Scientific Working Group on Digital Evidence

Best Practices for Internet of Things Seizure and Analysis

23-F-003-1.0

Disclaimer Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish standards, requirements, best practices, guidelines, technical notes, positions, and considerations in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

SWGDE requests notification by email before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, deprecated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

Redistribution Policy

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain this SWGDE cover page containing the Disclaimer Regarding Use.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or creation date) of the document and also indicate if the document is in a draft status.

Requests for Modification

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be submitted via the SWGDE Request for Modification Form or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)

c) Address
d) Telephone number and email address
e) SWGDE Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for suggested modification

Intellectual Property

All images, tables, and figures in SWGDE documents are developed and owned by SWGDE, unless otherwise credited.

Unauthorized use of the SWGDE logo or document content, including images, tables, and figures, without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Scientific Working Group on Digital Evidence

Best Practices for Internet of Things Seizure and Analysis

Table of Contents

1. Purpose

The purpose of this document is to provide general guidelines and best practices for interacting with devices considered to be part of the "Internet of Things" (IoT). These interactions include identification, seizure, preservation, acquisition/extraction, and analysis. This is a combined and updated document intended to supersede *SWGDE 22-F-001-2.0 Best Practices for On-Site Identification, Seizure, and Preservation of IoT Devices* and *SWGDE 23-F-001-1.0 Best Practices for Internet of Things (IoT) Acquisition and Analysis*, which are now in archived status.

For the purposes of this document, the term "examiner" is used broadly to refer to individuals who have specialized training, knowledge, skills, and abilities that allow them to handle a wide range of technical issues related to digital forensics, and who may be performing technical tasks to include collections, acquisitions, and/or analysis. The intended audience includes examiners and any other stakeholders in an investigation who may be dealing with IoT devices, such as first responders, investigators, attorneys who assist in the drafting of search warrants, and judges/magistrates who grant search authority.

Also, for the purposes of this document, the term "collection" refers to any operations involved in the gathering, seizing, etc., of items to be examined/analyzed.

2. Scope

IoT devices can range from consumer devices such as smart home devices and wearable technology, to industrial devices such as machinery, production equipment, and the systems and assets that comprise a country's critical infrastructure. This document focuses on IoT devices marketed for personal and consumer/residential use and will address acquiring and analyzing data derived from the internal storage capabilities of IoT devices as well as the integration of data acquired from the cloud, other collateral storage, and services in the examination of IoT devices. Additionally, this document will provide recommendations on additional items to consider that may be connected to the device via an application, Wi-Fi, or Bluetooth which may contain additional data related to connectivity.

3. Limitations

This document is not all-inclusive, does not contain information relative to or in support of specific commercial products, and is not intended to be a training manual or to specify operating procedures. The ideas, concepts, and technical aspects of acquiring and analyzing data from IoT devices are strictly related to what was available at the time this document was created.

4. Considerations

Due to the nature and size of these devices, the types of storage medium and format of data used by these devices are highly diverse and may include novel systems. Assumptions as to the type and location of potential artifacts should not be based on make, device type, or model, owing to the variety of chipsets that may be contained in them, changes that can occur from one software update to another, and other variables.

Due to the nature of technology, development, and manufacturing in the IoT space in particular, changes can happen quickly. There may be added features or capabilities developed in the future, both on the tool side and on the forensic target device side, that could alter the acquisition and analytic methodology addressed in this document, and any analysis or decision-making should take these variables into account.

Not all skill sets overlap. For example, someone who is proficient on vehicle forensics may not be as proficient with the considerations of drone seizure and acquisition. If a practitioner or other stakeholder is dealing with technology outside their area of expertise, particularly in an active environment (such as on-scene) where an incident has taken place that is now part of an investigation, they should consult with an appropriate specialist. For recommendations on training core competencies for IoT forensics, please see *SWGDE 19-F-001-1.0 Core Competencies for Embedded Device Forensics*.

5. Overview

IoT is a system of interrelated computing devices, which can be any combination of mechanical and digital machines or objects, that are provided with unique identifiers and the ability to transfer data over a network, whether internal or external, without requiring human-to-human or human-to-computer interaction. Additional information can be found in *SWGDE 20-F-004-1.0 Technical Notes on Internet of Things Devices* and *NIST Special Publication 1900-202 Cyber-Physical Systems and Internet of Things*.

Data can be generated by IoT devices in numerous ways (e.g., sensors, manual input, triggers, etc.), and the data collected by IoT devices can be used for a variety of purposes, including monitoring and controlling devices, automating processes, and improving efficiency.

The IoT concept is based on the idea that everyday objects can be connected to the internet and made to communicate with each other, creating a more connected and smarter world. This has the potential to transform many industries and aspects of our daily lives, from healthcare and transportation to agriculture and home automation.

IoT devices frequently communicate through a local area network, such as a home router or proprietary hub with wired and/or wireless access, typically send or receive commands and information to/from cloud service providers and may allow human and other interactions using companion applications on mobile devices or computers. IoT devices can also communicate with other devices and services through Bluetooth, mobile data (cellular), and proprietary and open-source communication protocols (e.g., Zigbee, Z-Wave).

Communication between devices can include logs that contain timestamps. For example, a cellular phone being carried around a residence that is paired with IoT devices in that same location could potentially log when it connects. An analysis of the log files from the IoT device can show when a phone or connected mobile device was in the vicinity.

