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

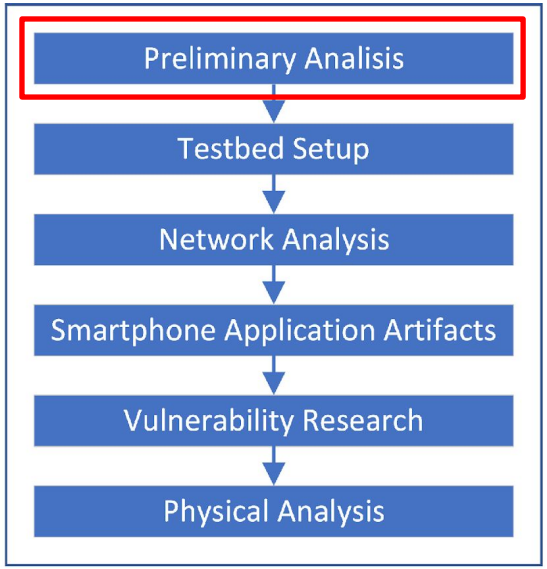
- Proactive collection

Home IoT

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

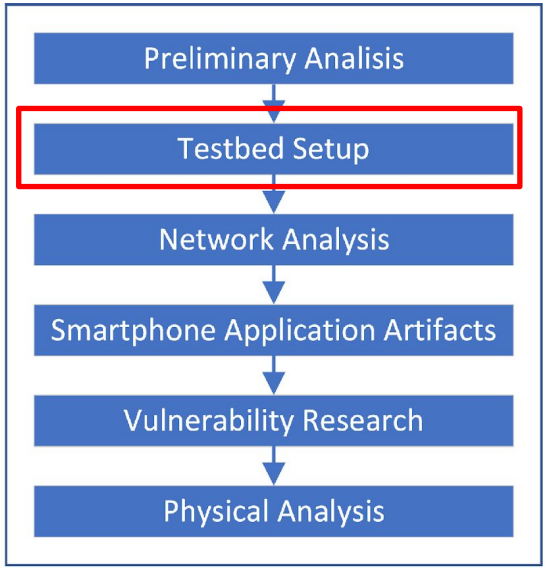
Methodology

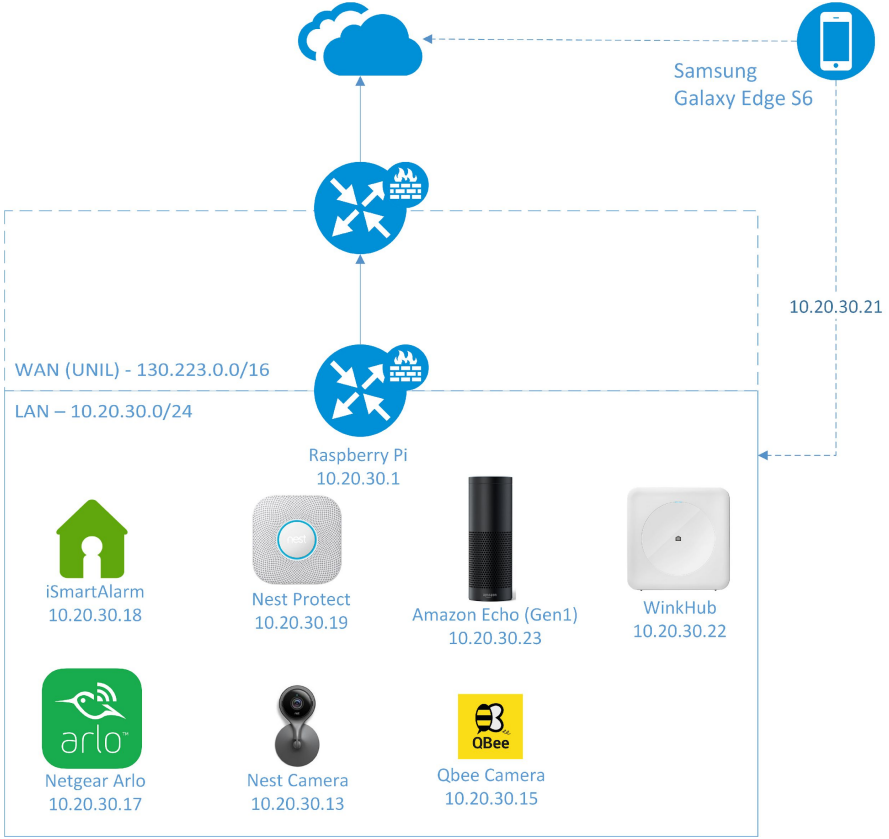
Methodology



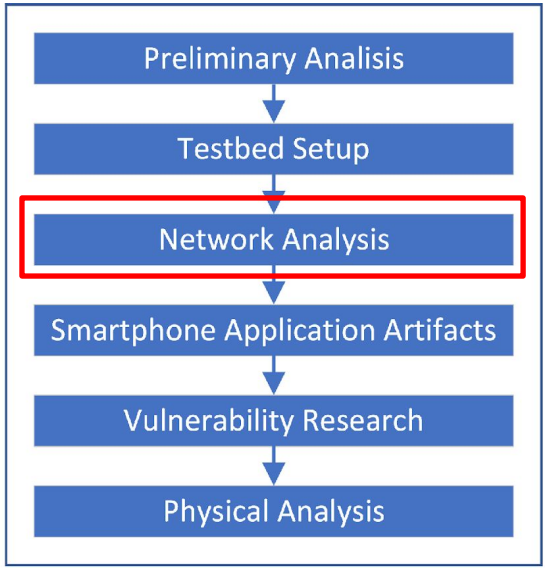
- Literature review
- Existing Vulnerability Reports
- Home automation communities

Methodology





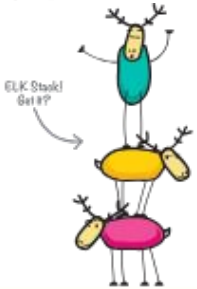
Methodology



Who? How? What?

