



# Automobile Hacking

## Telematics Unit SMS Hacking

[mongii@grayhash](mailto:mongii@grayhash)

# Summary

- SMS의 PDU 포맷 이해하기
- AT 커맨드로 SMS 보내보기
- 실제 SMS 공격 사례 분석
- Android Telephony Stack 분석
- SMS FUZZING

# It's possible to remote attack



# 왜 차량에 모뎀이?

- <http://news.kotra.or.kr/user/globalAllBbs/kotranews/album/2/globalBbsDataAllView.do?dataIdx=91740>

## EU, 자동차 교통사고 자동통보시스템 장착 의무화

2009-08-24 김선화 벨기에 브뤼셀무역관

EU, 신규차에 교통사고 자동통보시스템 장착 의무화 방침

- 올해 내 자발시행 안 될 경우 내년부터 법제화 -

□ EU 집행위의 Viviane Reding 정보사회 담당 집행위원은 신규차에 대한 교통사고 자동통보(eCall)시스템 장착이 자동차 산업계나 회원국에 의해 올해 내, 자발적으로 시행되지 않을 경우 더이상 기다릴 수 없고 내년부터 이를 의무화하는 법규를 제정하겠다고 밝힘.

○ 이는 교통사고에 의한 인명피해를 줄이기 위한 것으로 EU 집행위는 해마다 너무 많은 인명이 교통사고로 희생되고 있다고 밝히고, 자동차 산업계나 회원국이 이제는 행동으로 옮겨야 할 때라고 강조함.

□ 이러한 교통사고 자동통보시스템, 소위 'eCall'시스템은 심각한 자동차 사고가 발생했을 때, 센서가 자동적으로 발동해 사고 시간과 장소, 운전방향, 자동차 정보 등을 포함해 긴급상황을 구조대에 신속히 전달하고 음성전화도 자동연결되도록 한다는 것임.

# 국내 사례 - 현대

- <https://www.genesis.com/kr/ko/genesis-membership-connected.html>



원격제어

안전보안

차량 관리

길 안내

컨시어지

365일 24시간 GENESIS CONNECTED SERVICES  
와 함께 안심 운전하세요.

각종 사고와 위급상황에서 운전자를 든든하게 지켜 줍니다.

|             |           |       |
|-------------|-----------|-------|
| 에어백 전개 자동통보 | SOS 긴급출동  | 도난 추적 |
| 도난 경보 알림    | 운전자 주의 알림 |       |

# 국내 사례 - 기아

- [http://uvo.kia.com/uvo/uvo\\_info.html](http://uvo.kia.com/uvo/uvo_info.html)

## 에어백이 터지는 사고 발생 시 긴급 구조 및 사고처리를 지원해 드립니다

사고로 인한 에어백 전개 시, 에어백 전개 신호가 UVO 긴급구난센터에 전송되어 신속하게 차량사고에 대처할 수 있습니다.

### 서비스 소개

- 에어백이 터지는 사고로 에어백 전개 신호 발생시 자동으로 사고를 인식하고 고객을 도와드리는 서비스입니다.
- 에어백이 전개된 후에는 고객이 부상 등으로 전화를 받기 어려운 경우에도 자동으로 전화를 받으실 수 있도록 자동착신 모드로 전환됩니다.
- 차량 내 전화로 고객 연결에 실패하는 경우, 긴급연락처 등 연결 가능한 번호로 재시도하고 통화 실패 시 제휴사를 통해 견인차를 지원합니다.
- 자동 착신 모드는 상담원이 서비스를 종료하거나 시동을 끄면 해제됩니다.

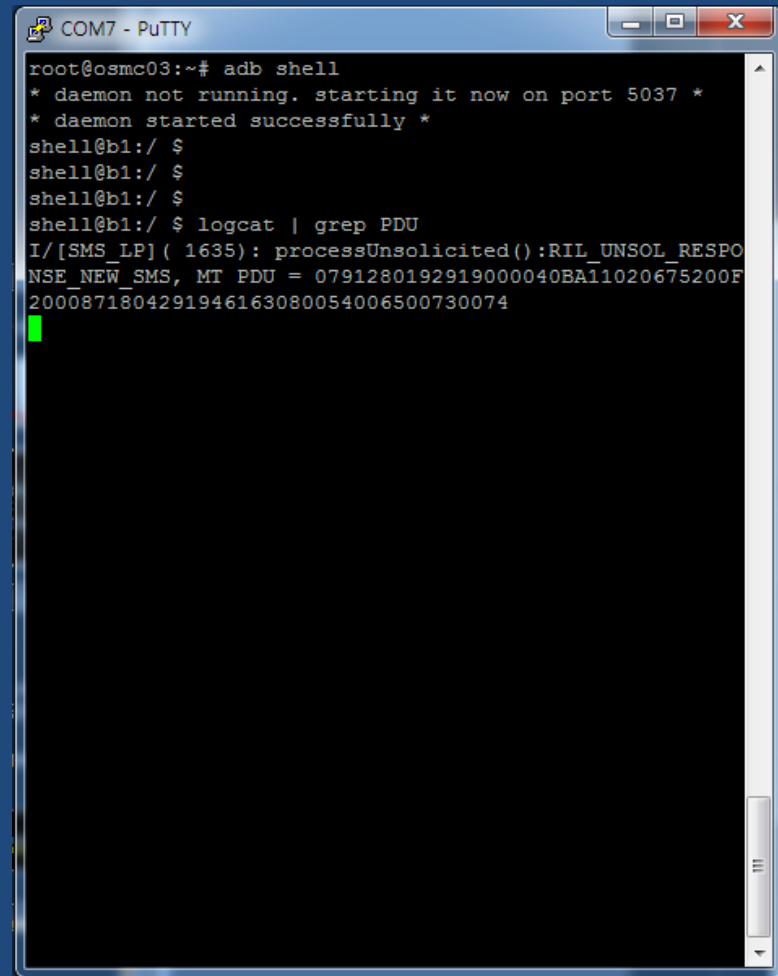
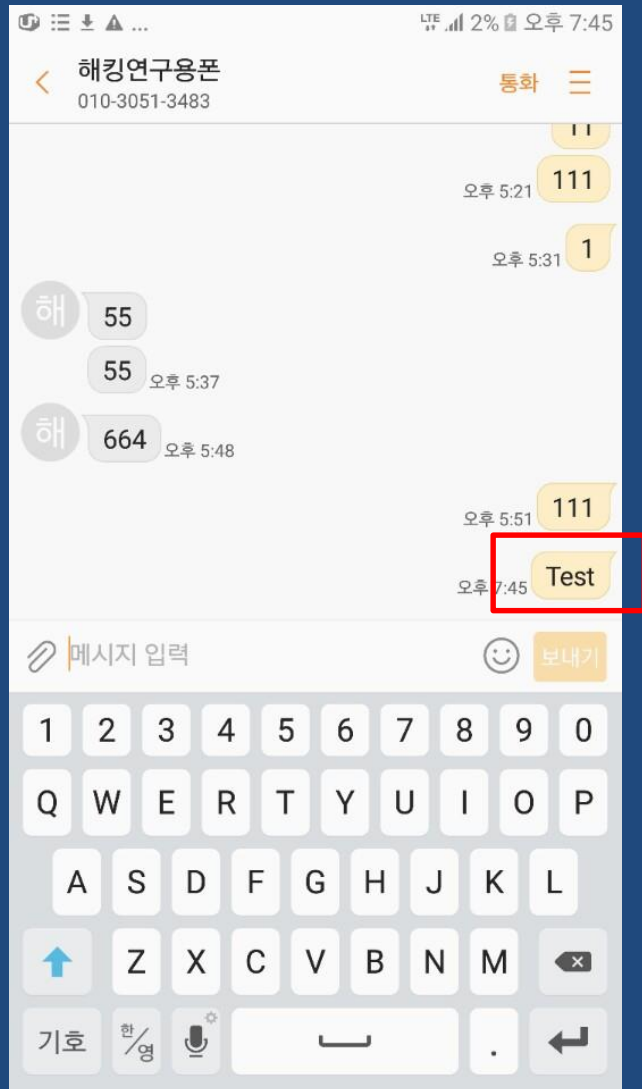


# PDU 포맷의 이해

- 우리가 주고 받는 SMS가 실제로는 PDU라는 이름의 데이터 포맷으로 이루어져 있다.
- PDU = Packet Data Unit
- PDU 데이터 안에는 각종 헤더와 SMS 문자 데이터 등이 포함되어 있다



# 수신 PDU 데이터 확인 예제





# PDU Decoding

- <https://www.diafaan.com/sms-tutorials/gsm-modem-tutorial/online-sms-deliver-pdu-decoder/>
- <http://www.smspdu.com/>

## Online SMS-DELIVER PDU Decoder

The SMS-DELIVER PDU (Packet Data Unit) is the encoded SMS message that is delivered to your GSM phone or modem.

Use this online PDU tool to decode any SMS-DELIVER PDU.

