UDIM: Formal User-Device Interaction Model for Approximating Artifact Coverage in IoT Forensics

Maximilian Eichhorn, Andreas Hammer, Gaston Pugliese, and Felix Freiling
Friedrich-Alexander-Universität Erlangen-Nürnberg
{maximilian.eichhorn, andreas.hammer, gaston.pugliese, felix.freiling}@fau.de

***Abstract*—Evidence from digital devices in general, and Internet of Things (IoT) and embedded devices in particular, plays an increasing role in modern investigations. Yet their diversity in hardware and software encumbers their analysis and analysis results appear fragmented and hard to assess. Investigators, therefore, face the challenge of finding and interpreting relevant digital evidence stored on these devices. In order to standardize the forensic analysis of digital devices and structure research results, we present the *User–Device Interaction Model* (UDIM), a device-centric formal model that is based on the types of interaction between a device, users, and other devices across interaction types and locations. By integrating the analysis results of 42 IoT devices from the literature, we show how UDIM supports standardized analysis, and helps law enforcement agencies prioritize resources during seizures. Furthermore, the model can be used to assess the coverage of forensic examinations, to ensure thoroughness and completeness of investigations.**

I. Introduction

As more and more smart objects populate our personal environment, an increasing amount of interesting digital evidence may be found on such devices. As a result, an ever increasing stream of device analyses are performed by digital forensic researchers, resulting in an abundance of scientific publications, white papers and blog posts. For forensic practitioners, this body of knowledge is a treasure chest, as it relieves them of laborious reverse engineering in their daily work.

When looking at previous work on the forensic analysis of various Internet-of-Things (IoT) and embedded devices, we observe that most examined devices differ substantially in terms of their recovered forensic artifacts. This is unsurprising given the breadth of form factors, use cases, and manufacturers. For example, a smart speaker [1] cannot be expected to contain exactly the same forensic artifacts as a washing machine [2] or a kitchen appliance [3], and a smart watch [4] will store different data than a smart light bulb [5] or a smart refrigerator [6]. The lack of a widely accepted analysis methodology for embedded devices further complicates comparisons of findings across researchers for the same device type. Without standardized approaches, it becomes difficult to determine the coverage level of such an examination, which makes it challenging to evaluate the thoroughness and comparability of research results.

This raises two practical questions: How can diverse and heterogeneous embedded device analyses be harmonized? And how can we make better use of insights from such analyses in digital investigations?

The structuring and comparison of artifacts from different IoT devices with respect to their *source* (e.g., device itself, companion device, cloud server) is still very rough and does not directly help investigators when they are seeking answers to concrete investigative questions. For example, seeking traces of *presence at the crime scene* would involve querying all three of the above sources. Similarly, the generic model of cognitive maps by Gruber et al. [7] offers too little structure to be able to compare concrete device analyses.

In this paper, we propose a new perspective on unifying generality with concreteness for IoT device analyses based on *interactions at system boundaries*, where we combine the location of traces with the implications of their existence. For example, traces of direct user interactions with devices at a crime scene indicate a person's presence. Therefore, focusing on interactions at system boundaries also helps to structure analysis results so that relevant traces can be found more easily and quickly. Systematically enumerating a device's interaction possibilities structures both research results and device analysis.

Conceptually, focusing on interactions means considering not only digital traces but also the activities that produce them. This corresponds to the observation made by Cook et al. [8] that forensic propositions appear at three abstraction levels: *Offense* level (legal questions about whether an offense occurred and who is responsible), *Source* level (concrete traces like fingerprints or timestamps), and *Activity* level (concrete activity descriptions). Interactions in our model correspond to Activity-level statements, which explain their usefulness in linking the *Offense* and *Source* levels.

A. Research Questions & Contributions

We aim to answer the following research questions:

RQ1 How can the communication of a digital device with other devices and users be described completely and formally in a model-based manner?

RQ2 Can the model help standardize forensic investigations of digital devices, and does it impact the work of law enforcement agencies?

Network and Distributed System Security (NDSS) Symposium 2026
23–27 February 2026, San Diego, CA, USA
ISBN 979-8-9919276-8-0
https://dx.doi.org/10.14722/sdiotsec.2026.23050
www.ndss-symposium.org

Overall, the contributions of this paper in answering the research questions are as follows:

- We present the *User-Device Interaction Model* (UDIM), a model of user-device communication and interaction, which can be used to describe a device's interactions with its interaction participants in different locations and classify them according to their possible existence and found forensic artifacts.
- We show how the model can support a standardized and comprehensive forensic examination of an IoT or embedded device and thereby also the work of law enforcement agencies with respect to the seizure of relevant devices.
- We created an example knowledge base by applying UDIM on 24 data sources about the possible interactions of 42 different devices with their interaction participants.

II. Related Work

As mentioned above, many publications reporting on concrete insights from actual technical analyses of specific devices exist, some very detailed, others very pragmatic with varying depth. In contrast, only few previous works have focused on the harmonization and classification of these insights.

Most artifact classification methodologies draw from approaches originally devised for physical evidence [9], [10]. For example, Cook et al. [11] proposed a model that is related to expert witness work. The authors divided this process into three phases: *customer requirement*, *case pre-assessment* and *service delivery*. The forensic examination occurs in the third phase, where final statements are formulated based on prepared investigation questions and a predefined strategy.

Bouchaud et al. [12] used this approach to abstract from concrete analyses of specific IoT devices and rather focus on the types of evidence that can be recovered from them. For example, they classified evidence as either coming from internal or external networks. These insights were reinforced by findings of Li et al. [1] and Servida et al. [5], who suggested that a forensic analysis should examine not only the actual IoT devices but also the companion apps and networks. Furthermore, Li et al. [1] classified IoT devices as *tools*, *targets*, or *witnesses* in the context of a criminal case.

Recently, attempts have been made to harmonize insights from specific IoT sub-areas. For example, Hammer et al. [13] presented a taxonomy for fitness trackers, smart watches, and other wearables and a model for the forensic investigation of fitness trackers. However, whether their model generalizes to all embedded devices remains unclear. In contrast, Gruber et al. [7] proposed *cognitive maps* based on a node-link representation to capture phenomenon-specific knowledge in cybercrime investigations. These maps guide the search for *relevant digital evidence* and thereby allow to "map" general process models to specific cases. Due to its simplicity, the approach is very expressive, but the creation of useful cognitive maps requires a lot of effort. Gruber and Freiling [14] also addressed the question of finding relevant digital evidence based on case-specific hypotheses, but within digital models that need to be created (i.e., mined) first.

