

# **SIM-APDU-Analyzer**

## **사용 매뉴얼 v3.1**

**2024.01.16**

## 문서 이력

[illegible]

## 문서 구성

- (1) APDU Tab
- (2) File System Tab
- (3) QCAT 로그 분석 방법
- (4) QXDM 로그 분석 방법
- (5) Shannon DM 로그 분석 방법

## (1) APDU Tab : 화면 구성

**File Open button**  
Text로 저장된 단말 로그 열기

**Clipboard button**  
QXDM 로그 복사 후 클립보드 붙여넣기

**로그 불러오기 결과**  
파일 또는 클립보드 붙여넣기 결과

**Combo box**  
SIM 포트1,2 선택

**Execute button**  
APDU Parsing 실행 버튼

**실행 결과**  
APDU Parsing 결과

APDU Tab

File System Tab

단말-SIM 간의 APDU 메시지 분석 기능

**Summary**  
선택된 SIM 포트의 APDU Parsing 시간 순으로 요약 정리  
※ 각 APDU 메시지 선택 가능

**Protocol-Level Analysis**  
선택된 APDU 메시지 상세 Protocol 메시지 확인

**Application-Level Analysis**  
선택된 APDU 메시지 상세 APDU Parsing 결과 확인

# (1) APDU Tab : 화면 예시

Open file

Clipboard

APDU logs included in <C:/Users/User/Python Tools/SIM APDU Analyzer/file\_sample/Clipboard\_eSIM\_Install\_C9100\_BIP\_Pass.txt>

SIM2

Execute

Complete

APDU

File System

Summary

[333]	05:20:58.679	SEARCH RECORD (SFI: 0x02)		PBC
[334]	05:20:58.689	READ RECORD		
[335]	05:20:59.398	SELECT		ADF ISIM
[336]	05:20:59.408	AUTHENTICATE		ADF ISIM
[337]	05:21:00.285	ENVELOPE (SMS-PP Download)		
[338]	05:21:00.499	ENVELOPE (SMS-PP Download)		
[339]	05:21:00.607	FETCH (OPEN CHANNEL)		
[340]	05:21:00.667	TERMINAL RESPONSE (OPEN CHANNEL)		
[341]	05:21:00.676	FETCH (SEND DATA)		
[342]	05:21:00.683	TERMINAL RESPONSE (SEND DATA)		
[343]	05:21:00.726	ENVELOPE (Event Download)		Data available
[344]	05:21:00.733	FETCH (RECEIVE DATA)		
[345]	05:21:00.737	TERMINAL RESPONSE (RECEIVE DATA)		
[346]	05:21:00.831	FETCH (SEND DATA)		
[347]	05:21:00.840	TERMINAL RESPONSE (SEND DATA)		
[348]	05:21:00.982	ENVELOPE (Event Download)		Data available
[349]	05:21:00.988	FETCH (RECEIVE DATA)		
[350]	05:21:00.993	TERMINAL RESPONSE (RECEIVE DATA)		
[351]	05:21:01.050	FETCH (SEND DATA)		
[352]	05:21:01.063	TERMINAL RESPONSE (SEND DATA)		
[353]	05:21:01.175	ENVELOPE (Event Download)		Data available
[354]	05:21:01.181	FETCH (RECEIVE DATA)		
[355]	05:21:01.185	TERMINAL RESPONSE (RECEIVE DATA)		
[356]	05:21:01.201	FETCH (RECEIVE DATA)		
[357]	05:21:01.206	TERMINAL RESPONSE (RECEIVE DATA)		
[358]	05:21:01.251	ENVELOPE (Event Download)		Data available
[359]	05:21:01.258	FETCH (RECEIVE DATA)		
[360]	05:21:01.262	TERMINAL RESPONSE (RECEIVE DATA)		
[361]	05:21:01.278	FETCH (RECEIVE DATA)		
[362]	05:21:01.282	TERMINAL RESPONSE (RECEIVE DATA)		
[363]	05:21:01.298	FETCH (RECEIVE DATA)		
[364]	05:21:01.302	TERMINAL RESPONSE (RECEIVE DATA)		
[365]	05:21:01.347	FETCH (RECEIVE DATA)		
[366]	05:21:01.351	TERMINAL RESPONSE (RECEIVE DATA)		
[367]	05:21:01.366	FETCH (RECEIVE DATA)		
[368]	05:21:01.371	TERMINAL RESPONSE (RECEIVE DATA)		
[369]	05:21:01.567	FETCH (SEND DATA)		
[370]	05:21:01.581	TERMINAL RESPONSE (SEND DATA)		
[371]	05:21:01.586	FETCH (SEND DATA)		
[372]	05:21:01.593	TERMINAL RESPONSE (SEND DATA)		
[373]	05:21:01.608	FETCH (SEND DATA)		
[374]	05:21:01.617	TERMINAL RESPONSE (SEND DATA)		
[375]	05:21:01.835	ENVELOPE (Event Download)		Data available
[376]	05:21:01.842	FETCH (RECEIVE DATA)		
[377]	05:21:01.846	TERMINAL RESPONSE (RECEIVE DATA)		
[378]	05:21:01.875	FETCH (SEND DATA)		
[379]	05:21:01.881	TERMINAL RESPONSE (SEND DATA)		

Protocol-Level Analysis

```
=====
[425] 05:21:13.848 [TX] 00 B0 87 00 09
      05:21:13.854 [RX] B0 08 49 05 60 01 38 33 40 73 90 00
=====
```

Application-Level Analysis

```
=====
[425] Logical Channel : 0
      Current DF File : A0000000871002FF82FFFF89010000FF [ADF USIM]
      Current EF File : 6F07 [IMSI]
      Current Command : READ BINARY (SFI: 0x07)
      -----
      Read Offset      : 0x00
      Read Length      : 0x09 (9 Bytes)
      Read Contents    : 08 49 05 60 01 38 33 40 73
      -----
      450061083330437
      -----
```

Copyright 2022, JUSEOK AHN<ajs3013@lguplus.co.kr> all rights reserved.

# (1) APDU Tab : 화면 설명

단말 로그에 포함된 APDU 로그 Parsing 결과 요약 출력

APDU		File System	
[순서]	CP Time	APDU Command (상세 Type)	EF File Name
[1189]	05:22:13.790	READ RECORD (SFI: 0x06) (X)	ARR
[1190]	05:22:13.795	SELECT	ARR
[1191]	05:22:13.803	READ RECORD (X)	
[1192]	05:22:13.806	READ RECORD (X)	
[1193]	05:22:13.809	SELECT	ARR
[1194]	05:22:13.817	READ RECORD	
[1195]	05:22:13.823	SELECT	SMSP
[1196]	05:22:13.831	READ RECORD (SFI: 0x17)	ARR
[1197]	05:22:13.840	SELECT	IMPI
[1198]	05:22:13.848	READ BINARY	
[1199]	05:22:13.854	SELECT (X)	XCAPConfigData
[1200]	05:22:13.856	SELECT	IMPI
[1201]	05:22:13.865	SELECT	PSISMSC
[1202]	05:22:13.873	SELECT	ARR
[1203]	05:22:13.882	READ RECORD	
[1204]	05:22:13.887	SELECT	MBDN
[1205]	05:22:13.896	READ RECORD (SFI: 0x17)	ARR
[1206]	05:22:13.904	SELECT (X)	7FFF7F665F304F34
[1207]	05:22:13.907	SELECT	ARR
[1208]	05:22:13.916	SELECT (X)	7FFF7F665F304F36
[1209]	05:22:13.918	SELECT	ARR
[1210]	05:22:13.927	READ RECORD (SFI: 0x19)	PNN
[1211]	05:22:13.936	READ RECORD (SFI: 0x17)	ARR
[1212]	05:22:13.944	SELECT	SMSP
[1213]	05:22:13.952	SEARCH RECORD (X)	
[1214]	05:22:13.959	SELECT (X)	7FFF6F15
[1215]	05:22:13.961	SELECT	SMSP
[1216]	05:22:13.970	SELECT	CFIS
[1217]	05:22:13.979	SELECT (X)	7FFF6F14
[1218]	05:22:13.981	SELECT	CFIS
[1219]	05:22:13.991	READ RECORD (SFI: 0x04)	IMPU
[1220]	05:22:14.001	SELECT	P-CSCF
[1221]	05:22:14.008	READ RECORD	
[1222]	05:22:14.015	SELECT	SMSP
[1223]	05:22:14.022	READ RECORD	
[1224]	05:22:14.028	SELECT	PSISMSC
[1225]	05:22:14.036	READ RECORD	
[1226]	05:22:14.042	SELECT	MBDN
[1227]	05:22:14.050	READ RECORD	
[1228]	05:22:14.055	SELECT	MSISDN
[1229]	05:22:14.063	READ RECORD	
[1230]	05:22:14.068	SELECT (X)	7FFF6F15
[1231]	05:22:14.071	SELECT	MSISDN
[1232]	05:22:14.080	SELECT	CFIS
[1233]	05:22:14.088	READ RECORD	
[1234]	05:22:14.092	SELECT	ADF USIM
[1235]	05:22:14.103	AUTHENTICATE	ADF USIM

SFI(Short File Identity) 사용 시 SELECT 없이 READ

(X) File not found (회색 표기)

3GPP 스펙에서 확인된 File Name 으로 표기

3GPP 스펙에서 확인되지 않는 File Id 는 직접 표기

USIM 인증 : 성공 (밝은 녹색 표기)

```

[2309] 00:48:53.922 SELECT | CBMI
[2310] 00:48:53.937 UPDATE BINARY |
[2311] 00:48:53.962 SELECT | CBMIR
[2312] 00:48:53.977 UPDATE BINARY |
[2313] 00:49:00.080 SELECT | ADF USIM
[2314] 00:49:00.109 AUTHENTICATE | Re-Sync
[2315] 00:49:06.576 SELECT | ADF USIM
[2316] 00:49:06.605 AUTHENTICATE | Re-Sync
[2317] 00:49:12.076 STATUS |
[2318] 00:49:13.006 SELECT | ADF USIM
[2319] 00:49:13.035 AUTHENTICATE | Re-Sync
[2320] 00:49:13.492 UPDATE BINARY (SFI: 0x08) | Keys

```

#### Application-Level Analysis

```

=====
[2319] Logical Channel : 0
      Current DF File : A0000000871002FF82FFFF89010000FF [ADF USIM]
      Current EF File :
      Current Command : AUTHENTICATE
=====
      RAND : 82580143E2D4A65B08B3764C4D251938
      AUTN : 074B1FFF48F48002EC32F995348908D9
      AUTS : 46A30A862690324B2321234E186D
=====

```

APDU File System

#### Summary

```

[338] 05:21:00.499 ENVELOPE (SMS-PP Download) |
[339] 05:21:00.607 FETCH (OPEN CHANNEL) |
[340] 05:21:00.667 TERMINAL RESPONSE (OPEN CHANNEL) |
[341] 05:21:00.676 FETCH (SEND DATA) |
[342] 05:21:00.683 TERMINAL RESPONSE (SEND DATA) |
[343] 05:21:00.726 ENVELOPE (Event Download) | Data available
[344] 05:21:00.733 FETCH (RECEIVE DATA) |
[345] 05:21:00.737 TERMINAL RESPONSE (RECEIVE DATA) |
[346] 05:21:00.831 FETCH (SEND DATA) |
[347] 05:21:00.840 TERMINAL RESPONSE (SEND DATA) |
[348] 05:21:00.982 ENVELOPE (Event Download) | Data available
[349] 05:21:00.988 FETCH (RECEIVE DATA) |
[350] 05:21:00.993 TERMINAL RESPONSE (RECEIVE DATA) |
[351] 05:21:01.050 FETCH (SEND DATA) |
[352] 05:21:01.063 TERMINAL RESPONSE (SEND DATA) |
[353] 05:21:01.175 ENVELOPE (Event Download) | Data available
[354] 05:21:01.181 FETCH (RECEIVE DATA) |
[355] 05:21:01.185 TERMINAL RESPONSE (RECEIVE DATA) |
[356] 05:21:01.201 FETCH (RECEIVE DATA) |
[357] 05:21:01.206 TERMINAL RESPONSE (RECEIVE DATA) |
[358] 05:21:01.251 ENVELOPE (Event Download) | Data available
[359] 05:21:01.258 FETCH (RECEIVE DATA) |
[360] 05:21:01.262 TERMINAL RESPONSE (RECEIVE DATA) |
[361] 05:21:01.278 FETCH (RECEIVE DATA) |
[362] 05:21:01.282 TERMINAL RESPONSE (RECEIVE DATA) |
[363] 05:21:01.298 FETCH (RECEIVE DATA) |
[364] 05:21:01.302 TERMINAL RESPONSE (RECEIVE DATA) |
[365] 05:21:01.347 FETCH (RECEIVE DATA) |
[366] 05:21:01.351 TERMINAL RESPONSE (RECEIVE DATA) |
[367] 05:21:01.366 FETCH (RECEIVE DATA) |
[368] 05:21:01.371 TERMINAL RESPONSE (RECEIVE DATA) |
[369] 05:21:01.567 FETCH (SEND DATA) |
[370] 05:21:01.581 TERMINAL RESPONSE (SEND DATA) |
[371] 05:21:01.586 FETCH (SEND DATA) |
[372] 05:21:01.593 TERMINAL RESPONSE (SEND DATA) |
[373] 05:21:01.608 FETCH (SEND DATA) |
[374] 05:21:01.617 TERMINAL RESPONSE (SEND DATA) |
[375] 05:21:01.835 ENVELOPE (Event Download) | Data available
[376] 05:21:01.842 FETCH (RECEIVE DATA) |
[377] 05:21:01.846 TERMINAL RESPONSE (RECEIVE DATA) |
[378] 05:21:01.875 FETCH (SEND DATA) |
[379] 05:21:01.881 TERMINAL RESPONSE (SEND DATA) |
[380] 05:21:01.886 FETCH (CLOSE CHANNEL) |
[381] 05:21:13.097 TERMINAL RESPONSE (CLOSE CHANNEL) |
[382] 05:21:13.132 FETCH (REFRESH) | FCN
[383] 05:21:13.139 SELECT | Routing_Ind
[384] 05:21:13.147 READ BINARY |

```

USIM 인증 Re-Sync (분홍색 표기)

ENVELOPE 메시지에 포함된 ENVELOPE Type 확인 (SMS-PP, Event 등)

FETCH, TERMINAL RESPONSE 메시지의 Proactive Type 확인 (Send data, Receive data, Refresh 등)

Event Download 아이템 확인 (Data available, Location Status, MT Call 등)

REFRESH Type 확인 (FCN, UICC Reset, Steering of Roaming 등)