TCPDUMP & LIBPCAP

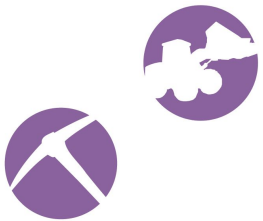
WIRESHARK



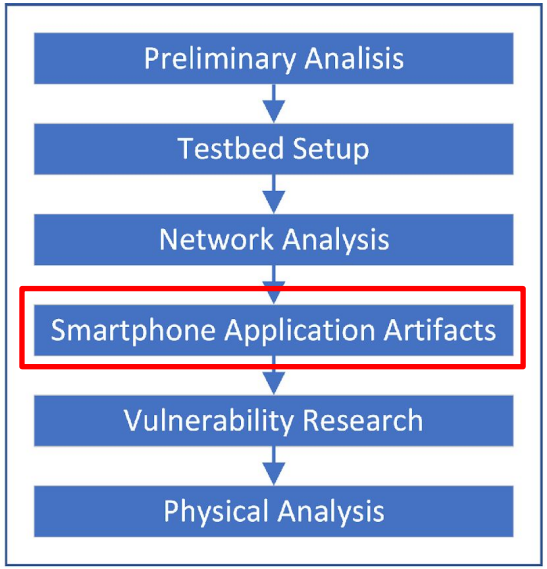
E Elasticsearch

L Logstash

K Kibana



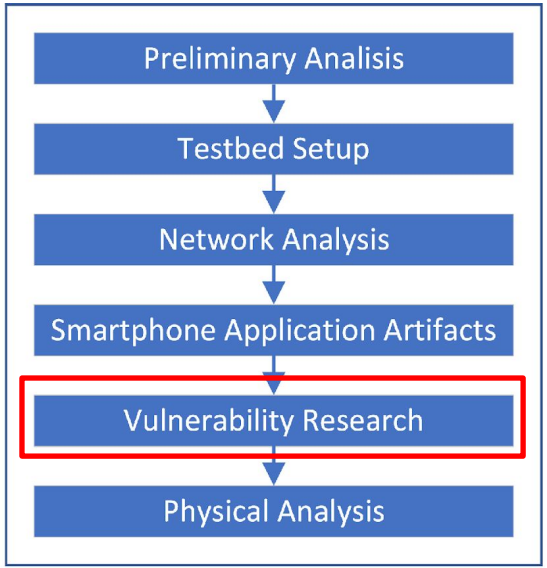
Methodology



What traces on a smartphone?

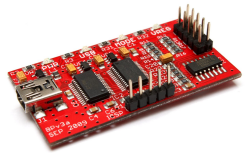
- Traditional Tools -> No parsers
- Manual investigation and correlation
- Plugin development