In addition to such cognitive maps, network-based maps can also be used by investigators for forensic analysis and describing IoT environments. Tournier et al. [15] described a graph-based model for IoT networks and addressed protocols such as ZigBee, Bluetooth, Wi-Fi, and others. In their modeling approach, they distinguish between different graphical representations of the same IoT network based on network layers (data link, network, transport, and application). Similarly, Wang et al. [16] employed graph-based representations with their ProvThings approach, creating provenance graphs from the Samsung SmartThings platform to explain system activities and trace malicious behavior during attacks by utilizing companion apps and device APIs. Beyond provenance-based approaches to behavior monitoring, spatial categorization can also assist forensic analysis in IoT environments. Almogbil et al. [17] classified attacks on smarthome environments based on the locality of the attack. They distinguish between *physical*, *nearby*, and *remote* devices and thereby adopt forensic analysis approaches that examine the device, its firmware, companion devices on the local network, and remote cloud servers for forensic artifacts.

Regarding concrete analysis procedures, Eichhorn and Freiling [3] performed a rigorous analysis of a kitchen appliance based on systematic test data generation on an identical reference device to analyse an unknown IoT device. The authors defined minimal actions as state transitions in a state machine [18]–[20] and then compared successive states using differential forensic analysis [21] to identify forensically relevant artifacts. While their analysis method is rather general, Eichhorn and Freiling [3] do not address the question of how to compare the types of artifacts resulting from their method.

III. User-Device Interaction Model

The *User-Device Interaction Model* (UDIM) formalizes the ways in which IoT devices can interact with users, their environment and other technical infrastructures (other devices or cloud services). The model is device-centric, i.e., the outset of any deliberation is some specific IoT device itself that is relevant to a criminal investigation.

A general overview of the model is depicted in Figure 1, which shows the device in the center targets of possible interactions around it ordered by "interaction distance", i.e., direct proximity, internal networks and external networks. The following sections describe UDIM in more detail: We first give some basic definitions (Section III-A) before showcasing its real-world usage based on an exemplary device (Section III-B).

A. Model Definition and Description

UDIM is an idealized representational model [22] intended to support forensic analysts as a visualization aid and structural guide, focusing on the interactions between a device and its user. At the center of the model is a concrete device.

Definition 1 (UDIM device)**.** A *UDIM device* (or simply *device*) is a computing system that has digital storage to store (a) usage data and (b) the firmware or operating system necessary for providing functionality.

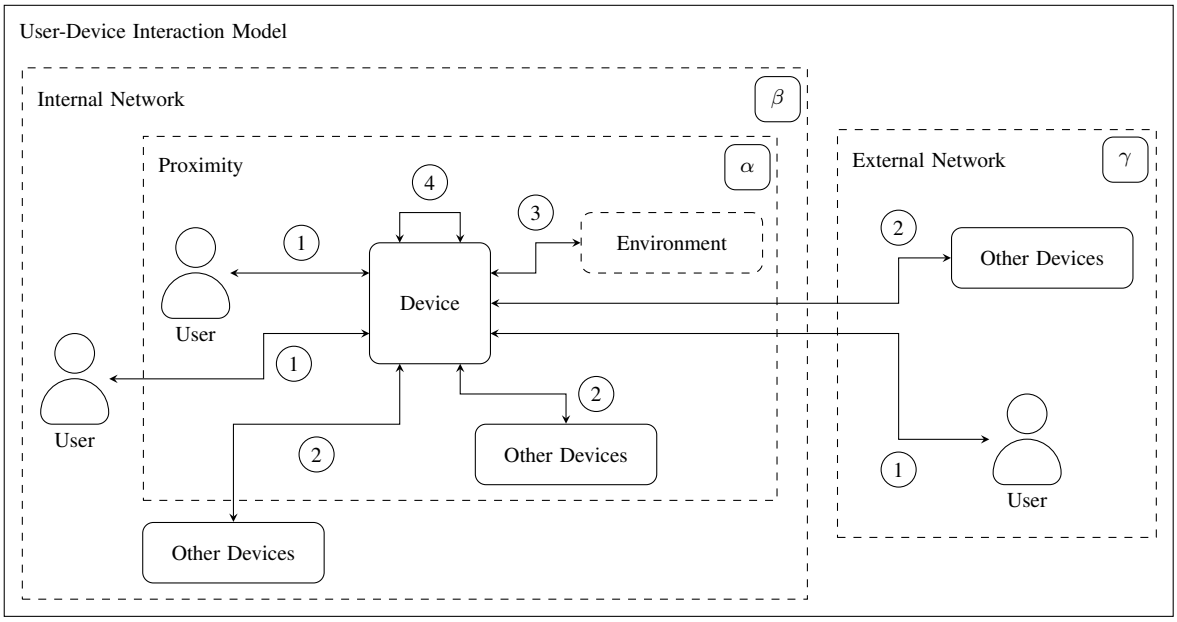

Fig. 1: *User-Device Interaction Model* with three sections: Proximity (α), Internal Network (β), External Network (γ). Numbers indicate the respective interaction pairs: User-Device (1), Device-Device (2), Device-Environment (3), Device-Internal (4).

The definition is slightly restrictive in that it focuses on devices that potentially store relevant digital evidence. Electronic devices that cannot persistently store usage data, such as an IR remote control, are uninteresting from a digital forensics point of view and therefore excluded from the definition, as their analysis cannot provide any traces of usage or interaction.

UDIM itself, i.e., the potential interactions of a specific device, is formalized as a directed graph structure $G = (V, E)$ where vertices (or nodes) V are entities between which interactions can take place and directed edges are representations of potential interactions. As UDIM is constructed around a specific device d, we demand that at least $d \in V$. And since we assume that devices have some internal interactions, we demand that $(d, d) \in E$. The set of graph nodes V also contains possible users, devices, and environments of the device as elements.

Definition 2 (environment of a device)**.** The *environment* of a device d refers to the spatial surroundings of a device with which it can interact via acoustic, visual, or other sensor-measurable means and may include other devices or users.

Note that the environment is device-specific and not necessarily identical for two devices. It is also possible that two devices have an intersection of each other's environments. If the environments overlap, the devices can interact indirectly via the environment. For example, if one device's microphone picks up the speaker output from another device, this would be an example of indirect interaction.

As shown in Figure 1, UDIM is structured according to the spatial location of devices and users in relation to the central device. We distinguish between three types of locations that differ in spatial/technical distance, i.e., UDIM is based not only on physical distance but also on the necessary technical protocols for communication. Distinguishing these location types is necessary because communication and forensic artifacts may vary depending on them. The three location types are (1) direct proximity, (2) the internal network, and (3) the external network.

