

IoT Forensics Challenges and Opportunities for Digital Traces

Francesco Servida, Eoghan Casey

Outline

- Smart Devices
- Forensic Interest
- Methodology
- Results
- Discussion

Smart Devices

Security systems

- cameras
- door locks
- motion sensors
- smoke & CO detectors

Smart assistants

- audio
- video

Smart hubs

Smart firewalls

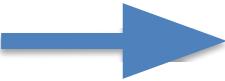
Smart:

- microwave, stove, grill, crock pot
- refrigerator
- grow system
- coffee maker
- television
- thermostat
- light bulbs
- plugs
- toys

...

Forensic Interest

- Myriad of sensors
- Highly connected
- Low security



- Direct Targets
 - Sensitive Data
- Secondary targets
 - Alarm Systems
 - «Trojan Horses»
 - Botnets (eg. Mirai)
- Witnesses

IoT forensics approach

Enterprise IoT

- Proactive collection

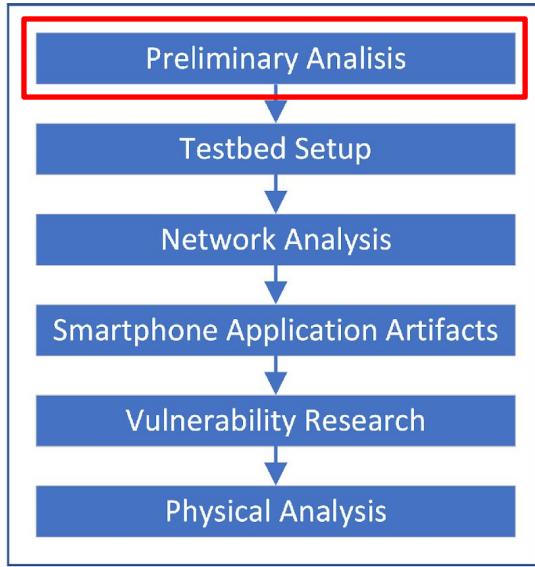
Home IoT

- What to do on an “unprepared” crime scene?

Methodology

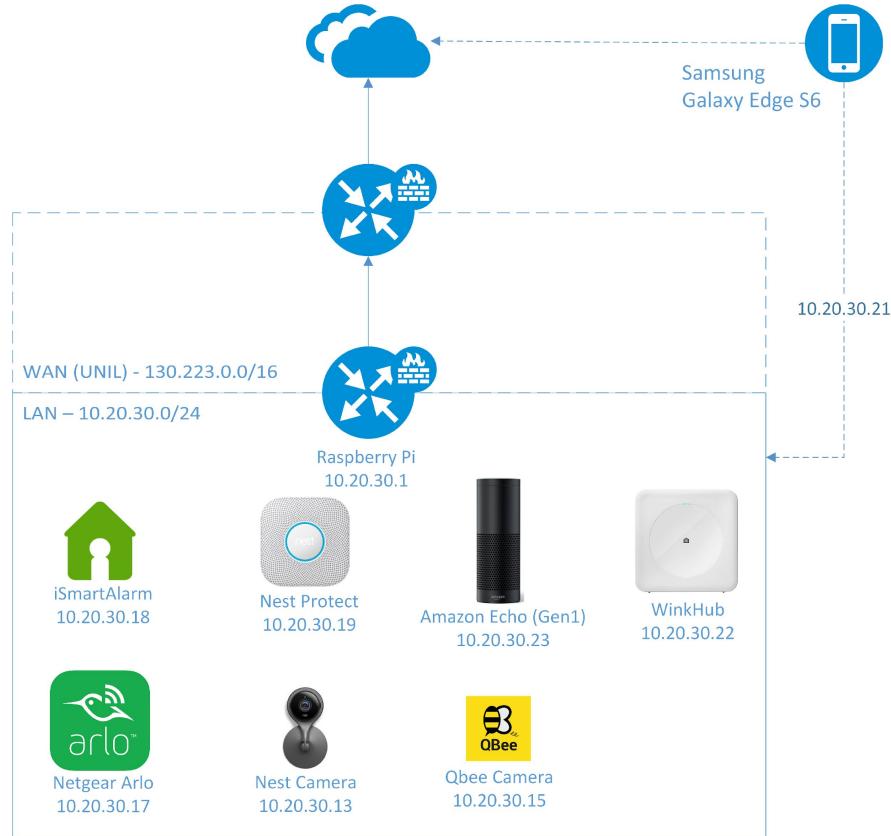
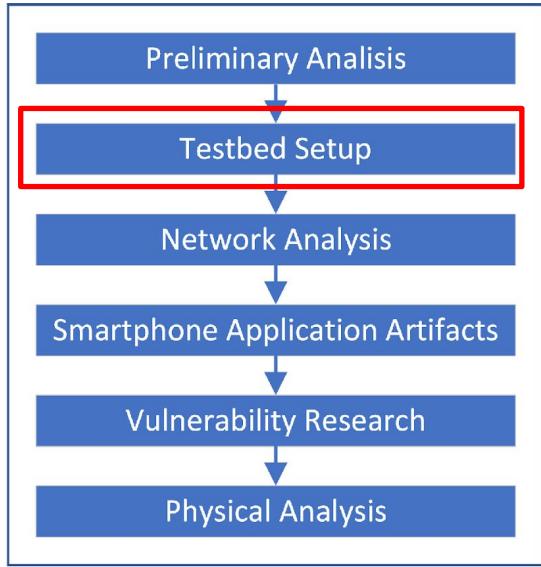