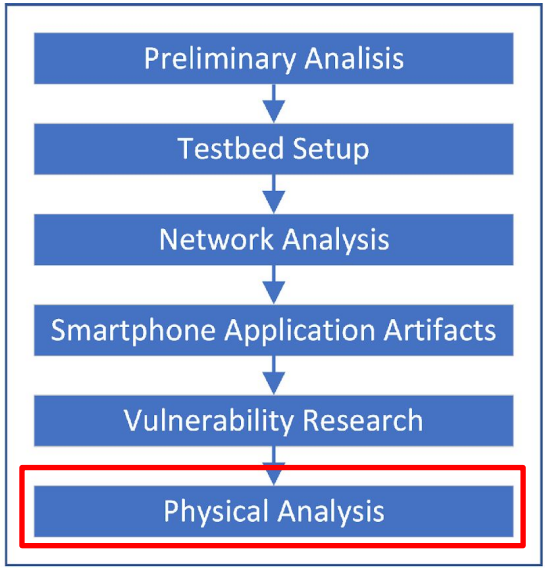
Methodology



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

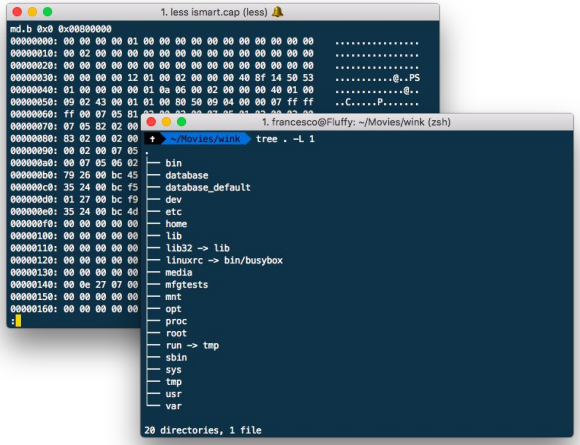
Methodology





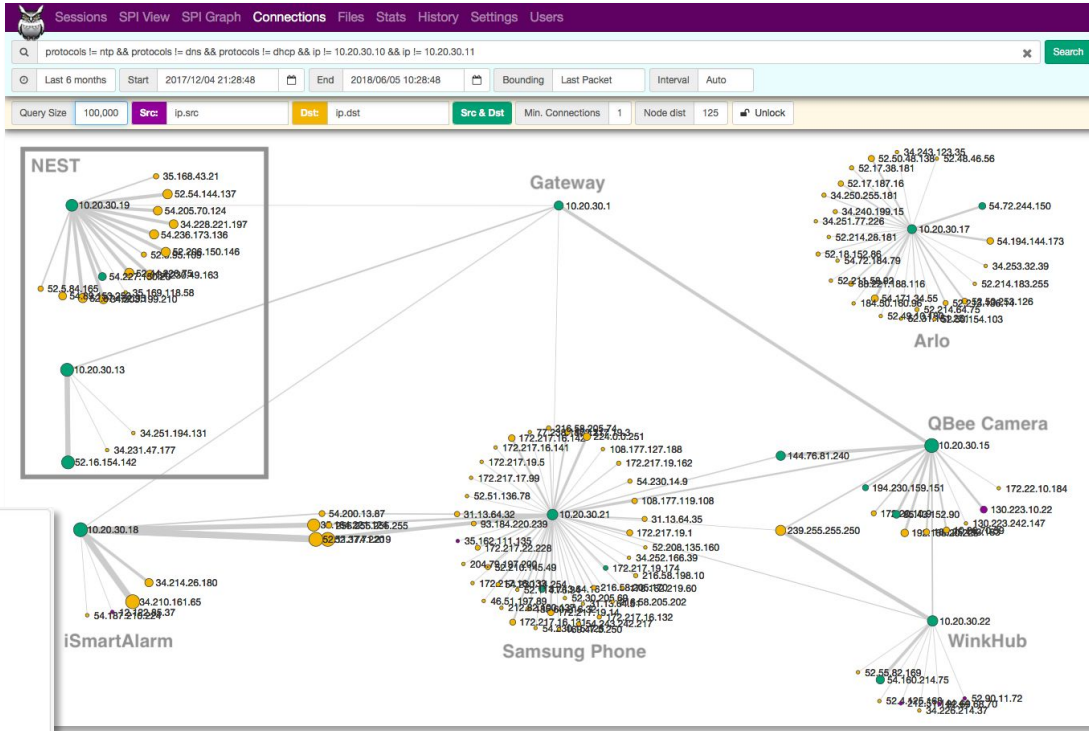
- Serial Connection
- Root Access