The location types are formalized as subgraphs of a UDIM graph. Formally, a subgraph $G' = (V', E')$ of a graph $G = (V, E)$ is a graph such that $V' \subseteq V$ and $E' \subseteq E$ such that E' only contains those edges from E that refer to nodes in V'.

We now are ready to define how UDIM is formed around a specific device and its environment.

Definition 3 (UDIM)**.** The *UDIM for device d and environment e* is a graph $G = (V, E)$ such that $d \in V$ and $e \in V$, $(d, d) \in E$. G consists of three subgraphs G_α, G_β and G_γ of G defined as follows:

- The *proximity subgraph* G_α comprises all graph nodes v that are in the same environment e of d, including d.
- The *internal network subgraph* G_β includes all graph nodes v located in the same network as the device d, including d.
- The *external network subgraph* G_γ includes all graph nodes v located in another network as the device.

When modeling a real device within UDIM, we understand the definition of the internal network as not distinguishing between the protocols used to implement this network. The network can be implemented using any wired or wireless communication technology (e.g., Ethernet, Wi-Fi, Bluetooth) or a combination thereof. Also note that the device is a node in G_α and G_β but not in G_γ.

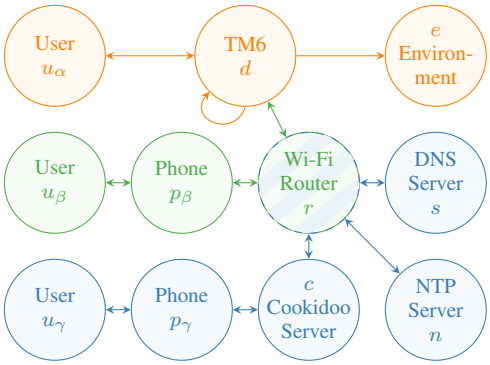

Fig. 2: Complete Graph G_{TM6} for the Thermomix TM6 device. The subgraphs proximity G_α (■), internal network G_β (■ & ■), and external network G_γ (■) are given as follows: $G_\alpha = (\{e, d, u_\alpha\}, \{(d, e), (d, d), \{d, u_\alpha\}\})$, $G_\beta = (V_\alpha \cup \{r, u_\beta, p_\beta\}, E_\alpha \cup \{\{d, r\}, \{u_\beta, p_\beta\}, \{r, p_\beta\}\})$, and $G_\gamma = (\{r, u_\gamma, p_\gamma, c, n, s\}, \{\{u_\gamma, p_\gamma\}, \{p_\gamma, c\}, \{r, c\}, \{r, n\}, \{r, s\}\})$.

B. Example of Model Usage: Thermomix TM6

To illustrate the use of UDIM, we apply the model to an existing analysis [3] of a specific IoT device: the Vorwerk Thermomix TM6 [23] is a smart kitchen appliance advertised as a multi-cooker with cloud and companion app features, which generated revenues of €1.7 billion in 2024 [24].

The TM6 has a touchscreen and a rotary knob as input devices for immediate physical user-device interaction. The rotary knob provides the user with haptic feedback, and the screen provides visual feedback on the interaction. The hardware is also equipped with a loudspeaker that allows the TM6 to interact with the environment. However, this interaction is not bidirectional, as the TM6 has no sensors to extract environmental information outside the attached mixing pot. These observations determine the proximity subgraph G_α.

To precisely define $G_\alpha = (V_\alpha, E_\alpha)$, the set of nodes V_α therefore consists of the TM6 itself as device node d and its environment e together with the user u_α in the device's proximity. The interactions are depicted in Figure 2 which shows the visual representation of the overall graph G with its subgraphs. The proximity subgraph is shown at the top (in orange) and formally is represented as:

$$G_\alpha = (\{e, d, u_\alpha\}, \{(d, e), (d, d), \{u_\alpha, d\}\}).$$

Note that we use the edge notation $\{x, y\}$ to represent the bidirectional edge between nodes x and y otherwise represented as two edges (x, y) and (y, x).

We now look at the internal network subgraph of the UDIM for the TM6. The set of nodes consists of all nodes of the proximity subgraph, i.e., the device itself, the user u_α, and the environment. Additionally, we add the phone p_β running the companion app and the user u_β of this phone (which may be different from the user u_α directly interacting with d). Since the phone interacts via the network router r, the resulting internal network subgraph is as follows:

$$G_\beta = (V_\alpha \cup \{r, u_\beta, p_\beta\}, E_\alpha \cup \{\{d, r\}, \{u_\beta, p_\beta\}, \{r, p_\beta\}\}).$$

The internal network graph is the union of orange and green elements shown in Figure 2.

Finally turning to the external network graph, we must examine the connectivity of the TM6 outside the internal network. In [3], three notable servers were identified as interaction participants in the external network: (1) the Vorwerk Group's Cookidoo recipe platform server c, (2) an NTP server n, and (3) a DNS server s. Since the Wi-Fi router r is accessible from both networks (internal and external), it plays a special role and must be added to both subgraphs. Also, in line with the TM6's range of functions, we need to add a phone p_γ with the companion app and again the user u_γ interacting via the external network with d. Hence, the external network subgraph $G_\gamma = (V_\gamma, E_\gamma)$ is formulated as:

$$\begin{aligned} V_\gamma =& \{r, u_\gamma, p_\gamma, c, n, s\} \text{ and} \\ E_\gamma =& \{\{u_\gamma, p_\gamma\}, \{p_\gamma, c\}, \{r, c\}, \{r, n\}, \{r, s\}\}. \end{aligned}$$

The complete UDIM graph for the TM6 is shown in Figure 2 as the combination of subgraphs G_α, G_β and G_γ In formal notation, the graph $G_{\text{TM6}} = (V, E)$ is expressed as:

$$\begin{aligned} V =& \{e, d, u_\alpha, r, u_\beta, p_\beta, u_\gamma, p_\gamma, c, n, s\} \text{ and} \\ E =& \{(d, e), (d, d), \{d, u_\alpha\}, \{d, r\}, \{u_\beta, p_\beta\}, \{r, p_\beta\}, \\ & \{u_\gamma, p_\gamma\}, \{p_\gamma, c\}, \{r, c\}, \{r, n\}, \{r, s\}\}. \end{aligned}$$

C. Classes of Interactions

Given the UDIM of a specific device, we now identify different types of interaction to identify devices involved in the respective interaction as possible sources of forensic artifacts of this interaction. We do this by using the standard concept of a *path* from graph theory. Given a graph $G = (V, E)$, a *path* within G is an ordered non-empty sequence of nodes $\langle x_0, x_1, x_2, \ldots, x_n \rangle$ from V such that for all i, $0 \leq i < n$ holds that $(x_i, x_{i+1}) \in E$. The first node x_0 of the path is called the *start node* and the last node x_n is called the *end node* of the path. For a path P, we denote by $|P|$ the *length* of the path, i.e., the number of edges contained in P. The number of edges contained in P corresponds to the number of nodes listed in the node sequence minus 1. Note that the length of a path can also be 0.

