



Internet of Things Forensics

Jonathan T Rajewski

Director – Senator Patrick Leahy Center for Digital Investigation

Associate Professor – Champlain College



Overview

Internet of Things Forensics

- We will cover a lot of devices today
- This will be a “learning lab”



If you want to play along --

PLEASE INSTALL THE FOLLOWING TOOLS

Sqlitebrowser - <http://sqlitebrowser.org/>

Google Chrome – install the following apps

chrome://apps/

JSON Editor Online

JSON Editor Online

XML Tree



XML Tree
alan.stroop

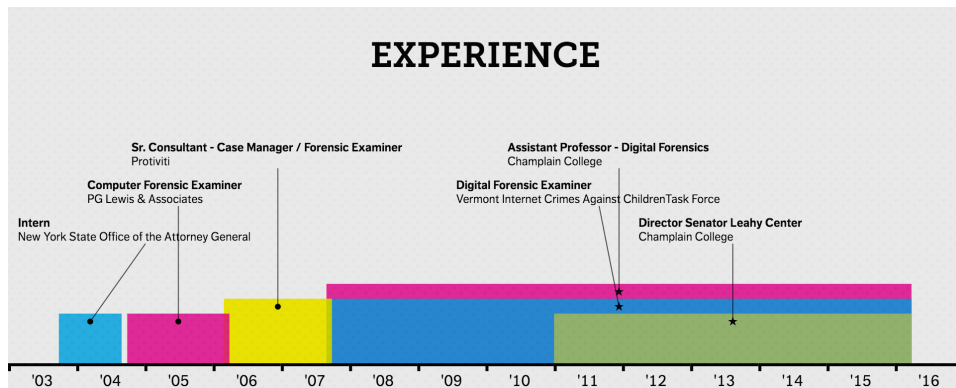
Displays XML data in a user friendly way.

Jonathan Rajewski

Speaker

@jtrajewski

EXPERIENCE



Professional Certifications

EnCe, CCE, CISSP, CFE

Professional Associations

Board Chair - BTV Ignite, DFCB – Digital Forensic Certified Practitioner “Founder”, CDFS - Consortium of Digital Forensic Specialists, ISFCE – International Society of Forensic Computer Examiners, ACFE – Association of Certified Fraud Examiners, HTCC – High Tech Crime Consortium

Recent Awards/Recognition

2014 US Ignite Application Summit Best Public Safety Application

2014 Honored by FBI director James B. Comey

2013 4 under 40 - Hilbert College

2013 C. Bader Brouillette Alumni Leadership Award - Champlain College

2012 Top Digital Forensic Professor – Digital Forensics - Princeton Review

2012 Best 300 Professors in the United States - Princeton Review

2011 Digital Forensic Examiner of the Year - Forensic 4cast Awards

Overview



"Behind this glass is incredible talent and this country in general and the FBI in particular needs those folks,"

*-FBI Director
James Comey*

LCDI Research Assistants

A Special Thank You to our student research teams (Echo and Iot)

Christopher Antonovich

Jason Ehlers

Matthew Lantange

Mary Braden Murphy

Tyler Nettleton

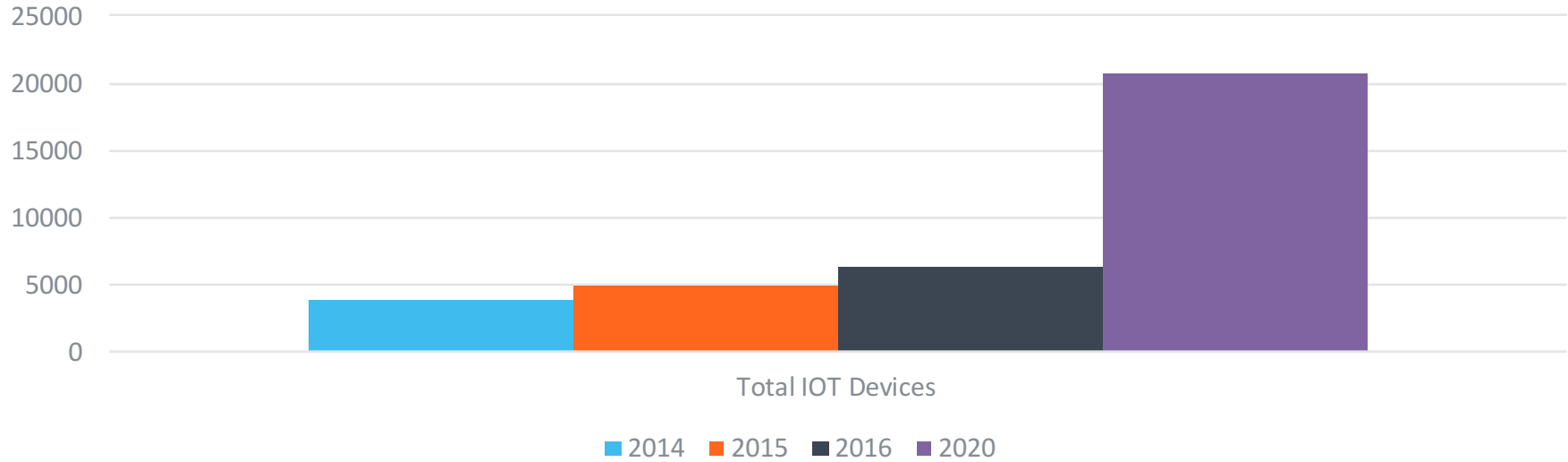
Zachary Reichert

Emily Shelton

Kelsey Ward

What is the Internet of Things?

IoT Devices



Gartner (November 2015)
<http://www.gartner.com/newsroom/id/3165317>

Master Title

Google Home

Always on call.

Google Home is a voice-activated home product that allows you and your family to get answers from Google, stream music, and manage everyday tasks.

Please send me the latest updates about Google Home.