### SMS-DELIVER PDU:

0791280192919000040BA11020675200F20008718022510333630400480069

Decode

### Text message

**From:** 01027625002  
**Message:** Hi

### Additional information

**PDU type:** SMS-DELIVER  
**Time stamp:** 22/08/2017 15:30:33  
**SMSC:** +821029190900  
**Data coding:** Unicode

### Original Encoded PDU fields

**SMSC:** 0791280192919000  
**PDU header:** 04  
**TP-MTI:** 00  
**TP-MMS:** 04  
**TP-SRI:** 00  
**TP-RP:** 00  
**TP-UDHI:** 00  
**TP-OA:** 0BA11020675200F2  
**TP-PID:** 00  
**TP-DCS:** 08  
**TP-SCTS:** 71802251033363  
**TP-UDL:** 04  
**TP-UD:** 00480069

# PDU 포맷 분석하기

- 0791280192919000040BA11020675200F20008718022510333630400480069

| HEX Data       | 필드 의미   | 필드 길이            |
|----------------|---|------------------|
| 07             | SMSC 번호의 길이 : N1                                | 1byte            |
| 91             | 번호의 타입 : 91 == International                    | 1byte            |
| 280192919000   | SMSC 번호 : 821029190900                          | N1-1(type) bytes |
| 04             | PDU Header : SMS_DELIVER                        | 1byte            |
| 0B (11)        | 송신자의 번호 길이 : N2                                 | 1byte            |
| A1             | 송신자 번호의 타입 == Local                             | 1byte            |
| 1020675200F2   | 송신자 번호 : 01027625002                            | N2 bytes         |
| 00             | TP-PID (Protocol Identifier)                    | 1byte            |
| 08             | TP-DCS (Data Encoding Schema) : UNICODE         | 1byte            |
| 71802251033363 | TP-SCTS (Time Stamp) : 17/08/22 15:30:33 36(TZ) | 7bytes           |
| 04             | TP-UDL (User Data Length) : N3                  | 1byte            |
| 00480069       | TP-UD (User Data) : "Hi"                        | N3 bytes         |

# PDU Header 더 자세히 보기

- 04
  - TP-MTI : 00
  - TP-MMS : 1
  - TP-SRI : 0
  - TP-RP : 0
  - TP-UDHI : 0
- TP-MTI
  - 00 : SMS-DELIVER
    - 수신 SMS
  - 01 : SMS-SUBMIT
    - 송신 SMS

The First-Octet field format is as follows:

| TP-RP | TP-UDHI | TP-SRI |   |   | TP-MMS | TP-MTI |   |
|-------|---------|--------|---|---|--------|--------|---|
| 0     | 0       | 0      | 0 | 0 | x      | 0      | 0 |

All the value are given for the most simple case, for more details see the GSM 03.40 (section 9.2.3).

**a) TP-Message-Type-Indicator (TP-MTI)**

In the case of a SMS-DELIVER, the two bits, bit 0 and bit 1, should be set with the values 0 and 0.

**b) TP-More-Messages-to-Send (TP-MMS)**

The TP-More-Messages-to-Send is a 1-bit field, located within bit no 2 of the First-Octet of SMS-DELIVER, and to be given the following values:

| Bit | 2 | Definition   |
|-----|---|--|
| 0   |   | More messages are waiting for the MS in this SC    |
| 1   |   | No more messages are waiting for the MS in this SC |

**c) TP-Status-Report-Indication (TP-SRI)**

For simplified SMS, the PDU does not contain any Status report, also the bit no. 5 of the first octet is given 0.

**d) TP-User-Data-Header-Indicator (TP-UDHI)**

For simplified SMS, the PDU does not contain any Header in addition to the short message, also the bit 6 within the First-Octet is equal to 0.

**e) TP-Reply-Path (TP-RP)**

For simplified SMS, the reply path is not specified. In this case the bit 7 within the First-Octet is equal to 0.

# PDU Header 더 자세히 보기

- 04
  - TP-MTI : 00
  - TP-MMS : 1
  - TP-SRI : 0
  - TP-RP : 0
  - TP-UDHI : 0
- TP-MTI
  - 00 : SMS-DELIVER
    - 수신 SMS
  - 01 : SMS-SUBMIT
    - 송신 SMS

The First-Octet field format is as follows:

| TP-RP | TP-UDHI | TP-SRI |   |   | TP-MMS | TP-MTI |   |
|-------|---------|--------|---|---|--------|--------|---|
| 0     | 0       | 0      | 0 | 0 | x      | 0      | 0 |

All the value are given for the most simple case, for more details see the GSM 03.40 (section 9.2.3).

**a) TP-Message-Type-Indicator (TP-MTI)**

In the case of a SMS-DELIVER, the two bits, bit 0 and bit 1, should be set with the values 0 and 0.

**b) TP-More-Messages-to-Send (TP-MMS)**

The TP-More-Messages-to-Send is a 1-bit field, located within bit no 2 of the First-Octet of SMS-DELIVER, and to be given the following values:

| Bit | 2 | Definition   |
|-----|---|--|
| 0   |   | More messages are waiting for the MS in this SC    |
| 1   |   | No more messages are waiting for the MS in this SC |

**c) TP-Status-Report-Indication (TP-SRI)**

For simplified SMS, the PDU does not contain any Status report, also the bit no. 5 of the first octet is given 0.

**d) TP-User-Data-Header-Indicator (TP-UDHI)**

For simplified SMS, the PDU does not contain any Header in addition to the short message, also the bit 6 within the First-Octet is equal to 0.

**e) TP-Reply-Path (TP-RP)**

For simplified SMS, the reply path is not specified. In this case the bit 7 within the First-Octet is equal to 0.

# PDU로 SMS 보내보기

Online PDU Converter : <http://rednaxela.net/pdu.php>

## Javascript PDU Converter Written by Swen-Peter Ekkebus [in](#)

Updated by [Andrew Alexander](#) [in](#) (v1.5) and Milan Chudik (v1.4)

I am available for work so check out my details on [LinkedIn](#) and [contact me](#).

PDU Format Converter (Encoder/Decoder) for GSM SMS. This release v1.5r9.

PDU SMS message creator

Hexadecimal PDU Message Entry/Display

Resultant 7/8/16 Bit readable PDU Message

SMSC

Receiver

Alphabet Size ☒ 7 ☐ 8 ☐ 16

Message Class

Receipt ☐

Validity (Relative) ☐

test message

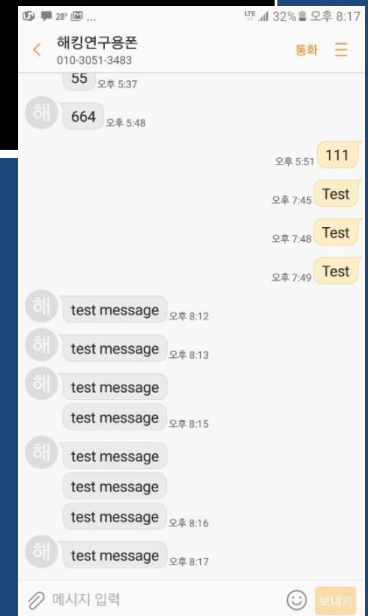
```
AT+CMGS=24
07912801111122220100088
11020675200F200000CF4F2
9C0E6A97E7F3F0B90C
```

[Show User data translation \(7 bit only\)](#)

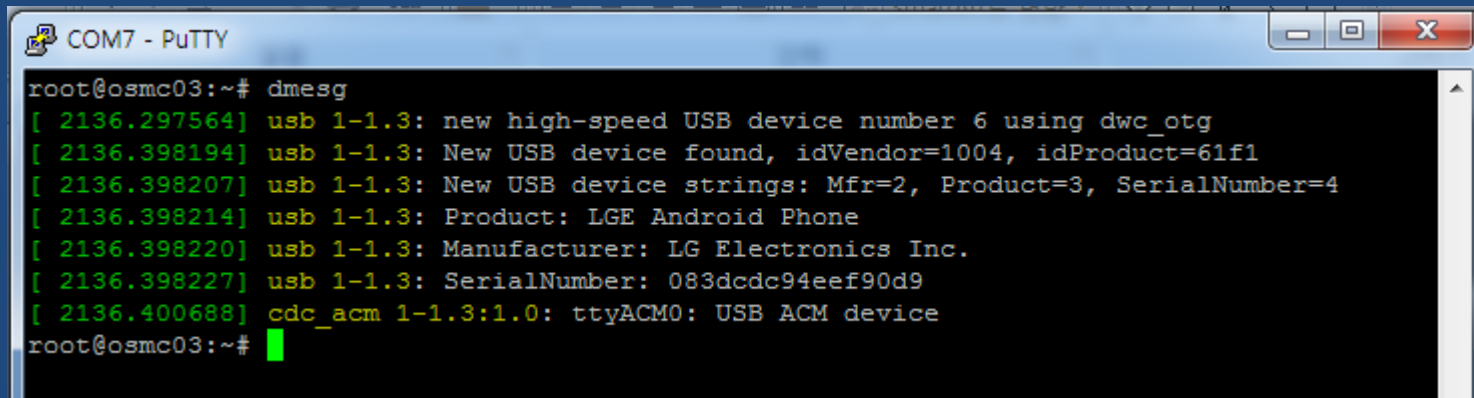
# PDU로 SMS 보내보기

Online PDU Converter : <http://rednaxela.net/pdu.php>

```
cat /dev/smd0 &  
./busybox printf "at+cmgf=0WrWn" > /dev/smd0 // PDU MODE  
./busybox printf "at+cmgs=18WrWn" > /dev/smd0 // Length  
./busybox printf  
"07912801111222201000B811080423429F60004054855583894Wx  
1a" > /dev/smd0
```