6. Reference Data

As IoT forensics is a relatively new practice, several organizations are working to provide datasets and processes to the community. The information will not only assist with tool development, but overall examiner understanding of the tasks involved in examining a device. There are several databases where practitioners collaborate on IoT device forensics, to include the following:

- NIST Computer Forensic Reference Dataset Portal https://www.nist.gov/programs-projects/computer-forensic-reference-data-sets
- The Artifact Genome Project, University of New Haven https://agp.newhaven.edu/about/start/
- Technical training organizations (e.g., NW3C, NCFI, FLETC, NCJTC)
- Educational institutions (e.g., Marshall University, Champlain College, Leahy Center for Digital Forensics & Cybersecurity, Purdue University, Oklahoma State University)

7. Identifying and Locating IoT Devices

Becoming familiar with IoT devices will assist in search warrant affidavits and identifying devices on scene. Proper identification of IoT devices on scene is necessary due to the potential investigative value of the data contained, much like a computer or mobile device. Artifacts recovered from IoT devices may answer who, what, when, where, and why questions that other devices may not; however, certain facts must be considered when identifying these devices.

A variety of IoT devices are currently available and the market is rapidly expanding. The usage and capabilities of most devices are identifiable by the manufacturer's marketing or user materials and conducting online research. However, some IoT devices may not be easily identifiable by their external appearance or markings. IoT devices have various functions and capabilities, and for the purpose of identification these devices can be separated into several classes, or groups of devices. The following is not meant to be an all-inclusive or comprehensive list, but rather supply information related to the various classes to aid investigators in their searches. For further reference, some examples of makes and models of devices have also been provided.

- Smart Speakers/Smart Displays – These devices typically contain a speaker/microphone combination device with an integrated virtual assistant that offers interactive actions and hands-free utilization with the help of an activation phrase, or "wake word". Devices may also be present with haptic (touch) feedback displays. Users may personalize the functionality, such as by setting individual voice recognition or selecting a wake word other than the default. These devices may include, but are not limited to:
    - Amazon Echo Dot/Spot
    - Google/Nest Home
    - Amazon Echo Show

  - Google Nest Hub
  - Facebook/Meta Portal
- Wearables – Wearable technology (also called wearable gadgets) is a category of technology devices that can be worn by a consumer. These devices may include, but are not limited to:
  - Watches and Fitness Trackers
    - Apple
    - Samsung Galaxy
    - Google Pixel
    - Fitbit
    - Garmin
    - Suunto
  - Shoes
    - Nike Adapt
    - Under Armour HOVR
  - Clothing
    - Levi's Commuter Jacket
    - Siren Socks
    - Hexoskin Shirts
  - External medical Devices (e.g., Continuous Positive Airway Pressure [CPAP], hearing aids, glucose/insulin pump)
- Smart Tags - An electronic tag with an embedded Radio-Frequency Identification (RFID), Bluetooth Low Energy (BLE), Near Field Communication (NFC), or GPS device, attached to an object for the purposes of tracking or storing data relating to its use. These devices may include, but are not limited to:
  - AirTag
  - Tile
  - Chiplo
  - FitBark
- Sensors – A sensor is a device that detects or measures a physical property and records, indicates, or otherwise responds to it. These devices may include, but are not limited to:
  - Motion
  - Light
  - Sound
  - Break/Separation Contact
  - Vibration
  - Position

  - Temperature
  - Humidity
  - Gas/Particulates
- Control Systems – A control system bridges and manages, commands, directs, or regulates the behavior of other devices or systems, and typically allows the manipulation of devices by using mechanisms such as actuators and motors to convert energy into motion. These devices may include, but are not limited to:
  - Door locks
  - Garage door openers
  - Irrigation
  - Fire suppression
  - Heating, Ventilation, and Air Conditioning (HVAC)
- Capture – Devices that capture information/data, may store for later exfiltration, and may broadcast data externally. These devices may include, but are not limited to:
  - Cameras (including smart doorbells)
  - Microphones
  - Magnetic Card Readers (Skimmers, Square, etc.)
  - Point of Sale (PoS) peripherals
  - Automated Teller Machines (ATM)
- Implants – Devices not readily accessible, since they are designed to operate internally to another body, typically a living being such as a human or animal. These devices may include, but are not limited to:
  - Cochlear
  - Pacemaker/Defibrillator
  - Radio Frequency Identification (RFID) Module
  - Near-Field Communication (NFC) Module
- Appliances – Machines/devices used to perform household functions. These devices may include, but are not limited to:
  - Refrigerators
  - Coffee makers
  - Washer & Dryers
  - TVs
  - Smart Locks
  - Robotic vacuums

8. Collection

When collecting any digital evidence, it is best to first reference the *SWGDE 18-F-002-1.0 Best Practices for Digital Evidence Collection*. In addition to those best practices, the following should be considered.

While documenting the scene, be sure to include the contents of a display or other device status indicators (eg., blinking lights), prior to taking any further action. Special attention should be paid to the preservation process and its impact on collection, as well as the potential for additional evidence (e.g., latent prints, DNA, spatter evidence on the surface of devices, etc.).

IoT devices can be set up maliciously to create obstacles for law enforcement responding to scenes, and while attempting to isolate a device, the collector also needs to be aware of trigger events. Trigger events may include (but are not limited to) manipulation of the device itself, motion/movement caused by collectors (which may be detected by connected sensors), manipulation of connected switches (e.g., light switch), making sounds within a detectable threshold of a device, disconnecting the power and/or data connection, etc. These actions may cause an update/alteration of the data to be analyzed, possibly alert the owner to the collector's presence, and may cause a cascade of other trigger events to include events that may be hazardous to the safety of the collector.

