Dial M for Mixer: A methodological approach to forensic analysis of unknown devices using the thermomix TM6

By:
Maximilian Eichhorn, Felix Freiling

From the proceedings of
The Digital Forensic Research Conference
DFRWS APAC 2025
Nov 10-12, 2025

Forensic Science International: Digital Investigation 54 (2025) 301983

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

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

DFRWS APAC 2025 - Selected Papers from the 5th Annual Digital Forensics Research Conference APAC

Dial M for Mixer: A methodological approach to forensic analysis of unknown devices using the thermomix TM6

Maximilian Eichhorn *, Felix Freiling

Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany

ARTICLE INFO

Keywords:
Digital forensics
Kitchen appliance
IoT device forensics
Smart home forensics
Hardware forensics

ABSTRACT

To forensically examine an unknown digital device, a method is proposed that involves to perform experiments on an identical device and systematically derive information from the observed behaviour while performing specific actions. We apply this method to the Thermomix TM6 from Vorwerk, a multifunctional kitchen appliance. Using differential forensic analysis together with our method, we identify various forensic artefacts from real-world use, e.g., timestamps when the system was turned on and logs of specific cooking actions like dough kneading and cooking. We also observe inadequate data sanitization after factory reset. Other forensic artefacts we found include Wi-Fi login details and account information for the Cookidoo online service provided by Vorwerk to exchange recipes.

1. Introduction

Fuelled by the amenities of always-on connectivity, regular households are becoming increasingly digital and are flooded by numerous "smart" or "intelligent" devices like door bells, picture frames or cleaning robots. From an investigatory viewpoint, all of these devices potentially store information that can be of relevance if a crime has been committed within the household. The challenge for modern police work is to (1) identify relevant sources of digital evidence and then (2) to extract and interpret the stored data to give answers that are helpful to investigators. Since the landscape of such smart gadgets is incredibly wide, law enforcement regularly encounters devices that have not been examined before. At this point, forensic computer scientists are faced with the problem of analysing the device for the existence of forensically relevant traces, a challenge that is extremely hard for appliances that have not been analysed before.

An example of a class of devices that has been poorly or not at all investigated to date is *smart kitchen appliances*. Because people spend a substantial amount of time in the vicinity of kitchens while cooking or eating, data store on devices in the kitchen can potentially be used to investigate alibi or specific types of criminal modus operandi.

1.1. Related work

Within the general literature on the forensic analysis of smart devices, previous work has traditionally investigated network traffic and forensic network analysis (Wu et al., 2019; Shin et al., 2020). The literature also deals with the general challenges of IoT forensics (Servida and Casey, 2019; Wu et al., 2021) or side-channel attacks (Sayakkara et al., 2019). Getting access to data stored on these devices is often cumbersome since decryption keys are often not available and the IoT device performs encryption with hardware support (Zunaidi et al., 2024). However, in many forensic analysis situations in practice, investigators *do* not only have physical access to a device but have also obtained correct passcodes to log in. This is why it makes sense to develop methods to increase the automation of digital forensic analysis of heterogeneous unknown digital devices based on these assumptions.

Although some smart objects have already been examined in the literature, there are still gaps in terms of devices and device classes that could be investigated further. Traditionally, much related work focuses on the forensic examination of means of transport such as bicycle computers, e-scooters (Hilgert et al., 2021; Stachak et al., 2024) and cars. In addition to means of transport, IoT devices that can be used in the context of a smart home have also become the subject of investigations. These include smart relays (Eichhorn and Pugliese, 2024), CCTV systems & IP cameras (Alshalawi and Alghamdi, 2017; Dragonas et al., 2024), and smart speakers & displays (Li et al., 2019; Crasselt and Pugliese, 2024). There are also forensic investigations of IoT devices from the smart home sector under realistic scenarios (Servida et al., 2023). In addition to such papers on IoT devices outside the kitchen,

* Corresponding author.
E-mail address: maximilian.eichhorn@fau.de (M. Eichhorn).

https://doi.org/10.1016/j.fsidi.2025.301983

Available online 3 November 2025

there is literature on smart refrigerators (Kebande et al., 2017). However, we are not aware of any other work which investigated a real kitchen appliance from a forensic viewpoint.

1.2. Motivation

So, while individual smart kitchen appliances have already been forensically examined (see Section 1.1), multifunctional kitchen appliances have not yet been investigated to the best of our knowledge. The general probability of encountering such devices in forensic investigations is steadily increasing due to the ever-growing number of Internet of Things (IoT) devices (Vailshery, 2024) in general and smart appliances (Statista, 2025) in particular. Such smart devices are often used daily, and it is not always clear what data is stored on them.

The Vorwerk SE & Co. KG (Vorwerk) (Vorwerk (2025b) group of companies is well known as a manufacturer of smart household appliances in Europe and, according to its figures, had a global turnover of 3.2 billion euros in 2023. Of this, 1.3 billion euros were generated in Germany and 1.6 billion euros in the rest of Europe. The company is best known for two major product groups that are also available as smart devices: vacuum cleaners and multifunctional kitchen appliances. The kitchen appliance division Thermomix alone accounted for 54 percent of the company's turnover in 2023. Accordingly, these multifunctional kitchen appliances are of essential importance to the company group.

To accompany the physical multi-cooker appliances in the Thermomix series, Vorwerk offers the digital recipe platform Cookidoo and the forum *Rezeptwelt*. In 2025, the forum rezeptwelt. de was the target of a hacker attack (Kunz, 2025; Ćemanović, 2025), and an unknown person offered three million data records on the darknet. In addition to one million affected users from Germany, data from users in England, Spain, France, Italy, and Poland was stolen. These high user numbers and the attackers' interest in this data emphasise the relevance and prevalence of such kitchen appliances.

In this paper, we present a structured method to analyse unknown digital devices. We employ hardware and software analysis methods to analyse a specific and popular kitchen appliance, namely the Thermomix TM6 (TM6) from Vorwerk.

1.3. Contributions

In this paper, we aim to describe a method that allows to systematically analyse an unknown device, taking the multifunctional kitchen appliance Thermomix TM6 as example. We aim to answer the following research questions.

1. Which forensic artefacts from our action sets can be found on the TM6's eMMC?
2. Can the artefacts be assigned to the individual action sets and the actions contained therein using our approach and differential forensic analysis?

Overall, the contributions of this paper to the research questions are as follows.

- To the best of our knowledge, we are the first to have conducted a forensic investigation of the Thermomix TM6.
- Using differential forensic analysis, we systematically and methodically examined the memory images of the TM6. We identified the local artefacts belonging to the respective delta and thus to the performed action sets.

Vorwerk has acknowledged our findings as part of a coordinated disclosure process.

1.4. Outline

First, we describe the basics of the Thermomix TM6 and the Cookidoo recipe platform in Section 2, followed by a presentation of our methodology and approach in Section 3. Subsequently, we list our results in Section 4 and discuss our findings and their implications in Section 5. Finally, we conclude the paper in Section 6.

2. Background

Carl Vorwerk founded the former carpet factory Vorwerk (Vorwerk, 2024, 2025b) in 1883 in Germany. The company expanded its product range to include electronic appliances, adding vacuum cleaners in 1929 and kitchen machines in 1971. Vorwerk is known for directly selling its products and is active in over 60 countries. In 2023, Vorwerk had 9127 employees and 94,231 independent consultants.