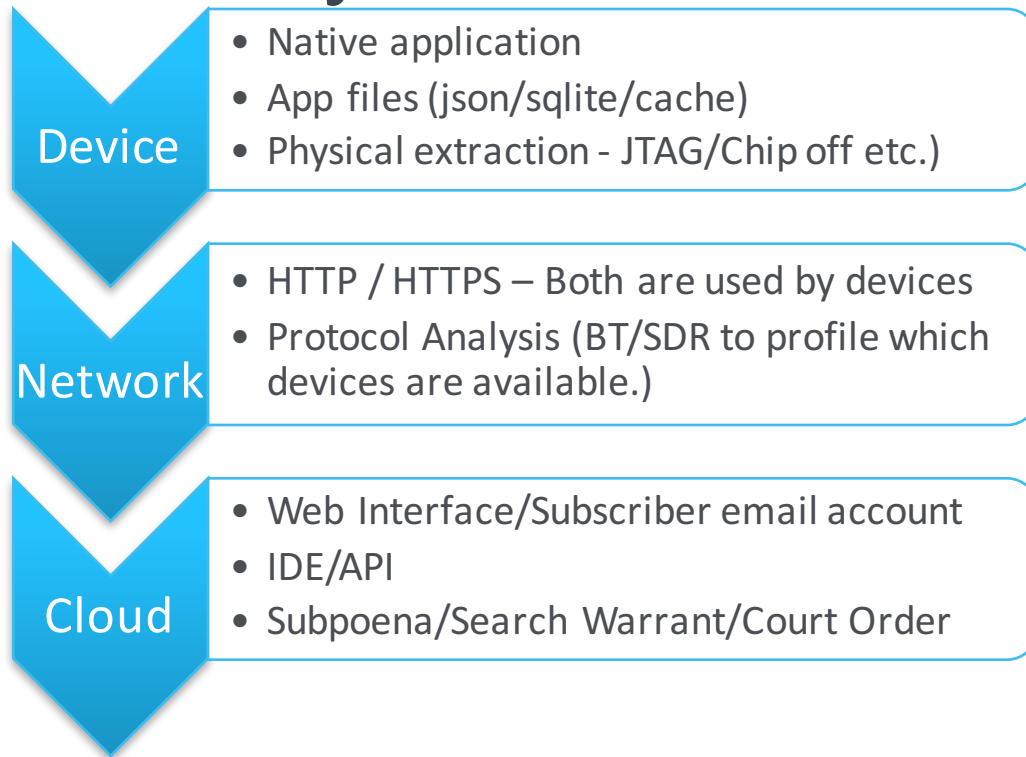
ENTER YOUR EMAIL

NOTIFY ME



Internet of Things Forensics is Fun

Data accessibility



Hatch Baby

A baby change table that's connected to the internet



Hatch Baby

Forensic Artifacts

WiFi SSIDs

Account Information

Biometric data



Hatch Baby

Forensic Artifacts

WiFi SSIDs

com.hatchbaby/cache/volley/582429184758663336

Monday May 16, 2016 10:42:21 (am)

```
.....1463409741634[{"ssid":"champstudent","sec":3},{ "ssid":"champlabs","sec":3}  
, {"ssid":"student","sec":0}, {"ssid":"facstaff","sec":3}, {"ssid":"student","sec":0}  
, {"ssid":"student","sec":0}, {"ssid":"champstudent","sec":3}, {"ssid":"champlabs"  
, "sec":3}, {"ssid":"facstaff","sec":3}, {"ssid":"champstudent","sec":3}, {"ssid"  
:"facstaff","sec":3}, {"ssid":"champlabs","sec":3}, {"ssid":"student","sec":0}  
, {"ssid":"champstudent","sec":3}, {"ssid":"champlabs","sec":3}, {"ssid":"TP  
-LINK_E73A","sec":3}, {"ssid":"champlabs","sec":3}, {"ssid":"student","sec":0}  
, {"ssid":"champstudent","sec":3}, {"ssid":"facstaff","sec":3}]
```

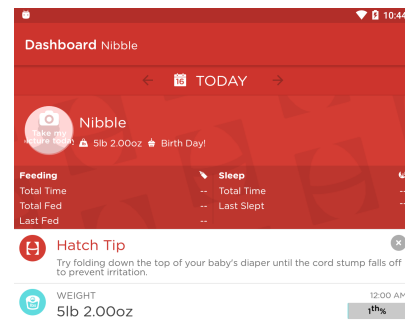
Hatch Baby

Forensic Artifacts

Account Information | Biometric

com.hatchbaby/shared_prefs/com.hatchbaby.HBPreferences.xml

```
<map>
  <string name="current_baby">
    {"birthWeight":2324.661,"birthDate":"2016-05-16","updateDate":"2016-05-16 07:41:49","createDate":"2016-05-16 07:41:49","name":"Nibble","id":11623,"gender":"FEMALE","dueDate":"2016-05-16"}
  </string>
  <string name="preferred_unit_of_measure">imperial</string>
  <string name="latest_updates_dates">{"11623":{"REFRESH":1463597639196}}</string>
  <boolean name="pending_notifications_update" value="false"/>
  <string name="token">
    MTA3NDM6MTYyMTA4OTcwOTg5NT03NzgWNDYzMzIxODk2MGMxNzExZGU5ZjZjM3NTI3ZTkxYg
  </string>
  <string name="current_user">
    {"active":true,"babies":[{"birthWeight":2324.661,"birthDate":"2016-05-16","updateDate":"2016-05-16 07:41:50","createDate":"2016-05-16 07:41:50","name":"Nibble","id":11623,"gender":"FEMALE","dueDate":"2016-05-16"},"createDate":"2016-05-16 07:41:50","defaultUnitOfMeasure":"imperial","email":"lcdiot2@gmail.com","firstName":"John","id":10743,"isActive":false,"timezone":"America/New_York","updateDate":"2016-05-16 07:41:50"}]
  </string>
  <long name="login_time" value="1463409710304"/>
  <boolean name="has_scale" value="true"/>
  <string name="notifications_map">
    {"ManualDiaper":false,"ManualFeedingWithAmount":true,"ManualFeedingWithoutAmount":true,"ManualLength":false,"ManualSleep":true,"ManualWeight":false,"ScpDiaper":false,"ScpFeeding":false}
  </string>
</map>
```



Master Title

Forensic Artifacts

Account Information | Biometric

com.hatchbaby/databases/redhenbaby-db

Table:

MEMBER

New RecordDelete Record

	_id	FIRST_NAME	EMAIL	ACTIVE	TIMEZONE	IS_ACTIVE	ILT_UNIT_OF_ME/	CREATE_DATE	UPDATE_DATE	
	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>
1	10743	John	lodliot2@gmail.com	1	America/New_York	0	imperial	1463398910000	1463398910000	NU

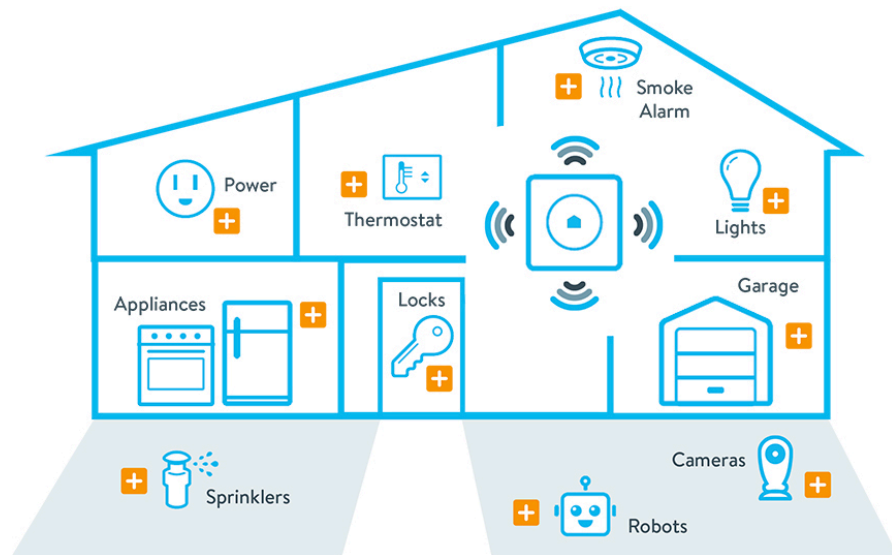
Table:

DIAPER

New RecordDelete Record

	_id	RHB_ID	DELETED	DIAPER_DATE	DIAPER_TYP/	CREATE_DATE	UPDATE_DATE	BABY_ID	MEMBER_ID
	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>	<div>Filter</div>
1	1	251666	0	1463410674000	Both	1463399878000	1463399878000	11623	10743
2	2	251679	0	1463411050000	Wet	1463400254000	1463400254000	11623	10743

WinkHub



WinkHub

Which products connect to the WinkHub?



