IoT Forensics: Analysis of a HIKVISION's mobile app

Evangelos Dragonas, Costas Lambrinoudakis, Michael Kotsis

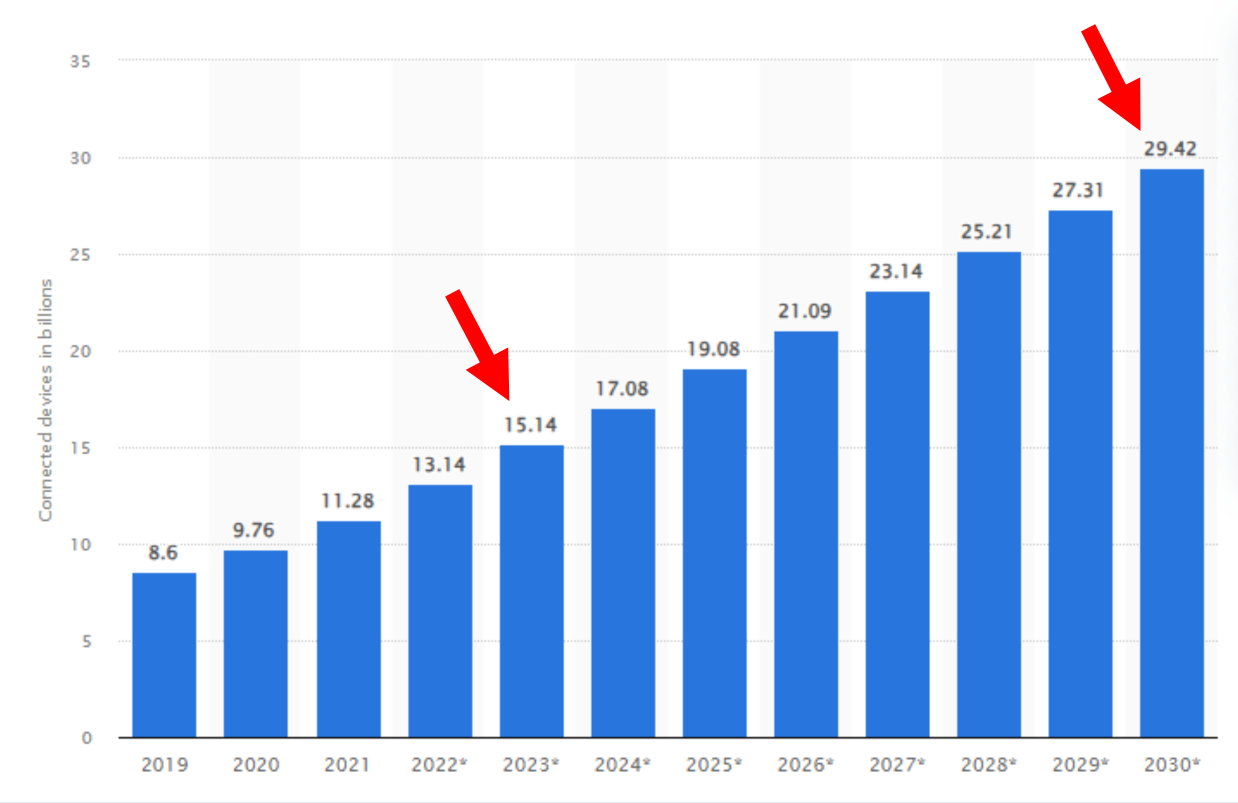
DFRWS USA 2023
10th JULY

Contents

- Introduction
- Equipment and Methodology
- Results
- Discussion
- Future Work

IoT Statistics

Number of IoT-connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030 (in billions)



source: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide

IoT Statistics - CCTV

source: Baig, et al., Future rity and digital forensics, Digital Investiga iin.2017.06.015

Literature Review - Research motivation
We do not know how to answer the following

- Which actions can the user perform remotely?

  -Anti-forensics?

  -Live View/Playback?

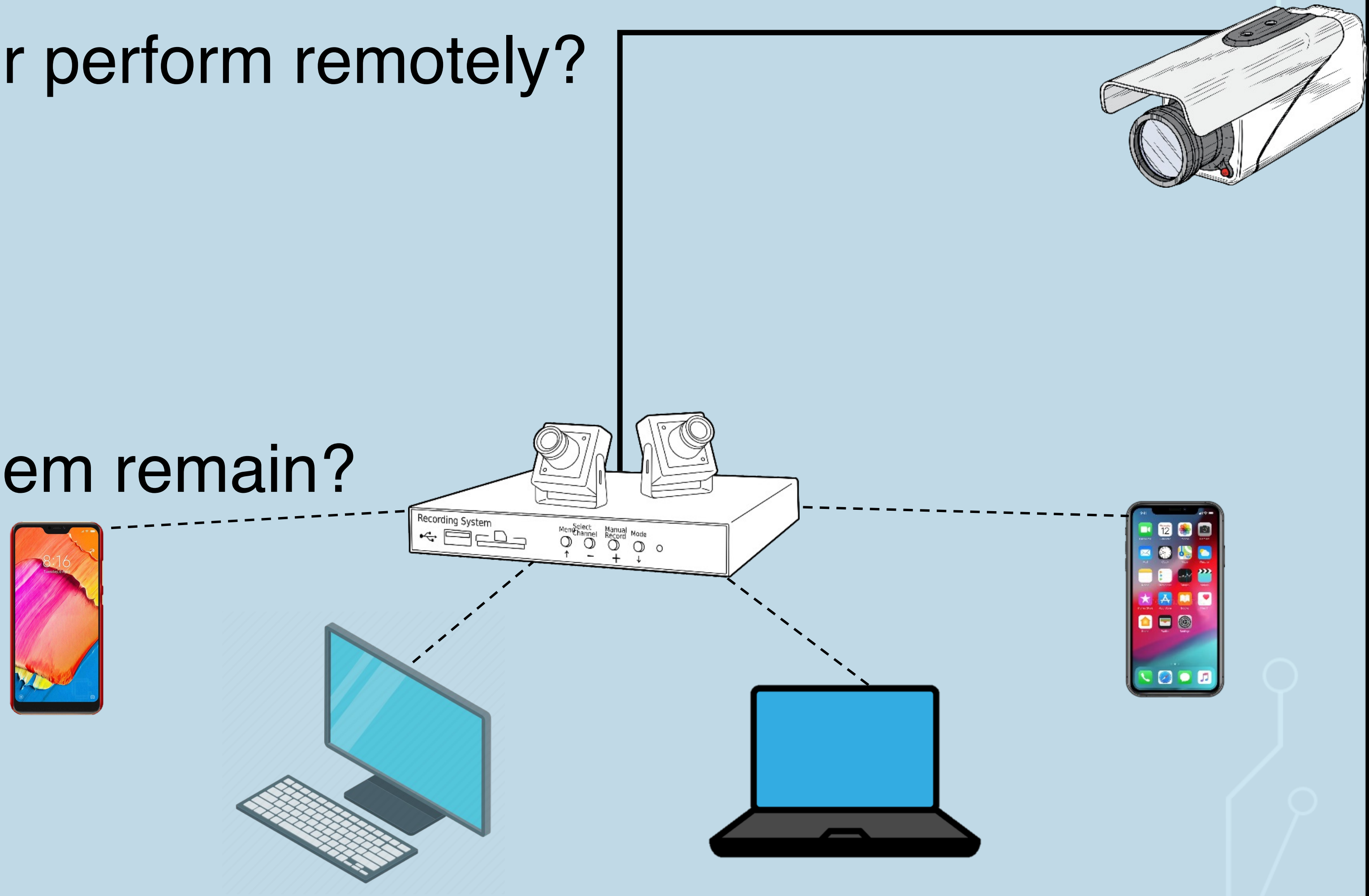
  -Anything else?