OTA 개통(BIP, NAS SMS) 관련 사항 (노란색 표기)

```

[1754] 00:48:43.855 RESET
[1755] 00:48:43.901 ATR_RX
[1756] 00:48:43.902 PPS_TX
[1757] 00:48:43.937 SELECT MF
[1758] 00:48:43.986 READ BINARY (SFI: 0x08) UMPC
[1759] 00:48:43.996 TERMINAL CAPABILITY
[1760] 00:48:44.008 SELECT ICCID
[1761] 00:48:44.019 READ BINARY
[1762] 00:48:44.028 MANAGE CHANNEL (OPEN) Logical channel number: 1
[1763] 00:48:44.036 SELECT ISD-R
[1764] 00:48:44.050 STORE DATA
[1765] 00:48:44.061 MANAGE CHANNEL (CLOSE) Logical channel number: 1
[1766] 00:48:44.066 SELECT PL

```

SIM RESET (COLD/WARM) 확인 (하늘색 표기)

Logical Channel 관리 (OPEN/CLOSE) 확인 (엷은 하늘색 표기)

```

[406] 07:50:13.013 ENVELOPE (SMS-PP Download)
[407] 07:50:13.333 ENVELOPE (SMS-PP Download)
[408] 07:50:13.651 ENVELOPE (SMS-PP Download)
[409] 07:50:13.879 SELECT ADF ISIM
[410] 07:50:13.887 AUTHENTICATE ADF ISIM
[411] 07:50:13.977 ENVELOPE (SMS-PP Download)
[412] 07:50:14.301 ENVELOPE (SMS-PP Download)
[413] 07:50:14.445 FETCH (REFRESH) UICC Reset
[414] 07:50:14.450 TERMINAL RESPONSE (REFRESH) ERROR (result'0x20')
[415] 07:50:14.475 FETCH (POLL INTERVAL) 30sec
[416] 07:50:14.499 TERMINAL RESPONSE (POLL INTERVAL)
[417] 07:50:21.568 STORE DATA
[418] 07:50:23.134 ENVELOPE (SMS-PP Download)
[419] 07:50:23.501 ENVELOPE (SMS-PP Download)
[420] 07:50:23.852 ENVELOPE (SMS-PP Download)
[421] 07:50:24.194 ENVELOPE (SMS-PP Download)
[422] 07:50:24.536 ENVELOPE (SMS-PP Download)
[423] 07:50:24.774 ENVELOPE (SMS-PP Download)
[424] 07:50:25.116 ENVELOPE (SMS-PP Download)
[425] 07:50:25.196 FETCH (REFRESH) UICC Reset
[426] 07:50:25.203 TERMINAL RESPONSE (REFRESH) ERROR (result'0x20')

```

#### Application-Level Analysis

```

[426] Logical Channel : 0
Current DF File : 7F105F3A [DF PHONEBOOK]
Current EF File : 4F09 [PBC]
Current Command : TERMINAL RESPONSE (REFRESH)

```

ERROR 원인 확인

\*result'0x20': Terminal currently unable to process command

ERROR 처리 확인 \*단말 에러 응답(T/R) 예시 (빨간색 표기)

```

[28] 09:00:27.684 POWER_OFF
[29] 09:00:27.958 COLD_RESET
[30] 09:00:28.010 ATR_RX
[31] 09:00:28.012 PPS_TX
[32] 09:00:28.024 PPS_RX
[33] 09:00:28.045 GET DATA
[34] 09:00:28.047 GET DATA
[35] 09:00:28.048 TERMINAL CAPABILITY
[36] 09:00:28.215 MANAGE CHANNEL (OPEN) Logical channel number: 1
[37] 09:00:28.219 MANAGE CHANNEL (OPEN) Logical channel number: 2
[38] 09:00:28.222 SELECT ISD-R
[39] 09:00:28.235 STORE DATA
[40] 09:00:28.247 STORE DATA
[41] 09:00:28.320 SELECT A00000000090203FFFFFFFF89010000FF
[42] 09:00:28.327 SELECT MF
[43] 09:00:28.363 READ BINARY (SFI: 0x08) UMPC
[44] 09:00:28.372 TERMINAL CAPABILITY
[45] 09:00:28.377 SELECT ICCID
[46] 09:00:28.383 READ BINARY
[47] 09:00:28.385 TERMINAL PROFILE ERROR (SW'6F00')

```

#### Application-Level Analysis

```

[47] Logical Channel : 0
Current DF File : 3F00 [MF]
Current EF File : 2FE2 [ICCID]
Current Command : TERMINAL PROFILE

```

ERROR 원인 확인

\*SW'6F00': Technical problem, no precise diagnosis

ERROR 처리 확인 \*SIM 에러 응답(SW) 예시 (빨간색 표기)



# (1) APDU Tab : Protocol / Application-Level 분석

Summary 창에서 로그를 선택 시 Protocol / Application-Level Analysis 창에 상세 내용 출력됨

APDU File System

Summary

[22]	23:37:37.661	STORE DATA		
[23]	23:37:37.693	STORE DATA		
[24]	23:37:38.620	SELECT		ADF USIM
[25]	23:37:38.631	AUTHENTICATE		ERROR (SW'9862')
[26]	23:37:38.647	STORE DATA		
[27]	23:37:38.694	STORE DATA		
[28]	23:37:38.717	STORE DATA		
[29]	23:37:38.732	UPDATE BINARY (SFI: 0x09)		KeysPS
[35]	23:37:39.380	UPDATE BINARY (SFI: 0x08)		Keys
[36]	23:37:39.387	STORE DATA		
[37]	23:37:39.403	STORE DATA		
[38]	23:37:39.418	STORE DATA		
[39]	23:37:39.433	STORE DATA		
[40]	23:37:40.064	SELECT		CBMI
[41]	23:37:40.072	UPDATE BINARY		
[42]	23:37:40.090	STORE DATA		
[43]	23:37:40.107	SELECT		CBMIR
[44]	23:37:40.115	UPDATE BINARY		
[45]	23:37:40.119	STORE DATA		
[46]	23:37:40.134	SELECT		CBMI
[47]	23:37:40.142	UPDATE BINARY		
[48]	23:37:40.152	STORE DATA		
[54]	23:37:41.611	STORE DATA		
[55]	23:37:41.626	STORE DATA		
[56]	23:37:42.905	STORE DATA		
[57]	23:37:43.693	STORE DATA		

**Protocol-Level Analysis**

- 1개의 Command 를 구성하는 전체 APDU Data 출력
- 단말 or SIM 이슈 분석에 활용

**Application-Level Analysis**

- 선택 시점의 Logical Channel / Current DF / Current DF 정보 출력
- APDU 상세 내용 및 Error 분석 제공

Protocol-Level Analysis

```
[25] 23:37:38.631 [TX] 00 88 00 81 22
-----
23:37:38.632 [RX] 88
-----
23:37:38.632 [TX] 10 0D B4 F0 0E 1A C2 4F 43 2D D5 E8 1C 3D 40 F1
48 10 C8 C0 68 37 3D AE 80 02 7D CA 83 46 DA D5
00 D2
-----
23:37:38.646 [RX] 98 62
-----
```

Application-Level Analysis

```
[25] Logical Channel : 0
Current DF File : A0000000871002FF82FFFF89010000FF [ADF USIM]
Current EF File :
Current Command : AUTHENTICATE
-----
RAND : 0DB4F00E1AC24F432DD5E81C3D40F148
AUTN : C8C068373DAE80027DCA8346DAD500D2
-----
*SW'9862': Authentication error, application specific
-----
```

## Application-Level Analysis

```
[214] Logical Channel : 4 [Extended]
Current DF File : A0000000871002FF82FFFF89010000FF [ADF USIM]
Current EF File : 6F16
Current Command : SELECT
-----
*SW'6A82': File not found
**7FFF6F16': Unknown file id in current DF
-----
```

## (2) File System Tab : 화면 구성

<b>File Open button</b> Text로 저장된 단말 로그 열기	<b>Clipboard button</b> QXDM 로그 복사 후 클립보드 붙여넣기	<b>로그 불러오기 결과</b> 파일 또는 클립보드 붙여넣기 결과
<b>Combo box</b> SIM 포트1,2 선택	<b>Execute button</b> APDU Parsing 실행 버튼	<b>실행 결과</b> APDU Parsing 결과

APDU Tab

File System Tab

단말에서 Read한 전체 File System 및 Contents 확인

**File System 구조**  
선택된 SIM 포트에서 단말이 Read (Binary or Record) 처리한 File 리스트  
(DF, File, DF Id, EF Id, File Type, SFI, REC #, Offset, Length, APDU reference)  
※ 각 File Item 선택 가능

**File Contents**  
선택된 File Item에 저장된 Hex값 확인

**File Contents Parsing**  
선택된 File Item에 대한 Parsing 결과  
※ 일부 EF File에 한정, 향후 필요에 따라 Parsing 기능 추가 개발 가능

## (2) File System Tab : 화면 예시 및 설명

단말이 READ BINARY / RECORD 처리로 읽은 모든 EF File Contents 및 Parsing 제공

APDU	File System									File Contents
DF	File	DF_Id	File_Id	Type	SFI	REC#	OffS	LEN	ref	
DF	EF name	DF ID	EF ID	LF/TF	SFI	REC#	Offset	Length	APDU 위치	
MF	PL	3F00	2F05	TF	-	-	00	14	[128]	APDU 탭의 로그 위치 확인
MF	UMPC	3F00	2F08	TF	08	-	00	05	[123]	
MF	ICCID	3F00	2FE2	TF	-	-	-	0A	[126]	
ADF USIM	LI	AID	6F05	TF	-	-	-	14	[153]	EF File Id 순 오름차순
ADF USIM	ARR	AID	6F06	LF	17	01	-	36	[297]	
ADF USIM	ARR	AID	6F06	LF	-	01	-	36	[646]	
ADF USIM	ARR	AID	6F06	LF	17	03	-	36	[284]	개별 Item 클릭 시 Contents 및 Parsing 확인
ADF USIM	ARR	AID	6F06	LF	-	04	-	36	[263]	
ADF USIM	ARR	AID	6F06	LF	17	06	-	36	[291]	
ADF USIM	IMSI	AID	6F07	TF	07	-	00	09	[190]	
ADF USIM	IMSI	AID	6F07	TF	07	-	00	09	[545]	
ADF USIM	Keys	AID	6F08	TF	08	-	00	21	[196]	
ADF USIM	KeysPS	AID	6F09	TF	09	-	00	21	[197]	
ADF USIM	HPPLMN	AID	6F31	TF	12	-	00	01	[222]	
ADF USIM	ACMmax	AID	6F37	TF	-	-	00	03	[238]	
ADF USIM	UST	AID	6F38	TF	-	-	00	19	[193]	
ADF USIM	ACM	AID	6F39	LF	1C	-	-	-	[234]	
ADF USIM	ACM	AID	6F39	LF	-	01	-	03	[236]	
ADF USIM	MSISDN	AID	6F40	LF	-	01	-	1E	[266]	
ADF USIM	MSISDN	AID	6F40	LF	-	01	-	1E	[634]	
ADF USIM	MSISDN	AID	6F40	LF	-	02	-	1E	[315]	
ADF USIM	MSISDN	AID	6F40	LF	-	03	-	1E	[329]	
ADF USIM	SMSP	AID	6F42	LF	-	01	-	2C	[309]	
ADF USIM	SMSP	AID	6F42	LF	-	02	-	2C	[322]	
ADF USIM	SMSS	AID	6F43	TF	-	-	00	02	[260]	
ADF USIM	SMSS	AID	6F43	TF	-	-	00	04	[355]	
ADF USIM	CBMI	AID	6F45	TF	-	-	00	32	[333]	
ADF USIM	CBMI	AID	6F45	TF	-	-	00	32	[687]	
ADF USIM	SPN	AID	6F46	TF	-	-	00	11	[204]	
ADF USIM	CBMID	AID	6F48	TF	-	-	00	10	[233]	
ADF USIM	SDN	AID	6F49	LF	-	01	-	1E	[375]	
ADF USIM	CBMIR	AID	6F50	TF	-	-	00	10	[340]	
ADF USIM	EST	AID	6F56	TF	-	-	00	0C	[219]	
ADF USIM	START-HFN	AID	6F5B	TF	0F	-	00	06	[198]	
ADF USIM	THRESHOLD	AID	6F5C	TF	10	-	00	03	[199]	
ADF USIM	PLMNwAcT	AID	6F60	TF	-	-	00	64	[226]	
ADF USIM	OPLMNwAcT	AID	6F61	TF	-	-	00	FF	[228]	
ADF USIM	OPLMNwAcT	AID	6F61	TF	-	-	FF	F5	[229]	
ADF USIM	HPLMNwAcT	AID	6F62	TF	-	-	00	32	[224]	
ADF USIM	PSLOCi	AID	6F73	TF	0C	-	00	0E	[195]	
ADF USIM	ACC	AID	6F78	TF	06	-	00	02	[191]	
ADF USIM	ACC	AID	6F78	TF	06	-	00	02	[546]	
ADF USIM	FPLMN	AID	6F7B	TF	-	-	00	3C	[231]	
ADF USIM	LOCi	AID	6F7E	TF	0B	-	00	0B	[194]	
ADF USIM	LOCi	AID	6F7E	TF	0B	-	00	0B	[549]	

File Contents Parsing

```
[X] Service n1 Local Phone Book
[X] Service n2 Fixed Dialling Numbers (FDN)
[X] Service n3 Extension 2
[O] Service n4 Service Dialling Numbers (SDN)
[O] Service n5 Extension3
[X] Service n6 Barred Dialling Numbers (BDN)
[O] Service n7 Extension4
[O] Service n8 Outgoing Call Information (OCI and OCT)
[O] Service n9 Incoming Call Information (ICI and ICT)
[O] Service n10 Short Message Storage (SMS)
[O] Service n11 Short Message Status Reports (SMSR)
[O] Service n12 Short Message Service Parameters (SMSP)
[O] Service n13 Advice of Charge (AoC)
[O] Service n14 Capability Configuration Parameters 2 (CCP2)
[O] Service n15 Cell Broadcast Message Identifier
[O] Service n16 Cell Broadcast Message Identifier Ranges
[X] Service n17 Group Identifier Level 1
[X] Service n18 Group Identifier Level 2
[O] Service n19 Service Provider Name
[O] Service n20 User controlled PLMN selector with Access Technology
[O] Service n21 MSISDN
[X] Service n22 Image (IMG)
[X] Service n23 Support of Localised Service Areas (SoLSA)
[O] Service n24 Enhanced Multi Level Precedence and Pre emption Service
[O] Service n25 Automatic Answer for eMLPP
[O] Service n26 RFU
[O] Service n27 GSM Access
[O] Service n28 Data download via SMS-PP
[O]
[O]
[O]
[O]
[X] Service n36 Depersonalisation Control Keys
[X] Service n37 Co-operative Network List
```

