Mikko Puustelli

KOTIAUTOMAATIOLAITTEIDEN FORENSINEN TUTKIMINEN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Puustelli, Mikko
Kotiautomaatiolaitteiden forensinen tutkiminen
Jyväskylä: Jyväskylän yliopisto, 2024, 57 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Takala, Arttu

Tämän tutkielman tarkoituksena oli tutkia kotiautomaatiohubien forensista tutkimista. Aihe on ajankohtainen, sillä kotiautomaatiolaitteiden käyttäminen lisääntyy globaalisti kovalla vauhdilla. Samaan aikaan markkinoille tulee jatkuvasti lisää laitevalmistajia ja tekniikoita. Digitaaliforensiikalla tarkoitetaan laitteiden tietosisällön tutkimista siten, että saadaan selville, mitä on tapahtunut. Kotiautomaatiolaitteiden kirjo on laaja. Niistä voidaan saada paljon tietoa esimerkiksi liike- tai ovisensoreiden perusteella. Vaikka kotiautomaatiolaitteiden tutkimiseen on kehitetty prosesseja, ei varsinaista yleistä analyysiteknologiaa ole saatavilla.

Tutkielmassa lähestyttiin laitteiden tutkimista Design Science Research -prosessin näkökulmasta. Kotiautomaatiolaitteiden tallentamaa tietoa pyrittiin tutkimaan hankkimalla laitteen pääkäyttäjän tunnukset ja selvittämällä laitteen toimintalogiikkaa. Mikäli tämä ei ollut mahdollista, iteroitiin vaihtoehtoisia keinoja saada kotiautomaatiohubista käyttötietoja selville.

Tutkimustulosten perusteella laitteiden tallentamien tietojen määrä vaihtelee suuresti. Joissakin tapauksissa laitteelta löytyy lokimerkintöjä pidemmältä ajalta, kun taas toisissa tapauksissa laitteesta saadaan ainoastaan muutamia ajankohtia selvitettyä.

Tutkielman myötä laitteiden tutkimisesta paljastui useita jatkotutkimusaiheita. Niiden toteuttaminen vaatisi erikoistyökaluja. Lisätutkimusten myötä olisi mahdollista selvittää tämän tutkielman ulkopuolelle jääneiden laitteiden tallentamaa tietoa.

Asiasanat: kotiautomaatio, forensiikka, digitaaliforensiikka, design science research

ABSTRACT

Puustelli, Mikko
Home automation forensics
Jyväskylä: University of Jyväskylä, 2024, 57 pp.
Cyber Security, Master's Thesis
Supervisor: Takala, Arttu

The purpose of this thesis was to investigate the forensic study of home automation hubs. The topic is topical as the use of home automation devices is increasing at a rapid pace globally. At the same time, more manufacturers and technologies are constantly entering the market. Digital forensics is the process of examining the data content of devices to find out what has happened. The range of home automation devices is broad. A lot of information can be obtained from them, for example from motion or door sensors. Although processes have been developed to analyze home automation devices, no general analysis technology is available.

This thesis approached the study of appliances from the perspective of the Design Science Research process. The aim was to study the data stored by home automation devices by obtaining the identity of the main user of the device and the operating logic of the device. If this was not possible, alternative means of extracting usage data from the home automation hub would be iterated.

The results of the study show that the amount of data stored by the devices varies widely. In some cases, the device provides log entries for a longer period, while in other cases only a few time points can be found.

The study revealed several areas for further research. Their implementation would require specialized tools. Further research would make it possible to investigate the data recorded by the devices not covered by this thesis.

Keywords: home automation, forensics, digital forensics, design science research

KUVAT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kotiautomaatiolaitteiden määrä on lisääntynyt viimeisen viiden vuoden aikana huimasti. Yleisesti kotiautomaatiosta puhuttaessa, monelle kuluttajalle tulevat ensimmäisenä mieleen Philipsin tai Ikean älyvalaisimet. Molemmat valmistajat tekevät myös muita laitteita, kuten kytkimiä tai liiketunnistimia. Kumpikaan näistä valmistajista ei kerro myyntilukujaan julkisesti, mutta Statistan tilastojen perusteella globaalisti 14,2 % kotitalouksista voidaan luokitella jollakin tasolla älykodeiksi vuonna 2022. Arvioiden mukaan vuoteen 2026 mennessä 25 % kotitalouksista sisältää joitakin älylaitteita. (Statista, 2023)

Samalla kun kotiautomaatiolaitteet helpottavat arjen rutiineja, jää niiden muistiin mahdollisesti tietoja siitä, milloin mitäkin tapahtumia on tehty. Automaatioon liittyvien rutiinien vuoksi jossakin pitää säilyttää tietoja siitä, milloin mitäkin on tapahtunut. Käyttäjä voi esimerkiksi haluta, että liiketunnistin kytkee tietyn valaisimen päälle viideksi minuutiksi päivällä täydellä teholla ja yöllä puolella teholla havaitsemansa liikkeen jälkeen. (Philips Hue, 2023a) Tämän vuoksi kotiautomaatiohubien pitää tallentaa tarkkoja aikaleimoja erilaisista tapahtumista. Nämä aikaleimat voivat tarjota myöhemmin tietoa siitä, mihin aikaan asunnossa on esimerkiksi liikuttu tai käytetty valoja.

Kuluttajakäyttöön suunnitellut kotiautomaatiolaitteet eivät tarjoa dokumentaatiota siitä, mitä kaikkea tietoa tallennetaan ja minne. Jotkut laitteet ja palvelut tallentavat kaiken pilveen, josta se on tietyissä tilanteissa saatavilla. Ainoastaan paikallisesti toimivat laitteet eivät tallenna tietoa pilveen. Niissä ei välttämättä ole ollenkaan tapahtumalokia.

Kotiautomaatiolaitteiden mahdollisesti tallentama tieto on saatava laitteista jotenkin ulos tutkittavaksi. Laitteiden tutkimista kutsutaan digitaaliforensiikaksi, jolla tarkoitetaan yksinkertaisesti selitettynä laitteiden digitaalisen tallennustilan ja digitaalisten ympäristöjen tutkimista, jotta saadaan selville, mitä on tapahtunut. (Kävrestad, 2018) Laitteiden tutkiminen digitaaliforensiikan periaatteiden mukaisesti jakaa prosessin muutamaan osaan. Osittamista on tehty usealla eri tavalla, mutta australialaisen Rodney McKemmishin (1999) mukaan pääkohdat prosessissa ovat laitteen tai datan tunnistaminen (1), digitaalisen todistusaineiston säilyttäminen muuttumattomana (2), tietosisällön

jäljentäminen ja analyysi (3) sekä raportointi (4). Kotiautomaatiolaitteet ovat vielä suhteellisen harvinaisia, joten niitä ei välttämättä osata tunnistaa oikein. Laitteelle tallennetun tiedon säilyminen muuttumattomana voi aiheuttaa ongelmia siinä vaiheessa, kun laite sammutetaan tai sitä käydään tutkimaan.

Tutkielmassa keskitytään edellä mainitun prosessin kohtiin 2 ja 3. Tutkielman tarkoituksena on vastata seuraaviin kysymyksiin:

1. Millä keinoin kotiautomaatiolaitteisto voidaan ottaa haltuun, jotta siinä olevat tiedot saadaan pysymään tallessa?
2. Mitä tietoja kotiautomaatiohubit tallentavat niihin liitettyjen laitteiden käytöstä?

Tutkielma seuraa Pfeffersin ym. artikkelissaan *A Design Science Research Methodology for Information Systems Research* (2007) kuvaamaa Design Science Research -prosessia sen eri vaiheita hieman yhdistellen. Kolmessa ensimmäisessä luvussa tunnistetaan ongelma ja määritellään tavoitteet. Tämä tapahtuu tekemällä katsaus erilaisiin myynnissä oleviin kotiautomaatiolaitteisiin ja niissä käytettäviin teknologioihin sekä avaamalla forensisen tutkimisen periaatteita ja mahdollisia yleisiä tutkimusmenetelmiä laitteiden tutkimiseen.

Luvuissa neljä suunnitellaan, luodaan ja demonstroidaan artefakti kehittämällä soveltuva tutkimusmenetelmä tutkittaville laitteille. Kahdessa viimeisessä luvussa arvioidaan artefaktin toiminta käymällä läpi tutkimustulokset ja miettimällä mahdollisia jatkotutkimusideoita. Viimeisessä luvussa tehdään yhteenveto ja johtopäätökset tutkimuksesta. Koko tutkielmaa voidaan pitää DSR-prosessin viimeisenä vaiheena, eli viestintänä ongelmasta ja siihen luodusta artefaktista.

Taustatutkimusta tehtiin hakemalla eri palveluista artikkeleita ja julkaisuja hakusanoilla ”iot”, ”internet of things” ja ”smart home” sekä ”forensic” ja ”forensics”. Suomeksi kirjoitettuja aiheeseen liittyviä artikkeleita ei taustatutkimusta tehtäessä löytynyt. Tässä tutkimuksessa hyödynnetyt artikkelit löytyvät IEEE Xprore - sekä Researchgate -palveluista. Kirjallisuuden perusteella tutkimukselle luotiin tavoitteet ja alustavat toimintamallit.

2 KOTIAUTOMAATIO

Automaatiolla tarkoitetaan itsestään tapahtuvaa toimintaa, jonka käyttäjä tai joku muu on ennalta määrittänyt. Kiinteistö-, koti- tai taloautomaatiossa automaatiolla tarkoitetaan varsinkin kyseiseen tilaan liittyvien laitteiden ohjaamista tai säätämistä. Kotiautomaation juuret ovat pitkällä taloautomaatiossa, jota on talotekniikassa käytetty jo 1960-luvulta lähtien. Seuraavalle vuosikymmenelle osunut energiakriisi lisäsi kiinnostusta talotekniikan automatisointiin, koska rakennusten lämmityskuluja haluttiin energian hinnan noustessa pienentää. Tämän jälkeen kiinteistöautomaatio lisääntyi ja kehittyi huimaa vauhtia. (Suomäki & Vepsäläinen, 2013)

Ensimmäinen kiinteistöautomaatioon tarkoitettu protokolla oli nimeltään X10. Se kehitettiin vuonna 1975 ja oli tarkoitettu valaistuksen ja sähkölaitteiden virransyötön ohjaamiseen. Se käytti kiinteistön normaaleja sähköjohtoja digitaalisen signaalin välittämiseen eri laitteiden välillä. Jokaisella laitteella oli oma osoite, ja yhdessä kiinteistössä saattoi olla maksimissaan 256 eri laitetta. (Zahariadis, 2003) Kotiautomaatio on kehittynyt vuosien varrella eteenpäin. Erityisesti langaton kotiautomaatio on yleistynyt. Tällä hetkellä myytävistä jälkiasennettavista kotiautomaatiolaitteista suurin osa on langattomia. Langattomissa kotiautomaatiolaitteissa on tällä hetkellä käytössä muutamia eri protokollia, jotka eivät ole keskenään yhteensopivia.

2.1 Protokollat

Kotiautomaatiossa käytettäviä langattomia protokollia on useita erilaisia. Tunnettujen WiFi- ja Bluetooth-protokollien lisäksi on olemassa muutamia protokollia, jotka on suunniteltu nimenomaan lyhyen matkan vähävirtaiseen kommunikaatioon. Nämä protokollat eivät ole keskenään yhteensopivia, joten niiden kaikkien käyttäminen samassa kokonaisuudessa vaatii suunnittelua. Langattomissa moderneissa kotiautomaatioprotokollissa käytetään usein mesh-verkkorakennetta. Mesh-verkolla tarkoitetaan laitteiden keskenään muodostamaa verkkoa,

jossa viestit voivat kulkea useamman laitteen kautta lähtöpisteestä kohteeseen. Tämän ansiosta kaikkien laitteiden ei tarvitse olla kotiautomaatiohubin kantoalueella, vaan ne voivat viestiä käyttäen hyväksi muita verkon laitteita.

2.1.1 ZigBee

Zigbee-protokollaa kehittävä ZigBee Alliance perustettiin vuonna 2002. Sen tehtävänä on kehittää avoimia standardeja IoT-laitteille, sertifioida ZigBee Alliancen kehittämiä standardeja käyttäviä laitteita ja toimia standardien äänitorvena globaalisti. ZigBee Alliancen kehittämillä protokollilla varustettuja piirejä on myyty laitevalmistajille yli miljardi kappaletta. (Connectivity Standards Alliance, 2023) Zigbee Alliance on sertifioinut jo yli 5000 erilaista laitetta. (ZigBee Alliance, 2023)

Zigbee-protokolla on kehittynyt monta sukupolvea ensimmäisestä julkaisustaan. Protokollan alemman tason kerroksena käytettävä IEEE 820.15.4 -standardi ratifioitiin vuonna 2004, ja seuraavana vuonna ZigBee Alliance julkaisi ensimmäisen ylemmän kerroksen spesifikaationsa nimeltään ZigBee 2004. Vuonna 2006 protokollan ylemmät tasot uudistettiin kokonaan, ja heti seuraavana vuonna julkistettiin ZigBee Pro. (Gislason, 2008) ZigBee Pro toimii verkkokerroksena käytännössä kaikissa tänä päivänä myytävissä ZigBee-protokollaan perustuvissa laitteissa. Verkkokerroksen päällä toimii sovelluskerros, joka nykyään on ZigBee 3.0. Ennen tätä versiota sovelluskerroksessa oli paljon erilaisia profiileja, jotka eivät suoraan olleet keskenään yhteensopivia. Esimerkkinä erilaisista profiileista on ZigBee Home Automation ja ZigBee Light Link. Profiilit on suunniteltu tiettyjen laitteiden väliseen kommunikointiin, eivätkä ne olleet yhteensopivia toistensa kanssa. ZigBee 3.0 yhdistää kaikki aiemmat profiilit yhden profiilin alle, jotta laitteiden yhteensopivuus olisi parempaa. Jokaista ZigBee-laitetta kehitettäessä, laitteen tarvittavat klusterit valitaan ZigBee Cluster Library:sta (ZCL). (NXP, 2016) Jotkut valmistajat päivittivät ohjelmallisesti ZigBee-hubinsa tukemaan ZigBee 3.0 -profiilia, vaikka laitteen julkaisuhetkellä sitä ei olisi ollut saatavilla. (Philips, 2023a)

TAULUKKO 1 ZigBeen verkkokerrokset

Sovelluskerros	ZigBee Cluster Library
Verkkokerros	ZigBee PRO
Fyysinen ja MAC-kerros	802.15.4

ZigBee tukee mesh-verkkotopologian lisäksi tähti- ja puuverkkotopologioita. ZigBee-verkossa on kolmenlaisia laitteita: koordinaattoreita, reitittimiä ja päätelaitteita. Koordinaattoreita voi verkossa olla tasan yksi. Sen tehtävänä on hoitaa verkon muodostamiseen liittyvät toimenpiteet, jotta muut laitteet voivat kommunikoida keskenään. Reititin toimii verkon solmukohtana ja välittää tietoa muiden laitteiden välillä. Se ei voi mennä virransäästötilaan, joten yleensä reitittimet ovat verkkovirralla toimivia laitteita. Ne voivat myös säilöä viestejä, jos viestin vastaanottaja ei ole saatavilla. Päätelaitteet ovat suurimman osan ajasta virransäästötilassa ja heräävät aina välillä kuuntelemaan komentoja. Päätelaitteita ovat

esimerkiksi lämpömittarit tai liiketunnistimet. ZigBee-laitteiden välinen tiedonsiirtonopeus on 2.4 GHz taajuudella maksimissaan 250kbps. (Wilmshurst, 2017) ZigBee-verkossa voi olla 65 540 laitetta, ja viestit voivat hyppiä 30 laitteen kautta. (Gislason, 2008)

2.1.2 Z-Wave

Z-Wave-protokollan historia ulottuu vuosituhannen vaihteeseen, jolloin muutamat Nokian ja Erikssonin entiset insinöörit perustivat tanskalainen Zensys-nimisen yhtiön. Yrityksen toiminta oli alussa pienimuotoista. Vasta vuonna vuonna 2005 Zensysin toiminta laajeni kunnolla, kun viisi suurta yritystä otti Z-Wave-protokollalla varustetut tuotteet portfolioihinsa. Samalla perustettiin Z-Wave Alliance, jonka tarkoituksena oli tuoda esille Z-Wave-protokollan etuja ja samalla markkinoida sitä sekä kuluttajille että laitevalmistajille. Z-Wave Alliancen perustamisvuonna protokollaa tukevia laitteita oli markkinoilla kuusi kappaletta. (Westervelt, 2012) Sigma Designs osti Zensysin vuonna 2009, jolloin Z-Wave-protokolla oli käytössä jo 250 eri tuotteessa (Erlich, 2008). Vuonna 2018 Silion Labs osti Z-Wave-liiketoiminnan Sigma Designsiltä. Tässä vaiheessa protokollaan perustuvia laitteita valmisti yli 700 laitevalmistajaa.
Yrityskaupan jälkeen kasvu jatkui, ja vuonna 2023 Z-Wave-protokollaa käyttäviä laitteita on jo yli 4 000 kappaletta (Z-Wave Alliance, 2023a)

Z-Wave-laitteet toimivat alle yhden gigahertsin taajuusalueella riippuen hieman maantieteellisestä alueesta. Euroopan Unionissa myytävissä laitteissa taajuus on joko 868.4 MHz tai 869.85 MHz. Protokollan toteutus laitteissa tapahtuu valmistajan myymällä järjestelmäpiirillä tai moduulilla. Valmistajan myymän komponentin lisäksi kaikki laitteet pitää sertifioida sekä Silicon Labsilla että Z-Wave Alliancella, jotta ne ovat varmasti teknisesti toimivia sekä yhteensopivia muiden laitteiden kanssa. (Z-Wave Alliance, 2023b)

Z-Wave on mesh-tyyppinen verkko, joka kykenee 100kbps nopeuksiin laitteiden välillä. Viestiliikenne kaikkien laitteiden välillä on nykyisin salattu AES-salauksella. (Z-Wave Alliance, 2020a) Z-Wave-laitteita voi olla yhdessä kotiautomaatioverkossa 232 kappaletta. Mesh-verkossa viesti voi tehdä maksimissaan neljä hyppäystä laitteelta toiselle, mikä tarkoittaa yhteensä maksimissaan noin neljänsadan metrin välimatkaa. Z-Waven uusimmassa Long Range -teknologiassa (LR) välimatka voi olla jopa 1,6 kilometriä, mutta verkko on topologialtaan tähti. (Z-Wave Alliance, 2023c)

2.1.3 Thread

Thread on yksi uusimmista kotiautomaatioprotokollista. Sitä kehittävä Thread Group perustettiin vuonna 2014, ja samana vuonna julkaistiin protokollan versio 1.0. Protokollan tämänhetkinen uusin julkinen versio 1.3 julkaistiin vuonna 2022. Thread-protokollan kehitys aloitettiin, koska haluttiin tuoda turvallinen, vähävirtainen, kehityskelpoinen ip-pohjainen mesh-verkkoprotokolla IoT-laitteille.

Thread-verkko toimii samalla IEEE 820.15.4 matalan tason protokollalla kuin ZigBee. Verkkokerroksena on IPv6 yhdessä 6LoWPAN:n kanssa, joka on

akronyymi termistä *IPv6 over Low-Power Wireless Personal Area Network*. Tämä kerros on monissa laitteissa toteutettu avoimeen lähdekoodiin perustuvalla OpenThread-kokonaisuudella, esimerkkinä Googlen Nest- tai Amazonin Eero-tuotteet. Thread ei määritä sovelluskerrosta verkkoliikenteelle ollenkaan, ja se sallii useamman sovellusprotokollan toiminnan samassa verkossa samaan aikaan. Sovelluskerroksessa käytetään yleisimmin tällä hetkellä Matter-standardia. Thread-verkossa voi olla kahdenlaisia laitteita: reitittimiä ja päätelaitteita. Päätelaitteet eivät reititä viestejä eteenpäin, ja ne kommunikoivat ainoastaan reitittimien kanssa.

