DIGITAL FORENSIC RESEARCH CONFERENCE

Digital Forensic Practices and Methodologies for AI Speaker Ecosystems

By

Wooyeon Jo

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2019 USA

Portland, OR (July 15th - 19th)

Digital Forensic Practices and Methodologies for AI Speaker Ecosystems

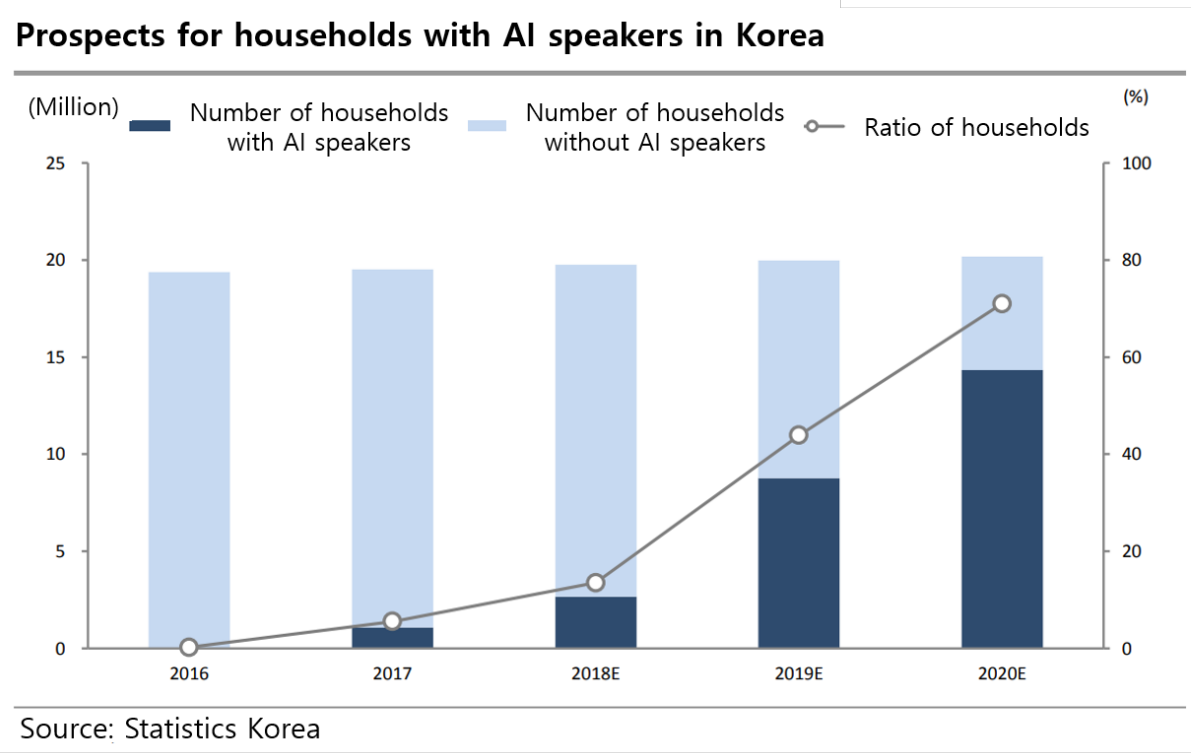
Ajou University

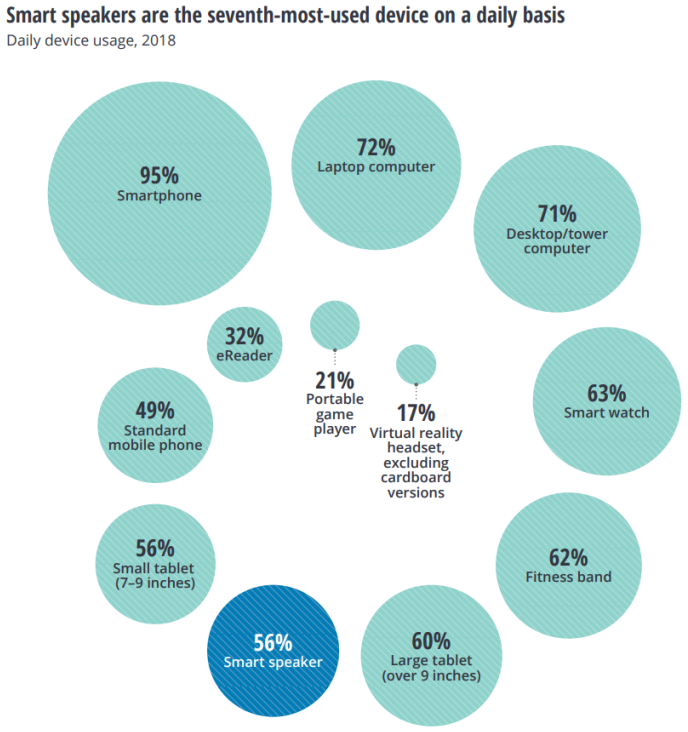
Wooyeon Jo

2019.07.16

Motivation

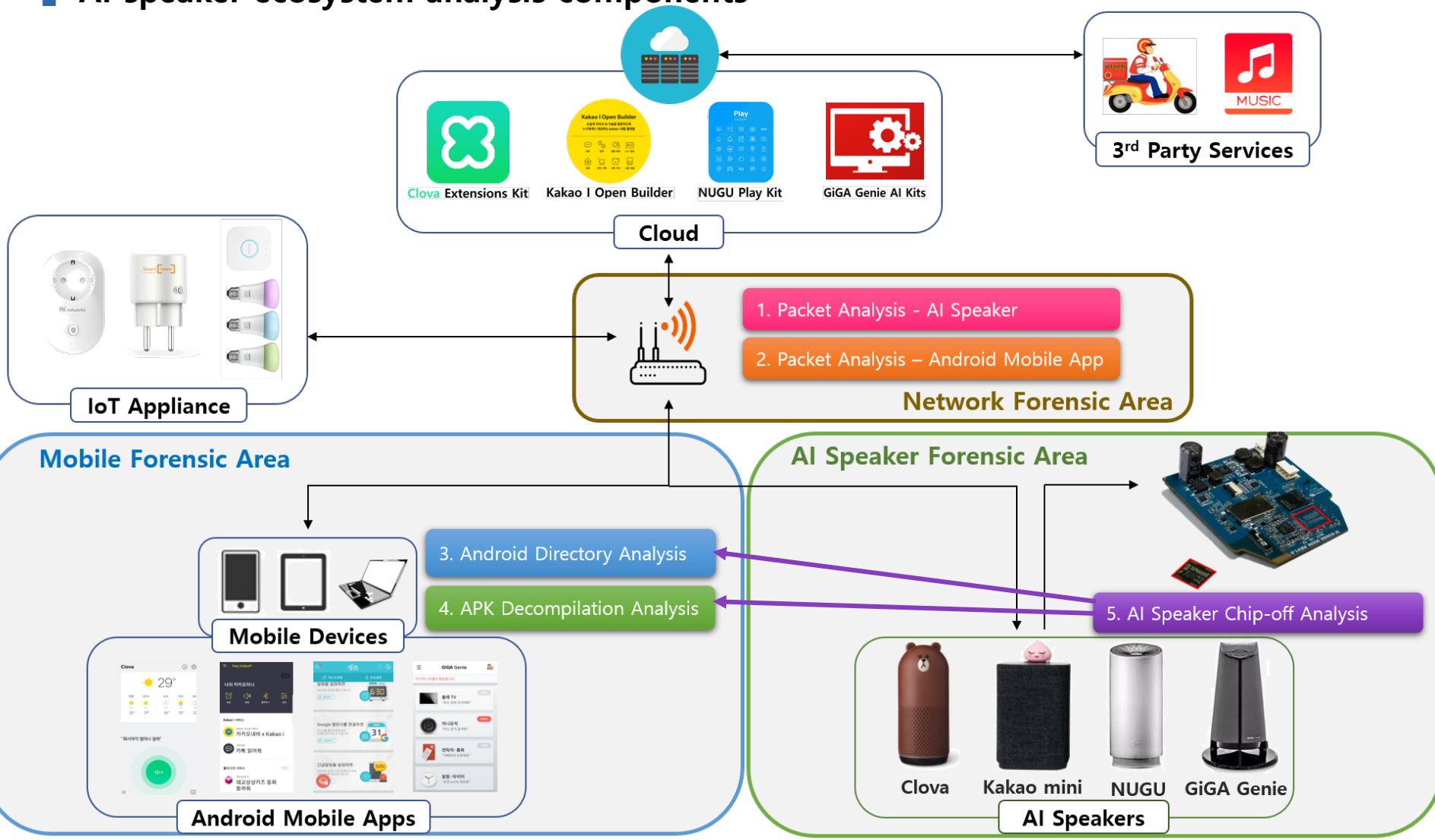
- [2018] U.S. AI speaker owners rose 39.8% to reach 66.4 million with total smart speakers in use rising to 133 million
- [2018] South Korea AI speaker owners rose over 900% to reach 1 million