# Modem device를 통해 SMS 보내기



```
COM7 - PuTTY
root@osmc03:~# dmesg
[ 2136.297564] usb 1-1.3: new high-speed USB device number 6 using dwc_otg
[ 2136.398194] usb 1-1.3: New USB device found, idVendor=1004, idProduct=61f1
[ 2136.398207] usb 1-1.3: New USB device strings: Mfr=2, Product=3, SerialNumber=4
[ 2136.398214] usb 1-1.3: Product: LGE Android Phone
[ 2136.398220] usb 1-1.3: Manufacturer: LG Electronics Inc.
[ 2136.398227] usb 1-1.3: SerialNumber: 083dc94eef90d9
[ 2136.400688] cdc_acm 1-1.3:1.0: ttyACM0: USB ACM device
root@osmc03:~#
```

```
screen /dev/ttyACM0 115200
```

```
at+cmgf=0
```

```
at+cmgs=24
```

```
07912801111222201000B811020675200F200000CF4F29C0E6A97E
7F3F0B90C[CTRL+Z]
```

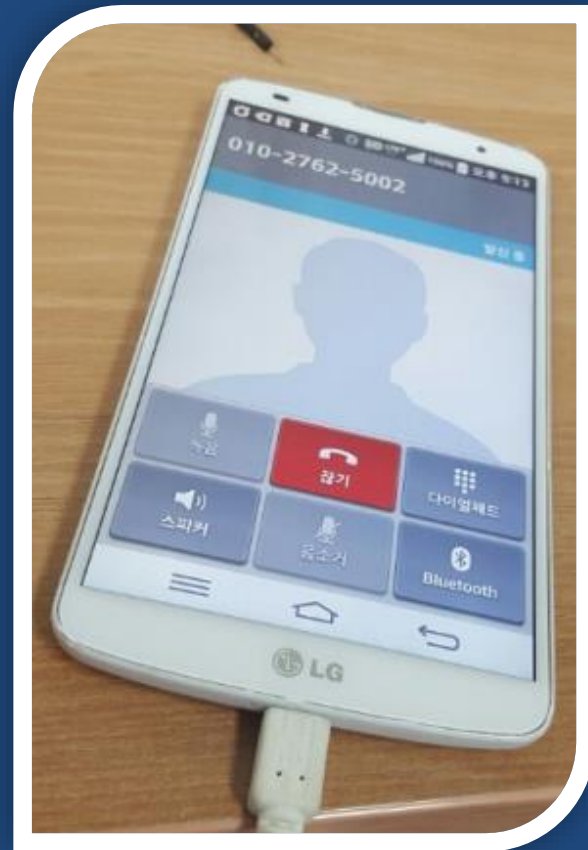
```
+CMGS: 59
```

```
OK
```



# Modem device를 통해 전화 걸기

- ATD01027625002;



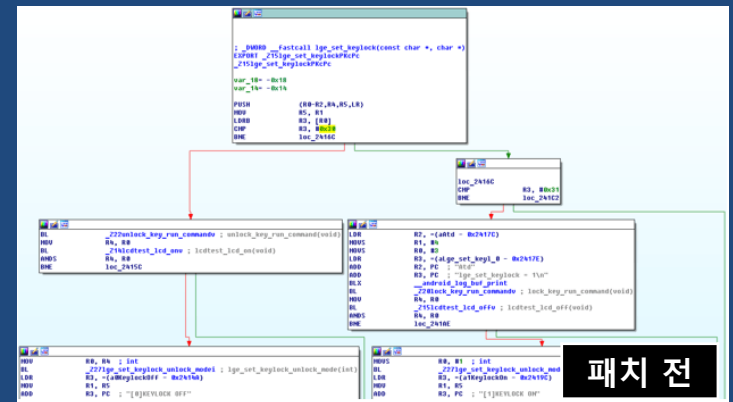
# Modem device를 통해 Lock 풀기

- AT%KEYLOCK=0

| Address          | Length   | Type | String         |
|------------------|----------|------|----------------|
| .rodata:0004E... | 00000007 | C    | AT%AVR         |
| .rodata:0004E... | 00000009 | C    | AT%SIMID       |
| .rodata:0004E... | 00000009 | C    | AT%LGPWD       |
| .rodata:0004E... | 00000009 | C    | AT%CALDT       |
| .rodata:0004E... | 00000008 | C    | AT%LCDINFO     |
| .rodata:0004E... | 00000007 | C    | AT%EMT         |
| .rodata:0004E... | 00000007 | C    | AT%VLC         |
| .rodata:0004E... | 0000000A | C    | AT%MAXCPU      |
| .rodata:0004E... | 00000008 | C    | AT%ULCV        |
| .rodata:0004E... | 0000000A | C    | AT%DIAGNV      |
| .rodata:0004E... | 00000007 | C    | AT%ACS         |
| .rodata:0004E... | 00000009 | C    | AT%VZWHM       |
| .rodata:0004E... | 0000000C | C    | AT%VZWIOTHM    |
| .rodata:0004E... | 00000008 | C    | AT%IMEI        |
| .rodata:0004F... | 0000000C | C    | AT%3WAYSJNC    |
| .rodata:0004F... | 00000008 | C    | AT%KEYLOCK     |
| .rodata:0004F... | 00000009 | C    | AT%LCATT       |
| .rodata:0004F... | 00000008 | C    | AT%SULC        |
| .rodata:0004F... | 00000009 | C    | AT%DBCHK       |
| .rodata:0004F... | 00000008 | C    | AT%GNSS        |
| .rodata:0004F... | 00000009 | C    | AT%GNSS1       |
| .rodata:0004F... | 0000000D | C    | AT%LGANDROID   |
| .rodata:0004F... | 00000008 | C    | AT%VLST        |
| .rodata:0004F... | 00000009 | C    | AT%TSNS        |
| .rodata:0004F... | 0000000D | C    | AT%EMMREJECT   |
| .rodata:0004F... | 0000000A | C    | AT%MDMPVS      |
| .rodata:0004F... | 0000000F | C    | AT%LCIMSSETCFG |
| .rodata:0004F... | 00000007 | C    | AT%CAM         |
| .rodata:0004F... | 0000000A | C    | AT%CHARGE      |
| .rodata:0004F... | 00000008 | C    | AT%GYRO        |
| .rodata:0004F... | 00000008 | C    | AT%SURV        |
| .rodata:0004F... | 00000009 | C    | AT%HWVER       |
| .rodata:0004F... | 00000009 | C    | AT%BATMP       |
| .rodata:0004F... | 00000008 | C    | AT%IMPL        |
| .rodata:0004F... | 0000000E | C    | AT%OSPPWDINIT  |

AT%

```
Pseudocode-A Strings window IDA View-A
int __fastcall sub_37770()
{
    return sub_34CC8("AT%KEYLOCK", (int)sub_3776C);
}
```

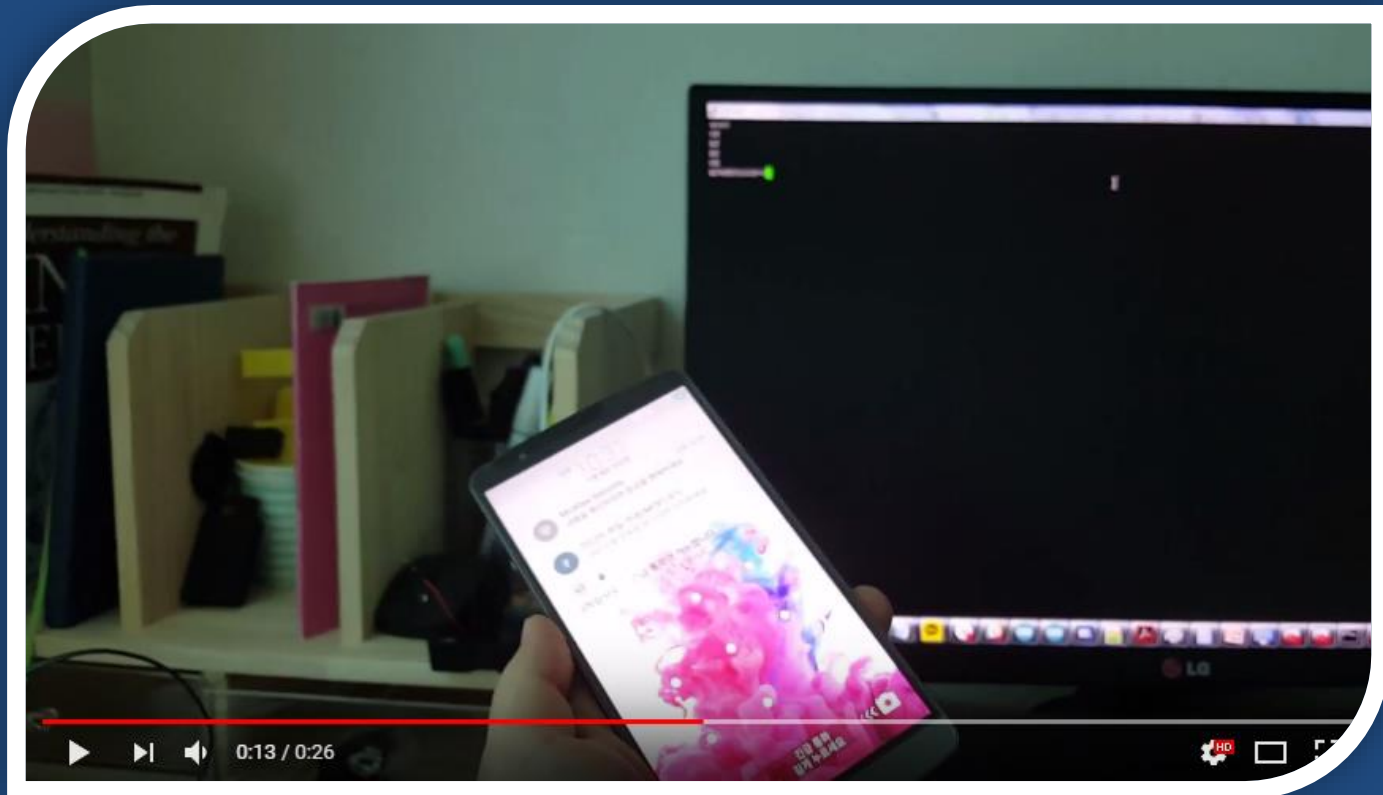


```
Pseudocode-A Strings window
signed int __fastcall sub_3776C()
{
    return 1;
}
```

