

Investigative opportunities from smart heating technology: a preliminary evaluation

Graeme Horsman 

Cranfield University, Bedford

ABSTRACT

This work provides a case study documenting one of the first digital forensic examinations of a smart home heat system – Hive. The case study tries to address the forensic questions that law enforcement are likely to have in regards to smart home heating systems as well as highlighting relevant digital investigative opportunities. Data extracted from the Hive smart heating app (v. 10.54.2 (3)) when used on iOS v. 14.2 is presented and evaluated in order to determine whether it is possible to understand who has control over a heating system and what their controlling actions look like in regard to operating the system. Findings show that user information, pincode details and records of how the heating and water functionality can be acquired.

ARTICLE HISTORY

Received 17 July 2023

Accepted 26 February 2024

KEYWORDS

Smart heating; digital forensics; investigation; digital evidence

1. Introduction

Developments in ‘smart’ technology now allow us to control many of the functions of our households, ranging from lighting to heating. This level of greater control is often seen as beneficial, giving more detailed insight into our behaviours, and ultimately as a tool for lowering or controlling our energy consumption and to save money¹. These devices have arguably become more popular since the beginning of the COVID pandemic² and then as many societies face a ‘cost of living crisis’ in 2022/23 and seek to save costs with increasing energy bills. However, with greater control over household functions comes the opportunity for the abuse of this technology^{3,4}. This work focuses on the use of smart home heating systems, where their use by perpetrators to commit acts of domestic abuse have already been noted^{5–8}. Riley⁹ states that ‘if one person in the household is the account administrator of everyday items like the heating system . . . they can each be used as tools of coercion and control. If these devices stop functioning properly, only one person can put things straight again – a classic method of enforcing dependence’. In these cases, victims can be deprived of heat, and are also aware that if they interact with the heating system to turn it up/on, it is likely that a perpetrator will be alerted⁷.

At the time of writing, it would appear that there are no documented and published forensic examinations of commercially available smart home systems. As a result, it is

CONTACT Graeme Horsman  graeme.horsman@cranfield.ac.uk  Canfield Forensic Institute, Cranfield University, College Rd, Cranfield, Wharley End, Bedford MK43 0AL, UK

© 2024 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

difficult to ascertain the investigative opportunities that such systems may offer law enforcement when conducting their inquiries. This work provides an introductory case study for this area of digital forensics and tries to address a number of forensic questions that law enforcement may have in regards to smart home heating systems. As a case study, a Hive¹⁰ Home smart system has been subject to forensic examination and relevant evidence types have been highlighted and discussed. In 2018, YouGov¹¹ suggested that over 50% of those who owned a smart thermostat had a Hive. In [Section 2.1](#) the functionality of the Hive system is outlined and the investigative methodology used in this work is specified in [Section 2.1.1](#). The investigative questions that law enforcement may have regarding the system are discussed throughout [Section 2](#), where [Section 2.2.1](#) explores records relating to system access, before [Sections 2.2.2–2.2.3](#) examine records relating to heating and water system usage. Finally, concluding thoughts are offered.

2. Case study

The smart home thermostats market is forecast to grow to 25.5 billion dollars worldwide by 2030¹² where market leading brands include Hive¹⁰ Home, tado¹³, Google Nest¹⁴ and Honeywell¹⁵. Whilst the smart home heating systems may not be considered an obvious source of inquiry-relevant information, it is difficult to obtain a full understanding as to how an examination of this type could contribute to an inquiry without first understanding the capability of these systems. As a result, it is important to explore these technologies to determine their potential investigative worth, not only to identify opportunities but also to prevent resources being wasted examining such devices if data needed to answer an investigators queries does not exist upon them or within their ecosystem. To start this case study, consideration of Hive's functionality is provided.