Methodologies

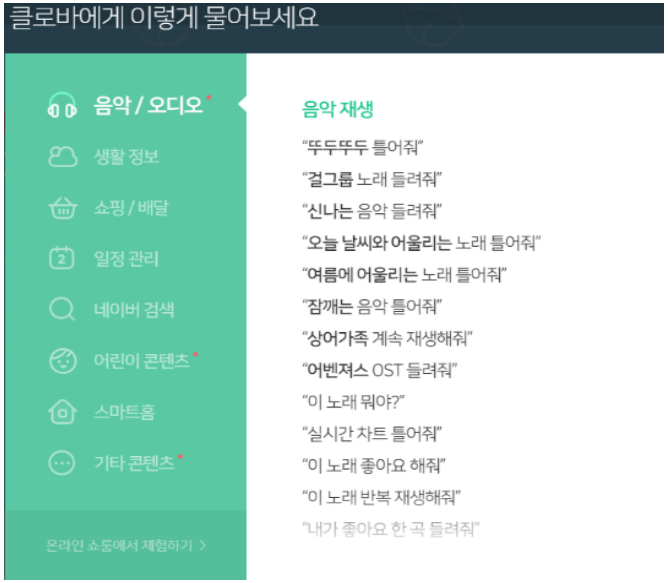
AI speaker ecosystem analysis components



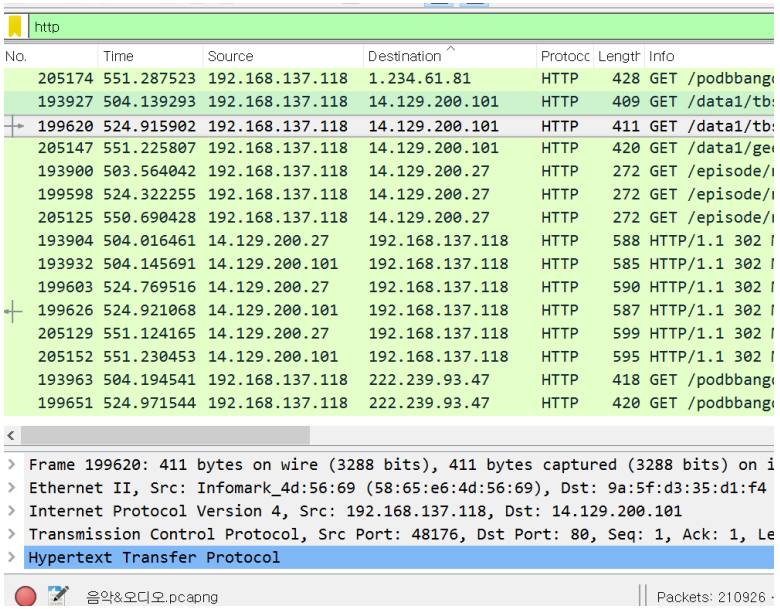
Methodologies
S01: Packet Analysis – AI Speaker

Data Collection and Analysis Methods

- **Proxy setting of speaker device impossible → Use Wireshark for packet sniffing**
  - HTTPS encrypted packets can not be analyzed, only HTTP traffic is analyzed
- **User Manual-based data collection**
  - Follow the instruction manual provided on the homepage to voice command and collect data with Wireshark tool
  - Capture the initial sequence between AI Speaker ↔ Android Mobile