Some devices listen passively, and only trigger with the verbalization of an activation/wake word. On scene this could be done accidentally, such as by one collector telling another that they found an Alexa device, and the conversation was picked up by the microphone of a device using "Alexa" as the wake word. A sampling of default "wake words" are as follows:

Device	Virtual Assistant / AI Interface	Default Wake Word
Amazon Echo	Alexa	Alexa
Google Home	Google	Hey Google OK Google
Facebook/Meta Portal	Alexa	Alexa Hey Portal
Apple Home Pod	Siri	Hey Siri

Table 1. Sampling of Default "Wake Words." (Table Credit: SWGDE)

Many IoT devices utilize multiple forms of communications technology, some of which may even allow a device to serve as the central hub for user control of multiple other IoT devices. Each device can have its own designated interface and features and is usually controlled via application or home automation software. To find devices that may not be immediately apparent, one may perform a wireless scan of a subject area using a variety of protocols e.g., 4G/5G

Cellular, Wi-Fi, Bluetooth, Zigbee and Z-Wave. There is an assortment of tools to accomplish this task, (e.g., Fing, Redfang) as part of the Kali Linux distribution (detects items in promiscuous mode). Additionally, router reboots may assist in detecting additional devices connected to the network. It is important to note that mesh networks such as Zigbee and Z-Wave can add additional distance by serving as a "hop" to the primary device; therefore, at some distances some but not all devices may be detected. Additionally, BLE devices may be sleeping until woken.

As IoT devices may access the internet through hubs and routers, those items should be identified as well. Consideration should also be taken in preserving (sending in a preservation order) and capturing data that is possibly stored in the cloud, on mobile and other linked devices, and with other parties.

Although many IoT devices may not currently store a significant amount of data on the device, they could provide information leading to data stored elsewhere, such as with a cloud service provider, personally owned computer, mobile device, or other IoT devices. Relevant data may be accessible from those devices. If additional devices are discovered, the same collection and acquisition procedures should be followed to secure/isolate the newly discovered devices.

Devices must be isolated from their network(s). One method of isolating a device from the network is to unplug the power to the device or remove the battery power. If the device cannot be powered off using these methods, use RF isolation and treat all devices as though they have power. Never place a loose battery into an RF isolation unit, as it could create a fire hazard or turn the shielding material into an antenna. In cases where IoT devices are hardwired into power supplies, and first responders lack either the knowledge or authority to remove the device, remove power at the circuit breaker (being mindful of other devices of evidentiary interest that may be on the same circuit). Where the power cannot be removed, and the devices cannot be directly isolated from the network, removing Internet connectivity can be achieved by disconnecting the network cable, wireless access point, switch, router, or modem. This action should be weighed against the potential impact of removing network connectivity to any non-targeted devices. Be mindful of IoT devices that may be actively reporting their location (e.g., AirTags) that may be beaconing, and possibly interacting with other devices (including that of the responder) in the environment.

Collection procedures are dependent on several device characteristics due to the disparate way IoT devices receive power and communicate. The characteristics include the following items.

- Form Factor - The differences in the devices can range from the discreet to visually obvious. Devices may contain any number of items to include cameras, microphones, or other sensors that can be miniaturized and embedded in other objects. Radio frequency technology may be used in less than intuitive ways, such as for motion detection.
- Power - When collecting a device from a scene, to minimize changes one must remove power from the device. Devices may be wired for power, run on a battery, or perhaps may have both wired and battery power. Device configuration and hardware mounting,

such as a smart doorbell mounted to an exterior door frame, may make power assessment challenging and require pre-collection research.

- Artifact/Data Storage - IoT devices store artifacts across an array of locations. Probative data may exist locally or remotely to a sensor or device and have finite storage and persistence. One must be ready to collect a physical device and investigate a network storage location. That location could be near the device, or within a vendor's cloud storage.
- Connectivity - IoT devices use several communication protocols. To properly seize and preserve a device, one may need to assess if there is a presence of a hub, a router, or if the device connects directly to the internet. In instances wherein a hub or a router are used, those items should also be collected.
- Artifact/Data Spoliation - Specific Considerations/Cautions (Instances where probative data exists in volatile memory only or where data overwrites or appends in a finite storage setting)
- Specific Device Risk - Considerations or exposures to avoid (Instances where fragility, temperature, moisture, or other sensitivity risk to the device and data exist)
- Device Security - Considerations regarding security design (Technology designed to invoke security related to locally stored data, network or ad hoc connections, and data transmission)
- Identifiers - Taking pictures of the make/model/serial number and Media Access Control (MAC) address of the device may be useful documentation when attempting to match connections to other devices such as smartphones. Identifiers in an IoT Standard are typically divided into the following categories:
    - Object identifier
    - Communication identifier
    - Application identifier

9. Preservation

Just as the integrity of the data of more traditional devices needs to be preserved through write-blocking or other means, IoT devices and associated applications similarly need information protected and preserved.

Each IoT device has different considerations. Maintaining power and/or connectivity on some devices could be detrimental to preserving artifacts of interest while other devices must have power and/or network connectivity maintained to preserve the data.

For IoT devices where power needs to be severed during collection procedures, one must ensure all power and consequently all network connectivity to the device remains off throughout all packaging, transport, and pre-examination storage. Beware of capabilities such as hibernation

mode, which may still allow network connectivity. This may require complete disassembly of the device. In some instances, the battery may be embedded and not easily removable.