- What artifacts related to them remain?

  -Timestamps?

  -IP/Geolocation?

  -Log of actions?



HIKVISION

- Chinese manufacturer of surveillance equipment
- Leader in the global surveillance market[1]
- Variety of applications (available for multiple operating systems)
- Research regarding digital investigation of HIKVISION’s products is scarce

[1] https://www.researchandmarkets.com/report/surveillance-camera

Research motivation –Scope of this Paper

- Which actions can the user perform remotely?

  -Anti-forensics?

  -Live View/Playback?

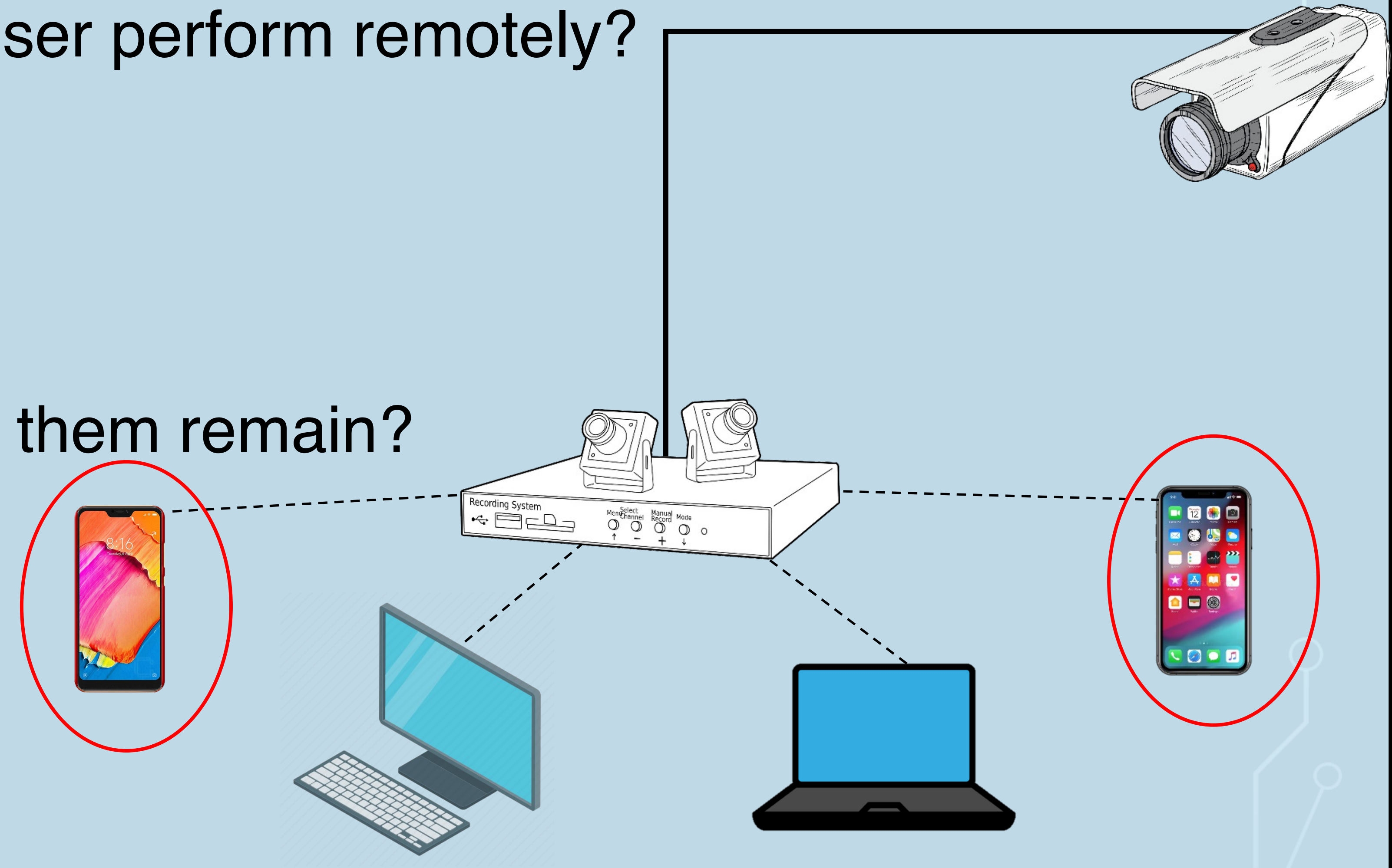
  -Anything else?

- What artifacts related to them remain?

  -Timestamps?

  -IP/Geolocation?

  -Log of actions?