WinkHub

Forensic Artifacts

Account information

Devices connected/paired

Recent activity of devices

WinkHub

Forensic Artifacts

User Account

com.quirky.android.wink.wink/shared_prefs/com.quirky.android.wink.wink_preferences.xml

```
▼ <map>
  <int name="APP_LAUNCHES" value="17"/>
  <string name="App Restrictions">AAAAAA==</string>
  <string name="com.quirky.android.wink.core.login.pref.EMAIL">lcdiiot2@gmail.com</string>
</map>
```

WinkHub

Forensic Artifacts

As devices are provisioned with Wink, an entry is populated in PersistenceDB

com.quirky.android.wink.wink/databases/PersistenceDB

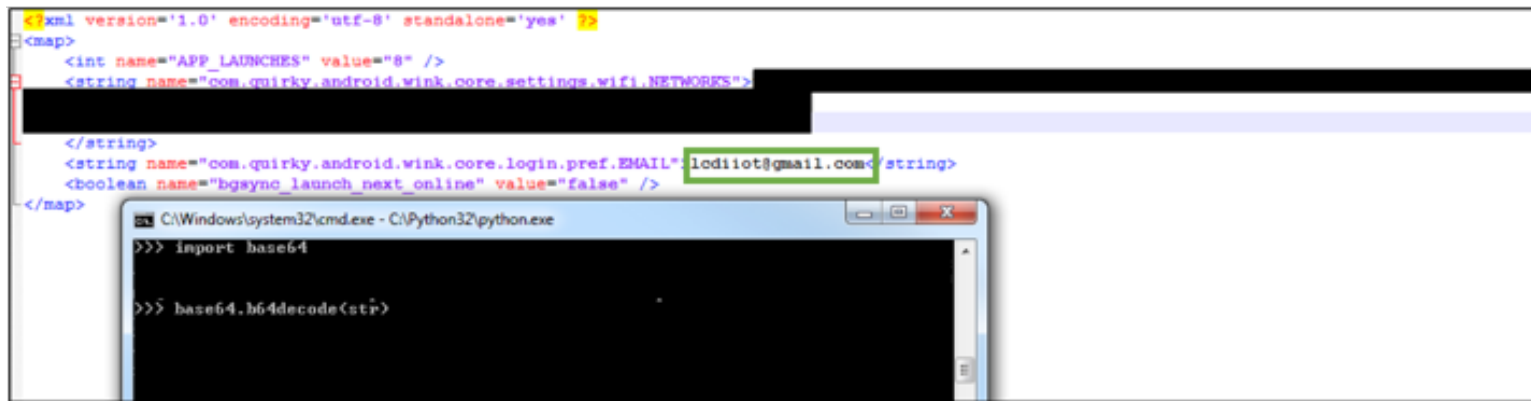
SQLite database

	ID	Type	Json
	Filter	Filter	Filter
1	412	provisioning_flow	{"manufacturer_name":"Kwikset","model_name":"Z-Wave Deadbolt","onboarding_media": [],"provisioning_flow_id":"412","provisioning_media":{"button_text":null,"copy":"Connecting your Kwiks...
2	853	provisioning_flow	{"manufacturer_name":"Wink","model_name":"HUB","onboarding_media": [],"provisioning_flow_id":"853","provisioning_media":{"button_text":null,"copy":"Connecting your Wink ...
3	458	provisioning_flow	{"manufacturer_name":"Quirky + GE","model_name":"Tripper","onboarding_media": [],"provisioning_flow_id":"458","provisioning_media":{"button_text":null,"copy":"Connecting your Quirky...
4	536	provisioning_flow	{"manufacturer_name":"Dropcam","model_name":"Dropcam Pro","onboarding_media": [],"provisioning_flow_id":"536","provisioning_media":{"button_text":null,"copy":"Connecting your Nest ...

WinkHub

Forensic Artifacts

data/data/com.quirky.android.wink.wink/shared_prefs/wink_preferences.xml



The image shows a screenshot of an XML file named `wink_preferences.xml` and a terminal window. The XML file contains the following content:

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <int name="APP_LAUNCHES" value="8" />
  <string name="com.quirky.android.wink.core.settings.wifi.NETWORKS">
    [REDACTED]
  </string>
  <string name="com.quirky.android.wink.core.login.pref.EMAIL">lediiot@gmail.com</string>
  <boolean name="bgsync_launch_next_online" value="false" />
</map>
```

The terminal window shows the following commands and output:

```
C:\Windows\system32\cmd.exe - C:\Python32\python.exe
>>> import base64
>>> base64.b64decode(sti)
```

- Wifi SSID and Password
 - Base64 encoded

*This has been patched in current versions of Wink

WinkHub + Quirky GE Tripper

Forensic Artifacts

Security sensors (contact sensors)

com.quirky.android.wink.wink/databases/PersistenceDB

	ID	Type	Json
	Filter	Filter	Filter
1	412	provisioning_flow	{"manufacturer_name":"Kwikset","model_name":"Z-Wave Deadbolt","onboarding_media":[],"provisioning_flow_id":"412","provisioning_media":{"button_text":null,"copy":"Connecting your Kwiks..."}}
2	853	provisioning_flow	{"manufacturer_name":"Wink","model_name":"HUB","onboarding_media":[],"provisioning_flow_id":"853","provisioning_media":{"button_text":null,"copy":"Connecting your Wink ..."}}
3	458	provisioning_flow	{"manufacturer_name":"Quirky + GE","model_name":"Tripper","onboarding_media":[],"provisioning_flow_id":"458","provisioning_media":{"button_text":null,"copy":"Connecting your Quirky..."}}
4	536	provisioning_flow	{"manufacturer_name":"Dropcam","model_name":"Dropcam Pro","onboarding_media":[],"provisioning_flow_id":"536","provisioning_media":{"button_text":null,"copy":"Connecting your Nest ..."}}

```
▼ object {13}
  manufacturer_name : Quirky + GE
  model_name : Tripper
  ▶ onboarding_media [0]
  provisioning_flow_id : 458
  ▶ provisioning_media [7]
  ▶ supported_upcs [4]
  title : Tripper
  version : 2
  icon_id : null
  name : null
  object_id : 458
  object_type : provisioning_flow
  subscription : null
```


WinkHub + Quirky GE Tripper

Forensic Artifacts

com.quirky.android.wink.wink/databases/PersistenceDB

```
opened_changed_at : 1463761361
connection_changed_at : 1463427407
tamper_detected_updated_at : 1463761361
firmware_version_updated_at : 1463761361
tamper_detected_true_changed_at : 1463586004
opened_updated_at : 1463761361
battery_changed_at : 1463427409
connection_updated_at : 1463761361
icon_id : null
name : Secure Door
object_id : 196682
object_type : sensor_pod
```

ID	Type	Json	Name
Filter	Filter	Filter	Filter
196682	sensor_pod	{"sensor_pod_id":"196682","bridge_id":null,"capabilities":{"configuration":null,"fields":{"attribute_id":null,"choices":null,"field":"opened","mutability":"read-only","placement":null,"range":null,"...	Secure Door

created_at:1463427407	5/16/2016, 3:36:47 PM GMT-4:00
device_manufacturer:"quirky_ge"	
hub_id:"421947"	
lat_lng:[44.460903, -73.21597]	
manufacturer_device_model:"quirky_ge_tripper"	
model_name:"Tripper"	
radio_type:"zigbee"	
user_ids:["471209"]	
opened:false	
firmware_version:"1.8b00 / 5.1b21"	
connection:true	
firmware_version_changed_at:1463427409	
battery:1.0	
tamper_detected:false	
opened_changed_at:1463761361	5/20/2016, 12:22:41 PM GMT-4:00
connection_changed_at:1463427407	5/16/2016, 3:36:47 PM GMT-4:00
tamper_detected_updated_at:1463761361	5/20/2016, 12:22:41 PM GMT-4:00
firmware_version_updated_at:1463761361	5/20/2016, 12:22:41 PM GMT-4:00
tamper_detected_true_changed_at:1463586004	5/18/2016, 11:40:04 AM GMT-4:00
opened_updated_at:1463761361	5/20/2016, 12:22:41 PM GMT-4:00
battery_changed_at:1463427409	5/16/2016, 3:36:49 PM GMT-4:00
connection_updated_at:1463761361	5/20/2016, 12:22:41 PM GMT-4:00
name:"Secure Door"	
object_id:"196682"	

WinkHub + Quirky GE Tripper

Forensic Artifacts

com.quirky.android.wink.wink/shared_prefs/winkdevices.xml