동일 File 중복 제거 상태  
단, File 값 변경이 있을 시 제외 및 색상 표기

- 개통 데이터 포함 EF 파일 (노란색 표기)
- 개통 데이터 외 EF 파일 (연녹색 표기)

## [참고] 색상 규칙 정리

### (1) APDU Tab

APDU Summary 요약 메시지의 하기 문자열 포함 여부 기준으로 색상 적용

Red	= ['ERROR']
Magenta	= ['Re-Sync']
Grey	= ['(X)', '(*)', 'Unknown']
Yellow	= ['ENVELOPE', 'REFRESH']
Cyan	= ['RESET', 'POWER']
Light blue	= ['MANAGE CHANNEL']
Light green	= ['AUTHENTICATE']

(\*) : APDU 메시지 내 누락 발생 시

APDU		File System
Summary		Protocol-Level Analysis
[46]	09:00:28.383	READ_BINARY
[47]	09:00:28.385	TERMINAL_PROFILE
[48]	09:00:54.236	STATUS (*)
[49]	09:00:55.523	POWER_OFF
[50]	09:00:55.798	COLD_RESET

Unknown : 스펙 미포함 Instruction(INS) code

[1]	23:37:18.417	STATUS
[2]	23:37:18.431	STATUS
[3]	23:37:23.941	INS: 0x51
[4]	23:37:23.969	INS: 0x51
[5]	23:37:24.854	INS: 0x51
[6]	23:37:24.882	INS: 0x51

### (2) File System Tab

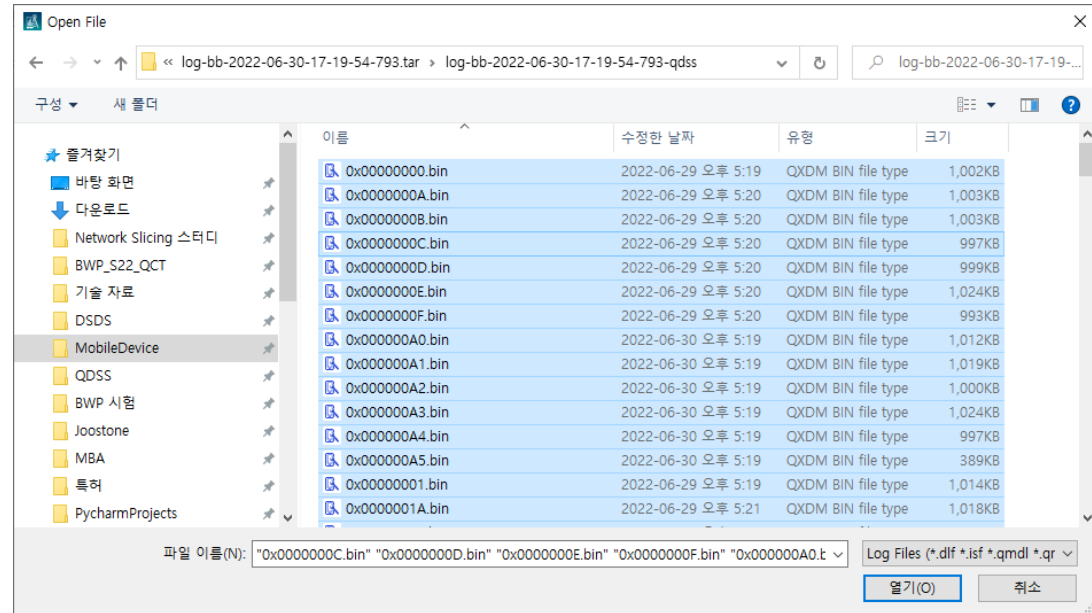
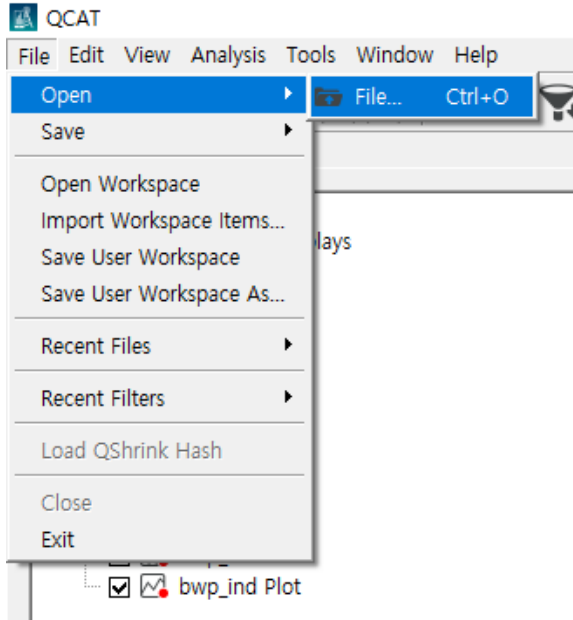
EF File의 Contents 변경 발생 시에만 적용, 하기 문자열 포함 여부에 따라 자사 개통 데이터 대상 EF 파일 구분

Yellow	= ['IMSI', 'MSISDN', 'OPLMNwAcT', 'ACC', 'Routing Indicator', 'IMPI', 'IMPU']
Light green	= 상기 EF 파일 외

### (3) QCAT 로그 분석 방법 [1/6]

#### 1. QCAT 에서 단말 CP 로그 열기 (\*.bin / \*.qdss)

※ 단말 제조사 별 CP 로그 확보 방법은 각 제조사 PM 통해 확인 (삼성 silent log dump, 애플 carrier dump)



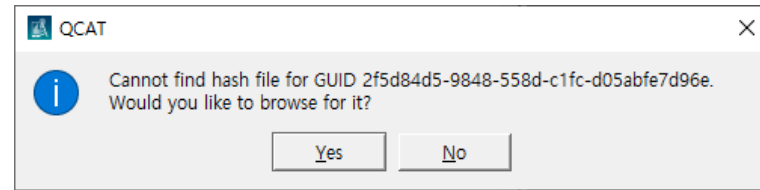
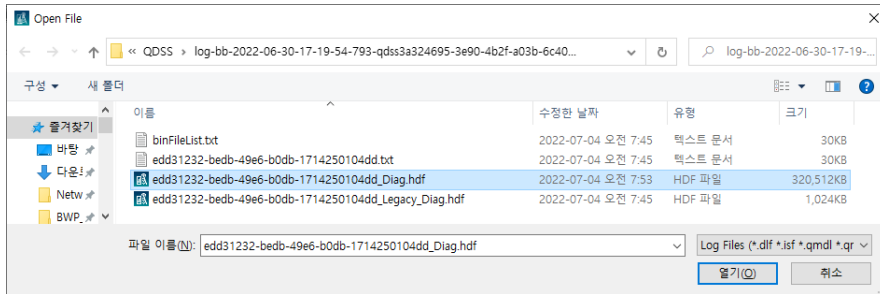
#### 2. QCAT 에서 파일 Open 시 HDF 로그 파일 자동 생성됨

※ HDF(\*.hdf) 파일 생성 루트 : C:\Users\User\AppData\Local\Temp\QDSS

aj3013 > AppData > Local > Temp > QDSS > log-bb-2022-06-30-17-19-54-793-qdss3a324695-3e90-4b2f-a03b-6c40297864f1			
이름	수정한 날짜	유형	크기
binFileList.txt	2022-07-04 오전 7:45	텍스트 문서	30KB
edd31232-bedb-49e6-b0db-1714250104dd.txt	2022-07-04 오전 7:45	텍스트 문서	30KB
edd31232-bedb-49e6-b0db-1714250104dd_Diag.hdf	2022-07-04 오전 7:45	HDF 파일	320,512KB
edd31232-bedb-49e6-b0db-1714250104dd_Legacy_Diag.hdf	2022-07-04 오전 7:45	HDF 파일	1,024KB

### (3) QCAT 로그 분석 방법 [2/6]

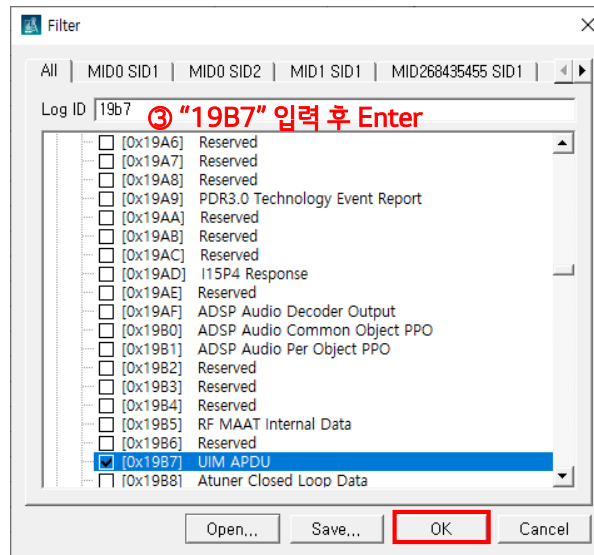
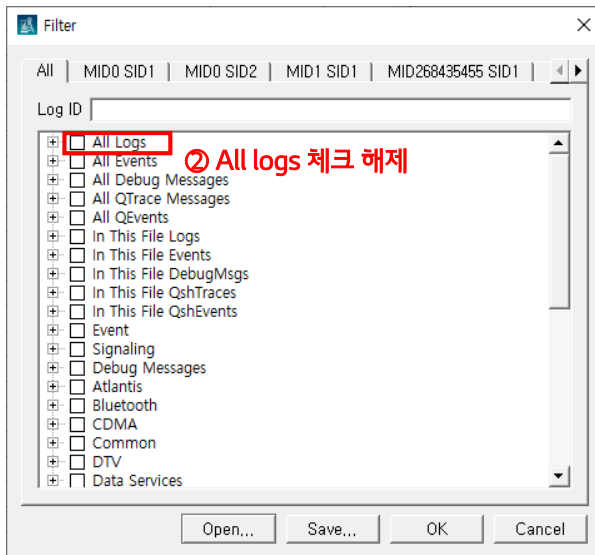
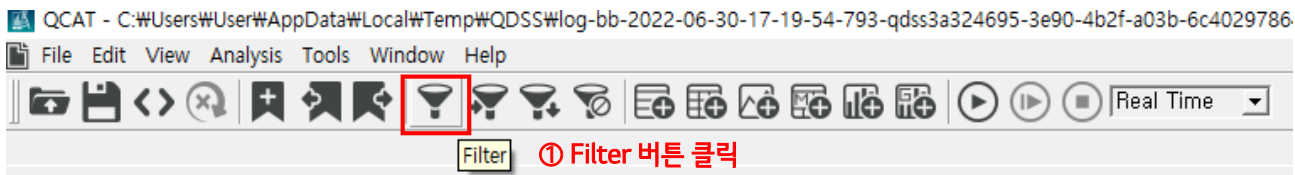
#### 3. QCAT 에서 HDF 로그 파일 열기 (\*.hdf)



※ "No" 선택 가능 (SIM APDU 로그는 hash 파일 없이도 Parsing 가능함)

#### 4. 로그 파일 열기 완료 → "Filter" 버튼 클릭 → All Logs 체크 해제 → "19B7" 검색 후 선택

※ SIM APDU 로그는 hash 파일 없이도 Parsing 가능함 ("No" 선택)



④ "UIM APDU" 체크

⑤ "OK" 클릭하여 필터 적용

### (3) QCAT 로그 분석 방법 [3/6]

#### 5. 필터 적용 완료 후 텍스트 파일로 저장하기 (\*.txt)

QCAT - C:\Users\User\AppData\Local\Temp\QDSS\log-bb-2022-06-30-17-19-54-793-qdss3a324695-3e90-4b2f-a03b-6c40297864f1\edd31232-bedb-49e6-b0db-1714250104dd\_Diag.hdf - [Packet Text]

File Edit View Analysis Tools Window Help

Open Save Text... Ctrl+S Bookmarked to Text... ISF... Ctrl+I DLF... Ctrl+D HDF... Ctrl+H PPP Info... CFA Info...

Open Workspace Import Workspace Items... Save User Workspace Save User Workspace As... Recent Files Recent Filters Load QShrink Hash Close Exit

2022 Jun 29 08:10:33.070 1 UIM APDU  
2022 Jun 29 08:19:36.164 2 UIM APDU  
2022 Jun 29 08:19:36.164 2 UIM APDU  
2022 Jun 29 08:19:36.169 2 UIM APDU  
2022 Jun 29 08:19:36.176 2 UIM APDU  
2022 Jun 29 08:19:36.177 2 UIM APDU  
2022 Jun 29 08:19:36.177 2 UIM APDU  
2022 Jun 29 08:19:36.185 2 UIM APDU  
2022 Jun 29 08:19:36.185 2 UIM APDU  
2022 Jun 29 08:19:36.186 2 UIM APDU  
2022 Jun 29 08:19:38.336 1 UIM APDU  
2022 Jun 29 08:19:39.147 1 UIM APDU  
2022 Jun 29 08:19:39.160 1 UIM APDU  
2022 Jun 29 08:19:39.971 1 UIM APDU  
2022 Jun 29 08:19:40.007 1 UIM APDU  
2022 Jun 29 08:19:40.818 1 UIM APDU  
2022 Jun 29 08:19:40.831 1 UIM APDU  
2022 Jun 29 08:19:41.837 1 UIM APDU  
2022 Jun 29 08:19:41.874 1 UIM APDU  
2022 Jun 29 08:19:42.880 1 UIM APDU  
2022 Jun 29 08:19:50.336 1 UIM APDU  
2022 Jun 29 08:19:51.146 1 UIM APDU  
2022 Jun 29 08:19:51.159 1 UIM APDU  
2022 Jun 29 08:19:51.969 1 UIM APDU  
2022 Jun 29 08:19:52.005 1 UIM APDU  
2022 Jun 29 08:19:52.815 1 UIM APDU  
2022 Jun 29 08:19:52.828 1 UIM APDU  
2022 Jun 29 08:19:53.833 1 UIM APDU  
2022 Jun 29 08:19:53.870 1 UIM APDU  
2022 Jun 29 08:19:54.875 1 UIM APDU  
2022 Jun 29 08:20:02.337 1 UIM APDU  
2022 Jun 29 08:20:03.147 1 UIM APDU  
2022 Jun 29 08:20:03.160 1 UIM APDU  
2022 Jun 29 08:20:03.970 1 UIM APDU

Save As

Save in: C:\Users\User\PycharmPr...DU-Analyzer\file\_sample

My Computer User

Name	Size	Type	Date Modified
iPhone13_GP_BIP_fail.txt	408.54 KIB	t...e	2022-06-29 0...
NED_eSIM_install_fail.txt	181.75 KIB	t...e	2022-06-27 0...
S22_pSIM_single.txt	191.79 KIB	t...e	2022-06-26 0...
Flip4_eSIM_install_fail.txt	406.27 KIB	t...e	2022-06-24 0...
iPhone13_eSIM_install_fail.txt	518.16 KIB	t...e	2022-06-23 0...
Fold4_eSIM_OTA.txt	1.72 MiB	t...e	2022-05-30 0...
iPhone13_OTA.txt	1.61 MiB	t...e	2022-04-14 0...