Clova User Manual

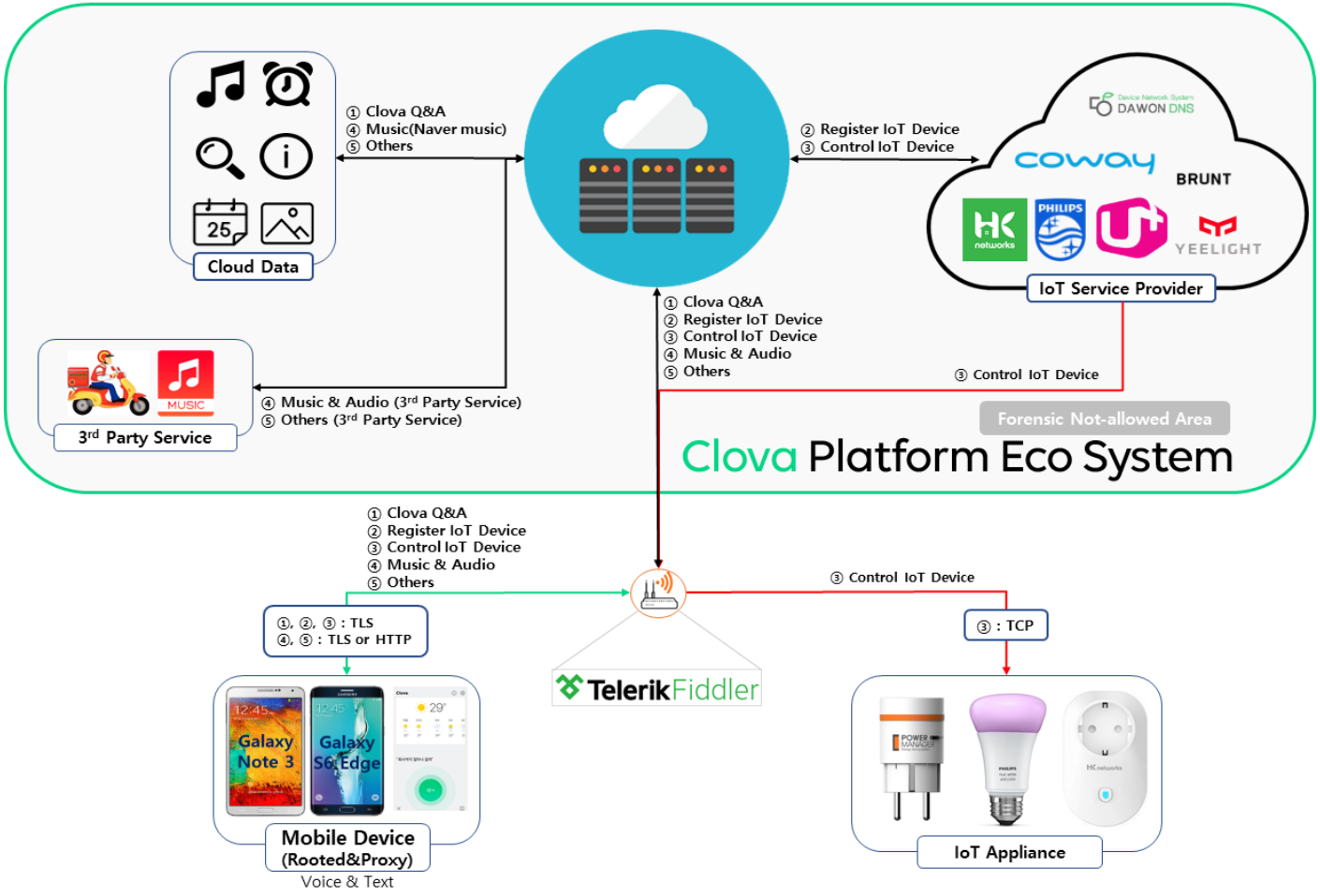


Wireshark HTTP Packet

Methodologies
S02: Packet Analysis – Android Application

Web Proxy Debugging – Fiddler

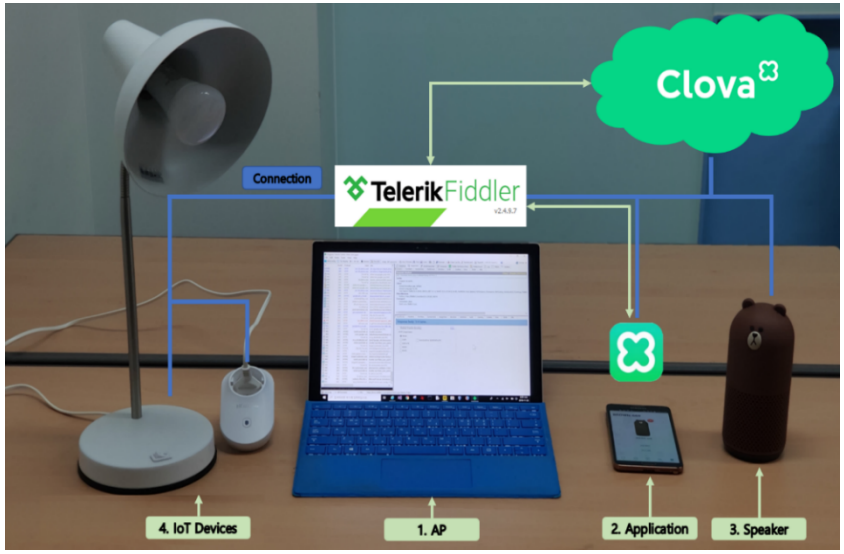
- Using MITM to see inside of HTTPS packet

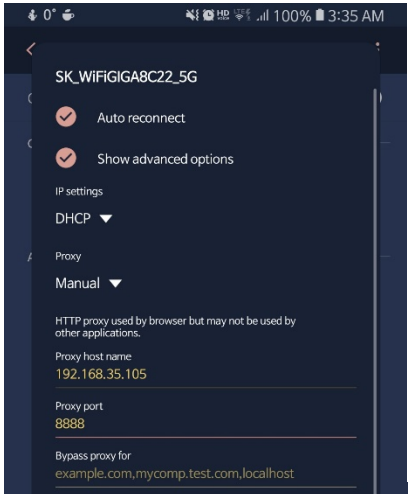


Methodologies
S02: Packet Analysis – Android Application

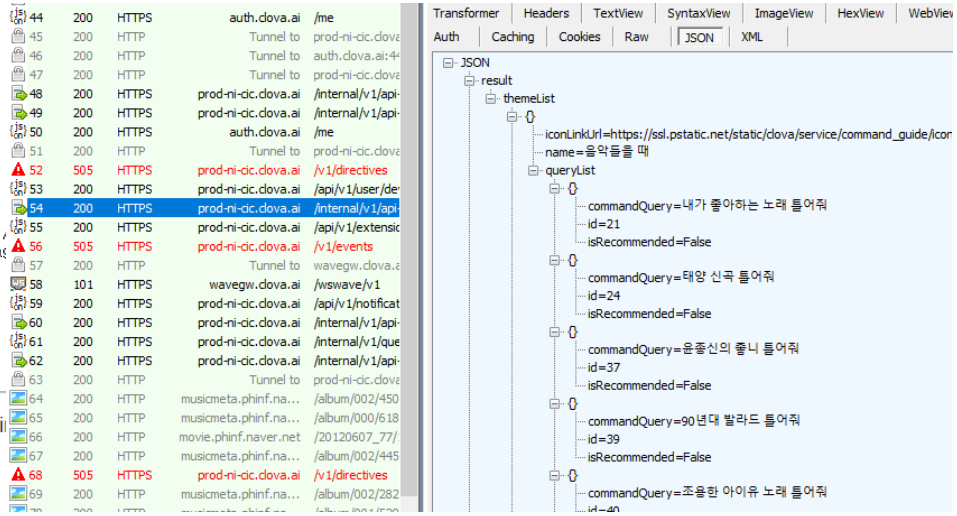
Data Collection and Analysis Methods

- **Web proxy tool Fiddler can analyze HTTPS (install Fiddler's Certificate on smartphone)**
- **User Manual-based data collection**
- **Analysis of domain-specific roles and cloud structure**
  - Comparison with AI speaker(Wireshark)
  - List up all exposed domains