```
<string name="activity/39f8b98d-6cd9-440e-bcb2-b453ee1e7ee3">
  {"action":{"object_id":null,"object_name":null,"object_type":null,"reading":
  {"opened":true},"target_actor_email":null,"target_actor_first_name":null,"target_actor_last_name":null},"activity_id":"39f8b98d-6cd9-440e-bcb2-
b453ee1e7ee3","category":"reading","context":
  {"cuepoint_id":null,"cuepoint_type":null,"initial_actor":null,"media_url":null,"notes":null,"triggering_object":null},"created_at":1.463760528550257E9,"object":
  {"object_id":"196682","object_name":"Secure Door","object_type":"sensor_pod"},"icon_id":null,"name":null,"object_id":null,"object_type":null,"subscription":null}
</string>
```

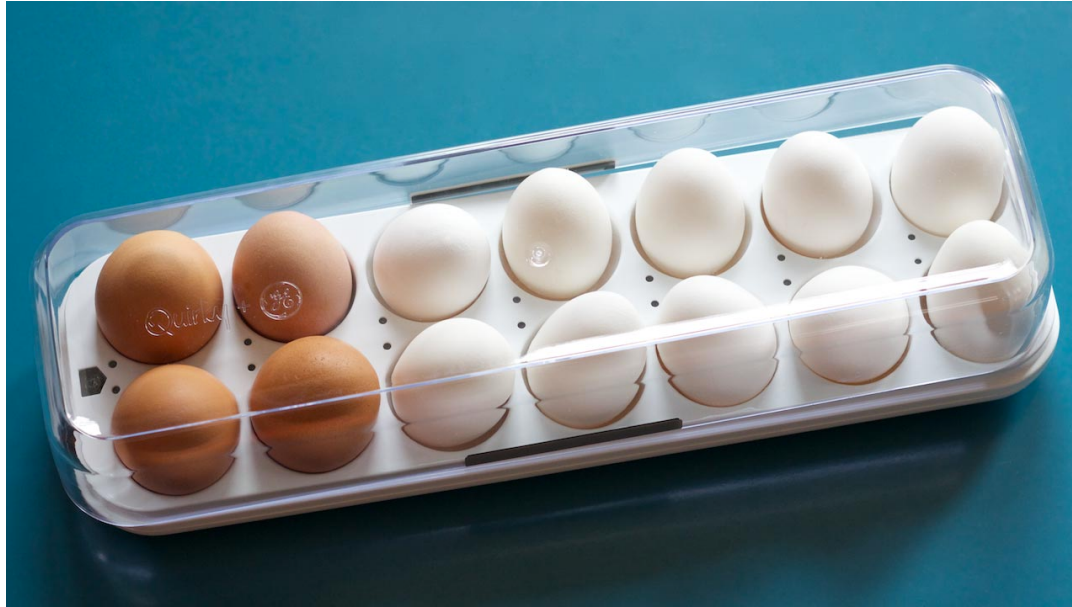
5/20/2016, 12:08:48 PM

```
<string name="activity/f8ff88be-1214-457b-b062-450cb4727494">
  {"action":{"object_id":null,"object_name":null,"object_type":null,"reading":
  {"opened":true},"target_actor_email":null,"target_actor_first_name":null,"target_actor_last_name":null},"activity_id":"f8ff88be-1214-457b-b062-
450cb4727494","category":"reading","context":
  {"cuepoint_id":null,"cuepoint_type":null,"initial_actor":null,"media_url":null,"notes":null,"triggering_object":null},"created_at":1.4637604571958694E9,"object":
  {"object_id":"196682","object_name":"Fridge","object_type":"sensor_pod"},"icon_id":null,"name":null,"object_id":null,"object_type":null,"subscription":null}
</string>
```

5/20/2016, 12:07:37 PM

WinkHub + Egg Minder

An internet connected egg tray



WinkHub + Egg Minder

Forensic Artifacts

com.quirky.android.wink.wink/databases/persistenceDB

ID	Type	Json	Name
Filter	Filter	Filter	Filter
152815	eggtray	{"eggs": [0,1444150557,1444150561,1444150566,1444150570,1444150578,144...	Egg Minder



```
{"eggs":  
[0,1444150557,1444150561,1444150566,1444150570,1444150578,1444150764,0,1444150562,1444150566,1444150571,1444150575,1444150578,1444152005],"eggtray_id":"152815","freshness_period":  
2419200,"last_reading":{"connection_changed_at":1444150128,"inventory_updated_at":1444151994,"inventory":12,"freshness_remaining":2417763,"freshness_remaining_updated_at":  
1444151994,"battery_changed_at":1444151994,"connection_updated_at":1444150128,"battery_updated_at":1444151994,"connection":true,"battery":0.81},"capabilities":  
{"configuration":null,"desired_state_fields":null,"fields":null,"sensor_types":null},"created_at":  
1444150128,"device_manufacturer":"quirky_ge","gang_id":null,"hidden_at":null,"hub_id":null,"lat_lag":  
[44.460907,-73.215721],"linked_service_id":null,"local_id":null,"locale":"en_us","location":"","mac_address":"0c2a6905fcf0","manufacturer_device_id":null,"manufacturer_device_model":nu  
ll,"model_name":"Egg Minder","order":0,"radio_type":null,"serial":"ABAA00027468","upc_id":"23","user_ids":["345253"],"icon_id":null,"name":"Egg  
andMinder","object_id":"152815","object_type":"eggtray","subscription":{"pubnub":{"channel":"0f2934c6a8945025b3ed71b2647585a3387bcb7e|eggtray-152815|user-345253"},"subscribe_key":"sub-  
c-f7bf7f7e-0542-11e3-a5e8-02ee2ddab7fe"}}}
```

WinkHub + Kwikset Lock

An internet connected lock



WinkHub + Kwikset Lock

Forensic Artifacts

com.quirky.android.wink.wink/databases/persistenceDB

ID	Type ▼	Json	Name
Filter	Filter	Filter	Filter
82725	lock	{"lock_id":"82725","bridge_id":null,"capabilities":{"configuration":null,"fields":{"attribute_id":null,"choices":null,"field":"connection","mutability":"read-only","pla...	Lock

WinkHub + Kwikset Lock

Unlock with Phone

```
created_at":1456331248
desired_state":{}
last_reading":{"last_error":null
desired_locked_changed_at":1461162483
locked":false
connection":true
locked_changed_at":1461162483
battery_updated_at":1461162483
battery":1.0
last_error_updated_at":null
desired_locked_updated_at":1461162483
locked_updated_at":1461162483
connection_updated_at":1461162483}
```

These values updated when
unlocked with phone

Unlock with Key or Keypad