Thread-protokolla tukee yhdessä verkossa 32 samanaikaista reititintä, joihin jokaiseen voi liittää 511 päätelaitetta. Thread-verkossa jokainen laite kytkeytyy ensin päätelaitteena mutta nostaa itsensä reitittimeksi tarpeen mukaan. Jokaiseen verkkoon konfiguroituu automaattisesti yhdestä reitittimestä leader-reititin, jonka vikaantuessa toinen reititin ottaa roolin automaattisesti hoitaakseen. Thread-verkon ja muun verkon rajalla toimii border-reititin, jonka tehtävänä on toimia reitittimenä esimerkiksi yrityksen lähiverkkoon tai internetiin. Yhdessä Thread-verkossa voi olla useita border-reitittimiä samanaikaisesti käytössä, jolloin yhden vikaantuminen ei aiheuta ongelmaa. (Håkansson & Loska, 2020)

2.2 Kotiautomaatiohubit

Kotiautomaatiolaitteiden ohjauskeskuksia kutsutaan usein kotiautomaatiohubeiksi, kotiautomaatio-ohjaimiksi tai pelkästään hubeiksi. Kotiautomaatiolaitteet ottavat yhteyttä kotiautomaatiohubiin, jota voidaan ohjata esimerkiksi matkapuhelimella, tabletilla, ääniohjauksella tai muilla laitteilla. (Kim;Park;Lee;& Kim, 2020) Kotiautomaatiohubit voidaan jakaa useilla eri tavoilla niiden ominaisuuksien perusteella. Jotkut laitteet toimivat pelkästään lähiverkossa, kun taas toiset vaativat jatkuvan internet-yhteyden toimiakseen. Lisäksi on olemassa laitteita, jotka toimivat paikallisesti lähiverkossa mutta mahdollistavat etäohjauksen internetin välityksellä esimerkiksi mobiililaitteesta. Lähes kaikkia kotiautomaatiohubeja voidaan käyttää rajapinnan kautta, jolloin niitä voidaan ohjata toisella palvelulla tai laitteella. Rajapinnat eivät ole standardoituja, joten niiden yhteensopivuus eri laitteiden välillä vaihtelee. Seuraavissa luvuissa käydään läpi yleisimpiä kotiautomaatiohubeja ja niiden ominaisuuksia.

2.2.1 Philips Hue

Philips julkaisi ensimmäisen Hue-järjestelmän laitteet lokakuussa 2012 Applen kaupoissa. Kolmen vuoden kuluttua julkaistiin HomeKit-yhteensopiva versio, joka on vieläkin myynnissä. Philipsin Hue-lamput toimivat vuoteen 2019 asti pelkästään ZigBee-protokollan avulla, kunnes Philips alkoi valmistaa myös Bluetooth-versioita lampuistaan. Philips kutsuu kotiautomaatiohubiaan nimellä Hue Bridge. Se tukee sekä ZigBee- että Bluetooth-protokollia, joten kaikki Hue-lamput toimivat myös Hue Bridgen kanssa. Bluetooth-versioitakin voi ohjata

pelkällä matkapuhelimella. Philips tarjoaa mahdollisuuden hallita valoja myös käyttäjän oman lähiverkon ulkopuolelta käsin Philipsin omalla sovelluksella. (Philips, 2023b)

2.2.2 Lidl Smart Home

Lidl julkaisi oman kotiautomaatiolaitteistosarjan loppuvuodesta 2020 nimeltään Lidl Smart Home. Sarjassa on hubin lisäksi polttimoita, erilaisia valaisimia, kaukosäädin sekä liikkeentunnistin. Laitteet tukevat Zigbee 3.0 -versiota, joten ne ovat erittäin hyvin yhteensopivia muiden Zigbee-laitteiden kanssa. (Kemppi, 2020)

Lidl Smart Home -tuotesarjan tuotemerkkejä ovat LivarnoLUX sekä SilverCrest. Ne ovat Kiinalaisen IoT-valmistaja Tuyan alustoille valmistettuja laitteita. (Tuya, 2023a) Tuya mahdollistaa oman kotiautomaatioratkaisun kehittämien myyntiin ilman omaa varsinaista kehitystä. Yrityksen tuotteita myydään useilla eri tuotemerkeillä yli 200 eri maassa. Tuyan portaalissa on yli 800 000 kehittäjää 7 600 yrityksessä ja heidän laitteitaan myydään 120 000 kaupassa. (Tuya, 2023b)

2.2.3 Ikea Trådfri ja Dirigera

Ikea julkaisi oman ZigBee-protokollaa käyttävän Trådfri-kotiautomaatiotuotesarjansa neljässä Euroopan maassa lokakuussa 2016. Loppuihin Euroopan maihin sekä Pohjois-Amerikkaan sarja tuli myyntiin huhtikuussa 2017. (Ikea, 2017) Trådfri-valikoima koostuu erilaisista lampuista ja valaisimista, kauko-ohjattavasta pistorasiasta, kytkimistä, signaalinvahvistimesta, liiketunnistimesta sekä hubista, jota Ikea kutsuu termillä Gateway. Ikealla on myös muita älylaitteita, jotka ovat yhteensopivia hubin kanssa. Vanhemmat Trådfri-tuotteet käyttävät ZigBee-protokollan ZigBee Light Link -profiilia (ZLL), mutta uudemmat, hubi mukaan luettuna, ovat Zigbee 3.0 -standardin mukaisia.

Ikean kotiautomaatiolaitteet eivät tarjoa mahdollisuutta ohjata laitteita kodin ulkopuolella ilman kolmannen osapuolen ratkaisuja. Trådfri Gateway voidaan liittää yhteen Amazon Alexan, Google Assistantin tai Apple HomeKitin kanssa, minkä jälkeen kaikkia samaiseen Gateway-laitteeseen liitettyjä laitteita voidaan ohjata edellä mainittujen palveluiden kautta. Tämä mahdollistaa laitteiden ohjauksen myös kodin ulkopuolelta käsin. (Ikea, 2023a)

Ikean tarjoamissa dokumentaatioissa ei mainita, keskusteleeko Gateway suoraan kolmannen osapuolen palvelimien kanssa vai kiertääkö data Ikean palvelinten kautta. Dokumentaatiossa mainitaan, että kolmansille osapuolille menee tieto polttimon tyypistä, nimestä ja tilasta.

Vuonna 2022 Ikea julkaisi uuden version hubistaan nimeltään Dirigera Hub. Laite tarjoaa Trådfrin lisäksi enemmän kapasiteettia tallennustilan, käyttömuistin sekä laskentatehon suhteen sekä mahdollisuuden kommunikoida hubin kanssa myös lähiverkon ulkopuolelta ilman kolmansia osapuolia.

2.2.4 Amazon Alexa

Amazon Alexa on ääniohjattu virtuaalinen avustaja, joka on käytettävissä Amazonin Echo-sarjan älykaiuttimissa ja joissakin kolmannen osapuolen tuotteissa. Vaikka laite on pääasiassa tarkoitettu virtuaaliseksi avustajaksi, on sen uusimpiin versioihin lisätty tuki ZigBee-protokollalle kotiautomaatiolaitteiden suoraa ohjausta varten. Laite tukee Wi-Fi-yhteyden lisäksi myös Bluetooth-yhteyttä. (Prospero, 2023) Alexa tukee myös useita erilaisia integraatioita eri laitevalmistajien kotiautomaatiohubeihin, kuten edellisessä kappaleessa mainittuihin Ikean hubeihin. Neljännen sukupolven Amazon Echo -laitteessa on Nordic Semiconductorin nRF52832-järjestelmäpiiri sekä 8 GB:n kokoinen NAND-tyyppinen flash-muisti. (Teschler, 2022)

2.2.5 Samsung SmartThings

SmartThingsin tarina alkoi vuonna 2012 samannimisen kasvuyrityksen kehittämänä tuotteena. Laite sai suurta suosiota muun muassa onnistuneen joukkorahoituskampanjan myötä, ja pian Samsung osti SmartThingsin vuonna 2014. (Tilley, 2013)

SmartThings-kotiautomaatiohubista on julkaistu tällä hetkellä kolmas versio, joka tukee langattomista protokollista Z-Wavea, Zigbeetä ja Wi-Fiä. SmartThings-tuoteperheeseen kuuluu myös erilaisia sensoreita, painikkeita, kameroita ja pistorasioita. SmartThings-hubiin voi liittää eri valmistajien Z-Wave-, ZigBee- tai Wi-Fi-tuotteita ja useiden valmistajien laitteita tai palveluita julkisten rajapintojen kautta. Samsungin sivuston perusteella SmartThings-hubeja on tulossa myyntiin muiltakin valmistajilta. (SmartThings, 2023a)

2.2.6 Apple HomeKit ja Google Home

Apple HomeKit ei varsinaisesti ole kotiautomaatiohubi vaan Applen laitteissa toimiva sovellusympäristö. Sen avulla voi ohjata yhteensopivia Bluetooth- tai Wi-Fi-laitteita suoraan samassa tilassa olevien Applen laitteiden kanssa. HomeKit mahdollistaa iPadin, Apple TV:n, HomePodin tai HomePod minin käytön kotiautomaatiohubina, jolloin HomeKitiin yhdistettyjä laitteita voi ohjata kodin ulkopuolelta. (Apple, 2020) Apple HomeKit julkaistiin vuonna 2014 IOS 8.0:n yhteydessä. (Ochs, 2014) Applen HomeKit -järjestelmää voi ohjata Applen Siri -virtuaaliavustajan avulla samalla tavalla kuin Amazonin Alexaa. Applen HomeKitiin voi liittää useiden valmistajien laitteita tai palveluita julkisten rajapintojen kautta.

Googlen kotiautomaatio koostuu Google Home -älykaiuttimista ja älynäytöistä, Google Home -sovelluksesta ja Google Assistant -virtuaaliavustajasta. Toimintaperiaatteeltaan Googlen ratkaisu vastaa Applen palveluita sillä poikkeuksella, että jotkut laitteet vaativat Googlen Home -älykaiuttimen tai Google Nest Hub -älynäytön ohjatakseen paikallisia laitteita. Osa laitteista toimii pelkällä Google Assistant -sovelluksella matkapuhelimessa, jolloin erillisiä älykaiuttimia ei tarvita. Googlen Nest-tuoteperhe käyttää myös Thread-protokollaa muun

muassa termostaateissaan tai lämpötilasensoreissaan sekä uusimmissa älykaiuttimissaan tai -näytöissään. (Google, 2023) Myös Googlen ympäristöön voi liittää useiden eri valmistajien laitteita tai palveluita julkisten rajapintojen kautta.

2.3 Päätelaitteet

Kotiautomaatioon liitettäviä erilaisia päätelaitteita on paljon. Samsung SmartThings listaa sivuillaan omia järjestelmiään tukevat laitteet kategorioittain. Laitekategorioita ovat SmartThings-palveluiden lisäksi ääniavustajat, valvontakamerat, ovikellot, kytkimet, himmentimet, tuulettimet, ilmanvaihtoluukut, kodinkoneet, valaisimet, pistorasiat, erilaiset sensorit, älylukot, palovaroittimet, kaiuttimet, termostaatit, venttiilit ja verhot. Useissa kategorioissa on useita valmistajia, joilla jokaisella on mahdollisesti monia eri tuotteita. (SmartThings, 2023b)

Vaikka kotiautomaatiohubit tukevat mahdollisesti useita eri protokollia, niihin kytkettävät laitteet tukevat lähtökohtaisesti yhtä protokollaa. Edellä mainituista kotiautomaatiohubivalmistajista Apple on ainoa, joka ei valmista hubiin liitettäviä laitteita.

Päätelaitteiden yhteensopivuus hubien kanssa vaatii tuen hubien valmistajilta. Hubit voidaan tässä mielessä jakaa kahteen ryhmään: toiset tukevat ainoastaan itse valmistamiaan päätelaitteita, ja toisiin käyvät useiden valmistajien päätelaitteet. Hyvänä esimerkkinä ensimmäisistä on Ikean Trådfri (IKEA, 2023b) ja jälkimmäisestä Samsung SmartThings. Kotiautomaatiolaitteiston päätelaitteiden dokumentaatiossa ei ole syvällisiä tietoja laitteiden teknisistä ratkaisuista, vaan niissä keskitytään päätelaitteiden tarjoamiin ominaisuuksiin.

3 FORENSINEN TUTKIMINEN

Forensinen tutkimisen pohjana on forensiikka tai forensiset tieteet. Forensinen tiede sisältää useita tutkimusaloja. Kimmo Himberg määrittää forensisen tieteen kirjassaan *Tekninen Rikostutkinta – Johdatus forensiseen tieteeseen* seuraavasti.

> Forensinen tiede: teknisten ja luonnontieteiden soveltaminen rikostorjuntaan, erityisesti rikosten esitutkinnan yhteydessä tehtävät laboratoriotutkimukset ja niiden tiedeperusta; myös oikeuslääketiedettä sivuavat oikeuskemia ja oikeustoksikologia luetaan siihen sisältyviksi (Himberg, 2002, s. 11)

Forensinen tiede pyrkii vastaamaan kysymyksiin, joita kullakin tutkimusalalla voidaan kysyä. Esimerkiksi sormenjälkiä tutkittaessa voidaan verrata rikospaikalta otettua sormenjälkeä epäillyltä otettuun vertailunäytteeseen tai käytettävissä rekistereissä oleviin sormenjälkiin. Vastaavasti aseita tutkittaessa voidaan vastata kysymykseen, voiko takavarikoidulla aseella ampua normaalisti. (Himberg, 2002) Tutkimusaloja on tullut koko ajan lisää eri alojen kehittyessä eteenpäin. Yhtenä esimerkkinä on tietoteknisten laitteiden lisääntyessä digitaaliforensiikan tutkimusala.

Digitaaliforensiikka on samalla tavalla yksi forensisen tieteen tutkimusala. Sen alaisuuteen kuuluvat tietotekniset laitteet sekä niiden sisältämä data. Digitaaliforensiikka keskittyy tiedon tunnistamiseen, prosessoimiseen, analysointiin sekä raportointiin. Analysoitava data voi tulla esimerkiksi tietokoneista, matkapuhelimista, pilvipalveluista, droneista tai mistä tahansa dataa käsittelevistä tai tallentavista ratkaisuista. (Interpol, 2024)

Kotiautomaatiojärjestelmien digitaaliforensiikassa ennakkosuunnittelu on tärkeässä roolissa, koska laitteistojen, järjestelmien ja palvelujen tarjonta on laajaa. Laitteistojen käyttöjärjestelmissä tai tiedon tallentamisessa ei ole yleisiä tunnettuja standardeja käytössä, joten tutkimiseen käytettävät menetelmät ja keinot ovat laite- tai valmistajakohtaisia. Jotta kohteessa olevien laitteiden haltuunotto voidaan toteuttaa siten, että tarvittava data säilyy muuttumattomana, laitteiden merkit ja mallit pitäisi saada selville etukäteen. Riskinä on, että tutkija menee kohteeseen sisälle tietämättä kotiautomaatiosta ja laukaisee liiketunnistimen,

mikä käynnistää jonkin prosessin. Tämä saattaa esimerkiksi aiheuttaa hälytyksen tai muuttaa laitteisiin tallentunutta dataa.

Goudbeek, Choo ja Le-Khac (2018) esittelevät *A Forensic Investigation Framework for Smart Home Environment* -artikkelissaan forensisen mallin kotiautomaatioympäristön tutkimiseen. Heidän mallissaan prosessi on jaettu seitsemään osaan, joista käytetään jokaiseen tapaukseen soveltuvia osia. Vaiheessa 1 (valmistautuminen) varmistetaan tutkijoiden osaaminen kotiautomaatiosta yleisellä tasolla. Tämä tarkoittaa muun muassa tietoisuutta protokollista ja tuntemusta yleisimmistä laitteista. Myös kotiautomaatiolaitteiden havaitsemiseen ja datan talteenottoon tarvittavat tekniikat ja laitteet pitää valmistella. Vaihe 2 (kotiautomaation etsiminen kohteesta) käsittää paikan päällä tapahtuvan laitteiden dokumentoinnin ja talteenoton. Vaiheessa 3 (kotiautomaation haltuunotto sellaisenaan) selvitetään, voisiko palveluntarjoajalta saada jotakin lokitietoa sekä irrotetaan laite julkisesta verkosta, jotta sitä ei pystytä etänä esimerkiksi tyhjentämään. Vaihe 4 (kotiautomaatiojärjestelmän kartoittaminen) sisältää laitteiden fyysisen etsimisen lisäksi verkkoskannausta ja dokumentointia. Vaihe 5 (tietoturvan selvitys) kuvaa keinoja, joilla pyritään selvittämään laitteiston mahdolliset käyttäjät ja heidän käyttöoikeutensa. Tässä vaiheessa myös selvitetään laitteiston ohjelmistoversio mahdollisten hyödynnettävien tietoturva-aukkojen varalta. Vaiheessa 6 (tietosisällön paikannus ja jäljennys) aloitetaan tietosisällön jäljentäminen laitteistoista. Tämä voi tarkoittaa esimerkiksi massamuistien jäljentämistä, mikrokontrollerien muistien lukemista laitteiden ollessa päällä (engl. *live acquisition*) tai etäohjaukseen käytettyjen laitteiden takavarikointia myöhempää analysointia varten. Vaihe 7 (datan prosessointi ja analysointi) käsittää talteen otetun datan purkamisen ja analysoinnin. (Goudbeek;Choo;& Le-Khac, 2018)

Snehal Sathwara ja Nitul Dutta (2018) käsittelivät samaa aihetta artikkelissaan *IoT Forensic A Digital investigation framework for IoT systems*. Artikkelissa käsitellään IoT-laitteiden forensista tutkimista niihin liittyvissä rikoksissa, kuten IoT-laiteiston hakkeroinnissa tai rikoksissa, joissa kyseisiä laitteita käytetään. Forensinen tutkinta jaetaan artikkelissa neljään osaan: laitteiden tunnistaminen, tietosisällön jäljentäminen, analysointi ja analysoidun tiedon koostaminen esitettävään muotoon. Laitteiden etsimisessä ja tunnistamisessa suurimman haasteen luo laitteiden pieni koko ja niissä käytetyn tekniikan vieraus. Kunnollisia työkaluja kotiautomaatiolaitteiden etsimiselle ei ole, joten niiden löytäminen on hankalaa, varsinkin laitteiden ollessa lepotilassa. Laitteiden tietosisällön jäljentämisessä suuri haaste ovat heterogeeniset ohjelmisto- ja laitteistoratkaisut sekä eri laitteiden tallennus- ja prosessointiresurssien vaihtelevuus. Monet laitteet tyhjentävät lokinsa sammuessaan, joten tiedon saaminen niistä on lähes mahdotonta. Analyysivaiheessa ongelmia aiheuttaa laitteiden tuottaman turhan tiedon suuri määrä. Sensoreihin tai muihin päätelaitteisiin ei välttämättä tallenneta mitään lokeja tai metadataa, jolloin niiden hyödyntäminen tutkimuksissa on mahdotonta. Analysoidun tiedon tuottaminen esitettävään muotoon ei tuota hankaluuksia, mikäli kaikki edelliset vaiheet ovat onnistuneet. (Sathwara;Dutta;& Pricop, 2018)

Keshav Kaushikin, Akashdeep Bhardwajin ja Susheela Dahiyan (2023) julkaisema artikkeli *Smart Home IoT Forensics: Current Status, Challenges, and Future Directions* käy läpi myös IoT-forensiikan ongelmia. Päällimmäisiksi ongelmiksi he nostavat tiedon tallentamiseen käytettävien standardien puuttumisen, tiedon korruptoitumisen laitteissa, kotiautomaatiohubien käyttämät datan salaukset, yksityisyyttä suojaavat lait, IoT-laitteiden heterogeenisuus ja koulutuksen puute IoT-laitteiden tutkinnassa. Artikkelin mukaan IoT-laitteiden lisääntyminen johtaa uusien tutkintalaitteiden ja -ohjelmistojen kehittymiseen, mutta IoT-laitteiden tutkinta tulee pysymään monimutkaisena.