Methodology

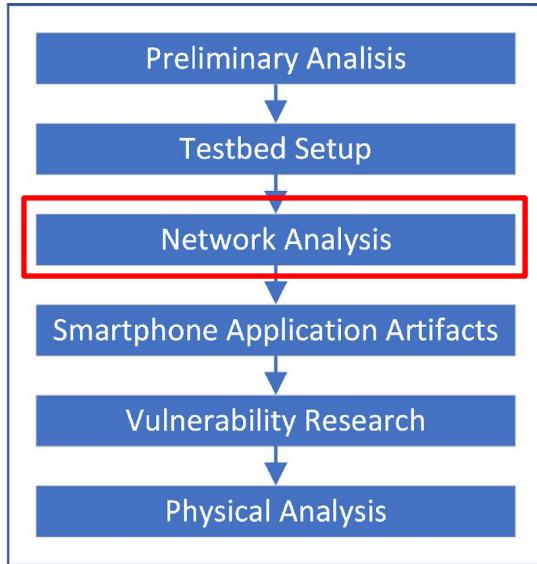


- Literature review
- Existing Vulnerability Reports
- Home automation communities

Methodology



Methodology



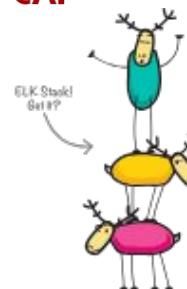
Who?

TCPDUMP & LIBPCAP

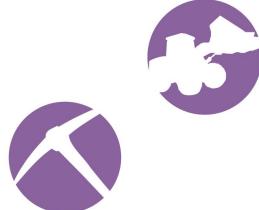


How?

WIRESHARK

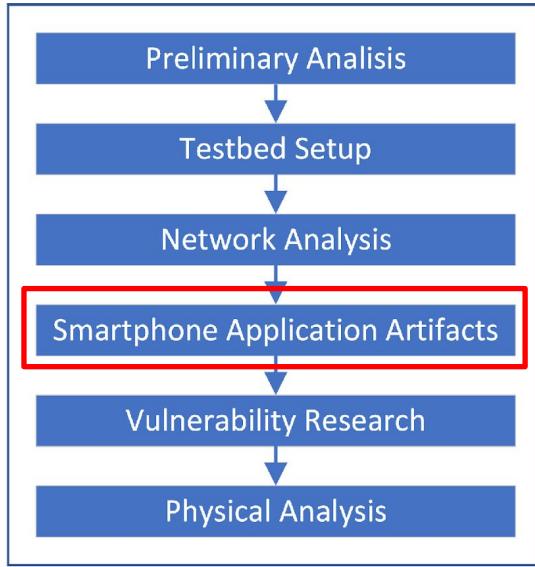


E Elasticsearch
L Logstash
K Kibana



What?

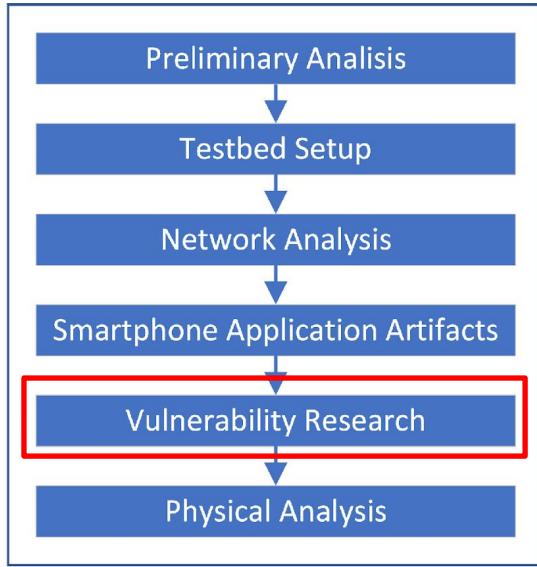
Methodology



What traces on a smartphone?