2.1. Thermomix TM6

The multifunctional TM6 kitchen appliance (Vorwerk, 2025c, 2025d) was launched in 2019 and features Wi-Fi 5 and Bluetooth 4.2 connectivity. Fig. 1 shows the black TM6 model (Vorwerk, 2022), which was released in 2022 and which we examined. The special model is only a visual variation, and the functionality corresponds to the standard TM6. It is operated via a 6.8-inch touchscreen and a rotary knob. The TM6 has a pot with a capacity of 2.2 L and a blade head inside the pot. In addition to classic blending, the pot can also be heated. The appliance also has a temperature sensor and a loudspeaker.

2.2. Cookidoo

In addition to the Thermomix appliances, Vorwerk offers a digital recipe platform Cookidoo with a subscription model and (2023) 4.7

Fig. 1. The Thermomix TM6 Sparkling Black with the Varoma steam cooking unit on (Vorwerk, 2025a).

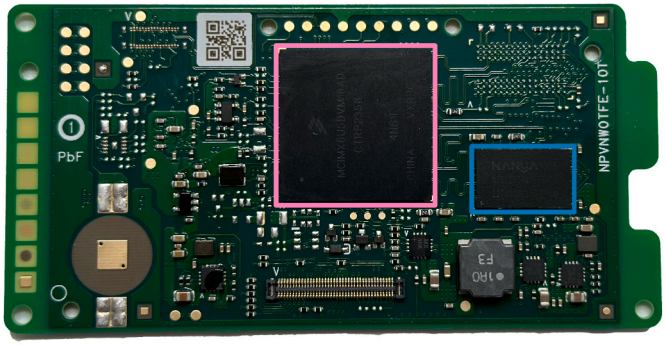
million subscribers. The recipe platform provides official recipes that can be downloaded to the Thermomix device as step-by-step instructions. Users can also modify existing recipes or create their own. The recipes can then not only be downloaded to the Thermomix, but also integrated into a weekly preview. In this preview, users can save recipes for each day of the week. The recipe platform can be accessed via the Cookidoo smartphone app, a web browser or the Thermomix itself. Depending on the country, access via the web browser may be available via other URLs (such as cookidoo. de, cookidoo. at, cookidoo. international, and cookidoo.thermomix.com). Without a subscription, only the ingredients and general information, such as preparation time, are visible for existing recipes, but not the individual preparation steps.

3. Methodology

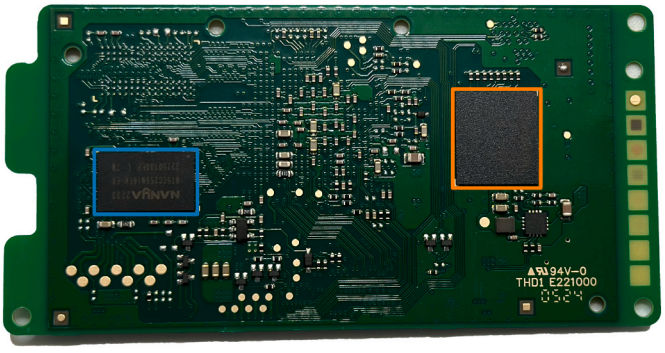
In this section, we will explain the methodology we used in the forensic examination of the TM6. In order to examine such a previously uninvestigated device and interpret forensic artefacts accurately, we recommend purchasing a new device of the same design, systematically generating usage traces on it, and methodically evaluating the artefacts generated in the process. We base our methodology and structured approach on the work of Eichhorn et al. (2024) and apply this to the TM6. The investigation will therefore be carried out on a new Thermomix TM6 Sparkling Black from 2024.

3.1. Baseline Image

After unpacking the device, the initial digital image should be read out as a baseline. To get access to the storage, we opened and disassembled the device and identified the relevant hardware components. The TM6 examined has a 16 GB eMMC (`Kingston EMMC16G-TB29`), two 4 GB DDR2 SDRAM (`NT5CC256M16ER-EK`), and an MPU (`NXP MCIMX6U5DVM10AD`) with two ARM Cortex A9 cores. The components



(a) Front view of circuit board



(b) Back view of circuit board

Fig. 2. Circuit board of the TM6 with eMMC (■), SDRAM (■) and MPU (■).

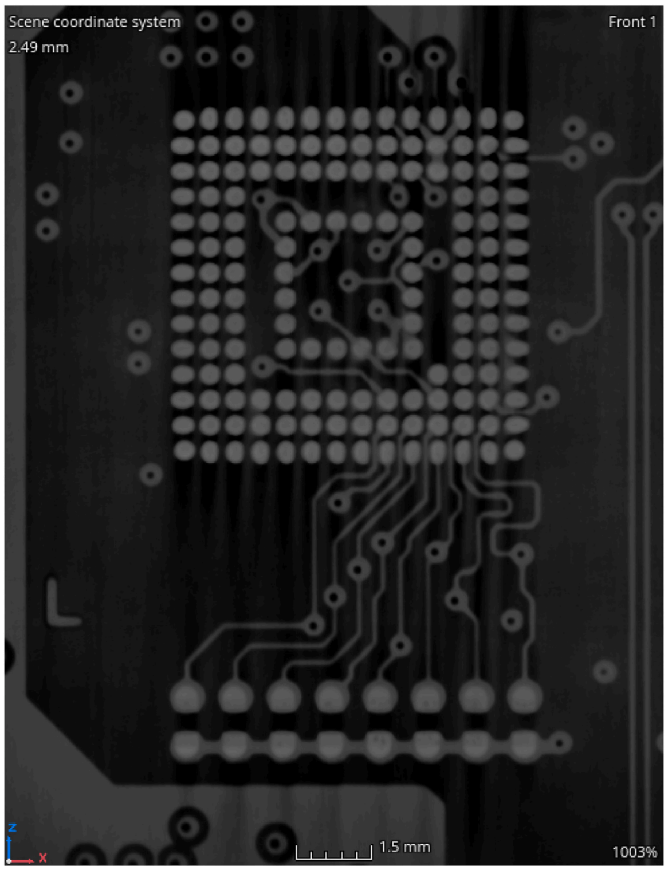


Fig. 3. X-Ray scan of the PCB with the eMMC pins.

described are mounted on a printed circuit board (PCB) labelled `NPVNW0TFE-10T` behind the display. Fig. 2 shows both sides of the circuit board with the components marked.

As this is a proprietary board layout for which no documentation is publicly available, we had to use other methods to determine the pins and contacts required to read the eMMC memory. Using a continuity measurement, we identified the GND pins and contacts, but no others. Due to the lack of information on the PCB's power supply, we could not connect an external power supply. Owing to the device's design, connecting the contacts in the installed state is hard.

An obvious approach by Crasselt and Pugliese (2024) to determine the contacts with an identical replacement PCB using an invasive procedure also had to be omitted, as no identical PCB could be purchased. However, with the aid of an X-ray machine (Phoenix V|tome|x M300), we could follow the internal conductor paths. Starting from the soldering points of the eMMC, all pins can now be traced to a freely accessible contact. Fig. 3 shows the X-ray image of the eMMC's soldering points. Of the data lines D0 to D7, D0 is sufficient for reading out at reduced speed. The contacts VCC, VCCQ, CMD, and CLK are also required for readout. The necessary contacts are marked and labelled in Fig. 4. In order to connect the CMD contact, we had to carefully scrape off the top layer of the PCB with a scalpel to expose the soldering point Fig. 5 shows the exposed soldering point and the connected measuring tips at the CMD, CLK, VCC and GND contacts. We used an EasyJTAG[1] Plus Box in conjunction with the EasyJTAG Classic Suite software to read out the eMMC memory. With the following settings within the software, the eMMC partitions (except RPMB) could be read out: IO Voltage 2.8V, bus width of 1 bit, and clock rate of 21 MHz.