- (JTAG)
- (Chip Off)

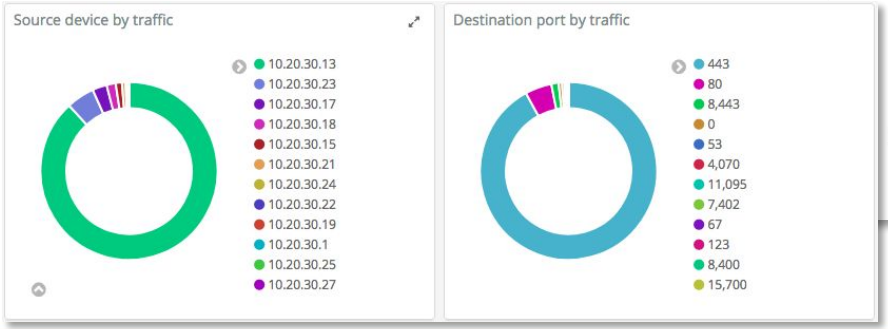
- Physical Images
- NVRAM Settings
- Filesystem Images



Network Analysis

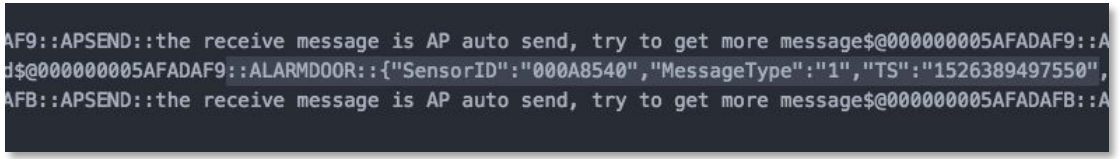
- Mostly TLS
- Only a minority is local traffic.