2.1. Hive - what can it do?

Hive is a product produced by Centrica, and is considered one of the leading smart home brands in the United Kingdom¹⁶, with the brand also acknowledged in the U.S¹⁷. Hive offers users the ability to control their home boiler remotely, either via their mobile device using the Hive application, or with some models, a physical thermostat device. Effectively, the Hive system provides users with greater flexibility to control their home boiler. A boiler's static control panel is replaced by a Hive receiver, then through a hub which is attached to the homes' Wi-Fi router, commands can be sent to it to control its function. All of the functions on the Hive thermostat can be replicated through the Hive application and commands issued on the thermostat are reflected in the Hive application interface. Hive offers two levels of functionality, a free option, and 'Hive Heating Plus' costing approximately £40 a year in the U.K. as of July 2022¹⁸. The following is an overview of the core ability of Hive:-

- (1) Turn a boiler's heating function on/off, define a minimum temperature and 'boost it' (allowing heating to be instantly put on for a defined period).
- (2) Turn a boiler's hot water function on/off, define a minimum temperature and 'boost it' (allowing heating to be instantly put on for a defined period).
- (3) Define a weekly schedule for a boiler's heating and hot water functions.

Hive Heating Plus provides the user with finer grained information regarding their heating actions and historical data of potentially up to a year of activity (as opposed to only 1 days worth of history in the free version).

2.1.1. Methodology

For the purposes of this case study, the Hive application (v. 10.54.2 (3)) was installed on iOS v14.2 and used to control the model of Hive titled the 'Hive Thermostat' (the Hive Thermostat mini also exists). Privileged access to the device was obtained via jailbreaking (a technique frequently utilized within the forensic community to obtain access to a device's content^{19,20}, allowing the Hive application folder to be extracted and examined. Test actions were conducted on the application which were designed to elicit responses from the system's core functionality. Accessing the system via a designated account in order to utilize both the heating and water system functions has been conducted and attempts have been made to identify and interpret digital traces related to these activities.

The forensic examination was confined to the Hive application rather than deploying more invasive methods on the Hive hardware. This was determined to be the most appropriate approach given that in many instances, hardware interrogation in this space may require specialist input from electricians and heating engineers, which in a policing operational environment may not be practical. Therefore opportunities arising from the mobile application may be more operationally acquirable and usable.

2.2. What are the investigative questions and opportunities that may be available?

When approaching the digital opportunities that may be available from a smart home heating system, it is arguably beneficial to consider the investigative questions that any law enforcement official may seek to ask as part of their inquiry. As a result, we have approached the initial analysis of Hive in that way.

2.2.1. Can the system be accessed, and by who?

When a user downloads the Hive system, a primary account must be created for it and used to access the Hive app. For households that intend to have more than one intended user, there are two potential options. The credentials for the primary account could be shared and logged into the Hive app on each individual's device. Alternatively, the primary account can issue an 'invite' to other individuals, which if accepted allows them to become an 'invited person', with the ability to control the system. Invited persons come in two categories, 1) 'Partner', who has an equal ability to control the system as the primary user, and 2) 'Family' who can control the system but not remove devices or edit settings. A primary account holder can remove an invited person from the system at any point.

Access to the Hive heating system may be prohibited or protected by a PIN, but this only affects the device where the app resides (it does lock the app for other system users on their devices). The Hive application allows a 4 digit numeric PIN lock to be applied, preventing any of the system's settings and menu options from being accessed. Testing suggests that setting a PIN lock has limited impact on the application's resident data

inside of its app folder (i.e. no encryption appears to be applied), meaning an extraction of the device should still provide all of the resident application data. Determining that a PIN lock is set, and, what that PIN lock is requires an examination of the manifest.json file stored at location '<Hive App Folder>/Library/Application Support/uk.co.britishgas.hive/RCTAsyncLocalStorage_V1/'. This JSON formatted file contains the following structure where the user account's email address is first proceeded by a boolean value determining whether the PIN lock is enabled (pinLockEnabled\': \"true\") followed by the actual 4 digital PIN (for example, pin\': \"9999\") (see [Figure 1](#)).

