Nondestructive Data Acquisition Methodology for IoT Devices: A Case Study on Amazon Echo Dot Version 2

Albert M. Villarreal, III, Robin Kumar Verma, Oren Upton, and Nicole Lang Beebe, *Senior Member, IEEE*

***Abstract*—The smart speaker is becoming a common part of the modern household, which usually includes an AI-powered Intelligent Voice Assistant to communicate with its users. Amazon Echo Dot is a popular smart speaker that extends the above-stated functionality by acting as a communication hub for other Internet of Things (IoT) and mobile devices within its local network. The nature and volume of data that an Echo Dot handles make it a potential source of evidence, if one is seized for a digital forensics investigation. Researchers and practitioners have explored various techniques to extract data from these IoT devices. However, traditional methods make changes to the physical device and/or its data, which is undesirable from a digital forensics perspective. The current work focuses on developing a nondestructive methodology for extracting data from IoT devices, with Amazon Echo Dot version 2 as an example, which use embedded Multimedia Card (eMMC)/embedded Multichip Package (eMCP) chips as their primary storage. We identify all in-system programming (ISP) pins using the computed tomography (CT) Scan imagery of the main printed circuit board (PCB) of the device. We created a 3-D fixture that accommodates pogo pin connectors to create contact with the already identified ISP taps on the main PCB. The 3-D Test Probe Jig can extract data from an IoT device's memory chip using an eMMC reader. The proposed nondestructive solution is reproducible, portable, and affordable.**

***Index Terms*—Digital forensics, Internet of Things (IoT), nondestructive data acquisition.**

I. Introduction

SMART speakers are one of the biggest-selling Internet of Things (IoT) device types in the world. The global sale of smart speakers was an estimated 146.9 million units in 2019 [1]. Each of these smart speakers hosts an "Intelligent Voice Assistant" that receives voice commands from the user. The voice assistant provides verbal information back or executes instructions on other devices in the smart home network. Statista.com estimates that 4.2 billion digital voice assistants are being used in devices around the world as of 2020 [2]. The same report also estimates that there are 110 million virtual assistant users in the United States alone [3]. Amazon is the current market leader in the global smart speaker market with a 21.6% share in 2020 [4].

Amazon's smart speaker product line includes various devices, such as Echo, Echo Dot, Echo Show, Echo Studio, and Echo Flex. Some of these devices including the Echo, Echo-Dot, and the Echo Show have evolved over the last few years, resulting in different versions being produced. Echo Studio and Echo Flex were launched in 2019 and are in their first generation. This article focuses primarily on Amazon Echo Dot version 2.

Amazon Alexa is an "Intelligent Voice Assistant" that allows a user to manage all Amazon-supported IoT devices connected within the smart home or smart office device pool. All IoT devices in the device pool communicate with each other over a stable local Wi-Fi connection or other wired or wireless communication channels. When a user activates Alexa with the appropriate verbal commands, the Alexa Voice Service (AVS) system transmits the verbal command to the central Alexa system hosted in the cloud-based Amazon Web services to make decisions on how to verbally communicate with the user or handle IoT devices in the pool. The voice recognition and interpretation used in the Alexa system requires robust computing resources, which cannot fit in the smart speaker and therefore the computing is done in the cloud. The smart speaker is a small relatively resource-constrained device like the Echo Dot, which includes a microphone and speaker, and a circuit board with limited memory, storage, and processing power. The small device primarily needs to capture the voice command and forward it to the cloud, and then playback the response to the user. The Echo Dot version 2 is one of the most common Alexa devices, so analysis of this device was the focus of this work.

The Amazon Echo Dot 2 is a potentially important device from a digital forensics perspective, because they are so common in the home and office environment. If a smart home or smart office environment setup includes the Echo Dot 2, it will be useful for a digital forensics investigator to know what potential evidence may be gathered from this device and how to collect it. Currently, forensic analysis has focused on the data stored in the cloud, communication between the device and the cloud, and some analysis of data on the device itself, which can be collected through chip-off data extraction methods. Similarly, other IoT devices in a smart home and smart office environment could be potential sources of digital

Manuscript received 28 October 2021; revised 2 February 2022; accepted 14 October 2022. Date of publication 23 November 2022; date of current version 20 February 2023. *(Corresponding author: Robin Verma.)*

The authors are with the Cyber Center for Security and Analytics, University of Texas at San Antonio, San Antonio, TX 78249 USA (e-mail: albert.villareal@utsa.edu; robin.verma@utsa.edu; oren.upton@utsa.edu; nicole.beebe@utsa.edu).

Digital Object Identifier 10.1109/JIOT.2022.3218524

evidence. The current work takes Amazon Echo Dot version 2 as an example device and develops a nondestructive solution to extract data from its onboard memory chip.

Standard methods involved in removing the chips can damage the device and the data stored on the chip, which puts potential evidence at risk. Chip-off extraction in digital forensics is considered to be a destructive method for data extraction, because it removes the memory chip from the circuit board. So, this article examines a method, which extracts the data without the associated risks of chip-off methods.

Interest in forensic data collection from IoT devices in general, and the Echo Dot specifically, is increasing. The first time an Echo Dot was seized as evidence that we could find, occurred in 2015, when law enforcement seized an Echo Dot as evidence in a murder investigation in Bentonville Arkansas [5]. Ultimately, the evidence on the device itself was not beneficial, and the case was eventually dropped, but it was a precedent-setting case [6]. Amazon pushed back on the initial court requests for evidence stored in the cloud as being too broad. An Amazon Echo was seized in a double homicide case in January 2017 in Farmington, NH [7]. It is not clear what evidence came from the forensic analysis of the device from news articles, but voice recordings from Amazon included some statements to Alexa from the murder suspect, and these statements were used in the case to establish that he spent significant time at the home in the days leading up to the murder [8]. In the first six months of 2020, Amazon responded to 3105 court orders, warrants, and subpoenas from the U.S., with an additional 539 requests from outside the U.S. [9]. Amazon does not provide the detail to know how many of these might be related to requests for data related to Alexa devices, but it is quickly becoming normal for law enforcement to make requests related to these devices.

Although there is research that focuses on extracting potential pieces of evidence from Echo Dot 2, we could not find any published research describing a nondestructive data extraction solution for the data stored on the chips in this device. Oxygen forensics has a solution that gathers data from the cloud, but not the chips on the device itself [10].

In the current paper, we present a nondestructive method to extract data from the embedded multimedia card (eMMC) chip, which is the main memory of the Echo Dot version 2.

II. Related Work

A. Forensic Data Retrieval From NAND Chips

Maintaining the integrity of data is a top priority in digital forensic analysis. Identifying tools or methods, which can improve the integrity of collecting forensic data is vital to the improvement of forensic research. When we collect data from IoT devices like the Echo Dot, and many other devices without clear interfaces for data extraction and unknown circuit board traces, a common method is removing the memory chips and reading the data directly from the chip, a process known as "chip-off" analysis. This method poses some inherent risks. First, Fukami et al. [11] pointed out that heat-based chip removal methods may introduce raw data errors in NAND flash memory's resident data during the chip-off process. They show that using the "read-retry" mechanism, available on multilevel cell (MLC) NAND chips, can reduce such errors. The read-retry mechanism is implemented as a vendor-specific operation that adjusts NAND flash memory cells' threshold voltage to minimize bit errors. They conclude that digital forensic data acquisition procedures for NAND-based chips should include the read-retry mechanism. Second, another paper by van Zandwijk and Fukami [12] highlights that bit-errors in NAND chip's resident data could increase after a forensic chip-off procedure.

In addition to the above-stated research, which establishes that heat-based chip removal can cause read errors or make the chip unreadable in some instances, Ence et al. [13] did not found a safe temperature range that could guarantee a successful chip-off read.

Overall, these papers establish the fact that thermal-based chip-off procedures involve risk and may not be 100% successful. Ence et al. [13] demonstrated that chip-off extraction resulted in damage to 14 chips out of a research sample of 258 chips. This means that there may be cases when the forensic investigator could not read from the NAND chip after the thermal-based chip-off process. These failures can be critical in digital forensic investigations that depend on evidence from the respective devices from which these chips are analyzed through chip-off analysis.

Because there are risks, it is important to explore other methods for collecting forensically sound data from IoT devices. This will become even more important in cases where the manufacturer has purposely designed the device to prevent reverse engineering and they have not made electronic schematics of the printed circuit board (PCB) or chips public. There is a need for nondestructive chip reading methods for the eMMC chips that guarantee a successful data read from the respective chips with lower risk and higher potential data integrity. We have presented a nondestructive way to read from the Echo Dot 2's eMMC chip. The method is affordable, portable, and reproducible.

