 2ALBE-0301 MODEL NO: VN94DQ
INPUT: 12.0V 1.25A ASSEMBLED IN CHINA
remove rubber piece glued to bottom
2
3
11
12
camera
Use suction cups to turn screen to 11 o'clock position
A812 - Echo Spot
4
5
This metal piece is just glued in - remove
6
Ribbon cable latches
7
This metal piece glued in - remove
8
Ribbon cable latches
9
Hidden screw deep inside this hole
10
2 Screws anchoring entire frame to outer housing
Unplug
11
12
Remove 4 screws. Metal shield covering front screws are glued and can be peeled back to access screws.
13
Remove metal shield, logic board, uplug cable

Fig. 4. Step-by-Step tear-down of Amazon Echo Spot.

visual of the entire process described in the companion diagram. The diagram and video are designed to be used together by forensic examiners and practitioners. The entire procedure can be viewed in a clear, high-definition video before beginning the procedure and the companion diagram can be used as a quick reference for examiners during disassembly and soldering.

5. Experimental setup

In carrying out our experiments we used video to document our experiments and device seeding with accurate time stamps. This made it possible to locate files and metadata created or altered by our interaction with the devices. Fig. 6 shows the four-step process we used to conduct the experiments on the selected IoT devices. We describe these four steps in the next sections.

Multiple tests were conducted using the process presented above which can be easily repeated as many times as needed without damage to the IoT device. This allowed modification and follow-up tests based on possible scenarios in which users might interact with the IoT device under normal usage.

As follows, we provide the technical details and testing environment regarding the operating systems of the Amazon IoT devices used in our study.

Amazon operating systems: Amazon Echo devices run an Android-based operating system called Fire OS. Amazon refers to Fire OS as, “a fork of Android” (Amazon, n.d.). There are three versions of Fire OS. Fire OS 5 is based on Android 5.1. Fire OS 6 is based on Android 7.1. Fire OS 7 is based on Android 9. Amazon list all of their Fire TV devices and the corresponding version of Fire OS and Android version online.[5] Amazon Echo devices, including the Echo Show devices, also run Fire OS based on Android. Despite the fact that Amazon devices are based on the Android operating system, they do not follow all of the rules of Android as do most Android-based mobile phones. For the forensic examiner, the most important rule not followed by Amazon devices is default encryption.

Amazon IoT devices encryption: Most Android mobile phones running Android 7, 8, and 9 are encrypted out of the box. Android required devices running Android 6 or higher to be encrypted by default but exceptions existed for devices that did not have the hardware capable of supporting encryption. Amazon Tablets and IoT devices are relatively inexpensive. Many new, inexpensive mobile devices sold with Android 6 or higher avoided the encryption requirement until Android 9 because they were made with relatively inexpensive hardware, and running encryption on those devices would significantly impact their performance. The Amazon IoT devices we tested were running Fire OS 5, 6, and 7 with their corresponding versions of Android. None of the devices were encrypted. There is no method for the user to enable encryption in the settings on any of the Echo Show devices currently released.

5.1. Seed IoT devices

Amazon’s devices are designed for users to primarily interact with them via voice commands which are processed at the Amazon site. Therefore, Amazon IoT devices must be connected to the internet to function. Amazon responds to users after being signaled by the users’ use of a “wake word”. Amazon gives users the choice of several different wake words including Amazon, Alexa, Echo, and Computer. Echo Show devices also allow users to interact with the device via the touchscreen. We use the term “seeding” to describe the process whereby we intentionally interact with the device as a typical user would use the device in an everyday scenario including sending a message, setting an alarm, or other activities in which the

[5] https://developer.amazon.com/docs/fire-tv/fire-os-overview.html.

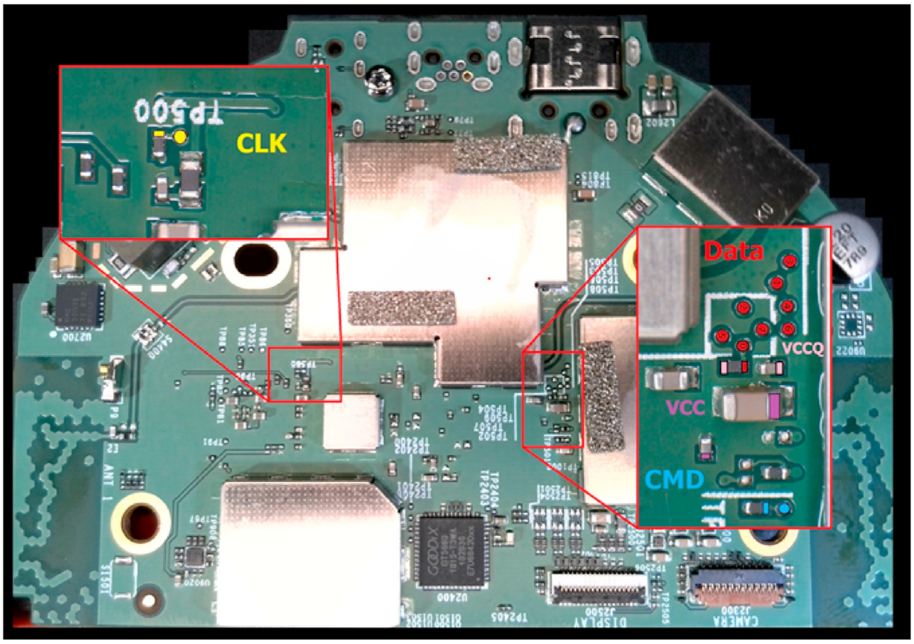
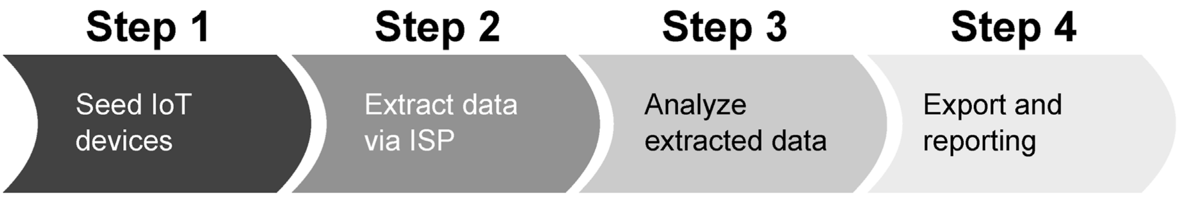


Fig. 5. In-system-programming locations for the amazon echo spot.



We interacted with the IoT devices with the intention of seeding them with evidences and leaving traces of user interactions

We extracted data from the eMMC of the IoT devices via In-System Programming

We analyzed the extracted data to document any data created and stored on the eMMC during our controlled seeding

We used forensic software and python script to parse, export, and report relevant data recovered from the IoT devices

Fig. 6. Experimental process.

device responds to the user's voice commands or contact with the touchscreen. Our controlled tests involved voice commands and interacting with the device through the touchscreen to determine if evidence of our interaction was stored on the eMMC storage.