It may also be pertinent to an investigation to ascertain the details of the account associated with the Hive application. This information is present in the SQLite file Cache.db which can be located at path '<Hive App Folder>/Library/Caches/uk.co.britishgas.hive/' and this database consists of four tables. Table cfurl_cache_receiver_data contains a number of JSON formatted records, where records commencing with {'user': { contain information about the account signed into the application. A typical records internal structure contains the account ID, email address, name, address, coordinates of the address (longitude and latitude), previously set PIN codes (if there is one) and mobile number linked to the account. A focused version of this structure is shown in [Figure 2](#) with relevant user metadata highlighted.

When the system has multiple users, it is necessary to determine what privileges they have on the system, i.e are they the primary account holder, a 'partner' or

```
"USER ACCOUNT EMAIL-pinLockEnabled\":"true\", \"USER ACCOUNT
EMAIL-pin\":"9999\"
```

[Figure 1](#). PIN lock information.

```
"<USER EMAIL
ADDRESS>", "firstName": "TOM", "lastName": "JONES", "address"
: "10 Jones Street", "city": "London", "country": "United
Kingdom", "countryCode": "GB", "postcode": "LL1 2LL
", "longitude": -5.9274389, "latitude": 34.0987231,
"pin": "5555" "email": "<USER EMAIL
ADDRESS>", "mobile": "+4455555555", "phone": "+4455555555", "
timezone": "Europe/London", "locale": "en-GB", "temperatureU
nit": "C"}
```

[Figure 2](#). Cache.Db JSON formatted records.

'family'. In addition to the information shown in [Figure 2](#) for JSON formatted records, where records commencing with `{'user':{}`, it is necessary to identify the `'homeUsers':{string` further down in the record itself. Here, account IDs that are preceded by `'OWNER'` indicate the primary account holder for the system, account IDs preceded by `'SUPERUSER'` indicate partner account holders and finally, account IDs preceded by `'SECONDARY_USERS'` indicate family account holders. Attributing account information (names etc.) the account IDs has been shown above and demonstrated in [Figure 2](#).

2.2.2. How is the heating/water used?

Hive allows a seven day schedule to be programmed where schedule records are also present in the `Cache.db` file. Table `cfurl_cache_receiver_data` may contain a JSON formatted record commencing with `{'schedule':{}`. This record sets out the weekly programmed schedule where each can be split into up to six time slices and a target heat set. The day of each week is listed, followed by a `'start'` time which is an integer value representing the number of minutes from 00:00 (so in the example below shown in [Figure 3](#), Monday's start time is 06:30 ($390/60 = 6.5$ hours – then add to 00:00)). The `'target'` is set in degrees celsius (unless the settings are changed to fahrenheit).

2.2.3. Historical records

When the user selects the 'heating history' option, up to seven days of history is shown to the user allowing them to see the temperature reported on their thermostat. By selecting and refreshing this screen, historical records of the intervals of when the heating and water were on/off are cached and the thermostat temperature in an alphanumerically named JSON file at location `'<Hive App Folder>/Library/Caches/uk.co.britishgas.hive/fsCachedData/'`. This file contains a series of sections where `'heating_relay'` shows the time intervals (stored in a UNIX timestamp format) of when the heat is on (shown by a '1') or off (shown by a '0'). This format is also utilized for showing when the water is on/off under the heading of `'water_relay'`. Finally, `'temperature'` shows the temperature on the thermometer in timed intervals. Examples of heating history records are shown in [Figure 4](#).

This folder may also contain additional 'heating history' JSON files from previous times that the 'heating history' screen has been interacted with or refreshed. It was not possible to establish how long these files may reside in this folder before they are removed.