```
created_at":1456331248
desired_state":{}
last_reading":{"last_error":null
desired_locked_changed_at":1461165781
locked":false
connection":true
locked_changed_at":1461166122
battery_updated_at":1461166122
battery":1.0
last_error_updated_at":null
desired_locked_updated_at":1461165781
locked_updated_at":1461166122
connection_updated_at":1461166122}
```

Values not updated

WinkHub + Kwikset Lock

POP QUIZ – Which data represents an app unlock?

desired_locked_changed_at:1463421866,	5/16/2016, 2:04:26 PM
locked:true,	
locked_changed_at:1463421866,	5/16/2016, 2:04:26 PM
desired_locked_updated_at:1463421866,	5/16/2016, 2:04:26 PM
locked_updated_at:1463421866,	5/16/2016, 2:04:26 PM
connection_updated_at:1463421866	5/16/2016, 2:04:26 PM

App Unlock @ 2:04

desired_locked_changed_at:1463421866,	5/16/2016, 2:04:26 PM
locked:false,	
locked_changed_at:1463422892,	5/16/2016, 2:21:32 PM
desired_locked_updated_at:1463421866,	5/16/2016, 2:04:26 PM
locked_updated_at:1463422892,	5/16/2016, 2:21:32 PM
connection_updated_at:1463422892	5/16/2016, 2:21:32 PM

Manual Key Unlock @ 2:21


WinkHub - Phillips Hue Light Bulbs



WinkHub - Phillips Hue Light Bulbs

Forensic Artifacts

com.quirky.android.wink.wink\databases\persistenceDB

ID		Type	Json	Name 
	Filter	Filter	Filter	Filter
204	1091438	light_bulb	{\"light_bulb_id\":\"1091438\",\"bridge_id\":null,\"capabilities\":{\"configuration\":null,\"fields\":{\"attribute_id\":null,\"choices\":null,\"field\":\"connection\",\"mutability\":\"read-only\",\"placement\":null,\"range\":null,\"type\":\"boolean\"},...	Hue Lamp 3
205	1091437	light_bulb	{\"light_bulb_id\":\"1091437\",\"bridge_id\":null,\"capabilities\":{\"configuration\":null,\"fields\":{\"attribute_id\":null,\"choices\":null,\"field\":\"connection\",\"mutability\":\"read-only\",\"placement\":null,\"range\":null,\"type\":\"boolean\"},...	Hue Lamp 2
206	1091436	light_bulb	{\"light_bulb_id\":\"1091436\",\"bridge_id\":null,\"capabilities\":{\"configuration\":null,\"fields\":{\"attribute_id\":null,\"choices\":null,\"field\":\"connection\",\"mutability\":\"read-only\",\"placement\":null,\"range\":null,\"type\":\"boolean\"},...	Hue Lamp 1

```
"created_at":1447363101,
"desired_state":{,"last_reading":

{"color_updated_at":1460983521,
"desired_saturation_changed_at":1461004499
,"hue_changed_at":1461004541,
"color_x_changed_at":1461004541,
"color_y_changed_at":1461004541,
"color_model_updated_at":1461004751,
"color_temperature_updated_at":1461004751,
"saturation_changed_at":1461004541,
"powered_changed_at":1461004705,
"desired_hue_updated_at":1461004499,
"desired_brightness_updated_at":1461004624,
"desired_color_model_updated_at":1461004499
,"connection":true,
"desired_color_updated_at":1461004624,
"brightness_updated_at":1461004751,
"powered":false,
"desired_powered_changed_at":1461004705,
"saturation":0.980315,
"desired_saturation_updated_at":1461004499,
"color_temperature":2000,
"hue_updated_at":1461004751,
"color_x_updated_at":1461004751,
"hue":0.987335,
"color":null,
"color_y_updated_at":1461004751,
"connection_changed_at":1461002301,
"saturation_updated_at":1461004751,
"brightness":1.0,
"powered_updated_at":1461004751,
"color_model_changed_at":1461004485,
"desired_color_x_updated_at":1461004624.
```

WinkHub - Phillips Hue Light Bulbs

Forensic Artifacts

```
"powered_updated_at":1461004751,
"color_model_changed_at":1461004485,
"desired_color_x_updated_at":1461004624,
"desired_color_y_updated_at":1461004624,
"color_x":0.6468,"color_y":0.3106,
"desired_color_temperature_updated_at":1461004624,
"color_temperature_changed_at":1461004541,
"desired_hue_changed_at":1461004499,
"color_model":"hsb",
"desired_brightness_changed_at":1460983522,
"desired_powered_updated_at":1461004705,"
desired color model changed at":1461004499,
```

Light Bulb

Get Light Bulb



Desired State Attributes

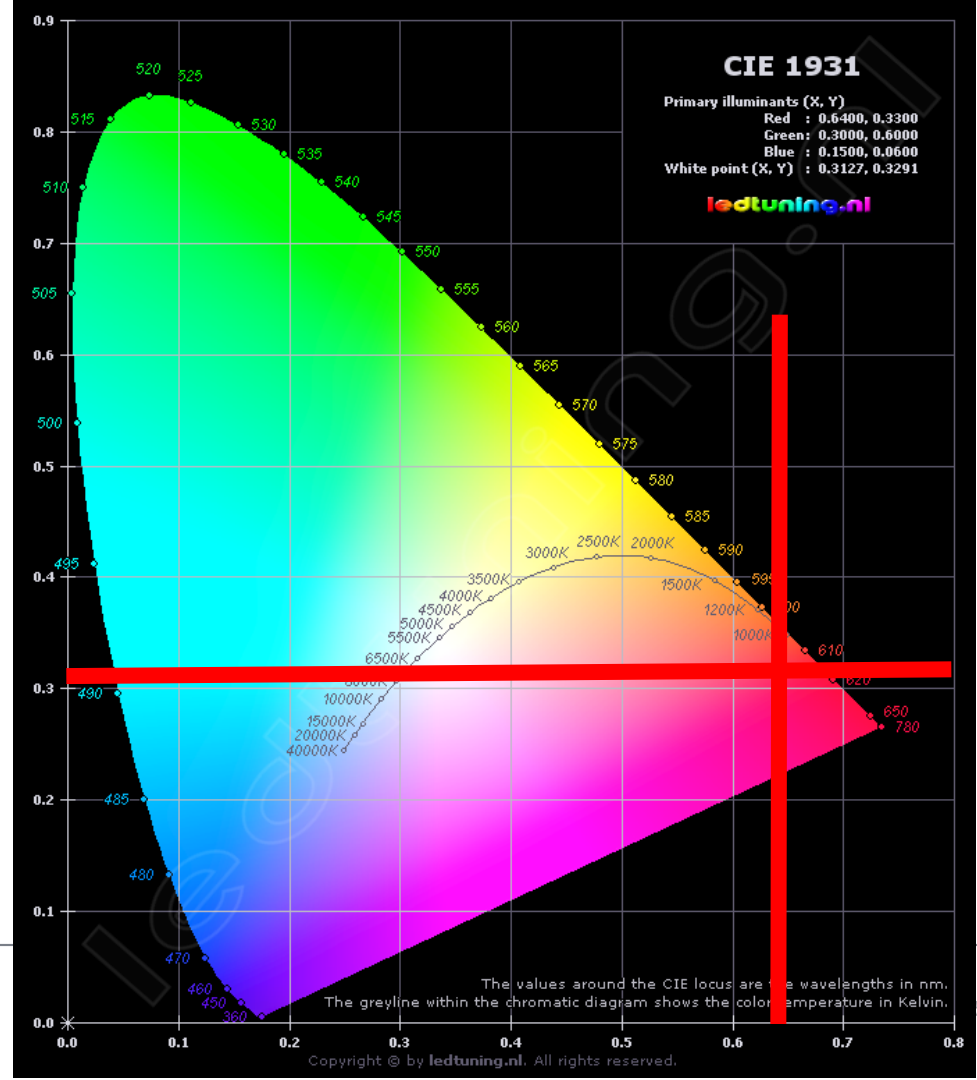
API field	Attributes	Description
powered	boolean	whether device is powered on
brightness	float	0.0 to 1.0, dimness level (binary_switch and light_bulb)
color_model	(string)	one of: "xy", "hsb", "color_temperature", or "rgb"
color_x	(float, precision 4)	the CIE 1931 coordinates of the bulb's color [0.0, 1.0]
color_y	(float, precision 6)	he CIE 1931 coordinates of the bulb's color [0.0, 1.0]

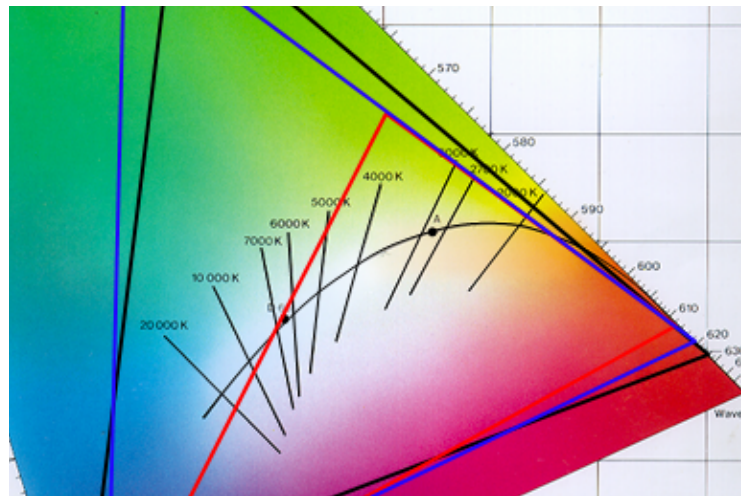
Make all lights red.

Light 1 in persistence DB has the following x and y values