B. Amazon Echo and Alexa Forensics

Li et al.'s [14] paper provides a digital forensic investigation model that investigators can use to gather potential pieces of evidence from the IoT devices. They have demonstrated their investigation model using an Amazon Echo Pi (Echo simulated on a Raspberry Pi [15]) image. This article was useful in providing a forensic overview of the Echo Dot ecosystem. Our work seeks to add more depth, and focuses on the actual Echo Dot 2 hardware and software, rather than an emulation of the Echo Dot. Earlier, Chung et al. [16] also proposed a tool, Cloud-Based IoT Forensic Toolkit (CIFT) for short, that can identify, acquire, and analyze potential evidence from the Amazon Alexa Ecosystem. They aimed to collect artifacts from the hardware device, network, client side, and cloud-related artifacts. The above-stated research works have not explored the actual hardware data acquisition from an Amazon Echo device. Tristan et al. [17] have provided detailed information about the board layout and hardware components included in the Echo Dot 2. Their analysis did not focus on the data extraction methodology that our research does explore.

Although Jo et al. [18] introduced the overall layout of an AI-based smart speaker ecosystem and performs network traffic analysis to and from these speakers, the authors did not explicitly include Amazon products in their work. A follow-up paper by some of the same authors (Shin et al. [19]) includes the Amazon Echo Dot. The authors (Shin et al.) first carried out a chip-off on Amazon Echo Dot, followed by certificate and proxy injection into the flash memory. Finally, they perform a reballing operation to attach the NAND chip back to the mainboard. This procedure helps them to intercept the encrypted communication between the Echo Dot and Amazon cloud. However, the Echo Dot uses secure socket layer (SSL) pinning, which is used to prevent man-in-the-middle attacks. And thus, the authors were only able to obtain the Amazon cloud server addresses. The authors tried the same, with Alexa-Pi, but the results were the same and they were only able to capture the encrypted communication.

The first two research papers used a Raspberry Pi-emulated version of the Amazon Echo Dot 2. There are significant differences between the actual hardware of the Raspberry Pi and the Echo Dot 2 circuit board and chips. This motivated us to study forensic techniques that could be used to collect data directly from the chips of the Echo Dot 2. The last two research papers discussed the chip-off technique for data extraction, but showed the risks of using destructive forensic methods. Our research focused on avoiding the risks of chip-off analysis by exploring nondestructive methods of data extraction.

Conti at al. [20] highlighted that "data acquisition from IoT devices does not follow a standardized procedure that is forensically sound." Stoyanova et al. [21] have raised similar concerns. Our work makes a step forward toward solving this problem. Orr and Sanchez [22] established the evidential value of data stored by Amazon Echo in the cloud, the Alexa app, and the cache of a connected mobile device. This research extends their work by finding potential pieces of evidence on the Echo device itself.

C. PCB Testing Techniques for Digital Forensic Investigation Purposes

In-system programming (ISP), also referred to as in-circuit serial programming (ICSP), is designed to read the onboard eMMC and embedded multichip package (eMCP) chips without invoking the CPU [23]. Read and write operations can be performed directly on the ball grid array (BGA) pin connections of eMMC/eMCP using the ISP pins. There are two ways in which ISP connections can be used to dump the data from a given eMMC/eMCP chip (Bair) [24]. The first method is to read from the BGA pins of an eMMC chip that has been removed from the main PCB. This method is a destructive way of extracting data using ISP connections. The second method is where micro-soldering is used to attach to locations on the board that connect to the ISP pins of the eMMC chip. This method is a relatively nondestructive way of extracting data from the chip. Both of the above-stated techniques have been used by digital forensic investigators to extract data from mobile phones. There are micro-soldering experts in law enforcement agencies who use their specialized knowledge and experience to carry out these techniques. They also share the ISP pinout information of specific mobile phones with their fellow investigators. Websites like "www.emmcpinouts.com" [25] provide pinout information and detailed documentation about selective make and models of smartphones, tablets, and GPS devices to their paid subscribers. However, we were not able to find any online repository for ISP pinout information and documentation related to IoT devices. The current work focuses on the second method, where we have replaced the micro-soldering part with pogo pins to make connections with the onboard ISP connections.

Even though the information about ISP pinouts of individual mobile devices is available within the digital forensic community, it takes a great level of expertise for an investigator first to learn those techniques and then use them on the devices they wish to work on. There is no alternate practical solution, that could be used by an ordinary forensic investigator, to extract data from such devices without having micro-soldering expertise. So, our secondary goal is to develop a solution that ordinary digital forensic investigators can use. PCB manufacturers also use nondestructive techniques to collect and validate data from chips to test and ensure that the device is functioning properly before it is shipped. In-circuit testing (ICT) and functional testing (FCT) are the two most common methods for testing a PCB. Other testing techniques include flying probe testing, automated optical inspection, burn-In testing, X-Ray inspection, and more.

There is no academic literature on the development of nondestructive PCB testing techniques for the forensic investigation of IoT devices to the best of our knowledge. We sought to fill a gap by exploring techniques that would collect data directly from the eMMC chip of the Echo Dot 2, but doing so in a nondestructive manner, without chip-off risks. We explored a mixed approach that takes inspiration from the ICT and the X-Ray Inspection technique. The proposed solution uses a 3-D printed fixture with pogo pins, which resembles the "ICT" technique. Moreover, we used a CT-Scan to find the hidden ISP pins that manufacturers can deliberately obfuscate to make data extraction from the device inherently more challenging. This method is like an extension of the "X-Ray Inspection" technique.

III. Methodology

We developed a generic framework for creating a nondestructive way to extract data from the eMMC/eMCP chip used in IoT devices (Algorithm 1). A Test Probe Jig, a device-specific 3-D printed fixture, is obtained as the end-result after following the framework's procedures. The Test Probe Jig for a given IoT device holds pogo pins on ISP contact points on the device's PCB for directly interacting with its eMMC/eMCP chip, bypassing the CPU.

The framework uses at least two donor devices (identical copies) per target IoT device. If a researcher or the practitioner successfully creates a Test Probe Jig for a given IoT device, they can easily share their work with peers by sending them the 3-D model of the jig. So, developing a nondestructive Test

Algorithm 1 Nondestructive Data Acquisition

Input: *Actual IoT device, Donor IoT devices*
Output: *Non-destructive data dump*

1. **if** Onboard Connections Available[1] **then**
2. Jump to Line 7
3. **else**
4. Perform Chip-off on the *Donor Device* {*ref. §3.1*}
5. Perform a CT Scan of the *Donor Device* {*ref. §3.2*}
6. **end if**
7. Design a 3D model {*ref. §3.4*}
8. 3D Prototype Printing
9. Connect the *Actual device* and extract data {*ref. §3.5*}

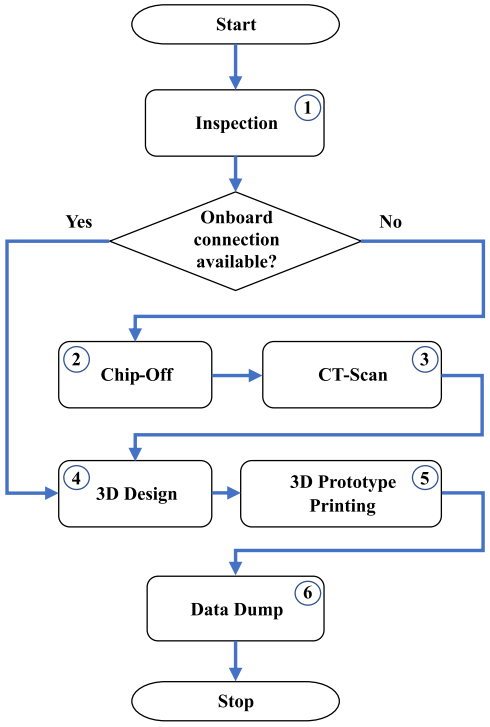

Fig. 1. Generic framework for nondestructive data extraction from IoT devices.

Probe Jig for a particular IoT device is a one-time effort for the research and practitioner community.

The use of a Test Probe Jig fixture makes it easy for new and relatively inexperienced investigators to investigate a given IoT device. Currently, only experts can understand and implement advanced data extraction methods like chip-off and ISP micro-soldering. The Test Probe Jig greatly reduces the complexity of this problem, as a new or inexperienced investigator only needs a serial reader device to read from the IoT device's eMMC/eMCP.

Here, is the outline of the framework.

The generic framework is also shown as a flowchart in Fig. 1. The current work aims to invent a nondestructive method to extract data from the Amazon Echo Dot 2 as an example IoT device and analyze it using digital forensic tools. We adopted a two-step approach for the above-stated purpose.

[1]ISP connections.