File name: edd31232-bedb-49e6-b0db-1714250104dd\_Diag.txt Save

Save as type: QCAT Output Files (\*.txt) Cancel

☐ Hex Dump ☐ QCAT 3.x Compatible ☐ Save Debug Messages Only

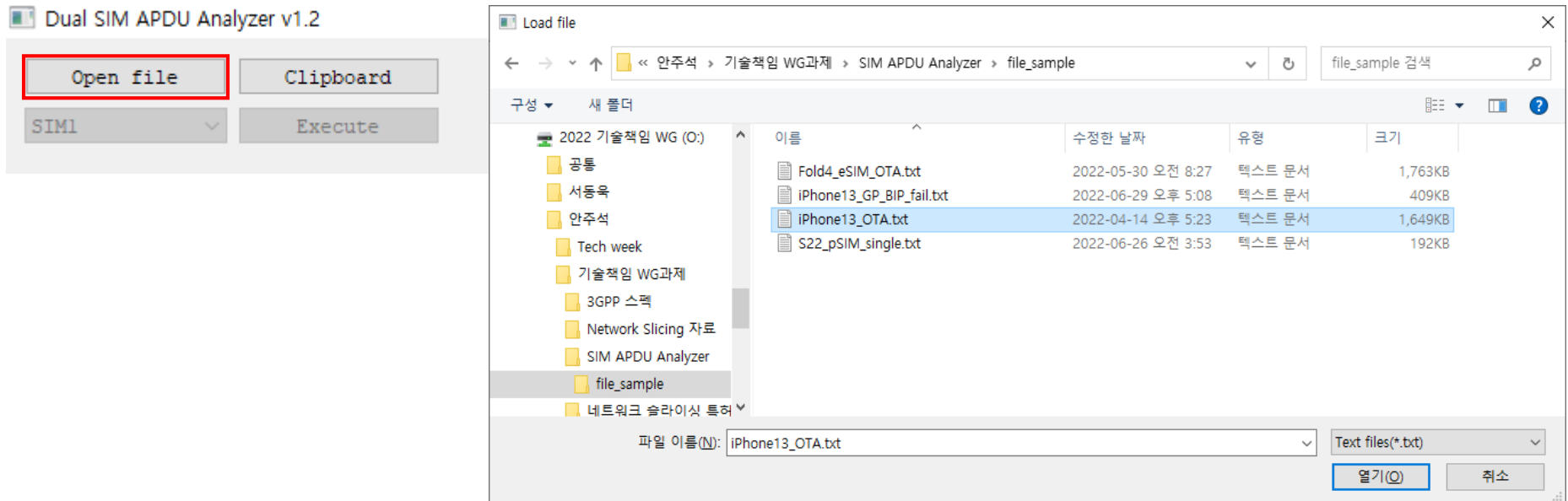
※ QXDM-SIM-APDU-Analyzer 실행 파일 (\*.exe) 있는 루트에 저장

Displays Packets Configuration

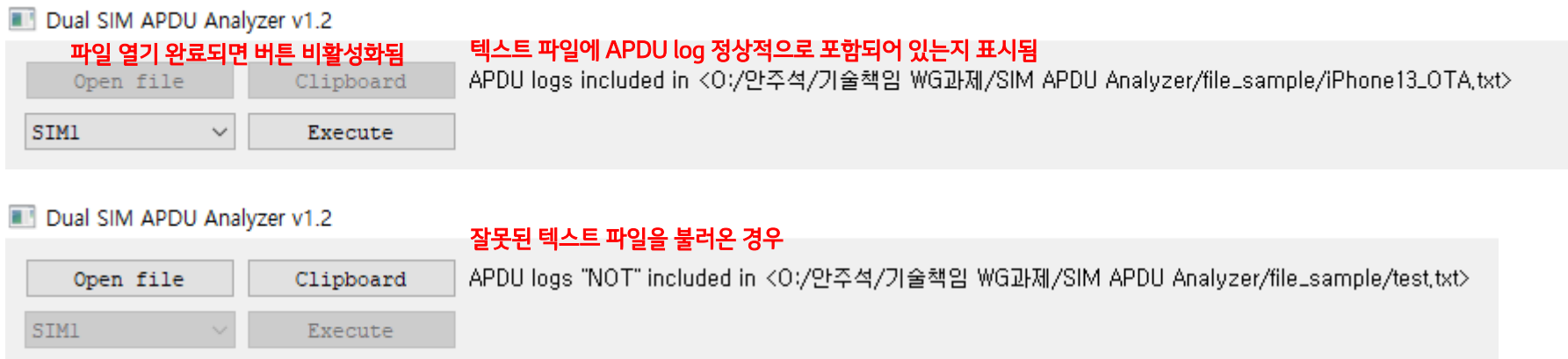
Ready 2189835 Packets; 0 Selected

### (3) QCAT 로그 분석 방법 [4/6]

#### 6. QXDM-SIM-APDU-Analyzer 실행 후 "Open file" 버튼 클릭하여 저장한 텍스트 파일 열기



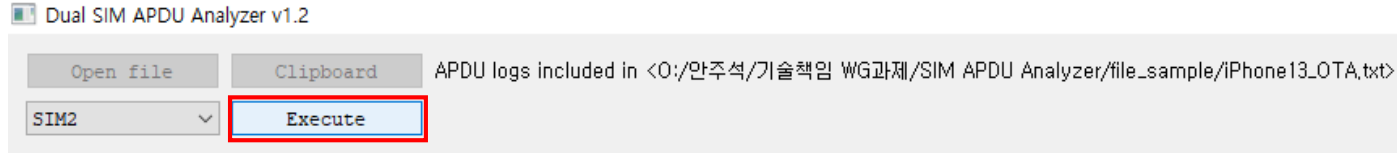
#### 7. 텍스트 파일 열기 완료 화면



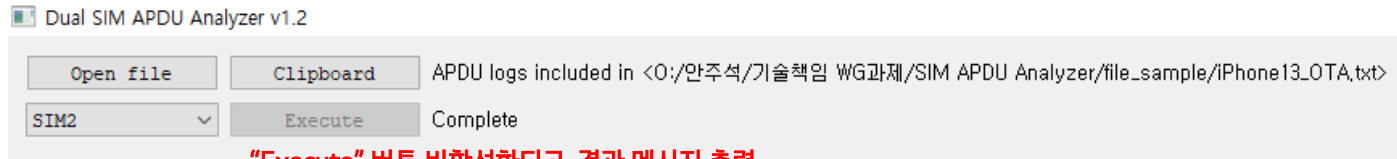


### (3) QCAT 로그 분석 방법 [5/6]

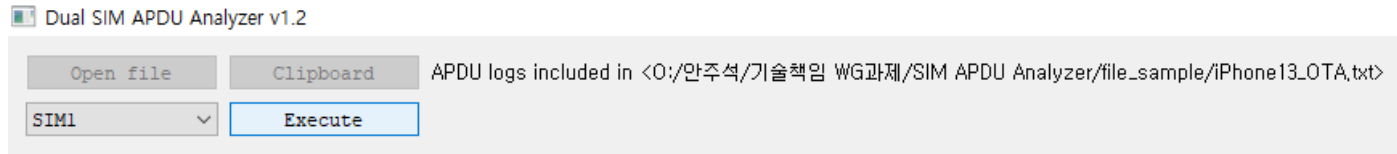
#### 8. SIM1,2 선택 후 "Execute" 버튼 클릭



SIM1,2 선택 후 "Execute" 버튼 클릭



"Execute" 버튼 비활성화되고, 결과 메시지 출력



SIM1,2 변경 시 "Execute" 버튼 다시 활성화됨

### (3) QCAT 로그 분석 방법 [6/6]

#### 9. 결과 화면

Open file

Clipboard

APDU logs included in <E:/PycharmProjects/SIM-APDU-Analyzer-for-QXDM/file\_sample/Clipboard\_eSIM\_Install\_C9100\_BIP\_Pass.txt>

SIM2

Execute

Complete

APDU

File System

Summary

[1]	05:20:53.786	STORE DATA	
[2]	05:20:54.199	SELECT	ADF USIM
[3]	05:20:54.217	STORE DATA	
[4]	05:20:54.309	SELECT	ECC
[5]	05:20:54.317	READ RECORD	
[6]	05:20:54.320	READ RECORD	
[7]	05:20:54.324	READ RECORD	
[8]	05:20:54.327	READ RECORD	
[9]	05:20:54.330	READ RECORD	
[10]	05:20:54.333	READ RECORD	
[11]	05:20:54.336	READ RECORD	
[12]	05:20:54.339	READ RECORD	
[13]	05:20:54.343	SELECT	LI
[14]	05:20:54.352	READ BINARY	
[15]	05:20:54.360	STORE DATA	
[16]	05:20:54.369	SELECT	MF
[17]	05:20:54.398	READ BINARY (SFI: 0x08)	UMPC
[18]	05:20:54.403	TERMINAL CAPABILITY	
[19]	05:20:54.407	SELECT	ICCID
[20]	05:20:54.414	READ BINARY	
[21]	05:20:54.418	SELECT	PL
[22]	05:20:54.426	READ BINARY	
[23]	05:20:54.430	TERMINAL PROFILE	
[24]	05:20:54.883	MANAGE CHANNEL (OPEN)	Logical channel number: 4
[25]	05:20:54.886	SELECT	DIR
[26]	05:20:54.894	READ RECORD	
[27]	05:20:54.900	READ RECORD	
[28]	05:20:54.906	SELECT	DIR
[29]	05:20:54.911	FETCH (SETUP EVENT LIST)	Data available, Channel status
[30]	05:20:54.914	SELECT	ADF USIM
[31]	05:20:54.927	TERMINAL RESPONSE (SETUP EVENT LIST)	
[32]	05:20:54.932	FETCH (POLL INTERVAL)	30sec
[33]	05:20:54.935	SELECT	ECC
[34]	05:20:54.963	READ RECORD	
[35]	05:20:54.966	TERMINAL RESPONSE (POLL INTERVAL)	
[36]	05:20:54.971	READ RECORD	
[37]	05:20:54.974	STORE DATA	
[38]	05:20:55.065	READ RECORD	
[39]	05:20:55.068	READ RECORD	
[40]	05:20:55.071	READ RECORD	
[41]	05:20:55.075	READ RECORD	
[42]	05:20:55.078	READ RECORD	
[43]	05:20:55.082	READ RECORD	
[44]	05:20:55.087	SELECT	LI
[45]	05:20:55.095	READ BINARY	
[46]	05:20:55.100	UNBLOCK PIN	
[47]	05:20:55.102	VERIFY PIN	

Protocol-Level Analysis

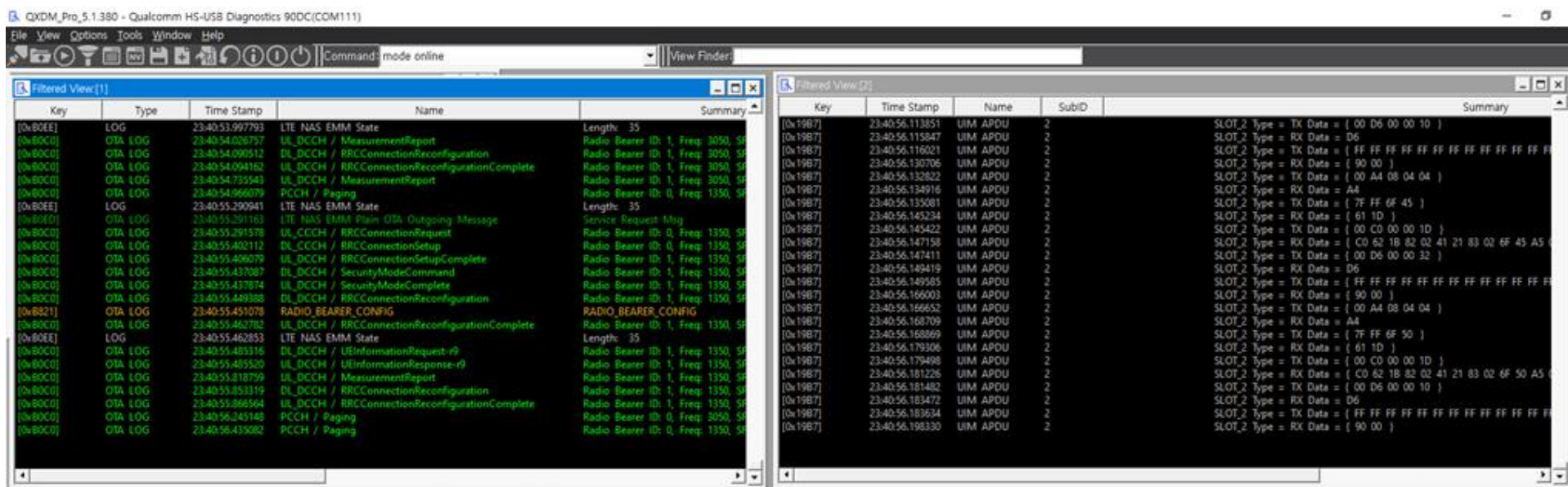
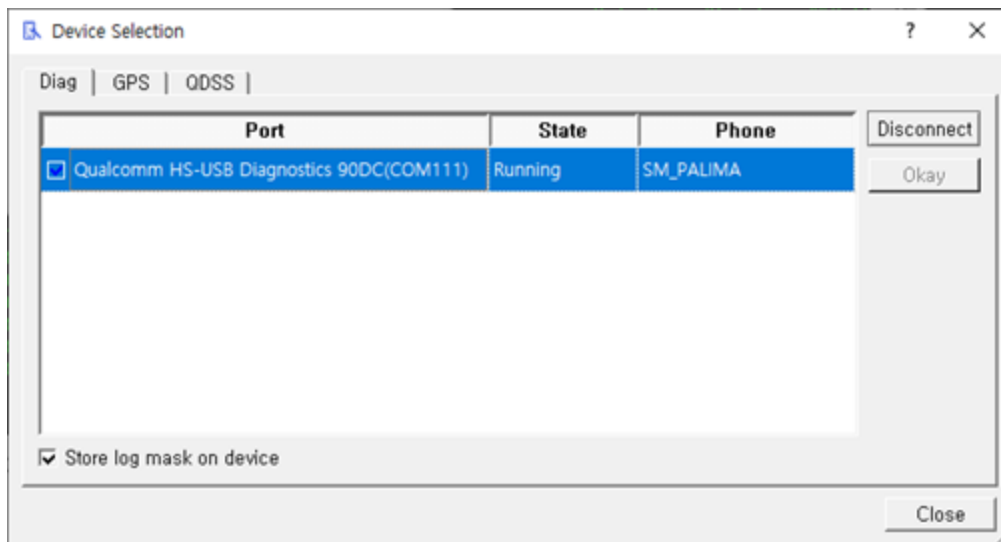
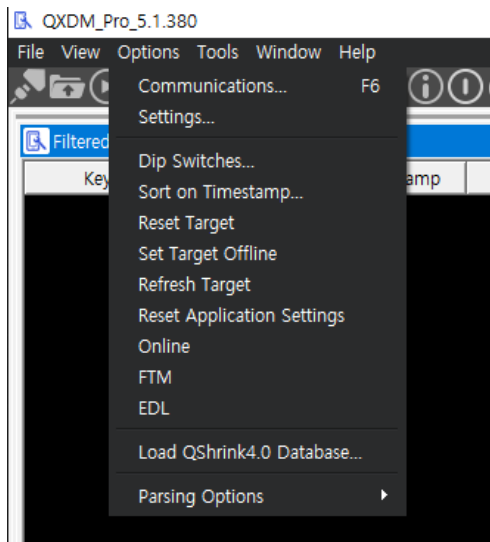
Application-Level Analysis

Copyright 2022, JUSEOK AHN<ajs3013@lguplus.co.kr> all rights reserved.