5.1.1. *Seeding methodology*

From the previous examination of Amazon IoT devices, we knew there was not much user content stored on the eMMC. However, with the Echo Show devices, there are exceptions to that general rule and because the Echo Show devices have a touchscreen, there is more user content related to photos and internet browsing likely. Using newly added Alexa Skills, we added email accounts that can be checked with requests to Alexa. This skill added email contacts and email content to the IoT storage. Making phone calls with the IoT device also added phone numbers and times of calls. With our experiments, we wanted to make sure we also examined the devices thoroughly for non-content related user interaction – metadata. The most obvious method for looking for metadata is based on the time of the interaction with the device. To create an accurate record, we video-recorded device seeding with precise time displays to allow for targeted searches for evidence across the physical extraction after ISP. With each seeding procedure, we set up a video to record our interaction while displaying time in local, daylight savings time, UTC, and UNIX accurately to the millisecond. After the seeding procedure we could move frame by frame through the video to determine the precise time of our interaction, e.g., using our finger to touch the screen. The image showing the clicking of the gear icon to open settings in Fig. 7 demonstrates how accurate the device logs are in recording user interactions with the IoT device. These videos with the precise time displayed were crucial in locating the metadata associated with our interactions. Having the time-stamped video to review, provided us with a high degree of confidence that our interpretation of the metadata is correct. We believe that the video recording of our seeding will also allow other examiners to see a clear demonstration of our methodology, conclusions, and how these devices are typically used related to data recovered during a forensic exam.

5.2. Extract data via ISP

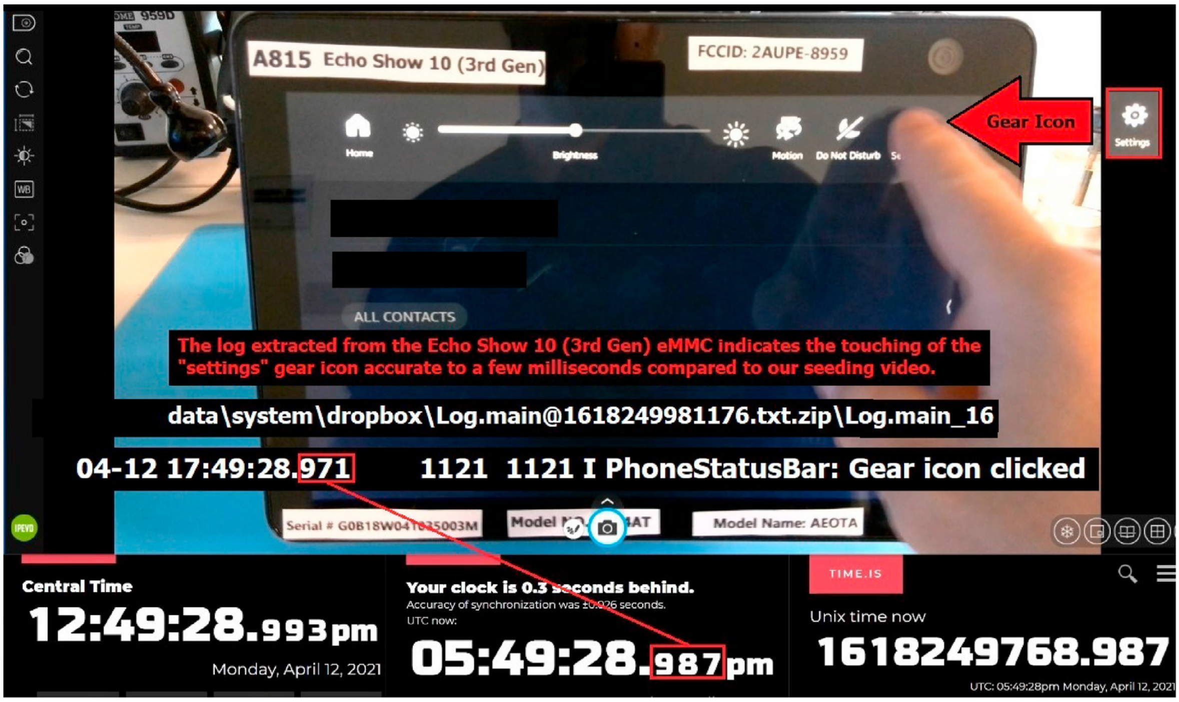
Amazon Echo Show devices do not have a battery and will not function if unplugged from an outlet. It is possible to shut down Echo Show devices by pressing the mute button and holding it for several seconds until a message on the screen asks if you want to shut down your device. Selecting “okay”, with your finger, will power down the device even though it is still connected to an outlet. Powering on the device is accomplished the same way. Holding down the mute button for several seconds will boot the device. Plugging an Echo Show device into an outlet will automatically power on and boot a device. Shutting down the device with the mute button and screen creates metadata in log files that a user creates by depressing the mute button and touching the screen. Securing the crime scene by securing the IoT device Accidently using the wake word verbally by anyone in proximity of an Amazon IoT device can create log data also, and brief recorded audio of what is occurring at the crime scene when the wake word is triggered can be stored in the user’s account just like any other verbal request made intentionally. These are considerations for the investigator when entering a crime scene with IoT devices and for any manual inspection of devices that create log files documenting human interaction with the device menus including Touch Events and menu selections.

5.2.1. Seizing the amazon IoT device

Our preferred method of collecting Echo Show devices is to forgo the shutdown process and just unplug the device from the electrical outlet. Amazon Show devices do store some content and metadata, but they also delete content and metadata after certain events like the delivery of a scheduled message or after an unspecified period or usage of the device. Metadata created and stored in zipped device logs are eventually deleted. In our testing of devices, logged events we created and recovered via ISP disappeared from the device after continued future use. We were able to recover some device logs by carving for zipped headers and footers in unallocated space, but only to a limited degree. Without knowing precisely when these deletions occur it is our preference to forgo shutdown procedures and just remove power from the device. If there is no planned and legally permissible manual inspection of the IoT devices at a crime scene, this power disconnection should be done as soon as possible to avoid unintentional logged events and possible deletion of older logged files. Our subsequent physical extraction of the eMMC is done without powering on the device and thus we avoid unwanted contamination of the device by disconnecting and depriving the device of power.

5.2.2. Storing the IoT device and data

Extraction via ISP while the device is in the off-state, avoids altering any data present when the device had power removed and is the most complete, forensically sound method of collecting data from Echo Show devices. The IoT device can be stored in evidence in the exact condition it was seized and future physical extraction via ISP will yield an identical extraction with the same hash as the original exam performed by the examiner when the device was seized. It may also be advisable to package and mark the power adaptor with a warning not to power on the device. The power cord can be used during an ISP procedure without powering on the device, providing all ISP points are connected to a flasher box and the box is grounded to the device or connected to USB. Amazon IoT device with a screen will not boot if the Data, CLK, or CMD points are grounded or connected to USB via the flasher box. Accidental booting of the IoT device can occur even if the examiner is not aware of these conditions. This is especially true with the Echo Show 10 (3rd Generation) as we were able to boot the device using one processor and its OS on the connected 8 GB eMMC, while simultaneously extracting data from the 4 GB eMMC connected to the AZ1 processors, via ISP. Our recommendation is to extract both eMMC chips powering only through ISP connections.