2.3. Overriding any settings

The heating and water functionalities can be controlled by a user via interacting with the Hive Thermostat interface, and through the Hive app itself. Therefore whilst one party may not have access to the Hive app, if they can access the Hive Thermostat, then they can adjust any settings defined by in the app. However, any changes will be reflected in the app interface. In addition, the Hive Thermostat is portable, and to work it must be connected to the household Wi-Fi. An offender could opt to remove this device so it cannot be accessed by someone else.

```

{"schedule":{"monday":[{"start":390,"value":{"target":20}},{"start":510,"value":{"target":7}},{"start":720,"value":{"target":7}},{"start":840,"value":{"target":7}},{"start":990,"value":{"target":20}},{"start":1320,"value":{"target":7}}],"tuesday":[{"start":390,"value":{"target":20}},{"start":510,"value":{"target":7}},{"start":720,"value":{"target":7}},{"start":840,"value":{"target":7}},{"start":990,"value":{"target":20}},{"start":1320,"value":{"target":7}}],"wednesday":[{"start":390,"value":{"target":20}},{"start":510,"value":{"target":7}},{"start":720,"value":{"target":7}},{"start":840,"value":{"target":7}},{"start":990,"value":{"target":20}},{"start":1320,"value":{"target":7}}],"thursday":[{"start":330,"value":{"target":22}},{"start":390,"value":{"target":7}},{"start":720,"value":{"target":7}},{"start":840,"value":{"target":7}},{"start":990,"value":{"target":20}},{"start":1320,"value":{"target":7}}],"friday":[{"start":390,"value":{"target":20}},{"start":510,"value":{"target":7}},{"start":720,"value":{"target":7}},{"start":840,"value":{"target":7}},{"start":990,"value":{"target":20}},{"start":1320,"value":{"target":7}}],"saturday":[{"start":390,"value":{"target":20}},{"start":510,"value":{"target":32}},{"start":885,"value":{"target":7}},{"start":900,"value":{"target":7}},{"start":990,"value":{"target":19.5}},{"start":1320,"value":{"target":7}}],"sunday":[{"start":390,"value":{"target":20}},{"start":510,"value":{"target":7}},{"start":720,"value":{"target":12.5}},{"start":840,"value":{"target":7}},{"start":990,"value":{"target":20}},{"start":1320,"value":{"target":7}}]}}
```

Figure 3. Schedule record example.

```
"heating_relay": {"1682378340":0, "1682379480":0, "1682380680":0, "1682381880":0, "1682383080":0, "1682384220":0, "1682385420":0, "1682386620":0, "1682387700":1, "1682387820":1,
```

```
"temperature": {"1682378340":13.3, "1682378820":13.3, "1682380140":13.1, "1682381580":13.1, "1682382780":13, "1682383740":12.8, "1682385060":12.8, "1682386440":12.6, "1682387700":12.6, "1682387820":12.6,
```

```
"water_relay": {"1682378340":0, "1682379480":0, "1682380680":0, "1682381880":0, "1682383080":0, "1682384220":0, "1682385420":0, "1682386620":0, "1682387700":0, "1682387820":0, "1682388960":1, "1682390160":1, "1682391360":0,
```

Figure 4. Examples of heating history records.

In addition, if two users are logged into the Hive app using the same account details, or one as the account holder, the other as an 'invited person', then each can override the other's actions in real time.

2.3.1. Removing devices

If a user removes the Hive thermostat from the home and out of signal range from the Hive receiver (located on or near the boiler where its controls were previously situated before Hive's installation), testing showed the heating system to register in the Hive application as being 'offline' and therefore the system cannot be controlled remotely using the application alone (see [Figure 5](#)). Similarly, the heat system cannot be controlled via the thermostat itself as it registers 'no signal', and is unable to communicate with the heating system. It is however possible to remove the option of controlling the system using the Hive application whilst maintaining control using the thermostat alone (providing it remains within signal range). To do this, the Hive hub (a device connected to the household router allowing the Hive application to communicate remotely with the thermostat) can be removed (powered off or disconnected), where in this case, testing showed that control of the system was maintained by the thermostat, but the Hive application reported the system as offline.