## (4) QXDM 로그 분석 방법 [1/5]

### 1. 단말 포트 연결

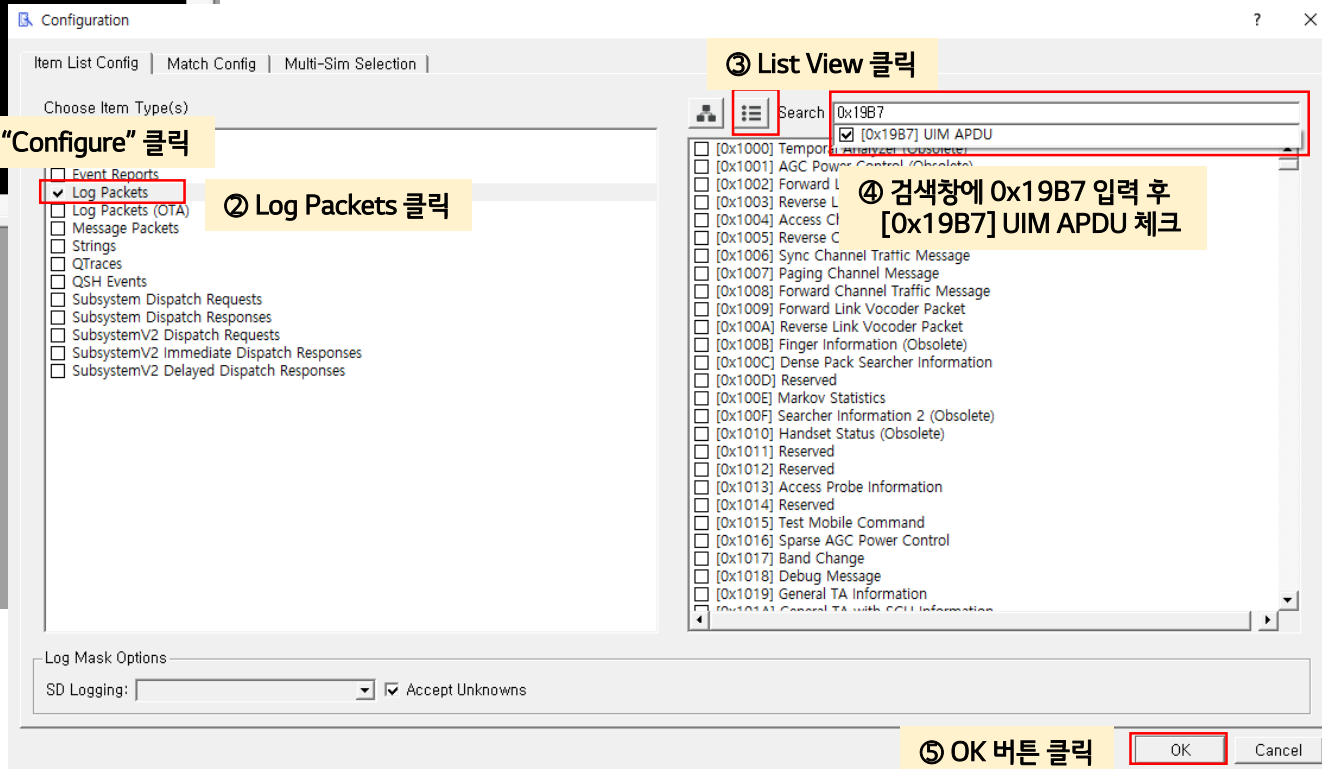
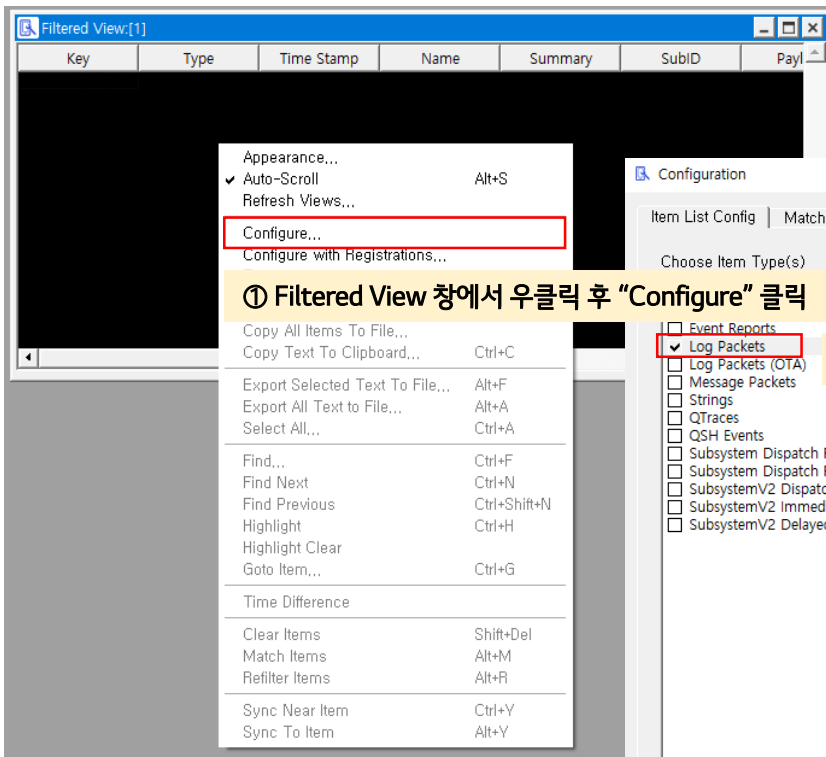
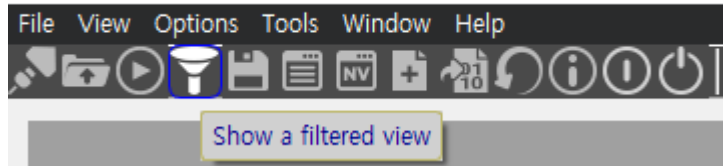
※ 단말 제조사 별 포트 연결 방법은 각 제조사 PM 통해 확인 (삼성 usb setting, 애플 logging port 변경)



## (4) QXDM 로그 분석 방법 [2/5]

### 2. Filtered View 생성 (0x19B7 UIM APDU)

QXDM\_Pro\_5.1.460 (Disconnected)



## (4) QXDM 로그 분석 방법 [3/5]

### 3. UIM APDU (0x19B7) 로그 복사하기

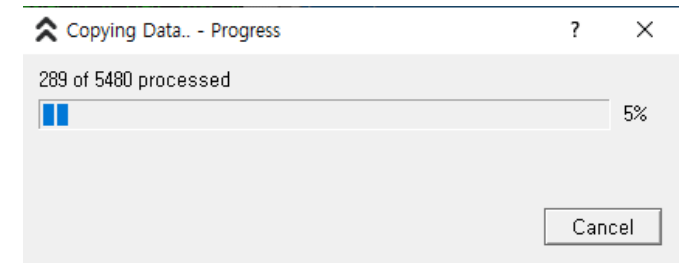
- Filter View 창에서 "Ctrl+A" + "Ctrl+C"

The screenshot shows the 'Filtered View: [2]' window with a table of log entries. The table has columns: Key, Time Stamp, Name, SubID, and Summary. The entries are filtered for 'UIM APDU' with 'Key' 0x19B7. A right-click context menu is displayed over the table, with the following options and shortcuts:

- Appearance...
- Auto-Scroll
- Refresh Views...
- Configure...
- Configure with Registrations...
- Tag
- Copy Selected Items To File...
- Copy All Items To File...
- Copy Text To Clipboard... Ctrl+C**
- Export Selected Text To File... Alt+F
- Export All Text to File... Alt+A
- Select All... Ctrl+A**
- Find...
- Find Next
- Find Previous
- Highlight
- Highlight Clear
- Goto Item...
- Time Difference
- Bookmark Item(s)
- Bookmark Up
- Bookmark Down
- Clear Items
- Match Items
- Refilter Items
- Sync Near Item
- Sync To Item

The bottom pane shows the details of the selected log entry (Key: 0x19B7, Time Stamp: 23:41:48.524154):

```
23:41:48.524154 [0x19B7] UIM APDU
Version = 1
Version 1 {
  Sequence Number = 28178
  Slot Id = SLOT_2
  Message Type = TX
  Control byte = 160
  TX Data = { 81 , E2 , 91 , 00 , 20 }
}
```

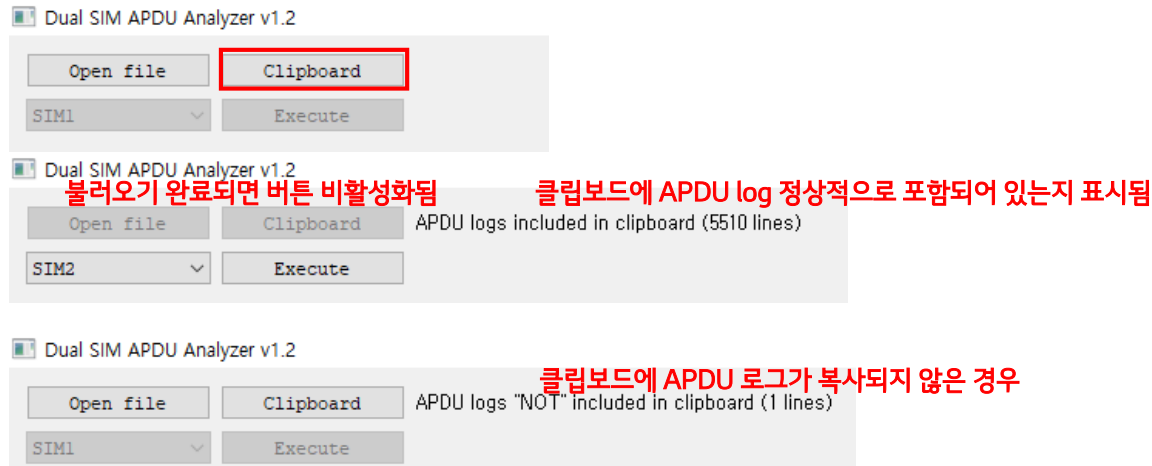


② Filter View:[2] 우클릭 후 Copy Text To Clipboard 선택 (Ctrl+C)

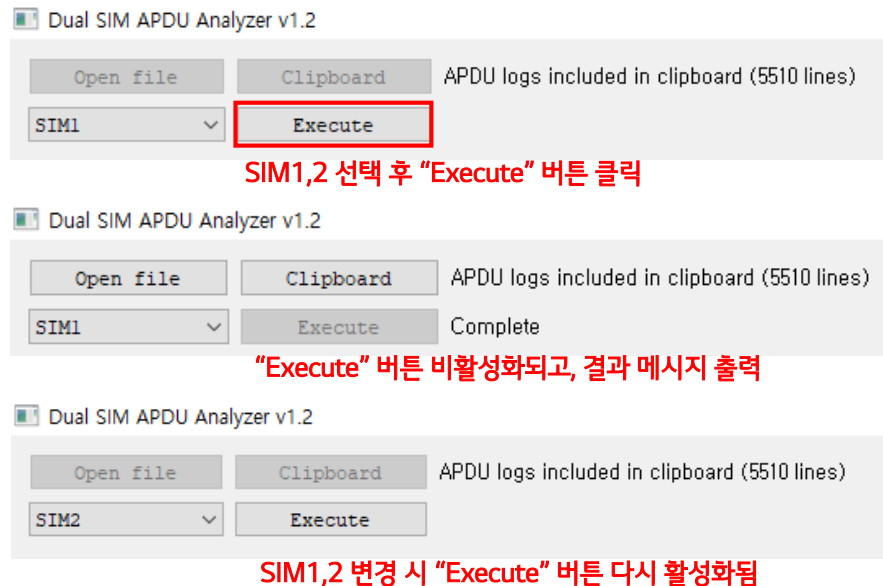
① Filter View:[2] 우클릭 후 Select All 선택 (Ctrl+A)

## (4) QXDM 로그 분석 방법 [4/5]

### 4. QXDM-SIM-APDU-Analyzer 실행 후 “Clipboard” 버튼 클릭하여 클립보드에 복사된 로그 불러오기



### 5. SIM1,2 선택 후 “Execute” 버튼 클릭



## (4) QXDM 로그 분석 방법 [5/5]

### 6. 결과 화면 클립보드 복사한 로그는 텍스트 파일(\*.txt)로 저장 시 나중에 “Open File” 기능으로 다시 불러올 수 있음

The screenshot displays the SIM APDU Analyzer v3.0 interface. At the top, there are buttons for 'Open file', 'Clipboard', and 'Execute'. Below these, a dropdown menu shows 'SIM2' and a status indicator 'Complete'. The main area is divided into two tabs: 'APDU' and 'File System'. The 'APDU' tab is active, showing a list of APDU logs. The logs are organized into columns: index, timestamp, command, and response. The 'File System' tab is also visible, showing a list of files. The interface includes a 'Summary' section on the left and a 'Protocol-Level Analysis' section on the right. The 'Summary' section lists various commands such as 'MANAGE CHANNEL (OPEN)', 'SELECT', 'STORE DATA', and 'MANAGE CHANNEL (CLOSE)'. The 'Protocol-Level Analysis' section shows a detailed view of the APDU logs, including the 'Logical channel number' and 'ISD-R' status. The interface is designed for analyzing APDU logs and providing a detailed summary and analysis of the data.

Copyright 2022, JUSEOK AHN <ajs3013@lguplus.co.kr> all rights reserved.