```
"powered_updated_at":1461004751,  
"color_model_changed_at":1461004485,  
"desired_color_x_updated_at":1461004624,  
"desired_color_y_updated_at":1461004624,  
"color_x":0.6468,"color_y":0.3106,  
"desired_color_temperature_updated_at":1461004624,  
"color_temperature_changed_at":1461004541,  
"desired_hue_changed_at":1461004499,  
"color_model":"hsb",  
"desired_brightness_changed_at":1460983522,  
"desired_powered_updated_at":1461004705,"  
desired_color_model_changed_at":1461004499,
```

Using the CIE 1931 color graph to plot these values, the resulting color is in the red area of the graph and thus matches with the user action of changing lamp 1 to red.





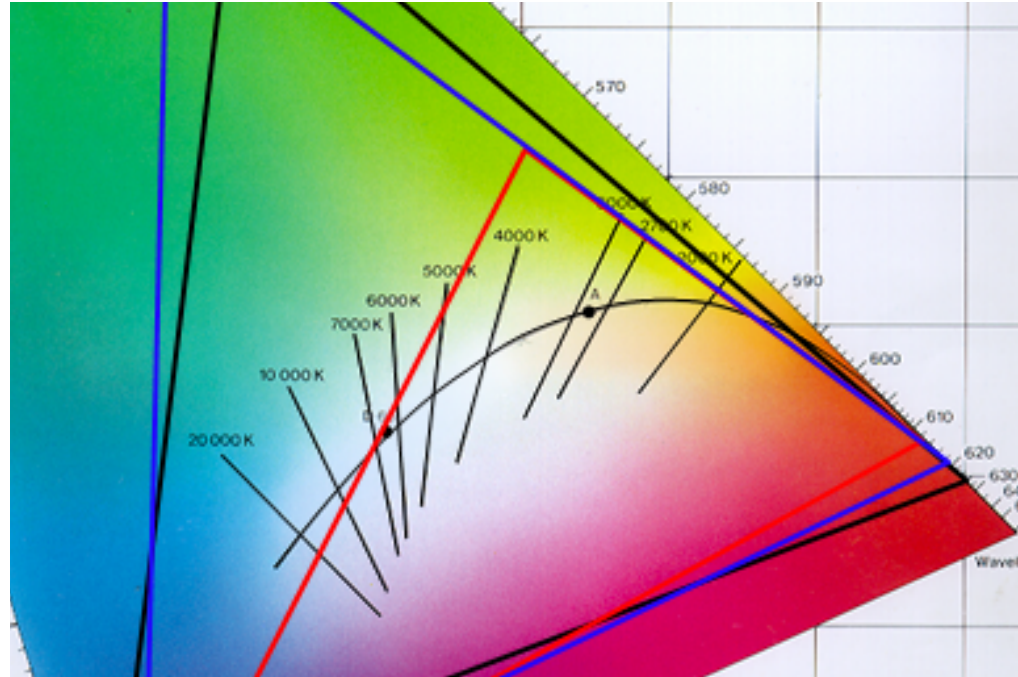
```
desired_powered_changed_at":1461611530
saturation":0.96063
desired_saturation_updated_at":1461611530
color_temperature":2638
hue_updated_at":1461611517
color_x_updated_at":1461611517
hue":0.303395
desired_hue":0.646505
```



Zoomed in on the CIE 1931 graph, there is a curved black line that represents these values on the color spectrum.

The “color_temperature” value in the data represents the Kelvin number [2000 .. 6500]

```
desired_powered_changed_at":1461611530  
saturation":0.96063  
desired_saturation_updated_at":1461611530  
color_temperature":2638  
hue_updated_at":1461611517  
color_x_updated_at":1461611517  
hue":0.303395  
desired_hue":0.646505  
...
```



Amazon Echo

Alexa is always listening...

She doesn't record your voice until you say her name



Amazon Echo

Forensic Artifacts

Account information

Timestamps of what Alexa heard during the period activated

The actual text of what Alexa heard

The given response

The URL of the file location on Amazon server

The actual audio of the last played response (via the app)

Amazon Echo

Forensic Artifacts

Account information

com.amazon.dee.app/cache/org.chromium.android_webview

Step 1 - Decompress the gzipped files

Step 2 - search for the following:

{"accounts":[{"email": - This will give you the base account as well as the Amazon customer ID

customerEmail": - This will give you the Amazon Prime Music email account and customer ID

Amazon Echo

Forensic Artifacts

Account Information

com.amazon.dee.app/cache/org.chromium.android_webview