We use the concept of a path to define what we call an interaction.

Definition 4 (interaction)**.** A path $P = \langle x_0, x_1, x_2, \ldots, x_n \rangle$ of the graph G with $|P| > 0$ that contains the device d as its starting or ending node is called an *interaction*. The nodes contained in the interaction are called *interaction participants*.

We now define different types of interactions. We start with internal interactions within d. These model interactions between applications or services within the device.

Definition 5 (internal interaction)**.** The interaction $P = \langle d, d \rangle$ of the graph G is called *device-internal interaction*.

For example, when a web server on the device sends an email to the local mail server, this is a device-internal interaction. Figure 3 gives an abstract overview over different

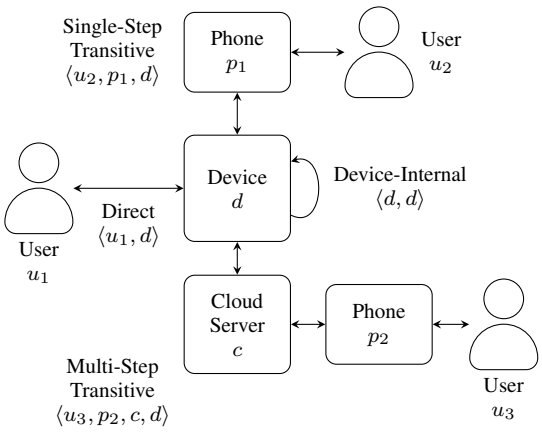

Fig. 3: Example of different interaction types and paths.

types of interactions and shows a device-internal interaction $P_d = \langle d, d\rangle$ with $|P_d| = 1$ schematically.

Other types of interaction depend on the length of the path.

Definition 6 (interaction types)**.** Let P be an interaction of a UDIM graph G. Depending on the length $|P|$ of the interaction, we define the following interaction types:

(A) if $|P| = 1$, then P is a *direct* interaction,
(B) if $|P| = 2$, then P is a *single-step transitive* interaction,
(C) if $|P| > 2$, then P is a *multi-step transitive* interaction.

The different types of interactions are illustrated in Figure 3. A direct interaction is the interaction $P_A = \langle u_1, d\rangle$ between a user u_1 and the device d. For this special case, we also use the term "direct user-device interaction". Direct user-device interaction is the most basic form of interaction and can be performed by the user, for example, via the device's keyboard or touchscreen. However, since it is not always possible to interact directly with a device, it may be necessary to perform the interaction via at least one other device and thus transitively. Figure 3 shows a typical single-step user-device interaction $P_B = \langle u_2, p_1, d\rangle$ between the user u_2 and device d via a smartphone p_1 and the device's companion app on it.

The distinction between single-step and multi-step transitive interactions is relevant because these may exhibit different forensic artifacts, and the interaction itself may leave artifacts on multiple devices. A typical multi-step user-device interaction occurs when the user operates the device via the companion app, but all device traffic is routed through the vendor's cloud server. Hence, two devices are interposed in the interaction between the user and the actual device. Figure 3 schematically illustrates such a multi-step transitive interaction $P_C = \langle u_3, p_2, c, d\rangle$ using the example of user-device interaction via the device's companion app on the phone p_2, which is routed to the device d via the vendor cloud c.

D. Example of Model Usage (Continued)

Revisiting the TM6 UDIM graph from Figure 2, in practice, not all nodes are always relevant for forensic examination in terms of their forensic artifacts. Thus, it may be legitimate to simplify the graph under certain circumstances. For instance, as the TM6 does not establish any other connections in the local network except for the connection to the Wi-Fi router, when considering the device's interactions, and since the router only forwards the connections, it is possible to consider whether we should include the Wi-Fi router, or whether it is negligible for the specific case. Also, the TM6 does not allow single-step or multi-step transitive user-device interaction via the companion app. It only offers functions such as editing recipes or weekly plans on the Cookidoo server and does not allow device control. So overall, the users u_β and u_γ from the internal and external network as well as the phones p_β and p_γ with the companion app in these locations, should be omitted.

Given the final UDIM graph of the TM6, we can now identify the relevant interactions and the respective interaction participants. If we want to conduct a forensic examination of the TM6 device, it is much easier to identify relevant interactions and search for their forensic artifacts. The graph also indicates whether an investigation concerning all possible interactions was complete. Accordingly, the possible direct user-device interaction can, for example, be used to investigate the presence of a person to verify an alibi with the TM6. Furthermore, it allows us to specify which devices were involved as interaction participants for each interaction and where forensically relevant artifacts of these may occur.

IV. Evaluation

To evaluate the applicability of UDIM, we apply the model to devices that have been examined in previous papers and those that have not yet been examined. The evaluation of the model refers to its applicability to prior research and general IoT devices. Table I shows the results of the model application for the respective devices and their companion apps.

A. Table Structure

In Table I, we first divide the entries for each device into the four pairs of interaction participants and then differentiate further between the user-device and device-device pairs based on their location. Since UDIM is device-centric, the location refers to the other interaction participant, such as the user or the other device. The user can be located in any of the three subgraphs in the user-device pair, but not every interaction type is possible for every subgraph. For example, direct interaction between the user and the device is impossible outside the device's proximity. We also consider the location of the other device for the device-device pair in the various subgraphs. Though, a further distinction between the proximity and internal network subgraphs is rarely necessary because device-device interaction usually occurs via a network and its respective protocol. However, if there is physical interaction between the devices, it is necessary to distinguish between their locations. Since there was no physical interaction for any of the devices, we have not made a distinction in the table.