Research contribution

- Explore features of a HIKVISION's mobile application
- Present artifacts from its forensic analysis on Android/iOS
- Exploit RAM to decrypt realm databases
- Contribute relevant parsers to ALEAPP and iLEAPP

Contents

- Introduction
- Equipment and Methodology
- Results
- Discussion
- Future Work

Equipment - Hardware

Hardware	Model/Version
HIKVISION Gen. 4th XVR	DS-7104HQHI-K1
LG G6	H870 - Android 9 (SPL May 2019)
iPhone X	A1901 – iOS 15.5
PC workstation	Windows 10 Pro (21H2)

Equipment - Software

Software	Version
Magisk	23
Palera1n	1.4.0
X-Ways Forensics	20.3 SR-4
DB Browser for SQLite	3.12.2
Realm Studio	13.0.2
ADB (Platform-Tools for Windows)	33.0.3
SSH	OpenSSH_for_Windows_8.1p1, LibreSSL 3.0.2
Magnet Acquire	2.59.0.32716
libimobiledevice	1.3.0
Frida	16.0.7
fridump3	-
CyberChef	9.55.0

Equipment – HIKVISION app of choice

- HIKVISION offers 2 mobile apps:

  -**“Hik-Connect - for End user”** and “HiLookVision”

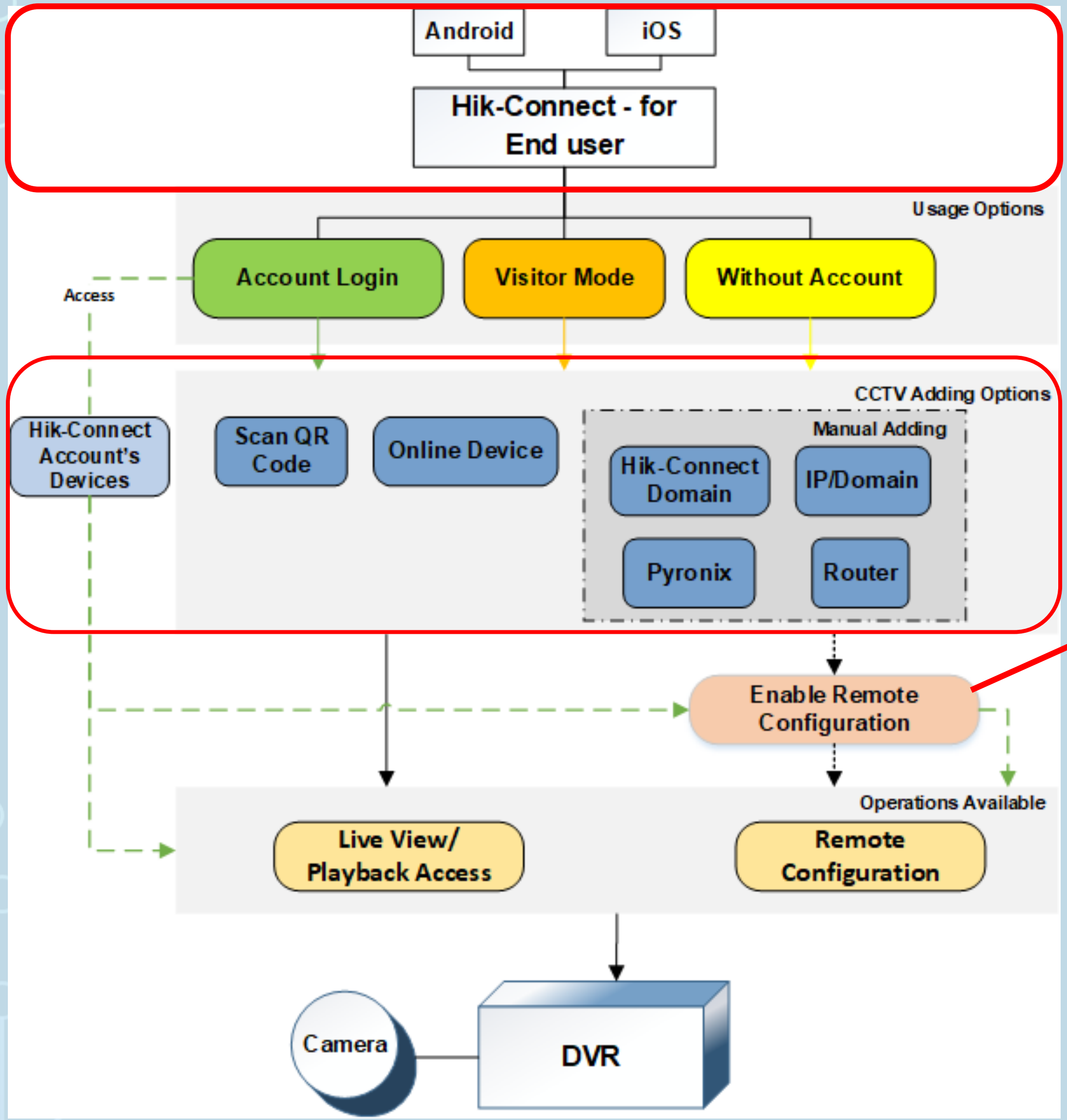
  -“Hik-Connect - for End user” surpassed 5 million Google Play Store downloads

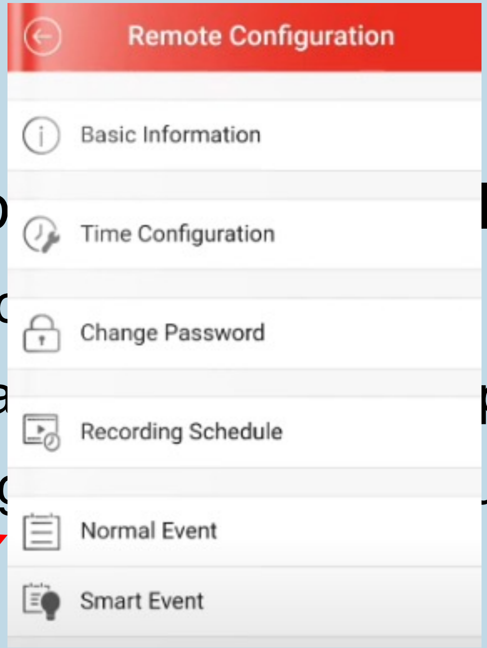
Application	Versions
Hik-Connect - for End user (com.connect.enduser)	Android versions- 5.0.0.1125, 5.0.1.1207 and 5.0.2.1213
Hik-Connect - for End user (com.hikvision.hikconnect)	iOS versions - 5.0.0, 5.0.1 and 5.0.2