Network Analysis

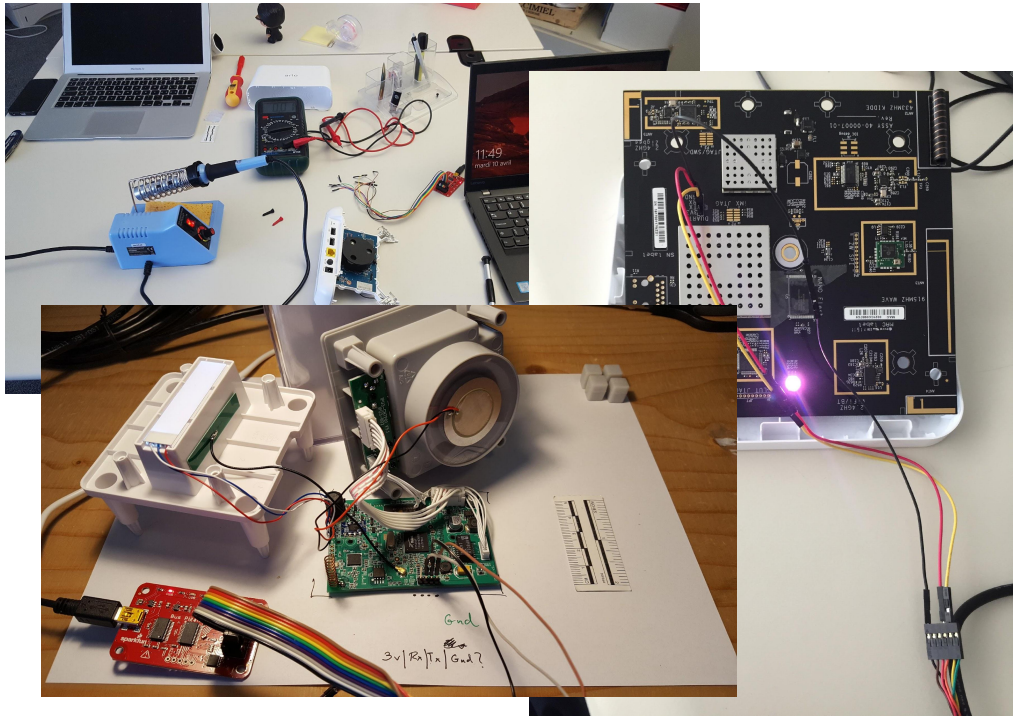
- iSmartAlarm
  - «Encrypted» traffic with Android app [1]
  - Unauthenticated diagnostic logs access (CVE-2018-16224)



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

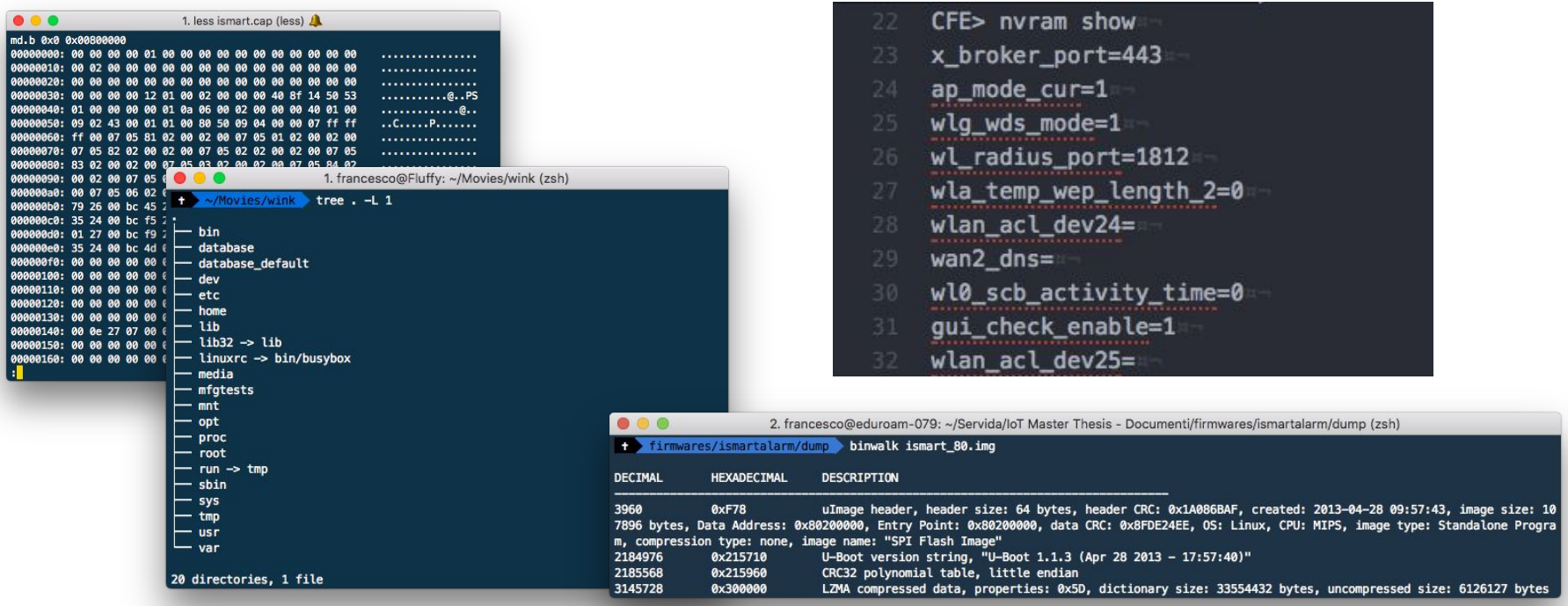
(1) https://dojo.bullguard.com/dojo-by-bullguard/blog/burglar-hacker-when-a-physical-security-is-compromised-by-iot-vulnerabilities/