For devices containing volatile data or other considerations that require network connectivity, time may be critical (such as in the case of certain location monitoring/tracking devices, where analysis must be completed within a limited number of days of losing contact with the connected account or data loss will occur) and analysis should be prioritized with these considerations in mind.

Potential artifacts may also be stored at third party cloud service providers. As such, one should send preservation notices to the appropriate providers as soon as any user accounts are realized.

10. Other Considerations

One of the major challenges in data acquisition from IoT devices is the lack of available training, tools, research documents, and collection procedures. Manufacturers may be reluctant to provide assistance or access to information regarding their proprietary intellectual property and may not be forthright regarding the device or user data available.

Relevant investigative data may be found on one, or across multiple IoT devices in a network, as they communicate and share data with each other. This data may be stored within a particular device, within a companion app stored on a mobile device or tablet, or with a cloud service provider. The totality of the scene, the nature of the investigation and the potential for a device to store data of interest should dictate the necessity to interrogate or seize particular IoT devices.

There may also be data located in unexpected places due to the integration of devices and platforms via third party and other connective services. An example of this is “If This Then That” (IFTTT.com), which allows for triggers and data from one cloud (e.g., Amazon) to cause events and/or replicate data in another cloud (e.g., Google) in ways that may not have been originally intended or particularly advocated/featured by each manufacturer.

Many devices have the capability to record audio/video or perform live-listening which collectors and others on-site should be cognizant of, as it may alert the owner to the presence of people on-site and/or create concerns of recorded or broadcasted movement and conversations. If an IoT device records audio while investigators are on scene and the resulting speech-to-text conversion is inaccurate, the statements made could be misinterpreted.

Some devices may require additional safety considerations (e.g., wearables have a higher propensity of skin contact and may allow for transfer of pathogens or biological hazards. Some devices may have moving parts that could cause bodily injury).

The examiner shall consider how the seizure of or interaction with a device could impact the safety and wellness of the owner or user of the device. For example, IoT devices that offer a direct impact on the health of an individual (e.g., medical IoT devices), should not be seized if it would endanger the wellbeing of its user.

11. Artifact Locations

IoT devices commonly store data in one or more locations.

- Locally on the device
- Manufacturer Companion Applications/Programs
- Other connected devices
- Cloud Storage
- Communication/Networking Devices and Providers Router or Internet Service Provider logs and transactional data
- Third Party Companion Applications and Cloud Storage

This information can be important investigative material and could also be used to gain access to other devices that need to be considered for potential evidence. Examples of artifacts may include:

- Connectivity logs, user information, time/date stamps
- SSIDs (identifying current and possibly even previous networks where the device has established a connection)
- Passwords
- Bluetooth MAC addresses (of one or more of the devices that had been previously connected)
- Modified, Accessed, and Created times
- Application use logs
- Internet browser searches and history
- Videos watched

Regardless of whether it is suspected that the different locations will have the same or similar artifacts, efforts should be made to analyze each location. Updates can change the content of previously known artifacts, user activity can change artifacts in one location and the artifacts from another location can help an examiner understand the changes, etc. Artifacts in all locations should always be considered as a whole to form a complete picture.

11.1 Artifact Locations Locally on the Device

IoT devices may locally store a variety of data, both persistently and in a volatile manner, that could be relevant to an investigation.

- Persistent
    - Data stored persistently is not purged when power is disconnected or when the storage medium containing the data is removed from the environment/system.
- Volatile

- Data stored in a volatile manner is data that is more vulnerable to unintentional change or loss and may be purged/lost or easily affected by changes to the environment/system such as loss of power.

11.2 Artifact Locations on Manufacturer Companion Applications/Programs

Program or application located on a connected mobile or computing device used for monitoring and control of the IoT device being analyzed.

11.3 Artifact Locations on Other Connected Devices

Other devices may be connected within the same ecosystem or network. These may contain more or less data and may or may not use the same storage type/standard with some data being volatile and some being persistent. The consideration here is that more than one device may be part of the full picture or the device of interest may not even contain the artifacts it is responsible for generating.

11.4 Artifact Locations in Cloud Storage

Most readily accessible and retrievable data relating to an IoT device can be expected to reside primarily within the manufacturer's cloud or designated cloud service provider.

11.5 Artifact Locations on Communication/Networking Devices and Providers

- Transactional records and/or logs from a manufacturer's device hub (if present)
- Logs from routers and network equipment
- Transactional records and/or logs from an Internet Service Provider
- Transactional records and/or logs from a Cellular Service Provider

11.6 Artifact Locations in Third-Party Companion Applications and Cloud Storage

Data may also be stored by third parties in a companion app and/or a third-party cloud location.

12. Assessment and Handling

Some devices may have special considerations, such as volatile data or connectivity needs. In these cases, time may be of the essence (data loss may occur in the case of certain location monitoring/tracking devices, where the analysis must be completed within a limited number of days of losing contact with the owner) and analysis should be prioritized with these considerations in mind.

Factors to consider:

- Determine the steps taken during seizure and preservation.
- Assess the preserved state of the device and connected devices (if it's in faraday isolation, cloud preserved, etc.).
- Determine environmental needs for analysis and establish an appropriate environment.

- Determine, if possible, the level of invasive analysis needed.
    - Are Universal Serial Bus (USB) or other standard user-interface ports available?
    - Are In-System Programming (ISP), Joint Test Action Group (JTAG), and/or Universal Asynchronous Receiver-Transmitter (UART) connections and pinouts available?
    - Is chip-off necessary?