TABLE I
INTEGRATED CIRCUIT CHIPS ON THE ECHO DOT 2 BOARDS

Chips	Function
Mediatek MT6625LN	4 in 1 Wi-FI, Bluetooth, FM and GPS chip
Mediatek MT8163v	64-bit Quad-core ARM Cortex-A53 MPCore
Micron 6PA98 JWB30	4GB LPDDR3 memory module
Mediatek MT6323LGA	Power Management IC
DAC 32031 TI 6AK D6KE	Digital to Analog converter

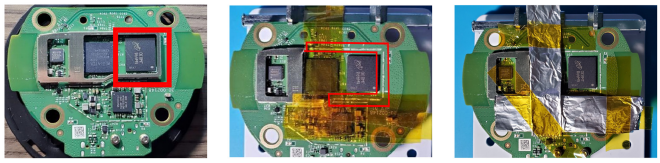

Fig. 2. (a) Memory chip within the metal shielding. (b) Portion of the shielding removed. (c) Heat-resistant tape with aluminum foil to prepare the board for chip-off.

The first step is to investigate the device's hardware, followed by the second step in which we analyze the extracted data.

We used the following equipment and resources for this investigation.

1) Two donor devices—duplicate device on which the chip-off is performed, followed by a CT-Scan. Micro-soldering to ISP connections is done on the second donor.
2) Information about the BGA pinouts of the respective eMMC chip.
3) Voltage checking hardware (such as a logic analyzer, oscilloscope, or multimeter) to inspect and verify the individual ISP pin and voltages.
4) A Stereolithography (SLA) or polylactic acid (PLA) 3-D printer.
5) eMMC readers like EasyJTAG or RIFF Box.

Details about these components and the context in which they are used in the current work are given in the text below. We used two donor devices to carry out the chip-off analysis, computed tomography (CT) scan imaging, and the ISP micro-soldering in order to obtain sufficient information for developing the Test Probe Jig. Then, the Test Probe Jig was used to extract data from the evidence device.

Our investigation process consisted of the following steps.

1) *Gathering Information About the Device:* We started the hardware investigation with an FCC ID lookup for the Echo Dot 2 on the Internet. This is often a very useful first step when analyzing IoT devices. In this case, the analysis of the data provided by the FCC ID search was not helpful. We then opened the case and visually inspected all hardware components and chips on the Echo Dot 2's main PCB to determine their role. Table I shows details about these essential chips.
2) *Concentrating on the Memory:* Our main focus was on the memory chip (Micron 6PA98 JWB30, as shown in Fig. 2) to determine a nondestructive way to extract data from it. Micron assigns its eMMC and eMCP

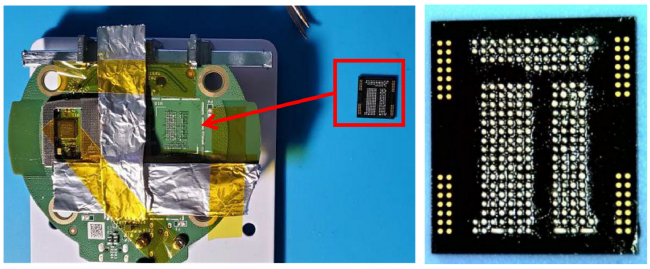

Fig. 3. (a) Board and the memory chip after chip-off. (b) BGA connections under the memory chip.

TABLE II
ISP PINOUT (SOURCE: JEDEC* STANDARD JESD84-B451 PP. 4–8 [26])

Pin	Description
CMD	Clock Signal
CLK	Bidirectional Command Signal
DAT0	Bidirectional Data Channel Zero (first out of 8 channels)
GND	Ground Signal (VSS for Core; VSSQ for I/O)
VCC	Power supply for Core
VCCQ	Power supply for I/O (Input/Output)
RST	Reset

chips with a fine-pitch BGA (FBGA) code as the last five characters of the chip's name ("JWB30" for the current one). We found the webpage for the memory chip,[2] which provides only basic information, with no datasheet. The chip is a BGA 221 eMCP that holds a 4-GB MLC eMMC and a 4-GB low-power double data rate 3 (LPDDR3) random access memory (RAM). Since the datasheet is not available, we carried out a chip-off on the donor device to confirm that it uses a BGA 221 ball socket system-on-chip (SOC) eMCP.

3) *Finding a Memory Reading Method—ISP:* JTAG and UART connections need the CPU to extract data from an eMMC chip on a given board. Thus, the CPU may change the state of a seized device from a digital forensic perspective. Moreover, most device manufacturers do not disclose their JTAG and UART connections information publicly, as in the case of Echo Dot 2. Therefore, we thought a nondestructive data reading method could be worked out if all the ISP pins (Table II), VCC, GND, VCCQ, CMD, DAT0, and RST, were available. This research identified all ISP pins located on the bottom of the memory chip, which was mounted face down on the board before we carried out the chip-off analysis on the donor device (Fig. 3). *More details are available in Section III-A.*
4) *Locating the ISP Pins Using CT Scan:* After locating the ISP pins on the memory chip, the next step is to trace connections from the Echo Dot 2's PCB that terminate on the respective ISP pins under the memory chip (Fig. 4). We found out that two connections leading to the required ISP pins are not directly available on the PCB circuit surface. These connections are untraceable on either of the board's surfaces (top and bottom) as they travel inside the PCB board substrate. Working with a partner organization, we were able to obtain a CT Scan of the Echo Dot 2 donor device's main PCB to determine the two hidden ISP pin connections from the portion of PCB under the memory chip to two different points on the bottom of the board [Fig. 5(a) and (b)]. *More details are available in Section III-B.*
5) *Verifying the ISP Connections:* We micro-soldered to all six points, four on the top and two on the bottom, corresponding to the six ISP pins. We used an oscilloscope and logic analyzer to read the assumed ISP connections. After testing the connections with an oscilloscope and logic analyzer, we connected the soldered wires to an eMMC reader. The eMMC reader was used to obtain a full data dump from the memory chip. More details are available in Section III-C. Data extraction from an onboard memory chip using ISP connections is considered relatively nondestructive as compared to chip-off. However, the process of micro-soldering using the ISP connections makes slight modifications to the original device, and if not done correctly (by an expert), it could also damage the board. Our method enables us to bypass the micro-soldering step and is thus completely nondestructive.
6) *Developing Nondestructive Reading Mechanism—Test Probe Jig:* The goal of this research was to explore and identify a genuinely nondestructive way of data extraction, which would not require micro-soldering expertise. We devised a "Test Probe Jig" that uses pogo pins (spring-loaded contact pins) mounted on a 3-D printed fixture to connect and later dump data from the Echo Dot 2 memory chip. *More details are available in Section III-A.*
7) *Getting the Data Dump:* We now use the Test Probe Jig on the evidence device. The Test Probe Jig is attached to the PCB with the pogo pins in direct contact with the ISP pin locations. The Jig is connected to the eMMC reader. The eMMC reader is connected to a computer to complete the data dump.

The second step that deals with the analysis of the memory dump is explained in Section III-E. We provided an overview

[2]https://bit.ly/3p5XV51

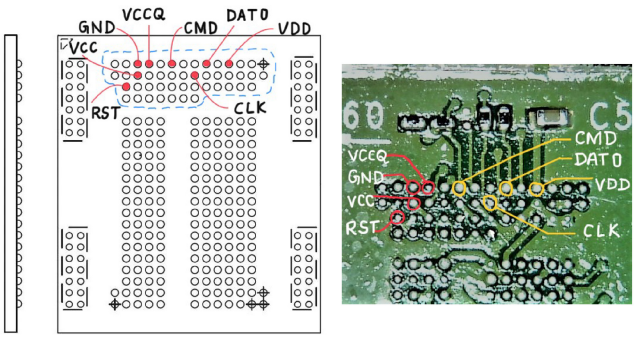

Fig. 4. (a) Flipped pin mapping of a BGA 221 ball socket SOC—as visible on board that hosts the eMMC chip. (b) Corresponding pin mapping on Echo Dot 2's board. We traced the connections marked on the right side on the PCB next to the chip; however, we had to use CT scan images to trace connections marked on the left side.