```
{ "accounts": [ { "email": "lcdiiot2@gmail.com", "eulaAcceptance": true, "firstName": "John", "fullName": "John", "id": "A3PH5BQNQV2I6K", "pendingUserPin": null, "role": "ADULT" } ], "id": null }
```

Amazon Echo

Forensic Artifacts

Interactions with Alexa

com.amazon.dee.app/cache/org.chromium.android_webview

- Step 1 - Decompress the gzipped files
- Step 2 – Find your favorite Json viewer and/or forensic tool 😊
- Step 3 – Search for the following:
 - *Alexa heard:* or *playbackAudioAction* - This will show you the location of “cards” that contain text Alexa heard from the user
 - *primaryActions* – This is what Alexa did with the query (backend)
 - *"descriptiveText":* or *"title":* - *This will show you the response from Alexa – what was said out loud or played.*
 - *,"cardType":* - This is present in all “cards”, will yield more results

Amazon Echo

Forensic Artifacts

Interactions with Alexa

com.amazon.dee.app/cache/org.chromium.android_webview

Alexa heard: or **playbackAudioAction** - This will show you the location of “cards” that contain text Alexa heard from the user

primaryActions – This is what Alexa did with the query (backend)

"descriptiveText": or *"title":* - This will show you the response from Alexa – what was said out loud or played.

,"cardType": - This is present in all “cards”, will yield more results

Samsung SmartCam

Motion/Voice/Night Vision

Wi-Fi or Hardwire




Samsung SmartCam

Registration

Found camera(s).

Select the camera listed below and tap <Next>. If the cameras are not listed, enter the camera serial number manually.

 CAMERA SERIAL NUMBER

Serial number

Enter the 15-digit serial number. ?

Prev Next

Camera Settings

Time Event Network

Enable motion and/or audio detection to receive event alerts on your devices.

Event alert ☒


Motion Detection ☒

Audio Detection ☒

Next

Camera Setup About

+ Add Camera

 LCDIcam

Camera Setup About

+ Add Camera

Camera password

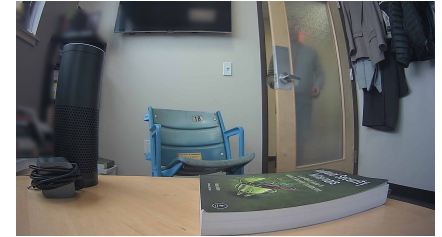
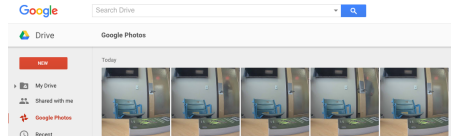
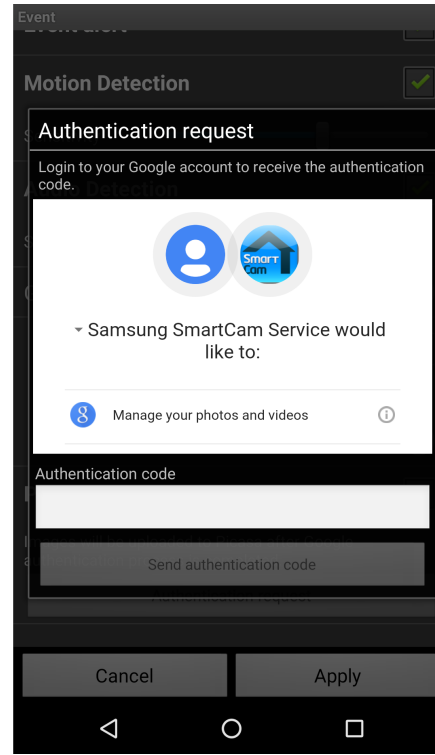
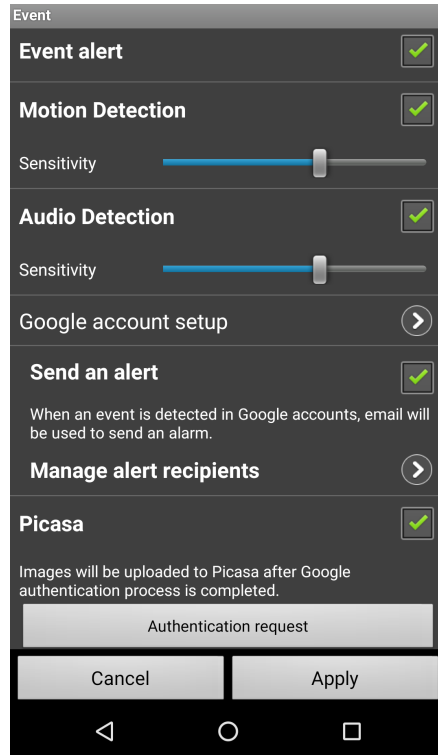
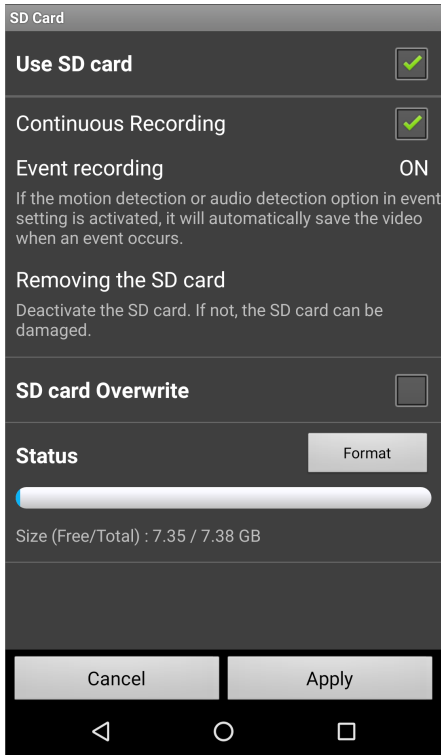
Enter the camera password.

☐ Save

Cancel OK

1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p
a s d f g h j k l
↑ z x c v b n m ×
?123 , . ↵

Samsung SmartCam



Samsung SmartCam

Username and password in plaintext