For each column provided, an entry is made for a device or a combination of device and companion app. We first indicate

	Device(s) (Number of distinct device models) [+ App]	User-Device G'_α A	G'_α B	G'_α C	G'_β B	G'_β C	G'_γ C	Device-Device $G'_\alpha \vee G'_\beta$	Device-Device G'_γ	Device-Env.	Device-Internal
Academic Papers on IoT and Embedded Device Forensics	[3]										
	Vorwerk Thermomix TM6 (1)	●	–	–	–	–	–	–	●	○	●
	[25]										
	Shelly Relays (5) + Shelly App	◐	●	●*	●	●*	●*	◐	●	–	–
	LoraTap (2), eMylo (1), Maxcio (1), SIUES (1) Relays + Tuya App	◐	–	●	–	●	●	–	●	–	–
	MoesGo Relay (1) + Tuya App	◐	–	●	–	●	●	–	●	◐*	–
	Meross Relays (2) + Meross App	◐	◐	●	◐	●	●	◐	●	–	–
	Sonoff Relays (2) + eWeLink App	●	●	●	●	●	●	◐	●	–	–
	Newgoal Relay (1) + eWeLink App	◐	●	●	●	●	●	◐	●	–	–
	[26]										
	Amazon Echo Show 15 (1) + Alexa App & Photos App	●	●	●	●	●	●	●	–	●	●
	[27]										
	Bosch Nyon (2014 & 2021) (2) + eBike Connect App	●	∣	●	∣	●	●	○	●	–	○
	[28]										
	Valve Steam Deck (1)	●	–	○*	–	○*	○*	○	●	○	●
	[5]										
	Meross Thermostat (1)	∣	○	●	○	●	●	○	●	◐	∣
	Google Home Mini (1)	○	∣	●	∣	●	●	○	●	●	○
	Google Nest Protect v2 Smoke Detector (1)	○	∣	●	∣	●	●	○	●	●	○
	Xiaomi Sensors (Motion & Environment) (2)	–	∣	●	∣	●	●	○	●	●	∣
	QBee Camera (1)	○	∣	●	∣	●	●	∣	●	●	∣
	IKEA Light Bulbs (2)	–	∣	●	∣	●	●	○	●	–	∣
	IKEA Motion Sensor (1)	–	∣	●	∣	●	●	○	●	◐	∣
	myStrom Wi-Fi Switches (1)	∣	∣	●	∣	●	●	∣	●	●	∣
	Netatmo Environment Sensors (1)	∣	∣	●	∣	●	●	∣	●	●	∣
	[1]										
	Amazon Echo (1) + Alexa App	●	●	●	●	●	●	○	–	○	○
Blog Articles	[29]–[31]										
	Apple HomePod (1)	●	∣	●	∣	●	●	○	●	●	∣
	[6]										
	Samsung Refrigerator RF22M9581SG (1)	●	∣	●	∣	●	●	●	●	●	●
	[32]–[34]										
	Apple TV (4 & 4k) (1)	○	∣	●	∣	●	●	●	●	○	∣
	Apple Watch (1)	○	●	●	●	●	●	○	●	●	–
Data Sheets	[4], [35]										
	Apple Watch Series 6 (1) + Watch App	○	○	○	○	○	○	○	○	○	–
	[2], [36], [37]										
	Bosch Washing Machine WGH254A0GB (1) + Home Connect App	○	○	○	○	○	○	○	○	–	–
	[38]										
	Melitta Barista TS Smart (1) + Melitta Connect App	○	○	–	○	–	–	–	–	–	–
	[39]–[41]										
	Milwaukee Percussion Drill M18 ONEPD3-0X (1) + One-Key App	○	○	–	○	–	–	○	–	–	–
	[42]										
	Garmin Fenix 6 (1) + Garmin Connect App	○	○	○	○	○	○	○	○	○	–

Interaction state: ○ possible, ◐ examined, ● artifacts detected, – not possible, ∣ unclear whether possible * *only possible after changing the default settings*

TABLE I: Applying the model to selected publications analyzing IoT devices reveals where the various devices have been adequately investigated and where shortcomings can be identified. When depicting interactions, we address the location of the other interaction participant in the three subgraphs: proximity (G'_α), internal network (G'_β), and external network (G'_γ). Furthermore, where necessary, a distinction is made with regard to the path length of the interaction. We distinguish between direct (A), single-step transitive (B), and multi-step transitive (C) interactions.

whether interaction with the given interaction participants is *possible* (○) or *not possible* (–) in the given subgraph G'_i. However, since it is not always clear from the given source whether a specific interaction is possible, we label this as *unclear whether possible* (∣). In addition to a certain degree of uncertainty, an interaction may be impossible under the given conditions in the default settings and can only be enabled by changing the settings. Besides assessing whether a specific interaction with given interaction participants is possible in the given location, we consider whether the authors have *examined* (◐) a *possible* interaction. Interactions that are not possible or unclear whether they are possible cannot be investigated. If the authors have analyzed an interaction, we assess whether the authors have *detected* (●) forensic artifacts of the interaction. The authors may find such artifacts of an interaction on the device itself or the other interaction participants.

B. Data Sources

Since the possible interactions of a device can change due to software updates or new hardware revisions, we indicate for each row in Table I from which reference we have derived

the values for individual cells. We divide the table entries horizontally into three categories: academic papers, blog articles, and data sheets. The table entries in the first category refer to peer-reviewed papers and the devices examined therein. In the second category, we consider devices whose values we have filled into the table based on information from technical blog posts or other non-peer-reviewed sources. Finally, the entries in the third category are based on data sheets or other information published by device manufacturers. Below, we discuss the applicability of UDIM for devices in these three categories and examine individual entries of Table I.

a) Academic Papers: Academic papers are the most common sources for forensic investigations of IoT or embedded devices. While they undergo peer review, artifact evaluation is not necessarily formal in the digital forensics community[1], which creates some uncertainty about forensic artifacts. Still, most academic papers are well documented and specify app or firmware versions, providing analysts with necessary reference values. Without standardization in forensic analyses, however, authors may not examine all interactions.

To begin with, we take another look at the graph of the Thermomix TM6 (Figure 2) and can already identify the possible interactions from it. Possible interactions include direct user-device interactions, device-device interactions in the external network subgraph G'_γ, device-environment interactions, and device-internal interactions. [3] analyzed the TM6, and we can use their information to determine whether they examined the possible interactions and found forensic artifacts. According to the authors, the user-device interactions via the rotary knob were documented in various log files, which means that forensic artifacts are available. Furthermore, the authors stated that the `systemd-journald` service logged the device-device and device-internal interactions. The authors only mentioned the loudspeaker and a temperature sensor (inside the mixing pot) in the device description, providing no further information about device-environment interactions via the loudspeaker. We therefore assume they did not investigate this interaction.

Some papers describe multiple devices that can be added to the knowledge base using UDIM. For example, [5] describe various IoT devices (smoke detectors, temperature sensors, motion detectors) and their forensic artifacts within a practical forensic scenario. We could, however, not determine whether specific interactions were possible for all devices based on the paper alone. In these cases, we noted the possibility of interaction as unclear. Such unclear interaction possibilities exhibit that UDIM can identify missing information and gaps in investigations w.r.t. interactions and interaction participants.