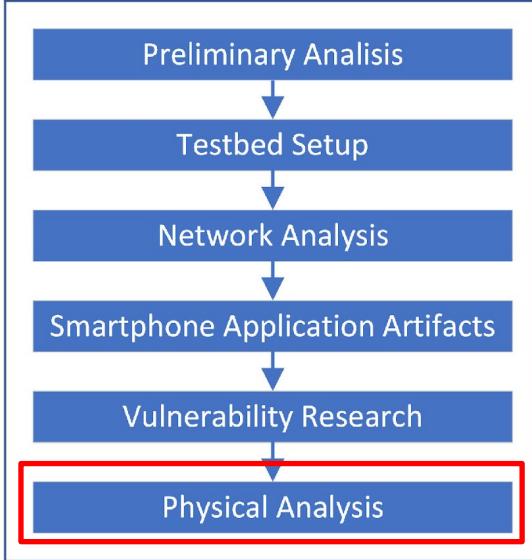
- Traditional Tools -> No parsers
- Manual investigation and correlation
- Plugin development

Methodology



- Builds on Network Analysis
 - Listening ports, Traffic Type, Traffic Content
- MITM
 - mitmproxy, SSLsplit
- Firmware Analysis
 - Binwalk, strings, hexdump...

Methodology



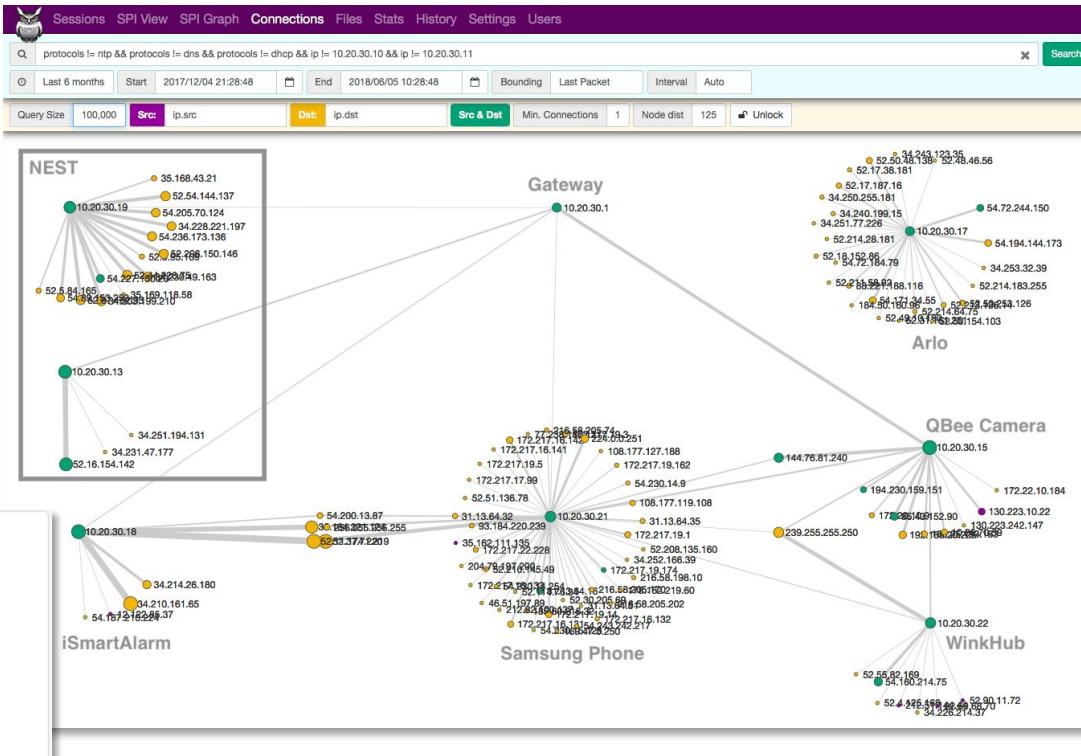
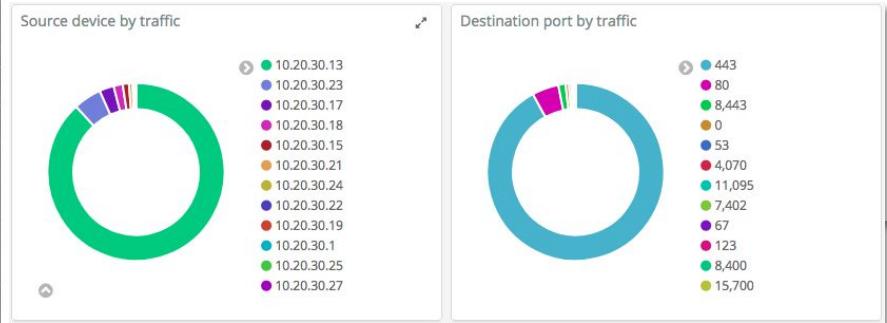
- Serial Connection
- Root Access
- (JTAG)
- (Chip Off)
- Physical Images
- NVRAM Settings
- Filesystem Images



A screenshot of a terminal window titled 'less ismart.cap (less)'. The window displays hex dump data starting with '00000000: 00 00 00 00 00 00 00 00' and ending with '00000160: 00 00 00 00 00 00 00 00'. Below the hex dump is a file tree command output: 'francesco@Fluffy: ~/Movies/wink (zsh)\$ tree . -L 1'. The tree output shows the directory structure: '.' containing 'bin', 'database', 'database_default', 'dev', 'etc', 'home', 'lib', 'lib32 -> lib', 'linuxrc -> bin/busybox', 'media', 'nftests', 'mnt', 'opt', 'proc', 'root', 'run -> tmp', 'sbin', 'tmp', 'usr', and 'var'. At the bottom, it says '20 directories, 1 file'.