Julkaisuja erilaisten IoT-laitteiden tutkimisesta löytyy verkosta jonkin verran. Monessa tutkimuksessa lähestytään kotiautomaatio- ja IoT-laitteiden tutkimista useasta eri näkökulmasta. Yksi esimerkki on tutkijoiden Shinelle Hutchinson, Yung Han Yoon, Neesha Shantaram ja Umit Karabiyik (2020) julkaisema Internet of Things Forensics in Smart Homes: Design, Implementation and Analysis of Smart Home Laboratory. Julkaisussa tutkitaan puhelinsovellusten sisältämää dataa, yksityisyydensuojaa, kyberturvallisuutta, tietojen jakamista eri laitteiden välillä sekä parhaita tapoja kotiautomaatiolaitteiden tallentaman tiedon hankintaan ja analysointiin. Tutkimuksessa oli 11 erilaista laitetta tutkittavana Wi-Fi-tukiasemasta aktiivisuusrannekkeeseen. Lähestymistapana oli tutkia tutkittavien laitteiden puhelinsovellusten tallentamia tietoja soveltuvilla forensiikkasovelluksilla. Tutkimuksessa todettiin myös monien verkkolaitteiden sisältävän haavoittuvuuksia, jotka lähiverkossa ollessaan tarjoavat hyökkääjille potentiaalisen reitin.

Käytännönläheisemmän tavan IoT-laitteen tutkimiseen tarjoaa Akshay Awasthin, Huw O.L. Readin, Konstantinos Xynosin ja Iain Sutherlandin julkaisema Welcome pwn: Almond smart home hub forensics (2018). Siinä tutkitaan Almond+ -kotiautomaatiohubia, jossa on myös reititin kodin internet-yhteyden jakamiseksi päätelaitteille. Laitteessa on oletuksena päällä SSH-palvelin, johon laitteen käyttäjällä on oikeudet kirjautua. Tämän avulla laitteesta voidaan ottaa jäljennökset ja tutkia niiden sisältöä. Laitteelta löytyi puolet 512 MB:n käyttömuistista käyttävä tmpfs-partitio, jossa oli valtava määrä lokitietoja. Lokeista löytyi muun muassa kotiautomaatiohubin kosketusnäytön käyttöloki, hubiin liitettyjen laitteiden käyttöönottoon liittyvä loki sekä pilveen siirrettävän ja vastaanotettavan datan siirtoloki. Mobiililaitteiden kotiautomaatiohubin käyttöön tarkoitetun sovelluksen käyttötietoja ei sen sijaan lokitietoihin tutkimuksen mukaan tallentunut. Tutkimuksessa käytiin läpi myös mobiilisovelluksen sekä pilvipalvelun tallentamat tiedot sekä tehtiin lopulta tutkijoille suositeltava järjestys tutkia Almond+-järjestelmä. Julkaisun johtopäätöksissä mainittiin, että siinä keskityttiin juurikin yhden laitteen tutkimiseen ja että yleisemmän toimintamallin kehittämiseksi pitäisi tutkia useita vastaavanlaisia laitteita.

Digital Investigation 28 -lehdessä julkaistu artikkeli IoT forensic challenges and opportunities for digital traces (Servida & Casey, 2019) käsittelee neljän eri

valmistajan kotiautomaatiolaitteiden tutkimista. Siinä kuvaillaan tuntemattomien IoT-laitteiden tutkimisprosessia eri lähestymiskulmista eri vaiheissa. Laitteiden fyysistä analyysia tarvitaan esimerkiksi rikostutkinnassa, koska esimerkiksi IoT-laitteen verkkoliikenteen tallentamisesta ole enää mitään hyötyä rikoksen tapahduttua. Fyysisen tutkimisen metodeiksi artikkelissa mainitaan UART- ja JTAG-väylät sekä piirin irroittaminen ja sen lukeminen erillislaitteistolla (chip-off). Kolmelle laitteelle neljästä saatiin UART-väylän kautta eri keinoin pääsy tiedostojärjestelmään, mitä kautta laitteiden sisältämiä tietoja pystyttiin tutkimaan. Tutkimus tuo esille ongelman myös laitteiden haltuunotossa: jotkut laitteet tallentavat laajasti tietoa ainoastaan viimeisimmästä tapahtumasta. Tämän vuoksi laitetta haltuun ottaessa voi tahattomasti hävittää merkityksellisen edellisen tapahtuman tiedot.

3.1 Kotiautomaatiolaitteiden paikantaminen

Kotiautomaatiolaitteiden etsiminen kohteesta voi joissakin tapauksissa olla haastavaa, vaikkakin suurin osa laitteista löytyy todennäköisesti niille tarkoitetuista paikoista. Tuulettimiin, venttiileihin ja verhoihin liittyvät kotiautomaatiolaitteet löytyvät todennäköisesti niiden käyttöpaikoista, ellei niitä käytetä johonkin muuhun tarkoitukseen. Ovisensoreiden paikka on ovissa, josta ne ovat helposti nähtävissä. Markkinoilla tosin on malleja, jotka upotetaan oven runkoon ja karmiin, minkä takia niitä ei välttämättä havaitse. Liiketunnistimet on asennettu näkyville paikoille, sillä niiden tarkoitus on nimenomaan havaita liikettä. Useissa malleissa liikkeen havaitseminen sytyttää pienen merkkivalon, joskin joistakin malleista sen saa kytkettyä pois päältä.

Mikäli kaikkia laitteita ei löydetä, voidaan käyttää apuna esimerkiksi signaalien haistelijaa (engl. *sniffer*). Sen avulla voidaan kuunnella ZigBee- ja Thread-liikennettä, koska ne käyttävät samaa 802.15.4-standardia. (Nordic Semiconductor, 2023) Z-Wave-laitteille on mahdollista rakentaa oma haistelija käyttäen normaaleja Z-Wave-laitteita soveltuvan ohjelmiston kanssa.

3.2 Tietosisällön jäljentäminen ja analysointi

Laitteiden tietosisältöön käsiksi pääseminen voidaan toteuttaa usealla eri tavalla. Karkeasti jaotellen laitteeseen voidaan ottaa jollakin tavalla yhteys ja tutkia sen sisältöä tai vaihtoehtoisesti irrottaa muistipiiri ja lukea sen sisältö toisella laitteella. Mikäli laitteen tietosisältö jäljennetään käyttäen laitetta itseään, pitää analyysissä myöhemmin huomioida jäljentämisen aiheuttamat muutokset varsinaiseen tietosisältöön.

Muistipiirien lukeminen vaatii yleensä niiden irrottamista piirilevyistä. Tätä operaatiota kutsutaan yleensä englanninkielisellä termillä *chip-off*, joka suoraan suomennettuna tarkoittaa piirin irrotusta. BGA-piirin irrotus tapahtuu

lämmittämällä pelkkää piirilevyä esimerkiksi infrapunauunissa tai irrotettavaa piiriä lämpöpuhaltimella, kunnes piirin kiinnittämiseen käytetty tina sulaa. Piiri nostetaan pois piirilevyltä, ja siihen jäänyt tina puhdistetaan tinaimurilla tai imusukalla. Tämän jälkeen muistipiirin sisältö luetaan soveltuvalla laitteistolla ja analysoidaan sopivalla ohjelmistolla. (Mikhaylov & Skulkin, 2023) SPI-muistipiirejä ei yleensä tarvitse irrottaa piirilevyltä, vaan ne voidaan joissakin tapauksissa lukea suoraan käyttäen siihen soveltuvia työkaluja kytkemällä lukijan vaatimat johdot suoraan piirin jalkaan. (Graceful, 2023)

RAM-muistin lukeminen laitteen ollessa käynnissä vaatii pääsyn laitteen käyttöjärjestelmään. Laitevalmistajat eivät tarjoa loppukäyttäjille pääsyä kotiautomaatiolaitteisiin, mutta monesta kotiautomaatiohubista löytyy jonkinlainen virheenkorjausportti (engl. *debug*). Tästä esimerkkinä toimii Philipsin Hue Gateway, jonka piirilevyltä löytyy sarjaportti virheenkorjausta varten. Konsoliin pääsee sarjaportin kautta käsiksi aiheuttamalla virheen muistipiirissä oikosulun avulla. (Seger, 2016)

Flash-muistin tai RAM-muistin jäljentämisen jälkeen niiden analysointi vaatii erityisosaamista ja -ohjelmistoja. Ennalta tuntemattomien kotiautomaatiolaitteistojen tallennustilan tutkiminen voidaan aloittaa laiteohjelmiston (engl. *firmware*) tutkimisella. Laiteohjelmisto voidaan takaisinmallintaa (engl. *reverse engineer)* siihen tarkoitettujen sovellusten avulla. (Attify, 2017) Takaisinmallinnuksen avulla voidaan saada selville, mitä laite tallentaa tallennustilaan tai käyttömuistiin.

4 TUTKIMUSMENETELMÄ

Tutkimuksessa käytetään tutkimusmenetelmänä Design Science Research -menetelmää. Design Science Research (DSR) on tutkimusmenetelmä, joka pyrkii vastaamaan tosielämän ongelmiin kehittämällä artefakteja, joiden avulla voidaan tuottaa uutta tieteellistä näyttöä. DSR:n perusperiaatteena onkin, että tieto ja ymmärrys ongelmasta sekä sen ratkaisusta saadaan rakentamalla ja käyttämällä artefaktia. (Hevner & Chatterjee, 2010)

DSR:n mainitsemia artefakteja voivat olla esimerkiksi konstruktiot, mallit tai menetelmät. Myös sosiaaliset innovaatiot sekä uudet ominaisuudet teknisiin, sosiaalisiin tai tiedollisiin resursseihin voidaan lukea DSR:n artefakteiksi. Yksinkertaistettuna artefakti tarjoaa ratkaisun tutkimusongelmaan. (Peffers;Marcus;& Tuunanen, 2007)

DSR:n prosessi koostuu muutamasta vaiheesta, jotka vaihtelevat hieman asiasta julkaistujen artikkelien välillä. Peffers ym. (2007) ovat käyneet artikkelissaan läpi useampia julkaisuja ja koostaneet niissä esitetyt vaiheet taulukon 2 mukaisesti. Taulukossa avataan prosessin vaiheita lyhyesti.

TAULUKKO 2 DSR-prosessin vaiheet

Vaihe	**Selitys**
1. Ongelman tunnistaminen ja motivaatio	Määritellään ongelma ja sen ratkaisun arvo. On hyvä tietää, kuinka monimutkainen ongelma on ja miten vaikuttava ratkaisu voi olla.
2. Ratkaisun tavoitteiden määritys	Selvitetään mikä on mahdollista ja mikä erittäin hankalaa tai mahdotonta. Artefakti voi tuoda ratkaisun ongelmiin, joita ei vielä ole ratkaistu.
3. Artefaktin suunnittelu ja toteutus	Artefakti suunnitellaan ja kehitetään.
4. Artefaktin demonstraatio	Artefaktin toimintaa testataan yhteen tai useampaan ongelmaan.
5. Artefaktin toiminnan arviointi	Arvioidaan, tukeeko artefakti ongelman ratkaisua.

6. Kommunikaatio	Viestitään ongelmasta ja luodusta artefaktista kohderyhmille.

DSR-prosessi etenee taulukon mukaisessa järjestyksessä, mutta se voi sisältää iteraatioita. Esimerkiksi vaiheesta viisi voidaan palata takaisin vaiheeseen kolme, mikäli huomataan, että artefakti ei ratkaise haluttua ongelmaa tehokkaasti tai täsmällisesti. (Peffers;Marcus;& Tuunanen, 2007)

Tutkielmassa DSR-prosessin tavoitteena on luoda artefakti, joka on toimintamalli tutkimuksessa käsiteltävien neljän kotiautomaatiohubin tutkimiselle. Artefaktin avulla pyritään vastaamaan tutkielman kahteen tutkimuskysymykseen. Vaikka valmiilla artefaktilla voidaan tutkia tässä tutkielmassa käsiteltäviä kotiautomaatiohubeja, sen ei voida taustatutkimuksen perusteella olettaa toimivan suoraan muiden valmistajien laitteissa. Tutkimuksessa käytettäviä tekniikoita tai ratkaisuja voidaan hyödyntää soveltaen mahdollisesti muissakin laitteistoissa.

Tutkielmassa on sovellettuna kaikki DSR-prosessin vaiheet mukana. Ongelman tunnistaminen ja motivaatio (vaihe 1) on esitelty luvuissa kaksi ja kolme. Ratkaisun tavoitteiden määritys (vaihe 2) on tehty jo johdannossa tutkimuskysymyksissä, ja sitä tarkennetaan hieman seuraavassa luvussa. Artefaktin suunnittelu ja toteutus (vaihe 3) sekä artefaktin demonstraatio (vaihe 4) on yhdistetty tutkimuksen luonteen takia luvussa viisi. Näiden kahden vaiheen yhdistämisen syy perustuu tutkimuksen toteuttamisen konstruktiiviseen lähestymistapaan; demonstraatio rakentuu jo artefaktin toteutuksessa. Varsinaista erillistä demonstraatiovaihetta ei näin ollen ole tarpeen toteuttaa. Mikäli kehitetty artefakti ei toimi kaikissa tutkittavissa case-esimerkeissä, voidaan prosessia iteroida tarpeen mukaan. Laitteita pyritään tutkimaan niissä olevien liitäntöjen kautta, sillä piirin irrottamiseen liittyvät tekniikat sekä ram-muistin suora lukeminen vaativat kalliita erikoislaitteistoja. Lisäksi tutkimusta tehdessä piiri pitäisi irrottaa ja juottaa takaisin piirilevylle useita kertoja tallennustilalle tapahtuvien muutosten selvittämiseksi. Edellisessä luvussa useissa tutkimuksissa mainittu puhelinsovellusten tallentaman tiedon analysointi rajataan myös pois tästä tutkimuksesta.

Taustatutkimusta tehtiin kirjallisuuden avulla, mutta sieltä ei onnistuttu löytämään tutkittaviin laitteisiin liittyviä julkaisuja. Kirjallisuudesta kuitenkin löytyi vastaaville laitteille tehtyjä tutkimuksia, joiden pohjalta saadaan tutkimukselle hyviä lähtökohtia. Artikkelissa *IoT forensic challenges and opportunities for digital traces* käytetyt JTAG- ja UART-liitännät ja niiden käyttöön liittyvä tutkimus antavat hyvän pohjan laitteiden tutkimiselle (Servida & Casey, 2019).

Artefaktin toiminnan arviointi tapahtuu osittain samanaikaisesti artefaktin suunnittelun, toteutuksen ja demonstraation kanssa, mutta lopullinen artefaktin arviointi käydään läpi luvussa kuusi, jossa analysoidaan tuloksia.

DSR-prosessin viimeinen vaihe, kommunikaatio, hoidetaan tämän tutkielman kautta. Tutkielman lukijat voivat sen perusteella ottaa itse artefaktin käyttöön laitteita tutkiessaan, jolloin DSR-prosessi saadaan päätökseen.

5 TUTKIMUKSEN TOTEUTTAMINEN

Kotiautomaatiolaitteiden markkinaosuuksia ei Suomessa tilastoida, eivätkä jälleenmyyjät julkaise myymiensä laitteiden määrää. Tutkittavaksi valittiin neljä kotiautomaatiohubia, jotka ovat olleet Suomessa myynnissä. Laitteiden valinnassa painopisteinä olivat yleisimpien protokollien tuki ja edullinen hinta. Laitteistot ovat Philips Hue Bridge, Lidl Smart Home Gateway, Ikea Trådfri Gateway sekä Ikea Dirigera Hub. Kaikkien kotiautomaatiohubien vähittäismyyntihinta oli alle 100 euroa. Valituista laitteista yksikään ei tukenut Z-Wave-protokollaa, mutta sen sijaan kaikissa oli Zigbee-tuki. Tutkimuksessa käytettiin päätelaitteita, kuten liiketunnistimia, kytkimiä tai valaisimia.

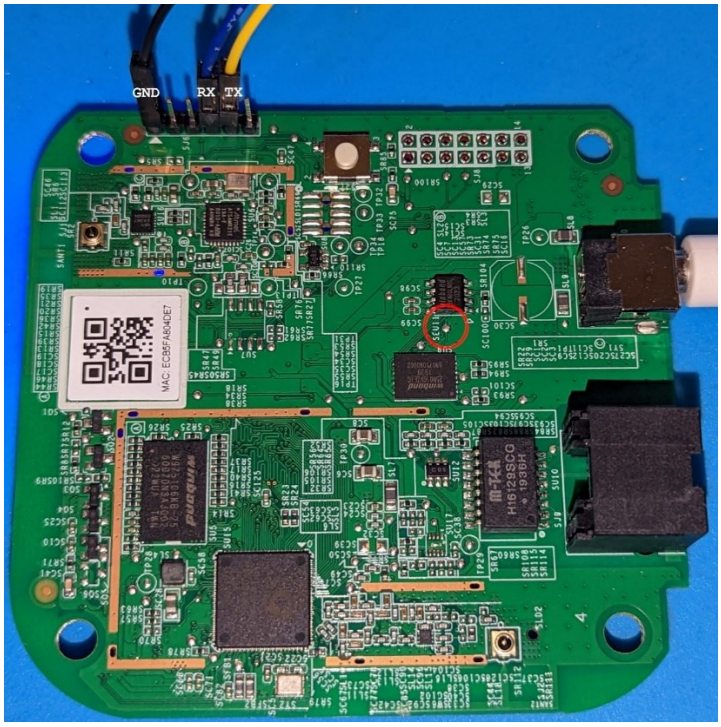
Valittujen laitteiden tallentaman tiedon tutkimisesta ei löytynyt julkaistuja tutkimuksia, vaikka hakkeriyhteisö on tutkinut laitteita laajasti. Heidän motiivinsa laitteiden tutkimiselle on esimerkiksi ottaa käyttöön ominaisuuksia, joita laite tarjoaa, mutta valmistaja ei halua ottaa käyttöön. Esimerkkinä useissa kotiautomaatiohubeissa voi olla valmius Wi-Fi-toiminnallisuuteen, jota valmistaja ei syystä tai toisesta ole ottanut käyttöön. Tutkittavista laitteista ainakin Philips Hue Bridge on mahdollista hakkeroida siten, että se käyttää Wi-Fi-yhteyttä langallisen verkkoyhteyden sijaan.

Tutkimukseen valitut laitteet tutkitaan satunnaisessa järjestyksessä sen hetkisillä uusimmilla laitteisto-ohjelmistoilla. Mikäli laitteisto-ohjelmisto päivittyy tutkimuksen aikana, päivitys asennetaan laitteelle valmistajan ohjeistuksen mukaisesti. Päivityksen mahdollisesti tuomat muutokset laitteen toimintaan huomioidaan tutkimusta tehdessä tarvittaessa.

Tutkittavalle laitteelle pyritään saamaan pääkäyttäjän oikeudet, jotta laitteen toimintalogiikka nähdään kokonaisuudessaan. Mikäli julkisesti tunnettuja tapoja laitteille pääsyyn ei ole, pyritään selvittämään, onko laitteella mahdollisesti liitäntöjä, joita voidaan käyttää.

5.1 Philips Hue Bridge

Tutkittava Philips Hue -kotiautomaatiohubi on laitteistoversioltaan 2.1 ja sen mallikoodi on 3241312018A. Laitteen piirilevy sisältää 64 MB:n Winbondin W9751G6KB-RAM-muistipiirin, Atmelin SAMR21-järjestelmäpiirin ja 128 MB:n Winbondin W25N01GV-flash-muistipiirin. Piirilevyllä on myös sarjaportti, johon kytkeytymällä pääsee käsiksi järjestelmään. (Seger, 2016)
Laitteiston saa avattua torx-ruuvimeisseleillä, minkä jälkeen piirilevyn voi irrottaa kotelostaan. Piirilevyllä on sarjaportti, johon kytkeytymällä sen pystyy ottamaan haltuun. Sarjaportti on helpoiten käytettävissä, mikäli siihen juottaa piikkiriman. Kuvassa 1 on nähtävillä piikkirima sekä siinä olevat sarjaportin pinnit.