```
13:19:06.677 [main]          [ap]          [DEBUG] ReceiverRestrictedContext , id = [REDACTED] , password = [REDACTED]
13:19:06.678 [main]          [ap]          [DEBUG] connect id = [REDACTED] , password = [REDACTED] , timeOut = 30000
```

- Username and password
- The SSID that the phone was connected to can also be seen
- The log no longer exists after an the version 2.71 update

Samsung SmartCam

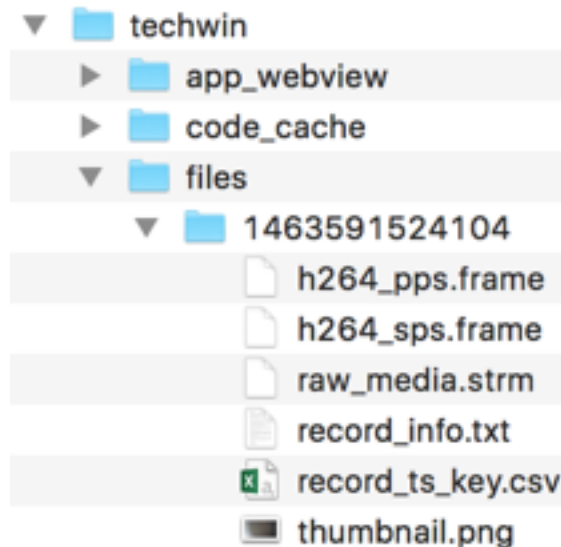
Forensic Artifacts

/data/data/com.techwin.shc/files/

Videos are saved in this location

Folders named in epoch time
corresponding to when user began
recording

Folders created when user saves a video
(live record) (you hit I want to record)

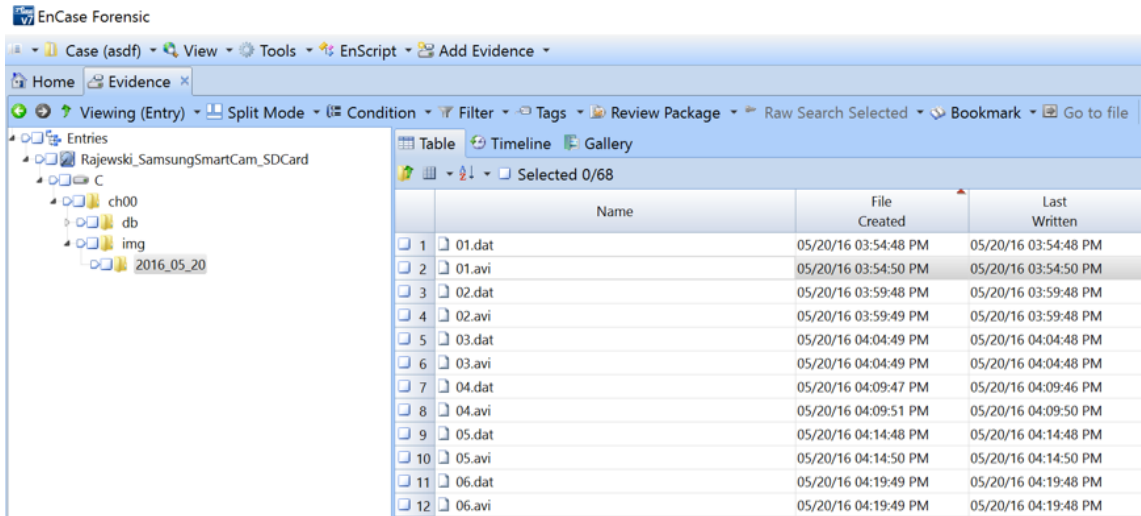


Samsung SmartCam

Where is the data?

SD Card – User initiated action – Insert MicroSD and enable it in the App

Pictures and videos saved here



	Name	File Created	Last Written
1	01.dat	05/20/16 03:54:48 PM	05/20/16 03:54:48 PM
2	01.avi	05/20/16 03:54:50 PM	05/20/16 03:54:50 PM
3	02.dat	05/20/16 03:59:48 PM	05/20/16 03:59:48 PM
4	02.avi	05/20/16 03:59:49 PM	05/20/16 03:59:48 PM
5	03.dat	05/20/16 04:04:49 PM	05/20/16 04:04:48 PM
6	03.avi	05/20/16 04:04:49 PM	05/20/16 04:04:48 PM
7	04.dat	05/20/16 04:09:47 PM	05/20/16 04:09:46 PM
8	04.avi	05/20/16 04:09:51 PM	05/20/16 04:09:50 PM
9	05.dat	05/20/16 04:14:48 PM	05/20/16 04:14:48 PM
10	05.avi	05/20/16 04:14:50 PM	05/20/16 04:14:50 PM
11	06.dat	05/20/16 04:19:49 PM	05/20/16 04:19:48 PM
12	06.avi	05/20/16 04:19:49 PM	05/20/16 04:19:48 PM

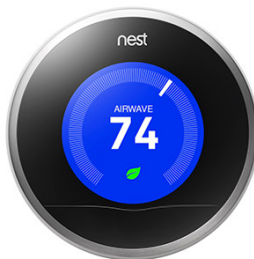
Samsung Smartthings

IOT Hub



Nest

Camera, Thermostat, Fire/CO Alarm



Nest

Forensic Artifacts

When Nest sensed a presence

Video

Nest

Forensic Artifacts

Nest Account Information

Com.nest.android/cache/cache/

▼	cache	--
▼	cache	--
	cache-199259282.json	4 KB
	cache-656117153.json	70 KB
	cache726260100.json	68 KB
	cache1219483713.json	4 KB

▼ object {7}

tier : home.nest.com

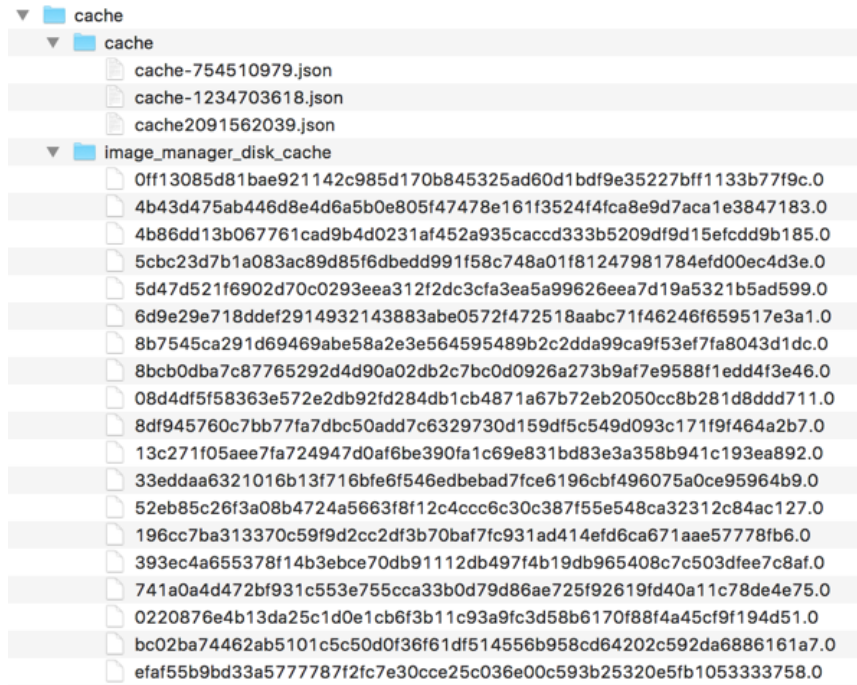
email : lcdiiot2@gmail.com

Nest

Forensic Artifacts

Com.nest.android/cache/cache/
image_manager_disk_cache

Use ffmpeg to convert the files



Nest

Forensic Artifacts

Ffmpeg

```
ffmpeg -f h264 -i VIDEOFILE -vcodec copy OUTPUT.mp4
```

```
ffmpeg -f h264 -i VIDEOFILE -vcodec copy OUTPUT.mp4
```

Nest

Forensic Artifacts

Nest Protect

Com.nest.android/cache/cache/

```
▼ 28 {2}
  ▼ value {3}
    schema_version : 1.0
    ▼ products [1]
      ▼ 0 {3}
        product : topaz.18B43000002D24D6
        start : 1460851200000
        end : 1461801600000
      ► events [182]
    object_key : structure_history.055ab850-c465-11e4-8ad1-22000b490616
```

Nest

Forensic Artifacts

Nest Protect

Com.nest.android/cache/cache/

```
▶ 136 {4}
▶ 137 {4}
▶ 138 {4}
▼ 139 {4}
    type : 0101
    product : topaz.18B43000002D24D6
    start : 1463395114191
    end : 1463395124875
▼ 140 {4}
    type : 0101
    product : topaz.18B43000002D24D6
    start : 1463395127427
    end : 1463395141792
▼ 141 {4}
    type : 0102
    product : topaz.18B43000002D24D6
    start : 1463399448821
    end : 1463399448821
```

Monday May 16, 2016 06:38:34 (am)

Monday May 16, 2016 06:38:45 (am)

Monday May 16, 2016 06:38:47 (am)

Monday May 16, 2016 06:39:02 (am)

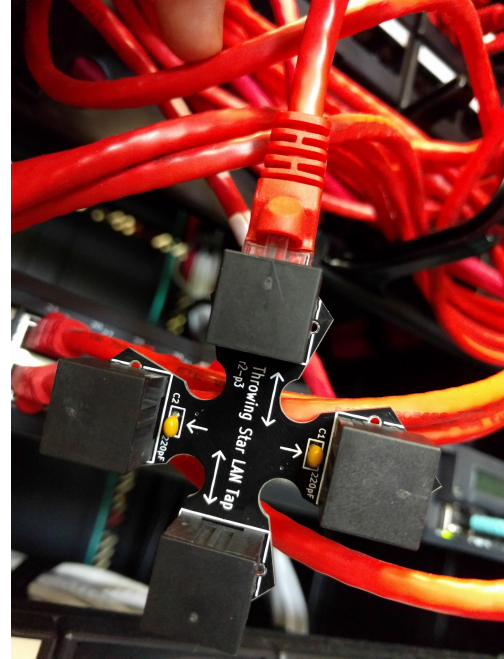
Monday May 16, 2016 07:50:49 (am)

Monday May 16, 2016 07:50:49 (am)

Hands-on Scenario

We just found this on our air-gapped network

Can you use data from the IOT devices installed at this facility to determine what happened?



Hands-on Scenario

Data for you to review

Amazon Echo

Samsung Camera - SamsungSmartCam_SDCard.Ex01

Samsung Smartthings

Wink

Email me your answer



Leahy Center for
Digital Investigation

Thank You

Jonathan Rajewski | Director | Senator Patrick Leahy Center for Digital Investigation
@jtrajewski | rajewski@champlain.edu | jtrajewski@gmail.com