Network Analysis

- Mostly TLS
- Only a minority is local traffic.



Network Analysis

- iSmartAlarm
 - «Encrypted» traffic with Android app ¹
 - Unauthenticated diagnostic logs access (CVE-2018-16224)

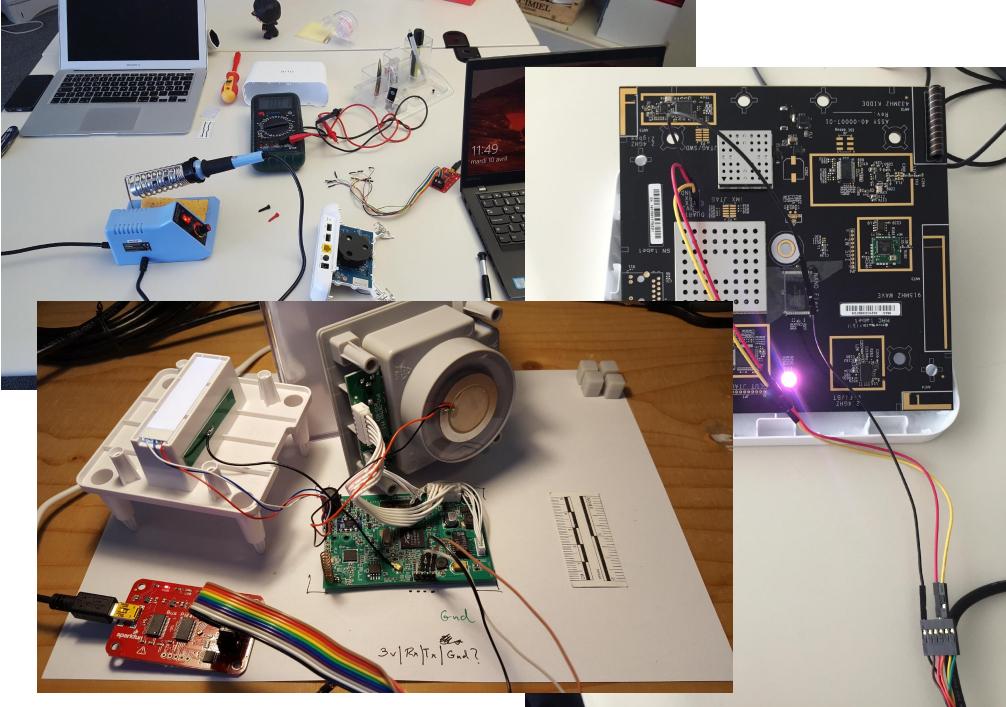
```
{
  "SensorID": "000A8540",
  "MessageType": "0",
  "TS": "1526290387832",
  "IsAlarm": "1",
  "fileGroup": "0",
  "ProfileId": "2",
  "ModeId": "2",
  "DetectAlarm": "0",
  "timestamp": "2018-05-14T11:33:07",
  "event": "Door Open"
},
```

```
AF9::APSEND::the receive message is AP auto send, try to get more message$@00000005AFADAF9::A
d$@00000005AFADAF9::ALARMD00R::{"SensorID":"000A8540","MessageType":"1","TS":"1526389497550",
AFB::APSEND::the receive message is AP auto send, try to get more message$@00000005AFADAFB::A
```

- QBee
 - Cleartext traffic with Android app (CVE-2018-16225)
 - (UPnP port forwarding)

```
▼ Hypertext Transfer Protocol
  ▶ GET /config/get?service=webdis HTTP/1.1\r\n
    Host: 10.20.30.15:15700\r\n
    Accept-Encoding: gzip\r\n
    Connection: keep-alive\r\n
    Content-Type: application/json; charset=UTF-8\r\n
  ▼ Cookie: JSESSIONID=0b1b2466-0715-4399-83bd-e82e79daa81d, SERVICE=WEBDIS, GC_ID=14602, LD_ID=14887\r\n
```

Physical Analysis



- Memory Images
 - Arlo, iSmartAlarm Cube One
- Filesystem Images
 - Wink, Arlo (Partially)
- NVRAM Settings
- Settings & Events depending on device