Methodology

- Reconnaissance
- Preparation/ Collection
- Analysis

Methodology - Reconnaissance





Remote Configuration

- Basic Information
- Time Configuration
- Change Password
- Recording Schedule
- Normal Event
- Smart Event

- A Hik-Co lows:
  - Binding Io
  - Sharing a products
  - Accessing ucts
- The mobile app allows:
  - Viewing Live Footage/Stored Recordings
  - Creating/Storing media files
  - Remote Configuration of CCTV:
    --Users are **not able to format** the CCTV but they **can** disable the recording of any CCTV Camera

Methodology - Preparation

- CCTV was initialized and configured ☑
- DynDNS was utilized ☑
- The application was installed on both mobile devices ☑
- It was used for a period of 2 months ☑
- During that period multiple actions were performed ☑

Methodology - Collection

- Application’s data was collected using ADB and SSH commands ☑
- Application’s RAM was collected using Frida and fridump3 ☑
- Application’s data and RAM were collected more than 80 times ☑
- An FFS image was acquired from both mobile devices in pursuit of any residual artifacts outside the application’s space ☑

Methodology - Collection

Action Performed	No. of Android App's Data/RAM Evidence	No. of iOS App's Data/RAM Evidence
Install App	1 Data	1 Data
Login/Logout to Hik-Connect Account	2 Data + 2 RAM	2 Data + 2 RAM
Add CCTV-Scan QR Code	2 Data + 2 RAM	2 Data + 1 RAM
Add CCTV-Online Device	2 Data + 2 RAM	2 Data + 1 RAM
Add CCTV-Manual Adding-Hik-Connect Domain	3 Data + 3 RAM	3 Data + 2 RAM
Add CCTV-Manual Adding-IP/Domain	4 Data + 4 RAM	4 Data + 3 RAM
Access CCTV-Live View	3 Data + 1 RAM	3 Data + 1 RAM
Access CCTV-Playback	3 Data	3 Data
Access CCTV-Create Screenshot	2 Data	2 Data
Access CCTV-Save Video	2 Data	2 Data
Config. CCTV-Disable/Enable Recording	3 Data + 1 RAM	3 Data
Config. CCTV-Time Sync.	2 Data	2 Data
Uninstall App	1 Data	1 Data
Total	**30 Data + 15 RAM**	**30 Data + 10 RAM**

Methodology – Analysis objectives

- Identify all potentially valuable artifacts
- Verify actions performed by the user of the app
- Determine how the application handles these artifacts
- Contribute to FOSS

Contents

- Introduction
- Equipment and Methodology
- Results
- Discussion
- Future Work

Results

- Android app’s artifacts
- iOS app’s artifacts
- Verify user actions
- Contribute to FOSS

Results - Android app’s data artifacts

Artifact	Format	Information About
/databases/ezvizlog.db	SQLite	-CCTV system: (IP, S/N, etc.) -user’s actions: (e.g. Live View)
/databases/database.hik	SQLite	-CCTV system’s channels
/databases/image.db	SQLite	-user’s created media through the app.
/files/devmgr.user-ID{5}.sec.realm	realm -Encrypted	-CCTV system: (IP, S/N, sharing status, etc.)
/files/hc.realm	realm	-connected WiFi networks while using the app.
/shared_prefs/user-ID.xml	XML	-user’s login date -user’s actions: (Live View, Playback)
/shared_prefs/default.xml	XML	-user’s logon type -user’s actions: (Live View, Playback)
/shared_prefs/videoGo_device_info.xml	XML	-exists if “Remote Configuration” is enabled
/shared_prefs/system_config.xml	XML	-network traffic of the app
/media/0/Pictures/Hik-Connect Album	folder	-media files stored through the app