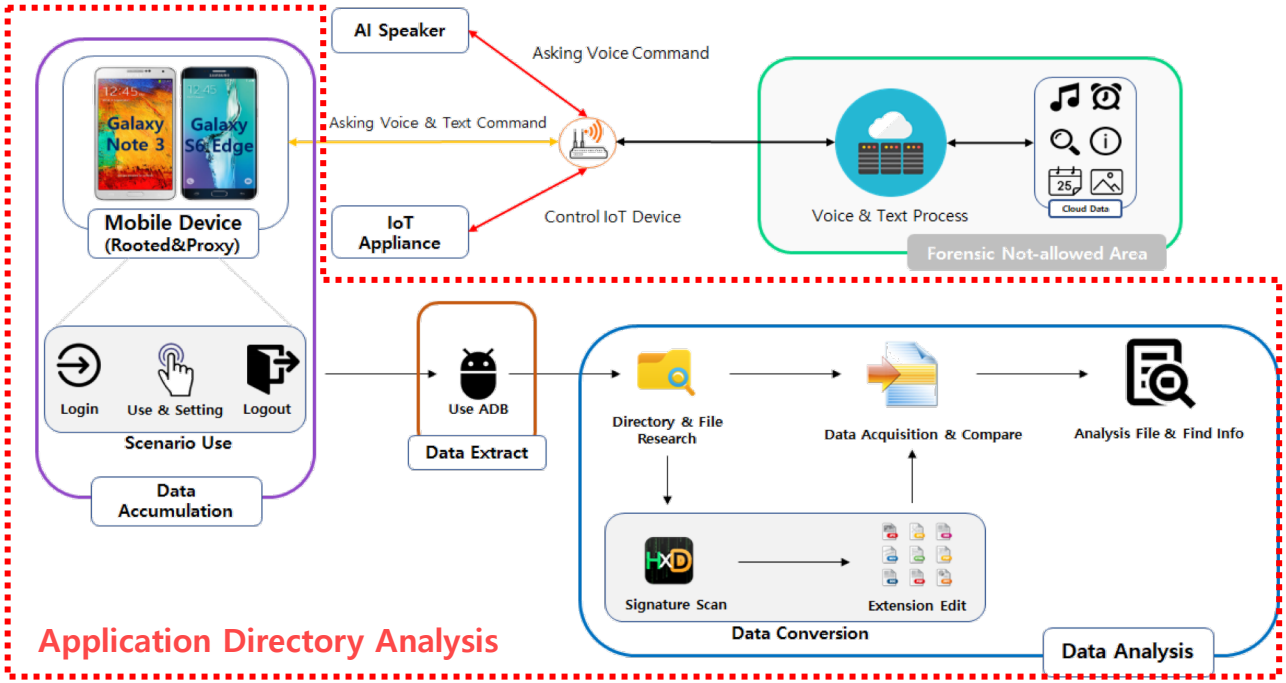


Proxy settings and certificate installation screen on smartphone



Fiddler View

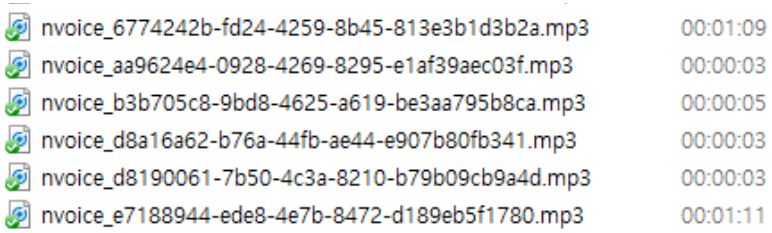
Methodologies
S03: Android Directory Analysis