패치 후

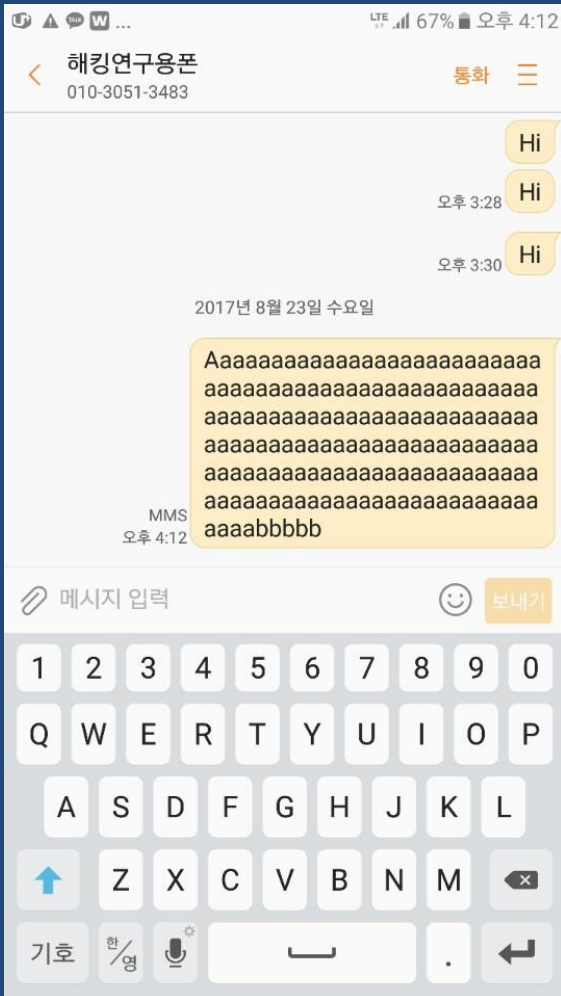
# Modem device를 통해 Lock 풀기

- <https://www.youtube.com/watch?v=O4jKegDiEpM>



# MMS(Multimedia Messaging Service) 보내기

# MMS의 PDU 데이터



- `shell@b1:/ $ logcat | grep PDU`
- `I/[SMS_LP]( 1664):`  
`processUnsolicited():RIL_UNSOL_RESPONSE_NEW_SM`  
`S, MT PDU =`  
`0791280192919000400BA11020675200F200047180326`  
`1211263820B05040B8423F00003770201770622617070`  
`6C696361746966E2F766E642E7761702E6D6D732D6`  
`D65737361676500AF848C829831397748384E4730433`  
`14958443030008D928A808E01A788058103093A80836`  
`87474703A2F2F642D6D6D73632E6B746677696E672E`  
`636F6D3A393038332F31397748384E47304331495844`  
`303000`
- `I/[SMS_LP]( 1664):`  
`processUnsolicited():RIL_UNSOL_RESPONSE_NEW_SM`  
`S, MT PDU =`  
`0791280192919000440BA11020675200F200047180326`  
`12112632E0B05040B8423F00003770202890F800DEA3`  
`03130323736323530303200960FEA416161616161616`  
`16161616100`

# PDU 1/2

Resultcode : 10  
Resultmessage: Success  
Type: SMS-DELIVER  
PDU len: 157 bytes  
Originator: 01027625002  
Message: 0B05040B8423F000037702017706226170706C69636174696F6E2F766E642E7761702E6D6D732D6D65737361676500AF848C829831397748384E473043314958443030008D928A808E01A788058103093A8083687474703A2F2F642D6D6D73632E6B746677696E672E636F6D3A393038332F31397748384E47304331495844303000  
Timestamp: 23/08/2017 17:12:21  
SMSC: +821029190900  
Data coding scheme: Binary (4)  
Message-part: 1/1

---

**Original values:**

SMSC: 0791280192919000  
PDU-Header: 40  
TP-MTI: 00  
TP-MMS: 00  
TP-SRI: 00  
TP-RP: 00  
TP-UDHI: 40  
TP-OA: 0BA11020675200F2  
TP-PID: 00  
TP-DCS: 04  
TP-SCTS: 71803261211263  
TP-UDL: 82  
TP-UD: 0B05040B8423F000037702017706226170706C69636174696F6E2F766E642E7761702E6D6D732D6D65737361676500AF848C829831397748384E473043314958443030008D928A808E01A788058103093A8083687474703A2F2F642D6D6D73632E6B746677696E672E636F6D3A393038332F31397748384E47304331495844303000

# PDU 2/2

Resultcode : 10  
Resultmessage: Success  
Type: SMS-DELIVER  
PDU len: 73 bytes  
Originator: 01027625002  
Message: 0B05040B8423F00003770202890F800DEA303130323736323530303200960FEA41616161616161616161616100  
Timestamp: 23/08/2017 17:12:21  
SMSC: +821029190900  
Data coding scheme: Binary (4)  
Message-part: 1/1

---

**Original values:**

SMSC: 0791280192919000  
PDU-Header: 44  
TP-MTI: 00  
TP-MMS: 04  
TP-SRI: 00  
TP-RP: 00  
TP-UDHI: 40  
TP-OA: 0BA11020675200F2  
TP-PID: 00  
TP-DCS: 04  
TP-SCTS: 71803261211263  
TP-UDL: 2E  
TP-UD: 0B05040B8423F00003770202890F800DEA303130323736323530303200960FEA41616161616161616161616100

---



# TP-UDHI

- SMS에 추가 헤더를 포함시킴

The First-Octet field format is as follows:

| TP-RP | TP-UDHI | TP-SRI |   |   | TP-MMS | TP-MTI |   |
|-------|---------|--------|---|---|--------|--------|---|
| 0     | 0       | 0      | 0 | 0 | x      | 0      | 0 |

All the value are given for the most simple case, for more details see the GSM 03.40 (section 9.2.3).

**a) TP-Message-Type-Indicator (TP-MTI)**

In the case of a SMS-DELIVER, the two bits, bit 0 and bit 1, should be set with the values 0 and 0.

**b) TP-More-Messages-to-Send (TP-MMS)**

The TP-More-Messages-to-Send is a 1-bit field, located within bit no 2 of the First-Octet of SMS-DELIVER, and to be given the following values:

| Bit | 2 | Definition   |
|-----|---|--|
| 0   |   | More messages are waiting for the MS in this SC    |
| 1   |   | No more messages are waiting for the MS in this SC |

**c) TP-Status-Report-Indication (TP-SRI)**

For simplified SMS, the PDU does not contain any Status report, also the bit no. 5 of the first octet is given 0.