## (5) Shannon DM 로그 분석 방법 [1/6]

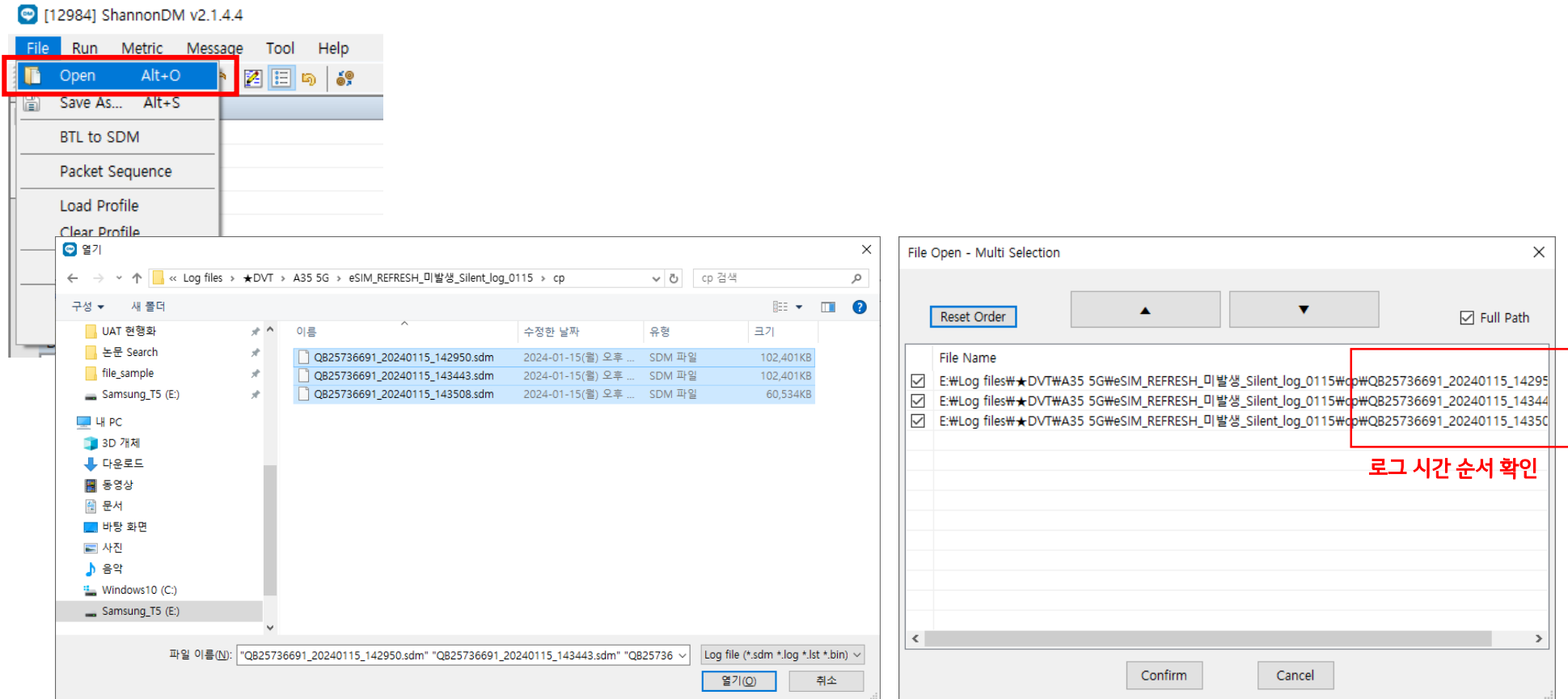
### 1. Shannon DM License 권한 업데이트

APDU 로그 분석을 위해선 DM 권한 업데이트 필요 ※ License 관련 사항은 별도 공유

### 2. Shannon DM 에서 단말 CP 로그 열기

File → Open → 로그 파일 (\*.sdm) 불러오기 (복수 로그 파일의 경우 시간 순 정렬 필수 확인, Reset Order 클릭 후 Confirm 클릭)

※ 단말 제조사 별 CP 로그 확보 방법은 각 제조사 PM 통해 확인 (삼성 silent log dump)

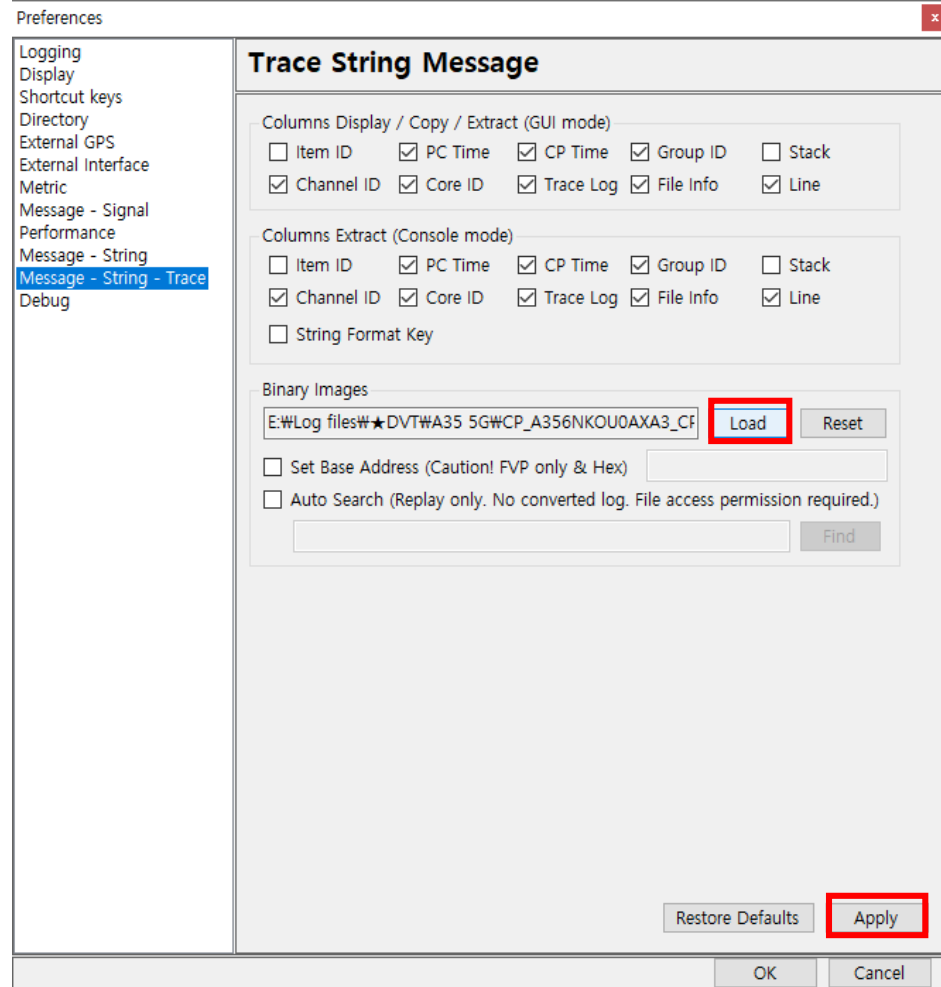
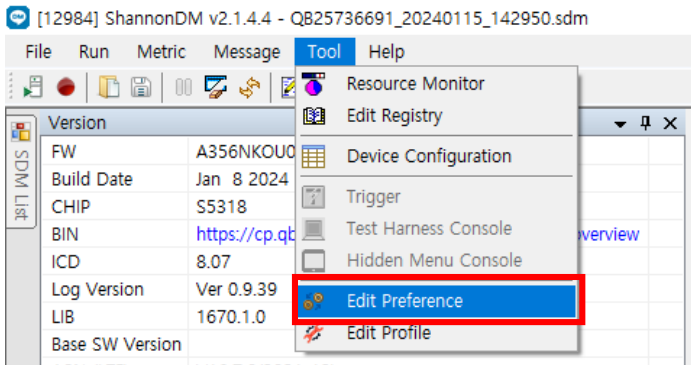
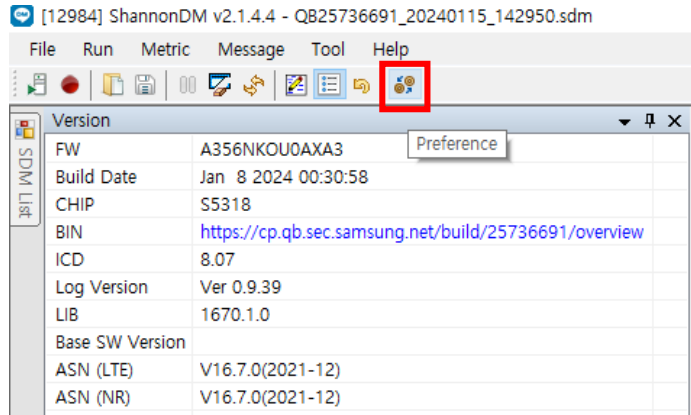




## (5) Shannon DM 로그 분석 방법 [2/6]

### 3. CP 바이너리 매칭

Tool → Edit Preference → “Message – String – Trace” → Binary Images → Load → CP 바이너리(\*.md5) 불러오기 → Apply  
(필수) 단말에 현재 적용된 CP 바이너리



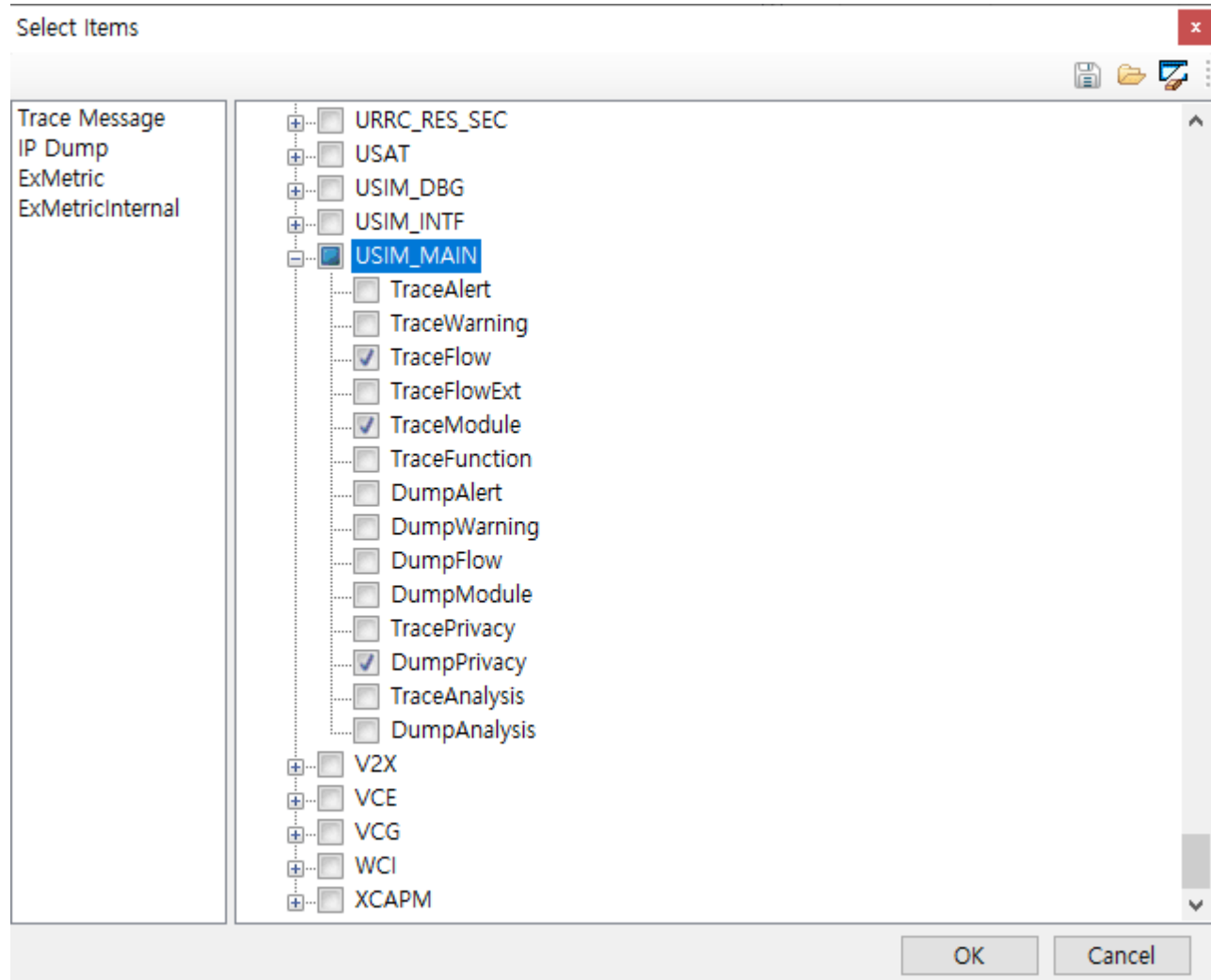
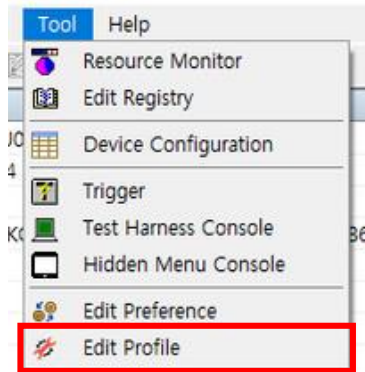
## (5) Shannon DM 로그 분석 방법 [3/6]

### 4. Edit Profile 적용

Tool → Edit Profile → Trace Message → USIM\_MAIN → 'TraceFlow', 'TraceModule', 'DumpPrivacy' 체크

※ APDU 분석에 필요한 최소 항목

→ 아이템 선택이 많아질수록 Trace 창 로드 심해지는 현상 있음



# (5) Shannon DM 로그 분석 방법 [4/6]

## 5. Trace 메시지 확인

Message → Trace → Trace Window 생성 및 SIM APDU 로그 출력 확인 (raw data)

The screenshot displays the ShannonDM v2.1.4.4 interface. The main window is titled "Signalng (0)" and "Trace (0)". The "Trace (0)" window is active, showing a list of trace events. The "Data" panel on the left shows various metrics and values. The "Basic" panel at the bottom shows basic device information.