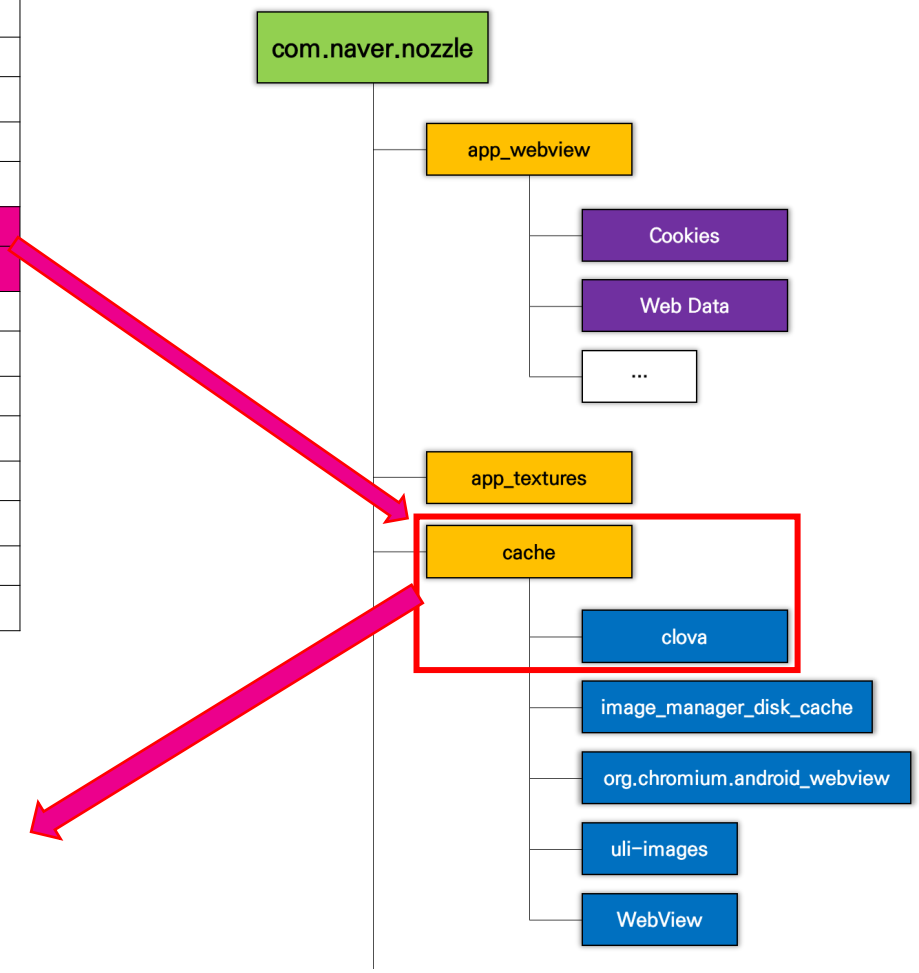


- **Scenario 3 analyzes the storage space of smartphone applications and extracts artifacts**
  - **AI application data accumulation**
    - It communicates with AI speakers, IoT devices, cloud servers, etc. and accumulates data in the internal directory
  - **Extract application data**
  - **Detailed analysis of collected data**

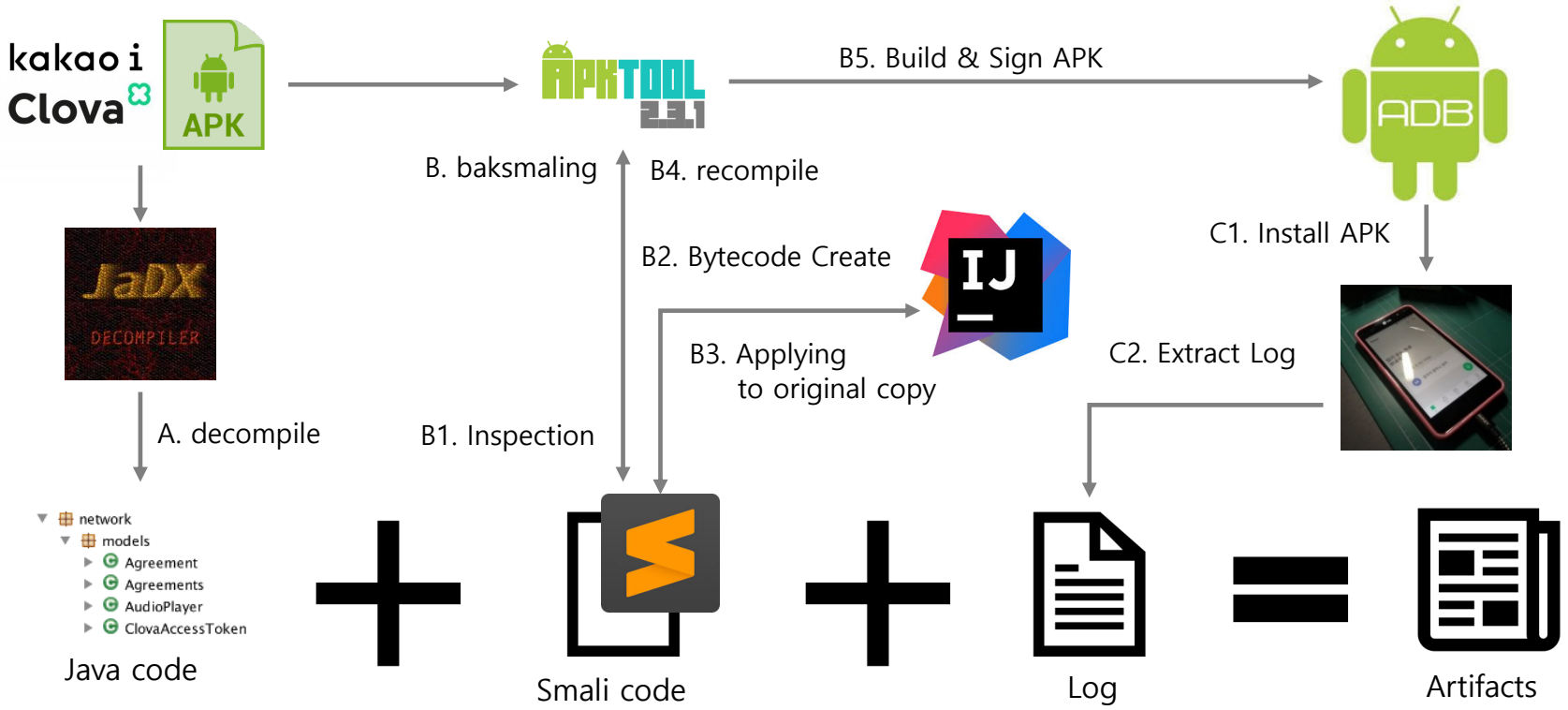
Methodologies
S03: Android Directory Analysis

Artifact Type	File Type	Path File Name
Cookie Data	SQLite DB	app_webview/ *
Webview Data	SQLite DB	app_webview/ *
Voice Response Cache Data	**MP3**	**cache/clova/** ***.mp3**
Cache Image Data	JPEG, PNG	cache/image_manager_disk_cache/ *.0
Cache Communication Data	GZIP	cache/org.chromium.android_webview/ *_0, *_1
User Setting Data	XML	shared_prefs/ clova.xml
Interlocking Account Data	XML	shared_prefs/ NaverOAuthLoginPreferenceData.xml





Methodologies
S04: APK Decompilation Analysis



Data Collection and Analysis Methods

- **A. Java code analysis after decompiling .apk file using JaDX**
- **B. Analyze Smali code after baksmaling .apk file using Apktool**
- **C. If Debug mode exists, modifies Flag value to True and re-installs output log analysis**
  - To avoid application tampering detection, only the apk where the Debug Flag exists (CLOVA case)

Methodologies
S04: APK Decompilation Analysis

Logcat to find artifacts

- **Step 1. Calling Clova speech recognizer (Trigger: saying wake-word or clicking voice button)**

```
08-09 01:39:51.351 23732 23732 D Clova.recognize.y: ClovaRequest=ai.clova.cic.clientlib.api.clovainterface.ClovaRequest@5d0339d
namespace=SpeechRecognizer name=Recognize dialogRequestId=3e983b9e-fa70-42d8-8fcf-050f8f738405 isDownchannel=false -called by a
08-09 01:39:51.352 23732 23732 D Clova.recognize.a: doOnSubscribe() dialogRequestId=3e983b9e-fa70-42d8-8fcf-050f8f738405 -calledby a
08-09 01:39:51.352 23732 23732 D Clova.recognize.g: doOnSubscribe dialogRequestId=3e983b9e-fa70-42d8-8fcf-050f8f738405 -called by a
08-09 01:39:51.353 23732 23910 D Clova.recognize.y:  -called by b
08-09 01:39:51.353 23732 23910 D Clova.DefaultSpeechRecognizerManager:  -called by b
08-09 01:39:51.361 23732 23732 D Clova.a :  -called by b
```