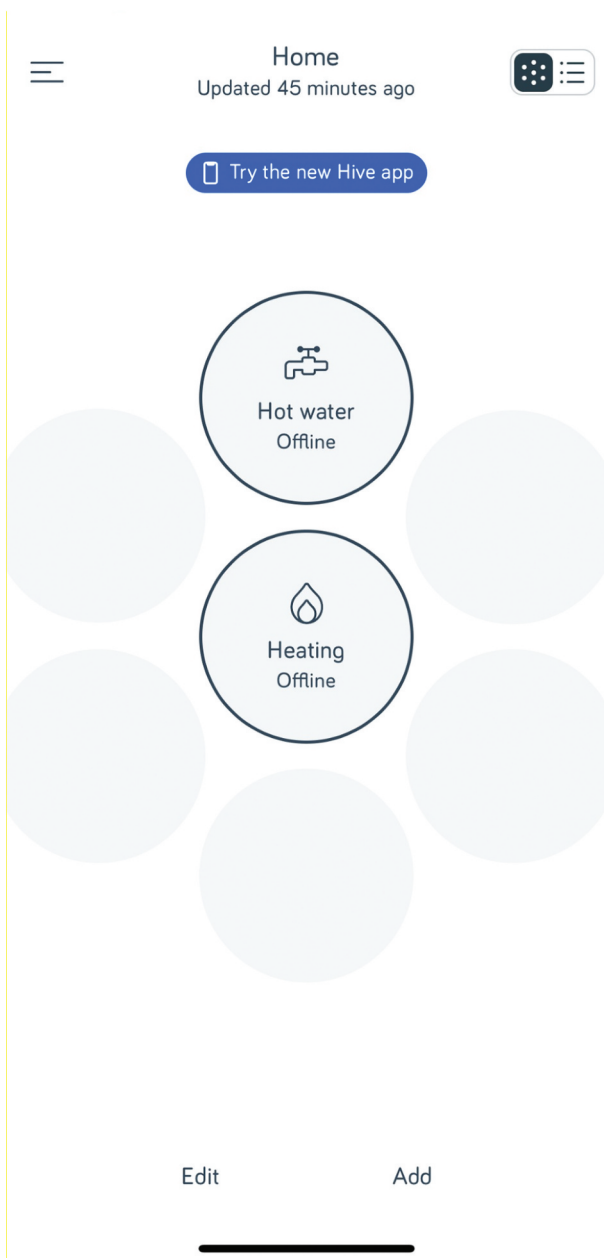


Figure 5. The hive application shows the heating system as 'offline' when the thermostat is removed from the home.

3. Concluding discussions

It is likely that smart home heating systems will be encountered relatively frequently by law enforcement who conduct inquiries at domestic dwellings given the statistics on ownership of this technology, and therefore maintaining an appreciation of the potential digital value of these systems is important. They are unlikely to consistently feature in

investigations given the limited scope of their functionality, however, in cases of abuse, documented use of these systems may provide insight into acts of coercive control. This introductory case study demonstrates that in the context of Hive, the applications used by smart home systems do maintain local records of user control and usage behaviours and these records may be pertinent to show how the system has been used. This information alone is not sufficient to show illegal behaviour, however it may form part of a larger package of intelligence that describes a course of abusive conduct.

This work is a preliminary case study having explored one single brand of smart heating device, and therefore those in this field should continue to take opportunities to investigate further smart home systems, their functionality and any subsequent generated digital traces. Given that such systems often need to be expertly fitted to existing boilers, the chance to conduct forensic investigations of their usage could be limited, making it potentially difficult to keep up to date with developments in this area. Arguably at present, this area is not a priority, however given that these systems can be integrated into a wider smart home ecosystem and as their functionality develops, there may become a need in future.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Graeme Horsman  <http://orcid.org/0000-0002-0685-0650>

Author contributions

The author is responsible for all work in this article.

References

1. Jackman J. Smart home statistics. 2023 [cited 2023 April 24]. Available from: <https://www.theecoexperts.co.uk/smart-homes/statistics>
2. TechUK. The state of the connected home. 2022 [cited 2023 April 24]. Available from: <https://www.techuk.org/asset/E8F73B01-E875-434C-BC86775874E82342/>
3. Alshehri A, Salem MB, Ding L. Are smart home devices abandoning IPV victims? In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (p. 1368–1375); 2020 December; IEEE.
4. Sovacool B, Furszyfer-Del Rio DD, Martiskainen M. Can prosuming become perilous? Exploring systems of control and domestic abuse in the smart homes of the future. *Front Energy Res.* 2021;9:765817. doi:10.3389/fenrg.2021.765817
5. Beresford J. Anger as husband locks thermostat in family home: coercive Control. 2022 [cited 2023 April 24]. Available from: <https://www.newsweek.com/husband-locks-thermostat-family-home-coercive-control-mumsnet-1768650>
6. University of Portsmouth. Increasing use of technology driving new forms of domestic abuse. 2022 [cited 2023 April 24]. Available from: <https://www.port.ac.uk/news-events-and-blogs/news/increasing-use-of-technology-driving-new-forms-of-domestic-abuse>