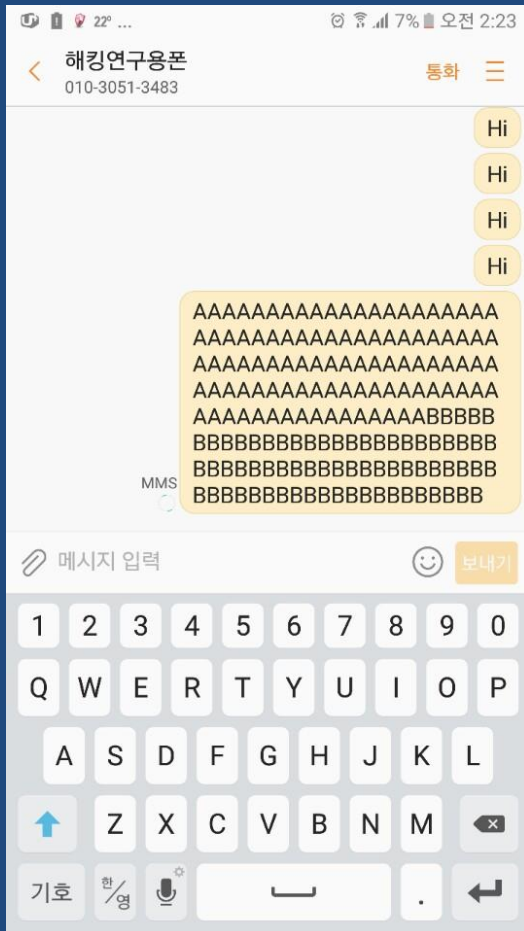
**d) TP-User-Data-Header-Indicator (TP-UDHI)**

For simplified SMS, the PDU does not contain any Header in addition to the short message, also the bit 6 within the First-Octet is equal to 0.

**e) TP-Reply-Path (TP-RP)**

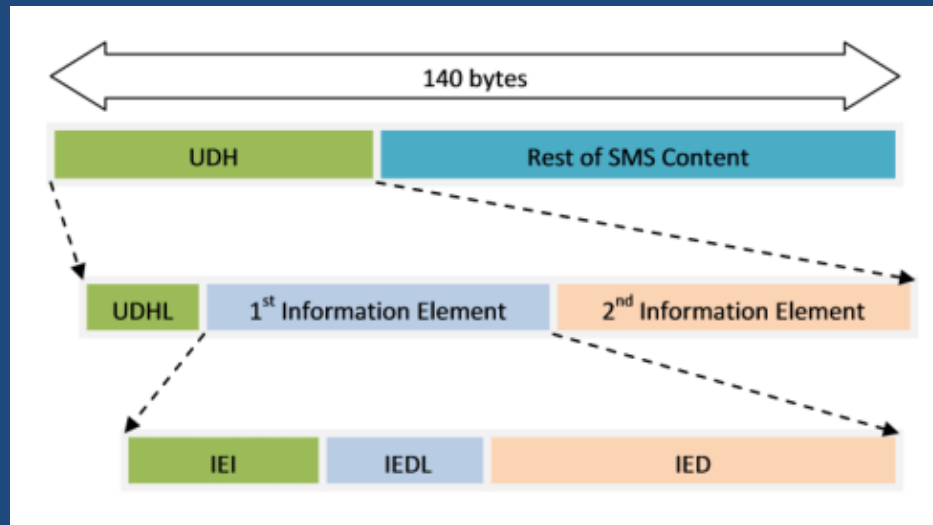
For simplified SMS, the reply path is not specified. In this case the bit 7 within the First-Octet is equal to 0.

# 다르게 해석되는 User Data



- `shell@b1:/ $ logcat | grep PDU`
- `I/[SMS_LP]( 1664):`  
`processUnsolicited():RIL_UNSOL_RESPONSE_NEW_SM`  
`S, MT PDU =`  
`0791280192919000400BA11020675200F200047180326`  
`1211263820B05040B8423F00003770201770622617070`  
`6C696361746966E2F766E642E7761702E6D6D732D6`  
`D65737361676500AF848C829831397748384E4730433`  
`14958443030008D928A808E01A788058103093A80836`  
`87474703A2F2F642D6D6D73632E6B746677696E672E`  
`636F6D3A393038332F31397748384E47304331495844`  
`303000`
- `I/[SMS_LP]( 1664):`  
`processUnsolicited():RIL_UNSOL_RESPONSE_NEW_SM`  
`S, MT PDU =`  
`0791280192919000440BA11020675200F200047180326`  
`12112632E0B05040B8423F00003770202890F800DEA3`  
`03130323736323530303200960FEA414141414141414`  
`14141414100`

# 다르게 해석되는 User Data



| 필드 의미   | 필드 길이           |
|---|-----------------|
| UDHL (User Data Header Length)                | 1byte           |
| IEI (Identity Element Identifier)             | 1byte           |
| IEDL (Length of the Information Element Data) | N-1(type) bytes |
| IED (Information Element Data)                | Nbyte           |

# 다르게 해석되는 User Data

- 820B05040B8423F000037702017706226170706C69636174696F6E2F766E642E7761702E6D6D732D6D65737361676500AF848C829831397748384E473043314958443030008D928A808E01A788058103093A8083687474703A2F2F642D6D6D73632E6B746677696E672E636F6D3A393038332F31397748384E47304331495844303000
- 2E0B05040B8423F00003770202890F800DEA303130323736323530303200960FEA4141414141414141414141414100
- 82 : TP-UDL (User Data Length)
- 0B : UDHL (User Data Header Length)
- IE : Information Elements
  - 05 : IEI (Identity Element Identifier)
    - Application Port (16bit mode)
  - 04 : IEDL (Length of the IE Data)
    - 0B84 (2948 - WAP push)
    - 23F0 (9200)

# IEI (Identity Element Identifier)

| VALUE (hex) | MEANING   |
|-------------|---|
| 00          | Concatenated short messages, 8-bit reference number         |
| 01          | Special SMS Message Indication                              |
| 02          | Reserved  |
| 03          | Value not used to avoid misinterpretation as <LF> character |
| 04          | Application port addressing scheme, 8 bit address           |
| 05          | Application port addressing scheme, 16 bit address          |
| 06          | SMSC Control Parameters                                     |
| 07          | UDH Source Indicator  |
| 08          | Concatenated short message, 16-bit reference number         |
| 09          | Wireless Control Message Protocol                           |
| <u>0A</u>   | <u>Text Formatting</u>                                      |
| <u>0B</u>   | <u>Predefined Sound</u>                                     |
| <u>0C</u>   | <u>User Defined Sound (iMelody max 128 bytes)</u>           |
| <u>0D</u>   | <u>Predefined Animation</u>                                 |

|               |  |
|---------------|--|
| <u>0E</u>     | <u>Large Animation (16*16 times 4 = 32*4 =128 bytes)</u>   |
| <u>0F</u>     | <u>Small Animation (8*8 times 4 = 8*4 =32 bytes )</u>      |
| <u>10</u>     | <u>Large Picture (32*32 = 128 bytes)</u>                   |
| <u>11</u>     | <u>Small Picture (16*16 = 32 bytes)</u>                    |
| <u>12</u>     | <u>Variable Picture</u>                                    |
| <u>13-1F</u>  | <u>Reserved for future EMS features (see section 3.10)</u> |
| <u>20A-6F</u> | Reserved for future use                                    |
| 70-7F         | (U)SIM Toolkit Security Headers                            |
| 80 - 9F       | SME to SME specific use                                    |
| A0 - BF       | Reserved for future use                                    |
| C0 - DF       | SC specific use  |
| E0 - FF       | Reserved for future use                                    |

# Samsung Galaxy 취약점

- <https://www.contextis.com/blog/wap-just-happened-my-samsung-galaxy>



# Application Port

- Port 2948 = WAP push
  - Wireless Application Protocol
    - 무선 어플리케이션 프로토콜
    - 무선 통신을 사용하는 응용 프로그램의 국제 표준
    - [https://namu.wiki/w/ 무선%20어플리케이션%20프로토콜](https://namu.wiki/w/무선%20어플리케이션%20프로토콜)
- Port 5499 = visual voicemail
- 등등



# 두 번째 Information Element

- 820B05040B8423F000037702017706226170706C69636174696F6E2F766E642E7761702E6D6D732D6D65737361676500AF848C829831397748384E473043314958443030008D928A808E01A788058103093A8083687474703A2F2F642D6D6D73632E6B746677696E672E636F6D3A393038332F31397748384E47304331495844303000
- 2E0B05040B8423F00003770202890F800DEA303130323736323530303200960FEA4141414141414141414141414100
- IE : Information Elements
  - 00 : IEI (Identity Element Identifier)
    - 00 : Concatenated SMS
  - 03 : IEDL (Length of the IE Data)
    - 77 : Reference Number
    - 02 : Total number of messages
    - 01 : Number of current message
- 참고 : <https://www.clockworksms.com/blog/concatenated-sms/>

# User Data 영역

- 820B05040B8423F000037702017706226170706C69636174696F6E2F766E642E7761702E6D6D732D6D65737361676500AF848C829831397748384E473043314958443030008D928A808E01A788058103093A8083687474703A2F2F642D6D6D73632E6B746677696E672E636F6D3A393038332F31397748384E47304331495844303000
- 2E0B05040B8423F00003770202890F800DEA303130323736323530303200960FEA4141414141414141414141414100



WAP Push Header

# User Data 영역

```
>>> str =
"b006226170706c696361746966e2f766e642e7761702e6d6d732d6d65737361676500af848c
8298343577483952323048305446343030008d928a808e01ac88058103093a8083687474703a
2f2f642d6d6d73632e6b746677696e672e636f6d3a393038332f3435774839523230483054463
4303000890f800dea303130323736323530303200960fea41414141414141414141414141414100"

>>> str.decode("hex")
'Wxb0Wx06"application/vnd.wap.mms-
messageWx00WxafWx84Wx8cWx82Wx9845wH9R20H0TF400Wx00Wx8dWx92Wx8aWx80Wx8eWx
01WxacWx88Wx05Wx81Wx03Wt:Wx80Wx83http://d-
mmssc.ktfwing.com:9083/45wH9R20H0TF400Wx00Wx89Wx0fWx80WxWxea01027625002Wx00W
x96Wx0fWxeaAAAAAAAAAAAAAAWx00'
```