**Trace (0) Data:**

PC Time	CP Time	Group	Channel	Core ID	Message	File	Line
14:35:50.030	14:35:59.228398	USIM_MAIN	TraceFlow	U0	[USIM_0] [UICC APDU RSP]Received the Following From the Device[UsimRxBuff->payload(1 usim_DeviceIntfM 921	usim_DeviceIntfM	921
14:35:50.030	14:35:59.228429	USIM_MAIN	DumpPrivacy	U0	[USIM_0] [UICC APDU RSP] Hex Dump -> : 62 37 82 02 78 21 83 02 3F 00 A5 11 80 01 C usim_Uilities.c (./ 5931	usim_Uilities.c	5931
14:35:50.030	14:35:59.228429	USIM_MAIN	DumpPrivacy	U0	[USIM_0] [UICC APDU RSP] Hex Dump -> : 01 05 88 03 2F 06 02 C6 12 90 01 78 83 01 C usim_Uilities.c (./ 5931	usim_Uilities.c	5931
14:35:50.030	14:35:59.228429	USIM_MAIN	TraceFlow	U0	[USIM_0] Payload Length 0x39	usim_DeviceIntfM	923
14:35:50.030	14:35:59.228429	USIM_MAIN	TraceModule	U0	[USIM_0] SW1: 0x90 SW2: 0x00	usim_DeviceIntfM	942
14:35:50.030	14:35:59.228429	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 5 result 0 Caller: [./././PSS/StackService/USIM/Code/Src usim_main.c (./ 9945	usim_main.c	9945
14:35:50.030	14:35:59.228429	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 16 result 0 Caller: [./././PSS/StackService/USIM/USIM_P usim_main.c (./ 9945	usim_main.c	9945
14:35:50.030	14:35:59.228429	USIM_MAIN	TraceFunction	U0	[USIM_0] [USIM-SM] <==> usim_ExitCriticalSection- eventType: MEP_LSI_SWITCHING	usim_main.c	12131
14:35:50.030	14:35:59.228490	USIM_MAIN	TraceModule	U0	[USIM_0] [USIM-SM] usim_ExitCriticalSection - Not in critical section. Do nothing.: NONE	usim_main.c	12172
14:35:50.030	14:35:59.228490	USIM_MAIN	DumpModule	U0	[USIM_0] Device Status Word -> : NORMAL_ENDING	usim_DeviceIntfM	9548
14:35:50.030	14:35:59.228490	USIM_MAIN	TraceModule	U0	[USIM_0] USIM Device Write Loop Count -> 1	usim_DeviceIntfM	8065
14:35:50.030	14:35:59.228490	USIM_MAIN	TraceFunction	U0	[USIM_0] No match found in CT/KOR Iccid table	usim_main.c	7615
14:35:50.030	14:35:59.228490	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Operator :FlagIndex 0 result 1 Caller: [./././PSS/StackService/USIM/USIM_PA usim_main.c (./ 9409	usim_main.c	9409
14:35:50.030	14:35:59.228490	USIM_MAIN	TraceModule	U0	[USIM_0] usim_Check_eSIM = 1	usim_PalIntfMana	2561
14:35:50.030	14:35:59.228490	USIM_MAIN	TraceFunction	U0	[USIM_0] << SendAndWaitForResponseFromDevice	usim_DeviceIntfM	8115
14:35:50.030	14:35:59.228490	USIM_MAIN	DumpModule	U0	[USIM_0] Device Interface Result Caller: [./././PSS/StackService/USIM/USIM_PAL/Code/Src usim_Uilities.c (./ 6527	usim_Uilities.c	6527
14:35:50.030	14:35:59.228490	USIM_MAIN	TraceFunction	U0	[USIM_0] >> CheckMandatoryTlvs	usim_Uilities.c	3519
14:35:50.030	14:35:59.228520	USIM_MAIN	TraceWarning	U0	[USIM_0] PropInfoTag = 0x80	usim_Uilities.c	3201
14:35:50.030	14:35:59.228520	USIM_MAIN	TraceWarning	U0	[USIM_0] Length = 0x1	usim_Uilities.c	3213
14:35:50.030	14:35:59.228520	USIM_MAIN	TraceWarning	U0	[USIM_0] Index = 0x3	usim_Uilities.c	3218
14:35:50.030	14:35:59.228520	USIM_MAIN	TraceWarning	U0	[USIM_0] PropInfoTag = 0x83	usim_Uilities.c	3201
14:35:50.030	14:35:59.228520	USIM_MAIN	TraceWarning	U0	[USIM_0] Length = 0x3	usim_Uilities.c	3213
14:35:50.030	14:35:59.228520	USIM_MAIN	TraceWarning	U0	[USIM_0] Index = 0x8	usim_Uilities.c	3218
14:35:50.030	14:35:59.228520	USIM_MAIN	TraceWarning	U0	[USIM_0] PropInfoTag = 0x87	usim_Uilities.c	3201
14:35:50.030	14:35:59.228520	USIM_MAIN	TraceModule	U0	[USIM_0] usim_TerminalCapa :0x1	usim_Uilities.c	4383
14:35:50.030	14:35:59.228520	USIM_MAIN	TraceWarning	U0	[USIM_0] usim_PowerSavingEnabled : 1, Result : 1	usim_main.c	6377
14:35:50.030	14:35:59.228551	USIM_MAIN	TraceFunction	U0	[USIM_0] usim_GetCsimAccessState 0 received, CDMA Access Over, stop the clock	usim_main.c	723
14:35:50.030	14:35:59.228551	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 37 result 1 Caller: [./././PSS/StackService/USIM/Code/S usim_main.c (./ 9945	usim_main.c	9945
14:35:50.030	14:35:59.228551	USIM_MAIN	TraceWarning	U0	[USIM_0] usim_PowerSavingEnabled : 1, Result : 1	usim_main.c	6377
14:35:50.030	14:35:59.228551	USIM_MAIN	TraceFunction	U0	[USIM_0] [USIM-SM] ==> usim_EnterCriticalSection- eventType: MEP_LSI_SWITCHING	usim_main.c	11945
14:35:50.030	14:35:59.228551	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 37 result 1 Caller: [./././PSS/StackService/USIM/Code/S usim_main.c (./ 9945	usim_main.c	9945
14:35:50.030	14:35:59.228551	USIM_MAIN	TraceFunction	U0	[USIM_0] [USIM-SM] usim_EnterCriticalSection : Not in MEP mode. Do nothing.	usim_main.c	12061
14:35:50.030	14:35:59.228551	USIM_MAIN	TraceFunction	U0	[USIM_0] Request for Clock Stop: 1	usim_main.c	599
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] Switching Off SIM clock.	usim_main.c	603
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] >> StopSimClock	usim_DeviceIntfM	8935
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 18 result 1 Caller: [./././PSS/StackService/USIM/USIM_P usim_main.c (./ 9945	usim_main.c	9945
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 37 result 1 Caller: [./././PSS/StackService/USIM/USIM_P usim_main.c (./ 9945	usim_main.c	9945
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceModule	U0	[USIM_0] Inside usim_PalDrvSocketReq , NAD: 0x0 send to SIM card	usim_PalIntfMana	942
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 37 result 1 Caller: [./././PSS/StackService/USIM/USIM_P usim_main.c (./ 9945	usim_main.c	9945
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 37 result 1 Caller: [./././PSS/StackService/USIM/USIM_P usim_main.c (./ 9945	usim_main.c	9945
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 37 result 1 Caller: [./././PSS/StackService/USIM/USIM_P usim_main.c (./ 9945	usim_main.c	9945
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceModule	U0	[USIM_0] NAD: 0x0 received from SIM card	usim_PalIntfMana	990
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 18 result 1 Caller: [./././PSS/StackService/USIM/USIM_P usim_main.c (./ 9945	usim_main.c	9945
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] [USIM-SM] <==> usim_ExitCriticalSection- eventType: MEP_LSI_SWITCHING	usim_main.c	12131
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceModule	U0	[USIM_0] [USIM-SM] usim_ExitCriticalSection - Not in critical section. Do nothing.: NONE	usim_main.c	12172
14:35:50.030	14:35:59.230626	USIM_MAIN	TraceFunction	U0	[USIM_0] ---USIM Flags---	usim_main.c	4617
14:35:50.030	14:35:59.230626	USIM_MAIN	DumpModule	U0	[USIM_0] USIM_SIMCLK_ACTIVATED_FLG-> : FALSE	usim_main.c	6430

**Data Panel:**

Metric	Value
DL TP(Mbps)	0.000
UL TP(Mbps)	0.000
DL BLER(%)	0.00
UL BLER(%)	0.00
DL FER(%)	NA
UL FER(%)	NA

**Basic Panel:**

Metric	Value
RAT	EUTRAN
Modem Status	INITIAL
MIMO Type(P-Cell)	2 x 1
RX Freq(MHz)	2120
TX Freq(MHz)	0
RX Freq2(MHz)	1930
Activated S-Cell	0
MIMO Type(S-Cell[0])	
MIMO Type(S-Cell[1])	
MIMO Type(S-Cell[2])	
MIMO Type(S-Cell[3])	
MIMO Type(S-Cell[4])	
MIMO Type(S-Cell[5])	
MIMO Type(S-Cell[6])	

Free Disk Space : 14,450MB | MODEM | IP | GPS

## (5) Shannon DM 로그 분석 방법 [5/6]

### 6. Trace 메시지 Export

Trace 메시지 전체 선택(Ctrl+A) → 우클릭 Export 선택 → 파일 형식 텍스트 파일(\*.txt)로 지정 후 저장

The screenshot displays the Shannon DM trace analysis interface. The main window shows a list of trace messages with columns for PC Time, CP Time, Group, Channel, Core ID, Message, File, and Line. A right-click context menu is open over the message list, with the 'Export' option highlighted. A secondary window titled '다른 이름으로 저장' (Save with name) is open, showing the file path 'Samsung\_T5 (E) > PycharmProjects > SIM-APDU-Analyzer-for-QXDM > file\_sample'. The file format is set to 'Text file (\*.txt)'. The file list on the right shows various log files, including 'LSI\_QB25736691\_20240115\_142950\_all' and 'ShannonDM\_APDU\_logs'.

PC Time	CP Time	Group	Channel	Core ID	Message	File	Line
14:35:50.030	14:35:59.228398	USIM_MAIN	TraceFlow	U0	[USIM_0] [UICC APDU RSP]Received the Following From the Device[UsimRxBuff->payload(1 usim_DeviceIntfM 921		
14:35:50.030	14:35:59.228398	USIM_MAIN	DumpPrivacy	U0	[USIM_0] [UICC APDU RSP] Hex Dump -> : 62 37 82 02 78 21 83 02 3F 00 A5 11 80 01 C usim_Utility.c (./ 5931		
14:35:50.030	14:35:59.228429	USIM_MAIN	DumpPrivacy	U0	[USIM_0] [UICC APDU RSP] Hex Dump -> : 01 05 88 03 2F 06 02 C6 12 90 01 78 83 01 C usim_Utility.c (./ 5931		
14:35:50.030	14:35:59.228429	USIM_MAIN	TraceFlow	U0	[USIM_0] Payload Length 0x39	usim_DeviceIntfM 923	
14:35:50.030	14:35:59.228429	USIM_MAIN	TraceModule	U0	[USIM_0] SW1: 0x90 SW2: 0x00	usim_DeviceIntfM 942	
14:35:50.030	14:35:59.228429	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 5 result 0 Caller[ ././PSS/StackService/USIM/Code/Src usim_main.c (./ 9945		
14:35:50.030	14:35:59.228429	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 16 result 0 Caller[ ././PSS/StackService/USIM/USIM_P usim_main.c (./ 9945		
14:35:50.030	14:35:59.228429	USIM_MAIN	TraceFunction	U0	[USIM_0] [USIM-SM] <==> usim_ExitCriticalSection- eventType: MEP_LSI_SWITCHING	usim_main.c (./ 12131	
14:35:50.030	14:35:59.228490	USIM_MAIN	TraceModule	U0	[USIM_0] [USIM-SM] usim_ExitCriticalSection - Not in critical section. Do nothing: NONE	usim_main.c (./ 12172	
14:35:50.030	14:35:59.228490	USIM_MAIN	DumpModule	U0	[USIM_0] Device Status Word -> : NORMAL_ENDING	usim_DeviceIntfM 9548	
14:35:50.030	14:35:59.228490	USIM_MAIN	TraceModule	U0	[USIM_0] USIM Device Write Loop Count -> 1	usim_DeviceIntfM 8065	
14:35:50.030	14:35:59.228490	USIM_MAIN	TraceFunction	U0	[USIM_0] No match found in CT/KOR		
14:35:50.030	14:35:59.228490	USIM_MAIN	TraceFunction	U0	[USIM_0] PropInfoTag = 0x87		
14:35:50.030	14:35:59.228520	USIM_MAIN	TraceWarning	U0	[USIM_0] usim_TerminalCapa : 0x1		
14:35:50.030	14:35:59.228520	USIM_MAIN	TraceWarning	U0	[USIM_0] usim_PowerSavingEnabled		
14:35:50.030	14:35:59.228551	USIM_MAIN	TraceFunction	U0	[USIM_0] usim_GetCsimAccessState 0		
14:35:50.030	14:35:59.228551	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 37 r		
14:35:50.030	14:35:59.228551	USIM_MAIN	TraceWarning	U0	[USIM_0] usim_PowerSavingEnabled		
14:35:50.030	14:35:59.228551	USIM_MAIN	TraceFunction	U0	[USIM_0] [USIM-SM] usim_EnterCriti		
14:35:50.030	14:35:59.228551	USIM_MAIN	TraceFunction	U0	[USIM_0] Request for Clock Stop: 1		
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] Switching Off SIM clock.		
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] >> StopSimClock		
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 18 r		
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 37 r		
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceModule	U0	[USIM_0] Inside usim_PalDnsSocketRe		
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 37 r		
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceModule	U0	[USIM_0] NAD: 0x0 received from SIM		
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] Get Function :FlagIndex 18 r		
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceFunction	U0	[USIM_0] [USIM-SM] <==> usim_ExitCriticalSection- eventType: MEP_LSI_SWITCHING	usim_main.c (./ 12131	
14:35:50.030	14:35:59.230595	USIM_MAIN	TraceModule	U0	[USIM_0] [USIM-SM] usim_ExitCriticalSection - Not in critical section. Do nothing: NONE	usim_main.c (./ 12172	
14:35:50.030	14:35:59.230626	USIM_MAIN	TraceFunction	U0	[USIM_0] ---USIM Flags---	usim_main.c (./ 4617	
14:35:50.030	14:35:59.230626	USIM_MAIN	DumpModule	U0	[USIM_0] USIM_SIMCLK_ACTIVATED_FLG-> : FALSE	usim_main.c (./ 6430	

Free Disk Space : 14,407MB | MODEM | IP | GPS

# (5) Shannon DM 로그 분석 방법 [6/6]

## 7. 결과 화면

SIM APDU Analyzer (v3.1 이상) 에서 “Open file” 버튼 클릭해 6번에서 저장한 텍스트 파일 불러오기

Open fileClipboardAPDU logs included in <E:/PycharmProjects/SIM-APDU-Analyzer-for-QXDM/file\_sample/LSI\_QB25736691\_20240115\_142950\_all.txt>