[redacted]

[redacted]

The log extracted from the Echo Show 10 (3rd Gen) eMMC indicates the touching of the "settings" gear icon accurate to a few milliseconds compared to our seeding video.

```
data\system\dropbox\Log.main@1618249981176.txt.zip\Log.main_16
04-12 17:49:28.971      1121  1121 I PhoneStatusBar: Gear icon clicked
```

Central Time
12:49:28.993pm
Monday, April 12, 2021

Your clock is 0.3 seconds behind.
Accuracy of synchronization was ±0.026 seconds.
UTC now:
05:49:28.987pm

Unix time now
1618249768.987
UTC: 05:49:28pm Monday, April 12, 2021

Fig. 7. Touch events logged on Echo Show devices.

5.3. Analyze extracted data

When it comes to forensic tools for the analysis of IoT data, there is no single tool that will provide everything needed to examine the data from every device. A recent study by Alenezi et al. (2019) used a set of commercial tools like Encase and FTK but, at the same time, the authors acknowledged that there is no one tool that is capable of doing everything very well when it comes to forensic analysis. After seeding Echo Show devices and then extracting the data using the ISP procedures detailed in this paper, we analyzed the data and conducted searches for evidence of our interaction with the device. We used the Z3X Plus hardware for extracting the data via ISP and the Encase and Cellebrite Physical Analyzer software to parse and examine the data.

5.4. Export and reporting

There are multiple forensic tools that can be used for processing and analysis of the physical extraction and we used more than one. For most of our analysis of the physical dumps from the Echo Show devices, we used ENCASE Forensic.[6] Because of the location and type of data, we determined ENCASE to be the best tool in our lab for this specific task, especially conducting keyword searches inside zipped files after processing the image with ENCASE. Our initial research in this paper does not focus on tool comparisons so our choices regarding tools do not reflect an exhaustive comparison of their performance with IoT devices.

5.4.1. Python script

We also used Cellebrite's Physical Analyzer[7] to open and analyze extractions, and developed scripts to extract user account information and device identifier information. Fig. 8 shows the python script applied to Cellebrite Physical analyzer. Our script automatically displays this information on Physical Analyzer's "Extraction Summary" tab. Physical Analyzer does parse some data from Amazon IoT devices when opening the physical image as a generic Android device. Our Python Script goes further into the details which will be needed by forensic examiners, especially when preparing search warrants for the cloud data associated with the Amazon device. Our script carves the Amazon Account number and username associated with the device. It also carves much more detail on the IoT device hardware. We also developed Python Script to carve data from exported script automatically displays this information on Physical Analyzer's "Extraction Summary" tab. We also developed Python Script to carve data from exported IoT logs. Our script carves and organizes specific events we detail later in this paper. These events are metadata created by specific user activity which also include the exact time and date a user touches the Echo Show screen accurate to a few milliseconds as demonstrated in the clicking of the gear icon in Fig. 7. The scripts are available on the CCI-TAMUCT github[8]

5.4.2. Comparing Echo Show devices to other amazon IoT devices without a screen

We performed many different seeding activities across all the Echo Show devices. Even though our initial research was designed to focus on the Echo Show devices, we also tested other Amazon IoT devices during our research. The other devices included the Fire TV Cube, Fire TV Sticks, and Echo Dot. This testing confirmed that our methods of data recovery could be applied to Amazon IoT devices other than the Echo Show. It also allowed us to verify that some data located on Echo Show devices was unique to Amazon IoT devices with a screen, currently only the Knight family and the Echo Spot. We also installed the Alexa App on Android and Apple mobile phones as part of our testing and viewed the results of our seeding through Amazon's API as methods of validating the data we recovered from the IoT hardware.

5.4.3. Preservation of data — separating the internet from the thing

Preservation of evidence starts with decisions to be made at the scene where the device is first identified and collected. Part of the definition of IoT is the Internet. Without a connection to the Internet Amazon IoT devices power on, but do not function as intended. Much of the content available through IoT devices is stored on the Internet and not on the IoT device, with few exceptions. It is important for investigators to understand the relationship of IoT hardware to the Internet and to consider the scope of a search warrant when collecting or viewing evidence on a running IoT device.

5.4.4. Legal considerations for the scope of the search

Contacts and limited message history including message content are available to be viewed during a manual inspection of a running Amazon IoT device with a screen if it is connected to Wi-Fi and logged into the user's account. This will most likely be the condition of an IoT device at a crime scene as they stay perpetually connected to the Internet and to the user's account if the device has power. However, this data is not stored on the IoT hardware, with few exceptions. This means the investigator is potentially viewing information stored exclusively in the cloud, in the user's Amazon account, during a manual inspection. This same information will likely not be present in the data extracted from the device hardware during a physical dump of the eMMC. A manual inspection also means an investigator is creating logged events and files with each touch, swipe, or menu selection. This may also cause older log files to be moved to unallocated space. These are important legal and practical considerations during the execution of a warrant at a crime scene.

6. Experiments

We ran experiments on the following Amazon devices: Echo Show (1st Generation), Echo Show (2nd Generation), Echo Show 5 (1st and 2nd Generation), Echo Show 8 (1st and 2nd Generation), Echo Show 10 (3rd Generation), and Amazon Echo Spot.

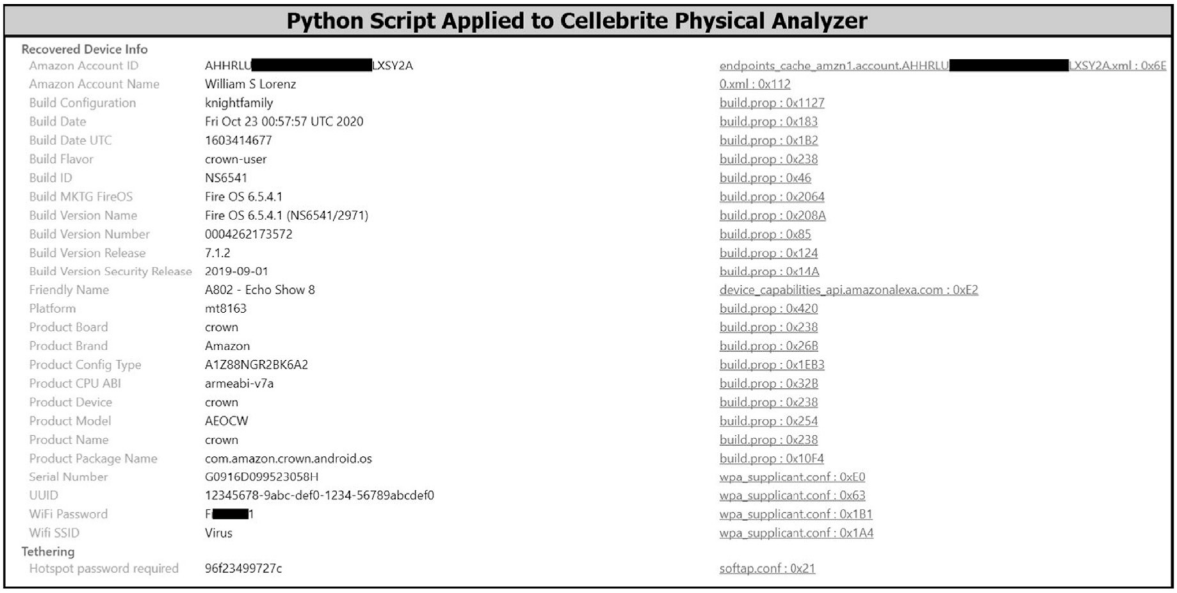
As follows, we discuss the main findings that were identified by carrying out our eight experiments.