13. Acquisition/Extraction

Some IoT devices are accessible through manufacturer-developed software or applications that work across multiple operating systems. In contrast, others may be accessed through third-party applications (e.g., video monitoring apps) or sub-applications. Some also may be accessible through a web interface or Application Programming Interface (API) and may require an authentication process to gain access. The technical capabilities and interactive monitoring or control of comparable product offerings from different manufacturers may vary.

After receipt of an IoT device, there are many different aspects to consider prior to acquisition. Before beginning an acquisition/extraction or analysis, community resources should be consulted to see if tools, solutions, and/or methodologies have already been developed for the device. With a constantly growing body of research and experience in the community, resources such as crowdsourced forensics and developments in efforts such as artifact catalogs may be able to provide substantial assistance as well as be benefitted from any new findings encountered in an investigation. Additional resources on these topics can be found at *Crowdsourcing Forensics: Creating a Curated Catalog of Digital Forensic Artifacts* and *The Artifact Genome Project (website)*.

13.1 Acquisition/Extraction Locally on the Device

- Persistent
    - Storage mediums capable of persistently storing data may vary in type and standard. This type of storage is typically composed of embedded microchips that operate using NOR or NAND standards in their various forms, each of which has different options/considerations/tools/requirements for interfacing and processing. For examples of working with persistent storage, potentially at the chip level, refer to *SWGDE 15-F-002-1.0 Best Practices for Chip-Off*, *SWGDE 16-F-004-1.0 Tech Notes Regarding Chip-off via Material Removal Using a Lap and Polish Process*, and *SWGDE 15-F-001-1.0 Best Practices for Examining Mobile Phones Using JTAG*.
- Volatile
    - Not generally accessible with today's technology and processing tools. At the time of this publication, limited research exists regarding the viability of unencrypted data recovery from volatile memory contained in IoT devices. Unless

accessing volatile memory is necessary and critical to an investigation, IoT devices should generally be powered off.

Technical investigators seeking information directly from an IoT device may be required to utilize invasive, and potentially destructive, forensic techniques like those used for mobile devices (e.g., smartphones and tablets). See *SWGDE 18-F-03-1.2 Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition*, *SWGDE 15-F-002-1.0 Best Practices for Chip-Off*, and *SWGDE 16-F-004-1.0 Tech Notes regarding Chip-off via Material Removal Using a Lap and Polish Process*. However, minimally invasive techniques (e.g., JTAG, ISP, UART) may be available to acquire even a full physical acquisition of the on-board memory of IoT devices, see *SWGDE 15-F-001-1.0 Best Practices for Examining Mobile Phones Using JTAG*.

13.2 Acquisition/Extraction of Manufacturer Companion Applications/Programs

A platform, such as a mobile device or computer, that has been connected to an IoT device may contain evidentiary data from the linked device, which can be recovered using traditional forensic methods and tools.

13.3 Acquisition/Extraction of Other Connected Devices

Any additional connected devices should be processed with the same considerations and should not necessarily be expected to be similar to one another, but artifacts recovered should have consideration given as to how they corroborate as a whole.

13.4 Acquisition/Extraction of Cloud Storage

Accessing data derived from IoT Cloud storage may require a legal process served upon the cloud storage provider. Some cloud service providers may encrypt the data, and a decryption/forensic tool may be needed to view the data. See *SWGDE 19-F-002-1.0 Best Practices for Digital Evidence Acquisition, from Cloud Service Providers.*

13.5 Acquisition/Extraction of Communication/Networking Devices and Providers

Analysis of network traffic of the device in its original environment may be necessary to find/understand artifacts. Considerations may include:

- Communication/Networking equipment are typically embedded systems with similar properties as IoT devices (and are actually often considered to be IoT devices themselves), so extracting transactional records and/or logs from physical equipment may need to be extracted the same way and with the same considerations as an IoT device, with some data being persistent, some volatile, some requiring static analysis, and some requiring dynamic analysis to be fully examined and/or understood.
    - These types of artifacts may establish details such as when data was sent or received, identifying information, addressing, etc., however, the content from the device may be encrypted or otherwise protected/obfuscated.

- Transactional records and/or logs from Internet Service Providers and Cellular Service Providers may also be available and retrieved by methods such as subpoena request or search warrant.

13.6 Acquisition/Extraction of Third-Party Companion Applications/Programs and Cloud Storage

IoT devices often have additional functionality and connectivity available via third parties. These third parties may gather and store data from devices the same as the device manufacturers and not only may retain the same or even additional data than what the manufacturer preserves but may also have different storage and handling requirements that do not have the same rigors or legal restrictions.

- Examples of third parties could include entities such as media content providers for smart speakers, monitoring entities for smart sensors, online data storage providers for surveillance systems, services for augmenting and amplifying connectivity between manufacturer ecosystems, and more.

14. Post Extraction/Acquisition Data Analysis

14.1 Post Extraction/Acquisition Data Analysis Locally on the Devices

- Many IoT devices utilize file systems that some traditional digital forensic tools do not support
    - Examples of these filesystems include Unsorted Block Image File System (UBIFS), Yet Another Flash Filesystem (YAFFS), and SquashFS.
- Unique operating systems may also be used, which may necessitate the use of different examination methods and tools, even if a familiar filesystem is present. These include operating systems, such as the Fire OS, used in a variety of Amazon devices, and Tizen, which is used in devices such as Samsung Smart TVs.
    - Figure 1 displays the identified filesystem from a Tizen based IoT refrigerator. The tool used in this example was partially successful as it was able to show logical files from the filesystems and partitions marked with the “+” icon. However, the tool was unable to parse logical data from all the other identified filesystems and partitions.