D/WAP PUSH( 1636): Rx: b006226170706c696361746966e2f766e642e7761702e6d6d732d6d65737361676500af848c8298343577483952323048305446343030008d928a808e01ac88058103093a8083687474703a2f2f642d6d6d73632e6b746677696e672e636f6d3a393038332f34357748395232304830544634303000890f800dea303130323736323530303200960fea41414141414141414141414100

**V/WAP PUSH( 1636): appid found: 4:application/vnd.wap.mms-message**

**W/WAP PUSH( 1636): wap push manager not found!**

## V/WAP PUSH( 1636): fall back to existing handler

V/WAP PUSH( 1636): Delivering MMS to: com.android.mms com.android.mms.transaction.PushReceiver

**D/GsmInboundSmsHandler( 1636): dispatchWapPdu() returned -1**

**http://mmsc.ktfwing.com:9082|Proxy:|Port:**

```
V/Mms:transaction( 6933): url = http://d-mmsc.ktfwing.com:9083/29wH9R2151KKA00
```

```
V/Mms:transaction( 6933): hostUrl.getHost()=d-mmsc.ktfwing.com hostUrl.getPort()=9083
```



# Concatenated SMS

- 일반 SMS의 최대 길이는 160자
  - 7-bit encoding 기준
  - 8-bit encoding에선 140자
- Concatenated SMS를 이용하여 긴 길이의 문자 전송 가능

- PDU1

| IEI | IEDL | Reference Number | Total Number | This Number |
|-----|------|------------------|--------------|-------------|
| 00  | 03   | 77               | 2            | 1           |

- PDU2

| IEI | IEDL | Reference Number | Total Number | This Number |
|-----|------|------------------|--------------|-------------|
| 00  | 03   | 77               | 2            | 2           |

# Case study : iphone SMS RCE

- 0791947106004034c40d91947196466656f8000490108211421540040400030120

|                         |  |
|-------------------------|--|
| <b>SMS pdu:</b>         | 0791947106004034c40d91947196466656f8000490108211421540040400030120   |
| <b>Other examples:</b>  |  |
| SMS-SUBMIT:             | <u>0031000B912374374521F7000A72A5474AE4ACF4161378DA9C82A0C42AA88C0FB7E1EC32C82C7FB741F3F81C4EAEBBC6EF36</u>  |
| SMS-DELIVER:            | <u>07912374151616F6240B912374374521F70000318011416314802A5474AE4ACF4161378BD A0C82A0C42AA88C0FB7E1EC32C82C7FB741F3F81C4EAEBBC6EF36</u>   |
| SMS-STATUS-REPORT:      | <u>07912374151616F6067AD6812384460238F4318D11411300803180114113008000FFFFFFFF FFFFFFFF</u><br><u>FF</u><br><u>FF</u><br><u>FF</u><br><u>FF</u> |
| Resultcode :            | 10   |
| Resultmessage:          | Success  |
| Type:                   | SMS-DELIVER  |
| PDU len:                | 33 bytes   |
| Originator:             | +4917696466658   |
| Message:                | 0400030120   |
| Timestamp:              | 28/01/2009 11:24:51  |
| SMSC:                   | +491760000443  |
| Data coding scheme:     | Binary (4)   |
| Message-pair:           | 1/1  |
| <b>Original values:</b> |  |
| SMSC:                   | 0791947106004034   |
| PDU-Header:             | C4   |
| TP-MTI:                 | 00   |
| TP-MMS:                 | 04   |
| TP-SRI:                 | 00   |
| TP-RP:                  | 80   |
| TP-UDHI:                | 40   |
| TP-OA:                  | 00D91947196466656F8  |
| TP-PID:                 | 00   |
| TP-DCS:                 | 04   |
| TP-SCTS:                | 00108211421540   |
| TP-UDL:                 | 04   |
| TP-UD:                  | 0400030120   |

# Charlie Miller's Payload

- SMS PDU :  
0791947106004034c40d91947196466656f8000490108211421540040400030120
  - 07 : SMSC length
  - 91 : type of address
  - 947106004034 : SMSC
  - c4 : PDU Header → Additional header
  - 0d : length
  - 91 : type of address
  - 947196466656f8 : 송신자 address
  - 00 : TP-PID
  - 04 : TP-DCS
  - 90108211421540 : TP-SCTS : time stamp
  - 04 : TP-UDL length
    - 0400030120 : TP-UD (User Data)
      - 00 : IEI == Concatenated message
      - 03 : 3 bytes
        - » 01 : reference number
        - » 20 : total number of messages
        - » [none] : this message number



# Charlie Miller's Payload

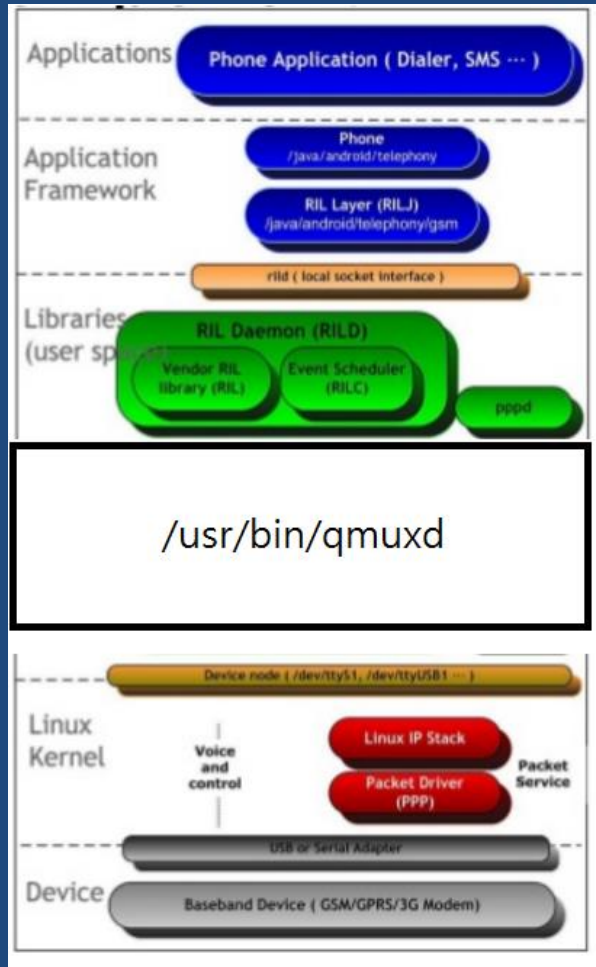
- 00 : IEI == Concatenated message
  - 03 : 3 bytes
    - 01 : reference number
    - 20 : total number of messages
    - [none] : this message number (일부러 1바이트 부족하게 놔둠)
      - 해당 값은 -1이 되어버림 (error return)
      - 마침 이 부분이 array의 index로 사용되면서 out of bound bug 발생
- [Controlled\_Address] | [ S0 S1 S2 S3 S4 ] 와 같이 heap을 구성한 후, S0~S4 array의 -1로 접근 => string\_array[-1] => Controlled Address의 값을 SMS contents로 변조 가능

# SMS Fuzzing

# SMS 전송 시의 문제점

- SMS 문자 전송료 과금
- 다량의 문자 전송 시 통신사의 모니터링, 차단 가능성
- 조작된 PDU 전송 불가
  - 중간 경유 서버들에 의한 packet drop
  - 중간 경유 서버들에 의한 PDU Data 가공
    - MMS가 서버로 저장된 후 그 URL이 상대방에게 전달 됨
- 특정 payload가 통신사 서버를 오작동 시킬 수 있음