- **Step 2. Sending voice file to server via HTTP multipart body**

```
08-09 01:39:51.401 23732 23910 D r       : using resourceSupplier, cicRequest=Request{method=POST, url=https://prod-ni-cic.clova.ai/v1/events,
tags={}} clovaRequest=ai.clova.cic.clientlib.api.clovainterface.ClovaRequest@5d0339d namespace=SpeechRecognizer name=Recognize
dialogRequestId=3e983b9e-fa70-42d8-8fcf-050f8f738405 isDownchannel=false -called by a
08-09 01:39:51.401 23732 23910 D Clova.ClovaEventProtocolClient: doOnSubscribe dialogRequestId=3e983b9e-fa70-42d8-8fcf-050f8f738405 -called by a
08-09 01:39:51.403 23732 23814 D Clova.recognize.y:  -called by b
08-09 01:39:51.403 23732 23814 D CicRequestInterceptor:  -called by b
08-09 01:39:51.403 23732 23814 D CicRequestInterceptor:  -called by b
08-09 01:39:51.403 23732 23814 D CicRequestInterceptor:  -called by b
```

- **Step 3. Getting speech recognizer response from server via JSON**

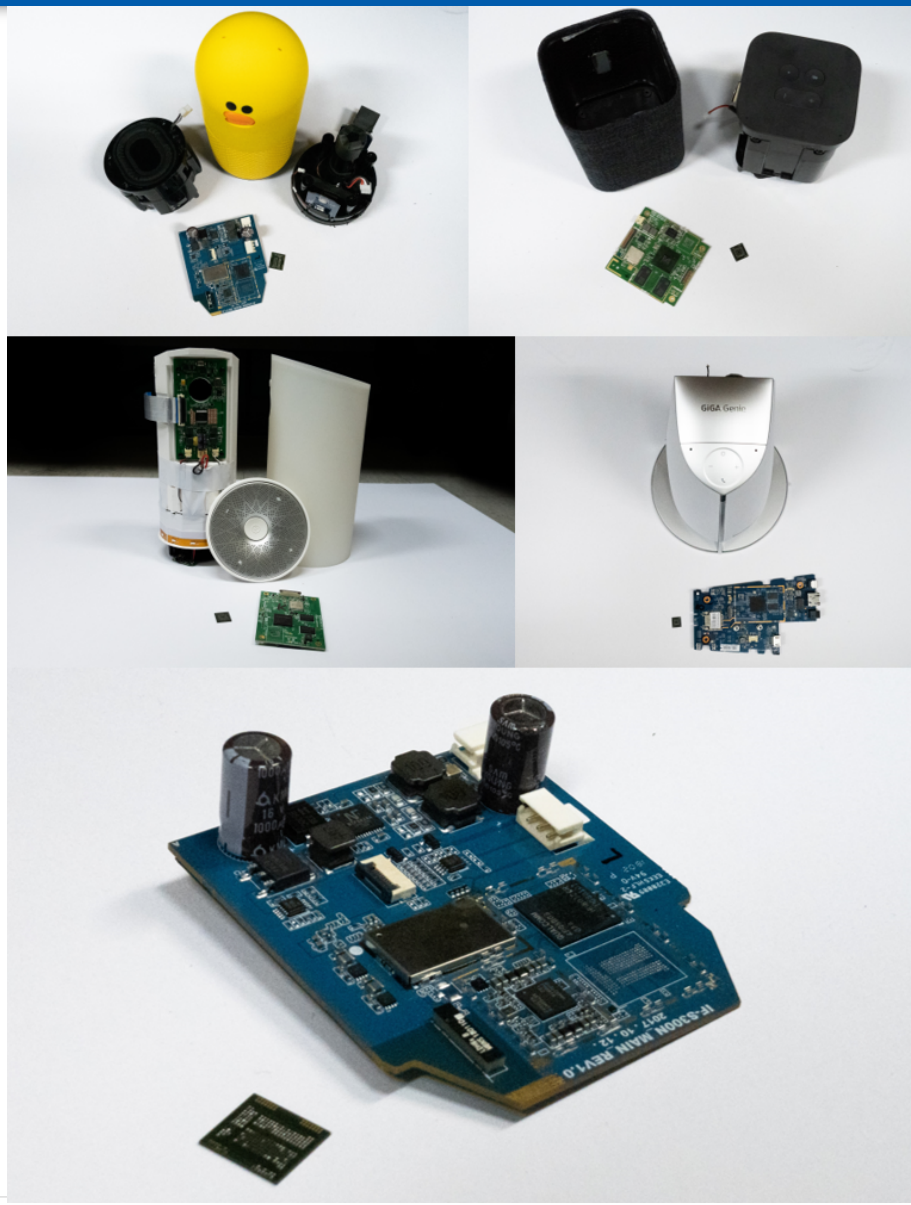
  (Repeat getting response from server until recognition procedure completes)

```
08-09 01:39:52.439 23732 23806 D Clova.data.ClovaServicePluginManager: responseBody={"directive":{"header":{"namespace":"SpeechRecognizer","name":"Show
RecognizedText","messageId":"c9216c84-ffa8-461c-8c01-4bfa4d59ae57","dialogRequestId":"3e983b9e-fa70-42d8-8fcf-050f8f738405"},"payload":{"text":"네"}}}
08-09 01:39:52.814 23732 23806 D Clova.data.ClovaServicePluginManager: responseBody={"directive":{"header":{"namespace":"SpeechRecognizer","name":"Show
RecognizedText","messageId":"67dd589e-028c-4f0f-9014-8fcfeb1839f6","dialogRequestId":"3e983b9e-fa70-42d8-8fcf-050f8f738405"},"payload":{"text":"내일"}}}
08-09 01:39:53.538 23732 23806 D Clova.data.ClovaServicePluginManager: responseBody={"directive":{"header":{"namespace":"SpeechRecognizer","name":"Show
RecognizedText","messageId":"1a7d2461-0199-4d80-bdbf-e9e0bfd20b2d","dialogRequestId":"3e983b9e-fa70-42d8-8fcf-050f8f738405"},"payload":{"text":"내일
날씨 어때"}}}
08-09 01:39:53.538 23732 23806 D Clova.data.ClovaServicePluginManager:  -called by e
08-09 01:39:53.540 23732 23806 D Clova.data.ClovaServicePluginManager: dialogRequestId=3e983b9e-fa70-42d8-8fcf-050f8f738405 Directive:
SpeechRecognizer.ShowRecognizedText -called by a
```