Results - Android app’s data artifacts

- /com.connect.enduser/databases/ezvizlog.db

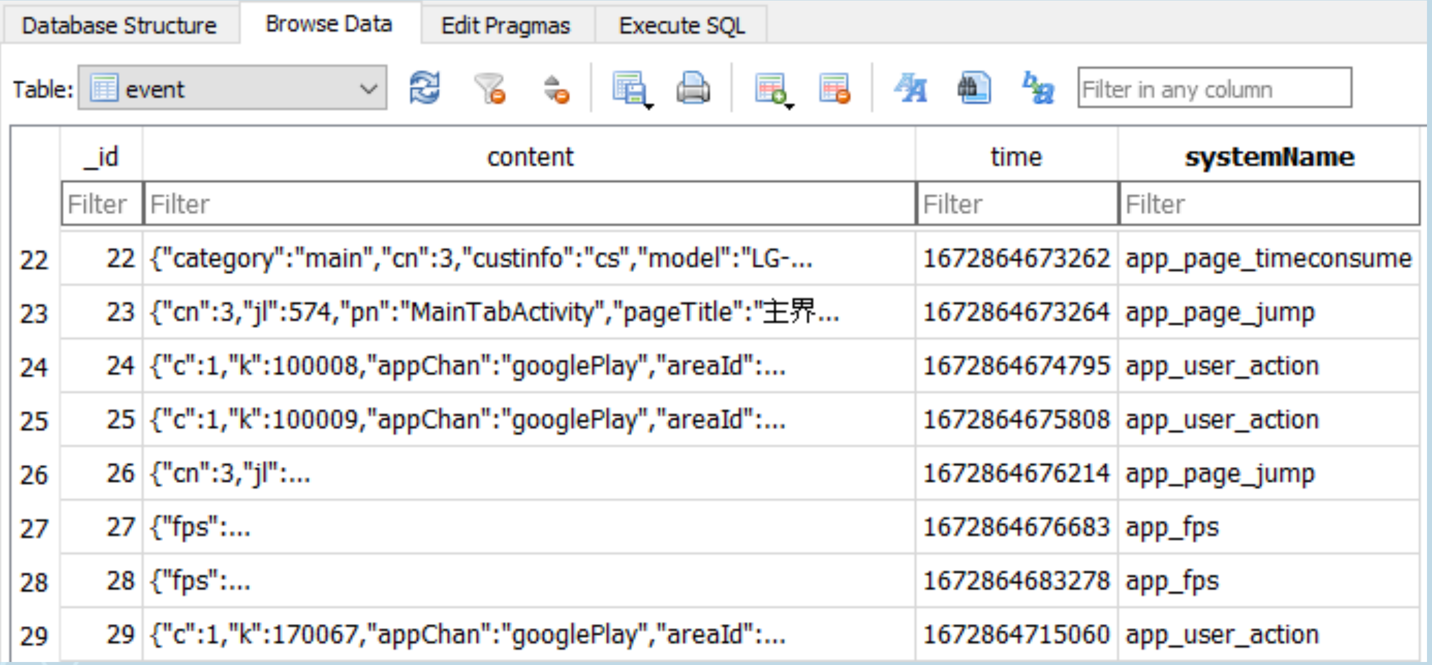


Table: event

	_id	content	time	systemName
	Filter	Filter	Filter	Filter
22	22	{"category":"main","cn":3,"custinfo":"cs","model":"LG-...	1672864673262	app_page_timeconsume
23	23	{"cn":3,"jl":574,"pn":"MainTabActivity","pageTitle":"主界...	1672864673264	app_page_jump
24	24	{"c":1,"k":100008,"appChan":"googlePlay","areaId":...	1672864674795	app_user_action
25	25	{"c":1,"k":100009,"appChan":"googlePlay","areaId":...	1672864675808	app_user_action
26	26	{"cn":3,"jl":...	1672864676214	app_page_jump
27	27	{"fps":...	1672864676683	app_fps
28	28	{"fps":...	1672864683278	app_fps
29	29	{"c":1,"k":170067,"appChan":"googlePlay","areaId":...	1672864715060	app_user_action

Information about:

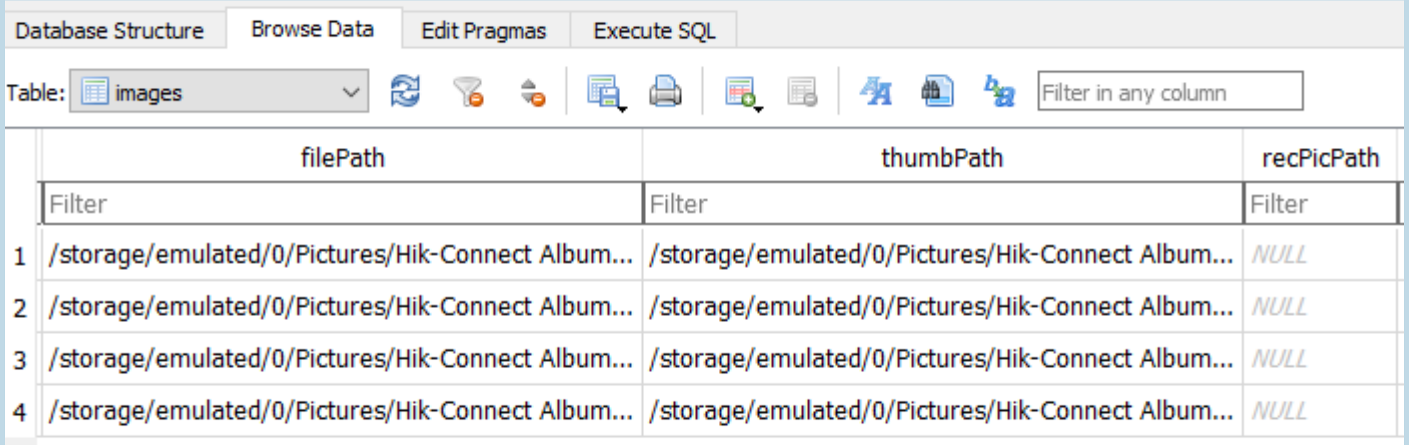
-CCTV system (IP, serial number)

-Certain user actions

(LiveView/Playback)

Results - Android app’s data artifacts

- /com.connect.enduser/databases/image.db



	filePath	thumbPath	recPicPath
	Filter	Filter	Filter
1	/storage/emulated/0/Pictures/Hik-Connect Album...	/storage/emulated/0/Pictures/Hik-Connect Album...	NULL
2	/storage/emulated/0/Pictures/Hik-Connect Album...	/storage/emulated/0/Pictures/Hik-Connect Album...	NULL
3	/storage/emulated/0/Pictures/Hik-Connect Album...	/storage/emulated/0/Pictures/Hik-Connect Album...	NULL
4	/storage/emulated/0/Pictures/Hik-Connect Album...	/storage/emulated/0/Pictures/Hik-Connect Album...	NULL

Information about:

-User created media files

- /media/0/Pictures/Hik-Connect Album/

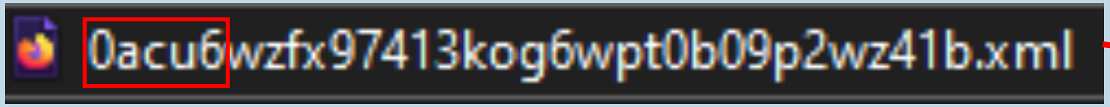
-Media files’ location

Results - Android app’s data artifacts

- When using the app with Hik-connect account/Visitor Mode:

1. /com.connect.enduser/shared_prefs/*

->An XML file gets created (filename consists of the “*user-ID*”, a 32-character long alphanumerical string



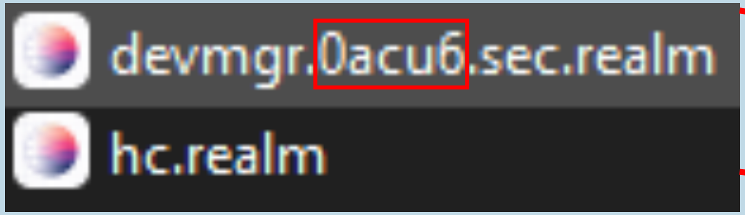
0acu6wzfx97413kog6wpt0b09p2wz41b.xml

Information about:

-When account logged in

-User’s actions: (Live View, Playback)

2. /com.connect.enduser/files/*



devmgr.0acu6.sec.realm

hc.realm

If decrypted and Hik-account used then holds Information about:

-If this CCTV is shared/bound with this account

- CCTV IP, SN

If Hik-account used then holds Information about:

-Wi-Fi networks connected to while the application was used

Results - Android app’s RAM artifacts

- /com.connect.enduser/files/devmgr.user-ID{5}.sec.realm

The Realm

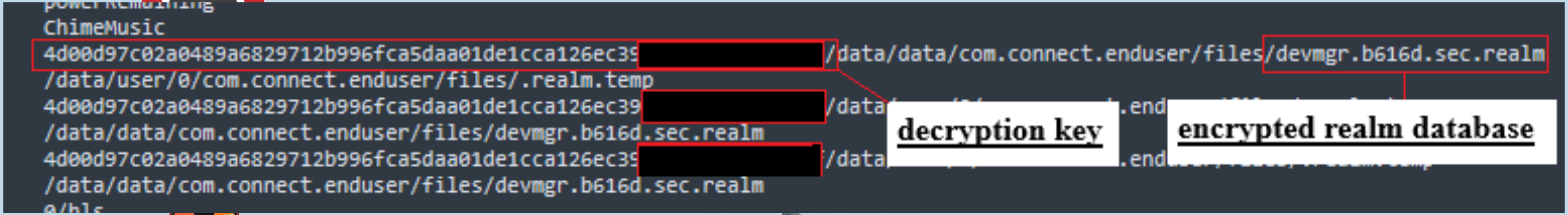
Either this is

128-charac

Results -Android app’s RAM artifacts

- /com.connect.enduser/files/devmgr.user-ID{5}.sec.realm

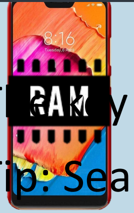
Hik-Connect - for End User



```
powerRemaining
ChimeMusic
4d00d97c02a0489a6829712b996fca5daa01de1cca126ec39[redacted]/data/data/com.connect.enduser/files/devmgr.b616d.sec.realm
/data/user/0/com.connect.enduser/files/.realm.temp
4d00d97c02a0489a6829712b996fca5daa01de1cca126ec39[redacted]/data                    .end
/data/data/com.connect.enduser/files/devmgr.b616d.sec.realm
4d00d97c02a0489a6829712b996fca5daa01de1cca126ec39[redacted]/data                    .end
/data/data/com.connect.enduser/files/devmgr.b616d.sec.realm
0/hls
```

decryption key

encrypted realm database

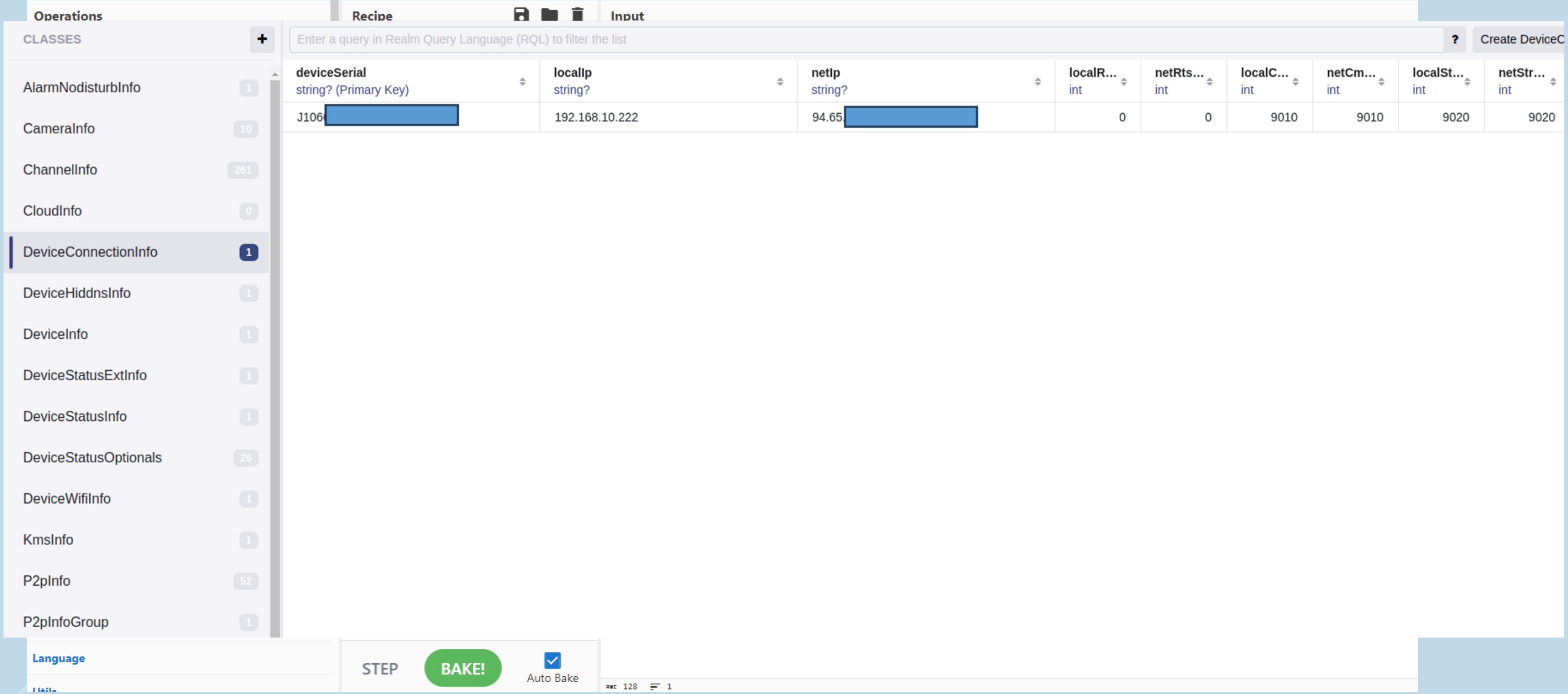


-The key needs to be converted to 128 hex

-Tip: Search for the term “.realm” to locate key

Results - Android app’s RAM artifacts

- /com.connect.enduser/files/devmgr.user-ID{5}.sec.realm



AlarmNodisturbInfo	1
CameraInfo	10
ChannelInfo	261
CloudInfo	0
DeviceConnectionInfo	1
DeviceHiddnsInfo	1
DeviceInfo	1
DeviceStatusExtInfo	1
DeviceStatusInfo	1
DeviceStatusOptionals	26
DeviceWifiInfo	1
KmsInfo	1
P2pInfo	52
P2pInfoGroup	1

deviceSerial string? (Primary Key)	localIp string?	netIp string?	localR... int	netRts... int	localC... int	netCm... int	localSt... int	netStr... int
J106[redacted]	192.168.10.222	94.65[redacted]	0	0	9010	9010	9020	9020