# Android telephony stack



← `com.android.mms`

← `com.android.phone`

← `/var/rild` 소켓

← `/sbin/rild`

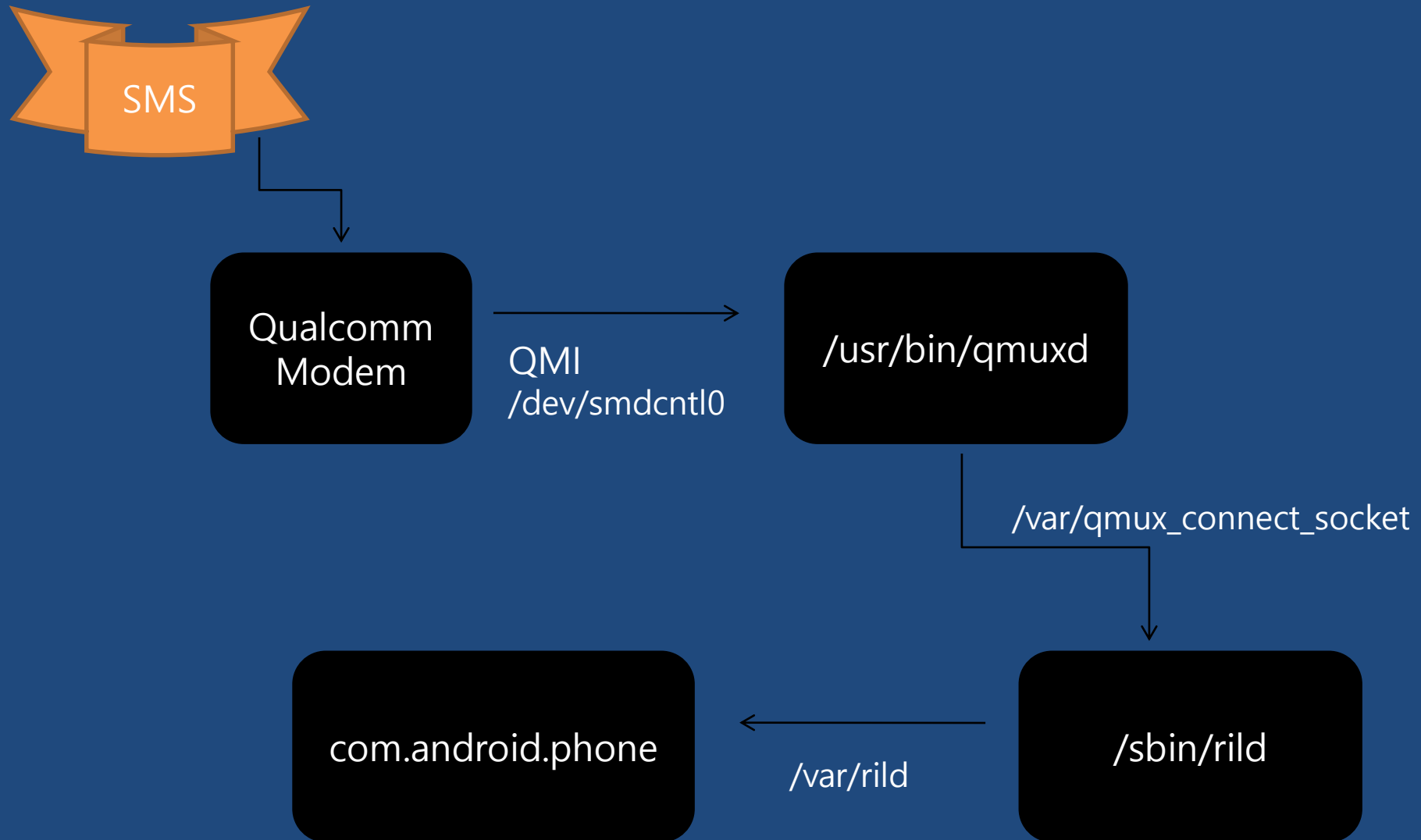
← `/var/qmux_connect_socket`

← `/usr/bin/qmuxd`

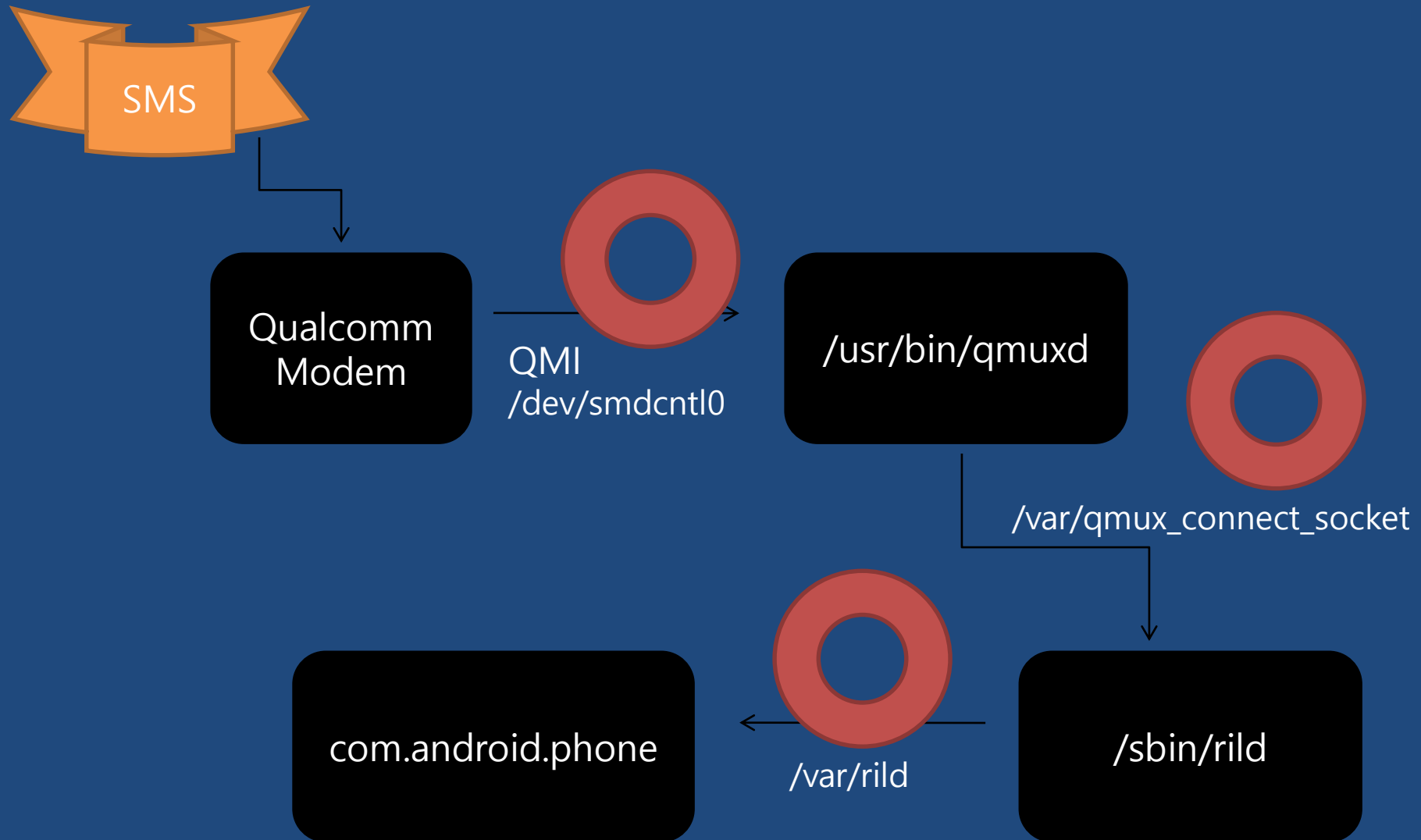
← `/dev/smdctl0`

← QUALCOMM MODEM

# SMS 수신 시의 이동 흐름



# SMS Fuzzing 가능 구간



# SMS Fuzzing

```
// QMUXD에서 신호가 오면..
if (pfd[0].revents & POLLIN == POLLIN && pfd[0].fd == smd_rild_c) {
    char buffer[1024*8] = {0};
    int rb = read(smd_rild_c, buffer, sizeof(buffer));
    if (rb <= 0) {
        close(smd_rild_c);
        smd_rild_c = -1;
    }
    else {

        // MODEM으로 전달 ****
        int wb = write(smdreal, buffer, rb);
        if (wb <= 0) {
            printf("error writing to smdreal\n");
        }
    }
}

// MODEM에서 신호가 오면..
if (pfd[1].revents & POLLIN == POLLIN) {
    char buffer[1024*8] = {0};
    int rb = read(smdreal, buffer, sizeof(buffer));
    if (rb <= 0) {
        printf("error reading from smdreal\n");
    }
    else {

        // QMUXD로 전달
        int wb = write(smd_rild_c, buffer, rb);
        if (wb <= 0) {
            printf("error writing to smb_rild_c\n");
            close(smd_rild_c);
            smd_rild_c = -1;
        }
    }
}
```