(1) **Location of content from seeding experiments.** There is a significant amount of content stored on Amazon devices with a screen. Table 3 shows the locations of content recovered from the eMMC during our seeding experiments. Amazon IoT devices with a screen are designed to display personal photos, and videos, and view streaming content. This means Amazon IoT devices are capable of storing both mere evidence and contraband which can be photos taken or downloaded with a user's mobile phone and stored in the user's Amazon Account. Depending on the IoT device's settings, the user may choose to upload Amazon photos or photos from their Facebook account to the IoT device. All users without a Prime membership get 5 GB of storage for photos and videos. Users with a prime membership are provided with unlimited photo storage and up to 5 GB of free video storage for photos and videos and may share these with up to five other members. It is possible to purchase up

[6] https://security.opentext.com/encase-forensic.

[7] https://cellebrite.com/en/physical-analyzer/.

[8] https://github.com/cci-tamuct/IoT-Forensic-Analysis.



Python Script Applied to Cellebrite Physical Analyzer

Recovered Device Info		
Amazon Account ID	AHHRLU[redacted]LXSY2A	endpoints_cache_amzn1.account.AHHRLU[redacted]LXSY2A.xml : 0x6E
Amazon Account Name	William S Lorenz	0.xml : 0x112
Build Configuration	knightfamily	build.prop : 0x1127
Build Date	Fri Oct 23 00:57:57 UTC 2020	build.prop : 0x183
Build Date UTC	1603414677	build.prop : 0x1B2
Build Flavor	crown-user	build.prop : 0x238
Build ID	NS6541	build.prop : 0x46
Build MKTG FireOS	Fire OS 6.5.4.1	build.prop : 0x2064
Build Version Name	Fire OS 6.5.4.1 (NS6541/2971)	build.prop : 0x208A
Build Version Number	0004262173572	build.prop : 0x85
Build Version Release	7.1.2	build.prop : 0x124
Build Version Security Release	2019-09-01	build.prop : 0x14A
Friendly Name	A802 - Echo Show 8	device_capabilities_api.amazonalexa.com : 0xE2
Platform	mt8163	build.prop : 0x420
Product Board	crown	build.prop : 0x238
Product Brand	Amazon	build.prop : 0x26B
Product Config Type	A1Z88NGR2BK6A2	build.prop : 0x1EB3
Product CPU ABI	armeabi-v7a	build.prop : 0x32B
Product Device	crown	build.prop : 0x238
Product Model	AEOCW	build.prop : 0x254
Product Name	crown	build.prop : 0x238
Product Package Name	com.amazon.crown.android.os	build.prop : 0x10F4
Serial Number	G0916D099523058H	wpa_supplicant.conf : 0xE0
UUID	12345678-9abc-def0-1234-56789abcdef0	wpa_supplicant.conf : 0x63
WiFi Password	F[redacted]1	wpa_supplicant.conf : 0x1B1
Wifi SSID	Virus	wpa_supplicant.conf : 0x1A4
Tethering		
Hotspot password required	96f23499727c	softap.conf : 0x21

Fig. 8. Python script.

to 30 TB of storage with a paid subscription plan. In addition to the photo and video data; the seeding experiments also included syncing address books, adding email accounts, checking email messages, setting reminders, and generating lists. We also tested the device's capability to provide content from the web via web browser and voice command and integrated applications such as Amazon's Ring camera integration.

The Echo Show devices contain a significant amount of metadata. Because these devices have a touchscreen, users can navigate menus and type directly into the device using the keyboard display. The actions generate unique metadata in device logs which can be identified and attributed to direct user interaction with the IoT device with timestamps accurate to the millisecond.

(2) **Log files.** In describing the complexity of IoT devices, Alenezi et al. (2019) stated that it is common for data to be broken up into numerous components and stored in various locations. Using ENCASE Forensic we were able to do keyword and date searches inside zipped log files. The files are located at the following path across all Echo Show devices - data\system\dropbox\. Individual zipped files are located inside the dropbox folder.

Inside each of the zipped log files are individual text files which contain logged events created by device functions and user interaction. The dates and time stamps are in plain text UTC-0, 24-h time in the following format to the millisecond (MM-DD HH:MM:SS:000). The events are line separated with each line beginning with the time stamp followed by codes categorizing the activity and then the actual event description. For example:

```
12-28 19:36:14.398 753 753 I SystemTrayPillView: Touch
event received.
```

This line in the log documented the touching of the screen to type the number "2" in a test message "12345" sent to another Amazon Account user under the name of Robert Paulson via the Alexa messaging app. The message was also received on a mobile phone with the Alexa App under Robert Paulson's account. The number "2" was typed on 12/28/2020 at precisely 1:36:14pm Central Standard Time or 7:36:14pm UTC-0. The frame-by-frame time-stamped video allowed us to freeze the video and precisely locate specific events like this one each time we touched the screen (see Fig. 7). The content of the message sent "12345" is not located anywhere on the physical dump of the Echo Show 5, but the metadata related to the sending of that message is meticulously logged and stored in log files in zipped folders in the dropbox. The "touch event" created by typing the number "2" is in a text file at the following path:

```
data\system\dropbox\Log.main\#221@160918
4485852.txt.zip\Log.main_6.
```

With this message we were able to account for every touch of the device screen when sending the message. With this information, we can target the dropbox folder and carve out all touch events logged when users touched the screen with a script targeting "SystemTrayPillView: Touch Event Received" returning one line in the log starting with the date/timestamp. In applying this knowledge toward a search warrant affidavit for an IoT device located at a crime scene, we can state that Echo Show devices are capable of logging evidence of users interacting with the device and can place some person at the screen of the device accurate to the millisecond. This type of evidence would be considered "mere evidence" depending on the nature and circumstances of the crime being investigated. In a hypothetical scenario it may be evidence that a murder victim was still alive at a particular time or place a potential suspect inside a home at a particular time.

Table 3
Location of Content on Echo Show devices.