[25] faced the challenge with multiple devices, but only in one device class (smart relays). Classifying the examined devices using UDIM reveals that some investigated interactions yielded no forensic artifacts. For smart relays, direct user-device interaction appears to leave no artifacts in most cases. For example, the authors found no firmware artifacts of physical button presses on a Shelly relay, as this interaction is not logged. They also note that while multi-step transitive user-device interaction via the vendor cloud server is possible, this option is disabled by default. To consider this special feature, we marked such cases with an asterisk in Table I.

b) Blog Articles: Unlike academic papers on IoT and embedded device forensics, blog articles pose other challenges as a basis for applying UDIM. Despite detailed artifact descriptions, blog articles often lack key device information (e.g., hardware version, model number), which hinders transfer to practical forensic analyses. They typically lack formal peer review and sufficient methodological description. However, they cover specialized devices often absent from academic literature, which makes them valuable information sources.

There are, nonetheless, well-written blog articles which contain all necessary information for applying our model. One such example is the forensic analysis of the Apple HomePod by [29]–[31], who described all steps of the investigation, from data acquisition to data analysis, in detail. The Apple HomePod has a microphone and a speaker, which enables it to sense its environment. The author found forensic artifacts in the data, such as which song was played at what time and thus output via the loudspeaker. Furthermore, direct user inputs such as pausing playback via the touchscreen are logged. Traces of multi-step transitive user-device interactions, such as adding podcasts via an iPhone and iCloud, can also be found in the logs. The location of the iPhone relative to the device seems irrelevant, as the data is synchronized via iCloud. Since the Apple HomePod also synchronizes itself with iCloud without user interaction, and the author specified artifacts for this, device-device interaction can also be found in the external network subgraph G'_γ in the data. The Bluetooth logs also contain references to paired devices; thus, such interaction is possible, but the author did not specify any further artifacts regarding device-device interaction outside the subgraph G'_γ. It also remains unclear whether device-internal interactions and single-step transitive interactions are possible.

c) Data Sheets: Unlike academic papers or blog articles, data sheets provide no forensic artifacts but only device descriptions, functions, and specifications. However, they are authentic sources (when obtained directly from manufacturers, excluding advertising claims) and typically provide more comprehensive information about possible interactions with fewer ambiguities. Though data sheets vary vastly in scope, structure, and layout, which makes them challenging to dissect, we can still extract interaction information and apply the model to corresponding devices.

The Milwaukee M18 ONEPD3-0X cordless screwdriver exemplifies a niche smart device that has not yet been forensically examined in academic literature or blogs. Still, manufacturer data sheets [39]–[41] provide interaction information for UDIM. The device communicates via Bluetooth with the One-Key companion app to transmit operating data. Direct user-device interaction occurs when used as a tool. Single-step user-device interaction via Bluetooth is possible, but it is unclear whether bidirectional communication (i.e., sending input to the device) is supported. Multi-step transitive interac-

[1]Exceptions include, e.g., the publication venue *DFIR Review*.

tion is impossible due to the Bluetooth-only connection. The firmware only sends operating data, precluding device-internal interaction. The device lacks sensors for device-environment interaction. Finally, device-device interaction occurs via the cyclical transmission of operating data to the companion app.

C. Practical Applicability

In addition to its applicability to results from various data sources, the UDIM-created Table I offers practical usability for law enforcement. Below, we show the practical applicability of the table's information for individual example scenarios.

First, we consider a classic alibi scenario where a person is suspected of murder. Law enforcement must determine whether the suspect was present at the crime scene at the time of the crime. Using UDIM, they can focus on direct user-device interactions to verify presence. In this example, the suspect claims to have been cooking at home. Law enforcement can examine kitchen devices using UDIM to investigate direct user-device interactions. The Thermomix TM6 entry in Table I shows that such interaction is possible and yields forensic artifacts. Hence, the alibi could be verified or disputed based on the forensic analysis of the TM6.

Beyond alibi scenarios, IoT devices can be directly linked to crimes in some cases: Suppose someone manipulated a smart relay to trigger a short circuit and cause a fire. Though the attempt failed, law enforcement must determine who activated the relay and their location. For the Shelly device with default settings, Table I indicates that only direct, single-step transitive user-device interaction is possible. Hence, the operator must have been in proximity or within the relay's internal network, spatially restricting and narrowing the suspect pool.

V. Discussion

When discussing UDIM, we should first consider the applicability results from Section IV. Using examples and entries in Table I, we demonstrated that all three data sources satisfy the model and can be applied to the described devices. Depending on source quality, type, and comparable table entries, forensic investigators can draw different conclusions. Even data sources without forensic investigation (e.g., data sheets) enable general statements about interaction possibilities. Also, UDIM can roughly classify devices without a complete forensic analysis.

Table I shows that forensic investigations are often incomplete and exhibit scenario-dependent coverage w.r.t. possible interactions and artifacts. Open entries and ambiguities regarding artifact verifiability can be problematic in criminal cases, which makes the standardization of device forensics essential. The model provides a way to verify whether all interaction types have been investigated for possible artifacts, thereby ensuring full coverage of an investigation. UDIM can analyze interactions beyond scenario-relevant artifacts and document when investigators find no artifacts. Our model thus represents a step towards the standardization of forensic analyses.

UDIM applies to all devices meeting Definition 1 (e.g., IoT devices, embedded devices, smartphones, or desktop PCs), to provide guidance for analyzing technical capabilities in the heterogeneous digital landscape. This universal applicability enables extensive use in digital forensic analyses. Accordingly, UDIM can compare devices or device classes based on expected forensic artifacts to help law enforcement determine whether seizing a device is worthwhile for a specific case. For example, verifying a person's presence requires knowing whether a device supports direct user-device interaction and whether forensic investigators may find related artifacts.

Based on the "hierarchy of propositions" [8], criminally relevant propositions at the *Offense* level must be broken down into *Activity* level statements and assigned to the *Source* level. Our model offers a way to systematize this breakdown and identifies devices where investigators can find relevant forensic artifacts at the *Source* level. Law enforcement can use digital interactions to break down *Offense* level statements into *Activity* level propositions. A common *Activity* level question involves a person's presence at a location (e.g., to check an alibi or presence at a crime scene). With UDIM, such questions map to interactions (e.g., direct user-device interaction indicates presence at the device's location).

With this knowledge, devices at the location of interest can be analyzed where such interaction is possible or where, based on other sources, an investigator can likely identify forensic artifacts. Similarly, questions about device presence can be assigned to UDIM interactions, to provide law enforcement clues about which devices warrant investigation. Beyond presence questions, crimes can be committed in a device's environment. UDIM identifies devices capable of sensory capturing the environment through device-environment interaction. For example, a verbal threat recorded by an Amazon Echo microphone represents device-environment interaction. Assuming it is already known that an investigator can find forensic artifacts from interactions between the device and its environment on Amazon Echo speakers or comparable models, forensic examination can yield statements at the *Source* level.

