DFRWS IoT Challenge

The report summarizes findings gathered during analysis of evidence given as part of the DFRWS IoT Forensics Challenge 2018.

Summary of investigations

The following key facts were identified during the investigation:

- The victim was having an affair with man named John Macron, which she ended just before the crime
- The man was on the spot in the time of crime
- Events recorded by the sensors at bedroom door suggest movements in the room at the time of murder (15:13 - 15:20)
- Voice recording identify quarrel in the of crime
- There were inaccuracies identified in the victim's husband's interrogation (he was rather listening to music then watching a movie, he probably was acquainted with other people - according to conversations in Alexa recordings).

Timeline

All times relate to Monday 17 July 2017, in KST (GMT +9).

- 15:03:45 - 15:05:40 - a Google Talk chat between the victim (Betty Hallym) and John Macron (supposed to be her lover). Betty dissolves the relationship, leaving John in angry mood.
- 15:03 - 15:19 - playing media on the TV set
- 15:12 - a quarrel recorded between Betty and John on the spot
- 15:13 - Event from door sensor, John entering the bedroom of victim
- 15:13:02 - Betty switches off music (Alexa)
- 15:20 - John leaves the room at (door sensor + audio recording from Alexa)
- 15:31 - the police department receives the alert call

Evaluating and Expressing Conclusions

According to collected evidence, we suppose that the third man, known as John Macron, is suspicious of murdering the victim. He had a motive (tough breakup with victim) and we found more evidence against him than against the husband.

Evidence against **John (lover):**

- Found harsh messages from John in victims phone after the sudden end of their affair
- Audio recordings of further fights at victims home short before the murder
- Executed bedroom door sensors inside victims home two times in 7 minutes right before the murder was reported - in this time windows there was a fight between him and the victim, according to recordings from alexa.

Evidence against **Simon (husband):**

- Lied about watching a movie - he was in fact listening to music, but it can be only a mistake in simulated data

Possible scenario of murder:

- John and victim having fight over messages (evidence **002)**
- John arrives at victims house
- John enters the bedroom of victim at 15:13 (door sensor(evidence **006**)
- Fighting (vocally) with victim (audio recording from Alexa (evidence **005**)
- Murder
- John leaves the bedroom at 15:20 (door sensor (**006**) + audio recording from Alexa(evidence **005**))

More details about the analysis of devices and network traces are described below.

Forensics analysis of gathered evidence

001 SmartTV-RaspberryPi

The device was used as a home media center connected to the TV set. The evidence handed for the investigation contained an image of the memory card used by the device. Analysis of the storage revealed two partition tables (boot and system) that were examined further. The analysis focused on identifying files on the filesystem, which were subject to operations in the given time frame.
Extraction of filesystem metadata from both the partition tables made it possible to establish a timeline listing files touched in the period. The list of files indicated only activity related to using the OSMC media application and working with its internal database files (stored as SQLite files). The contents of the database revealed two YouToube video clips that were played in the time frame:

- https://www.youtube.com/watch?v=ibOskbTPZYE (15:03 - 15:07)
- https://www.youtube.com/watch?v=VKfbVLmkQUs (15:07 - 15:19)