Physical Analysis



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

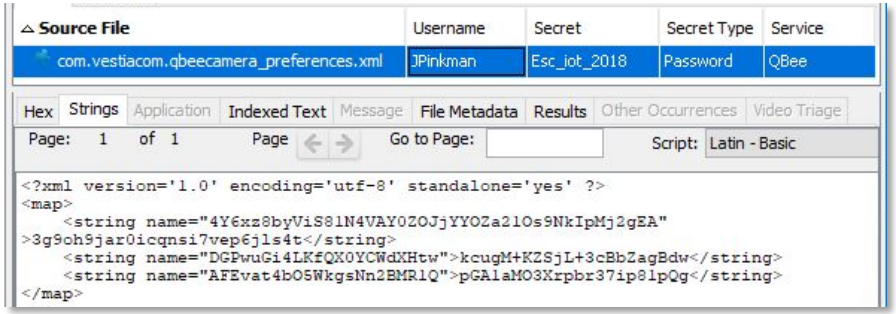
Physical Analysis

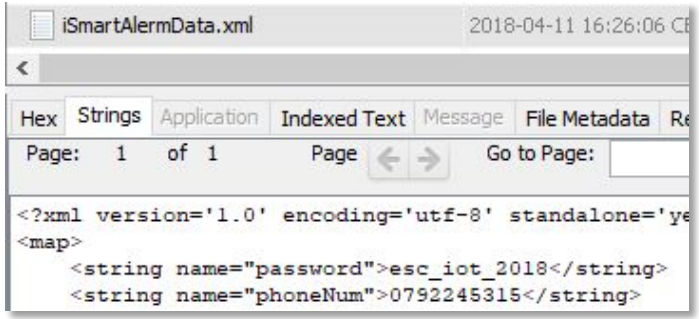


Smartphone Application Artifacts

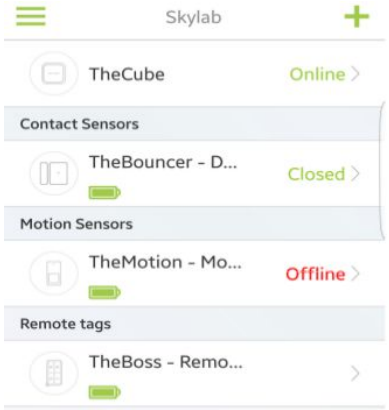
- Android Phone (Samsung Galaxy Edge S6)