Content	Example Location (*** is unique file name)
Email and email content	data\data\com.amazon.cloud9\app_amazon_webview\amazon_webview\databases\https_mail.google.com_0\1
Phone numbers and call times	Unallocated clusters using search term "@amcs-tachyon"
Amazon photos	data\data\com.amazon.zordon\cache\image_manager_disk_cache\***
Screenshot of reminder and content	data\system_ce\0\snapshots\***.jpg
Screenshot from ring video camera viewed via IoT device	data\system_ce\0\snapshots\***.jpg data\data\com.amazon.cardinal\cache\thumbnail-***
Screenshot of video viewed on Google drive	data\system_ce\0\recent_images\45_task_thumbnail.png
Screenshot of Google drive menus viewed in Firefox	data\system_ce\0\recent_images\37_task_thumbnail.png
Screenshot of device menu indicating pairing of bluetooth keyboard	data\system_ce\0\snapshots\37_reduced.jpg
Screenshot message confirmation received	Included the full name of sender and time message was received as displayed on the IoT screen. data\system_ce\0\snapshots\33.jpg
Names and content of lists created.	Only on Echo Show 10 (3rd Generation) on 4 GB eMMC data\alexahybrid\files\AmModel\nlu-personalized.OFFLINE.en-US.****\vocab.syms

(3) **Logged events.** We identified over 7,000 lines of logged events. The actual user involvement with the sending of this message started with the user's finger navigating to the messaging screen on the IoT device touchscreen, selecting the recipient from the contacts list "Robert Paulson", typing the message using the keyboard via the touchscreen, and sending the message. This entire transaction of sending the message took 34 s. This 34 s transaction created 7,229 lines of logged events stored in 33 individual text documents located in two zipped files:

- data\system\dropbox\Log.main#220@1609184164309.txt.zip
- data\system\dropbox\Log.main#221@1609184485852.txt.zip

Table 5 shows the location of selected events from the 7,229 lines of log which have significant identifiable events we can tie to user actions on video while sending the message during testing and seeding. This demonstrates that metadata created by single user events like sending a message or setting an alarm is not confined to one single log file or even a single zipped file. The flow of the timestamps is chronological, and the zipped files are named in part with a UNIX timestamp which helps for narrowing a search.

(4) **Log files triggered by human activities.** There are specific events in the log files which only occur when a human touches the screen or volume and mute buttons of the specific Amazon device. For the investigator, knowing what these events are and how to locate them can be useful in an investigation when trying to determine the presence of a person at a crime scene or that someone was alive and interacting with the device at a particular time. These events were accurate down to the millisecond in our test. The log event "Touch event received" only occurs when we touch the device screen with our finger. That event only occurs on Amazon devices with a screen. The content of messages will not be in these logs, but the metadata associated with the content is there. In our experiment we were also able to recover the Amazon account number of the recipient of messages we sent on all devices except the latest Echo Show 10 (3rd Generation). The username was not identified but the name could be identified with a request or warrant to Amazon to identify and/or search the data associated with the recipient of a particular message via the recipient's Amazon account number in the metadata.

(5) **Using the Echo Show touchscreen keyboard.** Opening and using the touchscreen keyboard on any of the Echo Show devices is logged as an event in the device logs.

```
12-28 19:36:08.646 753 753 I ANCHDN.StateMachine:
afaef40: state transition CLOSED −KEYBOARD_OPENING
−¿ NON_INTERACTABLE.
```

The log information is explicit, and we confirmed the accuracy of the time log with our video of the event. Typing the message creates a touch event for each character or space as we show in Table 5. After the message is typed using the keyboard, pushing "DONE" on the keyboard sends the message and closes the keyboard. The screen briefly displays "SENDING" as the keyboard fades out. The closing of the keyboard is logged.

```
12-28 19:36:20.520 753 753 I ANCHDN.StateMachine:a-
faef40: state transition NON_INTERACTABLE
−KEYBOARD_CLOSING−¿ CLOSED.
```

(6) **Confirmation of the sent message from the Amazon site.** The message is sent to the Amazon site and then sent to the recipient, in this case Robert Paulson, where it is received on his mobile phone through the Alexa App. Table 4 shows the content of messages and information from Amazon's API. Referring to Table 5, the message is logged under our Amazon account at "time":"2020-12-28T19:36:20.919Z". The time is 399 ms after the keyboard closes on the Echo Show 5. A response code is sent back to the Echo Show 5 and logged 64 ms later indicating the message has been sent.

```
12−2819:36:20.98319687334IACMSClient:Httpresponse
codeforsendMessage:200.
```

The Echo Show device now displays *"Text message sent to Robert Paulson from William"*. This message remains on the screen for several seconds. Further investigation outside the dropbox led us to the "recent_images" folder where we located a screenshot of the sent message confirmation screen stored as a.png file. The file is located at:

```
data\system_ce\0\recent_images\14_task_thumbnail.png.
```

While the content of this message "12345" was not stored on the IoT device there are many pieces of evidence that a message was sent to a specific person. The opening of the keyboard and touch events can even provide clues as to the length of messages by counting the number of touch events before the keyboard closes and the message is sent. These specific logged events contain specific search terms which can be searched and carved across the entire dropbox file to quickly locate metadata indicating specific user activity and interaction with the Echo Show device. We developed a Python script for this purpose.

Searches for the name Robert Paulson yielded no results across the entire eMMC including the zipped files in the dropbox. We can review previous messages received via our Alexa messaging app via any of the Echo Show devices. But the device must be connected to the internet as that message history is retrieved from the Amazon site and not stored on the IoT device itself. There is however another clue in the logs which will reveal the identity of our message recipients.

(8) **Review of the dropbox logs** The video recording of our seeding events with precise time displays allowed us to focus on a few thousand lines of logs created in a few dozen seconds surrounding sending a message. In carefully reviewing the lines of logged events created, we could locate important events which were explicit as to what activity was being logged. For our message "12345" sent to one of our contacts, refer to Table 5 inside the dropbox, zipped file, and text file located at:

```
data\system\dropbox\Log.main\#220@1609184164309.txt.
zip\Log.main_209.
```

The event at 12–28 19:36:03.707, is a single event triggered by selecting the contact "Robert Paulson" during the messaging process. Even though the name of our contact is not found in the event, his Amazon account number does appear as the "recipientCommsId". This author's account number also appears as the "senderCommsId". Of course, we know that by cheating as we created the account for research. But this account number is especially useful for investigators to discover this unique account number and any others identified as the "recipientCommsId". The gathering of these recipient account numbers can be useful when requesting the identity of their owners from Amazon during the investigation (see Table 5. Note that this event starts out as a TouchEvent in the log, which was created when a finger contacted the Echo Show 5's touch screen and selecting Robert Paulson as the

Table 4
Content of messages and information from Amazon API.