KUVA 1 Philips Hue Bridge 2.1 -piirilevy

Laitteen käynnistyksenlataajan (engl. *bootloader*) toiminnan voi pysäyttää kytkemällä kuvassa 1 ympyröidyn testipisteen maahan ja kytkemällä laitteeseen virran. Philips Hue 2.1 ei suostu käynnistymään, mikäli sarjaportin TX-pinni on kytketty. Toisin sanoen ensin pitää yhdistää testipiste maahan, kytkeä virrat ja jonkin ajan kuluttua kytkeä TX-pinni kiinni sarjaporttiin. (ukl, 2019) Laitetta käytettäessä yhteysnopeus on yleinen käytössä oleva 115200 baudia (Banaru, 2018).

Testipisteellä maahan kytkettynä laitteen kaikki tallennustila ei ole käytettävissä, joten käynnistyksenlataajaan pitää päästä käsiksi eri keinoin. Tätä varten määritetään bootdelay-ympäristömuuttujan arvoksi sekuntimäärä, jonka käynnistyksenlataaja odottaa ennen varsinaisen järjestelmän käynnistämistä. Arvo tallennetaan ja laite käynnistetään uudelleen (Kuva 2).

```
ath> setenv bootdelay 3
ath> saveenv
Saving Environment to Flash...
Protect off 9F050000 ... 9F05FFFF
Un-Protecting sectors 5..5 in bank 1
Un-Protected 1 sectors
Protect off 9F040000 ... 9F04FFFF
Un-Protecting sectors 4..4 in bank 1
Un-Protected 1 sectors
Erasing Flash... 9F040000 ... 9F04FFFF ...Erasing flash...
First 0x4 last 0x4 sector size 0x10000
Erased 1 sectors
Writing to Flash...  9F040005 ... 9F050000 ...write addr: 9f040000
write addr: 9f050004
done
Protecting sectors 4..4 in bank 1
Protected 1 sectors
Protecting sectors 5..5 in bank 1
Protected 1 sectors
ath> reset
```

KUVA 2 Käynnistyksenlataajan muokkaus

Kun laite käynnistyy uudelleen, on kolme sekuntia aikaa pysäyttää ohjelmiston lataus ja päästä uudelleen käsiksi käynnistyksenlataajaan. Tässä vaiheessa voidaan asettaa salasana muokkaamalla ympäristömuuttujaa security. Kuvassa 3 root-käyttäjälle asetetaan salasanaksi toor.

```
Hit any key to stop autoboot:  0
ath> setenv security '$5$wbgtECliF$ugIfQUoE7SNg4mplDI/7xdfLC7jXoMAkupeMsml0hY9'
ath> saveenv
Saving Environment to Flash...
Protect off 9F040000 ... 9F04FFFF
Un-Protecting sectors 4..4 in bank 1
Un-Protected 1 sectors
Protect off 9F050000 ... 9F05FFFF
Un-Protecting sectors 5..5 in bank 1
Un-Protected 1 sectors
Erasing Flash... 9F050000 ... 9F05FFFF ...Erasing flash...
First 0x5 last 0x5 sector size 0x10000
Erased 1 sectors
Writing to Flash...  9F050005 ... 9F060000 ...write addr: 9f050000
write addr: 9f040004
done
Protecting sectors 5..5 in bank 1
Protected 1 sectors
Protecting sectors 4..4 in bank 1
Protected 1 sectors
ath> reset
```

KUVA 3 Salasanan asettaminen

Kun laite on käynnistynyt, kirjaudutaan root-käyttäjänä sisään äsken asetetun salasanan kanssa. Laitteessa on skripti /usr/sbin/ssh-factory-key, jonka avulla SSH-palvelin voidaan konfiguroida käyttökuntoon. Kuvan 4 mukaisesti komennolle annetaan parametriksi tiedosto, jossa on tallennettuna julkinen avain. Avainparin voi generoida esimerkiksi Windows-tietokoneessa puttygen-ohjelmalla tai Linux-pohjaisissa järjestelmissä komennolla ssh-keygen. Avaimen voi tallentaa laitteelle liittämällä sen editori-ikkunaan ja tallentamalla tiedoston. Laitteen uudelleenkäynnistyksen jälkeen siihen voidaan ottaa yhteys SSH-yhteydellä käyttäen luotua yksityistä avainta. (Banaru, 2018)

```
root@Philips-hue:~# ls -la
drwxr-xr-x    1 root     root           232 Sep 24 15:19 .
drwxr-xr-x    1 root     root           352 Jan  1  1970 ..
-rw-r--r--    1 root     root           563 Sep 24 15:19 publickey
root@Philips-hue:~# ssh-factory-key -r publickey
replaced: mikko@FM
already installed: firewall rule for ssh
root@Philips-hue:~#
```

KUVA 4 SSH-palvelimen käyttöönotto

5.1.1 Philips Hue Bridgen tietosisällön jäljentäminen

Tutkintavaiheessa jäljentäminen on mahdollista tehdä verkon yli käyttäen laitteella jo olemassa olevia ohjelmia. Jäljentämistä varten laite pitää kytkeä samaan lähiverkkoon tutkintatyöaseman kanssa. Laitteen normaali toiminta ei vaadi internet-yhteyttä, joten se toimii täysin normaalisti jäljentämisen aikana. Laitteelle kirjautuminen tapahtuu aiemmin asetettujen SSH-avainten avulla. Dropbear-SSH-palvelin käyttää kuvan 5 mukaisesti vanhentuneita salausavainten vaihtometodeja, joten SSH-yhteysohjelman konfiguraatioon pitää lisätä tuki niille (OpenSSH, 2023). Tämän jälkeen kirjautuminen onnistuu avaimilla normaalisti, kuten kuvassa 6 osoitetaan.

```
mikko@FM:~$ ssh root@10.10.12.57
Unable to negotiate with 10.10.12.57 port 22: no matching key exchange method found. Their
 offer: diffie-hellman-group14-sha1,diffie-hellman-group1-sha1,kexguess2@matt.ucc.asn.au
```

KUVA 5 Vanhentuneet key exchange -metodit

```
mikko@FM:~$ ssh root@10.10.12.57


BusyBox v1.25.1 (2021-08-31 07:06:54 UTC) built-in shell (ash)

  _    _ _    _ _____  ____    _    _          ___   __  __
 | |  | | |  | |  __ \|  _ \  (_)  | |        |__ \ \ \/ /
 | |__| | |  | | |__) | |_) |_ __ _  __| | __ _  ___    ) | \  V /
 |  __  | |  | |  ___/|  _ <| '__| |/ _` |/ _` |/ _ \  / /   > <
 | |  | | |__| | |    | |_) | |  | | (_| | (_| |  __/ / /_ / . \
 |_|  |_|\____/|_|    |____/|_|  |_|\__,_|\__, |\___| |____/_/ \_\
                                            __/ |
                                           |___/
-----------------------------------------------------------------------
Version: 1947054060
-----------------------------------------------------------------------

root@Philips-hue:~#
```

KUVA 6 Kirjautuminen SSH-avaimilla laitteelle

Laitteen partitiot, mountit ja block devicet voidaan listata kuvan 5 osoittamilla komennoilla. Komennolla cat /proc/mounts voidaan selvittää RAM-muistissa tmpfs- ja sysfs-tyyppiset mountit. Näissä olevaa tietoa häviää, kun laitteesta katkaistaan virta. Kuvan 7 perusteella nähdään, että juuressa olevat hakemistot sys ja tmp ovat RAM-muistissa.

```
root@Philips-hue:~# cat /etc/fstab
cat: can't open '/etc/fstab': No such file or directory
root@Philips-hue:~# cat /proc/mounts
/dev/root /rom squashfs ro,relatime 0 0
proc /proc proc rw,nosuid,nodev,noexec,noatime 0 0
sysfs /sys sysfs rw,nosuid,nodev,noexec,noatime 0 0
tmpfs /tmp tmpfs rw,nosuid,nodev,noatime 0 0
/dev/ubi1_1 /overlay ubifs rw,noatime 0 0
overlayfs:/overlay / overlay rw,noatime,lowerdir=/,upperdir=/overlay/upper,workdir=/overlay/work 0 0
tmpfs /dev tmpfs rw,nosuid,relatime,size=512k,mode=755 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,mode=600 0 0
debugfs /sys/kernel/debug debugfs rw,noatime 0 0
root@Philips-hue:~# cat /proc/mtd
dev:    size   erasesize  name
mtd0: 00040000 00010000 "u-boot"
mtd1: 00020000 00010000 "u-boot-env"
mtd2: 00010000 00010000 "reserved"
mtd3: 00010000 00010000 "art"
mtd4: 00400000 00020000 "kernel-0"
mtd5: 02800000 00020000 "root-0"
mtd6: 00400000 00020000 "kernel-1"
mtd7: 02800000 00020000 "root-1"
mtd8: 02800000 00020000 "overlay"
mtd9: 00915000 0001f000 "rootfs"
mtd10: 023d8000 0001f000 "rootfs_data"
root@Philips-hue:~# cat /proc/partitions
major minor  #blocks  name

  31        0        256 mtdblock0
  31        1        128 mtdblock1
  31        2         64 mtdblock2
  31        3         64 mtdblock3
  31        4       4096 mtdblock4
  31        5      40960 mtdblock5
  31        6       4096 mtdblock6
  31        7      40960 mtdblock7
  31        8      40960 mtdblock8
  31        9       9300 mtdblock9
  31       10      36704 mtdblock10
root@Philips-hue:~#
```

KUVA 7 Philips Hue -kotiautomaatiohubin partitiot ja mountit

Flash-muistilla olevista partitioista luku- ja kirjoitusoikeuksin on varustettu ainoastaan /dev/ubi1_1, joka on mountattu hakemistoon /overlay. Overlayfs mahdollistaa vain lukuoikeuksin varustetun tiedostojärjestelmän yhdistämisen luku- ja kirjoitusoikeuksin varustettuun tiedostojärjestelmään. Kaikki muutokset ja uudet tiedostot luodaan luku- ja kirjoitusoikeuksin varustettuun tiedostojärjestelmään. Kuvassa 7 näkyy, kuinka /overlay -hakemistossa oleva overlayfs yhdistetään juureen siten, että juuri pysyy kirjoitussuojattuna ja /overlay/upper -hakemistoon tulevat kaikki muutokset sekä uudet tiedostot. (Brown, 2023)

Kaikki Philips Hue Bridgen käytön aikana syntynyt tieto tallennetaan joko RAM-muistiin tmpfs-tiedostojärjestelmän avulla tai /dev/ubi1_1-laitteelle, joka on mountattu hakemistoon /overlay/upper.

Tietosisällön jäljentäminen tiedostotasolla onnistuu käyttämällä komentoja tar, gzip ja nc. Halutut tiedostot, eli tässä tapauksessa /overlay/upper -hakemistopolku, pakataan jäljennettävällä laitteella ja pakattu tiedosto putkitetaan netcat-ohjelmalla tutkintatyöasemalle kuvassa 8 näkyvällä komennolla.

```
root@Philips-hue:~# tar cz /overlay/upper | nc 10.10.10.40 5555
tar: removing leading '/' from member names
root@Philips-hue:~#
```

KUVA 8 Tiedostojen pakkaus ja putkittaminen

Tutkintatyöasema laitetaan odottamaan netcatin lähetystä portissa 5555 ja tallentamaan vastaanotettu data tar.gz-tiedostoon kuvan 9 osoittamalla komennolla. Vastaanotetussa datassa kannattaa käyttää numerointia, jotta vastaanotettujen pakettien sisällä olevat muutokset ovat helposti jäljitettävissä.

```
qwert@virtbuntu:~/PhilipsHue$ nc -l 5555 > PhilipsHue-001.tar.gz
qwert@virtbuntu:~/PhilipsHue$ ls -la
total 20
drwxrwxr-x  2 qwert qwert  4096 elo    28 20:27 .
drwxr-x--- 17 qwert qwert  4096 elo    28 20:13 ..
-rw-rw-r--  1 qwert qwert 12164 elo    28 20:27 PhilipsHue-001.tar.gz
qwert@virtbuntu:~/PhilipsHue$
```

KUVA 9 Tiedostojen vastaanottaminen

Pakettien välinen vertailu onnistuu helposti esimerkiksi Package Changes Analyzer (pkgdiff) -ohjelmalla. Ohjelmalle syötetään parametreiksi vertailtavat paketit, ja se näyttää muuttuneet tiedostot selkeässä raportissa. Ohjelman toimintaa voidaan testata tässä tapauksessa liittämällä matkapuhelimen Hue-applikaatio laitteeseen ja vertaamalla ennen liittämistä ja sen jälkeen otettuja paketteja. Tämän jälkeen verrataan paketteja pkgdiff-ohjelmalla. Kuvassa 10 näkyvästä raportin otteesta nähdään, että matkapuhelimen applikaation liittäminen laitteeseen luo kaksi tiedostoa ja yhden hakemiston. Tokenstore-hakemistoon tallentuu matkapuhelimen sovelluksen token tai vastaava tieto, jolla puhelin yksilöidään vastaisuudessa.

Data Files (2)

Name	Status	Delta	Visual Diff
upper/home/.config/tokenstore/a6d990d5-fef6-480b-a55b-1b462f8aef38	added		
upper/home/ipbridge/var/NVRAM_20000000.dat	added		

Directories (1)

Name	Status
upper/home/.config/tokenstore	added

KUVA 10 Ote pkgdiff-raportista

5.1.2 Laitteeseen tallentuva tieto

Philips Hue Bridgeen pysyvästi tallentuvaa tietoa voidaan tutkia edellisessä kappaleessa esitellyillä keinoilla sekä tekemällä yksi muutos kerrallaan. Jotta laite voi toimia, sen pitää tallentaa vähintään siihen liitettyjen laitteiden tiedot, jotta ne säilyvät virran katkaisemisen jälkeen tallessa. Käyttömuistiin tallentuvien tietojen hyödyntäminen ei edellä mainitulla menetelmällä onnistu, sillä se vaatii laitteen uudelleen käynnistämisen. Taulukossa 3 on listattu otetut jäljennökset.

Laitteeseen liitettyjen Zigbee-laitteiden tiedot saadaan selville pkgdiff-työkalun tarjoamien raporttien avulla. Niissä näkyvät muuttuneet ja lisätyt tiedostot.

TAULUKKO 3 Philips Hue Bridgestä otetut jäljennökset

Jäljennöksen nimi	Tapahtuma
PhilipsHue-001.tar.gz	Hubi resetoitu käyttöohjeen mukaan
PhilipsHue-002.tar.gz	Annettu laitteen olla päällä 30 minuuttia
PhilipsHue-003.tar.gz	Mobiililaite lisätty
PhilipsHue-004.tar.gz	Tehdasasetusten palautus painikkeella tehty
PhilipsHue-005.tar.gz	Laite päivitetty versioon 1953188020
PhilipsHue-006.tar.gz	Tehdasasetusten palautus painikkeella tehty
PhilipsHue-007.tar.gz	Annettu laitteen olla päällä 10 minuuttia
PhilipsHue-008.tar.gz	Lisätty mobiililaite ja liiketunnistin
PhilipsHue-009.tar.gz	Päivitetty liiketunnistimen laiteohjelmisto
PhilipsHue-010.tar.gz	Lisätty lamppu
PhilipsHue-011.tar.gz	Lisätty lamppu sovelluksessa huoneeseen
PhilipsHue-012.tar.gz	Laitettu lamppu päälle
PhilipsHue-013.tar.gz	Käytetty lamppua useaan kertaan
PhilipsHue-014.tar.gz	Odotettu 50 minuuttia tekemättä mitään
PhilipsHue-015-tmp.tar.gz	Laitettu valo päälle.
PhilipsHue-016-tmp.tar.gz	Laitettu valo pois
PhilipsHue-017.tar.gz	Tehty automaatio

Hubin resetoinnin ja sen 30 minuutin päällä olon välisissä jäljennöksissä ei ole eroa. Vasta mobiililaitteen lisääminen tekee muutoksia laitteelle tallentuvaan tietoon. Hakemistoon /overlay/upper/home/.config/tokenstore ilmestyy tiedosto nimeltään a6d990d5-fef6-480b-a55b-1b462f8aef38. Tiedosto sisältää 16 heksatavua, jotka eivät vaikuta liittyvän tiedoston nimeen. Edellä mainitun tiedoston lisäksi /overlay/upper/home/ipbridge/var -hakemistoon on luotu tiedosto NVRAM_20000000.dat. Tiedoston sisältä löytyy tokenstore-hakemistosta löytyvän tiedoston nimi, pitkä merkkijono sekä mobiililaitteelle sovelluksessa annettu nimi.

Laitteen tehdasasetusten palauttamisen jälkeen laitteelle ilmestyneet tiedostot ovat poistuneet. Lisäksi useita muita tiedostoja on muutettu. Esimerkkinä verkkoasetusten määritystiedostossa /overlay/upper/etc/config/network IPV6-osoitteiden ula_prefix -parametri on määritetty uudelleen satunnaiseksi arvoksi. Kyseinen parametri määrittää yksityisten verkkojen osoitealueen, jota käytetään paikallisten laitteiden kommunikointiin samassa lähiverkossa. Myös Dropbear-ssh-palvelimen dss- sekä rsa-avaimet on määritelty uudelleen sekä kaikki hakemistojen /overlay/upper/home/homekit/var ja /overlay/upper/home/behaviord/var tiedostot on luotu uudelleen.

Laitteen päivitys versioon 1953188020 tekee suuren määrän muutoksia hakemistorakenteeseen ja tiedostoihin. Hakemistoon /overlay/upper/etc on ilmestynyt kaksi hakemistoa: iot-credentials sekä mosquitto. Molemmat hakemistot liittyvät Mosquitto MQTT broker -viestinvälitysohjelmistoon, jonka avulla laite viestii Google IoT Core -palvelun kanssa. Kyseinen palvelu on lopetettu elokuussa 2023, joten laitteen uudemmat päivitykset ovat todennäköisesti korvanneet sen jollakin toisella ratkaisulla. Uudessa tiedostossa /overlay/upper/etc/board.json on määritelty kolme asiaa: laitteessa käytettävä piirilevyversio, verkkoyhteyksien nimet sekä onko ip-osoite staattinen vai dynaaminen. Muiden tiedostolisäysten lisäksi /overlay/upper/home -hakemistoon on ilmestynyt

stream-niminen hakemisto, jossa on stream.lmdb- sekä stream.lmdb-lock-tiedostot.

Tehdasasetusten palautuksen sekä ohjelmiston päivityksen jälkeen kaikki autentikointiin liittyvät avaimet on taas generoitu uudelleen ja puhelimen yhdistämiseen liittyvä tokenstore-hakemisto on poistettu tiedostoineen. Kun laite on ollut päällä 10 minuuttia, tiedostoissa ei näy muutoksia.

Kahdeksannessa jäljennöksessä puhelimen ja liiketunnistimen liittämisen jälkeen tokenstoresta löytyy taas laitteen tunniste ja NVRAM_20000000.dat -tiedostosta laitteen nimi ja tokenstoren tunniste. Tiedostosta NVRAM_20010004.dat löytyy selkokielisenä puhelimen aikavyöhyke. Lisäksi samaan /overlay/upper/home/ipbridge/var -hakemistoon on ilmestynyt useita muitakin NVRAM-alkuisia tiedostoja. Tiedostoista NVRAM_10100002.dat, NVRAM_10100003.dat ja NVRAM_10100004.dat löytyy selkokielisenä maininta liiketunnistimesta, valosensorista sekä lämpötila-anturista, jotka löytyvät kyseisestä Philipsin liiketunnistimesta. Applen Homekit-toiminnallisuuteen liittyvässä hakemistossa /overlay/upper/home/homekit/var oleva tiedosto hk_aad sisältää laitteeseen liitetyn liiketunnistimen tarjoamat palvelut samalla tavalla kuin ne löytyvät NVRAM-tiedostoistakin.