Results

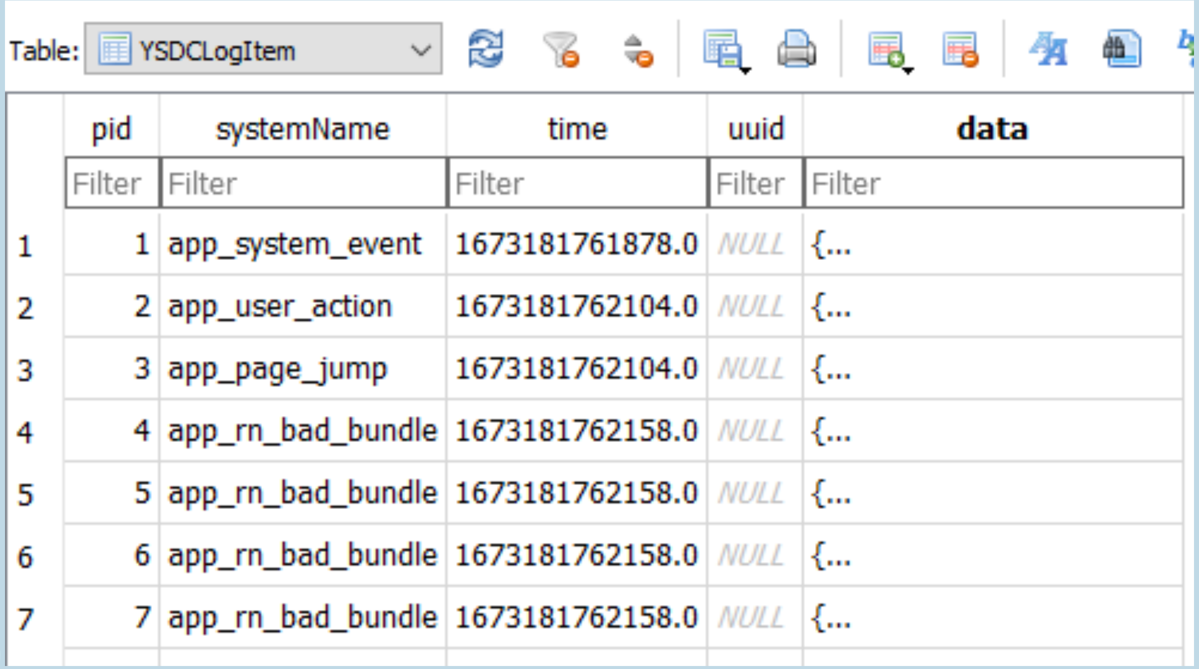
- Android app’s artifacts
- iOS app’s artifacts
- Verify user actions
- Contribute to FOSS

Results - iOS app’s artifacts

Artifact	Format	Information About
/Documents/DCLOG/YSDCLogItem.sqlite	SQLite	-CCTV system: (IP, S/N, etc.) -user’s actions: (e.g. Live View)
/Documents/database.hik	SQLite	-CCTV system’s channels
/Documents/TrafficStatistics.plist	PLIST	-network traffic of the app
/Documents/EZ_REALM/user-ID.realm	realm	-CCTV system: (IP, S/N, sharing status, etc.)
/Documents/requestBase	text	-CCTV system: (IP, S/N, etc.) -user’s account: (name, email, etc.)
/Documents/YYYY/MM/DD	folder	-user’s created media through the app.
/private/var/mobile/Media/DCIM/XXXAPPLE/	folder	-user’s created media through the app are assigned to “Hik-Connect Album”.

Results - iOS app's artifacts

- [Bundle-ID]/Documents/DCLOG/YSDCLogItem.sqlite



	pid	systemName	time	uuid	data
	Filter	Filter	Filter	Filter	Filter
1	1	app_system_event	1673181761878.0	NULL	{...
2	2	app_user_action	1673181762104.0	NULL	{...
3	3	app_page_jump	1673181762104.0	NULL	{...
4	4	app_rn_bad_bundle	1673181762158.0	NULL	{...
5	5	app_rn_bad_bundle	1673181762158.0	NULL	{...
6	6	app_rn_bad_bundle	1673181762158.0	NULL	{...
7	7	app_rn_bad_bundle	1673181762158.0	NULL	{...

Information about:

-CCTV system (IP, serial number)

-Certain user actions

(LiveView/Playback)

Equivalent of ezvizlog.db

Results - iOS app's artifacts

- [Bundle-ID]/Documents/YYYY/MM/DD/*

  -Media files' location

- /private/var/mobile/Media/DCIM/XXXAPPLE/*

  -Media files' location when also saved to *Photos* app

Results - iOS app’s artifacts

- [Bundle-ID]/Documents/EZ_REALM/user- ID.realm

-If this CCTV is shared/bound with this account

- CCTV IP, SN

Equivalent of devmgr.user-ID{5}.sec.realm

Results

- Android app’s artifacts
- iOS app’s artifacts
- Verify user actions
- Contribute to FOSS

Results - Verify user actions

- Very few artifacts are directly connected with user actions
- Live View, Playback, and Creation of Media Files could be verified from artifacts

☒ Disabling/Enabling camera recordings could not be verified

☒ Disabling/Enabling camera events (movement detection, etc.) could not be verified