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

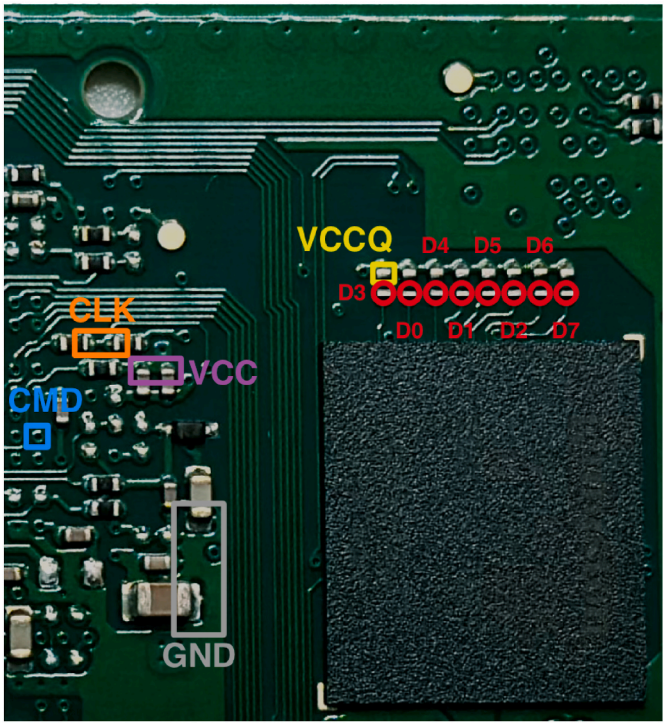


Fig. 4. Marked and labelled contacts D0-D7 (■), CLK (■), CMD (■), GND (■), VCC (■) and VCCQ (■) of the TM6 circuit board for connection to the Easy-JTAG Plus Box.

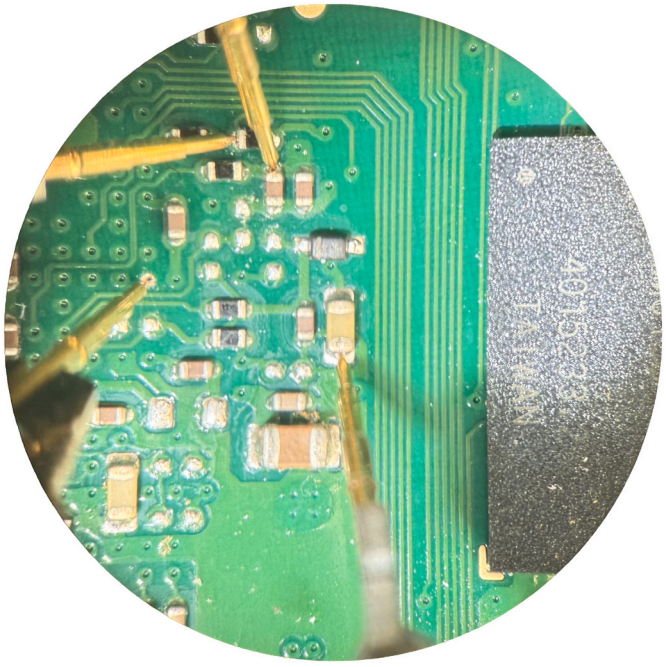


Fig. 5. Exposed soldering point (CMD) and connected measuring tips photographed under a microscope.

3.2. Creation of Test Data

In order to generate test data methodically, certain sets of actions must be planned on the TM6 and then carried out. Each set of actions σ_i should be kept as compact as possible and illustrate other functions and uses of the device. Real recipes were cooked to reflect realistic use and ensure the data is as realistic as possible. Some recipes are not freely available because they were from the Cookidoo recipe platform; the recipes are referred to differently below, and their preparation steps are only listed where necessary. The result of each action set σ_i is the state q_i. An overview of the states and the necessary action sets we have executed is shown in Table 1 and listed as σ-notation. The number of action sets or state transitions covers the device's most common uses and functions. Since no action set is required for the initial state q_0, the set of all state transitions must be specified with $\Sigma = \{\sigma_1, \ldots, \sigma_{12}\}$. The set of all states can be specified with $Q = \{q_0, \ldots, q_{12}\}$. The individual state sets are designated as follows: Baseline Image (q_0), Connect Wi-Fi (q_1), Recipe (q_2), Recipe + Wi-Fi (q_3), Login Cookidoo (q_4), Recipe + Cookidoo (q_5), Recipe + Heating (q_6), Recipe Dough (q_7), Recipe Aborting (q_8), Recipe Edited (q_9), Recipe Created (q_{10}), Update (q_{11}) and Factory Reset (q_{12}). The action sets required to achieve this are explained in Table 1 with notes.

Table 1
Set of all state transitions $\Sigma = \{\sigma_i | i \in \{1, \ldots, 12\}\}$ and states Q that were performed to generate test data on the TM6.

$\sigma_\# / q_\#$	Name	Notes
q_0	Baseline Image	First image without further actions
σ_1 / q_1	Connect Wi-Fi	First boot of device; connect to Wi-Fi
σ_2 / q_2	Recipe	Cooking recipe for the first time, uses of the functions scale & mixing; Wi-Fi disabled
σ_3 / q_3	Recipe + Wi-Fi	Cooking recipe with Wi-Fi enabled
σ_4 / q_4	Login Cookidoo	First login on Cookidoo platform on the device
σ_5 / q_5	Recipe + Cookidoo	Cooking recipe from Cookidoo; uses of the functions scale & mixing; Wi-Fi enabled
σ_6 / q_6	Recipe + Heating	Cooking recipe from Cookidoo; uses of the functions scale, mixing, pre-cleaning, stir & heating; Wi-Fi enabled
σ_7 / q_7	Recipe Dough	Cooking recipe; Wi-Fi disabled; uses of the functions scale, dough kneading & pre-cleaning; device was left on until it switched itself off; powered on again for pre-cleaning
σ_8 / q_8	Recipe Aborting	Cooking recipe with Wi-Fi disabled; uses of the functions scale, mixing, dough kneading & pre-cleaning; increasing of mixing level while mixing & aborting mixing and dough kneading while running
σ_9 / q_9	Recipe Edited	Cooking modified recipe from Cookidoo; recipe was modified beforehand; uses of the functions scale, mixing & pre-cleaning; Wi-Fi enabled
σ_{10} / q_{10}	Recipe Created	Cooking own recipe from Cookidoo; recipe was created beforehand; uses of the functions scale, mixing & pre-cleaning; Wi-Fi enabled
σ_{11} / q_{11}	Update	First initiated software update of device
σ_{12} / q_{12}	Factory Reset	Initiating factory reset on TM6

3.3. Differential Analysis

We resort to differential forensic analysis (Garfinkel, 2012; Garfinkel et al., 2012) to evaluate the effects of each action set methodically. After each action set, we read the eMMC storage according to the procedure described in Section 3.1 and created an image for each state q_i. Differential forensic analysis enables us to systematically determine the effects of the action sets based on the differences between two images. We use The Sleuth Kit (TSK)[2] and the Python script `idifference2.py`[3] in conjunction with the DFXML[3] library to perform the differential forensic analysis.