Physical Analysis

1. less ismart.cap (less)

```
md.b 0x0 0x00000000
00000000: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 .....  
00000010: 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000030: 00 00 00 00 12 01 00 02 00 00 00 48 8f 14 50 53 .....@..PS  
00000040: 01 00 00 00 00 01 02 00 00 02 00 00 48 01 00 .....P..@..  
00000050: 09 02 43 00 01 01 00 88 50 04 00 00 07 ff ff ..C...P..  
00000060: ff 08 07 05 81 02 00 02 00 07 05 01 02 00 02 00 .....  
00000070: 07 05 82 02 00 02 00 07 05 02 02 00 02 00 07 05 .....  
00000080: 83 02 00 02 00 07 05 03 02 00 02 00 07 05 84 02 .....  
00000090: 00 02 00 07 05 04 00 00 00 00 00 00 00 00 00 00 .....  
000000a0: 00 07 05 06 02 00 00 00 00 00 00 00 00 00 00 00 .....  
000000b0: 79 26 00 bc 45 20 00 00 00 00 00 00 00 00 00 00 .....  
000000c0: 35 24 00 bc f5 20 00 00 00 00 00 00 00 00 00 00 .....  
000000d0: 01 27 00 bc f9 20 00 00 00 00 00 00 00 00 00 00 .....  
000000e0: 35 24 00 bc 4d 00 00 00 00 00 00 00 00 00 00 00 00 .....  
000000f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000140: 00 0e 27 07 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
:  
20 directories, 1 file
```

+ ~/Movies/wink (zsh)

```
tree . -L 1
+ ~/Movies/wink
.
+- bin
  +- database
    +- database_default
  +- dev
  +- etc
  +- home
  +- lib
    +- lib32 -> lib
    +- linuxrc -> bin/busybox
  +- media
  +- mfgtests
  +- mnt
  +- opt
  +- proc
  +- root
  +- run -> tmp
  +- sbin
  +- sys
  +- tmp
  +- usr
  +- var
```

```
22 CFE> nvram show
23 x_broker_port=443
24 ap_mode_cur=1
25 wlg_wds_mode=1
26 wl_radius_port=1812
27 wla_temp_wep_length_2=0
28 wlan_acl_dev24=
29 wan2_dns=
30 wl0_scb_activity_time=0
31 gui_check_enable=1
32 wlan_acl_dev25=
```

2. francesco@eduroam-079: ~/Servida/IoT Master Thesis - Documenti/firmwares/ismartalarm/dump (zsh)

```
+ firmwares/ismartalarm/dump binwalk ismart_80.img
```

DECIMAL	HEXADECIMAL	DESCRIPTION
3960	0xF78	uImage header, header size: 64 bytes, header CRC: 0x1A086BAF, created: 2013-04-28 09:57:43, image size: 107896 bytes, Data Address: 0x00200000, Entry Point: 0x00200000, data CRC: 0x8FDE24EE, OS: Linux, CPU: MIPS, image type: Standalone Program, compression type: none, image name: "SPI Flash Image"
2184976	0x215710	U-Boot version string, "U-Boot 1.1.3 (Apr 28 2013 - 17:57:40)"
2185568	0x215960	CRC32 polynomial table, little endian
3145728	0x300000	LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 6126127 bytes

Smartphone Application Artifacts

- Android Phone (Samsung Galaxy Edge S6)

iSmartAlarm	Arlo	Nest	QBee	Wink
Cloud Credentials Events UPnP discovered devices <i>MQTT Topic Infos</i>	Cloud Credentials (token) Linked devices Thumbnails	User Informations Dispositifs Liés Events Video Extracts	Cloud Credentials	User Info Linked Devices Events (Long term storage)

△ Source File

com.vestiacom.qbeecamera_preferences.xml	Username	Secret	Secret Type	Service
	JPinkman	Esc_iot_2018	Password	QBee

Hex Strings Application Indexed Text Message File Metadata Results Other Occurrences Video Triage

Page: 1 of 1 Page Go to Page: Script: Latin - Basic

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="4Y6xz8byViS81N4VAY0Z0QjYYOZa21Os9NkIpMj2gEA">
>3g9oh9jar0icqnsi7vep6jls4t</string>
  <string name="DGPwuGi4LKfQX0YCwDXHtw">kcugM+KZSjL+3cBbZagBdw</string>
  <string name="AFevat4b05WkgsNn2BMR1Q">pGAlaM03Xrpbr37ip8lpQg</string>
</map>
```

iSmartAlermData.xml 2018-04-11 16:26:06 CB

Hex Strings Application Indexed Text Message File Metadata Results

Page: 1 of 1 Page Go to Page:

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="password">esc_iot_2018</string>
  <string name="phoneNum">0792245315</string>
```

Smartphone Application Artifacts

Skylab

- TheCube** Online >
- Contact Sensors**
- TheBouncer - D...** Closed >
- Motion Sensors**
- TheMotion - Mo...** Offline >
- Remote tags**
- TheBoss - Remo...** >