Liiketunnistimen päivitys saa aikaan muutoksia edellisessä kappaleessa mainituissa siihen liittyvissä NVRAM-tiedostoissa. Niissä versionumerolta vaikuttava numerosarja on muuttunut muodosta 6.1.0.18912 muotoon 6.1.1.27575. Myös muissa NVRAM-tiedostoissa on tapahtunut binääritason muutoksia, mutta niiden merkitys ei ole selvillä.

Kymmenennettä jäljennöstä edeltänyt lampun lisääminen toi laitteeseen paljon muutoksia. Lampun lisäämisen kannalta merkityksellinen tiedosto on NVRAM_10000001.dat, jossa on puhelinsovelluksessa lampulle annettu nimi sekä mallitiedot tallennettuna. Lampun mallitiedot löytyvät myös sekä Homekitin tiedostosta hk_aad että kokonaan uudessa hakemistossa /overlay/upper/home/.config/modelinfostore olevasta modelinfo_00178801093bc59d -tiedostosta. Myös /overlay/upper/home/behaviord/var/behaviord.db -sqlite-tietokantaan on tullut uusi taulu, jossa on valaistukseen liittyviä skriptejä kuvattuna taulussa Resource_ResourceBehavior_script. Kuvaukset liittyvät esimerkiksi valaistuksen ajastukseen tai muihin automatisointeihin ja ne löytyvät puhelinsovelluksesta valmiina vaihtoehtoina. NVRAM-tiedostoja on tullut lisää yhteensä viisi kappaletta, joista vain yhdessä on tekstimuotoisena aiemmin mainitut tiedot. Lisäksi 43 NVRAM-tiedostoa on muuttunut.

Edellisessä jäljennöksessä lamppu lisättiin sovellukseen, mutta ei vielä määritetty, mihin huoneeseen se kuuluu. Lampun lisääminen huoneeseen on pakollista, joten prosessi oli siinä vaiheessa kesken. Jäljennöksessä on kaksi uutta NVRAM-tiedostoa ja muutoksia kolmessa. Lisäksi /overlay/upper/home/devices/devices.ldbm -tiedosto on muuttunut. Aina kun hubiin on yhdistetty puhelin tai liitetty laite, päivittyy /overlay/upper/home/.config/uuidstore -tiedosto. Tiedostoon lisätään sekä poistetaan uuid-arvoja. Lampun lisääminen huoneeseen toi tiedostoon kolme uutta uuid-arvoa.

Ennen seuraavaa jäljennöstä, lamppu laitettiin päälle puhelinsovelluksella ilman mitään muita säätöjä. Edelliseen jäljennökseen verrattuna ainoastaan kolmeen NVRAM-tiedostoon on tullut muutoksia. Ne ovat NVRAM_10000500.dat, NVRAM_10000600.dat ja NVRAM_10105000.dat. Tiedostoissa ei ole selkokielistä tietosisältöä, joten niiden muutokset eivät ole selkeitä.

Muutokset lampun päälle ja pois laittamisen, himmentämisen ja valon lämpötilan määrityksen jälkeen näkyvät jäljennöksessä 13. Taas muutokset ovat tulleet ainoastaan NVRAM-tiedostoihin. Edellisessä jäljennöksessä muuttuneiden tiedostojen lisäksi tiedostot NVRAM_00000103.dat sekä NVRAM_20000000.dat ovat muuttuneet. Jälkimmäinen sisältää puhelimen nimen, uuid:n selkokielisenä sekä binääridataa.

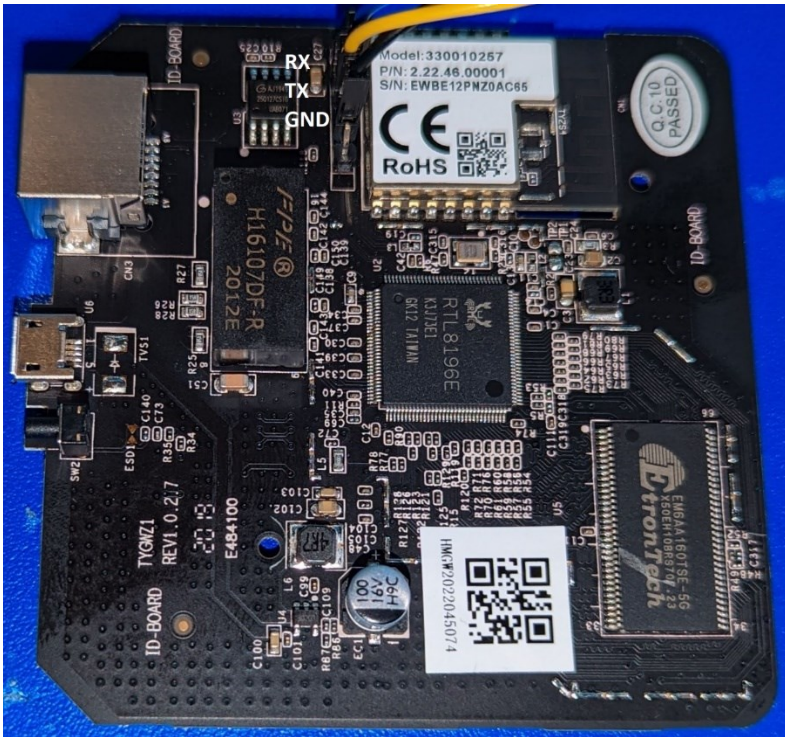
Kun hubi ja muut laitteet ovat olleet 50 minuuttia käyttämättömänä, on muutoksia havaittavissa ainoastaan NVRAM_10000500.dat, NVRAM_10000600.dat ja NVRAM_10105000.dat -tiedostoissa.

Seuraavan kahden jäljennöksen avulla tarkasteltiin, mitä muutoksia lampun päälle laittaminen saa aikaan käyttömuistissa olevassa /tmp -hakemistossa. Jäljennöksiä vertaillessa on havaittavissa, että niiden välillä ei ole eroa.

Viimeisenä testinä hubiin tehtiin automaatio puhelinsovelluksen avulla. Sen tarkoituksena on himmentää valoja hiljalleen nukkumaan mentäessä. Jäljennöstä 17 verrattiin jäljennökseen 14. Lisää uuid-arvoja oli tullut uuidstore-tiedostoon. Lisäksi behaviord.db -tietokantaan on tullut yksi muutos. Kannan Resource_ResourceBehavior_Instance -tauluun on tullut yksi rivi, jonka data-kenttään on tallentunut json-koodattuna automaatiota luodessa määritetyt parametrit sekä sille annettu nimi. Apple Homekit -toiminallisuuteen liittyvä hk_accessory_state_file on myös muuttunut. NVRAM-tiedostoista ovat muuttuneet NVRAM_10000500.dat, NVRAM_10000600.dat, NVRAM_10013000.dat NVRAM_10105000.dat ja NVRAM_20000000.dat. Lisäksi uutena tiedostona on tullut NVRAM_10014001.dat.

5.2 Lidl Smart Home Gateway

Tutkittava Lidl Smart Home Gateway on mallinumeroltaan HG06322 ja versioltaan 06/2020. Piirilevyllä on Gigadevicen GD25Q127CSIG 32 MB:n -flash-muistipiiri sekä Etron Technologin 32 MB:n EM6AA160TSE-5G-RAM-muistipiiri. Järjestelmäpiiri on RF-suojan alla, joten sen mallikoodi ei ole tiedossa. Laitteen avaamiseen ei tarvita ruuvimeisseleitä, sillä se on kiinni ainoastaan takakannen muoviklipseillä. Samalla tavoin kuin Philips Hue Gateway, Lidlin laitteessa on myös sarjaportti, jonka käyttämistä helpottaa piikkiriman juottaminen piirilevylle. Kuvassa 11 on kiinnitettynä piikkirimat ja tarvittavat kaapelit sarjaportin käyttämiseksi.



KUVA 11 Lidl Smart Home Gateway -piirilevy

Laitteeseen voidaan kytkeä sarjaportin kaapelit ja avata tietokoneelta yhteys ennen virtojen kytkemistä. Yhteysnopeus on 38400 baudia yleisen 115200 sijaan. Laitteen saa pysähtymään bootloaderiin painamalla ESC-näppäintä välittömästi virtojen kytkemisen jälkeen kuvan 12 mukaisesti.

```
ooting...

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@
@ chip__no chip__id mfr___id dev___id cap___id size_sft dev_size chipSize
@ 0000000h 0c84018h 00000c8h 0000040h 0000018h 0000000h 0000018h 1000000h
@ blk_size blk__cnt sec_size sec__cnt pageSize page_cnt chip_clk chipName
@ 0010000h 0000100h 0001000h 0001000h 0000100h 000010h 000004eh GD25Q128
@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
DDR1:32MB

---RealTek(RTL8196E)at 2020.04.28-13:58+0800 v3.4T-pre2 [16bit](400MHz)
P0phymode=01, embedded phy
check_image_header  return_addr:05010000 bank_offset:00000000
no sys signature at 00010000!

---Escape booting by user
P0phymode=01, embedded phy

---Ethernet init Okay!
<RealTek>
```

KUVA 12 Käynnistyksen keskeyttäminen

Laitteen root-käyttäjän salasana määritetään käynnistyksen yhteydessä siten, että se on kahdeksan viimeistä merkkiä auskeystä. Auskey on laitteen UUID kanssa sen yksilöivä tunnus, joita laite tarvitsee kommunikoidakseen Tuyan palvelinten kanssa.

Auskey on tallennettuna laitteen flash-muistissa, ja se on salattu toisella avaimella. Koska avainten tallennuspaikat flash-muistissa ovat identtisiä laitteiden välillä, voidaan ne bootloaderissa lukea suoraan flash-muistilta kuvan 13 esimerkin tapaan.

```
<RealTek>FLR 80000000 401802 16
Flash read from 00401802 to 80000000 with 00000016 bytes        ?
(Y)es , (N)o ? --> Y
Flash Read Successed!
<RealTek>DW 80000000 4
80000000:       2A7B6675        2A272724        7B69576C        2A483C3C
<RealTek>FLR 80000000 402002 32
Flash read from 00402002 to 80000000 with 00000032 bytes        ?
(Y)es , (N)o ? --> Y
Flash Read Successed!
<RealTek>DW 80000000 8
80000000:       F70A30B5        B6618E9F        699829DC        A5BAA241
80000010:       85756A4F        51D92D3C        8369ECE1        BE20E776
<RealTek>
```

KUVA 13 Avainten hakeminen flash-muistista

Paul Banks on julkaissut auskeyn salauksen purkamiseen ja sen viimeisen kahdeksan merkin tulostamiseen toimivan Python-skriptin (kuvassa 14), jolle syötetään flashilta luetut avaimet. Root-käyttäjän salasanan selvittämisen jälkeen laite voidaan käynnistää uudelleen, jonka jälkeen voidaan kirjautua sisään.

```
mikko@FM:~$ python3 lidl_auskey_decode.py
Enter KEK hex string line>2A7B6675        2A272724        7B69576C        2A483C3C
Encoded aus-key as hex string line 1>F70A30B5        B6618E9F        699829DC        A5BAA241
Encoded aus-key as hex string line 2>85756A4F        51D92D3C        8369ECE1        BE20E776
Auskey: LllnhGZXlb18UthAK5hiQiOAFO8S3WAx
Root password: FO8S3WAx
```

KUVA 14 Laitteen root-käyttäjän salasanan selvittäminen

Laitteen pääkäyttäjän salasanan selvityksen jälkeen laitteelle voidaan kirjautua sisään joko sarjaportin tai SSH-yhteyden kautta. Laitteella oli oletuksena käytössä Dropbear-SSH-palvelin portissa 2333 (Banks, 2021), mutta vuonna 2023 julkaistun päivitysten myötä se ei enää käynnisty automaattisesti. Päivitys muokkasi tuya_net_start.sh -skriptiä siten, että ssh-palvelin ei käynnisty ilman samaan hakemistoon tehtyä enable_ssh_flag-tiedostoa. Kun tiedosto on tehty, suoritetaan käynnistyksen yhteydessä skripti /tuya/ssh_monitor.sh, joka käynnistää Dropbear-SSH-palvelimen.

5.2.1 Lidl Smart Homen tietosisällön jäljentäminen

Hubin mountit listataan samalla tavalla kuin Philipsin laitteen kanssa (kuva 15). Listauksesta nähdään, että laite ei käytä tyypillistä fstab-tiedostoa mounttien määrittelyyn, vaan ne määritellään tiedostossa /etc/init.d/rcS.

```
# cat /etc/fstab
cat: can't open '/etc/fstab': No such file or directory
# cat /proc/mounts
rootfs / rootfs rw 0 0
/dev/root / squashfs ro,relatime 0 0
proc /proc proc rw,relatime 0 0
ramfs /var ramfs rw,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
tmpfs /dev tmpfs rw,relatime,size=64k,mode=0755 0 0
/dev/mtdblock4 /tuya jffs2 rw,relatime 0 0
# cat /proc/mtd
dev:    size   erasesize  name
mtd0: 00020000 00010000 "boot+cfg"
mtd1: 001e0000 00010000 "linux"
mtd2: 00200000 00010000 "rootfs"
mtd3: 00020000 00010000 "tuya-label"
mtd4: 00be0000 00010000 "jffs2-fs"
#
```

KUVA 15 Lidl Smart Home -kotiautomaatiohubin partitiot ja mountit

Hubin tallennustilan rakenne eroaa Philipsin rakenteesta jonkin verran. Philipsissä käytettiin overlay-tiedostojärjestelmää yhdistämään lukuoikeuksin liitetty partitio sekä luku- ja kirjoitusoikeuksin liitetty partitio yhdeksi. Lidlin laitteessa kaikki laitteen käyttöönoton jälkeen tallennettava sisältö on liitettynä /tuya -hakemistoon /dev/mtdblock4 -flash-muistilla.

Laitteen Linux-järjestelmässä ei ole Philipsiin verrattuna yhtä laajaa valikoimaa työkaluja tietosisällön jäljentämiseen. Olennaisimmat puuttuvat työkalut ovat varsinkin tar, nc, ssh sekä scp. Edellä mainittujen komentojen puuttuessa, ei laitteesta saada samoilla keinoilla tietosisältöä jäljennettyä.

Laitteen SSH-palvelimen avulla kuitenkin voidaan tutkintatyöasemasta käsin jäljentää koko /dev/mtdblock4 -block. Kuvassa 16 otetaan yhteys tutkintatyöasemalta Lidlin kotiautomaatiohubiin ja suoritetaan välittömästi komento cat /dev/mtdblock4. Tuloste ohjataan tutkintatyöaseman tiedostoon, josta se voidaan joko liittää tai purkaa haluttuun hakemistoon.

```
qwert@virtbuntu:~/lidl$ ssh root@10.10.12.117 -p 2333 "cat /dev/mtdblock4" > mtdblock4.bin
root@10.10.12.117's password:
qwert@virtbuntu:~/lidl$ file mtdblock4.bin
mtdblock4.bin: Linux jffs2 filesystem data big endian
qwert@virtbuntu:~/lidl$
```

KUVA 16 Levynkuvan jäljentäminen

Koko levynkuvan purkaminen onnistuu esimerkiksi Jefferson-työkalulla (Onekey, 2023) kuvan 17 mukaisesti.

```
qwert@virtbuntu:~/lidl$ jefferson mtd4.bin -d extracted/
dumping fs to /home/qwert/lidl/extracted/ (endianness: >)
Jffs2_raw_inode count: 56
Jffs2_raw_dirent count: 56
```

KUVA 17 Levynkuvan purkaminen Jefferson-työkalulla

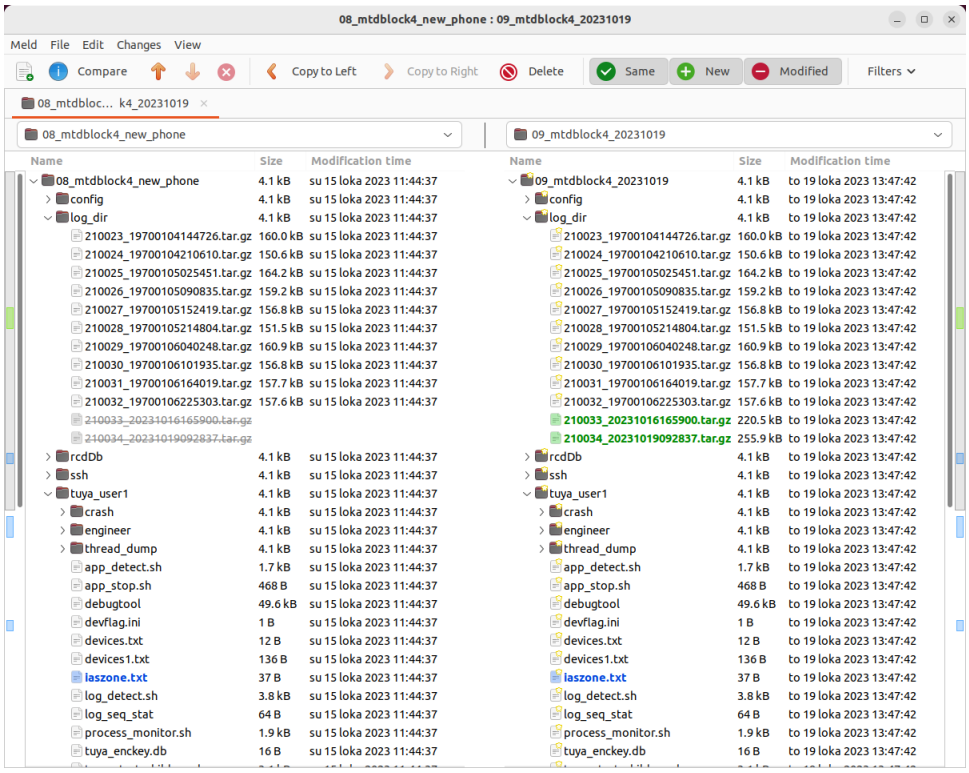
Levynkuvan purkamisen jälkeen hakemistorakennetta voi tutkia esimerkiksi teksti- tai heksaeditoreilla.

5.2.2 Laitteeseen tallentuva tieto

Kuten aiemmin mainittiin, Lidlin kotiautomaatiohubi perustuu Tuyan toteuttamaan laitteistoon. Kaikki konfiguraatiotiedostot ja laitteen määrittämiseen liittyvät skriptit sijaitsevat /tuya-hakemistossa. Laite tallentaa /tmp-hakemistoon väliaikaistiedostoja, kuten ladatut päivitykset ja lokitiedoston.

Valitettavasti /tmp -hakemisto on käyttömuistissa, joten laitteen uudelleenkäynnistyksen yhteydessä kaikki tieto sieltä häviää. Aikaisemmassa luvussa mainittu mtdblock4 sisältää /tuya -hakemiston sisällön ja se on ainoa paikka, johon laite tallentaa käyttäjäkohtaista tietoa.

Laitteen toiminnan tutkimista voi toteuttaa samalla tekniikalla kuin Philipsin laitteen kanssa. Jokaisen muutoksen jälkeen otettu jäljennös voidaan purkaa omaan hakemistoonsa, jonka jälkeen niiden vertailu onnistuu esimerkiksi Meld-nimisellä sovelluksella. Sovelluksen avulla on helppoa nähdä muuttuneet tiedostot ja avata ne vierekkäin vertailtavaksi. (Willadsen, 2023) Kuvassa 18 vertaillaan kahta jäljennöstä. Siinä on nähtävissä uudet tiedostot vihreällä ja muuttuneet sinisellä merkattuina.