Following the notation of Dewald (2015) and Eichhorn et al. (2024), we represent the set of all states and the set of all state transitions in a finite state machine. The state machine is shown in Fig. 6, and labelled with the names of the states. An image of each state has been created and thus the detectable differences between a state q_i and the previous state q_{i-1} can be noted as δ_i. The set of all differences is named $\Delta = \{\delta_1, \ldots, \delta_{12}\}$.

When applied to two images of consecutive states, the `idifference2.py` tool lists all paths within the delta that have changed. The paths refer to directories or files, which can be created, deleted, and renamed. The content and timestamp can also be changed. Accordingly, the output of `idifference2.py` contains paths for directories and files from five categories. All files unlikely to have anything to do with the actions performed are filtered out of the output, and we checked the remaining files manually. The number of files to be checked per $\delta_i \in \Delta$ was between 41 and 3543 before and between 15 and 87 after filtering.

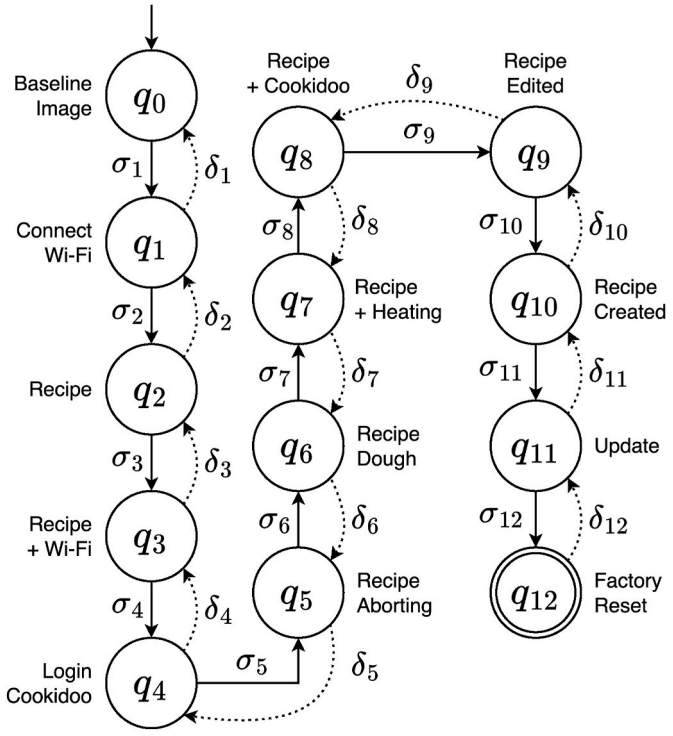


Fig. 6. Set of all state transitions $\Sigma = \{\sigma_i | i \in \{1, \ldots, 12\}\}$ and set of all states $Q = \{q_i | i \in \{0, \ldots, 12\}\}$ visualised as state machine including the set of all deltas $\Delta = \{\delta_i | i \in \{1, \ldots, 12\}\}$.

[2] https://www.sleuthkit.org/.
[3] https://github.com/dfxml-working-group/dfxml_python.

4. Results

In this section, we present excerpts of the results and examine the partitions, file systems, configuration files, log files and `blackbox` files found. We refer to files located in the `blackbox` directory as blackbox files. General Linux-specific artefacts are only touched upon and our focus is on the device-specific artefacts that were identified in the differential analysis. The subsections on the individual files all refer to a Btrfs file system.

4.1. Partitions

Following the procedure described in Section 4, we were able to read six of the seven hardware partitions of the installed eMMC using the EasyJTAG Plus Box. These include the partitions ROM1 (`uarea`), ROM2 (`boot0`), ROM3 (`boot1`), GP1 (`gp0`), GP2 (`gp1`) and GP3 (`gp2`). For the RPMB (`rpmb`) partition, we received the error message `EMMC RPMB is not yet programmed (clear)` or `Error: RPMB General failure (URL_RPMB_GENERAL)` within the EasyJTAG Suite and were unable to extract it.

Table 2 shows the hardware partitions with the labels specified in the EasyJTAG software (Label HW), the labels used in the operating system (Label OS), and further information. To avoid confusion, the Labels OS are used below. The largest partition, `uarea`, with 13.10 GiB, contains an LVM2 signature and thus splits the partition into two logical volumes (LVs), `plain_uarea` and `enc_uarea`. The changes to the partitions for each delta are listed in Table 3.

The `boot0` and `boot1` partitions contain ARMv7 executable code, are constant across all deltas, and are identical byte for byte.

The partitions `gp0`, `gp1`, and `gp2` each contain a partition table in

Table 2
Overview over the partitions of the eMMC.

Label HW	Label OS	Size MiB	FS Type	Notes
ROM1	`uarea`	13,416	LVM2	LVM2 with 2 LVs
	`plain_uarea`	3,069	BTRFS	User data
	`enc_uarea`	<7,700	LUKS1	Encrypted user data
ROM2	`boot0`	4	-	ARMv7 executable code
ROM3	`boot1`	4	-	ARMv7 executable code
RPMB	`rpmb`	4		Not readable (EasyJTAG)
GP1	`gp0`	512	-	Partition with GPT
	`gp0p1`	10		
	`gp0p2`	1	SquashFS	Some install scripts
	`gp0p3`	497	LVM2	LVM2 with 3 LVs
	`gp0-rootfs`	117	SquashFS	Root filesystem
	`gp0-appfs1`	137	LUKS1	Encrypted
	`gp0-appfs2`	94	LUKS1	Encrypted
GP2	`gp1`	512	-	Partition with GPT
	`gp1p1`	10		
	`gp1p2`	1	SquashFS	Some install scripts
	`gp1p3`	497	LVM2	LVM2 with 3 LVs
	`gp1-rootfs`	117	SquashFS	Root filesystem
	`gp1-appfs1`	137	LUKS1	Encrypted
	`gp1-appfs2`	94	LUKS1	Encrypted
GP3	`gp2`	512	-	Partition with GPT
	`gp2p1`	1		
	`gp2p2`	10	Ext4	Some `.blob` files
	`gp2p3`	497	LUKS1	Encrypted

Table 3
Overview over the changes for each $\delta_i \in \Delta$: no change (○), partition changed (●).

Partition	δ_1	δ_2	δ_3	δ_4	δ_5	δ_6	δ_7	δ_8	δ_9	δ_{10}	δ_{11}	δ_{12}
plain_uarea	●	●	●	●	●	●	●	●	●	●	●	●
enc_uarea	●	●	●	●	●	●	●	●	●	●	●	●
boot0	○	○	○	○	○	○	○	○	○	○	○	○
boot1	○	○	○	○	○	○	○	○	○	○	○	○
gp0p1	○	○	○	○	○	○	○	○	○	○	●	○
gp0p2	○	○	○	○	○	○	○	○	○	○	●	○
gp0p3	○	○	○	○	○	○	○	○	○	○	●	○
gp1p1	○	○	○	○	○	○	○	○	○	○	●	○
gp1p2	○	○	○	○	○	○	○	○	○	○	●	○
gp1p3	○	○	○	○	○	○	○	○	○	○	●	○
gp2p1	○	○	○	○	○	○	○	○	○	○	●	○
gp2p2	○	○	○	○	○	○	○	○	○	○	○	○
gp2p3	●	○	○	○	○	○	○	○	○	○	●	○

GPT layout, and each contains three partition table entries. The partition tables of the partitions `gp0` and `gp1` are identical, whereas the entries in `gp2` differ in size and type. The third entry in the partition table for `gp0` and `gp1`, `gp0p3` and `gp1p3`, contains an LVM2 signature divided into three LVs: `rootfs`, `appfs1`, and `appfs2`. The partitions `gp0` and `gp1` are constant for the subset of deltas $\Delta \setminus \{\delta_{11}\}$, and their partitions `gpXp1` and `gpXp2` they contain, as well as the LVs `rootfs`, `appfs1`, and `appfs2`, are identical to their respective counterparts.