TB_CameraDairy	(0)
TB_CountryInfo	(10)
TB_IPUDairy	(170)
TB_IPUVersionInfo	(4)
TB_ISC3Dairy	(0)
TB_ISC3VideoInfo	(0)
TB_PushMessageInfo	(0)
TB_SensorDairy	(178)
TB_camera	(0)
TB_ipulinfo	(0)
TB_isc3info	(0)
TB_logInfo	(1)
TB_profilecamera	(0)

date	action	IPUID	logType	sensorName	operator	sensorType	sensorID	userID	profileId	profileName
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
145	1521108904	004D3209D9E4	2		TheBoss (Remote Tag)				2	DISARM
146	1521108878	004D3209D9E4	2		TheBoss (Remote Tag)				1	HOME
147	1521108826	2	004D3209D9E4	5						
148	1521042170		004D3209D9E4	2	TheBoss (Remote Tag)				2	DISARM
149	1521041811	1	004D3209D9E4	5						
150	1521037461		004D3209D9E4	2	skyman				2	DISARM
151	1521037151		004D3209D9E4	2		TheBoss (Remote Tag)			2	DISARM
152	1521037119	1	004D3209D9E4	1	TheBounc...					

Investigation



App Decompilation

Source File	Data Source	Tags	Event	Event Timestamp	Event Type	Device	Device Type
iSmartAlarm.DB	blk0_sda.bin		Contact Sensor Closed	2018-05-17 14:58:15 CEST	Sensor Info	000A8540	Contact Sensor
iSmartAlarm.DB	blk0_sda.bin		Contact Sensor Open	2018-05-17 14:58:03 CEST	Sensor Info	000A8540	Contact Sensor
iSmartAlarm.DB	blk0_sda.bin		Contact Sensor Closed	2018-05-17 14:57:06 CEST	Sensor Info	000A8540	Contact Sensor
iSmartAlarm.DB	blk0_sda.bin		Contact Sensor Open	2018-05-17 14:52:10 CEST	Sensor Info	000A8540	Contact Sensor
iSmartAlarm.DB	blk0_sda.bin		Contact Sensor Closed	2018-05-17 11:39:50 CEST	Sensor Info	000A8540	Contact Sensor
iSmartAlarm.DB	blk0_sda.bin	DISARM		2018-05-17 10:37:52 CEST	Profile Change	pandadodu	Remote Tag or Smartphone
iSmartAlarm.DB	blk0_sda.bin		Contact Sensor Open	2018-05-17 10:34:36 CEST	Sensor Info	000A8540	Contact Sensor
iSmartAlarm.DB	blk0_sda.bin	DISARM		2018-05-17 10:34:31 CEST	Profile Change	pandadodu	Remote Tag or Smartphone
iSmartAlarm.DB	blk0_sda.bin	HOME		2018-05-17 10:34:17 CEST	Profile Change	TheBoss	Remote Tag or Smartphone
iSmartAlarm.DB	blk0_sda.bin		Unknown Action	2018-05-17 10:34:17 CEST	?User Info?	TheBoss	Remote Tag or Smartphone
iSmartAlarm.DB	blk0_sda.bin		Contact Sensor Closed	2018-05-17 10:34:15 CEST	Sensor Info	000A8540	Contact Sensor
iSmartAlarm.DB	blk0_sda.bin	DISARM		2018-05-17 10:22:30 CEST	Profile Change	TheBoss	Remote Tag or Smartphone
iSmartAlarm.DB	blk0_sda.bin	DISARM		2018-05-17 10:22:30 CEST	?User Info?	TheBoss	Remote Tag or Smartphone
iSmartAlarm.DB	blk0_sda.bin	ARM		2018-05-17 10:22:22 CEST	Profile Change	JPinkman	Remote Tag or Smartphone

Smartphone Application Artifacts



Arlo cache

Nest cache

```
joinman2018@gmail.com.json
{
  "userId": "A79GZB-316-31081729",
  "email": "joinman2018@gmail.com",
  "token": "...",
  "serial": "...",
  "paymentId": "35656366",
  "accountStatus": "registered",
  "serialNumber": "4B037B75A1EC9",
  "countryCode": "CH",
  "toUpdate": false,
  "policyUpdate": false,
  "appStore": {
    "validEmail": true,
    "arlo": true,
    "dateCreated": 1521034216242
  }
}
joinman2018@gmail.com.json 20:1
LF  UTF-B  JSON  0 files
```

Unil

UNIL | Université de Lausanne

Ecole des sciences criminelles

Arlo Settings (Realm DB)