(7) **Carving for other user's accounts in the dropbox logs.** In our analysis of the Echo Show device hardware, we wanted confine our searches for clues to the IoT hardware only. Of course, we did confirm the message was received by cheating – having access to our own account and login information. We also had access to Robert Paulson's account information and mobile device as we created that identity for testing purposes and confirmation. From our analysis of Echo Show IoT devices, we can say with a good degree of certainty that no "content" related to messages is stored on the IoT device eMMC. Unlike mobile devices with messaging apps, there is no SQLite database for message content on the Amazon IoT devices we tested. We also did not find any contacts, which we created in the Alexa app on our mobile device, stored on the Echo Show devices or that came from contacts we imported into our Alexa app on our mobile device.

Location of Data	Text files	Lines of Log inside Zipped Text Files from 8 GB eMMC Extracted Via ISP	User Actions
https://alexa-mobile-service-na-preview.amazon.com/users/amzn1.comms.id.person.amzn1~amzn1.account.AHHRLU73JWRVT******CQ2LXSY2A/conversations/amzn1.comms.messaging.id.conversationV2~3f6684b4-e62d-4669-bb1c-72e3195cb82b/messages?count = 1000&sort = asc	Alexa Mobile Service - Amazon.com	"conversationId":"amzn1.comms.messaging.id.conversationV2~3f6684b4-e62d-4669-bb1c-72e3195cb82b","clientMessageId":"7962c368-a02a-4bb7-af6c-602dcd90a57c","messageId":27,"sequenceId":27,"time":"2020-12-28T19:36:20.919Z","sender":"amzn1.comms.id.person.amzn1~amzn1.account.AHHRLU73JWRVT******CQ2LXSY2A","type":"message/text", "payload":{"text":"12345","templateId":null,"metadata":null}, "MessageContext":{"deviceType":null,"deviceId":null}, "globalMessageId":"amzn1.comms.message.global.id~5fd058f0-2a62-44f9-ad18-ae5da2c591c4","parentGlobal MessageId":null,"domain":null,"relatedEntities":null,"parentMessageType":null, "messageStatus":null,"read":false	Content and time of message recovered from Amazon Account

Table 5
Metadata stored on IoT device.

Location of Data	Text files	Lines of Log inside Zipped Text Files from 8 GB eMMC Extracted Via ISP	User Actions
data\system\dropbox\Log.main	Log.main_188	12−2819:35:53.570753753IANCHDN.PanelSwipedOpen …..SendingbroadcastIntent{act = amazon.anchordian.PANEL_SWIPED_OPEN}	Swipe from right to left to open panel
	Log.main_190	12−2819:35:55.392753753IANCHDN.StateMachine:afaef40:statetransitionOPEN–TOUCHED_INSIDE_PANEL– > OPEN	Swipe from right to left to open panel
\#220@1609184164309.txt.zip	Log.main_198	12−2819:35:59.596753753ISystemTrayPillView:Toucheventreceived	Select "Communicate" button
	Log.main_198	12−2819:35:59.59636263626DLR_GloriaListActivity:dispatchTouchEventMotionEvent ….. = TOOL_TYPE_FINGER, …. ….	Select "Communicate" button
	Log.main_198	' …..." class = "url" >12−2819:35:59.71636263626~VLR_RecyclerListViewHolder: …...Clickdata = 'AndroidIntent < COMMANDaction = onCommsButtonClickedcmd = onCommsButtonClicked("message")>' …...	selected "Message"
	Log.main_208	12−2819:36:03.551753753ISystemTrayPillView:Toucheventreceived	select "Robert Paulson" recipient
	Log.main_209	12−2819:36:03.70736263626~VLR_RecyclerListViewHolder: …. ….<COMMANDaction = onCommsButtonClickedcmd = onCommsButtonClicked(this,'{"identifier":"SEND_TEXT_MESSAGE_VIA_LINKS", "eventPayload":{"senderCommsId":"amzn1.comms.id.person.amzn~amzn1.account.AHHRLU73JWRVT*******CQ2LXSY2A","recipient CommsId":"amzn1.comms.id.person.amzn~amzn1.account. AF34U4AGZ*******2UCWVUQCNKXA"}}"contactId":"ddb53627-345b-41e9-ae20-e3d3f7a820f1","messageType":"SEND_TEXT_MESSAGE_VIA_LINKS" …...	Sender and recipient Amazon account #s found in the log
data\system\dropbox\Log.main	Log.main_5	12−2819:36:08.646753753IANCHDN.StateMachine:afaef40:statetransitionCLOSED–KEYBOARD_OPENING– > NON_INTERACTABLE	Keyboard opening
\#221@1609184485852.txt.zip	Log.main_5	12−2819:36:10.761753753ISystemTrayPillView:Toucheventreceived	select number pad "&123"
	Log.main_6	12−2819:36:12.757753753ISystemTrayPillView:Toucheventreceived	type "1"
	Log.main_6	12−2819:36:14.398753753ISystemTrayPillView:Toucheventreceived	type "2"
	Log.main_6	12−2819:36:15.715753753ISystemTrayPillView:Toucheventreceived	type "3"
	Log.main_6	12−2819:36:17.012753753ISystemTrayPillView:Toucheventreceived	type "4"
	Log.main_6	12−2819:36:18.431753753ISystemTrayPillView:Toucheventreceived	type "5"
	Log.main_7	12−2819:36:20.292753753ISystemTrayPillView:Toucheventreceived	select "send" button
	Log.main_7	12−2819:36:20.520753753IANCHDN.StateMachine:afaef40:statetransitionNON_INTERACTABLE–KEYBOARD_CLOSING– > CLOSED	keyboard closing
	Log.main_8	12−2819:36:20.98319687334IACMSClient:HttpresponsecodeforsendMessage:200	Confirmation - message was sent

recipient of a message to be created on the next screen. Searching for "recipientCommsId" in the device logs can yield hits for more than one individual messaged by the device owner. Exceptions to these rules on the Echo Show 10 (3rd Generation) Our analysis of the new Echo Show 10 (3rd Generation) revealed differences in what data was available in device logs as the logs did not reveal recipient's account numbers like all the other Echo Show devices we examined. However, the 4 GB eMMC storage did reveal the name Paulson and many other contact names in four locations to include:data\alexahybrid\files\AmModel\nlu-personalized.OFFLINE.en-US.7.125\vocab.syms

7. Related work

A variety of papers have been written about the expanse of IoT in the past several years. This includes defining IoT devices and technology, projections for the growth of the IoT universe, the effects IoT devices have on individual privacy (Stoyanova et al., 2020), the vulnerability of IoT devices to cyber attacks (Alenezi et al., 2019), and forensic investigation of IoT devices during criminal investigations (Li et al., 2019). As follows, we briefly discuss the most relevant research studies discussing the topic of forensic analysis and IoT devices.

Orr and Sánchez (2018) present a study that involves the use of an Echo Dot (2nd Generation) in a home environment to generate data through typical use of the device during a ten-week period. The examination of the data after this period involved a manual examination of the web-based Alexa interface and a logical backup of a mobile device that was utilizing the Alexa App. The authors discussed the potential usefulness of the data recovered in a criminal investigation to include dates and times of events.