Partition `g2` is constant for the subset of deltas $\Delta \setminus \{\delta_1, \delta_{11}\}$, and for delta1, only the byte at offset `0x05` changes from `0x39` to `0x38` in the partition `gp2p3`.

4.2. File Systems

In general, the TM6's eMMC has six storage areas encrypted with LUKS1 and three organised with LVM2. In addition to this, we were able to identify four SquashFS, one Ext4, and one Btrfs file system (see Table 2). The two LVs `rootfs` contain the actual mount point `/`. They are each SquashFS file systems and contain corresponding information about the operating system, such as the information from the file `/etc/os-release`. The operating system is a non standard Linux distribution `Vorwerk Embedded Linux Distribution` with the version number `1.0.0`, the name `dunfell` and the kernel version `5.4.210`. Furthermore, standard Linux information such as the host name `imx6qnwot` can be found. When extracting the user accounts from `/etc/passwd`, it is noticeable that there are 16 users with the prefix `nwot-`, and they have corresponding home `directories/home/nwot-...` However, only the directory of user `nwot-webkit` is present in the `rootfs`, which is empty of relevant files. The other two of the four SquashFS, `gp0p2` and `gp1p2`, are mounted via `/etc/fstab` at the mount point `/tmp/manifest_mount`. They contain individual pre- and post-install scripts, JSON files, and manifest files. The file content of these files suggests that `gp0` and `gp1` are used as primary and secondary partitions.

According to the TSK output, the Ext4 file system was last mounted at /mnt/blobs and it contains twelve files with the file extension `.blob`. These include interesting file names such as `clientSecret.blob`, `csiKey.blob`, `dmCryptKey.blob` and `Vorwerk.blob`. The files have no obvious file header and are between 80 and 1752 bytes in size. We could not successfully use any of the files to decrypt any of the LUKS1 encrypted memory areas. However, the LUKS1 encrypted areas, except for `enc-uarea`, only change during δ_{11} (Update), so they are of secondary importance for the examination. The following subsections provide further details on the Btrfs file system.

```
//config/settings/common/wifi-manager/wifi-manager.conf
{"country_code":"[CC]",
    "enabled":true, [...]
    "last_connected":"[SSID]",
    "networks": [{"enc":"WPA","enc_enabled":true,"
     psk":"[PSK]","ssid":"[SSID]"}]}

//config/state/defaultUser/auth-manager.conf
TRIAL"ACTIVE*2025-05-14T23:59:00Z2FULL:[EMAIL]B2025
     -04-14T08:07:19JRZ?
```

Listing 1. Snippets regarding Wi-Fi credentials and Cookidoo account information from two configuration files in config directory on `plain_uarea` partition.

4.3. Configuration Files

The `config/settings` and `config/state` directories contain several files that provide information about the current settings such as the speaker volume or Wi-Fi connection information. Listing 1 contains snippets from the `wifi-manager.conf` and `auth-manger.conf` files. They contain the Wi-Fi SSID, the Wi-Fi location settings, and the status of the Cookidoo account stored on the TM6. In the displayed case, it is a test subscription that is still active, and the login mail can be seen. In our assumption, the second timestamp represents the time of the last update of the Cookidoo account status.

4.4. Log Files

Unlike most Linux distributions, the log files from `journald` are not stored in `/var/log`, but on the Btrfs partition `plain_uarea` in the directory logs. Specifically, the log file of journald (`system.journal`) is also the only log file available in this path. In addition to general Linux events, device-specific events are logged. Listing 2 shows a few examples

```
//device ID
Apr 14 10:05:20 imx6qnwot HardwareManager[627]:
     PublishSystemData: {"BE-HW-Version
     ":"218169344","BE-SERIAL-NO":"[BE-NO]","BE-
     SERIAL-NO-MASKED":"[BE-NO-MASKED]",[...],"COMM-
     SECRET":"0","DEVICE-ID":"[DEVICE-ID]","DEVICE-
     SERIAL-NO":"[DEVICE-NO]","SERIAL-NO-MASKED":"
     [DEVICE-NO-MASKED]","FE-SERIAL-NO":"[FE-NO]","FE-
     SERIAL-NO-MASKED":"[FE-NO-MASKED]","FE-SW-Version
     ":{"FE-SW-release_label":"202309261610","MAJOR
     ":4,"MINOR":0,"PATCH":6},"MAC-ADDRESS":"
     E02DF0A77221","UNIQUE-ID":"0000aae4e0c71cde","
     WIFI-DOMAIN":"0","WIFI-OFFLINE":0}

//heating
Apr 16 14:45:35 imx6qnwot cookingEngineManager[629]:
      updateHeatingActive -> foodTemperature: 37,
     targetTemperature: 80, running: 1
Apr 16 14:44:53 imx6qnwot cookingEngineManager[629]:
      setting heating active to true

//mixing
May 12 13:54:48 imx6qnwot cookingEngineManager[652]:
      Set speed: 2000
May 12 13:54:48 imx6qnwot cookingEngineManager[652]:
      Published motor current speed: 1986
```

Listing 2. Snippets from the log file `system.journal` showing device information, downloaded recipe data and heating information.

of device-specific events. First, a JSON structure is listed, which contains the device ID and some other serial numbers. In addition, the log file can contain logged sensor data and information about the heating or mixing process. In the example in Listing 2, the heating is activated, and the current temperature of 37 °C and the target temperature of 80 °C are set. The mixer's set speed and a published message about the current speed are listed. In addition, the logs contain recipes from the Cookidoo platform that support guided cooking. Each of these recipes is listed with its name, individual ingredients and individual steps. All necessary information, including nutritional values and recommended accessories, is included.

4.5. Blackbox Files

The directory name `blackbox` stands out from the list of deltas, and a closer look at the files seems appropriate. Table 4 lists the `.log` files in the directory with notes on the file contents. Unlike all other log files in this directory, the file `usageboxdata.log` only exists in a subset of $q_i \in Q \setminus \{q_j | j \in \{1, 2, 3, 12\}\}$. The file contains log messages on specific changes to the device, such as the cooking status, language settings, and the like. However, we could only find these log messages in δ_7, δ_8 and δ_{11}, and the `usageboxdata.log` file seems to be overwritten repeatedly instead of being continued like a classic log file. Therefore, only actions of the state transitions σ_7, σ_8 and σ_{11} could be found. We have not noticed any reason for this behaviour.

On the other hand, the other `blackbox` log files have a CSV structure with the semicolon as a separator and are written continuously. Listing 3 first shows the content of the files `EventList.log` and `ErrorEvents.log` for q_3. For a clearer presentation, we have removed four leading `0x00` bytes in the first column of the `ErrorEvents.log` file. We will examine two of these CSV-based log files in the following. For all future examples of such file contents or excerpts from them, we will choose a tabular representation for readability and omit the first column where possible.

`EventList.log`

As we have no column headings or other indications of the file structure, we must make assumptions and check these for correctness using the remaining data. The representation of the error message events from the `ErrorEvents.log` file and the other log files leads us to the following assumptions: (1) the third column contains the abbreviation of the event which is referenced by this row, and the second column contains the abbreviation `EL` for event list; (2) the first column contains the hex value of the last occurrence of the event in the respective separate log files; (3) the fourth column contains a minimum value for the counter of the respective event.