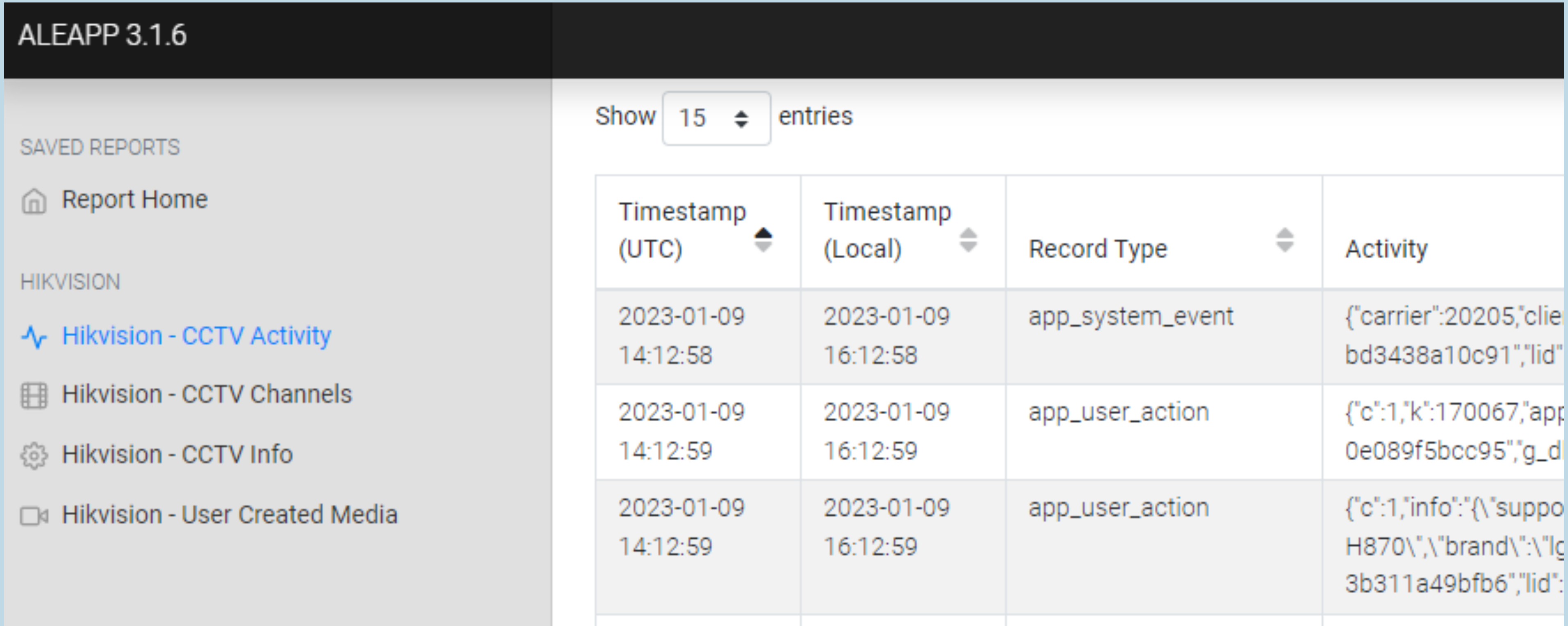
☒ Changing CCTV system’s password could not be verified

Results

- Android app’s artifacts
- iOS app’s artifacts
- Verify user actions
- Contribute to FOSS

Results - Contribute to FOSS

- Developed SQLite queries for recovering evidentiary data from “*ezvizlog.db*”, “*image.db*”, “*database.hik*”, and “*YSDCLogItem.sqlite*” databases
- These queries were integrated into ALEAPP and iLEAPP



ALEAPP 3.1.6

SAVED REPORTS

Report Home

HIKVISION

Hikvision - CCTV Activity

Hikvision - CCTV Channels

Hikvision - CCTV Info

Hikvision - User Created Media

Show 15 entries

Timestamp (UTC)	Timestamp (Local)	Record Type	Activity
2023-01-09 14:12:58	2023-01-09 16:12:58	app_system_event	{"carrier":20205,"clie bd3438a10c91","lid"
2023-01-09 14:12:59	2023-01-09 16:12:59	app_user_action	{"c":1,"k":170067,"app 0e089f5bcc95","g_d
2023-01-09 14:12:59	2023-01-09 16:12:59	app_user_action	{"c":1,"info":"{\"suppo H870\",\"brand\":\"lg 3b311a49bfb6","lid":

Contents

- Introduction
- Equipment and Methodology
- Results
- Discussion
- Future Work

Discussion – Good news

☑ User cannot format the CCTV using this mobile app

☑ Determine the account logged in the application

☑ Determine the IP of the CCTV system

☑ Verify certain user actions (Live View/Playback/Create Media Files)

☑ Methodology to potentially decrypt protected realm databases

☑ Some results are integrated into ALEAPP and iLEAPP

Discussion – Bad news

☒ Certain user actions cannot be verified by simply examining the mobile application

☒ Decrypting realm databases using the proposed method is hard in real investigations

☒ Rooting/Jailbreaking a mobile device jeopardizes evidence integrity

Discussion – Limitations

☒ This study does not take into consideration other evidence sources (like the CCTV system)

☒ Utilizing more feature-rich CCTV systems could potentially provide more capabilities to the end user

Discussion – Points of Consideration

☑ Not all artifacts are presented in this presentation (See Appendix B)

☑ Correlation of artifacts is needed to draw conclusions

☑ Use ALEAPP and iLEAPP along with this paper for better results

☑ Remember to seize CCTV system as complementary information may reside within

Contents

- Introduction
- Equipment and Methodology
- Results
- Discussion
- Future Work

Future Work

- Analysis of “HiLookVision” mobile application
- Analysis of HIKVISION’s desktop applications
- Correlation of artifacts retrieved from both applications’ data and CCTV system’s log records while tackling an “anti-forensics” scenario
- Test how many encrypted databases can be decrypted exploiting RAM

Q&A

Evangelos Dragonas
PhD Candidate, UNIPI, Greece

Contact info:

@theAtropos4n6

dragvag@ssl-unipi.gr

theatropos4n6

https://www.atropos4n6.com

Thank you!