KUVA 18 Kahden jäljennöksen vertailu Meld-sovelluksella

Laitteelle tallentuvaa sisältöä tutkittiin ottamalla se käyttöön yhden pir-liiketunnistimen kanssa. Käyttöönotto tapahtuu Lidl Smart Home -sovelluksen avulla. Laitteen pitää olla samassa lähiverkossa ja sillä pitää olla pääsy internettiin, vaikka yhteys tapahtuukin paikallisesti. Hubin ja puhelimen sovelluksen yhteen liittämisen jälkeen, voitiin hubiin liittää Lidlin liiketunnistin. Tämän jälkeen puhelimen sovellukseen saatiin ilmoitus aina, kun liikettä havaittiin. Ilmoitukset

saapuivat puhelimeen, vaikka se ei ollut samassa lähiverkossa hubin kanssa. Sekä hubi että liiketunnistin jätettiin muutamaksi viikoksi päälle tilaan, jossa kuljettiin päivittäin.

Laitteesta otettiin jäljennös taulukon 4 mukaisesti sekä jonkin toiminnon että ajan kulumisen jälkeen. Taulukosta on nähtävissä laitteelle tehdyt toiminnot sekä kulunut aika.

TAULUKKO 4 Lidl Smart Home Gatewaysta otetut jäljennökset

Jäljennöksen nimi	**Tapahtuma**
01_mtdblock4_resetted	Hubi resetoitu käyttöohjeen mukaan
02_mtdblock4_app_connected	Sovellus ja hubi liitetty yhteen
03_mtdblock4_motion_sensor_added	Liiketunnistin liitetty hubiin
04_mtdblock4_after_few_hours	Hubi jätetty muutamaksi tunniksi päälle
05_mtdblock4_next_day	Hubi jätetty päiväksi päälle
06_mtdblock4_next_week	Hubi jätetty viikoksi päälle
07_mtdblock4_20231015	Hubi jätetty viikoksi päälle
08_mtdblock4_new_phone	Sovellus asennettu uuteen puhelimeen ja liitetty hubiin
09_mtdblock4_20231019	Hubi jätetty neljäksi päiväksi päälle
10_mtdblock4_20231109	

Puhelimen sovelluksen liittäminen hubiin muokkaa tuya_user1/tuya_user.db-tiedostoa useiden muiden tiedostojen lisäksi. Tuyan dokumentoinnin mukaan tiedostossa on muun muassa laitteen aktivointiin ja verifiointiin liittyviä tietoja. Dokumentaatiossa mainitaan myös, että kyseisen tiedoston poistaminen vastaa tehdasasetusten palautusta.

Liiketunnistimen lisäys muokkaa tuya_user1/tuya_user.db -tiedostoa sekä samassa hakemistossa olevia devflag.ini ja devices1.txt -tiedostoja. Lisäksi samaan kansioon ilmestyy iaszone.txt -tiedosto. Devflag.ini -tiedostossa oleva numero muuttuu nollasta yhdeksi. Kyseisen tiedoston sisältö ei muutu myöhemmin otetuissa jäljennöksissä. Devices1.txt-tiedostoon ilmestyy yksi heksadesimaaliarvoja sisältävä rivi. Iaszone.txt-tiedosto on liiketunnistimiin liittyvä Intruder Alarm System Zone -tiedosto. Hakemistossa rcdDb muuttuvat tiedostot dub_dev_ddi.rdb sekä sub_dev_schm.rdb. Ensimmäisen tiedoston alusta löytyy devices1.txt-tiedostossa esiintyvä heksadesimaaliarvo sekä lopusta json-koodattuna dataa, jonka perusteella liiketunnistimen id-arvo on juuri kyseinen heksadesimaaliarvo ilmaistuna little endian -tavumuodossa. Jälkimmäisessä tiedostossa on tietoja liittyen liiketunnistimeen, mutta ei yksilöiviä arvoja.

Kun laite on ollut muutaman tunnin käynnissä, se on tehnyt varmuuskopiot rcdDB-hakemistossa olevista sub_deb_ddi.rbd ja sub_deb_schm.rdb -tiedostoista ja lisännyt niille uusien tiedostojen nimen loppuun _bak. Myös iaszone.txt -tiedostossa oleva arvo on muuttunut yhden tavun verran. Vuorokauden päällä olemisen jälkeen ainoa muuttunut tiedosto on zigbeeNetInfo.txt, jonka sisällä olevat Global FC ja Network FC ovat muuttuneet.

Viikon päällä oltuaan tuya_user.db ja sen varmuuskopio ovat muuttuneet, iaszone.txt on jälleen muuttunut yhden merkin verran sekä passwd-tiedostosta

on muuttunut root-käyttäjän salasanan hash. Laitteessa toimii kuitenkin vielä sama salasana, joten varsinaisen salasananvaihdon takia muutos ei ole tapahtunut. Tuya-hakemiston juuressa olevasta start_record_file-tiedostosta on poistettu alusta kymmeniä rivejä. Kyseinen tiedosto toimii eräänlaisena järjestelmälokina, johon tallentuu määrittämättömin aikavälein tietoja käynnissä olevista prosesseista, muistin käytöstä, levytilan käytöstä sekä /tmp -hakemiston sisältö.

Kun laite on ollut päällä seuraavan viikon, siihen on tallentunut /tuya/log_dir -hakemistoon tar.gz-pakattuja uusia lokitiedostoja. Kun laite on tarpeeksi kauan päällä, jotta juuren tmp-hakemiston lokitiedosto kasvaa tietyn koon yli, pakataan käyttömuistissa oleva loki ja tallennetaan se /tuya/log_dir-hakemistoon. Lokien käsittely tapahtuu /tuya/tuya_user1/log_detect.sh -skriptissä.

Tiedostot ovat pakattuna kooltaan noin 160–220 kilotavua, ja niitä on yhteensä yhdeksän kappaletta. Lisäksi /tuya/tuya_user1-hakemistoon on luotu logseq0 – logseq7 -tiedostot sekä loq_seq_stat-tiedosto. Jälkimmäisen tiedoston sisällä on merkkijono *{"max":8,"last":7,"first":0}*, jonka voi päätellä liittyvän logseq-tiedostojen määrään. Juuressa oleva log_index_file-tiedoston arvo on kasvanut arvosta 210 000 arvoon 210 032. Lisäksi aiemmin mainitut start_record_file- sekä passwd-tiedostot ovat muuttuneet.

Ennen kahdeksannen jäljennöksen ottamista Lidl Home -sovellus asennettiin uuteen puhelimeen, joka liitettiin sen jälkeen hubiin. Jäljennöksessä on /tuya/log_dir -hakemistoon ilmestynyt uusi tar.gz-pakattu lokitiedosto. Aiemmin mainitut logseq-tiedostot ovat kadonneet ja log_seg_stat-tiedoston merkkijono on muuttunut muotoon *{"max":0,"last":0,"first":0}*. Järjestelmälokina toimiva start_record_file on jälleen päivittynyt. Juuressa oleva log_index_file-tiedoston arvo on kasvanut yhdellä.

Yhdeksännessä jäljennöksessä lokitiedostoja on tullut kaksi kappaletta lisää ja log_index_file-tiedoston arvo on kasvanut kahdella. Hakemistossa /tuya/tuya_user1 oleva tietokanta tuya_user.db ja sen varmuuskopio on päivittynyt sekä samassa hakemistossa oleva iaszone.txt on jälleen muuttunut yhdellä numerolla.

Pakatut lokitiedostot on nimetty log_index_file-tiedostossa olevan arvon, päivämäärän ja kellonajan mukaan. Esimerkki tiedostonimestä on *210034_20231019092837.tar.gz*. Mikäli laite ei ole saanut verkkoyhteyttä käynnistyessään, lähtee ajanlasku aina epochin alusta, eli keskiyöstä 1.1.1970, sillä laitteessa ei ole paristovarmennettua RTC-piiriä. Heti kun laite saa verkkoyhteyden, se päivittää kellonajan verkosta, jolloin sen jälkeen luodut lokitiedostot ovat oikein nimettyjä. Pakattuja lokitiedostoja tutkittaessa selviää, että niiden rivimäärä on 30 000 ja 60 000 riviä. Lokitiedostojen log_detect.sh-skripti pakkaa lokin, kun se on kooltaan noin kolme megatavua. Kun levytilan käyttö ylittää 95 prosenttia, skripti poistaa vanhimman pakatun lokitiedoston.

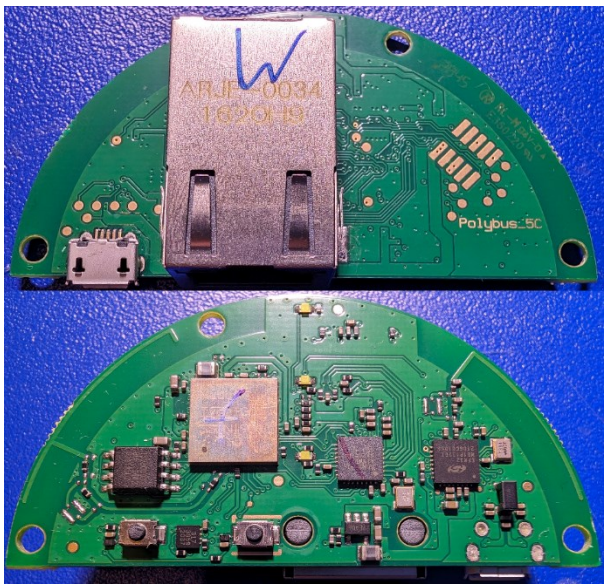
Päivitysten muutoslokeja tai versioita ei löydetty, joten ei ole tarkkaa tietoa, mitä laitteen versiopäivityksissä tapahtuu. Testien alussa laitteessa pääasiallisesti käynnissä olevan /tuya/tuya_user1/tyZ3Gw -binäärin versio oli 1.2.12, jolloin ssh-palvelin oli oletuksena päällä. Laitteen päivityttyä versioon

1.2.44, oli ssh-palvelin oletuksena pois päältä. Päivityksessä muuttuivat lähinnä edellä mainittu binääritiedosto sekä osa samassa hakemistossa olevista skripteistä.

5.3 Ikea Trådfri Gateway

Ikean ensimmäinen kotiautomaatiohubi Ikea Trådfri Gateway poistui myynnistä uuden Dirigera-mallin myötä. Vanhempi malli on kuitenkin vielä Ikean tuen piirissä ja olemassa olevat laitteet toimivat edelleen, joten Trådfri Gateway -laitteita voi olla vielä erittäin paljon käytössä.

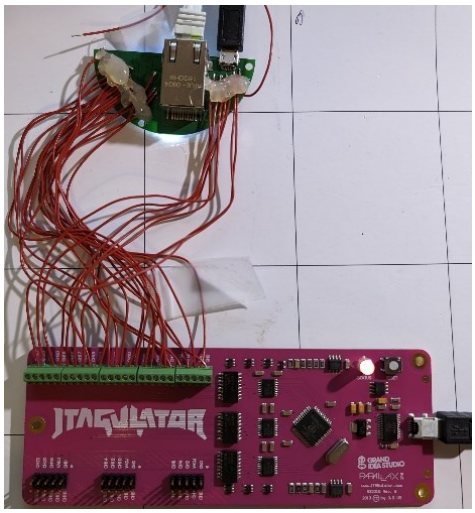
Tutkittava Ikea Trådfri Gateway on mallikoodiltaan E1526. Laitteen käyttöönoton jälkeen puhelinsovelluksessa näkyvä versionumero on 1.8.25. Sen piirilevyllä on 32 Mb:n SPI-muisti sekä Cypress CYW43907-järjestelmäpiiri. Lisäksi laitteessa on liittimiä, jotka vaikuttavat jonkinlaiselta huoltoportilta. (arturo182, 2017) Laitteen koteloinnissa ei käytetä ruuveja, mutta piirilevy on kiinnitetty kolmella Philips-ruuvilla. Piirilevy on pienikokoinen, kuten kuvassa 19 näkyy.



KUVA 19 Ikea Trådfri Gateway -piirilevy molemmilta puolilta

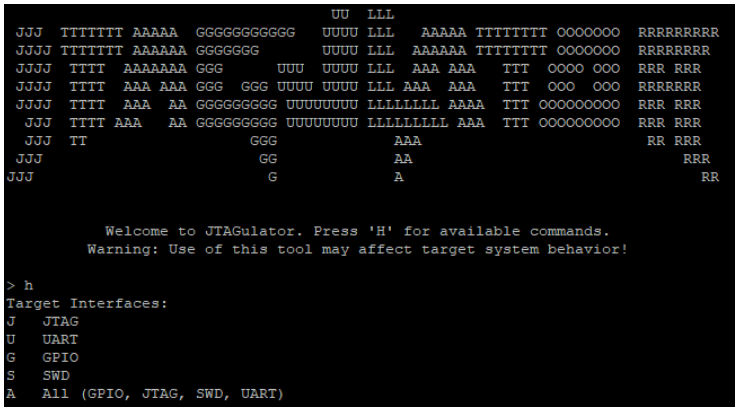
Kuvan 19 ylemmässä kuvassa näkyvät myös kontaktipisteet, mutta verkosta tai kirjallisuudesta ei löydy niille käyttötarkoitusta tai dokumentaatiota. Padien toimintaa voi tutkia esimerkiksi JTAGulator-laitteella, jonka avulla voidaan automaattisesti etsiä JTAG-, UART- tai ARM SWD-väylät piirilevyllä olevista kontakti- tai testipisteistä (Grand Idea Studio, 2024). Laitteessa on Murata 1GC -järjestelmäpiiri, jonka dokumentaation mukaan siinä on UART-väylä. JTAGulatorin avulla sitä voidaan paikallistaa, mutta koko väylää ei välttämättä ole kytketty piirilevylle. Mahdollinen UART-yhteys on nopeudeltaan 115 200 baudia.

JTAGulatorin käyttöä varten piirilevyn testipisteisiin ja padeihin juotettiin kiinni hyppylankoja, jotka kytkettiin laitteen kytkentärimaan kuvan 20 mukaisesti.



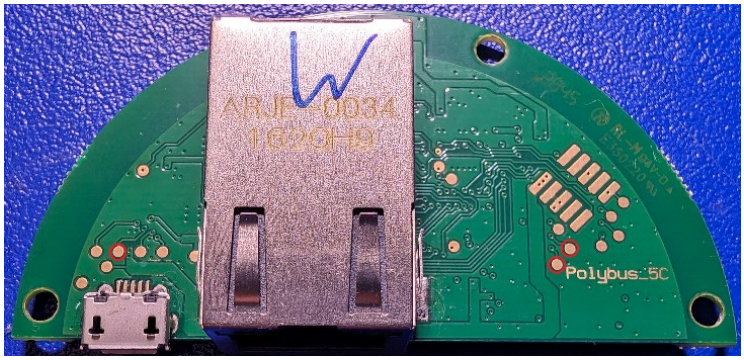
KUVA 20 JTAGulator kytketty Ikea Trådfri Gatewayn kontaktipisteisiin

JTAGulatorissa oleva ohjelmisto toimii itsenäisesti, ja sitä ohjataan USB-väylän yli toimivalla sarjaporttiyhteydellä. Yhteyden muodostamisen jälkeen voidaan valita, minkä tyyppistä väylää ollaan etsimässä, kuten kuvassa 21 näkyy.



KUVA 21 JTAGulatorin päävalikko

JTAGulator havaitsi kuvassa 22 näkyvistä testipisteistä laitteen käynnistyessä UART-liikennettä ulospäin suurilla nopeuksilla, jotka vaihtelivat välillä 851 063–8 888 888. JTAGulatorin maksimi baudinopeus on 307 200, joten ulostulevasta datasta ei saatu selkokielistä millään asetuksilla. Muista pisteistä ei havaittu mitään liikennettä edes laitteen käynnistyksen aikana.



KUVA 22 Laitteen käynnistyessä aktivoituvat testipisteet

Laitteen testipisteistä ei saatu odotettua 115 200 baudin nopeuksista UART-yhteyttä, joten on mahdollista, ettei sitä ole tuotu testipisteisiin. JTAG-yhteyden päälle kytkentä määritellään yhdellä järjestelmäpinnin kytkennällä, mutta sen tilaa on mahdotonta nähdä piirin ollessa kiinni piirilevyssä.

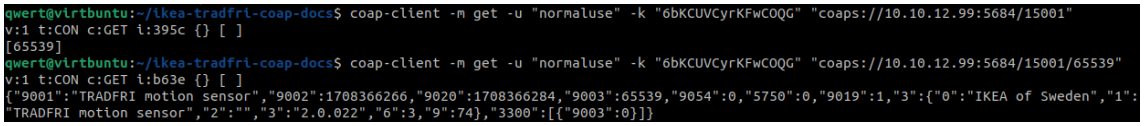
Koska laitteen tiedostojärjestelmään ei pääse piirilevyltä tai verkkoyhteyden kautta käsiksi, on vaihtoehtona irrottaa laitteen muistipiiri ja lukea se siihen tarkoitetulla lukijalla. Tämä toimenpide on riskialtis, koska piirin irrottamiseen käytetty lämpö voi vaurioittaa piiriä tai piirilevyä. Piiri on mahdollista juottaa lukemisen jälkeen takaisin piirilevylle ja saada laite takaisin toimimaan. Muistipiiri on myös mahdollista lukea kiinnitettynä piirilevylle, mutta se vaatii muutoksia piirilevyyn. Yksinkertaisinta on irrottaa flash-muistipiiri piirilevyltä ja lukea se SPI-väylää hyödyntäen siihen soveltuvalla laitteistolla.

Laitteeseen tallentuvia tietoja on mahdollista saada ulos myös verkkoyhteyden kautta. Hubin ja sovelluksen välinen tiedonsiirtoprotokolla on takaisinmallinnettu, ja sen avulla laitteen kanssa voi keskustella verkkoyhteyden välityksellä. Protokollan dokumentaatio löytyy avoimesta GitHub-palvelusta. (de Haan, 2024) Ennen tietojen lataamista hubilta, pitää coap-client -asiakasohjelmisto autentikoida. Tämä tapahtuu käyttämällä laitteen pohjassa olevaa Security Codea, jota käytetään matkapuhelinsovelluksen käyttöönotossa. Autentikointi palauttaa käyttäjälle luodun autentikointiavaimen, jota pitää käyttää laitteelle lähetetyissä komennoissa. Komento ja avain on nähtävillä kuvassa 23.

```
qwert@virtbuntu:~/ikea-tradfri-coap-docs$ coap-client -m post -u "Client_identity" -k "PuATQXbmPN1btwHY"
 -e "{\"9090\":\"normaluse\"}" "coaps://10.10.12.99:5684/15011/9063"
v:1 t:CON c:POST i:7f0d {} [ ]
{"9091":"6bKCUVCyrKFwCOQG","9029":"1.8.0025"}
```

KUVA 23 coap-clientin autentikointi

Autentikoinnin jälkeen hubilta voidaan pyytää listaus kaikista siihen yhdistetyistä laitteista. Jokaisesta laitteesta voi pyytää myös kaikki mahdolliset tiedot, kuten kuvassa 24 näkyy.



KUVA 24 Listaus laitteista ja tiedot liiketunnistimesta

Coap-client-ohjelmiston dokumentaation perusteella asiakasohjelmiston antamista tiedoista voidaan päätellä taulukon 5 mukaiset arvot.

TAULUKKO 5 Liiketunnistimen hubille tallentuneet tiedot

Numero	Selite	Arvo
3.0	Valmistaja	IKEA of Sweden
3.1	Tuote	TRADFRI motion sensor
3.3	Laiteohjelmiston versio	2.0.022
3.9	Pariston tila	74 (prosenttia)
5750	Laitteen tyyppi	0
9001	Laitteen nimi	TRADFRI motion sensor
9002	Hubiin yhdistämisaika	1708366266 (Epoch-aika)
9003	Laitteen id	65539
9020	Nähty viimeksi	1708366284 (Epoch-aika)
9019	Laitteen saavutettavuus	1 (saavutettavissa)

Taulukon 4 tiedoista voidaan nähdä, että liiketunnistin on liitetty laitteeseen 19.2.2024 klo 18.11.06, ja se on viimeksi nähty samana päivänä klo 18.11.24.

5.4 Ikea Dirigera Hub

Ikea Dirigera Hub tuli myyntiin elokuussa 2022, ja se korvasi aiemman Trådfri Gatewayn. Hubin laitteisto on huomattavasti kehittyneempää verrattuna aiempaan malliin, ja se on hieman kalliimpi. Toiminnoiltaan Dirigera Hub tarjoaa Zigbee-protokollan lisäksi tuen myös uudemmalle Thread-protokollalle.