Official Apps

Aggregators

Arlo
Nest

ID	Type	Json
Filter	Filter	Filter
3	activity	{"action":{"action_automation_mode":null}}
4	activity	{"action":{"action_automation_mode":null}}
5	activity	{"action":{"action_automation_mode":null}}
6	activity	{"action":{"action_automation_mode":null}}
7	activity	{"action":{"action_automation_mode":null}}
8	activity	{"action":{"action_automation_mode":null}}
9	activity	{"action":{"action_automation_mode":null}}
10	activity	{"action":{"action_automation_mode":null}}
11	activity	{"action":{"action_automation_mode":null}}
12	activity	{"action":{"action_automation_mode":null}}

```
('2018-04-10T00:23:00', u'SKYLAB Office Camera (LabCam)', u'camera', {u'capturing_video': True})
('2018-04-10T00:23:24', u'SKYLAB Office Camera (LabCam)', u'camera', {u'capturing_video': False})
('2018-04-10T00:23:25', u'SKYLAB Office Camera (LabCam)', u'camera', {u'capturing_video': True})
('2018-04-10T05:29:02', u'TheTabletter Watcher (Arlo Cam)', u'camera', {u'mode': None})
('2018-04-10T05:29:03', u'TheTabletter Watcher (Arlo Cam)', u'camera', {u'mode': u'armed'})
('2018-04-10T08:13:43', u'SKYLAB Office Camera (LabCam)', u'camera', {u'capturing_video': False})
('2018-04-10T08:13:44', u'SKYLAB Office Camera (LabCam)', u'camera', {u'capturing_video': True})
('2018-04-10T08:41:43', u'SKYLAB Office Camera (LabCam)', u'camera', {u'motion': True})
('2018-04-10T08:48:11', u'TheTabletter Watcher (Arlo Cam)', u'camera', {u'motion': True})
('2018-04-10T08:50:57', u'TheTabletter Watcher (Arlo Cam)', u'camera', {})
('2018-04-10T09:13:31', u'SKYLAB Office Camera (LabCam)', u'camera', {u'capturing_video': False})
('2018-04-10T09:13:38', u'SKYLAB Office Camera (LabCam)', u'camera', {u'capturing_video': True})

Process finished with exit code 0
```

Wink Hub Events

Cloud

Increased persistence

Access

- Reuse of credentials on smartphone
- Request to Service Provider

Arlo

- Recorded videos

DFRWS Challenge submissions

- Wink Hub - Devices & Events, iSmartAlarm - Members, Nest - Devices, Events & Clips ¹

The screenshot shows a code editor with a Python script titled 'arlo.py'. The script is designed to download recorded videos from an Arlo library. It uses the 'arlo' library to get the library of recordings from seven days ago and then iterates through them to download each video as an MP4 file. The script also includes logic to handle streaming and chunked downloads. The code is annotated with comments explaining its functionality.

```
#!/usr/bin/python
# coding: utf-8
# This file is part of the Arlo Forensic project.
# https://github.com/dfirfrancesco/arlo-forensic
# Copyright (C) 2018 Francesco Sestini
#
# This program is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 3 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program. If not, see <http://www.gnu.org/licenses/>.

# Project: https://github.com/dfirfrancesco/arlo-forensic
# Author: dfirfrancesco
# Date: 2018-05-31
# Version: 0.1.0

# This script is used to download recorded videos from an Arlo library.
# It uses the arlo library to get the library of recordings from seven days ago
# and then iterates through them to download each video as an MP4 file.

# The videos produced by Arlo are pretty small, even in their longest, best quality settings,
# but you should probably prefer the chunked stream (see below).
### Download the whole video into memory as a single chunk.
# video = arlo.GetRecording(recording['presignedContentUrl'])
# f = open('videos/' + recording['uniqueId'] + '.mp4', 'w')
# f.write(video)
# f.close()
# Or:
# Get video as a chunked stream; this function returns a generator.
stream = arlo.StreamRecording(recording['presignedContentUrl'])
with open('videos/' + recording['uniqueId'] + '.mp4', 'wb') as f:
    for chunk in stream:
        f.write(chunk)
    f.close()

print('Downloaded video ' + recording['uniqueId'] + ' from ' + recording['createdDate'] + ', ')
```

Run: /Users/francesco/.virtualenvs/Pentesting/bin/python /Users/francesco/Switchdrive/uni/msc/002_UNIL/999_Master_Thesis/pentesting/arlo/arlo.py

24:1 LF: UTF-8: Git: master : Event Log

Freezing the IoT crime scene?

Live Data (Transmitted)