002 BettyNote2Black

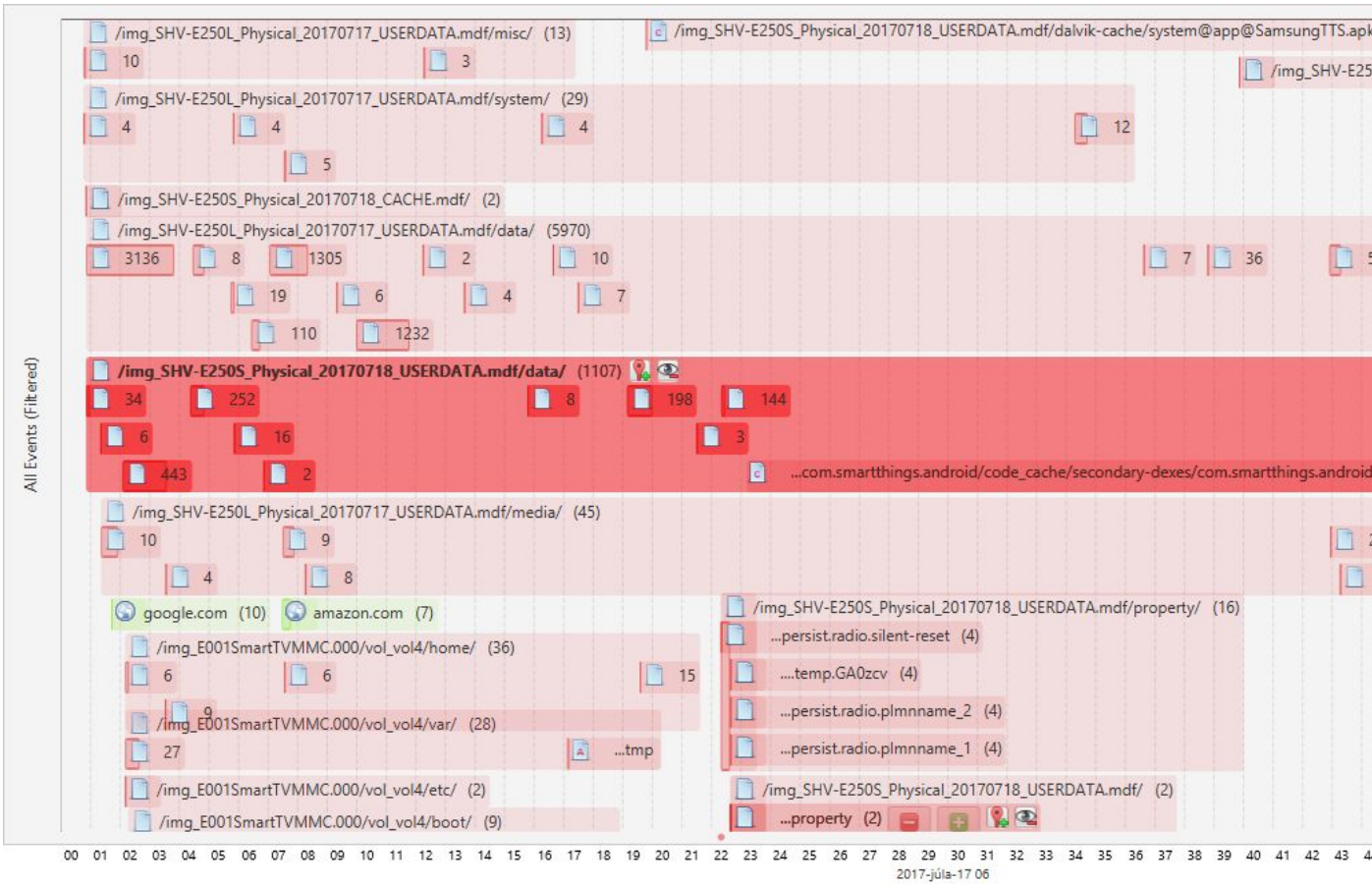
The evidence contained dumps of several partition tables containing images of the phone system. Similarly to the analysis of the 001 device, the partitions were examined to establish a timeline and identify files that could be affected during the time frame specified.
Additional file analysis revealed Google Talk history with possibly relevant conversation that finished just before the event.
Mon, 17 Jul 2017 13:39:08*John:* ;)
Mon, 17 Jul 2017 13:41:54*John:* How are you?
Mon, 17 Jul 2017 13:43:21***Betty:* Hey. Better now ;)
Mon, 17 Jul 2017 13:47:12***John:* Ugh. Work sucks
Mon, 17 Jul 2017 13:47:17***John:* I wanna see you later
Mon, 17 Jul 2017 15:03:45***Betty:* I cant keep doing this
Mon, 17 Jul 2017 15:04:12***John:* It's too late now! U promised

Mon, 17 Jul 2017 15:04:18***Betty:* Evwryone suspectbs
Mon, 17 Jul 2017 15:04:36***Betty:* It feels like they are warching us
Mon, 17 Jul 2017 15:04:45***John:* You're just paranoid....
Mon, 17 Jul 2017 15:05:09***Betty:* I cannot take it anymore
Mon, 17 Jul 2017 15:05:22***John:* ...
Mon, 17 Jul 2017 15:05:25***Betty:* Its over dont msg me
Mon, 17 Jul 2017 15:05:40***John:* Who the fuck do you think k you are!