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





Smartphone Application Artifacts



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_ipuInfo	(0)
TB_isc3Info	(0)
TB_logoInfo	(1)
TB_profileIcamera	(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

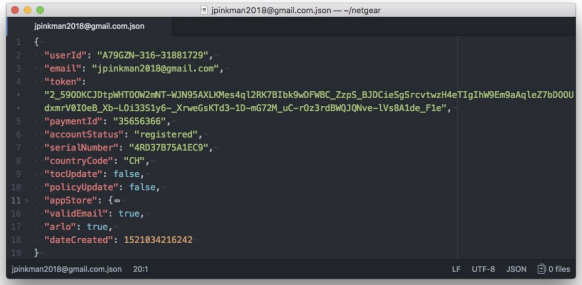
Nest cache

Arlo cache

Official Apps ..... Aggregators

Arlo
Nest

	ID	Type	Json
	Filter	Filter	Filter
3	5da92c11-f95c-...	activity	{"action":{"action_automation_mode":nu
4	285f4fc2-dc32-...	activity	{"action":{"action_automation_mode":nu
5	77b29345-9e9b...	activity	{"action":{"action_automation_mode":nu
6	9bbcedc4-68ae...	activity	{"action":{"action_automation_mode":nu
7	dd47f4a0-58e5-...	activity	{"action":{"action_automation_mode":nu
8	9d4ee653-c708...	activity	{"action":{"action_automation_mode":nu
9	1773b607-bb03...	activity	{"action":{"action_automation_mode":nu
10	4684cb1c-35fc-...	activity	{"action":{"action_automation_mode":nu
11	fd48b010-06e5-...	activity	{"action":{"action_automation_mode":nu
12	f921249d-6603-...	activity	{"action":{"action_automation_mode":nu