- Authentication Credentials (e.g. CVE-2018-16225)
- Current Events

Stored Data

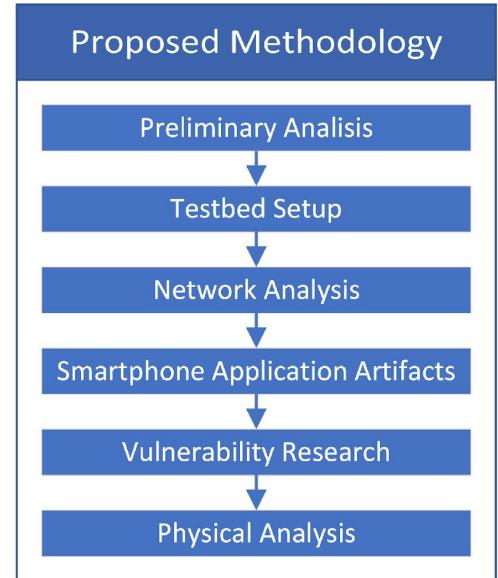
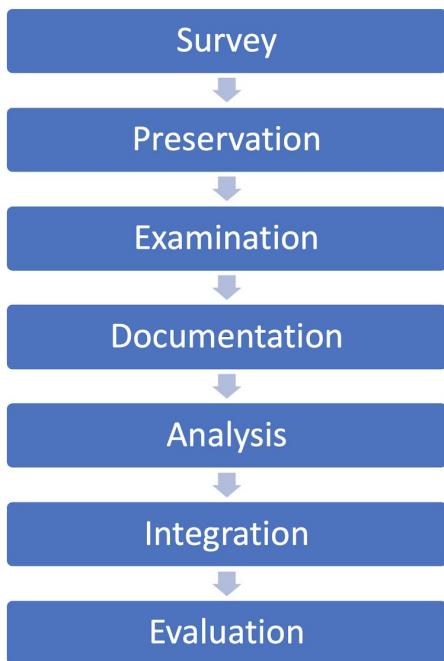
- Not always persistent
- Sometimes accessible live (w/ previous knowledge of the device)
 - E.g. CVE-2018-16224

First responder activities generate IoT traces at scene

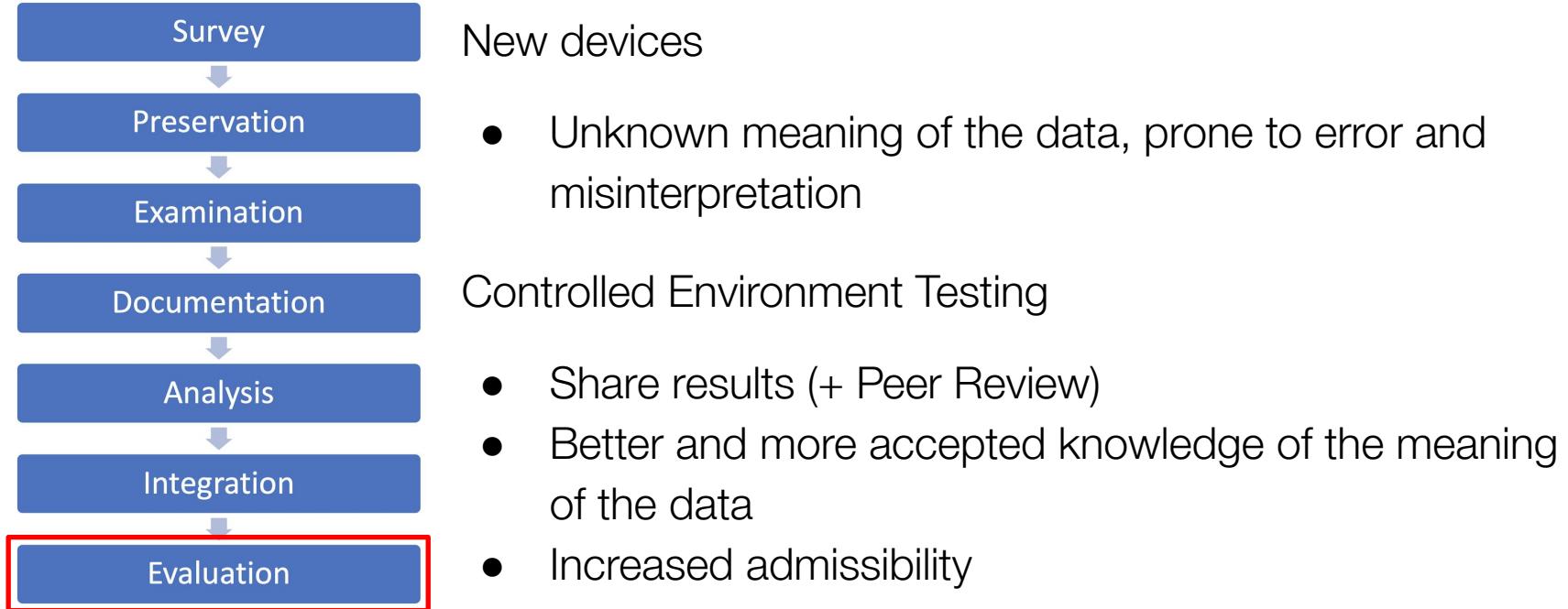
- Risk of data loss!



Discussion



Discussion



Issues

- Smartphone artifacts not produced in background
- Physical:
 - Extraction methods
 - Volatility of traces
- Variety of protocols

Future Research

Study common smarthome IoT devices

Analyse IoT RF activities (e.g., Zigbee, Z-Wave)

Chip-off analysis



https://github.com/fservida/msc_autopsy_plugins

https://github.com/fservida/msc_thesis



<https://francescoservida.ch>

francesco.servida@unil.ch

Thank You.