Scientific Working Group on Digital Evidence

Best Practices for On-Scene Identification, Seizure, and Preservation of Internet of Things (IoT) Devices

22-F-001-1.0

Disclaimer and Conditions 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 suggested best practices, practical guidance, technical positions, and educational information 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.

As a condition to the use of this document (and the information contained herein) in any judicial, administrative, legislative, or other adjudicatory proceeding in the United States or elsewhere, the SWGDE requests notification by e-mail 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 sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, 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 and Conditions of 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 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

Unauthorized use of the SWGDE logo or documents 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 On-Scene Identification, Seizure, and Preservation of Internet of Things (IoT) Devices

Table of Contents

1. Purpose 2
2. Scope 2
3. Limitations 2
4. Definitions 3
5. Reference Data 3
6. Identification of IoT Devices 3
7. Collection 7
8. Preservation 9
9. Other Considerations 9
10. References 10

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), including identification and seizure, as well as preservation preparatory to analysis. The intended audience includes first responders and others who are interacting with IoT devices (particularly in an active environment such as on-scene where an incident has taken place that is now part of an investigation), investigators, attorneys who assist in the drafting of search warrants, and judges who grant search authority.

IoT devices frequently communicate through a local area network, such as a home router or proprietary hub with wired or wireless access, and sends or receives commands or information through the use of applications to/from cloud service providers. 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, Zwave). As an example of an IoT recovered artifact, the communication between these devices is often logged with date and time stamps. For example, a cellular phone being carried around a residence that is paired with IoT devices in that same location will 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.

2. Scope

While IoT devices are designed for consumer and industrial use, this document focuses on consumer devices including devices marketed for personal and residential use. Cloud, other collateral storage, and services will not be explored in this document, but rather just internal/onboard storage capabilities accessible through direct physical access of the devices.

The ideas, concepts, and technical aspects of these devices are strictly related to what is available at the time of this document. There may be added features or capabilities developed in the future that could alter the collection, preservation, and general handling addressed in this document. The limited distribution of tested tools in this space, available training, and other complications also affect the ability to fully understand the current forensic challenges of these devices.

3. Limitations

This document is not intended to be a training manual or a specific operating procedure. This document is not all-inclusive and does not contain information relative to specific commercial products. If dealing with technology outside your area of expertise, consult with an appropriate specialist. For recommendations on training core competencies for IoT forensics, please see *2020-09-17 SWGDE Core Competencies for Embedded Device Forensics_v1.0*.

4. Definitions

4.1 IoT

As defined in ***SWGDE Technical Notes on Internet of Things Devices_v1.0***, IoT is a system of interrelated computing devices, mechanical and digital machines or objects that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. These devices are not limited to a particular type of data storage medium or format.

4.2 Artifact

An artifact can be defined as a single piece of identifiable data/information. In forensics, artifacts of interest are those most likely to have probative value, and a complete artifact reference would include its location within the device/dataset and suggested method of extracting/parsing the data preparatory to analysis.

5. 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:

5.1 NIST Computer Forensic Reference DataSet Portal https://www.nist.gov/programs-projects/computer-forensic-reference-data-sets

5.2 The Artifact Genome Project, University of New Haven https://agp.newhaven.edu/about/start/

5.3 Sources with restricted access

5.3.1 Technical training organizations (e.g. NW3C, NCFI, FLETC)

5.3.2 Educational institutions (e.g. Marshall University, Champlain College, Leahy Center for Digital Forensics & Cybersecurity, Purdue University, Oklahoma State University)

6. Identification of 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 taken into account 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.

- Wearables – Wearable technology (also called wearable gadgets) is a category of technology devices that can be worn by a consumer. This can include but is not limited to,
    - Watches
    - Shoes
    - Fitness Trackers
    - Clothing
    - Medical Devices, e.g., CPAP, hearing aid, glucose/insulin pump
- Smart Tags - An electronic tag with an embedded Radio-Frequency Identification (RFID), Bluetooth Low Energy
  (BLE) or GPS device, attached to an object for the purposes of tracking or storing data relating to its use. Some examples of Smart Tags are
    - AirTag
    - UWB Cellular
    - NFC
    - LiFi
    - Tile
    - Chiplo
    - Pet tags
- Smart Speakers – A smart speaker (voice assistant speakers) is a type of wireless speaker and voice command device with an integrated virtual assistant that offers interactive actions and hands-free activation with the help of an activation phrase, or "wake word". The particular “wake word” may be changeable by the user. Some smart speakers can also act as a smart device that utilizes Wi-Fi, Bluetooth and other wireless protocol standards to extend usage beyond audio playback, such as to control home automation devices. This can include, but is not limited to, features such as compatibility across a number of services and platforms, peer-to-peer connection through mesh networking, virtual assistants, and others. Each can have its own designated interface and features, usually launched or controlled via application or home automation software.
- Smart Displays -Smart Displays are a smart speaker with an added screen to display content. They provide an integrated virtual assistant and hands-free activation with the help of an activation phrase, or "wake word.” They may serve as the central hub for user control of multiple IoT devices. For example, a user may link a smart electrical plug to their Google Home account to allow control from a centralized

device. Smart Displays may have the capability of voice and/or video calls from the device.