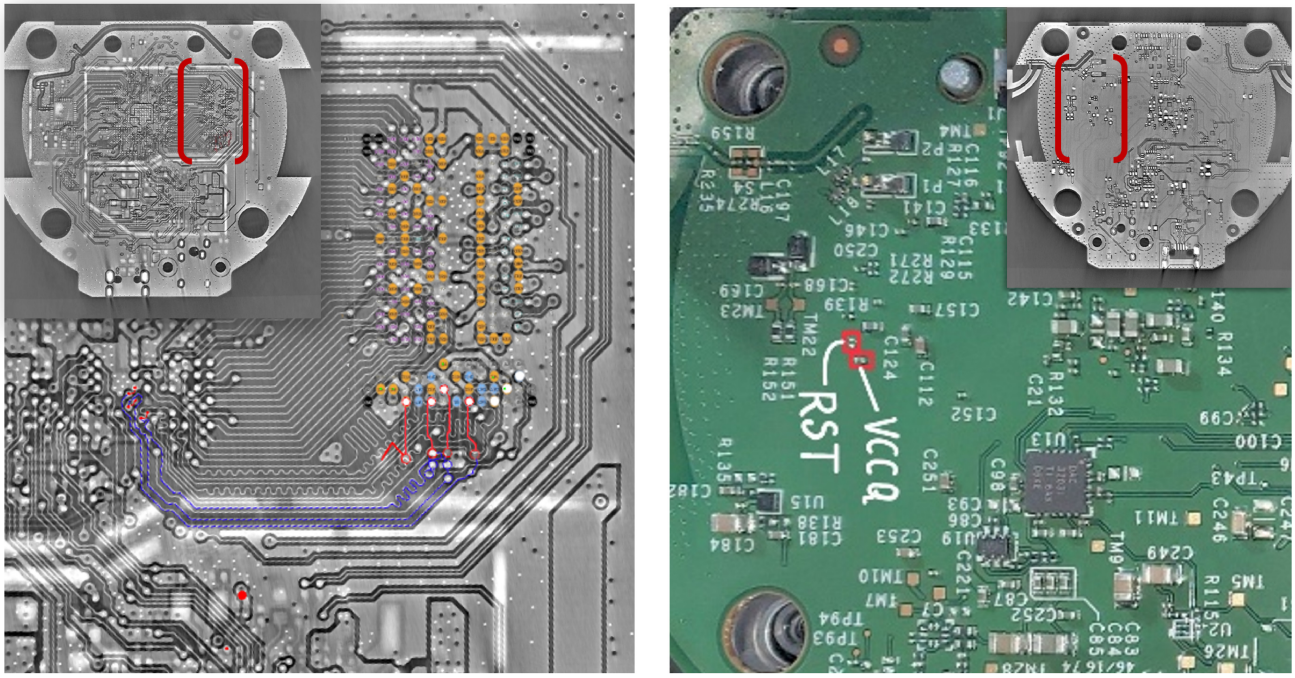

Fig. 5. (a) CT Scan top-view of the main board (top left); the zoomed-in portion of the image in background shows the BGA 221 pinout on the main PCB. The solid lines are contact points used in current research work; the dashed lines show them going under the CPU. (b) (*right*). Horizontally flipped CT Scan bottom view of the main PCB; the zoomed-in portion of the image shows contact points for the RST and VCCQ pins on the backside (bottom view) of the PCB.

of the methodology used. The following section provides an in-depth explanation of the same.

A. Finding the ISP Pins Using Chip-Off

In order to extract data from the eMCP memory chip (Micron 6PA98 JWB30, 4 GB, LPDDR3) we needed to identify the BGA package of the eMCP chip and the ISP pin connections on the PCB. Since information about neither the BGA package nor the ISP connections used in Echo Dot 2 memory chip is available in open literature; it was necessary to remove the chip from the donor device to find this information. Below we describe our chip-off procedure.

Together with the CPU and the wireless chip, the memory chip is enclosed inside metal shielding. We removed a portion of shielding around the memory chip to get better access to the shared space between the chip and the board. We then covered other components around the memory chip with heat-resistant tape and a layer of aluminum foil strips for added heat protection to prevent damage to the other circuitry on the board (Fig. 2). We removed the memory chip using a hot air station and learned that the chip uses "BGA 221 Ball Socket SOC" (Fig. 3).

We analyzed this chip and looked specifically for the ISP connections on the chip. ISP is a way to connect to eMMC and eMCP chips. We looked for the ISP connections so that we could extract data directly from the eMMC without powering on the whole board. We specifically were looking for these six pins: 1) VCC; 2) VCCQ; 3) CMD; 4) CLK; 5) DAT0; and 6) RST.

We examined the BGA connections on the Echo Dot 2 board to determine the above-stated ISP connections. Fig. 3 below shows data pin connections of the board. Out of these ISP pins, four pins, namely, GND, VCC, VCCQ, and RST, are entirely covered by the memory chip while attached to the Echo Dot 2 board. Fig. 4 shows these pins among the BGA connections on the board. These four pins connect to other board components through wire connections that are not visible on the board surface. The manufacturer has embedded some traces in the board substrate that do not show on the top or bottom surfaces.

Because the traces are embedded for two of the pins, it would not be possible to access the data from the eMMC chip using ISP connection to the board. This would require chip-off methods. In order to develop a nondestructive way to access the memory chip's data, it is necessary to find the hidden ISP connections that start from these four BGA pins and end at some location on the surface of the board. Because they are not visible, a CT scan was used to identify the traces.

B. CT-Scan of the Echo Dot 2's Main PCB

The current research used a CT Scan of the Echo Dot 2 board to find these hidden connections. Table III lists all details about the CT scan hardware and the corresponding software used.

By analyzing the traces revealed in the CT scan we successfully found hidden connections for VCCQ and RST BGA pins. We used metal shielding as the GND connection. The VDD pin substitutes for the VCC pin.

1) Logic Analyzer: Once we established a connection to all the ISP pins we used a logic analyzer to check the signal data

TABLE III
CT SCAN MACHINE MODEL AND RESPECTIVE SOFTWARE

CT Scan Machine	Software
NSI X3000 with PerkinElmer 1611 detector	efX-CT v2.1.8.0
NSI X5000 with Varian 4343 detector	efX-CT v2.1.8.0

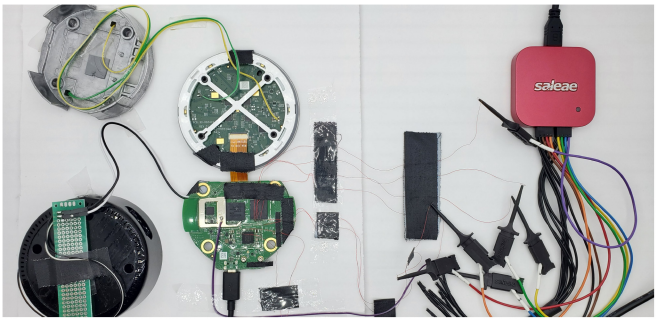

Fig. 6. Saleae Logic Pro 8 connected with the ISP pins that are micro-soldered on the main PCB of the second donor device.

TABLE IV
EMMC VOLTAGE COMBINATIONS (*Source*: JEDEC STANDARD JESD84-B451 PP-198 [26])

		VCCQ		
		1.1V - 1.3V	1.70V - 1.95V	2.7V - 3.6V
VCC	2.7V - 3.6V	Valid	Valid	Valid*
	1.7V - 1.95V	Valid	Valid	Not Valid

of the ISP connection (Fig. 6). The above-stated method cross-compares the BGA 221 pinout sheet from Section III-A and the CT-Scan images. The logic analyzer was also used to verify the individual pin voltages of recently identified ISP pins. The valid range for VCC and VCCQ is shown in Table IV.

C. ISP Data Dump

We first attempted to download all the data from the chip using the ISP connections through an eMMC reader. We micro-soldered all the ISP pins and connected them to the computer using an eMMC reader.

1) Reading as SD Card: The eMMC memory uses multimedia card (MMC), a type of embedded flash memory like an SD card, and follows a similar communication protocol.

Once we were able to test the following setup, we used an eMMC reader that connected the corresponding wires to the reader to pull data (as a binary file).

We also used additional tools like Binwalk, 7-Zip, PowerISO, and Magic ISO to inspect and extract the filesystem partitions from the dumped binary. Binwalk and 7-Zip are open-source tools, whereas Magic ISO and Power ISO are shareware. We used the shareware to verify the open-source tools' output.

D. Test Probe Jig Development

We measured the main PCB board's dimensions using a digital vernier caliper, converted a top-view image of the PCB board to scalable vector graphic (SVG) format, and verified the image's measurements with the caliper's readings before importing the SVG file to make an Stereolithography (STL) file for a 3-D printer. STL is a file format used to print on 3-D printers.

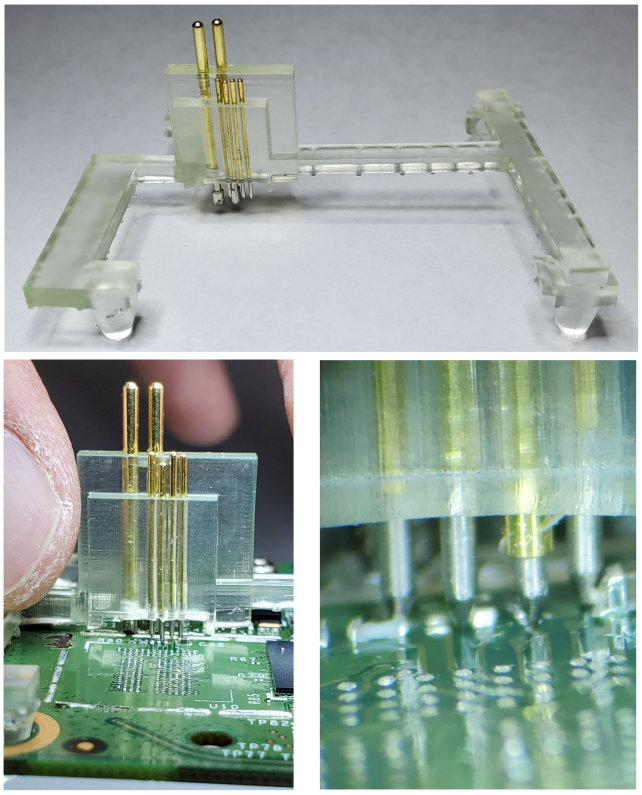

Fig. 7. Test Probe Jig.