VI. Conclusion

We presented the *User-Device Interaction Model* (UDIM) by formally defining the model and its components as a graph $G = (V, E)$. Alongside applying the model to an exemplary device (Thermomix TM6), we also applied UDIM to 42 devices from 24 different academic and non-academic sources and source types. For the latter, we created a tabular representation of device interactions using UDIM, to discuss whether interactions were possible, whether authors examined them, and whether forensic artifacts have been found.

Furthermore, we discussed UDIM's value in standardizing and ensuring the completeness of forensic analyses of IoT and embedded devices, and addressed its universal applicability to electronic devices (Definition 1). Additionally, we illustrated its applicability in law enforcement criminal cases as well as its usefulness for data reduction during seizures.

The UDIM graph allows forensic investigators to effectively identify device interactions and summarize them (e.g., Table I), which is why we encourage the inclusion of UDIM graphs in future forensic analyses of IoT or embedded devices.

Acknowledgments

We thank the anonymous reviewers for their helpful feedback. We also thank Jan Gruber, Jenny Ottmann and Katharina De Rentiis for their comments on an earlier version of this paper. This work has been supported by Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) as part of the Research and Training Group 2475 "Cybercrime and Forensic Computing" (grant number 393541319/GRK2475/2-2024), and by the Bavarian Ministry of Science and Arts as part of the project "Security in Everyday Digitization" (ForDaySec).

References

[1] S. Li, K.-K. R. Choo, Q. Sun, W. J. Buchanan, and J. Cao, "IoT Forensics: Amazon Echo as a Use Case," *IEEE Internet of Things Journal*, vol. 6, no. 4, Aug. 2019. [Online]. Available: https://doi.org/10.1109/JIOT.2019.2906946

[2] BSH Home Appliances Ltd., "Bosch Washing machine WGH254A0GB - User manual," 2025, accessed: 2025-08-26. [Online]. Available: https://media3.bsh-group.com/Documents/9001973321_B.pdf

[3] M. Eichhorn and F. Freiling, "Dial M for Mixer: A Methodological Approach to Forensic Analysis of Unknown Devices Using the Thermomix TM6," *Forensic Science International: Digital Investigation*, Oct. 2025. [Online]. Available: https://doi.org/10.1016/j.fsidi.2025.301983

[4] Apple Inc., "Apple Watch Series 6 - Technical Specifications," 2025, accessed: 2025-08-26. [Online]. Available: https://support.apple.com/en-us/111918

[5] F. Servida, M. Fischer, O. Delémont, and T. R. Souvignet, "Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations," *Forensic Science International*, vol. 348, Jul. 2023. [Online]. Available: https://doi.org/10.1016/j.forsciint.2023.111674

[6] M. Epifani, "A journey into IoT Forensics - Episode 1 - Analysis of a Samsung Refrigerator (aka thanks VTO Labs for sharing!)," Dec. 2020, accessed: 2025-08-26. [Online]. Available: https://blog.digital-forensics.it/2020/12/a-journey-into-iot-forensics-episode-1.html

[7] J. Gruber, L. L. Voigt, Z. Benenson, and F. C. Freiling, "Foundations of cybercriminalistics: From general process models to case-specific concretizations in cybercrime investigations," *Digit. Investig.*, vol. 43, no. Supplement, p. 301438, 2022. [Online]. Available: https://doi.org/10.1016/j.fsidi.2022.301438

[8] R. Cook, I. W. Evett, G. Jackson, P. J. Jones, and J. A. Lambert, "A hierarchy of propositions: deciding which level to address in casework," *Science & Justice*, vol. 38, no. 4, Oct. 1998. [Online]. Available: https://doi.org/10.1016/S1355-0306(98)72117-3

[9] P. L. Kirk, *Crime Investigation: Physical Evidence and the Police Laboratory*, 2nd ed. John Wiley & Sons Inc., 1974, ISBN: 9780471482475.

[10] L. Jones, *Scientific Investigation and Physical Evidence: A Handbook for Investigators*. Hutson Street Press, 2025, ISBN: 9781024177848.

[11] R. Cook, I. W. Evett, G. Jackson, P. J. Jones, and J. A. Lambert, "A model for case assessment and interpretation," *Science & Justice*, vol. 38, no. 3, Jul. 1998. [Online]. Available: https://doi.org/10.1016/S1355-0306(98)72099-4

[12] F. Bouchaud, G. Grimaud, and T. Vantroys, "IoT Forensic: identification and classification of evidence in criminal investigations," in *Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES'18)*. New York, NY, USA: ACM, Aug. 2018. [Online]. Available: https://doi.org/10.1145/3230833.3233257

[13] A. Hammer, J. Geus, F. Nicolai, P. Schütz, C. Fein, and F. Freiling, "Fit for Forensics: Taxonomy and Common Model for Forensic Analysis of Fitness Trackers," *Digital Threats*, vol. 5, no. 3, Oct. 2024. [Online]. Available: https://doi.org/10.1145/3687271

[14] J. Gruber and F. Freiling, "The Cyber-traceological Model: A Model-based View of the Cybercriminalistic Task," in *Digital Forensics Research Conference Asia–Pacific (DFRWS APAC'24)*, vol. 2024, 2024. [Online]. Available: https://dfrws.org/wp-content/uploads/2024/10/the-cyber-traceological-model-a-model-based-view-of-the-cybercriminalistic-task-1.pdf

[15] J. Tournier, F. Lesueur, F. L. Mouël, L. Guyon, and H. Ben-Hassine, "IoTMap: a protocol-agnostic multi-layer system to detect application patterns in IoT networks," in *Proceedings of the 10th International Conference on the Internet of Things (IoT'20)*. New York, NY, USA: ACM, Oct. 2020, pp. 1–8. [Online]. Available: https://doi.org/10.1145/3410992.3411007

[16] Q. Wang, W. U. Hassan, A. Bates, and C. Gunter, "Fear and Logging in the Internet of Things," *Network and Distributed Systems Symposium*, Feb. 2018. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_01A-2_Wang_paper.pdf

[17] A. Almogbil, M. Steele, S. Belikovetsky, A. Inam, O. Wu, A. Rubin, and A. Bates, "Using Behavior Monitoring to Identify Privacy Concerns in Smarthome Environments," in *Proceedings 2024 Workshop on Security and Privacy in Standardized IoT*. San Diego, CA, USA: Internet Society, 2024. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/sdiotsec2024-29-paper.pdf