Methodologies
S05: Chip-off Image Analysis

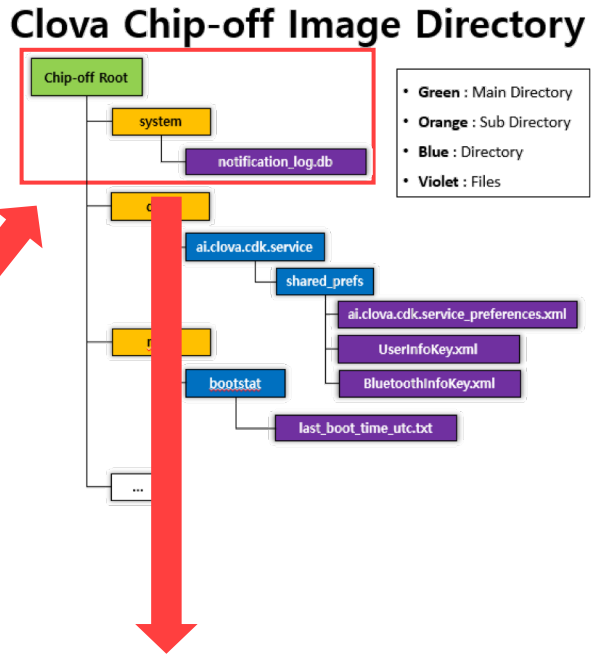
Data Collection and Analysis Methods

- **Filesystem identification**
  - Using signatures of the filesystems
- **Analyze operating system and directory structure**
  - Mount image and analyze as Scenario 3
- **Explore using file signatures and keywords**
  - Personal information or Key files(i.e. .mp3, .db)
- **Delete data recovery and comparison**
  - EXT4 recovery techniques using Journal area



Methodologies
S05: Chip-off Image Analysis

	Artifact Type	File Type	Path	File Name	Description
A	User Name	xml	root₩data₩ai.clova.cdk.service₩shared_prefs	BluetoothInfoKey.xml	
B	Personal Information	xml		UserInfoKey.xml	Address, Location (Latitude, Longitude)
C	Identification Information	xml		UserInfoKey.xml	User Key ID Wi-Fi mac address
D		xml		BluetoothInfoKey.xml	Connected Smartphone (mac, model name)
E	Time Information	**db**	**root₩system**	**notification_log.db**	**Event Log**
F		txt	root₩misc₩bootstat	last_boot_time_utc.txt	Last boot time
H	History	mp3	-	nvoice_<hash>.mp3	Deleted



테이블(T): log

새 레코드

	_id	event_user_id	event_type	event_time_ms	key	pkg	nid	tag	when_ms
	필터	필터	필터	필터	필터	필터	필터	필터	필터
1	231	0	1	1530749597926	0|ai.clova.ap…	ai.clova.app.friendsalert	1	NULL	1530749597926
2	232	0	1	1530749601511	0|ai.clova.ap…	ai.clova.app.friendsalert	1	NULL	1530749601511
3	233	0	1	1530761391146	0|ai.clova.ap…	ai.clova.app.friendssettings	1	NULL	1530761391146
4	234	0	1	1530761391159	0|ai.clova.ap…	ai.clova.app.friendsknocker	1	NULL	1530761391159
5	235	0	1	1530761391651	0|ai.clova.ap…	ai.clova.app.friendssound	10015	NULL	1530761391651

Test Environments

AI Speaker Android Application Installed Base

- SAMSUNG Galaxy Note 2, Note 3, S7

Chip-off Image Analysis Devices

Vendor	Naver	Kakao	SKT	KT
Model	Friends (NL-S1000KRL)	Kakao Mini (KM-1000)	NUGU (NU100)	GiGA Genie (CT1100)
AI	Clova	Kakao I	Aria	Giga genie

Results

Appendix A. Summary of Key Artifacts

Category	*Vendor*	*AI Cloud (Packet Analysis)*	*Android mobile (Android Chip-off Analysis)*	*AI speaker (AI Speaker Chip-off Analysis)*
User Information: Information that can be used or helpful in identifying a user (e.g. user's name, Interlocking Account Data, MAC, address, ID, email, Key value, Wifi MAC, etc.)	NAVER	auth.clova.ai(/user_profile/personal_info/*) prod-ni-cic.clova.ai(/result/{DEVICE_#}/*)	shared_prefs/ (NaverOAuthLoginPreferenceData.xml clova.xml)	root\data\ai.clova.cdk.service\shared_prefs (BluetoothInfoKey.xml, UserInfoKey.xml)
	KAKAO	auth.kakao.com(/account/profile/*) app.i.kakao.com(/contents/{DEVICE_#})	shared_prefs/(CrashReporter.Crashlytics.xml)	P6\misc\bluedroid\(bt_config.xml) P6\data\com.kakao.i.speaker\shared_prefs\(kakaoi.pref.xml)
	SKT	api.sktnugu.com (/*, /simpleSetting/*, accountSetting/*)	shared_prefs/(optiondata.xml)	userdata\data\com.skt.aicloud.speaker.service\shared_prefs\(AICloud.xml)
	KT	gbas.megatvdnp.co.kr (/user*, /devList/*) gsvr.ktipmedia.co.kr (/devUserList/{USER_#}/*)	shared_prefs/(*.xml)	data\com.kt.gigagenie.launcher\databases\(launcherCommon.db)
Time: Hard to deduce a specific command, but relevant information to build an event timeline. (e.g., use time, boot time, end time, package usage history, and alarm setting history)	NAVER	prod-ni-cic.clova.ai (/meta/*)	app_webview/(*)	root\system\notification_log.db root\misc\bootstat\last_boot_time_utc.txt
	KAKAO	app.i.kakao.com (/result/result/*) app.i.kakao.com /alarms/{alarm #}	databases/(com.kakao.kinsight.sdk.android.~.sqlite)	data\com.android.providers.media\databases\(external.db)
	SKT	pif.t-aicloud.com (/clientStatus/*)	databases/(aladdin.db)	system\usagestats\(usage-history)
	KT	gdialog.ktipmedia.com	files/(dxshield.sys)	data\com.kt.gigagenie.tts\shared_prefs\(com.kt.gigagenie.tts.xml) system\(appops.xml)
History: Information about the command history that can be used to infer the user's command (e.g., cookie data, webview data, cache image, event recording)	NAVER	prod-ni-cic.clova.ai (/result/historyQuery/*)	cache/clova/(*.mp3) cache/org.chromium.android_webview/(*_0, *_1) cache/image_manager_disk_cache/(*.0)	[deleted] nvoice_{hash}.mp3
	KAKAO	kinsight-event.kakao.com (/sessions/events/*, /sessions/headers/*)	-	**data\com.android.providers.media\databases\(external.db)** **media\0\KakaoICache\audio\(cached.{hash}.mp3)**
	SKT	-	databases/(aladdin.db) cache/image_manager_disk_cache/(*.0) app_webview/(*)	data\com.skt.aicloud.speaker.service\databases\ (AladdinGeneral.db) system\recent_tasks\(#_task.xml) system\recent_images(#_task_thumbnail.png)
	KT	gdialog.ktipmedia.com	**cache/picasso-cache/(*.0, *.1)**	