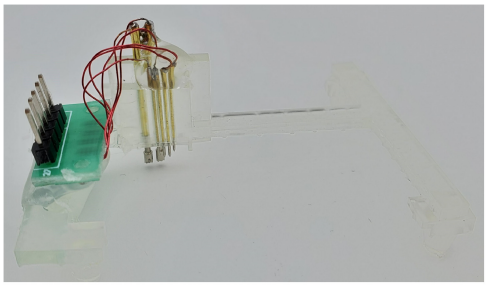

Fig. 8. Test Probe Jig's pogo pins are connected to a generic pinout using thin wires.

We used two programs, named Autodesk's Tinkercad and Fusion 360. We used Tinkercad to create a rapid prototype of the Test Probe Jig. When the jig design was closer to being finalized, we moved the 3-D model to Fusion 360 for further refinement before making the final 3-D print.

We used a Stereolithography (SLA) Liquid 3-D Printer (Elegoo Mars) to print a Test Probe Jig, as shown in Fig. 7. We used pogo pins, which are held together in the solidified Test Probe Jig resin, to connect with the preidentified ISP points on the PCB (Fig. 8).

We were able to read the memory chip using the Test Probe Jig by connecting to it with EasyJTAG as well as RIFF Box eMMC tools previously listed.

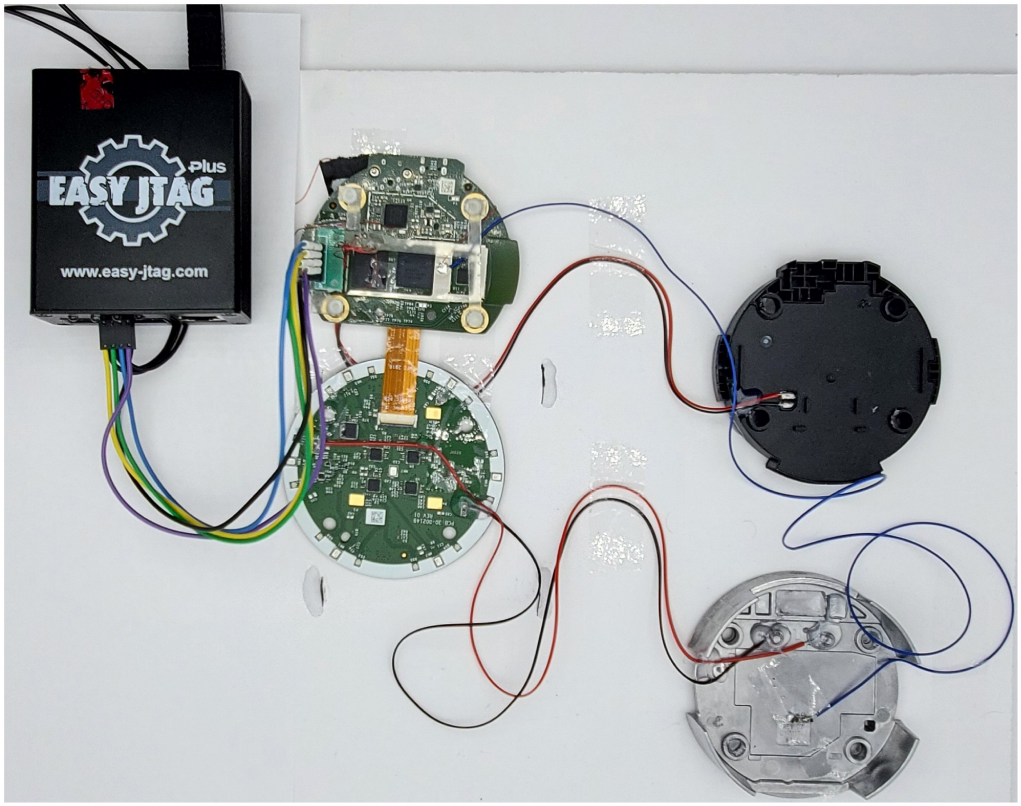

Fig. 9. Complete test Probe Jig setup. The USB connection from the EasyJTAG's top right goes into a laptop or computer.

E. Data Dump and Processing

We successfully downloaded all the data from the Echo Dot 2's memory as a binary file. The extracted data includes filesystem partitions used by the Echo Dot 2. Further details about the filesystem partitions are discussed in Section V.

IV. Experimental Setup

We connected the Test Probe Jig on the Echo Dot 2 with an eMMC reader and then to a computer. ISP can interact directly with the eMMC chip bypassing the need to use CPU to read the chip's data [24]. From a forensic perspective, it is important to ensure that the state of the digital device is preserved.

If the device is turned on accidentally, a substantial amount of data changes in the storage unit, as the CPU and the operating system will start making changes to several files. In other words, once a digital device is seized for investigation in a turned-off state, the investigators must not turn it on; otherwise, the seized device may not be considered admissible evidence in a court of law.

The ISP pins used by the Test Probe Jig could directly connect to the onboard eMMC chip and dump the data without starting the CPU or other components on the Echo Dot 2's PCB. This capability of the Test Probe Jig is similar to professional digital forensic tools and ensures that the Echo Dot 2's data dump is a forensically safe process.

We used two sets of pogo pins, namely, four P50-B1 (tip of 0.48 mm and length of 16 mm), and two P60H (tip of 1.5 mm and length of 24 mm). We used thin soldering wires to connect these six pogo pins to the eMMC reader (EasyJTAG).

The resistance of the connecting wires (between the pogo pins and the eMMC reader) should be as low as possible to avoid any potential voltage drops. The length of the wire should be as small as possible for a given width (diameter). The resistance of these connecting wires plays a crucial role in ensuring a successful data dump using the Test Probe Jig. We experimented with different thin wires for connecting the pogo pins to the EasyJTAG (Fig. 9). We were able to obtain a successful dump from the Test Probe Jig with wires that have a resistance of 0.083 Ω, with a width of 36 AWG (0.127 mm) and a length of 50.8-mm per wire. Once the setup was ready, we measured the respective voltages on all the pogo pins, which are presented in the table below (Table V).

A. Verification of the Extracted Firmware

We extracted Echo Dot 2's firmware (a binary file) residing in the eMMC chip using the Test Probe Jig. We used another tool called "Test Probe Wafer Station" to acquire the firmware of the same device.

The extracted firmware dump from the Test Probe Jig is then compared with the binary file obtained from the

TABLE V
VOLTAGES OBSERVED AT TEST PROBE JIG'S PINS WHEN IT IS FIXED ON ECHO DOT 2'S MAIN PCB AS SHOWN IN FIG. 1

Signal	Observed Voltage
VCC	3.30
VCCQ	1.80
CLK	1.78
DAT0	0.90
CMD	1.77

micro-soldered ISP pins (Section III-C). We then performed a chip-off on the same device, extracted the firmware, and compared it with the previous two cases. The comparison process is helpful to verify that the firmware dumps obtained from the Test Probe Jig, micro-soldering, and the chip-off methods are identical. We found that the SHA1 hashes of all partitions contained in the firmware obtained in these three cases match (refer Appendix B, Table VIII). Additionally, we also found that the partition hashes from these three cases also match with corresponding partitions obtained using the Test Probe Wafer station (refer Appendix B, TableTable IX). This verification proves that the firmware read from an Echo Dot 2 device using our Test Probe Jig produces same results when we use micro-soldering, chip-off, or the professional grade Test Probe Wafer Station.

V. RESULTS

We successfully extracted data from more than one Echo Dot version 2 device. One was new (hereafter referred to as the "baseline" or "new" device) and this contained no user data. A second device was previously used (hereafter referred to as a "used" device) and had been factory reset and resold from eBay as a "used and reset" device. We performed the factory reset process again, but we found that the device still contained some user data. The two separate data dumps from each of these devices were used for analysis and comparison. We used "Binwalk" on these respective binary files (from the new and the used Echo Dot 2) to examine their filesystem partitions.

The above-stated binaries were uncompressed into 25 "ext4" partitions, out of which there are nine unallocated spaces with sizes ranging from 33 to 32768 sectors (or 16.5 kB to 16.0 MB). The rest of the 16 partitions are shown in Table VI. These nine unallocated partitions are not present in the binary image of Alexa Pi (Echo Dot 2's firmware emulated on Raspberry Pi).

The last four partitions, namely, system_a, system_b, cache, and userdata, contain most of the forensically relevant data. We used "Autopsy," as one of our digital forensic tools, to process the above-stated binary files and the partitions inside them.

The current work presents some key forensic artifacts obtained from the used Echo Dot 2 device. We analyzed a fresh Echo Dot 2's binary dump, whose results are primarily used to compare with those of the used device. All results discussed below are from the used Echo Dot 2, unless specifically mentioned as having been obtained from the baseline device.