Analysis of the address book yielded a full name “John Macron” linked to the other chat participant. The account was found to be blocked.
In addition to these findings, a large number of files were modified or accessed on the filesystem, most of which was outcome of common operations. All the activities were performed on the userdata partition, the rest of examined partitions did not show any changes in the time window.

003 SimonNote2Black

We used Autopsy 4.5 to look at contents of Simon’s phone. We didn’t find any web browsing history or cookies on this phone from day of murder (17.07.), which is not usual. While looking at timeline of changes we found out that .dex executables of SmartThings app were changed at 15:19 and 15:23 respectively. There are also some quite massive changes in filesystem between 15:19 and 15:23. All of this can be seen in attached timeline form Autopsy - time window of timeline is 15:00-16:00. Simon’s phone is SHV-E250S.



The device contained an application to control the IoT equipment in the household. While it was possible to retrieve a database with recorded events related to the control of the IoT SmartThing Hub, it was not possible to identify any event that would be linked to the investigation.

004 Onhub-diagnostics-report

OnHub acted as the border router interconnecting local devices in the home network and providing the gateway to the Internet.

The device hosts several network interfaces - fixed Ethernet ports and WiFi (2.4MHz and 5MHz). The device was configured to offer two WiFi networks (HOME and HOME_GUEST). All the interfaces were assigned MAC addresses prefixed with F4:F2:6D, which is governed by TPLink (the vendor of network equipement for Google OnHub).

The device operates two L3 local networks:
192.168.86.0/24 (connected via 'br-lan' bridge that links together local Ethernet and wlan interfaces)
192.168.87.0/24 (connected via 'br-guest' linking wlan-guest* interfaces)

It seems the network configuration spans several L2 networks making it possible to access the network seamlessly via wired and wireless connections.

(no IPv6 configuration was detected in the setup).

The device's external address was 192.168.165.9 (assigned via DHCP), with 192.168.165.1 acting as the gw on the ISP side. The MAC address of the external device was 909f33000025.

Based on analysis of ARP records and DHCP logs that are available, it was possible to detect several devices available on the local network:

"Amazon Technologies Inc." (MAC: a002dc000020 []) 192.168.86.21
"Liteon Technology Corporation" (MAC: 2016d800001f [ademanafe]) 192.168.1.167,192.168.86.29,192.168.87.20
"Nest Labs Inc." (MAC: 18b430000021 [**********XDU]) 192.168.86.22
"Physical Graph Corporation" (MAC: d052a8000023 [st-**********]) 192.168.86.27
"Raspberry Pi Foundation" (MAC: b827eb000028 [osmc]) 192.168.86.25
"Samsung Electronics Co.,Ltd" (MAC: 109266000026 [android-**********]) 192.168.86.28
"Samsung Electronics Co.,Ltd" (MAC: 1caf05000022 [android-**********]) 192.168.86.24
"Samsung Electronics Co.,Ltd" (MAC: 50f520000027 [android-**********]) 192.168.86.20,192.168.86.26

All these devices got their IP addresses from the DHCP server, no other device was detected in ARP records (but the ISP gw).

The DHCP logs provided the following timeline of activity (times in local timezone, i.e UTC+9):