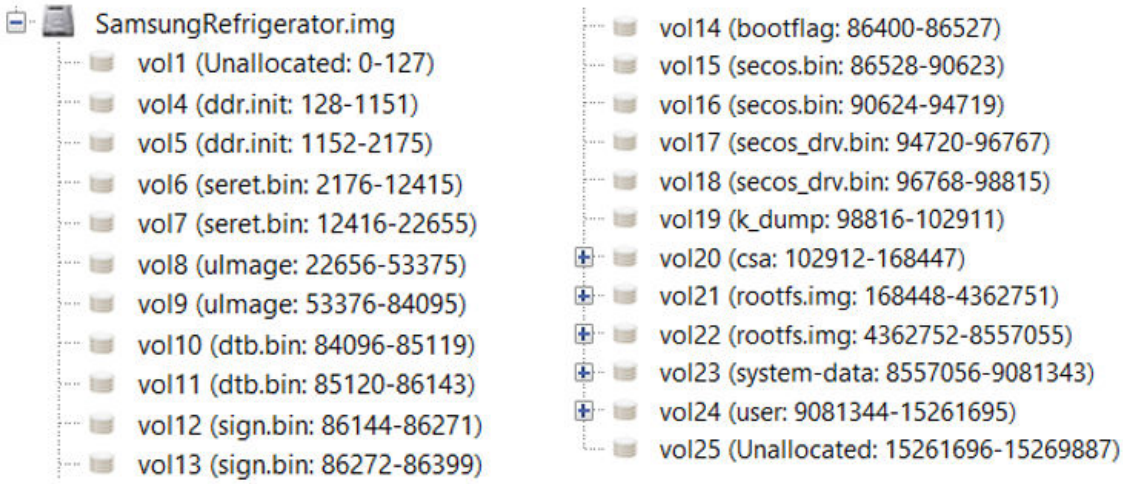
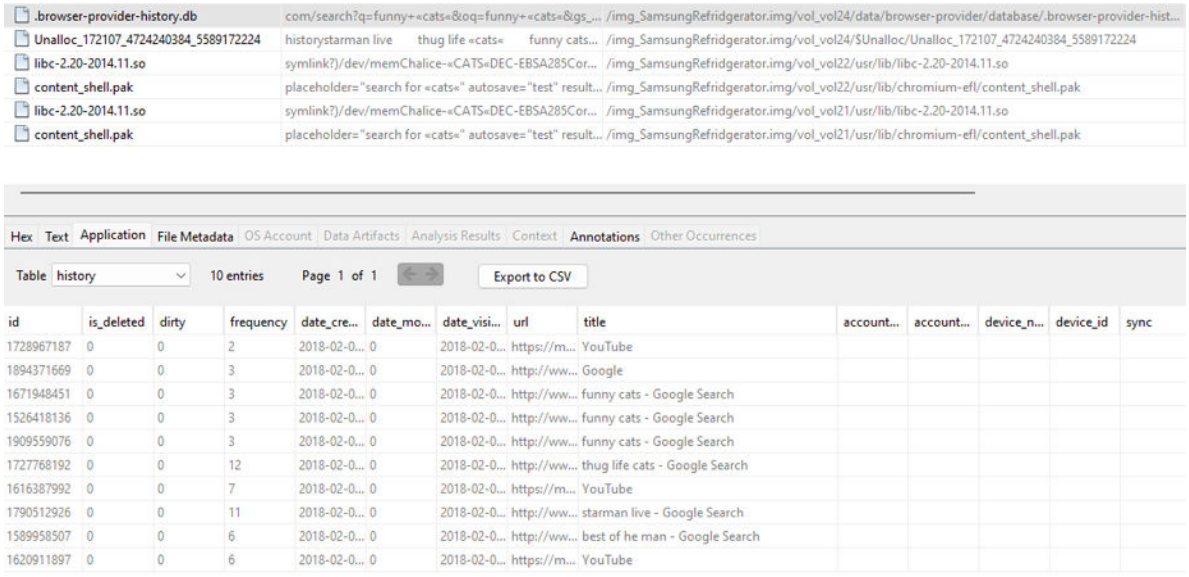


Figure 1 Files marked with the "+" icon. (Image Credit: SWGDE)

- The next example shows the logical files from an IoT device partition that was successfully identified and supported by the tool (Figure 2).



.browser-provider-history.db	com/search?q=funny+«cats«&oq=funny+«cats«&gs_...	/img_SamsungRefridgerator.img/vol_vol24/data/browser-provider/database/.browser-provider-hist...
Unalloc_172107_4724240384_5589172224	historystarman live thug life «cats« funny cats...	/img_SamsungRefridgerator.img/vol_vol24/$Unalloc/Unalloc_172107_4724240384_5589172224
libc-2.20-2014.11.so	symlink?)/dev/memChalice-«CATS«DEC-EBSA285Cor...	/img_SamsungRefridgerator.img/vol_vol22/usr/lib/libc-2.20-2014.11.so
content_shell.pak	placeholder="search for «cats«" autosave="test" result...	/img_SamsungRefridgerator.img/vol_vol22/usr/lib/chromium-efl/content_shell.pak
libc-2.20-2014.11.so	symlink?)/dev/memChalice-«CATS«DEC-EBSA285Cor...	/img_SamsungRefridgerator.img/vol_vol21/usr/lib/libc-2.20-2014.11.so
content_shell.pak	placeholder="search for «cats«" autosave="test" result...	/img_SamsungRefridgerator.img/vol_vol21/usr/lib/chromium-efl/content_shell.pak