However, the study by Orr and Sanchez did not involve a forensic examination of the Echo Dot hardware used to generate the evidence. While the results of their study are useful and may "suggest" the Echo Dot hardware contains evidence, that alone does not rise to the level of probable cause to believe the Echo Dot hardware contains data of evidentiary value. Nieto et al. (2018) present a research study focused on IoT forensics and privacy. They defined IoT-Forensics as the term coined to describe a new branch of computer forensics dedicated to the particular features and requirements of digital investigations in the Internet of Things (IoT) scenarios. Chi et al. (2018) present a framework for IoT data acquisition and forensics analysis. They predict a high demand for IoT forensic tools due to the projected growth of the IoT market to a cap of $195 Billion in 2023. Servida and Casey (2019) discussed the possibility of accessing data through various methods and included an Echo device in their research but did not extract data from the Echo Dot hardware. They also acknowledged that techniques such as JTAG and chip-off can be technically challenging for investigators with limited knowledge in that area and those techniques could be destructive to the device and evidence. The authors state that IoT devices are valuable sources of evidence for forensic investigations and law enforcement.

In addition to investigative possibilities provided with IoT device research, previous research indicates significant technical and legal weaknesses, gaps, and challenges. Li et al. (2019) points out, IoT forensics is relatively understudied and challenging in practice due to its complexity, diversity, and heterogeneity of IoT devices and ecosystems. They used the Echo Dot as the basis for their analysis and an IoT forensic model, but most of their data came from the cloud, analysis of network traffic, and Android and iOS devices with very little information on extracting data from the Echo Dot storage or its contents. In their analysis strategy which included Alexa-enabled device hardware, they concluded Each Alexa-enabled device needs to be decomposed for performing hardware-level analysis. They finally identified the need for specialized tools to acquire data from IoT hardware and customized tools to analyze data from IoT devices to present the data in court. Alenezi et al. (2019) predicts the IoT market will continue exponential growth with over 500 billion devices connected to the Internet by 2030. They determined IoT forensics presented new challenges for investigations regarding evidence acquisition and, procedures, guidelines, and standards that guide IoT investigations are urgently needed. They acknowledged the need for hardware analysis which they referred to as digital-level forensics needed to collect data from the local memory of the IoT device.

To summarize, the previous works indicated gaps in research and the need for detailed information for forensic examiners to identify and seize IoT devices. Previous research also demonstrated and articulated a lack of information on the disassembly and extraction of data from IoT hardware and a lack of specific information and tools needed for the analysis of data from IoT devices. This research work fills these gaps by providing specific, practical instructions on extracting data from IoT devices. In particular, we provide detailed diagrams and tear-down video guides detailing step-by-step instructions and ISP procedures for IoT devices. Our work will assist law enforcement professionals and practitioners in evaluating the required forensic tools and skills needed for each procedure.

8. Limitations and future work

Our study did not compare data recovered from IoT hardware to data stored in the cloud under the same user account which would usually be obtained with a warrant to Amazon. We were limited to what we could see through Amazon's API using our known account login information. We also did not have information on how much metadata, if any, from logs Amazon collects or stores for individual accounts or IoT devices. This study was carried out in the United States of America, in the state of Texas. The results obtained from the experiments and relative discussion are relevant to this geographic area. Nevertheless, we believe that our results can be reused (entirely or partially) by law enforcement personnel located in different national/state jurisdictions.

There is much room for future work in this area. Starting from the results obtained in this work, it would be interesting to determine what specific metadata Amazon stores or collects on individual devices or accounts. This can be done by specific requests and language used in search warrant affidavits based on data recovered from the IoT device logs. Continued experiments on IoT devices are needed to identify other metadata and content stored on Amazon IoT hardware. We also want to expand our study by including other Amazon IoT devices, without screens, and devices that do not use eMMC storage. This research can also expand to other, Alexa-enabled, IoT devices not manufactured by Amazon. Future research could focus on a more detailed comparison of forensic tools used to analyze data from IoT devices. We believe that, as IoT devices become more prolific, it is likely that forensic analysis tools will incorporate more in-depth IoT parsing and support into their abilities.

9. Conclusion

Lack of information makes it difficult for law enforcement professionals to describe and legally justify probable cause to seize IoT devices without knowing what these devices are capable of storing. The main objective of this research is to assist law enforcement professionals at every stage of an investigation involving Amazon IoT devices, from the drafting of search warrant affidavits to seizing, extracting, analyzing, and storing the evidence. This allows forensic examiners and practitioners the ability to evaluate the required forensic tools and skills which will be needed for each procedure. This also reduces device damage or contamination of evidence which can occur during blind forensic examinations. In particular, we created a set of comprehensive guides in the form of diagrams and start-to-finish tear-down extraction videos on all five Echo Show devices and the Echo Spot. Our research methodology and four-step experiment process could also be applied to other IoT devices without a screen, with only slight modifications. Through our experiments, we show how to identify forensic-related metadata from Amazon Echo Show and the Amazon Echo Spot devices. We provide a clear description of how to obtain a physical extraction from the eMMC storage on the considered Amazon IoT devices. We provide two Python scripts for carving device specifications and user account information from physical images of the IoT storage, and one which will automatically display the device specifications in Cellebrite's Physical Analyzer. We identified keyword searches that yield unique user activity in device logs and developed Python scripts for carving and organizing that data from exported device logs. We also identify specific forensic tools to accomplish each task. The methodology (see section 3) and four-step process (see section 5) we proposed for conducting experiments on IoT devices can be used, after the fact, by forensic examiners analyzing the same IoT devices in future investigations. If there is metadata or content uncovered during an investigation that we did not cover in our research, examiners can use our methodology, tear-down video guides, and diagrams to replicate our study and verify suspected activity located on an IoT device during an investigation by obtaining their own test device. These methods of testing and extraction are repeaTable for the purpose of validation or demonstration if needed, to show the origin of recovered data. Much of the data from the IoT hardware can be validated after obtaining legal access to information associated with the IoT owner's cloud accounts.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

We have uploaded both ISP diagrams and tear-down videos on Zenodo and shared the link in the revised version of the paper

Acknowledgment

This research was supported in part by the Air Force Research Laboratory (AFRL) and Department of Homeland Security (DHS) Science and Technology (S&T) Directorate under award FA8750-19-C-0077.

References

Afonin, O., Katalov, V., 2016. Mobile Forensics-Adavanced Investigative Strategies. Packt Publishing, Birmingham.

Alenezi, A., Atlam, H.F., Alsagri, R., Alassafi, M.O., Wills, G.B., 2019. Iot forensics: a state-of-the-art review, challenges and future directions. In: Muñoz, V.M., Firouzi, F., Estrada, E., Chang, V. (Eds.), Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk, COMPLEXIS 2019, Heraklion, Crete, Greece, May 2-4, 2019 (Pp. 106–115). SciTePress. https://doi.org/10.5220/0007905401060115, 10.5220/0007905401060115.

Bair, J., 2017. Seeking the Truth from Mobile Evidence: Basic Fundamentals, Intermediate and Advanced Overview of Current Mobile Forensic Investigations. Elsevier, London.