[18] P. Gladyshev and A. Patel, "Finite state machine approach to digital event reconstruction," *Digital Investigation*, vol. 1, no. 2, Jun. 2004. [Online]. Available: https://doi.org/10.1016/j.diin.2004.03.001

[19] B. D. Carrier and E. H. Spafford, "Categories of digital investigation analysis techniques based on the computer history model," *Digital Investigation*, vol. 3, Sep. 2006. [Online]. Available: https://doi.org/10.1016/j.diin.2006.06.011

[20] A. Dewald, "Characteristic evidence, counter evidence and reconstruction problems in forensic computing," *it - Information Technology*, vol. 57, no. 6, Dec. 2015. [Online]. Available: https://doi.org/10.1515/itit-2015-0017

[21] S. Garfinkel, A. J. Nelson, and J. Young, "A general strategy for differential forensic analysis," *Digital Investigation*, vol. 9, Aug. 2012. [Online]. Available: https://doi.org/10.1016/j.diin.2012.05.003

[22] R. Frigg and S. Hartmann, "Models in Science," Feb. 2006, accessed: 2025-06-24. [Online]. Available: https://plato.sydney.edu.au/entries/models-science/#OntoWhatMode

[23] Vorwerk, 2024. [Online]. Available: https://web.archive.org/web/20250818160528/https://www.thermomix.com/products/thermomix-tm6

[24] V. S. . C. KG, "Vorwerk Geschäftsbericht 2024," 2025. [Online]. Available: https://geschaeftsberichte.vorwerk.de/2024/fileadmin/static/pdfs/DE_Vorwerk_2024_GB.pdf

[25] M. Eichhorn and G. Pugliese, "*Do You "Relay" Want to Give Me Away?* – Forensic Cues of Smart Relays and Their IoT Companion Apps," *Forensic Science International: Digital Investigation*, vol. 50, Oct. 2024. [Online]. Available: https://doi.org/10.1016/j.fsidi.2024.301810

[26] J. Crasselt and G. Pugliese, "Started Off Local, Now We're in the Cloud: Forensic Examination of the Amazon Echo Show 15 Smart Display," in *Digital Forensics Research Conference USA (DFRWS USA'24)*, 2024. [Online]. Available: https://dfrws.org/wp-content/uploads/2024/07/dfrws-usa-2024-echo-show-15.pdf

[27] M. Stachak, J. Geus, G. Pugliese, and F. Freiling, "Nyon Unchained: Forensic Analysis of Bosch's eBike Board Computers," in *Digital Forensics Research Conference Europe (DFRWS EU'24)*, Apr. 2024. [Online]. Available: https://dfrws.org/wp-content/uploads/2024/03/Nyon-Unchained-Forensic-Analysis-of-Boschs-eBike-Board-Computer_2024.pdf

[28] M. Eichhorn, J. Schneider, and G. Pugliese, "*Well Played, Suspect!* – Forensic examination of the handheld gaming console "Steam Deck"," *Forensic Science International: Digital Investigation*, vol. 48, Mar. 2024. [Online]. Available: https://doi.org/10.1016/j.fsidi.2023.301688

[29] O. Afonin, "HomePod Forensics I: Pwning the HomePod," Mar. 2023, accessed: 2025-08-26. [Online]. Available: https://blog.elcomsoft.com/2023/03/homepod-forensics-i-pwning-the-homepod/

[30] ——, "HomePod Forensics II: checkm8 and Data Extraction," Mar. 2023, accessed: 2025-08-26. [Online]. Available: https://blog.elcomsoft.com/2023/03/homepod-forensics-ii-checkm8-and-data-extraction/

[31] ——, "HomePod Forensics III: Analyzing the Keychain and File System," Apr. 2023, accessed: 2025-08-26. [Online]. Available: https://blog.elcomsoft.com/2023/04/homepod-forensics-iii-analyzing-the-keychain-and-file-system/

[32] V. Katalov, "Apple TV and Apple Watch Forensics 01: Acquisition," Jun. 2019, accessed: 2025-08-26. [Online]. Available: https://blog.elcomsoft.com/2019/06/apple-tv-and-apple-watch-forensics-01-acquisition/

[33] M. Epifani, "Apple TV Forensics 03: Analysis," Sep. 2019, accessed: 2025-08-26. [Online]. Available: https://blog.elcomsoft.com/2019/09/apple-tv-forensics-03-analysis/

[34] ——, “Apple Watch Forensics 02: Analysis,” Jun. 2019, accessed: 2025-08-26. [Online]. Available: https://blog.elcomsoft.com/2019/06/apple-watch-forensics-02-analysis/
[35] Apple Inc., “Apple Watch User Guide,” 2025, accessed: 2025-08-26. [Online]. Available: https://support.apple.com/guide/watch/welcome/watchos
[36] BSH Home Appliances Ltd., “Bosch Home Appliances with Home Connect,” 2025, accessed: 2025-08-26. [Online]. Available: https://www.bosch-home.com/ne/specials/homeconnect#
[37] Home Connect GmbH, “About the app | Home Connect,” 2025, accessed: 2025-08-26. [Online]. Available: https://www.home-connect.com/global/home/home-connect-app
[38] Melitta Group, “Melitta-Barista-T TS-Smart: Operating Instructions,” 2025. [Online]. Available: https://www.melitta-international.com/content/dam/melitta-cp-c/me-cp/manuals/kaffeevollautomaten/Barista-T_TS-Smart_manual_total_Web.pdf.coredownload.pdf
[39] Milwaukee Electric Tool Corporation, “Digital Inventory | Milwaukee Tools Europe,” 2025, accessed: 2025-08-27. [Online]. Available: https://www.milwaukeetool.eu/systems/one-key/why-one-key/digital-inventory/
[40] ——, “M18 FUEL™ ONE-KEY™ Percussion Drill | Cordless Percussion Drills | Milwaukee Tool EU,” 2025, accessed: 2025-08-27. [Online]. Available: https://www.milwaukeetool.eu/en-eu/m18-fuel-one-key-percussion-drill/m18-onepd3/?variant=759473
[41] ——, “ONE-KEY™ Overview | Milwaukee Tools Europe,” 2025, accessed: 2025-08-27. [Online]. Available: https://www.milwaukeetool.eu/systems/one-key/
[42] Garmin Ltd., “fēnix 6 Series Owner’s Manual,” 2023, accessed: 2025-08-26. [Online]. Available: https://www8.garmin.com/manuals/webhelp/fenix6-6ssport/EN-US/fenix_6_6S_Sport_OM_EN-US.pdf