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Table: history | 10 entries | Page 1 of 1 | Export to CSV

id	is_deleted	dirty	frequency	date_cre...	date_mo...	date_visi...	url	title	account...	account...	device_n...	device_id	sync
1728967187	0	0	2	2018-02-0...	0	2018-02-0...	https://m...	YouTube					
1894371669	0	0	3	2018-02-0...	0	2018-02-0...	http://ww...	Google					
1671948451	0	0	3	2018-02-0...	0	2018-02-0...	http://ww...	funny cats - Google Search					
1526418136	0	0	3	2018-02-0...	0	2018-02-0...	http://ww...	funny cats - Google Search					
1909559076	0	0	3	2018-02-0...	0	2018-02-0...	http://ww...	funny cats - Google Search					
1727768192	0	0	12	2018-02-0...	0	2018-02-0...	http://ww...	thug life cats - Google Search					
1616387992	0	0	7	2018-02-0...	0	2018-02-0...	https://m...	YouTube					
1790512926	0	0	11	2018-02-0...	0	2018-02-0...	http://ww...	starman live - Google Search					
1589958507	0	0	6	2018-02-0...	0	2018-02-0...	http://ww...	best of he man - Google Search					
1620911897	0	0	6	2018-02-0...	0	2018-02-0...	https://m...	YouTube					

Figure 2. Logical files from an IoT device partition that was sucessfully identified and supported. (Image Credit: SWGDE)

- For filesystems not supported by a specific tool, viewing the acquired data in a hexadecimal viewer and performing string searches can assist in the carving of artifacts that may be useful to an examiner.
- In the below example screenshot of data extracted from an IoT light bulb, on the right-hand side, one can read the word “timestamp” followed by what appears to be numbers that may correspond to a known timestamp format (Figure 3).

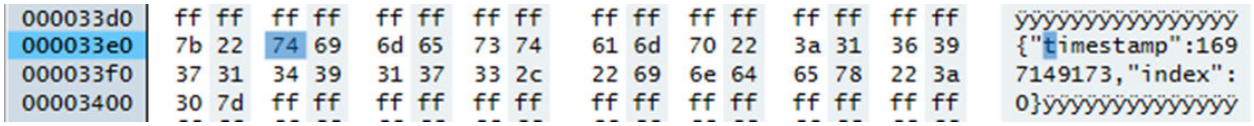


Figure 3. Timestamp followed by numbers corresponding to the known timestamp format. (Image Credit: SWGDE)

- From there, one can copy the numbers representing the timestamp into a date/time software decoding tool such as the one displayed below (Figure 4):

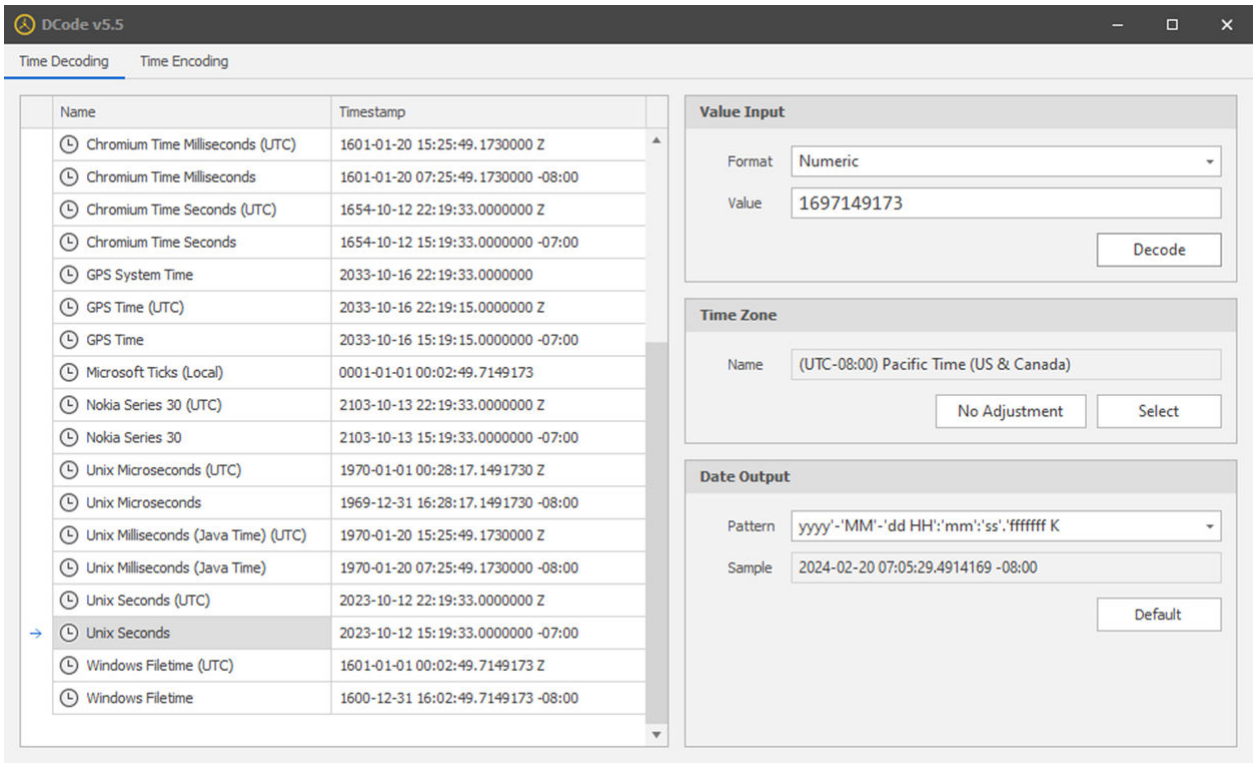


Figure 4. Date/time software decoding tool. (Image Credit: SWGDE)

Absent further testing, e.g. creating an exemplar dataset with known seeding information, the difficulty in this type of analysis is determining the relevance of this potential user artifact.