Naver Clova's History

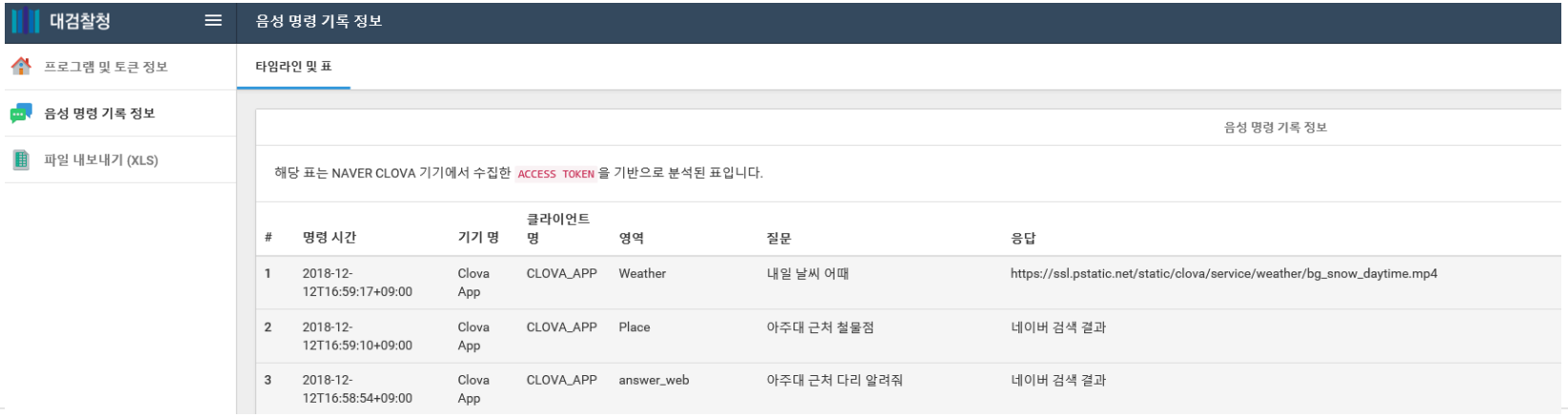
Differences from Clova application screen

- **Timestamp**
  - The application UI displays only the date, can not confirm the exact time.
- **Identification Information**
  - Identification information such as id, requestID, messageID, etc.,
- **Number of history (100 records at a time)**
  - The application UI displays only one or two records at a time, hard to see 100 records

Table 2. NAVER Clova's history artifact.

Field	Value
clientName	FRIENDS
deviceName	SALLY
dialogRequestId	09296c90-bd8e-4edf-af5a-3c35a40427c5
messageId	c2e8523c-b719-4f3e-ab5a-68736876ea9a
actionList::type	Action
actionList::value	clova://device-control?command=Increase&target=volume
paragraphText::type	String
paragraphText::value	Volume increased
domain	Control
query	Increase the volume three levels
id	586248fa-33d7-49f6-9203-c79935b7ea70
requestId	0c23cd9d-3368-48ee-bb63-5f4a91db343c
time	2018-06-21T13:58:59+09:00

meta : {'success': True, 'error': None, 'nextCursor': 1541075935000, 'current': 1542287739000}
result : {'id': 'f1476c8c-ec8d-4ca0-b867-c2b7b8d71d86', 'requestId': '792760f6-a640-4978-961b-d08a753d3120', 'time': '2018-11-05T16:57:11+09:00', 'type': 'Query', 'clientName': 'FRIENDS', 'deviceName': 'BROWN', 'historyQuery': {'query': '영어회화 틀어줘', 'domain': 'freetalking',
result : {'id': '6cea6d39-1405-4146-820c-72404e157d91', 'requestId': '1d25917e-17f5-435f-bda6-b54db7e1c376', 'time': '2018-11-05T16:56:49+09:00', 'type': 'Query', 'clientName': 'FRIENDS', 'deviceName': 'BROWN', 'historyQuery': {'query': '영어 듣기 틀어줘', 'domain': 'music', 'direct
result : {'id': '8dd9a80c-c61a-4850-becd-4cfd8a614459', 'requestId': '72f4d883-31a9-4a53-a085-26743615eed8', 'time': '2018-11-05T16:36:58+09:00', 'type': 'Query', 'clientName': 'FRIENDS', 'deviceName': 'BROWN', 'historyQuery': {'query': '아나두 영어', 'domain': 'answer_lang', 'dire
result : {'id': '216fb130-8b06-49c7-b91a-349cf14c841c', 'requestId': 'ff45abd0-2cc5-4f70-bc7a-4d59bea6bf99', 'time': '2018-11-05T16:36:48+09:00', 'type': 'Query', 'clientName': 'FRIENDS', 'deviceName': 'BROWN', 'historyQuery': {'query': '아나두 기초영어 회화', 'domain': 'none', 'di



Conclusion and Future Work

- **Personal information and ID artifacts**
  - **Law enforcement can request cooperation from service providers based on ID information**
  - **On most devices, the answers remain until reboot**
- **Classification of the server roles in the cloud**
  - **According to the type of information to be requested.**
  - **Confirmation of non-discrimination policy**
    - User's voice is not saved in device
- **Provide guidelines for the investigators when AI speakers are found in the field**
  - **The investigator can get personal information of user by chip-off image analysis**
  - **Compare Smartphone Mac address and Wi-Fi MAC address of user and suspect**
- **Present analysis directions for brand-new IoT devices through various approaches**
  - **Various approaches will be the base source to future works**
    - Rooting and Live Forensics on AI speaker / AI speaker application decompilation / AI speaker ROM to Raspberry Pi

Thank You

Contact Info.

dndusdndus12@gmail.com

Wooyeon Jo