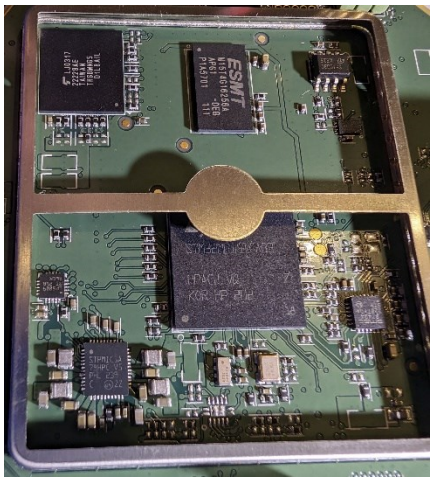
Dirigera Hub on fyysisesti pyöreä ja matala laite, jonka avaamiseen tarvitaan pientä torx-ruuvimeisseliä. Laitteen avaamisen jälkeen selviää, että piirilevy on kiinnitetty pohjaan kahdella pienellä Philips-ruuvilla. Laitetta tutkineet hakkerit ovat löytäneet siitä myös sarjaportin, jota voidaan käyttää laitteen tutkimiseen. (van der Wal, 2023) Järjestelmäpiirinä on STMicroelectronicsin STM32MP151C-järjestelmäpiiri ja Elite Semiconductor Memory Technologyn 4 Gbit M15T4G16256A DDR3 -muistipiiri. Tallennustilasta vastaa Toshiban 4GB THGBMNG5D1LBAIL. Laitteen piirilevyllä on myös UART-liitäntä (Wjtje, 2023).

Kuvasta 25 nähdään, että piirilevyyn kirjattu mallikoodi on E324220. Ulkoisessa koteloinnissa mallikoodi on E2003. Kuvaan on merkattu myös piirilevyltä löydetty sarjaportti, johon on juotettu piikkirima.

KUVA 25 Dirigera Hubin piirilevyn etu- ja takapuoli

Laitteen käynnistyessä sarjaportin kautta tulostuu sen käynnistymiseen liittyvää lokitietoa. Lokin perusteella voi päätellä laitteen olevan Linux-pohjainen. Sarjaportin kautta ei kuitenkaan pysty vaikuttamaan laitteen toimintaan millään tavalla, eikä esimerkiksi bootloaderiin pääse sitä kautta.

Piirilevyllä näkyvien testipisteiden liittäminen maahan ei keskeyttänyt käynnistymistä, mutta se sai aikaan lokiin rivin ” WARNING: FCONF: Invalid config id 26”. Yleinen tapa aiheuttaa vika käynnistyksen aikana on laittaa tallennustila oikosulkuun. Tällöin laite joutuu vikatilaan, eikä normaali käynnistys onnistu bootloaderia pidemmälle. Kuvan 26 vasemmassa yläkulmassa nähdään RF-suojan alla oleva eMMC-piiri.



KUVA 26 Piirilevy RF-suojan alta

Piiri on juotettu piirilevylle BGA-pallojen avulla, joten sen laittaminen oikosulkuun on mahdotonta irrottamatta sitä, ellei jotain sen liittimiä ole kytketty testipisteisiin.

Ikea Dirigera Hubin tiedonsiirtoprotokolla puhelimen kanssa viestimiseen on takaisinmallinnettu ja siihen on saatavilla esimerkiksi C#-, Java-, Typescript- sekä Python-kirjastot. Myös progressiivinen web-sovellus on kehitetty laitteen käyttöön, jolloin sitä voi käyttää helposti graafisella käyttöliittymällä ilman

matkapuhelinta. Laitteen tutkimiseen sopii parhaiten dirigera-niminen Python-kirjasto (Hilberg, 2024).

Python-kirjaston käyttö onnistuu komentoriviltä ja vaatii ainoastaan tietokoneen samaan lähiverkkoon sekä fyysisen pääsyn hubille. Dirigera-ohjelmiston pystyy asentamaan Pythonin pip-komennolla ”pip install dirigera”, sillä se on julkaistu pypi.org -sivustolla. Kirjaston asentamisen jälkeen käytössä on dirigera-niminen kirjasto sekä generate-token-skripti, jolla toteutetaan yhteyden autentikointi. Skriptille annetaan parametriksi hubin ip-osoite, jonka jälkeen painetaan hubin pohjassa olevaa toimintonappia. Skripti palauttaa autentikointiavaimen, jonka avulla hubia voidaan ohjata kirjaston funktioilla.

Autentikointiavaimen ja dirigera-kirjaston avulla voidaan tehdä yksinkertainen Python-skripti, joka tulostaa kaiken saatavilla olevan tiedon hubista.

```
import dirigera

dirigera_hub = dirigera.Hub(
   token="eyJhbGci-
OiJFUzI1NiIsInR5cCI6IkpXVCIImtpZCI6IjEzZGE5ZDUyY2QyZTA4YzBl
YTA3NWY2NTJiMmE3NDRkY2VmYWFkNzgyZjZjYzgxZTBmMTU2MDlhN2>
   ip_address="10.10.12.211"
)
print("Valot:")
print(dirigera_hub.get_lights())
print("Pistorasiat:")
print(dirigera_hub.get_outlets())
print("Ilmanpuhdistimet:")
print(dirigera_hub.get_air_purifiers())
print("Verhot:")
print(dirigera_hub.get_blinds())
print("Kaukosäätimet:")
print(dirigera_hub.get_controllers())
print("Sensorit:")
print(dirigera_hub.get_environment_sensors())
print("Scenet:")
print(dirigera_hub.get_scenes())
print("Liiketunnistimet:")
print(dirigera_hub.get_motion_sensors())
print("Ovitunnistimet:")
print(dirigera_hub.get_open_close_sensors())
```

Skripti tulostaa hubiin liitetyt laitteet kategorioittain listattuna.

```
Valot:
[Light(id='3dccbda0-6d67-4372-868a-833bd3dab79b_11',
type='light',           device_type='light',           cre-
ated_at=datetime.datetime(2024,   3,   5,   20,   58,   3,
tzinfo=TzInfo(UTC)),                    is_reachable=True,
last_seen=datetime.datetime(2024,   3,   6,   19,   18,   54,
```

```
tzinfo=TzInfo(UTC)),        attributes=LightAttributes(cus-
tom_name='', model='LTA001', manufacturer='Signify Nether-
lands  B.V.',  firmware_version='1.104.2',  hardware_ver-
sion='2', serial_number='00178801093BC59D', product_code='',
ota_status='upToDate',  ota_state='readyToCheck',  ota_pro-
gress=0,        ota_policy='autoUpdate',        ota_sched-
ule_start=datetime.time(0,          0),          ota_sched-
ule_end=datetime.time(0,                                0),
startup_on_off=<StartupEnum.START_ON:          'startOn'>,
is_on=True,    light_level=100,    color_temperature=2732,
color_temperature_min=6535,     color_temperature_max=2202,
color_hue=None, color_saturation=None), capabilities=Capa-
bilities(can_send=[],  can_receive=['customName',  'isOn',
'lightLevel', 'colorTemperature']), room=Room(id='29288e52-
a1a2-4ec9-b5a3-f7018e115700',      name='Living      room',
color='ikea_green_no_65', icon='rooms_sofa'), device_set=[],
remote_links=['85f8a173-6dfc-427a-b786-089e07157285_1'],
is_hidden=False, dirigera_client=<dirigera.hub.hub.Hub ob-
ject at 0x7f8751cfffd0>)]
Pistorasiat:
[]
Ilmanpuhdistimet:
[]
Verhot:
[]
Kaukosäätimet:
[]
Sensorit:
[]
Scenet:
[]
Liiketunnistimet:
[MotionSensor(id='85f8a173-6dfc-427a-b786-089e07157285_1',
type='sensor',       device_type='motionSensor',       cre-
ated_at=datetime.datetime(2024,   3,   5,   21,   33,   43,
tzinfo=TzInfo(UTC)),                    is_reachable=True,
last_seen=datetime.datetime(2024,   3,   6,   21,   3,   3,
tzinfo=TzInfo(UTC)), attributes=MotionSensorAttributes(cus-
tom_name='Sensor 1', model='TRADFRI motion sensor', manufac-
turer='IKEA  of  Sweden',  firmware_version='2.0.022',  hard-
ware_version='1',  serial_number='5C0272FFFEA282F9',  prod-
uct_code='E1745',  ota_status='upToDate',  ota_state='ready-
ToCheck',     ota_progress=0,     ota_policy='autoUpdate',
ota_schedule_start=datetime.time(0,     0),     ota_sched-
ule_end=datetime.time(0,     0),     battery_percentage=74,
is_on=False,    light_level=1.0),    capabilities=Capabili-
ties(can_send=['isOn', 'lightLevel'], can_receive=['custom-
Name']),             room=Room(id='29288e52-a1a2-4ec9-b5a3-
f7018e115700', name='Living room', color='ikea_green_no_65',
icon='rooms_sofa'),     device_set=[],     remote_links=[],
```

```
is_hidden=False, dirigera_client=<dirigera.hub.hub.Hub ob-
ject at 0x7f8751cfffd0>)]
Ovitunnistimet:
[]
```

Laitelistauksesta nähdään, että jokaisesta hubiin kytketystä laitteesta saadaan hyvin samankaltaisia tietoja kuin Ikean Trådfri Gatewaysta. Jokaisen laitteen valmistajakohtaisten tietojen lisäksi hubista saadaan hubiin liittämisajankohta, laitteelle annettu nimi, viimeisin saavutettavuusajankohta sekä laitteen tilatietoja. Lisäksi jokaisen laitteen kohdalla näkyy, mihin huoneeseen se on lisätty sekä huoneen sovelluskohtaisia tietoja. Esimerkiksi sovelluksessa näkyvän huoneen kuvituskuvan väri sekä taustakuva näkyvät tiedoissa.

Historiatietoja tai käyttötietoja ei rajapinnan kautta saa pyydettyä ainakaan julkisesti saatavilla olevien tunnettujen keinojen avulla.

6 TULOKSET JA ANALYYSI

Tässä luvussa käydään läpi edellisessä luvussa kuvatut tutkimukset neljälle eri kotiautomaatiohubille. Vaikka laitteet ovat toiminnallisuuksiltaan ja ulkoiselta olemukseltaan hyvin lähellä toisiaan, on niiden tutkimisessa jonkin verran eroa. Kaikkien laitteiden piireistä löytyy dokumentaatiot ja niiden perusteella jokaisen laitteen järjestelmäpiirissä on joko JTAG- tai UART-yhteys tai molemmat. Philipsin Hue Bridge, Lidlin Smart Home Gateway sekä Ikean Dirigera Hub mahdollistivat UART-yhteyden muodostamisen helposti. Kaikissa edellä mainituissa laitteissa oli selkeät piikkirimojen paikat, johon piikkiriman pystyi juottamaan. Sen sijaan Ikea Trådfri Gateway ei tarjonnut JTAG- eikä UART-yhteyttä, vaikka järjestelmäpiirin puolesta sellaiset olisivat olleet tarjolla. Jatkotutkimusaiheena kaikille hubeille on niiden muistipiirien tallentaman tiedon selvittäminen chip-off-tekniikalla. Tällöin saataisiin selville, onko tieto salatussa vai salaamattomassa muodossa muistipiirillä. Seuraavissa luvuissa käydään tarkemmin läpi laitteistokohtaiset tutkimustulokset sekä jatkotutkimusaiheet.

6.1 Philips Hue Bridge

Philipsin Hue Bridge -kotiautomaatiohubi on ollut markkinoilla laitteista pisimpään, ja se näkyy suoraan laitteelle tehtyjen skriptien ja takaisinmallinnukseen perustuvien projektien määrässä. Laitteen UART-yhteys on yleisesti tiedossa, ja pääkäyttäjän oikeuksien saaminen on hyvin dokumentoitu useilla sivustoilla.

Hue Bridgelle tallentuvat NVRAM-tiedostot muuttuvat välittömästi tehtyjen muutosten jälkeen, ja ne sijaitsevat laitteen flash-muistilla. Laitteen ottaminen irti virtalähteestä ei siten vaikuta niissä olevan tiedon säilyvyyteen. Jäljentämistä varten laitteen haltuun ottaminen onnistuu käyttämällä piirilevyltä löytyvää UART-väylää. Kun laitteelle aiheutetaan vikatila oikosulun avulla, päästään UART-väylän kautta laitteen bootloaderiin. Siellä voidaan määrittää laitteen pääkäyttäjän salasana uudelleen ja siten saada pääsy laitteelle. Tietosisällön

jäljentäminen onnistuu verkkoyhteyden kautta, joten laitteen sisältämän datan tutkinnassa ei sen suhteen ole ongelmaa.

Käyttömuistissa olevat väliaikaistiedostot /tmp-hakemistossa eivät vaikuttaneet muuttuvan millään tavalla, vaikka hubiin liitettyjen laitteiden tiloja vaihdeltiin. Kyseinen hakemisto vaikuttaa sisältävän järjestelmän käynnistyessä ladattavia konfiguraatiotiedostoja.

Aiemmin mainittujen NVRAM-tiedostojen sisällöistä oli selkokielisenä luettavissa muun muassa hubiin liitettyjen laitteiden nimiä sekä laitetta hallinnoivan matkapuhelimen nimi. Tiedostojen muu sisältö jäi tutkimusta tehtäessä selvittämättä, koska esimerkiksi lampun tilan muutos päältä pois sai aikaan useita muutoksia tiedostoissa. Tämän vuoksi tässä tutkimuksessa ei pystytty selvittämään, millä logiikalla laitteiden käyttö vaikuttaa NVRAM-tiedostoihin ja mitä tietoa niistä olisi saatavissa. Tiedostojen koko on erittäin pieni, ja tutkimuksen aikana niiden koko vaihteli ainoastaan muutaman tavun verran. Tämän perusteella voi päätellä, ettei tiedostoista löydy historiatietoja ainakaan kovin pitkältä ajalta. Sekä kyseisten tiedostojen toimintalogiikan että niihin tallentuneen tiedon selvittäminen on jatkotutkimusaihe.

Hubi tallentaa kaiken laitteiden käyttöön liittyvän tiedon suoraan flash-muistiin. Laitteen haltuunotossa virrat voi katkaista, jonka jälkeen laitteen voi jäljentää UART-yhteyden avulla. Tässä vaihtoehdossa on huomioitava järjestelmään tulevat muutokset haltuunotosta eteenpäin.

6.2 Lidl Smart Home Gateway

Lidl Smart Home Gateway on edullisuudellaan ja markettimyynnillään tarjonnut monelle ensimmäisen askeleen kotiautomaation polulle. Yhtenä syynä edullisuuteen on todennäköisesti sen pohjautuminen white label -valmistaja Tuyan tuotteisiin. Tuya tekee paljon erilaisia kotiautomaatiolaitteita useille tuotemerkeille, joten Lidlin tuotteet ovat jo julkaisuajankohtanaan päässeet todennäköisesti lastentaudeista yli. Hubin tutkimista helpottaa laaja hakkeriyhteisö, joka on selvittänyt monia laitteen tutkimiseen liittyviä ongelmia.

Laitteessa on UART-väylä, jota pitkin pääsee käsiksi bootloaderiin painamalla ESC-näppäintä. Bootloaderissa voidaan laitteen tallennustilasta lukea salattu AUSKEY sekä sen salausavain. Salauksen avaamiseen löytyy julkinen skripti, jonka jälkeen AUSKEY on tekstimuodossa. Laitteen root-käyttäjän salasana on AUSKEYn kahdeksan viimeistä merkkiä.

Kun laitteen pääkäyttäjän salasana on selvitetty, on laitteen jäljentäminen verkkoyhteyden kautta suoraviivaista. Laite tallentaa järjestelmälokia käyttömuistissa olevaan /tmp-hakemistoon, josta on nähtävissä kaikki käyttäjän tekemät muutokset hubiin liittyvien laitteiden toimintaan. Lokissa on aikaleima, joten käyttäjän toimintaa hubin kanssa voidaan selvittää useita päiviä tai viikkoja taaksepäin. Kun loki kasvaa noin kolmen megatavun kokoiseksi, se pakataan ja tallennetaan flash-muistille. Pakattujen lokitiedostojen määrää rajoittaa laitteen

tallennustila. Kun se tulee 95-prosenttisesti täyteen, vanhin pakattu lokitiedosto poistetaan.

Paras keino ottaa Lidl Smart Home Gateway haltuun on irrottaa siitä virtajohto ja jäljentää sen tietosisältö verkkoyhteyden yli. Mikäli halutaan tieto viimeisimmistä käyttäjän tekemisistä toimista hubille, kannattaa laitteesta irrottaa verkkoyhteys noin kahdeksaksi tunniksi. Tämä generoi noin kolme megatavua virheilmoituksia lokitiedostoon, jolloin se pakataan taas flash-muistille. Näin toimiessa viimeisimmät /tmp-kansiossa olevat lokitiedot eivät katoa virran katketessa.

Lidl Smart Home Gatewayn tapauksessa jatkotutkimusaihe olisi selvittää, tallentuvatko lokit samalla tavalla muillekin tuotemerkeille tehdyissä kotiautomaatiohubeissa. Tuyan kehittäjädokumentaatio viittaa tähän suuntaan, mutta hubin räätälöinnin vaihtoehtojen määrästä ei löydetty dokumentaatiota.

6.3 Ikea Trådfri Gateway

Ikean Trådfri Gateway on haastava laite tutkia. Siinä ei ole tunnistettuja JTAG- tai UART-yhteyksiä, eikä laitteen sisäisestä toiminnasta muutenkaan ole saatavilla dokumentaatiota tai tutkimuksia. Tutkimusten aikanakaan näitä ei paikallistettu, vaikka apuna oli erikoislaitteistoa. Laitteesta on saatavissa rajapintaa pitkin hieman laajemmat tiedot kuin mobiilisovelluksesta. Tämä tapahtuu käyttämällä jotakin useista julkisista työkaluista tietokoneella lähiverkkoyhteyttä hyödyntäen. Rajapinnan avulla saa selville esimerkiksi hubiin liitettyjen laitteiden käyttöönottohetken sekä viimeisen ajankohdan, jolloin hubi on keskustellut laitteen kanssa.

Hubin käyttämän järjestelmäpiirin tarjoamien JTAG- ja UART-yhteyksien selvittäminen esimerkiksi kolmiulotteisilla röntgenkuvilla on hyvä jatkotutkimusaihe. Koska järjestelmäpiirissä on tietty kontaktipiste, joka määrittää porttien päälläolon, näkisi röntgenillä otetuista kuvista, onko se kytketty vai ei.

Koska ei ole tietoa, tallentaako laite lokeja, voi laitteen irrottaa virtajohdosta ja tutkia siihen liitettyjen laitteiden aikaleimoja myöhemmin.

6.4 Ikea Dirigera Hub

Ikea Dirigera Hub on toinen haastava laite tutkittavaksi. Se on ollut markkinoilla tätä kirjoitettaessa noin puolitoista vuotta, mutta sen haltuunottoon ei ole saatavilla dokumentaatioita tai ohjeita hakkeriyhteisön suunnalta. Hubista on paikallistettu UART-yhteys, mutta sitä kautta ei ole toistaiseksi keksitty keinoa vaikuttaa sen toimintaan. Tutkimuksissakaan ei saatu yrityksistä huolimatta laitetta vikatilaan, jotta sen bootloaderiin pääsisi mahdollisesti käsiksi. Testipisteiden oikosulkuun laittaminen aiheuttaa vaan käynnistyksessä virheilmoituksen, minkä jälkeen laite käynnistyy normaalisti. Rajapintojen avulla saa Trådfri Gatewayn

tapaan tietoa hubiin liitetyistä laitteista käyttöönottohetken sekä viimeisimmän ajankohdan, jolloin hubi on keskustellut laitteen kanssa.