14.2 Post Extraction/Acquisition Data Analysis of Manufacturer Companion Applications/Programs

Just as with the acquisition/extraction, evidentiary data can be examined using traditional forensic methods and tools.

14.3 Post Extraction/Acquisition Data Analysis of Cloud Storage

Data retrieved from cloud storage locations can typically be either manually reviewed (as a report product) or examined/analyzed using traditional forensic methods and tools.

15. Additional Resources

- *Artifact Genome Project.* https://agp.newhaven.edu/login/?next=/. Accessed 13 Nov. 2024.
- Casey, Eoghan, et al. "Crowdsourcing Forensics: Creating a Curated Catalog of Digital Forensic Artifacts." *Journal of Forensic Sciences*, vol. 67, 2022, pp. 1846-1857. *Wiley Online Library*,. https://doi.org/10.1111/1556-4029.15053.
- Greer, Christopher, et al. *Cyber-Physical Systems and Internet of Things*. National Institute of Standards and Technology Special Publication 1900-202 Revision 1. National Institute of Standards and Technology, March 2019, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf.
- *If This Then That*, https://ifttt.com. Accessed 13 Nov. 2024.
- Scientific Working Group on Digital Evidence. *Core Competencies for Embedded Device Forensics.* SWGDE 19-F-001-1.0. *SWDGE*, 17 Sept. 2020*, https://www.swgde.org/19-f-001/*.
- Scientific Working Group on Digital Evidence. *Technical Notes on Internet of Things Devices.* SWGDE 20-F-004-1.0. *SWGDE,* 17 Sept. 2020*, https://www.swgde.org/20-f-004/*.
- Scientific Working Group on Digital Evidence. *Best Practices for Digital Evidence Collection*. SWGDE 18-F-002-1.0. *SWGDE*, 11 July 2018, https://www.swgde.org/18-f-002/.
- Scientific Working Group on Digital Evidence. *Best Practices for Chip-Off.* SWGDE 15-F-002-1.0. *SWGDE*, 8 Feb. 2016*, https://www.swgde.org/15-f-002/.*
- Scientific Working Group on Digital Evidence. *Tech Notes Regarding Chip-off via Material Removal Using a Lap and Polish Process.* SWGDE 16-F-004-1.0. *SWGDE,* 21 Feb. 2017*, https://www.swgde.org/16-f-004/.*

- Scientific Working Group on Digital Evidence. *Best Practices for Examining Mobile Phones Using JTAG.* SWGDE 15-F-001-1.0. *SWGDE*, 29 Sept. 2015, *https://www.swgde.org/15-f-001/*.
- Scientific Working Group on Digital Evidence. *Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition.* SWGDE 18-F-03-1.2. *SWGDE,* 17 Sept. 2020, *https://www.swgde.org/18-f-003/*.
- Scientific Working Group on Digital Evidence. *Best Practices for Digital Evidence Acquisition from Cloud Service Providers.* SWGDE 19-F-002-1.0. *SWGDE,*17 Sept. 2020, *https://www.swgde.org/19-f-002/*.
- Scientific Working Group on Digital Evidence. *Best Practices for On-Scene Identification, Seizure, and Preservation of Internet of Things (IoT) Devices.* SWGDE 22-F-001-1.0. *SWGDE,* 22 Sept. 2022, *https://www.swgde.org/22-f-001/*.
- Scientific Working Group on Digital Evidence. *Best Practices for the Acquisition of Data from Novel Digital Devices.* SWGDE 16-F-003-1.0. *SWGDE,* 21 Feb. 2017, https://www.swgde.org/16-f-003/.
- Scientific Working Group on Digital Evidence. *Best Practices for Vehicle Infotainment and Telematics Systems*. SWGDE 12-F-004-3.1. *SWGDE*, Dec. 2024.
- Scientific Working Group on Digital Evidence. *Best Practices for Digital & Multimedia Evidence Video Acquisition from Cloud Storage.* SWGDE 17-V-003-1.0 *SWGDE, 25 Apr. 2018, https://www.swgde.org/17-v-003/*.

16. History

Revision	Issue Date	History
1.0 DRAFT	1/13/2023	The contents from what are now the final drafts of the documents titled "2023-03-31 SWGDE Best Practices for On-Site Identification, Seizure, and Preservation of IoT Devices (22-F-001-2.0)" and "2023-03-31 SWGDE Best Practices for Internet of Things (IoT) Acquisition and Analysis (23-F-001-1.0)" were merged into a new initial draft and content expansion was initiated.
1.0 DRAFT	1/19/2023	Voted for release as a Draft for Public Comment.
1.0 DRAFT	5/14/2024	Public comments addressed. Minor grammar changes made. Added content to Section 10 to address concerns regarding seizure/acquisition of medical devices.
1.0	12/5/2024	SWGDE voted to approve as Final Approved Document. Formatted for release as a Final Approved Document.