TABLE VI
PARTITIONS OBTAINED FROM THE ECHO DOT 2'S BINARY FILE (GPT HEADER)

S.No	Partition	Offset	Size
1	kb	000000100000-000000200000	1.00 MB
2	dkb	000000200000-000000300000	1.00 MB
3	lk_a	000001000000-000001100000	1.00 MB
4	tee1	000001800000-000001D00000	5.00 MB
5	lk_b	000002000000-000002100000	1.00 MB
6	tee2	000002800000-000002D00000	5.00 MB
7	expdb	000003000000-000003A00000	10.00 MB
8	misc	000003A00000-000003A80200	512.00 KB
9	persist	000004000000-000005000000	16.00 MB
10	boot_a	000005000000-000006000000	16.00 MB
11	boot_b	000006000000-000007000000	16.00 MB
12	recovery	000007000000-000008000000	16.00 MB
13	system_a	000009000000-000039000000	768.00 MB
14	system_b	000039000000-000069000000	768.00 MB
15	cache	000069000000-00009A000000	784.00 MB
16	userdata	00009A000000-0000E8FFBE00	1.23 GB

We presented the potentially relevant forensic information available on the Echo Dot 2 in Table VII in Appendix A. We found information related to WiFi connections, paired Bluetooth devices, unique identifiers, software versions, SQLite 3 databases, and logs.

This research did not find any user audio recordings of the user's interaction with the Alexa smart assistant inside the partitions. However, the current information obtained on the Echo Dot 2's memory chip could help a digital forensic examiner to answer important investigative questions related to the device. All queries related to unique identifiers used by Echo, Wi-Fi networks, connected Bluetooth devices, system and installed app information, firmware updates, and system logs can be answered using the Echo Dot 2 device's eMMC dump.

VI. DISCUSSION

The current work's contribution demonstrates a nondestructive method to extract data from an IoT device (Amazon Echo-Dot version 2 being an example) using a Test Probe Jig, which could help in digital forensics and cybersecurity operations. The data dump from the eMMC will help in the digital forensic investigation of a given Echo Dot 2. This nondestructive data extraction technique can be replicated by downloading the Test Probe Jig's STL file that can be printed on an appropriate 3-D printer by other investigators. Cybersecurity experts could use the proposed method to take out the firmware of an infected Echo Dot 2 and examine extracted malware or for other digital forensic analysis. The cybersecurity analysts could carry out vulnerability analysis of firmware version updates of the Echo Dot 2 (if the OEM firmware updates are not publicly available). A variety of use cases could be thought of that require researchers and practitioners to read, write, or update Echo Dot 2's firmware

without making any physical changes to the device. The hidden RST pin, discovered during CT Scan, is not used for dumping firmware binary from the eMMC; however, it could be instrumental in programming the chip (i.e., for write operations) to help cybersecurity-related tasks mentioned above. CT scans are trivial to hardware engineers and professional factories, but our audience of interest is the typical/commonly trained digital forensic examiner. The value of our approach is that one team/entity with this knowledge and access to (or ability to outsource) the CT scanner, can create a one-time design the Test Probe Jig that the commonly trained digital forensic examiner can then repeatedly create and use without special equipment or training.

We created a 3-D model of the Test Probe Jig, where generic pogo pins are fixed on precalculated positions. The pogo pins touch specific pinouts/taps on the Echo Dot 2 main PCB. These pinouts/taps are the basic ISP pins that could interact with the onboard eMMC chip without depending on the CPU as an intermediate. The pogo pins connections on the Test Probe Jig could interface with an eMMC reader on the other side and enable read and write operations on the memory chip. We have observed during our experiments (with the Test Probe Jig) that the CPU does not get switched on. Therefore, we think the voltages applied to these ISP taps by the Test Probe Jig do not damage components on the PCB. We have conducted multiple tests on different devices and have had consistent results without damaging the CPU or other PCB components. In addition, we have been able to power on the device normally after our experiments. The proposed solution is nondestructive, easily reproducible, portable, and affordable. The same procedure described in this article could be applied to other IoT devices or computer devices that use eMMC/eMCP chips for firmware and user data storage to create a customized Test Probe Jig for the new device. The 3-D model of the Test Probe Jig could be shared with known security and law enforcement agencies to print their own copy of the Jig.

Our method does not depend on the FCC ID information of the given IoT device. Interested researchers/practitioners can perform a chip-off on the donor device to learn the respective BGA pinout. Then, the working voltages of individual ISP pins can be checked using a logic analyzer or multimeter. Second, it does not depend on the test points that may be hidden on the main PCB. Researchers/practitioners could use the ISP pins instead that allow them to read the memory chip.

Finally, our method does not require JTAG or UART connections. JTAG and UART connections need to run the CPU to extract data from an eMMC chip on a given board. Thus, the CPU will change the state of a seized device from the digital forensic perspective. Moreover, most device manufacturers do not disclose their JTAG and UART connections information publicly, as in the case of Echo Dot 2.

Limitations of the Current Work: The proposed nondestructive solution will work on a majority of devices, but there are some exceptions. One of these exceptions would be where the necessary communication pins are intentionally hidden. These traces travel within the PCB substrate and do not have any tap on the surface. A CT-Scan will reveal the wiring inside the substrate; however, the pogo pins used in the Test Probe Jig will not be able to make contact without causing physical changes to the board. Another exception would be where the chip designer has used sealing material (like epoxy) to cover all surface taps originating or ending on the eMMC chip. The Test Probe Jig could work after the sealing material or epoxy is removed from the PCB as suggested by Heckmann et al. [27]. A third exception, which is a rare case, occurs when the device manufacturer uses a nonstandard memory chip for which the ISP pinout information is not publicly available. Another limitation is that the current version of the Test Probe Jig does not access the reset pin. We have identified the reset pin on the underside of the circuit board, but we did not include a connection to it in this version of the Jig.

VII. Conclusion

The current work proposes a nondestructive mechanism to read and write from an IoT device's onboard eMMC/eMCP chip. We used the Amazon Echo Dot 2; however, we believe that the proposed methodology could work on most IoT devices (and other similar mobile devices) that use eMMC for firmware and data storage. The proposed mechanism benefits from ISP pins, identified in a CT scan, available on the eMMC chip. These ISP pins permit direct communication with the eMMC chip without involving the onboard CPU. We developed a Test Probe Jig, which is a 3-D printed fixture that attaches to the Echo Dot 2's main PCB, holds pogo pins at specified locations to facilitate read–write operations from the eMMC chip.

A CT scan of the main PCB board was critically important with the challenging task of finding the eMMC's hidden ISP pins, and their outbound connection points on both sides of the board. This methodology does not require the FCC ID information about the targeted IoT device, because the CT scan and logic analyzer identify and verify the ISP pin locations that may be hidden and not published in the public domain about the device. This ISP pin information is used to design a 3-D Test Probe fixture. The entire process of creating a 3-D model of the Test Probe Jig is a one-time effort for the research and practitioner community. After that, other interested parties, like forensic investigators or researchers, can share the 3-D model design (*the STL file*) with their partners, who can print the Test Probe Jig at their location. The above-stated properties make the proposed nondestructive solution reproducible, portable, and affordable.

However, in case the command and data lines between the eMMC and CPU do not have a network TAP, or the manufacturer applies industrial epoxy-like solutions on the PCB surface, the current methodology would not work. There are workarounds for the above-stated situations, but they are not nondestructive, because they would require minor modification to the PCB.

Future Work: We would like to extend the current methodology to include more IoT and other mobile computing devices that use eMMC memory chips. The current version of the