The first assumption represents our first working hypothesis and has not yet been disproved. All events except `BB` (listed in file `OperationalData.log`) are listed, and none are listed more than once.

Table 4
Overview over the log files in `blackbox/`.

File Name	Notes
`ErrorEvents.log`	Event log for error messages
`EventList.log`	List of event codes with counter and ID of last occurrence
`EventList_temp.log`	Temporary copy of `EventList.log` (identical)
`Events.log`	Event log for all non-error messages
`Matrix.log`	Matrix log with unknown entries
`Matrix_temp.log`	Temporary copy of `Matrix.log` (identical)
`OperationalData.log`	Log for operational data with unknown entries
`RepaEvents.log`	Log with unknown entries
`usageboxdata.log`	Log with updates regarding device settings (only used for some action sets)

```
1  //blackbox/EventList.log
2  0x000000000030386C;EL;BI;11
3  0x0000000000392811;EL;BO;3
4  0x00000000000E03C7;EL;DA;1
5  0x000000000028A69A;EL;ER584;3
6  0x000000000039791D;EL;LE;11
7  0x000000000038A167;EL;LL;9
8  0x0000000000037DF96;EL;LS;11
9  0x0000000000390BEB;EL;LU;18
10 0x000000000039699E;EL;OF;3
11 0x0000000000135A3A;EL;ON;2
12 0x000000000038F1CF;EL;SC;122
13 0x000000000038F1F4;EL;SS;106
14 0x0000000000281C83;EL;TB;9
15
16 //blackbox/ErrorEvents.log
17 0x000B3B04;ER;584;0;0;0;24;0;23;5;0;0;0;13608;20;0
18 0x000B9C8C;ER;584;0;0;0;24;0;23;5;0;0;0;13608;20;0
19 0x0028A69A;ER;584;0;0;0;22;0;23;5;0;0;0;13257;20;0
```

Listing 3. Content of `EventList.log` and `ErrorEvents.log` for q_3.

Furthermore, no abbreviations appear in the third column that does not appear in any other log file in the directory. Only the error events combine two columns as abbreviations.

The third assumption without the restriction to the lower limit is not correct with absolute certainty, as there are deviations of up to -3 for individual events, i.e. there are events that were logged three times more than specified in the list. We could not find any case where the number stated in the list is greater than the number logged elsewhere. All of the discrepancies we found were already present in q_1. As there is no `EventList.log` file in q_0, we cannot perform a plausibility check for q_0 and cannot explain the deviations.

The second assumption also results as a hypothesis from the review of all other log files and could not be refuted by us with any counterexamples. We cannot prove whether the ascending hex value is an identifier or something else.

`Events.log`

Most log entries are in the `Events.log`, which stores various event types. This file overviews power on and off actions and user inputs. Table 5 shows excerpts from the file. The snippets are arranged next to each other and separated by lines.

The first excerpt is the file's content in δ_{12} and shows the events during the factory reset action set. The file content for δ_{12} begins with an `LS` entry without a value followed by an `ON` with a UNIX timestamp as the value. This regularity applies to the subset of deltas $\delta_i \in \Delta \setminus \{\delta_1, \delta_3\}$. In δ_1, the two lines are swapped, and in δ_3, the `ON` line is missing. Finally, there are the events LE without a value followed by an `OF` with the text `Manual` or `Time`. The order of the two event entries can also vary. We assume that the abbreviations `ON` and `OF` refer to the two events, power-on and power-off. This assumption is consistent with the fact that the device can be shut down manually using the rotary knob or automatically via a timeout, and this is also consistently noted in the data. However, we must note that not every power-on is logged successfully and that a reboot triggered automatically by the software also triggers an `OF Manual` event. Furthermore, the UNIX timestamps should be treated cautiously, as deviations can occur without an internet connection. Before the initial Wi-Fi connection in δ_1, the deviations were considerable.

The temperature extract shows `ST` events followed by numerical values. Based on system. journal and supported by the differential analysis for known state transitions, we assume that `ST` is the abbreviation for *set temperature* and that a corresponding temperature setting triggers the event. During operation in the corresponding action set, the temperature was initially set to 90 °C instead of 80 °C and this error was

Table 5
Snippets of `Events.log` from several $\delta_i \in \Delta$ with artefacts regarding power on & off, heating, duration setting, speed setting, dough kneading, pre-clean quick and pre-clean dough.

δ_{12}		Temperature		Clock		Speed		Dough Kneading			Pre-Clean Quick			Pre-Clean Dough		
LS		ST	37	SC	1	SS	40	SS	600	S	SS	40	S	SS	40	S
ON	1747207908	ST	40	SC	2	SS	70	SS	0	S	SS	42	S	SS	42	S
SS	1	ST	45	SC	3	SS	350	SS	600	S	SS	44	S	SS	44	S
TB	0	ST	50	SC	6	SS	500	SS	0	S	SS	46	S	SS	46	S
BO	0	ST	55	SC	9	SS	800	SS	600	S	SS	48	S	SS	48	S
LU	1295	ST	60	SC	12	SS	1100	SS	0	S	SS	50	S	SS	50	S
TB	0	ST	65	SC	16	SS	1550	SS	600	S	SS	52	S	SS	52	S
BO	-39	ST	70	SC	19	SS	2000	SS	0	S	SS	54	S	SS	54	S
LU	1295	ST	75	SC	22	SS	2550	SS	600	S	SS	56	S	SS	56	S
SS	1	ST	80	SC	26			SS	0	S	SS	58	S	SS	58	S
TB	0	ST	85	SC	30			SS	600	S	SS	60	S	SS	60	S
BO	-39	ST	90	SC	34			SS	0	S	SS	62	S	SS	62	S
LU	1295	ST	85	SC	38			SS	0	S	SS	64	S	SS	64	S
SS	1	ST	80	SC	39			SS	1	S	SS	66	S	SS	66	S
OF	Manual			SC	43			SS	600	S	SS	68	S	SS	68	S
LE				SC	47			SS	0	S	SS	70	S	SS	70	S
LS				SC	51			SS	600	S	SS	72	S	SS	72	S
SS	1			SC	54			SS	0	S	SS	74	S	SS	74	S
TB	0			SC	58			SS	600	S	SS	76	S	SS	76	S
BO	0			SC	70			SS	0	S	SS	78	S	SS	78	S
LU	1294			SC	110			SS	600	S	SS	80	S	SS	80	S
TB	0			SC	120			SS	0	S	ST	45	S	ST	37	S
BO	-39			SC	150			SS	600	S	SS	0	S	SS	0	S
LU	1294			SC	180			SS	0	S	SS	1100	S	SS	800	S
SS	1			SC	220			SS	600	S	SS	0	S	SS	0	S
TB	0			SC	250			SS	0	S	SS	1100	S	SS	800	S
BO	-39			SC	260			SS	0	S	SS	0	S	SS	0	S
LU	1294			SC	270			SS	1	S	SS	0	S	SS	0	S
SS	1			SC	300			SS	600	S	SS	1	S	SS	1	S
OF	Manual							SS	0	S	SS	2000	S	SS	800	S
LE								SS	600	S	SS	0	S	SS	0	S

then corrected by turning it back. Similarly, we assume *set clock* was abbreviated to `SC` in the clock extract and *set speed* was abbreviated to `SS` in the speed extract. The numerical values for `SC` events appear to indicate the set duration in seconds, whereas for speed, the unit of the numerical values remains unclear. However, we could assign numerical values to set mixing levels based on the performed actions. A value of 2550 corresponds to level 5.5.