- Sensors – A sensor is a device that detects or measures a physical property and records, indicates, or otherwise responds to it. Some examples of sensor types are:
  - Motion
  - Lumen
  - Sound
  - Break/Separation Contact
  - Vibration
  - Position
  - Temperature
  - Humidity
  - Gas
- Control Systems – A control system bridges and manages, commands, directs, or regulates the behavior of other devices or systems. Examples of control systems are:
  - Actuators (e.g., door lock)
  - Thermostats
- Capture – Devices that capture information/data, may store for later exfiltration, and may broadcast data externally. Capture devices can include, but not limited to,
  - Cameras, including smart doorbells
  - Audio
  - 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 can include the following:
  - Cochlear
  - Pacemaker/Defibrillator
  - RFID Module
  - Near-Field Communication (NFC) Module
- Vehicles – A machine, device, or craft designed to travel and often contains a payload of some kind, whether it be a capture device (e.g. camera) or cargo. For information on vehicle systems, see *SWGDE Best Practices for Vehicle Infotainment and Telematics Systems*. Types of data sources on vehicles can include:
  - Infotainment
  - Telematics
  - Small Unmanned Aerial Systems (SUAS), aka. Drones
- Appliances – Machines/devices used to perform household functions, which can include, but not limited to,
  - Refrigerators

- Coffee makers
- Washer & Dryers
- TVs
- Smart Locks
- Robotic vacuums

Many IoT devices listen passively until an activation word is spoken. A sampling of these "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 Portal	Alexa	Alexa Hey Portal
Apple Home Pod	Siri	Hey Siri

These "wake words" are default settings. Users may personalize the functionality, e.g., individual voice recognition, or a different wake word.

IoT devices can be set up maliciously to create obstacles for law enforcement responding to scenes. Devices may record the first responders' actions, which may affect the identification and seizure of devices. Devices could act as triggers to delete data once they are aware of people on scene or to trigger kinetic events. As such, depending on the nature of the targeted collection site, a survey of device connectivity may want to be done sooner to ensure that data is not lost and personnel safety is maintained. Additional information regarding wake words and triggering events is offered below in the Collection section.

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, WiFi, Bluetooth, Zigbee and Z-Wave. There are 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.

7. Collection

When collecting any digital evidence it is best to first reference the *SWGDE 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, 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.).

While attempting to isolate the 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), verbalizing wake-words (saying you found an Alexa device, and "Alexa" is also the wake-word), making sounds above a detectable threshold, disconnecting the power and/or data connection, etc. This may cause an update/alteration of the data to be investigated, possibly alert the owner that a trigger event has occurred, and may cause the alteration and/or loss of volatile data of interest. 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 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 a Faraday bag/box or other network isolation method. If a battery is removed in order to isolate the device, do not place the battery in a Faraday enclosure with the IoT device as the shielded bag may actually create a connection and turn the Faraday enclosure into an antenna. In cases where IoT devices are hardwired into power supplies, and first responders lack either the knowledge or agency 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. Air Tags) that may be beaconing.

Collection procedures are dependent on several device characteristics due to the disparate manner in which 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 Ring 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 in close proximity to the device, or within a vendor's cloud storage.
- Connectivity - IoT devices use several communication protocols. In order 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

8. 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.

While power from IoT devices is 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 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.

IoT related potential artifacts may 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.

9. 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).

10. References

[March2019] Christopher Greer, Martin Burns, David Wollman, Edward Griffor, NIST Special Publication 1900-202 Revision 1 Cyber-Physical Systems and Internet of Things

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf

SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices
https://drive.google.com/file/d/1K0j5RiRY9UMcoDxOC58cTRiHpzJPTEIx/view

SWGDE Core Competencies for Embedded Device Forensics
https://drive.google.com/file/d/1UZL-kKq47odqa_uEmOEgBk9v3qcPC4ia/view

SWGDE Technical Notes on the Internet of Things (IoT) Devices
https://drive.google.com/file/d/1zcDxCLSrwTbwFlTAtjwB6UxMgMHOj3GY/view

Best Practices for Vehicle Infotainment and Telematics Systems
https://drive.google.com/open?id=1TdGbdmXqN9bc2VrMhch2coqB584RUdt7

History

Revision	Issue Date	History
1.0 DRAFT	6/7/2022	Initial draft created.
1.0 DRAFT	6/9/2022	Voted for release as a Draft for Public Comment.
1.0 DRAFT	9/22/2022	Corrections/edits made, voted for release as final publication.