TABLE VII
FORENSICALLY RELEVANT INFORMATION INSIDE ECHO DOT 2'S PARTITIONS

Category	Information	Address on Partition
WiFi	SSID	userdata/misc/wifi/wpa_supplicant.conf userdata/misc/wifi/wpa_supplicant.conf.tmp*
	DHCP	userdata/misc/dhcp/dnsmasq.leases
Bluetooth	MAC Addr.	userdata/misc/bluedroid/bt_config.xml userdata/misc/bluedroid/bt_config.old
	MAC Addr. of Supported Speakers	userdata/local/whad/btdevice.db.json; OR userdata/data/com.android.whad/btdevice.db.json
Identifiers	Account	userdata/data/com.amazon.client.metrics/shared_pref/account_change_observer.xml Userdata/data/com/amazon.imp/shared_prefs/account_change_observer.xml.bak*
	Customer; Device Serial; Session ID Keys	userdata/data/com.amazon.client.metrics/shared_pref/com.amazon.client.metrics.xml
	Various IDs	userdata/data/com.amazon.kindleautomatictimezone/shared_pref/SSOInfo.xml.bak, OR userdata/data/com.amazon.device.authutils/shared _pref/SSInfo.config.xml.bak*
Software Info	OS, Package list, Package usage	userdata/system/packages.list userdata/system/packages.xml userdata/system/package_usage.list
	GUID	userdata/local/system/guid
Databases	Timestamps of System Activities	userddata/vitals/vitals.db
	Published and Pending Updates	userdata/data/com.amazon.device.software.ota/databases/updates.db
	Downloads	usersdata/data/com.amazon.providers.downloads/databases/downloads.db
	System, Global, and Secure settings	userdata/data/com.android.providers.settings/databases/settings.db
	App Setting Variables	userdata/local/appreg.db system_a/etc/labdictionary/.dcp.db system_b/etc/labdictionary/.dcp.db
Text Files	Network	userdata/misc/wifi/networkHistory.txt
	Logs with timestamps in name	userdata/logd/Log.amazon_main@<UNIX Timestamp till miliseconds>.txt.zip userdata/system/dropbox/Log.amazon_main#<3 or 4 digit number>@<UNIX Timestamp till miliseconds>.txt.zip (*) userdata/logd/Log.kernel@<UNIX Timestamp till miliseconds>.txt.zip userdata/system/dropbox/Log.kernel#<3 or 4 digit number>@<UNIX Timestamp till miliseconds>.txt.zip (*) userdata/logd/Log.main@<UNIX Timestamp till miliseconds>.txt.zip userdata/system/dropbox/Log.main#<3 or 4 digit number>@<UNIX Timestamp till miliseconds>.txt.zip (*) userdata/logd/Log.metrics@<UNIX Timestamp till miliseconds>.txt.zip userdata/system/dropbox/Log.metrics#<3 or 4 digit number>@<UNIX Timestamp till miliseconds>.txt.zip (*) userdata/logd/Log.system@<UNIX Timestamp till miliseconds>.txt.zip userdata/system/dropbox/Log.system#<3 or 4 digit number>@<UNIX Timestamp till miliseconds>.txt.zip (*) userdata/logd/Log.radio@<UNIX Timestamp till miliseconds>.txt.zip userdata/system/dropbox/Log.radio#<3 or 4 digit number>@<UNIX Timestamp till miliseconds>.txt.zip (*) userdata/logd/Log.vitals@<UNIX Timestamp till miliseconds>.txt.zip userdata/system/dropbox/Log.vitals#<3 or 4 digit number>@<UNIX Timestamp till miliseconds>.txt.zip (*)
	System Events	userdata/system/dropbox/SYSTEM_LAST_KMSG#<3 or 4 digit number>@<UNIX Timestamp till miliseconds>.txt.gz (*) userdata/system/dropbox/system_app_crash#<3 or 4 digit number>@<UNIX Timestamp till miliseconds>.txt.gz (*) userdata/system/dropbox/SYSTEM_AUDIT#<3 or 4 digit number>@<UNIX Timestamp till miliseconds>.txt (*) userdata/system/dropbox/SYSTEM_BOOT#<3 or 4 digit number>@<UNIX Timestamp till miliseconds>.txt (*) userdata/system/dropbox/SYSTEM_RECOVERY_LOG#<3 or 4 digit number>@<UNIX Timestamp till miliseconds>.txt (*) userdata/system/dropbox/system_app_wtf#<3 or 4 digit number>@<UNIX Timestamp till miliseconds>.txt (*) userdata/system/dropbox/traces_commonlog.txt userdata/system/dropbox/drop112.tmp

*Deleted files; (*)Active as well as Deleted files

probe does not access the reset pin as it is not required for the read operation, but it is critical for writing back to the chip. Since our analysis did identify the reset pin on the underside of the board, an additional feature could be added to the Jig to connect to the bottom side, allowing writing capability to the jig setup.

APPENDIX A

See Table VII.

APPENDIX B

See Tables VIII and IX.

TABLE VIII
SHA1 HASHES OF ALL PARTITIONS INSIDE ECHO DOT 2'S FIRMWARE, EXTRACTED USING THREE DIFFERENT METHODS

Partition Name	Test Probe Jig	Micro-Soldering	Chip-off
kb.img	abb49fa42b4d0d772ddeee85dacbc873ef072b68	abb49fa42b4d0d772ddeee85dacbc873ef072b68	abb49fa42b4d0d772ddeee85dacbc873ef072b68
dkb.img	efd77635683a19e370178842437e84b95171b792	efd77635683a19e370178842437e84b95171b792	efd77635683a19e370178842437e84b95171b792
lk_a.img	0e2df990d50838a43909b5063a1a4537c87d1b28	0e2df990d50838a43909b5063a1a4537c87d1b28	0e2df990d50838a43909b5063a1a4537c87d1b28
tee1.img	5360d863883180ed359af3b8ec3c219eb47f1a94	5360d863883180ed359af3b8ec3c219eb47f1a94	5360d863883180ed359af3b8ec3c219eb47f1a94
lk_b.img	0e2df990d50838a43909b5063a1a4537c87d1b28	0e2df990d50838a43909b5063a1a4537c87d1b28	0e2df990d50838a43909b5063a1a4537c87d1b28
tee2.img	5360d863883180ed359af3b8ec3c219eb47f1a94	5360d863883180ed359af3b8ec3c219eb47f1a94	5360d863883180ed359af3b8ec3c219eb47f1a94
expdb.img	8c206a1a87599f532ce68675536f0b1546900d7a	8c206a1a87599f532ce68675536f0b1546900d7a	8c206a1a87599f532ce68675536f0b1546900d7a
misc.img	1904ddb1feb2f16d9ce69236cf859485614193bc	1904ddb1feb2f16d9ce69236cf859485614193bc	1904ddb1feb2f16d9ce69236cf859485614193bc
persist.img	3b4417fc421cee30a9ad0fd9319220a8dae32da2	3b4417fc421cee30a9ad0fd9319220a8dae32da2	3b4417fc421cee30a9ad0fd9319220a8dae32da2
boot_a.img	3372a7e8271a2235564a8906d8ea92b4c1c53f7b	3372a7e8271a2235564a8906d8ea92b4c1c53f7b	3372a7e8271a2235564a8906d8ea92b4c1c53f7b
boot_b.img	3372a7e8271a2235564a8906d8ea92b4c1c53f7b	3372a7e8271a2235564a8906d8ea92b4c1c53f7b	3372a7e8271a2235564a8906d8ea92b4c1c53f7b
recovery.img	6fe87320edc55c6382b7558857dff49f6685c527	6fe87320edc55c6382b7558857dff49f6685c527	6fe87320edc55c6382b7558857dff49f6685c527
system_a.img	c6d8411f98e94d13537fb3dd1635b915ce51bcfd	c6d8411f98e94d13537fb3dd1635b915ce51bcfd	c6d8411f98e94d13537fb3dd1635b915ce51bcfd
system_b.img	c6d8411f98e94d13537fb3dd1635b915ce51bcfd	c6d8411f98e94d13537fb3dd1635b915ce51bcfd	c6d8411f98e94d13537fb3dd1635b915ce51bcfd
cache.img	2ab18a3823b3a561b7055eaf5c08404eaa70b725	2ab18a3823b3a561b7055eaf5c08404eaa70b725	2ab18a3823b3a561b7055eaf5c08404eaa70b725
userdata.img	b7cf9dc702d5c1575551595154dbee903f4133e1	b7cf9dc702d5c1575551595154dbee903f4133e1	b7cf9dc702d5c1575551595154dbee903f4133e1

TABLE IX
SHA1 HASHES OF PARTITIONS INSIDE THE FIRMWARE OBTAINED USING TEST PROBE WAFER STATION

Partition Name	Test Probe Wafer Station
kb.img	abb49fa42b4d0d772ddeee85dacbc873ef072b68
dkb.img	efd77635683a19e370178842437e84b95171b792
lk_a.img	0e2df990d50838a43909b5063a1a4537c87d1b28
tee1.img	5360d863883180ed359af3b8ec3c219eb47f1a94
lk_b.img	0e2df990d50838a43909b5063a1a4537c87d1b28
tee2.img	5360d863883180ed359af3b8ec3c219eb47f1a94
expdb.img	8c206a1a87599f532ce68675536f0b1546900d7a
misc.img	1904ddb1feb2f16d9ce69236cf859485614193bc
persist.img	3b4417fc421cee30a9ad0fd9319220a8dae32da2
boot_a.img	3372a7e8271a2235564a8906d8ea92b4c1c53f7b
boot_b.img	3372a7e8271a2235564a8906d8ea92b4c1c53f7b
recovery.img	6fe87320edc55c6382b7558857dff49f6685c527
system_a.img	c6d8411f98e94d13537fb3dd1635b915ce51bcfd
system_b.img	c6d8411f98e94d13537fb3dd1635b915ce51bcfd
cache.img	2ab18a3823b3a561b7055eaf5c08404eaa70b725
userdata.img	b7cf9dc702d5c1575551595154dbee903f4133e1

ACKNOWLEDGMENT

The authors are grateful to CACI, Inc.-Federal, for their support of research activities at The Cyber Center for Security and Analytics, UTSA. They acknowledge that key parts of this research are based on work supported by the DEVCOM Army Research Laboratory—Research Associateship Program under Cooperative Agreement W911NF-21-2-0165. They also thank the Laboratory for Physical Sciences, College Park, MD, USA, for their technical assistance.