In the last three snippets listed, we could match stored standard programmes to the event entries shown. We could assign the entry pattern with pulsed set speed values between 600 and 0 or 1 to the *Dough Kneading* programme. In contrast, the slow increase in the set speed values to later switch to pulsed values can be attributed to the pre-cleaning programs. The *Pre-Clean Quick* and *Pre-Clean Dough* programmes differ in the duration of the pulsed speed values set, their level, and the temperature set. Table 3 shows only the beginning of the three standard programmes mentioned here for reasons of space.

4.6. Factory Reset

According to our data, a factory reset overwrites the files in the `config` directory as δ_{12} and deletes the `usagebox*` files in the `blackbox` directory. However, the logs in the `blackbox` directory and those of `journald` are retained and continue to contain usage data about the appliance. Accordingly, the recipes that are carried out with guided cooking are still contained in the system log. In our data, we detected the SSIDs of previous Wi-Fi connections based on the `WifiManager` messages in the journal even after a factory reset.

5. Discussion

When we discuss the results in Section 4.6 we need to address the privacy implications and possible circumvention of paywalls. The undeleted log files contain information about the use of the device even after a factory reset. Accordingly, the privacy of the previous user can be violated when a used device is purchased, as the logs described above can be read out without restrictions. Furthermore, a buyer can read recipes behind a paywall in the Cookidoo portal from the log files of the journald and thus circumvent the paywall and the subscription obligation. For example, such inadequate sanitization practices and their effects have already been discussed for second-hand hard drives (Garfinkel and Shelat, 2003; Freiling et al., 2008) and USB storage devices (Schneider et al., 2025).

If we look at the evaluation of the Events. log file, we could only establish and substantiate the assumptions for interpreting the data based on our procedure and differential forensic analysis. In our approach, we had to weigh whether to use the state transitions $\sigma_i \in \Sigma$ as realistically as possible or only carry out actions as atomically as possible. With our approach, we were able to identify a corresponding non-exhaustive set of forensic artefacts. If the TM6 is not used realistically, a different number of forensic artefacts can be obtained with more atomic state transitions or a completely different approach.

Our approach for forensic analysis of unknown devices is based on generating test data on identical devices and separating practical actions into action sets. The state transitions $\sigma_i \in \Sigma$ of the state machine are based on these action sets, and the resulting forensic artefacts can be

identified and examined using differential forensic analysis. We kept the methodology very general, as the unknown devices can belong to various device classes. A kitchen appliance has different functionalities and realistic executable actions than, for example, a gaming console. The more we narrow the device class, the more we can specialise in the method.

The types of insights obtained from our methodology correspond nicely to the abstraction levels formulated as the "hierarchy of propositions" by Cook et al. (1998). This hierarchy structures insights within a forensic investigation into three levels: The *Offence* level refers to legal questions, i.e., whether a crime has actually happened or not. The *Activity* level refers to hypotheses about which concrete actions actually took place, which are mainly a concern of investigators. Finally, the *Source* level deals with hypotheses on concrete traces found at the crime scene which are analysed by forensic scientists. The insights obtained using the methodology clearly fall into the *Source* level. However, when applied to a specific device, such as the TM6, it is also possible to identify individual activities on the device, enabling statements to be made at the *Activity* level. Reaching the *Activity* level is acceptable, as no such methodology can generally provide statements at the *Offence* level.

As the multifunctional kitchen machine also has other standard programmes and functions that we were unable to test due to resource constraints, it is worth looking at the appliance's forensic artefacts in the future. Furthermore, Vorwerk offered the Thermomix TM7 (TM7), the successor model of the TM6, for sale on 7 April 2025. This TM7 no longer has a rotary knob and only a touchscreen as an input interface. It might also be worth checking our results on the new hardware.

To assess our assumptions and data interpretations and to support future work, we are making the log files of the blackbox directory publicly available at https://github.com/mxchhrn/tm-blackbox. The data collection contains the log files for each state $q_i \in Q$.

6. Conclusion

In this paper, we have shown that a forensic investigator can examine unknown devices by generating structured, controlled test data on an identical device with a methodical approach and a clear distinction between the set of states Q, set of state transitions Σ, and set of deltas Δ. Not every action of a state transition q_i can also be found in the delta δ_i from the difference between the two states q_{i-1} and q_i.

In our investigation of the TM6, we identified forensic artefacts in the device's eMMC and interpreted the data found based on assumptions. The forensic artefacts include Wi-Fi credentials, Cookidoo account information, and various usage data from the device. Furthermore, we could recognise patterns in the usage data and link them to individual standard programmes.

CRediT authorship contribution statement

Maximilian Eichhorn: Conceptualization, Methodology, Validation, Formal Analysis, Investigation, Writing -Original Draft, Writing - Review & Editing, Visualization, Project administration. **Felix Freiling:** Conceptualization, Methodology, Resources, Writing - Review & Editing, Visualization, Supervision, Project administration, Funding acquisition.

Acknowledgments

We thank the anonymous reviewers for their helpful comments and feedback, which have improved this paper. We would also like to thank Gaston Pugliese for his tips on using the EasyJTAG Plus Box and Jan Gruber for suggesting an anonymous GitHub link for reviewers. Work was 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).

References

Alshalawi, R., Alghamdi, T., 2017. Forensic tool for wireless surveillance camera. In: 2017 19th International Conference on Advanced Communication Technology (ICACT), pp. 536–540. https://doi.org/10.23919/ICACT.2017.7890148. https://ieeexplore.ieee.org/abstract/document/7890148.

Ćemanović, A., 2025. Data Breach at Thermomix Forum Exposed Info of 3.1 Million Users. https://cyberinsider.com/data-breach-at-thermomix-forum-exposed-info-of-3-1-million-users/. (Accessed 20 May 2025).

Cook, R., Evett, I.W., Jackson, G., Jones, P.J., Lambert, J.A., 1998. A hierarchy of propositions: deciding which level to address in casework. Sci. Justice 38, 231–239. https://doi.org/10.1016/S1355-0306(98)72117-3. https://www.sciencedirect.com/science/article/pii/S1355030698721173.

Crasselt, J., Pugliese, G., 2024. Started off Local, Now We're in the Cloud: Forensic Examination of the Amazon Echo Show 15 Smart Display. https://doi.org/10.48550/arXiv.2408.15768. http://arxiv.org/abs/2408.15768.

Dewald, A., 2015. Characteristic evidence, counter evidence and reconstruction problems in forensic computing. IT Inf. Technol. 57, 339–346. https://doi.org/10.1515/itit-2015-0017. https://www.degruyterbrill.com/document/doi/10.1515/itit-2015-0017/html.

Dragonas, E., Lambrinoudakis, C., Kotsis, M., 2024. IoT forensics: Exploiting log records from the DAHUA technology CCTV systems. J. Forensic Sci. 69, 117–130. https://doi.org/10.1111/1556-4029.15401. https://onlinelibrary.wiley.com/doi/abs/10.1111/1556-4029.15401.

Eichhorn, M., Pugliese, G., 2024. *Do You "Relay" Want to give Me Away?* – Forensic cues of smart relays and their IoT companion apps. Forensic Sci. Int.: Digit. Invest. 50, 301810. https://doi.org/10.1016/j.fsidi.2024.301810. https://www.sciencedirect.com/science/article/pii/S2666281724001343.