7. Vella H. IoT devices and smart domestic abuse: who has the controls? 2018 [cited 25 April 2023]. Available from: <https://eandt.theiet.org/content/articles/2018/06/iot-devices-and-smart-domestic-abuse-who-has-the-controls/>
8. Waterfield S. Smart home devices can be used in domestic abuse, researcher warns 2022 [cited 2023 April 24]. Available from: <https://techmonitor.ai/policy/privacy-and-data-protection/smart-home-domestic-abuse-leonie-tanczer>
9. Riley A. How your smart home devices can be turned against you. 2020 [cited 2023 April 25]. Available from: <https://www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse>
10. Hive. Hive thermostat. 2023a [cited 2023 April 25]. Available from: <https://www.hivehome.com/>
11. YouGov. The dawn of the connected home. 2018 [cited 2023 April 24]. Available from: https://trend-monitor.co.uk/wp-content/uploads/2019/01/YouGov_UK_2018_08_smart_homes.pdf
12. Statista. Size of smart thermostat market worldwide from 2021 to 2030. 2023 [cited 2023 April 25]. Available from: [statista.com/statistics/1256264/worldwide-smart-thermostat-market-revenues/](https://www.statista.com/statistics/1256264/worldwide-smart-thermostat-market-revenues/)
13. Tado. Control your heating and bills. 2023 [cited 2023 April 25]. Available from: <https://www.tado.com/gb-en>
14. Google. What makes a nest thermostat a nest thermostat?. 2023 [cited 2023 April 24]. Available from: https://store.google.com/magazine/compare_thermostats?hl=en-GB
15. Honeywell. Thermostats. 2023 [cited 2023 April 25]. Available from: <https://www.honeywellhome.com/us/en/products/air/thermostats/>
16. Statista. Leading smart home brands ranked by brand awareness in the United Kingdom in 2022. 2022 [cited 2023 November 22]. Available from: <https://www.statista.com/statistics/1341550/most-well-known-smart-home-brands-in-the-uk/>
17. Statista. Leading smart home brands ranked by brand awareness in the United States in 2022. 2022 [cited 2023 November 22]. Available from: <https://www.statista.com/statistics/1341441/most-well-known-smart-home-brands-in-the-united-states/>
18. Hive. Hive heating plus. 2023b [cited 2023 April 26]. Available from: https://www.hivehome.com/shop/smart-heating/hive-heating-plus?cid=ppc.cid_tool%3Dgoo.cid_ctype%3Dbran.cid_cname%3DHive_Brand_Core_Exact&icid=mname%3Amega-menu.iname%3Ahive-active-heating-plus
19. Elcomsoft. Forensic implications of iOS jailbreaking. 2019 [cited 2023 November 22]. Available from: <https://blog.elcomsoft.com/2019/06/forensic-implications-of-ios-jailbreaking/#:~:text=Jailbreaking%20is%20used%20by%20the,with%20any%20other%20extraction%20methods>
20. Mahalik H, Tamma R, Bommisetty S. Practical mobile forensics. Packt Publishing Ltd.; 2016.



DSPACE

<https://dspace.org/>

Investigative opportunities from smart heating technology: a preliminary evaluation

Horsman, Graeme

2025-06

Taylor & Francis

<https://doi.org/10.1080/00450618.2024.2333360>

Horsman G. (2025) Investigative opportunities from smart heating technology: a preliminary evaluation. Australian Journal of Forensic Sciences, Volume 57, Issue 3, June 2025, pp. 312-321