REFERENCES

[1] "Strategy analytics: New record for smart speakers as global sales reached 146.9 million in 2019." Feb. 2020. [Online]. Available: https://bwnews.pr/2WZINyk

[2] "Number of digital voice assistants in use worldwide 2019–2024," 2022. [Online]. Available: https://www.statista.com/statistics/973815/worldwide-digital-voice-assistant-in-use/

[3] S. Liu. "U.S. voice assistant users 2017–2022." 2022. [Online]. Available: https://www.statista.com/statistics/1029573/us-voice-assistant-users/

[4] "Global smart speaker market share 2016–2021." 2022. [Online]. Available: https://www.statista.com/statistics/792604/worldwide-smart-speaker-market-share/

[5] R. Brandom. "How much can police find out from a murderer's echo?" Jan. 2017. [Online]. Available: https://www.theverge.com/2017/1/6/14189384/amazon-echo-murder-evidence-surveillance-data

[6] E. D. L. Garza. "Charges dropped in Amazon echo murder case." Nov. 2017. [Online]. Available: https://www.courthousenews.com/charges-dropped-in-amazon-echo-murder-case/

[7] "Judge orders Amazon to hand over echo recordings in double murder case." ABC News. 2017. [Online]. Available: https://abcnews.go.com/US/judge-orders-amazon-hand-echo-recordings-double-murder/story?id=59100572

[8] K. H. U. L. Correspondent. "DNA evidence, Alexa recordings and second girlfriend come up in Farmington double murder trial." 2019. [Online]. Available: https://bit.ly/3Bu6623

[9] "Amazon information request report January–June 2020." 2020. [Online]. Available: https://d1.awsstatic.com/certifications/Information_Request_Report_June_2020.pdf

[10] H. Shafi. "Alexa is the new target in digital forensics investigation." Feb. 2020. [Online]. Available: https://medium.com/swlh/alexa-is-the-new-target-in-digital-forensics-investigation-e5eccba32e9f

[11] A. Fukami, S. Ghose, Y. Luo, Y. Cai, and O. Mutlu, "Improving the reliability of chip-off forensic analysis of NAND flash memory devices," *Digit. Investig.*, vol. 20, pp. S1–S11, Mar. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287617300415

[12] J. P. V. Zandwijk and A. Fukami, "NAND flash memory forensic analysis and the growing challenge of bit errors," *IEEE Security Privacy*, vol. 15, no. 6, pp. 82–87, Nov./Dec. 2017.

[13] C. Ence, J. R. Through, and G. Cantrell, "Chip-off success rate analysis comparing temperature and chip type," *J. Digit. Forensics Security Law*, vol. 13, no. 4, pp. 33–59, 2018. [Online]. Available: http://www.proquest.com/docview/2199174627/abstract/5F4DE74A3CC84EC5PQ/1

[14] S. Li, K.-K. R. Choo, Q. Sun, W. J. Buchanan, and J. Cao, "IoT forensics: Amazon echo as a use case," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6487–6497, Aug. 2019.

[15] "Alexa-Pi/AlexaPi." Feb. 2021. [Online]. Available: https://github.com/alexa-pi/AlexaPi

[16] H. Chung, J. Park, and S. Lee, "Digital forensic approaches for Amazon Alexa ecosystem," *Digit. Investig.*, vol. 22, pp. S15–S25, Aug. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287617301974

[17] S. Tristan, S. Sharma, and R. Gonzalez, "Alexa/Google home forensics," *Digital Forensic Education*, Cham, Switzerland: Springer, Jul. 2019, pp. 101–121. [Online]. Available: https://doi.org/10.1007/978-3-030-23547-5_7

[18] W. Jo et al., "Digital forensic practices and methodologies for AI speaker ecosystems," *Digit. Investig.*, vol. 29, pp. S80–S93, Jul. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287619301628

[19] Y. Shin, H. Kim, S. Kim, D. Yoo, W. Jo, and T. Shon, "Certificate injection-based encrypted traffic forensics in AI speaker ecosystem," *Forensic Sci. Int. Digit. Investig.*, vol. 33, Jul. 2020, Art. no. 301010.

[20] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 78, pp. 544–546, Jan. 2018.

[21] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1191–1221, 2nd Quart., 2020.

[22] D. A. Orr and L. Sanchez, "*Alexa*, *didyougetthat*? determining the evidentiary value of data stored by the Amazon® echo," *Digit. Investig.*, vol. 24, pp. 72–78, Mar. 2018.

[23] J. Bair, "Chapter 20—Nondestructive hardware and software solutions," in *Seeking the Truth from Mobile Evidence*, J. Bair, Ed. London, U.K.: Academic, Jan. 2018, pp. 297–309. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128110560000200

[24] J. Bair, "Chapter 30—eMMC reading and in-system programming," in *Seeking the Truth from Mobile Evidence*, J. Bair, Ed. London, U.K.: Academic, Jan. 2018, pp. 457–478. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128110560000303

[25] "eMMC pinouts—Home." Accessed: 2022. [Online]. Available: https://emmcpinouts.com/

[26] *EMBEDDED MULTIMEDIACARD(e•MMC) e•MMC/CARD PRODUCT STANDARD, HIGH CAPACITY, Including Reliable Write, Boot, Sleep Modes, Dual Data Rate, Multiple Partitions Supports, Security Enhancement, Background Operation and High Priority Interrupt (MMCA, 4.51)* JEDEC Standard JESD84-B451, 2010. [Online]. Available: https://www.jedec.org/sites/default/files/docs/JESD84-B451.pdf

[27] T. Heckmann, J. P. McEvoy, K. Markantonakis, R. N. Akram, and D. Naccache, "Removing epoxy underfill between neighbouring components using acid for component chip-off," *Digit. Investig.*, vol. 29, pp. 198–209, Jun. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287618302767

Albert M. Villarreal, III was born in Chicago, IL, USA, in 1995. He received the Associate degree in computer science in cybersecurity from Texas State Technical College (TSTC) in Harlingen, TX, USA, in 2016. He is currently pursuing the B.S. degree in computer science in cybersecurity and the B.S. degree in computer engineering with the University of Texas at San Antonio (UTSA), San Antonio, TX, USA.

Since 2019, he has been working as a Research Assistant with the Cyber Center for Security and Analytics, UTSA. His research interests include digital forensics, Internet of Things security and tool development, embedded security, reverse engineering, firmware emulation, chip-off data extraction, and PCB fabrication.

Mr. Villarreal, III won the Best Cybersecurity Presentation Award at UTSA Undergrad Research Showcase 2020.

Robin Kumar Verma received the Ph.D. degree in computer science and engineering from the Indraprastha Institute of Information Technology Delhi, New Delhi, India, in 2018.

Since 2018, he has been working as a Postdoctoral Researcher with the Cyber Center for Security and Analytics, University of Texas at San Antonio, San Antonio, TX, USA. His research interests include digital forensics, Internet of Things security and forensics, application of machine learning in digital forensics, cybersecurity, and privacy-preserving technologies.

Oren Upton received the bachelor's degree from The University of Texas at San Antonio (UTSA), San Antonio, TX, USA, in 1993, and the master's degree in national security affairs from the Naval Postgraduate School, Monterey, CA, USA, in 2004. He is currently pursuing the Ph.D. degree in information technology with UTSA.

He spent 24 years in the U.S. Air Force in fields of computer operations, software engineering, as well as intelligence analysis and red teaming, and he spent most of his career in the Air Force Office of Special Investigations conducting computer forensics, cyber intrusion investigations and cyber operations, as well as counter-intelligence operations and as an International Liaison Officer in Germany. He has also worked in industry in predictive data analytics and training for DOD defensive cyber teams. He currently works as a Researcher with UTSA in the field of cyber security with a focus in the area of Internet of Things devices, including vulnerability analysis, digital forensics, and IoT honeypots.

Nicole Lang Beebe (Senior Member, IEEE) received the B.S. degree in electrical engineering from Michigan Technological University, Houghton, MI, USA, the M.S. degree in criminal justice from Georgia State University, Atlanta, GA, USA, and the Ph.D. degree in information technology from The University of Texas at San Antonio (UTSA), San Antonio, TX, USA.

She is the Melvin Lachman Endowed Chair, the Professor of Cybersecurity, and the Chair of the Department of Information Systems and Cyber Security, UTSA. UTSA a National Center of Academic Excellence in Information Assurance and Cyber Defense for both education and research. She has over 20 years of experience in information security and digital forensics, from both the commercial and government sectors and is a Certified Information Systems Security Professional. She has published several journal articles related to information security and digital forensics in Decision Support Systems, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, *Digital Investigation*, and many other journals. Her research interests include digital forensics, cybersecurity, and data analytics.