Bechham, D., Abbott, W., Johnson, J., Kugler, E., Hall, P., 2018. Warrants manual, Austin: Texas district & county attorneys association. https://www.tdcaa.com.

Boztas, A., Riethoven, A.R.J., Roeloffs, M., 2015. Smart TV forensics: digital traces on televisions. Supplement 1, S72–S80 Digit. Invest. 12. https://doi.org/10.1016/j.diin.2015.01.012, 10.1016/j.diin.2015.01.012.

Chi, H., Aderibigbe, T., Granville, B.C., 2018. A framework for iot data acquisition and forensics analysis. In: Abe, N., Liu, H., Pu, C., Hu, X., Ahmed, N.K., Qiao, M., Song, Y., Kossmann, D., Liu, B., Lee, K., Tang, J., He, J., Saltz, J.S. (Eds.), IEEE International Conference on Big Data (IEEE BigData 2018), Seattle, WA, USA, December *10-13, 2018*. IEEE, pp. 5142–5146. https://doi.org/10.1109/BigData.2018.8622019, 10.1109/BigData.2018.8622019.

Chung, H., Park, J., Lee, S., 2017. Digital forensic approaches for amazon alexa ecosystem. Supplement, S15–S25 Digit. Invest. 22. https://doi.org/10.1016/j.diin.2017.06.010, 10.1016/j.diin.2017.06.010.

DoJ, 2009. Searching and seizing computers and obtaining electronic evidence in criminal investigations. United States, computer crime and intellectual property section criminal division. Office of Legal Education Executive Office for United States Attorneys. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

DoJ, 2020. Citizen's Guide to u.S. Federal Law on Child Pornography. *Retrieved from United States. Department of Justice*. https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography.

Ferguson, A., 2015. The internet of things and the fourth amendment of effects. Calif. Law Rev. 104 (4), 805–880. https://www.jstor.org/stable/24758739.

Gómez, J.M.C., Gómez, J.R., Mondéjar, J.C., Martínez, J.L., 2019. Non-volatile memory forensic analysis in windows 10 iot core. Entropy 21, 1141. https://doi.org/10.3390/e21121141, 10.3390/e21121141.

Goulart, A., Chennamaneni, A., Torre, D., Hur, B., Al-Aboosi, F.Y., 2022. On wide-area iot networks, lightweight security and their applications – a practical review. Electronics 11. https://www.mdpi.com/2079-9292/11/11/1762, 10.3390/electronics11111762.

Hadgkiss, M., Morris, S., Paget, S., 2019. Sifting through the ashes: amazon fire TV stick acquisition and analysis. Digit. Invest. 28, 112–118. https://doi.org/10.1016/j.diin.2019.01.003, 10.1016/j.diin.2019.01.003.

Karabiyik, U., Akkaya, K., 2019. Digital forensics for iot and wsns. Springer vol. 164. In: Ammari, H.M. (Ed.), Mission-oriented Sensor Networks and Systems: Art and Science - Volume 2: Advances, pp. 171–207. https://doi.org/10.1007/978-3-319-92384-0_6, 10.1007/978-3-319-92384-0_6.

Li, S., Choo, K.R., Sun, Q., Buchanan, W.J., Cao, J., 2019. Iot forensics: amazon echo as a use case. IEEE Internet Things J. 6, 6487–6497. https://doi.org/10.1109/JIOT.2019.2906946, 10.1109/JIOT.2019.2906946.

Lorenz, S., Stinehour, S., Chennamaneni, A., Subhani, A.B., Torre, D., 2022. IoT forensic analysis: a family of experiments with amazon echo devices (ISP diagrams and teardown videos). https://doi.org/10.5281/zenodo.7383668, 10.5281/zenodo.7383668.

Meffert, C., Clark, D., Baggili, I.M., Breitinger, F., 2017. Forensic state acquisition from internet of things (fsaiot): a general framework and practical approach for iot forensics through iot device state acquisition. In: Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, August 29 - September 01, 2017 (Pp. 56:1–56:11). ACM. https://doi.org/10.1145/3098954.3104053, 10.1145/3098954.3104053.

Nieto, A., Rios, R., López, J., 2018. Iot-forensics meets privacy: towards cooperative digital investigations. Sensors 18, 492. https://doi.org/10.3390/s18020492, 10.3390/s18020492.

Novak, M. (2020). Smart TV forensics: digital traces on televisions. J. Digit. For. Secur. Law, 14, 1–42. (URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/digital-evidence-criminal-cases-us-courts-appeal-trends-and-issues).

Orr, D.A., Sánchez, L., 2018. *Alexa, did you get that?* determining the evidentiary value of data stored by the amazon® echo. Digit. Invest. 24, 72–78. https://doi.org/10.1016/j.diin.2017.12.002, 10.1016/j.diin.2017.12.002.

Pawlaszczyk1, D., Friese, J., Hummert, C., 2019. “Alexa, tell me …” - a forensic examination of the amazon echo dot 3 rd generation. In: Bertino, E., Georgakopoulos, D., Srivatsa, M., Nepal, S., Vinciarelli, A. (Eds.), International Journal of Computer Sciences and Engineering. JCSE, pp. 20–29. https://doi.org/10.26438/ijcse/v7i11.2029 doi.org/10.26438/ijcse/v7i11.2029.

Reiber, L., 2019. Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation. McGraw-Hill, New York.

Servida, F., Casey, E., 2019. Iot forensic challenges and opportunities for digital traces. Supplement, S22–S29 Digit. Invest. 28. https://doi.org/10.1016/j.diin.2019.01.012, 10.1016/j.diin.2019.01.012.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E.K., 2020. A survey on the internet of things (iot) forensics: challenges, approaches, and open issues. IEEE Commun. Surv. Tutorials 22, 1191–1221. https://doi.org/10.1109/COMST.2019.2962586, 10.1109/COMST.2019.2962586.

Wu, T., Breitinger, F., Baggili, I.M., 2019. Iot ignorance is digital forensics research bliss: a survey to understand iot forensics definitions, challenges and future research directions. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES 2019, Canterbury, UK, August 26-29, *2019* (Pp. 46:1–46:15). ACM. https://doi.org/10.1145/3339252.3340504, 10.1145/3339252.3340504.

Yaqoob, I., Hashem, I.A.T., Ahmed, A., Kazmi, S.M.A., Hong, C.S., 2019. Internet of things forensics: recent advances, taxonomy, requirements, and open challenges. Future Generat. Comput. Syst. 92, 265–275. https://doi.org/10.1016/j.future.2018.09.058, 10.1016/j.future.2018.09.058.

Youn, M.-A., Lim, Y., Seo, K., Chung, H., Lee, S., 2021. Forensic analysis for ai speaker with display echo show 2nd generation as a case study. Forensic Sci. Int.: Digit. Invest. 38, 301130. https://www.sciencedirect.com/science/article/pii/S2666281721000287, 10.1016/j.fsidi.2021.301130.