SIM1ExecuteComplete

APDUFile System

Summary

[652] 14:34:45.658 SELECT | SMSS

[653] 14:34:45.682 SELECT | SMSS

[654] 14:34:53.520 SELECT | MF

[655] 14:34:53.536 ENVELOPE (SMS-PP Download) |

[656] 14:34:54.002 ENVELOPE (SMS-PP Download) |

[657] 14:34:54.299 FETCH (OPEN CHANNEL) |

[658] 14:34:54.345 TERMINAL RESPONSE (OPEN CHANNEL) |

[659] 14:34:54.383 FETCH (SEND DATA) |

[660] 14:34:54.395 TERMINAL RESPONSE (SEND DATA) |

[661] 14:34:54.416 FETCH (TIMER MANAGEMENT) |

[662] 14:34:54.425 TERMINAL RESPONSE (TIMER MANAGEMENT) |

[663] 14:34:54.444 ENVELOPE (Event Download) | Data available

[664] 14:34:54.468 FETCH (RECEIVE DATA) |

[665] 14:34:54.477 TERMINAL RESPONSE (RECEIVE DATA) |

[666] 14:34:54.670 FETCH (SEND DATA) |

[667] 14:34:54.688 TERMINAL RESPONSE (SEND DATA) |

[668] 14:34:54.710 FETCH (TIMER MANAGEMENT) |

[669] 14:34:54.719 TERMINAL RESPONSE (TIMER MANAGEMENT) |

[670] 14:34:54.739 ENVELOPE (Event Download) | Data available

[671] 14:34:54.763 FETCH (RECEIVE DATA) |

[672] 14:34:54.773 TERMINAL RESPONSE (RECEIVE DATA) |

[673] 14:34:54.890 FETCH (SEND DATA) |

[674] 14:34:54.911 TERMINAL RESPONSE (SEND DATA) |

[675] 14:34:54.936 FETCH (TIMER MANAGEMENT) |

[676] 14:34:54.945 TERMINAL RESPONSE (TIMER MANAGEMENT) |

[677] 14:34:54.965 ENVELOPE (Event Download) | Data available

[678] 14:34:54.989 FETCH (RECEIVE DATA) |

[679] 14:34:54.997 TERMINAL RESPONSE (RECEIVE DATA) |

[680] 14:34:55.044 FETCH (RECEIVE DATA) |

[681] 14:34:55.053 TERMINAL RESPONSE (RECEIVE DATA) |

[682] 14:34:55.171 FETCH (TIMER MANAGEMENT) |

[683] 14:34:55.178 ENVELOPE (Event Download) | Data available

[684] 14:34:55.208 TERMINAL RESPONSE (TIMER MANAGEMENT) |

[685] 14:34:55.241 FETCH (RECEIVE DATA) |

[686] 14:34:55.250 TERMINAL RESPONSE (RECEIVE DATA) |

[687] 14:34:55.296 FETCH (RECEIVE DATA) |

[688] 14:34:55.304 TERMINAL RESPONSE (RECEIVE DATA) |

[689] 14:34:55.352 FETCH (RECEIVE DATA) |

[690] 14:34:55.361 TERMINAL RESPONSE (RECEIVE DATA) |

[691] 14:34:55.911 FETCH (SEND DATA) |

[692] 14:34:55.932 TERMINAL RESPONSE (SEND DATA) |

[693] 14:34:55.953 FETCH (SEND DATA) |

[694] 14:34:55.971 TERMINAL RESPONSE (SEND DATA) |

[695] 14:34:55.993 FETCH (TIMER MANAGEMENT) |

[696] 14:34:56.001 TERMINAL RESPONSE (TIMER MANAGEMENT) |

[697] 14:34:56.067 ENVELOPE (Event Download) | Data available

[698] 14:34:56.091 FETCH (RECEIVE DATA) |

Open fileClipboardAPDU logs included in <E:/PycharmProjects/SIM-APDU-Analyzer-for-QXDM/file\_sample/LSI\_QB25736691\_20240115\_142950\_all.txt>

SIM1ExecuteComplete

APDUFile System

DF	File	DF_Id	File_Id	Type	SFI	REC#	OPS	LEN	ref
MF	DIR	3F00	2F00	LF	1E	01	-	32	[749]
MF	DIR	3F00	2F00	LF	1E	02	-	32	[750]
MF	PL	3F00	2F05	TF	-	-	00	14	[234]
MF	ICCID	3F00	2FE2	TF	-	-	00	0A	[232]
ADF USIM	Unknown EF AID	2F30	TF	-	-	00	0C	[495]	
ADF USIM	Unknown EF AID	4F06	TF	-	-	00	04	[356]	
ADF USIM	Unknown EF AID	4F08	LF	-	01	-	0A	[358]	
ADF USIM	Unknown EF AID	4F0A	TF	-	-	00	04	[360]	
ADF USIM	Unknown EF AID	4F0A	TF	-	-	00	04	[868]	
ADF USIM	Unknown EF AID	4F20	TF	-	-	00	09	[321]	
ADF USIM	Unknown EF AID	4F20	TF	-	-	00	09	[807]	
ADF USIM	Unknown EF AID	4F52	TF	-	-	00	09	[323]	
ADF USIM	Unknown EF AID	4F52	TF	-	-	00	09	[809]	
ADF USIM	Unknown EF AID	4F63	TF	-	-	00	14	[325]	
ADF USIM	Unknown EF AID	4F64	TF	-	-	00	01	[319]	
ADF USIM	LI	AID	6F05	TF	02	-	00	14	[845]
ADF USIM	IMSI	AID	6F07	TF	07	-	00	09	[382]
ADF USIM	IMSI	AID	6F07	TF	07	-	00	09	[781]
ADF USIM	Keys	AID	6F08	TF	08	-	00	21	[894]
ADF USIM	Keys	AID	6F08	TF	-	-	00	21	[306]
ADF USIM	KeysFS	AID	6F09	TF	09	-	00	21	[895]
ADF USIM	KeysFS	AID	6F09	TF	-	-	00	21	[308]
ADF USIM	HPLMN	AID	6F31	TF	-	-	00	01	[290]
ADF USIM	ACHmax	AID	6F37	TF	-	-	00	03	[405]
ADF USIM	UST	AID	6F38	TF	-	-	00	14	[280]
ADF USIM	MSISDN	AID	6F40	LF	-	01	-	1E	[349]
ADF USIM	MSISDN	AID	6F40	LF	-	01	-	1E	[857]
ADF USIM	MSISDN	AID	6F40	LF	-	02	-	1E	[350]
ADF USIM	MSISDN	AID	6F40	LF	-	03	-	1E	[351]
ADF USIM	SMSF	AID	6F42	LF	-	01	-	2C	[415]
ADF USIM	SMSF	AID	6F43	TF	-	-	00	02	[334]
ADF USIM	CBMI	AID	6F45	TF	-	-	00	32	[410]
ADF USIM	SPN	AID	6F46	TF	-	-	00	11	[338]
ADF USIM	CBMID	AID	6F48	TF	-	-	00	10	[316]
ADF USIM	CBMIR	AID	6F50	TF	-	-	00	10	[412]
ADF USIM	EST	AID	6F56	TF	-	-	00	0C	[282]
ADF USIM	ACL	AID	6F57	TF	-	-	00	FF	[284]
ADF USIM	START-HFN	AID	6F5B	TF	-	-	00	06	[312]
ADF USIM	THRESHOLD	AID	6F5C	TF	-	-	00	03	[314]
ADF USIM	PLMNWAcT	AID	6F60	TF	-	-	00	64	[296]
ADF USIM	OPLMNWAcT	AID	6F61	TF	-	-	00	00	[288]
ADF USIM	OPLMNWAcT	AID	6F61	TF	-	-	00	F4	[299]
ADF USIM	HPLMNWAcT	AID	6F62	TF	-	-	00	32	[292]
ADF USIM	PSLOCI	AID	6F73	TF	0C	-	00	0E	[893]
ADF USIM	ACC	AID	6F78	TF	-	-	00	02	[288]
ADF USIM	ACC	AID	6F78	TF	-	-	00	02	[774]
ADF USIM	FPLMN	AID	6F7B	TF	-	-	00	3C	[310]

File Contents

98FF9CFE7FE5F0040C30004000007801000000

File Contents Parsing

[X] Service n1 Local Phone Book

[X] Service n2 Fixed Dialling Numbers (FDN)

[X] Service n3 Extension 2

[O] Service n4 Service Dialling Numbers (SDN)

[O] Service n5 Extension3

[X] Service n6 Barred Dialling Numbers (BDN)

[X] Service n7 Extension4

[O] Service n8 Outgoing Call Information (OCI and OCT)

[O] Service n9 Incoming Call Information (ICI and ICT)

[O] Service n10 Short Message Storage (SMS)

[O] Service n11 Short Message Status Reports (SMSR)

[O] Service n12 Short Message Service Parameters (SMSF)

[O] Service n13 Advice of Charge (AoC)

[O] Service n14 Capability Configuration Parameters 2 (CCP2)

[O] Service n15 Cell Broadcast Message Identifier

[O] Service n16 Cell Broadcast Message Identifier Ranges

[X] Service n17 Group Identifier Level 1

[X] Service n18 Group Identifier Level 2

[O] Service n19 Service Provider Name

[O] Service n20 User controlled PLMN selector with Access Technology

[O] Service n21 MSISDN

[X] Service n22 Image (IMG)

[X] Service n23 Support of Localised Service Areas (SoLSA)

[O] Service n24 Enhanced Multi Level Precedence and Pre-emption Service

[O] Service n25 Automatic Answer for eMLPP

[O] Service n26 RFU

[O] Service n27 GSM Access

[O] Service n28 Data download via SMS-PP

[O] Service n29 Data download via SMS CB

[O] Service n30 Call Control by USIM

[O] Service n31 MO-SMS Control by USIM

[O] Service n32 RUN AT COMMAND command

[O] Service n33 shall be set to '1'

[O] Service n34 Enabled Services Table

[O] Service n35 APN Control List (ACL)

[X] Service n36 Depersonalisation Control Keys

[X] Service n37 Co-operative Network List

Copyright 2022, JUSEOK AHN <ajs3013@iguplus.co.kr> all rights reserved.

Copyright 2022, JUSEOK AHN <ajs3013@iguplus.co.kr> all rights reserved.



# 개발 배경

## ❖ eSIM 은 단말 내부에 장착되어 있어 USIM 에 사용 중인 분석 Tool 활용이 불가함

- 단말과 SIM간의 통신은 APDU (Application Protocol Data Unit) 구조를 사용하며, Byte로 구성된 값의 의미를 Decoding 해주는 분석 Tool이 필요함  
Ex. SIM에 저장된 파일 값 Read, LTE/5G 인증 로그, OTA 개통 로그 등을 분석



단말에 물리적인 케이블 연결하는 방식

#	Command	Field	Value
49	SELECT (UST)	Command:	SELECT
50	READ BINARY (Offset 0, Len 12)	Status:	Normal ending of command.
51	SELECT (EST)	Current DF:	USIM Application Directory (3F00.7FFF)
52	READ BINARY (Offset 0, Len 12)	Current EF:	USIM Service Table (6F38)
53	READ BINARY (5F1:07, IMSI, Offset 0, Len 9)	Time:	134.341 s
54	SELECT (7FFF.7F66.5F30.4F34)	P1:	Select by File ID
55	SELECT (CBMID)	P2:	Return FCP
56	READ BINARY (Offset 0, Len 16)	Logical Channel:	00
57	SELECT (NETPAR)	Secure Messaging Indicate:	No SM used between terminal and card
58	READ BINARY (Offset 0, Len 255)		

#	Sequence	Dir	Description	Value	Delay	Meaning
52	APDU		Header [CLA INS P1 P2]	00 A4 00 04	273.56 etu	SELECT
			Incoming data	6F 38		
			Outgoing data	62 17 82 02 41 21 83 02 6F 38 8A 01 05 8B 03 6F	41.38 etu	
			Return code [SW1 SW2]	06 04 80 02 00 0C 88 01 20		
				90 00		

## ➤ 단말 모뎀 로그 기반의 단말과 SIM 간의 APDU 통신 로그 분석 Tool 개발

- 현재 퀄컴과 COMPRION 양사 간 Tool 호환성 제공을 위한 개발 검토 계약을 진행 중이나 올해 9월 이내에 상용 솔루션 제공은 불가할 것으로 예상됨  
eSIM 상용화 전까지 퀄컴 모뎀 로그 기반의 분석 Tool 자체 개발 계획을 수립함

- eSIM 단말은 USIM, eSIM 과 동시에 통신 가능하여 2개 Path의 로그가 단말 모뎀 로그에 함께 남음 → Path 별 로그 구분하여 별도 분석 필요
- 퀄컴 모뎀 로그는 APDU Decoding 범위가 제한적임 → eSIM 단말 DVT에 필요한 필수 값을 표준 기반으로 Decoding하는 기능 제공

2022 Mar 13 22:35:41.890	UIM APDU	
2022 Mar 13 22:35:41.899	UIM APDU	
2022 Mar 13 22:35:41.899	UIM APDU	
2022 Mar 13 22:35:41.903	UIM APDU	
2022 Mar 13 22:35:41.903	UIM APDU	
2022 Mar 13 22:35:41.908	UIM APDU	
2022 Mar 13 22:35:41.908	UIM APDU	
2022 Mar 13 22:35:41.913	UIM APDU	
2022 Mar 13 22:35:41.913	UIM APDU	
2022 Mar 13 22:35:41.928	UIM APDU	
2022 Mar 13 22:35:41.929	UIM APDU	
2022 Mar 13 22:35:41.935	UIM APDU	
2022 Mar 13 22:35:41.936	UIM APDU	
2022 Mar 13 22:35:41.942	UIM APDU	
2022 Mar 13 22:35:41.943	UIM APDU	
2022 Mar 13 22:35:41.950	UIM APDU	
2022 Mar 13 22:35:41.950	UIM APDU	
2022 Mar 13 22:35:41.957	UIM APDU	

APDU Parsing 결과 보여주기

2022 Mar 13 22:35:41.875 [15] 0x19B7 UIM APDU	
Subscription ID = 1	
Version = 1	
Sequence Number = 188	
Slot Id = SLOT_1	
Message Type = RX	
Control byte = 0	
RX Data = { B0 98 FF 9C FF E7 FE 5F 00 40 C3 00 04 90 00 }	
APDU Parsing	
Transaction Start : 2022/03/13 22:35:41.866	
slot value:1	
READ BINARY	
Logical Channel: 0	
UICC instruction class	
CLA - No SM used between terminal and card	
Offset: 0x00	
Bytes Read: { 0x98 0xFF 0x9C 0xFF 0xE7 0xFE 0x5F 0x00 0x40 0xC3 0x00 0x04 }	
Status Words - 0x90 0x00 - Normal ending of the command	
Length: 39	
Header: 27 00 B7 19 15 BF 5B 41 C3 F6 F7 00	
Payload: 01 BC 00 01 05 00 00 00 00 0F 00	
04 90 00	

Bytes 값에 대한 Decoding 추가