2017-07-16 16:05:26+09:00 192.168.86.22 ("Nest Labs Inc.")
2017-07-16 17:18:49+09:00 192.168.86.25 ("Raspberry Pi Foundation")
2017-07-16 17:23:44+09:00 192.168.86.21 ("Amazon Technologies Inc.")
2017-07-16 17:39:26+09:00 192.168.86.27 ("Physical Graph Corporation")
2017-07-16 20:11:46+09:00 192.168.86.21 ("Amazon Technologies Inc.")
2017-07-16 20:24:32+09:00 192.168.86.21 ("Amazon Technologies Inc.")
2017-07-17 02:39:06+09:00 192.168.86.24 ("Samsung Electronics Co.,Ltd")
2017-07-17 02:57:10+09:00 192.168.86.26 ("Samsung Electronics Co.,Ltd")
2017-07-17 04:05:26+09:00 192.168.86.22 ("Nest Labs Inc.")
2017-07-17 05:18:50+09:00 192.168.86.25 ("Raspberry Pi Foundation")
2017-07-17 05:39:24+09:00 192.168.86.27 ("Physical Graph Corporation")
2017-07-17 08:24:32+09:00 192.168.86.21 ("Amazon Technologies Inc.")
2017-07-17 13:41:30+09:00 192.168.86.28 ("Samsung Electronics Co.,Ltd")
2017-07-17 14:11:50+09:00 192.168.86.24 ("Samsung Electronics Co.,Ltd")
2017-07-17 14:16:14+09:00 192.168.86.21 ("Amazon Technologies Inc.")
2017-07-17 14:25:54+09:00 192.168.86.22 ("Nest Labs Inc.")
2017-07-17 15:00:45+09:00 192.168.86.26 ("Samsung Electronics Co.,Ltd")
2017-07-17 15:00:47+09:00 192.168.86.24 ("Samsung Electronics Co.,Ltd")
2017-07-17 15:02:05+09:00 192.168.86.25 ("Raspberry Pi Foundation")
2017-07-17 15:11:55+09:00 192.168.86.28 ("Samsung Electronics Co.,Ltd")
2017-07-17 16:28:00+09:00 192.168.86.29 ("Liteon Technology Corporation")

Having correlated the figures with the police reports, one can see device with 192.168.86.29 (Liteon Technology Corporation) that first appeared after the police was called in. We suppose it's a device used by the investigator to acquire the forensics data.

Based on the appearance of personal devices we can estimate presence of people in the flat:

192.168.86.24:
2017-07-17 02:39:06+09:00
2017-07-17 14:11:50+09:00
2017-07-17 15:00:47+09:00

192.168.86.26:
2017-07-17 02:57:10+09:00
2017-07-17 15:00:45+09:00

192.168.86.28:
2017-07-17 13:41:30+09:00
2017-07-17 15:11:55+09:00

N.B. - one of them is assigned to the Samsung Smartthing Hub (?), that doesn't move!

We can also see logs started to appear on 2017-07-17 13:41:30+09:00 (after a break, probably with people being at work (it was Monday)), to 2017-07-17 15:11:55+09:00. The incident is supposed to have occured in that window.