Arlo Settings (Realm DB)

```
('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

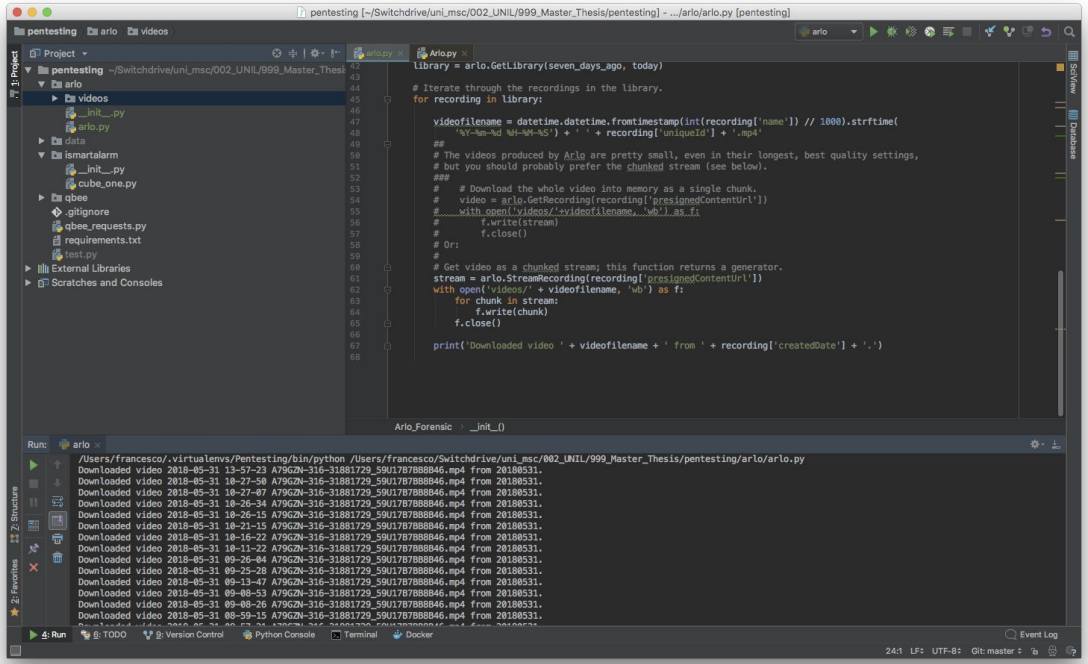
Increased persistence

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]

Freezing the IoT crime scene?

Live Data (Transmitted)

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

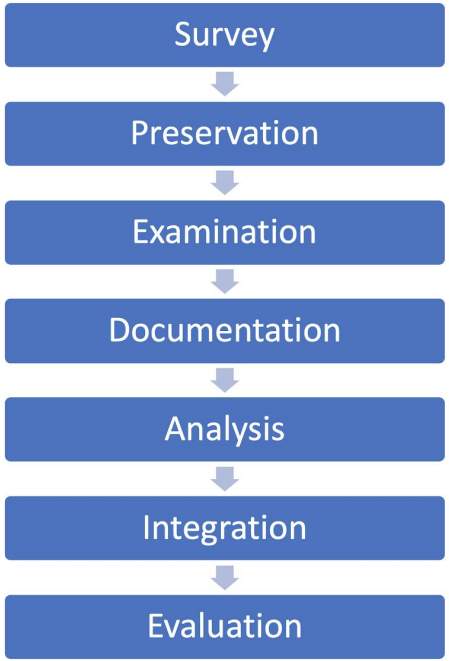
Stored Data

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

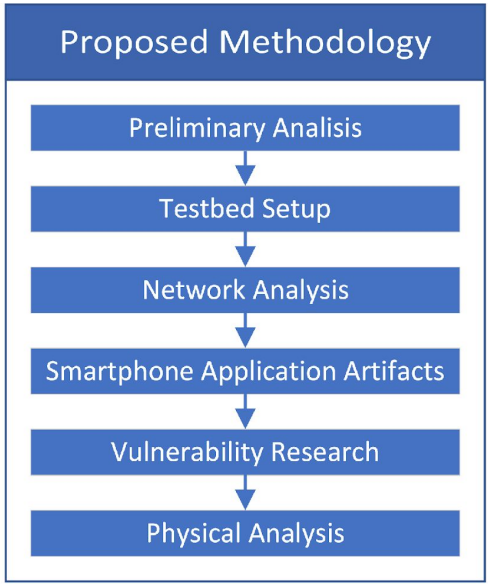
First responder activities generate IoT traces at scene

- Risk of data loss!

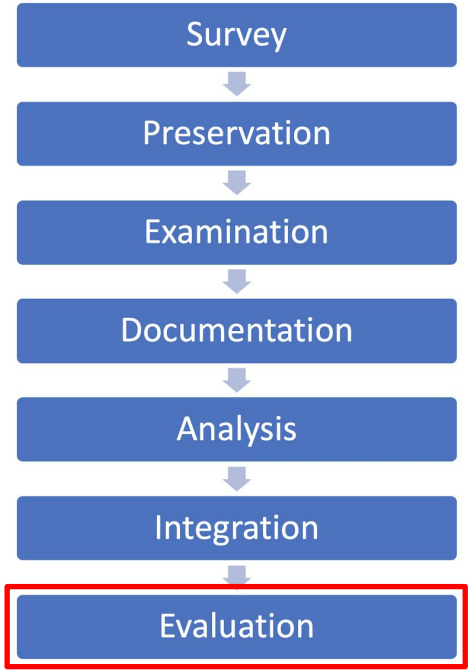
Discussion


Survey
Preservation
Examination
Documentation
Analysis
Integration
Evaluation


Which Traces? Where?
Developed Knowledge & Tools


Proposed Methodology
Preliminary Analisis
Testbed Setup
Network Analysis
Smartphone Application Artifacts
Vulnerability Research
Physical Analysis

Discussion



New devices

- Unknown meaning of the data, prone to error and misinterpretation

Controlled Environment Testing

- Share results (+ Peer Review)
- Better and more accepted knowledge of the meaning of the data
- Increased admissibility

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.