Eichhorn, M., Schneider, J., Pugliese, G., 2024. *Well Played, Suspect!* – Forensic examination of the handheld gaming console "Steam Deck". Forensic Sci. Int.: Digit. Invest. 48, 301688. https://doi.org/10.1016/j.fsidi.2023.301688. https://www.sciencedirect.com/science/article/pii/S266628172300207X.

Freiling, F.C., Holz, T., Mink, M., 2008. Reconstructing People's Lives: A Case Study in Teaching Forensic Computing. Gesellschaft für Informatik e.V., pp. 125–141. https://dl.gi.de/handle/20.500.12116/23588

Garfinkel, S., 2012. Digital forensics XML and the DFXML toolset. Digit. Invest. 8, 161–174. https://doi.org/10.1016/j.diin.2011.11.002. https://www.sciencedirect.com/science/article/pii/S1742287611000910.

Garfinkel, S., Shelat, A., 2003. Remembrance of data passed: a study of disk sanitization practices. IEEE Security & Privacy 1, 17–27. https://doi.org/10.1109/MSECP.2003.1176992. https://ieeexplore.ieee.org/document/1176992.

Garfinkel, S., Nelson, A.J., Young, J., 2012. A general strategy for differential forensic analysis. Digit. Invest. 9, S50–S59. https://doi.org/10.1016/j.diin.2012.05.003. https://www.sciencedirect.com/science/article/pii/S174228761200028X.

Hilgert, J.N., Lambertz, M., Hakoupian, A., Mateyna, A.M., 2021. A forensic analysis of micromobility solutions. Forensic Sci. Int.: Digit. Invest. 38, 301137. https://doi.org/10.1016/j.fsidi.2021.301137. https://www.sciencedirect.com/science/article/pii/S2666281721000354.

Kebande, V.R., Karie, N.M., Michael, A., Malapane, S.M., Venter, H., 2017. How an IoT-enabled "smart refrigerator" can play a clandestine role in perpetuating cyber-crime. In: 2017 IST-Africa Week Conference (IST-Africa), pp. 1–10. https://doi.org/10.23919/ISTAFRICA.2017.8102362. https://ieeexplore.ieee.org/abstract/document/8102362.

Kunz, C., 2025. Data Leak at Thermomix: Data from 1 Million German Users on the Darknet. https://www.heise.de/en/news/Data-leak-at-Thermomix-data-from-1-million-German-users-on-the-darknet-10273939.html. (Accessed 18 May 2025).

Li, S., Choo, K.K.R., Sun, Q., Buchanan, W.J., Cao, J., 2019. IoT Forensics: Amazon Echo as a Use case. IEEE Internet Things J. 6, 6487–6497. https://doi.org/10.1109/JIOT.2019.2906946. https://ieeexplore.ieee.org/document/8672776/.

Sayakkara, A., Le-Khac, N.A., Scanlon, M., 2019. Leveraging Electromagnetic Side-Channel Analysis for the Investigation of IoT Devices. Digit. Invest. 29, S94–S103. https://doi.org/10.1016/j.diin.2019.04.012. https://www.sciencedirect.com/science/article/pii/S1742287619301616.

Schneider, J., Fukami, A., Lautner, I., Eichhorn, M., Moussa, D., Wolf, J., Scheler, N., Deuber, D., Freiling, F., Haasnoot, J., Henseler, H., Malik, S., Morgenstern, H., Westman, M., 2025. Poor Sanitization Practices and Questionable Digital Evidence: a Comprehensive Study of Scope and Impact of Recycled NAND Flash Chips. IEEE Trans. Dependable Secure Comput. 1–15. https://doi.org/10.1109/TDSC.2025.3579237. https://ieeexplore.ieee.org/document/11032166.

Servida, F., Casey, E., 2019. IoT forensic challenges and opportunities for digital traces. Digit. Invest. 28, S22–S29. https://doi.org/10.1016/j.diin.2019.01.012. https://www.sciencedirect.com/science/article/pii/S1742287619300222.

Servida, F., Fischer, M., Delémont, O., Souvignet, T.R., 2023. Ok Google, Start a Fire. IoT devices as witnesses and actors in fire investigations. Forensic Sci. Int. 348, 111674. https://doi.org/10.1016/j.forsciint.2023.111674. https://www.sciencedirect.com/science/article/pii/S037907382300124X.

Shin, Y., Kim, H., Kim, S., Yoo, D., Jo, W., Shon, T., 2020. Certificate Injection-Based Encrypted Traffic Forensics in AI Speaker Ecosystem. Forensic Sci. Int.: Digit. Invest. 33, 301010. https://doi.org/10.1016/j.fsidi.2020.301010. https://www.sciencedirect.com/science/article/pii/S2666281720302596.

Stachak, M., Geus, J., Pugliese, G., Freiling, F., 2024. Nyon Unchained: Forensic Analysis of Bosch's eBike Board Computers. https://doi.org/10.48550/arXiv.2404.12864. http://arxiv.org/abs/2404.12864.

Statista, 2025. Penetration Rate of the Smart Homes Market Worldwide from 2019 to 2028. https://www.statista.com/forecasts/887636/penetration-rate-of-smart-homes-in-the-world. (Accessed 15 May 2025).

Vailshery, L.S., 2024. Number of Internet of Things (IoT) Connected Devices Worldwide from 2022 to 2023, with Forecasts from 2024 to 2033. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. (Accessed 15 May 2025).
Vorwerk, 2022. Black Limited Edition Thermomix TM6 - Sold Out!. https://thermomix.com.au/blogs/blog/black-limited-edition-tm6. (Accessed 15 March 2025).
Vorwerk, 2024. Geschäftsbericht 2023: Ideenraum. https://geschaeftsberichte.vorwerk.de/2023/assets/downloads/VOR_GB23_DE_Gesamt.pdf. (Accessed 15 May 2025).
Vorwerk, 2025a. Thermomix TM6 Sparkling Black. https://www.thermomix.ca/products/tm6%C2%AE-sparkling-black. (Accessed 13 May 2025).
Vorwerk, 2025b. This Is Vorwerk. https://www.vorwerk-group.com/en/home/about_vorwerk/this_is_vorwerk. (Accessed 15 May 2025).
Vorwerk, 2025c. TM6: Technical Specifications. https://thermomix.com.au/products/thermomix-tm6. (Accessed 7 March 2025).
Vorwerk, 2025d. User Manual: Thermomix TM6 V2.0. https://www.vorwerk.com/gb/en/c/dam-home/service/instruction-manuals/TM6_digital_manual_MGB-en-GB_prefill_20190207.pdf. (Accessed 10 March 2025).
Wu, T., Breitinger, F., Baggili, I., 2019. IoT Ignorance is Digital Forensics Research Bliss. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, pp. 1–15. https://doi.org/10.1145/3339252.3340504. https://dlnext.acm.org/doi/10.1145/3339252.3340504.
Wu, T., Breitinger, F., Niemann, S., 2021. IoT network traffic analysis: opportunities and challenges for forensic investigators? Forensic Sci. Int.: Digit. Invest. 38, 301123. https://doi.org/10.1016/j.fsidi.2021.301123. https://www.sciencedirect.com/science/article/pii/S2666281721000214.
Zunaidi, M.R., Sayakkara, A., Scanlon, M., 2024. A Digital Forensic Methodology for Encryption Key Recovery from Black-Box IoT Devices. In: 2024 12th International Symposium on Digital Forensics and Security (ISDFS), pp. 1–7. https://doi.org/10.1109/ISDFS60797.2024.10527284. https://ieeexplore.ieee.org/abstract/document/10527284.