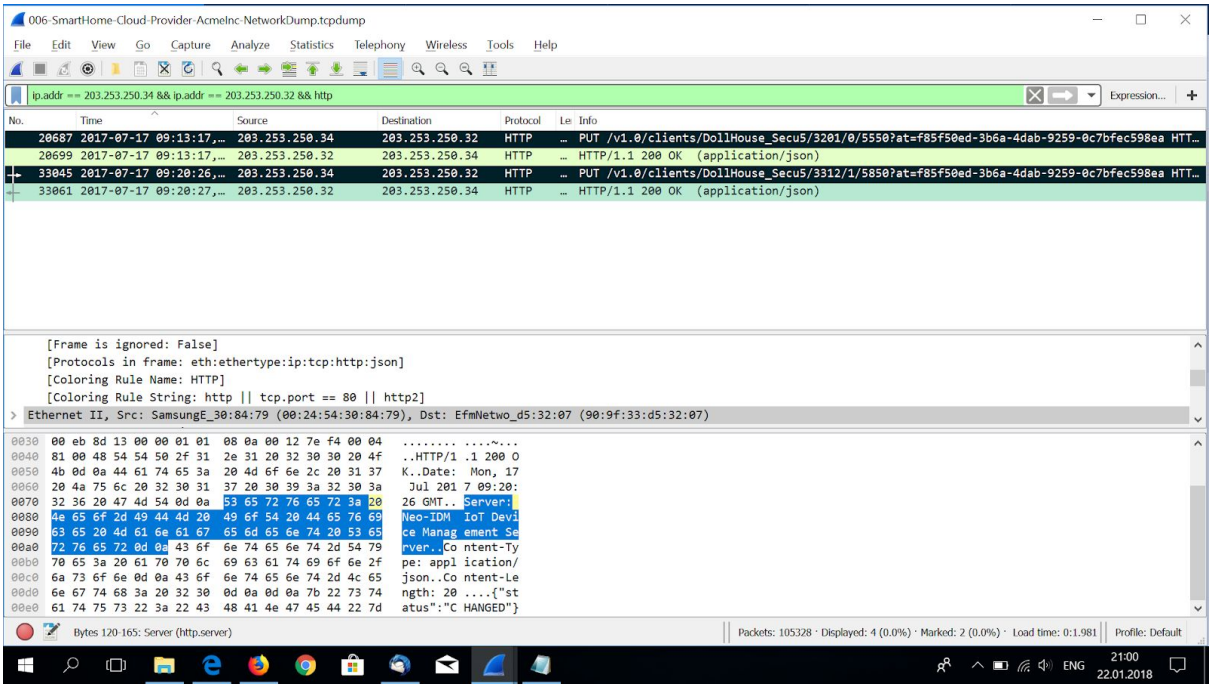
005 Amazon Echo Alexa Web Scrape

The evidence is composed of a number of voice recording and other media material stored by the device. The transcription of most relevant findings are quoted below

- There is a third man, not husband Simon, whose voice is recorded on Alexi. It is probably **John,** the man the victim had an affair with.
- (14.wav) John is heard on Alexi recording at 9:59 local time
- John is heard at 15:12 **I cant believe you would do this to me, we said we would, what are you thinking**
- (08.wav) John is shouting at 15:12:39 **How could you do this**
- (06.wav) 15:13:02 Victim turns off music (Alexa stop).
- (04.wav) 15:20:07 John enters the room (door closing) and says **Alexa Turn of TV**

006 SmartHome Cloud Provider Network Dump

Packet capture spans from 15:00:09 to 15:57:58 local time (according to NTP servers responses found).



In the screenshot above there are two HTTP PUT requests visible with few interesting parameters:

- URI contains name of the application **DollHouse_Secu**, indicating a security system
- Response Server name is **Neo-IDM IoT Device Management Server**, which is a server for managing IoT devices and sensors

- Both URIs contain parameter **at=f85f50ed-3b6a-4dab-9259-0c7bfec598ea**, indicating that it is the same device. Together with evidence from Alexa we know, that this must be ID specifying **bedroom door sensor** (audio capture of closing door + same second HTTP PUT request)
- In time **T (15:13:17)** there is a request to this management server with URL parameter **0**, which may indicate turning off or executing of IoT sensor (door?). Response says **status: CHANGED**, so the command was executed successfully.
- In time **T+7minutes (15:20:26)** there is a request with same (probably) device ID with parameter **1**, indicating turning on of IoT sensor.
- This may mean that someone entered the room at time **T** (see above) and left the room at time **T+7minutes.** We know, that the one who left the room was John, so he must have also entered the room before (= not the husband)

These time windows (when the sensor was down) together with the fight between victim and John (happening just before) indicates the **time of murder.**

- Request origin IP address: **203.253.250.34 (90:9f:33:d5:32:07)**
- Response address **203.253.250.32** seems to be the **public IP** of the home **router** of the victim, so the IoT management server is located inside the home network of the victim.
- Both addresses are geolocated in South Korea
- Both addresses communicate a lot on TCP. Address **203.253.250.32** is pushing (TCP PSH, ACK) the state information of the *Dollhouse_secu* and *Dollhouse_reader* devices to address **203.253.250.34**. Also, there is a strong **CoAP** communication between them.

Other interesting info from packet capture:

- **15:38:07:** IP address **203.253.250.32(00:24:54:30:84:79)** is downloading **rkhunter** (rootkit hunter)
- This might indicate someone in the home network is being suspicious about having an **infected device**. Device was downloading information about *bad_programs, backdoorports and suspscan.*

Techniques and tooling

Solely open source tools were used to analyse the evidence. To perform specific forensics task the Sleuthkit toolset was utilized. Commands like mmls, fls and mactime were used to obtain information about partitions and generating filesystem timelines. The Autopsy application was used to more detailed examination of filesystems given. The pcap dumps were analysed using Wireshark. The Onhub-diagnostics-report was decoded using tool https://github.com/benmanns/onhub, which produced a JSON file that was in turn processed using a custom Python script (enclosed to the submission).

Authors

Dávid Kosť, Daniel Kouřil, Benjamin Král, Ivo Nutár
CSIRT-MU
Institute of Computer Science
Masaryk University
Botanická 554/68a
602 00 Brno
Czech Republic