Jatkotutkimusaihe olisi pyrkiä saamaan laite vikatilaan, jotta UART-yhteyden kautta voisi yrittää pääsyä bootloaderiin.

6.5 Tulosten yhteenveto

Neljän kotiautomaatiohubin tutkimukset osoittivat, että Philips Hue Bridge ja Lidl Smart Home Gateway ovat helpoiten tutkittavia laitteita. Molempiin on saatavilla UART-väylän kautta pääkäyttäjän oikeudet, jos käyttää apuna julkisesta internetistä löytyvien hakkeriyhteisöjen ohjeita. Pääkäyttäjän oikeuksien avulla laitteiden toimintaa pääsee tarkkailemaan järjestelmätasolla. Philipsin laite tallentaa kaikista siihen kytketyistä laitteista jotakin toistaiseksi tuntematonta tietoa. Vähäisen tallennustilan käytön perusteella, siinä ei ole kytkettyjen laitteiden historiatietoja. Lidlin myymä laite on kiinalaisen Tuyan valmistama, ja se tallentaa ja arkistoi järjestelmälokia. Loki tallentuu käyttömuistiin, kunnes se on kolmen megatavun kokoinen. Tämän jälkeen se pakataan ja tallennetaan laitteen tallennustilaan. Laite arkistoi vanhat järjestelmälokit ja poistaa aina vanhimman, kun tallennustila täyttyy. Järjestelmälokista löytyvät sekä laitteen omien sovellusten viestit että käyttäjän tekemät toiminnot. Lokissa on myös tapahtumakohtaiset aikaleimat, mikäli laite on ollut kytkettynä julkiseen internettiin käynnistyessään. Laitteen haltuunotossa pitää päättää, haluaako viimeisimmät vai vanhimmat tapahtumat tutkittavaksi. Mikäli haluaa vanhimmat tapahtumat, kannattaa laitteesta ottaa virrat heti pois. Uusimmat tapahtumat tallentuvat flash-muistille vasta aiemmin mainitun rajan täyttyessä. Tutkimuksessa huomattiin, että laitteen ollessa päällä kahdeksan tuntia ilman verkkoyhteyttä, kyseinen raja täyttyi ja lokitiedosto arkistoitiin flash-muistille.

Ikea Trådfri Gateway ja Dirigera Hub ovat molemmat haastavia tutkittavia. Niiden tutkimisesta tai järjestelmään pääsystä ei ole saatavilla dokumentaatiota, eikä niistä havaittu tutkimuksissa käytössä olevia JTAG- tai UART-yhteyksiä. Molemmista laitteista on saatavissa vähän tietoa puhelinsovellusta varten tarkoitetun rajapinnan kautta, mutta hubeihin liitettyjen laitteiden historiatietoja niistä ei saa. Dirigera Hubissa on UART-liitäntä, mutta sieltä tulostuu ainoastaan laitteen käynnistyksen aikaisia viestejä. Kaikkien hubien muistipiirien tallentaman tiedon mahdollinen selvittäminen chip-off-tekniikalla on mielenkiintoinen jatkotutkimusaihe. Tutkimustulokset on esitetty yksinkertaistettuna kootusti taulukossa 6.

TAULUKKO 6 Tutkittujen laitteiden tutkimustuloksia

	Philips Hue Bridge	**Lidl Smart Home Gateway**	**Ikea Trådfri Gateway**	**Ikea Dirigera Hub**
UART-portti käytettävissä	X	X	-	X[1]
Pääkäyttäjän oikeudet saatavissa	X	X	-	-
Laitteen tallennustila jäljennettävissä	X	X	-	-
Laite tallentaa lokia	-	X	-[2]	-[2]

1. Portin kautta näkee ainoastaan käynnistyksen aikaisia tietoja, eikä se vastaanota syötettä.
2. Laitteen tiedostojärjestelmää ei pystytty tutkimaan, joten lokin olemassaoloa ei voida varmentaa.

Tutkimustulosten vertailua muihin laitteisiin liittyviin tutkimuksiin ei voitu tehdä, sillä julkaistuja tutkimuksia neljän tutkitun laitteen osalta ei löydetty.

7 YHTEENVETO

Tässä tutkimuksessa käsiteltiin kotiautomaatiojärjestelmien forensista tutkimista ja sen haasteita. Ensin tehtiin katsaus yleisimpiin kotiautomaatiohubeihin sekä niissä käytettäviin protokolliin. Yleisimmissä laitteissa käytetään yleensä tunnettuja Wi-Fi- tai Bluetooh-yhteyksiä ja lyhyen kantaman vähävirtaiseen kommunikaatioon tarkoitettuja ZigBee- tai Z-Wave-protokollia. Myös uusi tulokas Thread on yleistymässä.

Kotiautomaatiohubeihin kytkettävissä päätelaitteissa valikoima on todella laaja. ZigBee-laitteita on vähintään yli 5 000, ja Z-Wave-protokollaa käyttäviä laitteita yli 4 000. Lisäksi sertifioimattomat Wi-Fi- ja Bluetooth-laitteet kasvattavat erilaisten laitteiden kokonaismäärän useisiin tuhansiin.

Kotiautomaatiolaitteiden tutkimiselle on kehitetty erilaisia malleja, jotka noudattavat samaa kaavaa. Tutkijan asiantuntemus kotiautomaatiosta on tärkeässä roolissa, sillä ala on verrattain uusi. Normaali prosessi etenee löytämisen, jäljentämisen ja analysoimisen kautta löydösten esittämiseen. Vaikka ylätasolla kotiautomaatiojärjestelmien tutkiminen on määritetty selkeästi, on varsinaisen työn tekeminen haastavaa valmiiden ohjelmisto- ja laitteistoratkaisujen puuttuessa. Erilaisia tekniikoita laitteiden tutkimiseen on olemassa, mutta niiden käytöstä ei ole kunnollisia tutkimuksia. Laitteiden, ohjelmistojen ja parhaiden käytänteiden puute tulee olemaan ongelma kotiautomaatiolaitteiden lisääntyessä kodeissa ja työpaikoilla.

Laitteiden tutkimiselle on olemassa edellytykset, mutta niiden käyttöönotto vaatii paljon tutkimista ja suunnittelua. Tämän takia jokainen tapaus vaatii omaa lähestymistapaa riippuen kotiautomaatiojärjestelmän kokoonpanosta.

Tutkimuksen perustella ei ole mahdollista tehdä yleistä sääntöä kotiautomaatiohubien tallentaman tiedon määrän suhteen. Tutkittavista laitteista yksi tallensi tarkan lokin useiden päivien tai viikkojen ajalta. Toisesta laitteesta ei lokeja löydetty, ja kahden laitteen osalta niitä ei päästy tutkimaan järjestelmätasolta. Laitteiden haltuunoton suhteen on myös hankala tehdä yleistä sääntöä. Mikäli laite tallentaa tmpfs-tiedostojärjestelmään tai yleensäkin käyttömuistiin jotakin, virran katkaiseminen poistaa kaiken niihin tallentuneen tiedon. Tämän vuoksi

on erityisen tärkeää selvittää laitteen toimintalogiikka ennen kuin tutkittavaa laitetta käydään ottamaan haltuun.

Yhteinen jatkotutkimusaihe kaikille laitteille on tallennustilan tutkiminen chip-off-tekniikalla, jolloin tallennustila voidaan lukea ilman pelkoa tietojen muuttumisesta tutkittaessa. Laitteissa on myös tuntemattomassa muodossa tallentuvaa tietoa, jonka tutkiminen ja sisällön selvittäminen olisi toinen jatkotutkimusaihe.

Suurten valmistajien lisäksi markkinoilla on useita pienempiä kotiautomaatiohubien valmistajia, joiden tekemät ratkaisut eivät välttämättä ole lähelläkään muiden tekemiä ratkaisuja. Näiden laitteiden tutkiminen voi onnistua tässä tutkimuksessa luodulla artefaktilla, mutta laitevalikoiman heterogeenisyyden takia tätä on mahdotonta sanoa.

LÄHTEET

Apple. (15. 11 2020). *Set up HomePod, HomePod mini, or Apple TV as a home hub*. Noudettu osoitteesta Apple: https://support.apple.com/en-us/HT207057

arturo182. (31. 3 2017). *Ikea TRÅDFRI Gateway Teardown*. Noudettu osoitteesta Ifixit: https://www.ifixit.com/Teardown/Ikea+TR%C3%85DFRI+Gateway+Teardown/85936

Attify. (16. 6 2017). *Firmware Analysis for IoT Devices*. Noudettu osoitteesta Attify - Simplifying Security: https://medium.com/@attify/firmware-analysis-for-iot-devices-fb8df961c19d

Awasthi, A.;Read, H. O.;Xynos, K.;& Sutherland, I. (2018). Welcome pwn: Almond smart home hub forensics. *DFRWS 2018 USA*. Elsevier Ltd.

Banaru, A. (27. 03 2018). *Philips Hue 2.1 – Enabling WIFI*. Noudettu osoitteesta IoT Blog: https://blog.andreibanaru.ro/2018/03/27/philips-hue-2-1-enabling-wifi/

Brown, N. (09. 11 2023). *Overlay Filesystem*. Noudettu osoitteesta The Linux Kernel: https://docs.kernel.org/filesystems/overlayfs.html

Connectivity Standards Alliance. (24. 1 2023). *Introducing Zigbee Direct, Simplifying Integration with Bluetooth Low Energy Devices*. Noudettu osoitteesta Connectivity Standards Alliance: https://csa-iot.org/newsroom/the-connectivity-standards-alliance-introduces-zigbee-direct-simplifying-integration-with-bluetooth-low-energy-devices/

de Haan, G. (21. 1 2024). *Ikea Tradfri CoAP Docs*. Noudettu osoitteesta Github: https://github.com/glenndehaan/ikea-tradfri-coap-docs

Erlich, D. (2008, 1218). *Sigma Designs Buying Smart Network Chipmaker Zensys*. From Gigaom: https://gigaom.com/2008/12/18/sigma-designs-buying-smart-network-chipmaker-zensys/

Gislason, D. (2008). *Zigbee Wireless Networking.* Elsevier Inc.

Google. (09. 11 2023). *How Google products use Thread*. Noudettu osoitteesta https://support.google.com/googlenest/answer/9249088

Goudbeek, A.;Choo, K.-K. R.;& Le-Khac, N.-A. (2018). A Forensic Investigation Framework for Smart Home. *TrustCom/BigDataSE.2018.00201*.

Graceful, H. (03. 07 2023). *Extracting Flash Memory over SPI*. Noudettu osoitteesta Akimbo Testing: https://akimbocore.com/article/extracting-flash-memory-over-spi/

Grand Idea Studio. (19. 2 2024). *JTAGulator®*. Noudettu osoitteesta Grand Idea Studio: https://grandideastudio.com/portfolio/security/jtagulator/

Hevner, A.;& Chatterjee, S. (2010). *Design Research in Information Systems.* New York: Springer Science+Business Media.

Hilberg, N. (25. 02 2024). *Leggin/dirigera: This repository provides an unofficial Python client for controlling the IKEA Dirigera Smart Home Hub.* Noudettu osoitteesta Github: https://github.com/Leggin/dirigera

Himberg, K. (2002). *Tekninen rikostutkinta - Johdatus forensiseen tieteeseen.* Helsinki: Edita Oyj.

Hutchinson, S.;Han Yoon, Y.;Shantaram, N.;& Karabiyik, U. (2020). Internet of Things Forensics in Smart Homes: Design, Implementation, and Analysis of Smart Home Laboratory. *2020 ASEE Virtual Annual Conference Content Access.*

Håkansson, P.;& Loska, K. (14. 10 2020). Introduction to Thread. Nordic Semiconductor.

Ikea. (28. 3 2017). *IKEA launches its first digital home furnishing product*. Noudettu osoitteesta Ikea: https://www.ikea.com/global/en/newsroom/innovation/ikea-launches-its-first-digital-home-furnishing-product--an-app-to-adjust-lighting-170328/

Ikea. (29. 10 2023a). *Voinko ohjata IKEA-älykotia äänelläni?* Noudettu osoitteesta Ikea: https://www.ikea.com/fi/fi/customer-service/knowledge/articles/c05db4g6-341d-42f5-9c09-23g15f024370.html

IKEA. (09. 11 2023b). *Is it possible to add smart products from other brands to the IKEA Home smart app?* Noudettu osoitteesta IKEA: https://www.ikea.com/gb/en/customer-service/knowledge/articles/7g6702ff-91fe-468g-8ee9-9e74b885540f.html

Interpol. (24. 03 2024). *Digital forensics*. Noudettu osoitteesta Interpol: https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics

Kaushik, K.;Bhardwaj, A.;& Dahiya, S. (2023). Smart Home IoT Forensics: Current Status, Challenges, and Future Directions. *2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, 716-721.

Kemppi, J. (3. 12 2020). *Testissä Lidlin uusi älykotisarja – tällaiset ovat 70 euron älyvalot*. Noudettu osoitteesta Iltalehti: https://www.iltalehti.fi/digitestit/a/6dabc9ab-0b1e-4b0a-a2e1-e08130aa74ee

Kim, S.;Park, M.;Lee, S.;& Kim, J. (2020). Smart Home Forensics—Data Analysis of IoT Devices. *Electronics*, 13.

Kävrestad, J. (2018). *Fundamentals of Digital Forensics*. Skövde: Springer International Publishing AG.

McKemmish, R. (1999). What is Forensic Computing? *Australian Institute of Criminology: Trends and Issues in Crime and Justice*, 1-6.

Mikhaylov, I.;& Skulkin, O. (09. 11 2023). *Chip-off technique in mobile forensics*. Noudettu osoitteesta Digital Forensics Corp: https://www.digitalforensics.com/blog/articles/chip-off-technique-in-mobile-forensics/

Nordic Semiconductor. (09. 11 2023). *nRF Sniffer for 802.15.4*. Noudettu osoitteesta Nordic Semiconductor: https://www.nordicsemi.com/Products/Development-tools/nrf-sniffer-for-802154

NXP. (26. 08 2016). *ZigBee 3.0–Facilitating the Internet of Things.* Noudettu osoitteesta NXP: https://www.nxp.com/docs/en/brochure/75017677.pdf

Ochs, S. (2. 6 2014). *Apple's HomeKit will bring smart home control to iOS 8*. Noudettu osoitteesta Macworld: https://www.macworld.com/article/223505/apples-homekit-will-bring-smart-home-control-to-ios-8.html

Onekey. (31. 3 2023). *onekey-sec/jefferson: JFFS2 filesystem extraction tool*. Noudettu osoitteesta Github: https://github.com/onekey-sec/jefferson/

OpenSSH. (09. 11 2023). *OpenSSH Legacy Options*. Noudettu osoitteesta OpenSSH: https://www.openssh.com/legacy.html

Peffers, K.;Marcus, R. A.;& Tuunanen, T. (2007). A design science research methodology for information systems. *Journal of Management Information Systems*, 45–77.

Philips. (29. 10 2023a). *Zigbee 3.0 support in Hue ecosystem*. Noudettu osoitteesta Philips Hue Developer Program: https://developers.meethue.com/zigbee-3-0-support-in-hue-ecosystem/

Philips. (09. 11 2023b). *Hue Hardware FAQs*. Noudettu osoitteesta Philips Hue: https://www.philips-hue.com/en-us/support/faq/hardware-and-connectivity#I_am_unable_to_control_my_light_when_I_am_away_from_home_

Philips Hue. (1. 8 2023a). *Philips Hue*. Noudettu osoitteesta Top tips for using Philips Hue motion sensors: https://www.philips-hue.com/en-us/explore-hue/blog/motion-detection-lighting

Prospero, M. (26. 10 2023). *The best smart home hubs of 2023*. Noudettu osoitteesta tom's guide: https://www.tomsguide.com/us/best-smart-home-hubs,review-3200.html

Sathwara, S.;Dutta, N.;& Pricop, E. (2018). ECAI 2018 - International Conference – 10th Edition. *IoT Forensic A digital investigation framework for IoT systems*, (ss. 1-4). Iasi.

Seger, R. X. (16. 8 2016). *Enabling the hidden Wi-Fi radio on the Philips Hue Bridge 2.0: Adventures with 802.11n, ZigBee 802.15.4 and OpenWrt*. Noudettu osoitteesta Medium: https://medium.com/@rxseger/enabling-the-hidden-wi-fi-radio-on-the-philips-hue-bridge-2-0-42949f0154e1

Servida, F.;& Casey, E. (2019). IoT forensic challenges and opportunities for digital traces. *Digital Investigation 28*, 22-29.

SmartThings. (19. 10 2023a). *SmartThings Enabled Hubs*. Noudettu osoitteesta Smartthings: https://support.smartthings.com/hc/en-us/articles/360052390151-SmartThings-Enabled-Hubs

SmartThings. (09. 11 2023b). *Works with SmartThings List*. Noudettu osoitteesta SmartThings: https://www.smartthings.com/supported-devices

Statista. (23. 10 2023). *Smart Home*. Noudettu osoitteesta Statista: https://www.statista.com/outlook/dmo/smart-home/worldwide#smart-homes

Suomäki, J.;& Vepsäläinen, S. (2013). *Talotekniikan automaatio - Käyttäjän opas.* Kiinteistöalan Kustannus oy ja kirjailijat.

Teschler, L. (29. 12 2022). *Teardown: Amazon 4th generation Echo Dot*. Noudettu osoitteesta Microcontroller tips: https://www.microcontrollertips.com/teardown-amazon-4th-generation-echo-dot-faq/

Tilley, A. (14. 8 2013). *Samsung Acquires SmartThings, A Fast-Growing Home Automation Startup*. Noudettu osoitteesta Forbes: https://www.forbes.com/sites/aarontilley/2014/08/14/samsung-smartthings-acquisition-2/

Tuya. (09. 11 2023a). *Building a new IoT retail channel with lower prices, IoT-enabled products, and enhanced experience.* Noudettu osoitteesta Tuya: https://www.tuya.com/developer-stories/lidl

Tuya. (09. 11 2023b). *Tuya*. Noudettu osoitteesta Why choose Tuya Smart: https://www.tuya.com/about

ukl. (25. 11 2019). *Philips Hue Bridge v2.1*. Noudettu osoitteesta ukl's blog: https://blog.kleine-koenig.org/ukl/philips-hue-bridge-v21.html

van der Wal, W. (19. 02 2023). *General information about the next generation Ikea smart home hub, DIRIGERA*. Noudettu osoitteesta Github: https://github.com/wjtje/DIRIGERA

Westervelt, A. (12. 3 2012). *Could Smart Homes Keep People Healthy?* Noudettu osoitteesta Forbes:

https://www.forbes.com/sites/amywestervelt/2012/03/21/could-smart-homes-keep-people-healthy/#73991a0b579a

Willadsen, K. (09. 11 2023). *Meld Visual diff and merge tool*. Noudettu osoitteesta Meld: https://meldmerge.org/#features

Wilmshurst, T. (2017). *Fast and Effective Embedded Systems Design (Second Edition)*. Elsevier inc.

Wjtje. (29. 10 2023). *Dirigera*. Noudettu osoitteesta Github: https://github.com/wjtje/DIRIGERA

Zahariadis, T. B. (2003). *Home Networking Technologies and Standards.* Boston: Artech House, Inc.

ZigBee Alliance. (29. 10 2023). *About Us*. Noudettu osoitteesta ZigBee Alliance: https://zigbeealliance.org/about/

Z-Wave Alliance. (29. 10 2023a). *Markets & Use Cases*. Noudettu osoitteesta Z-Wave Alliance: https://z-wavealliance.org/z-wave-markets-and-cases/

Z-Wave Alliance. (29. 10 2023b). *Z-Wave Certification: The Key To Interoperability*. Noudettu osoitteesta Z-Wave Alliancee: https://z-wavealliance.org/interoperability/

Z-Wave Alliance. (29. 10 2023c). *What is Z-Wave Long Range and How Does it Differ from Z-Wave?* Noudettu osoitteesta Z-Wave Alliance: https://z-wavealliance.org/what-is-z-wave-long-range-and-how-does-it-differ-from-z-wave/