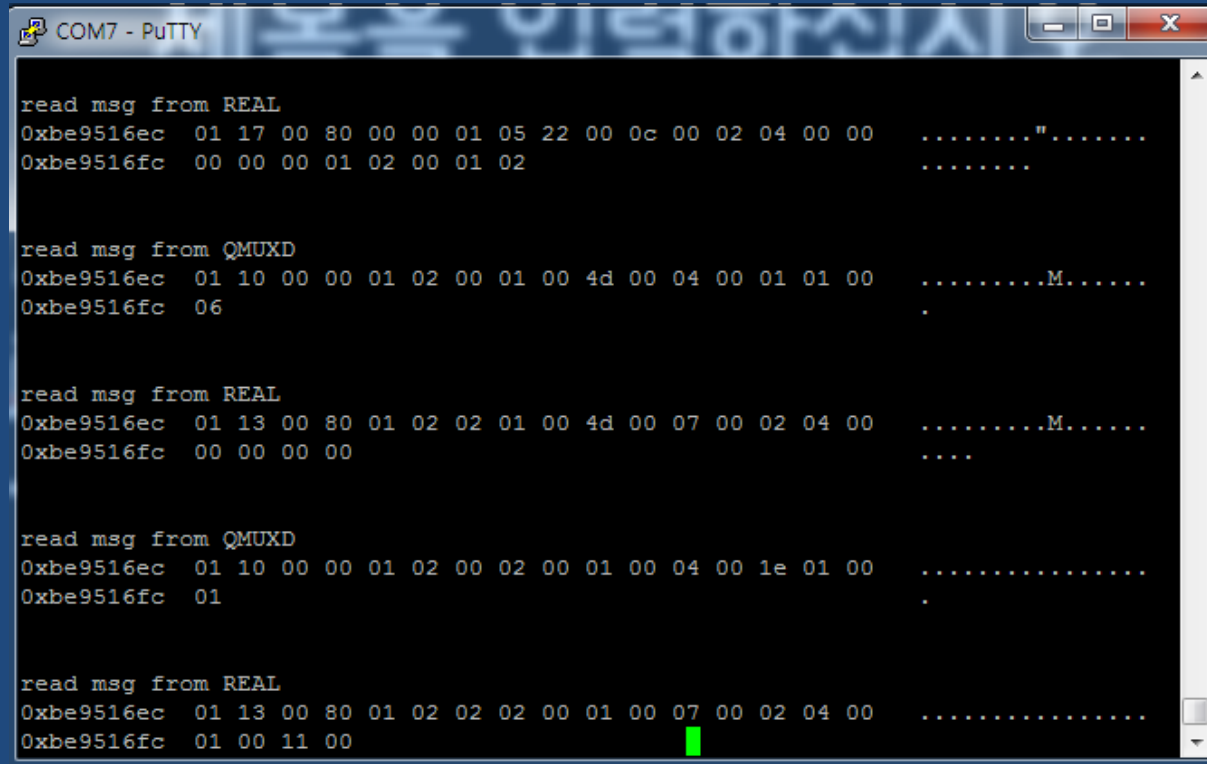
# SMS Fuzzing

```
// 서버에 연결이 들어오면..
if (pfd[2].revents & POLLIN == POLLIN && pfd[2].fd == nss) {
    printf("client connected!Wn");
    nsc = accept(nss, NULL, NULL);
    if (nsc < 0) {
        nsc = -1;
    }
    else {
        if (dolog) fprintf(log, "fuzz network connectedWn");
    }
}
// 클라이언트로부터 데이터가 들어오면..
else if (pfd[2].revents & POLLIN == POLLIN && pfd[2].fd == nsc) {
    char buffer[4096] = {0};
    int rb = read(nsc, buffer, sizeof(buffer));
    if (rb <= 0) {
        close(nsc);
        nsc = -1;
        if (dolog) fprintf(log, "fuzz network disconnectedWn");
    }
    else {
        // QMUXD로 전달
        int wb = write(smd_rild_c, buffer, rb);
        if (wb <= 0) {
            printf("fuzz write failedWn");
        }
    }
}
```



# SMS Fuzzing

- Phone side
  - ./injectord &



```
COM7 - PuTTY

read msg from REAL
0xbe9516ec 01 17 00 80 00 00 01 05 22 00 0c 00 02 04 00 00 ....."......
0xbe9516fc 00 00 00 01 02 00 01 02 .....

read msg from QMUXD
0xbe9516ec 01 10 00 00 01 02 00 01 00 4d 00 04 00 01 01 00 .....M.....
0xbe9516fc 06 .

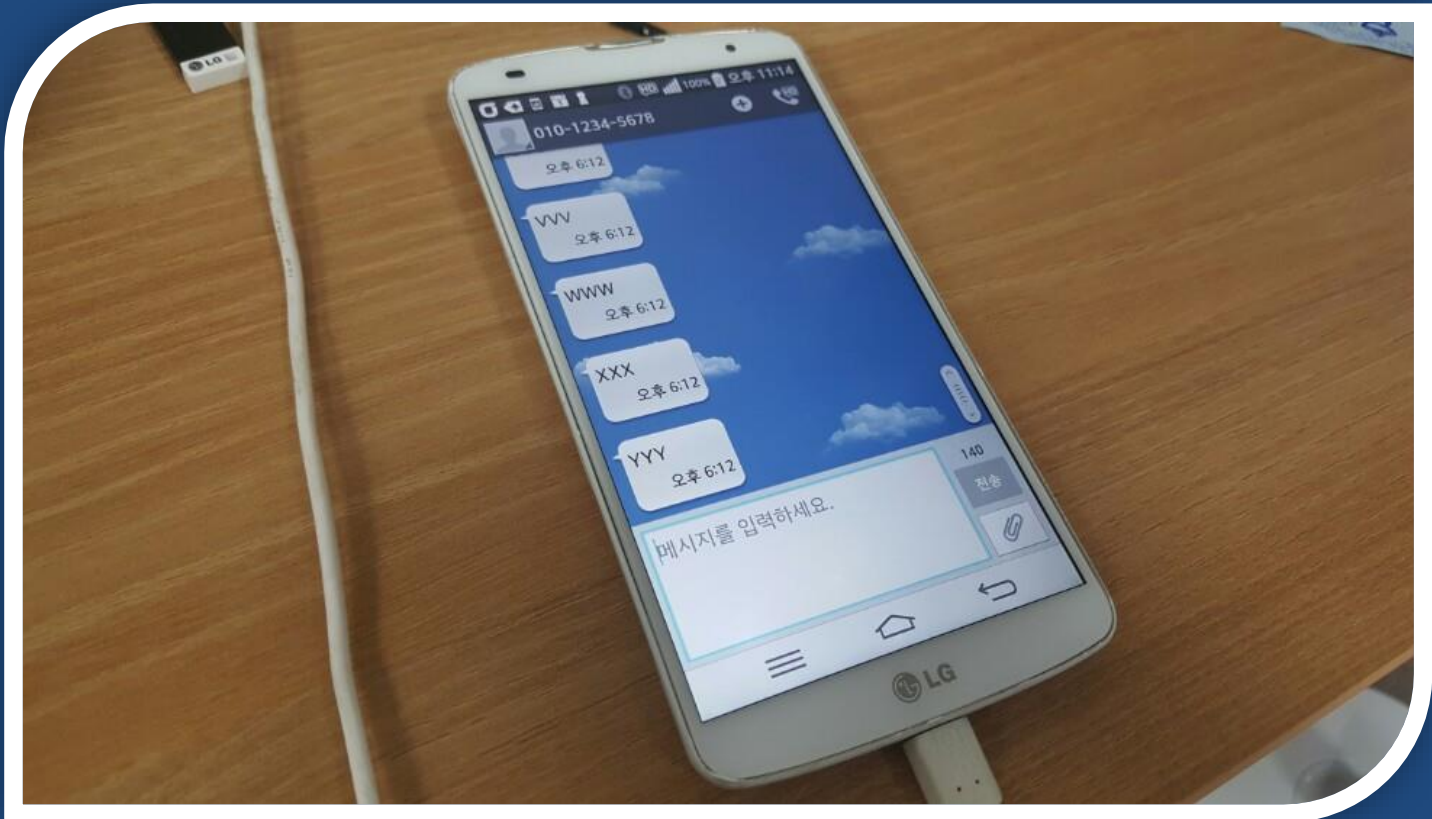
read msg from REAL
0xbe9516ec 01 13 00 80 01 02 02 01 00 4d 00 07 00 02 04 00 .....M.....
0xbe9516fc 00 00 00 00 ....

read msg from QMUXD
0xbe9516ec 01 10 00 00 01 02 00 02 00 01 00 04 00 1e 01 00 .....
0xbe9516fc 01 .

read msg from REAL
0xbe9516ec 01 13 00 80 01 02 02 02 00 01 00 07 00 02 04 00 .....
0xbe9516fc 01 00 11 00
```

# SMS Fuzzing

- PC Side
  - python sms\_fuzzing.py



# sms\_fuzzing.py

```
import socket
import time

client_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
client_socket.connect(("127.0.0.1", 5050))
i = 0

payload =
"013f00800501040000010033001601000011210000020000000061900040ba11010325476f80008718042712595630600310033003115080007912801
92919000"

#time

for n in range(0x41, 0x41+28):
    i = i + 1

    data = payload[:94] + "00" + chr(n).encode('hex') + "00" + chr(n).encode('hex') + "00" + chr(n).encode('hex') + payload[94+12:]

    data = data.decode('hex')
    #print data
    print "\n\n[%d] send payload : %s\n" % (i, data)
    client_socket.send(data)
    time.sleep(1)

client_socket.close()
print "Finished"
```

# Mutated PDU datas

[illegible]

07919471173254F6440D91947187674523F10000993092516195808215BA353B746F756368202F746D702F53554C4C45593B6AB55AAD56ABD56AB  
55AAD56ABD56AB55AAD56ABD56AB55AAD56ABD56AB55AAD56ABD56AB55AAD56ABD56AB55AAD56ABD56AB55AAD56ABD56AB55AAD56ABD  
56AB55AAD56ABD56AB55AAD56ABD56AB55AAD56ABD56AB55AAD56ABD56AB55AAD56ABD56AB55AAD56ABD56AB55AAD56ABD56AB55AAD56ABD

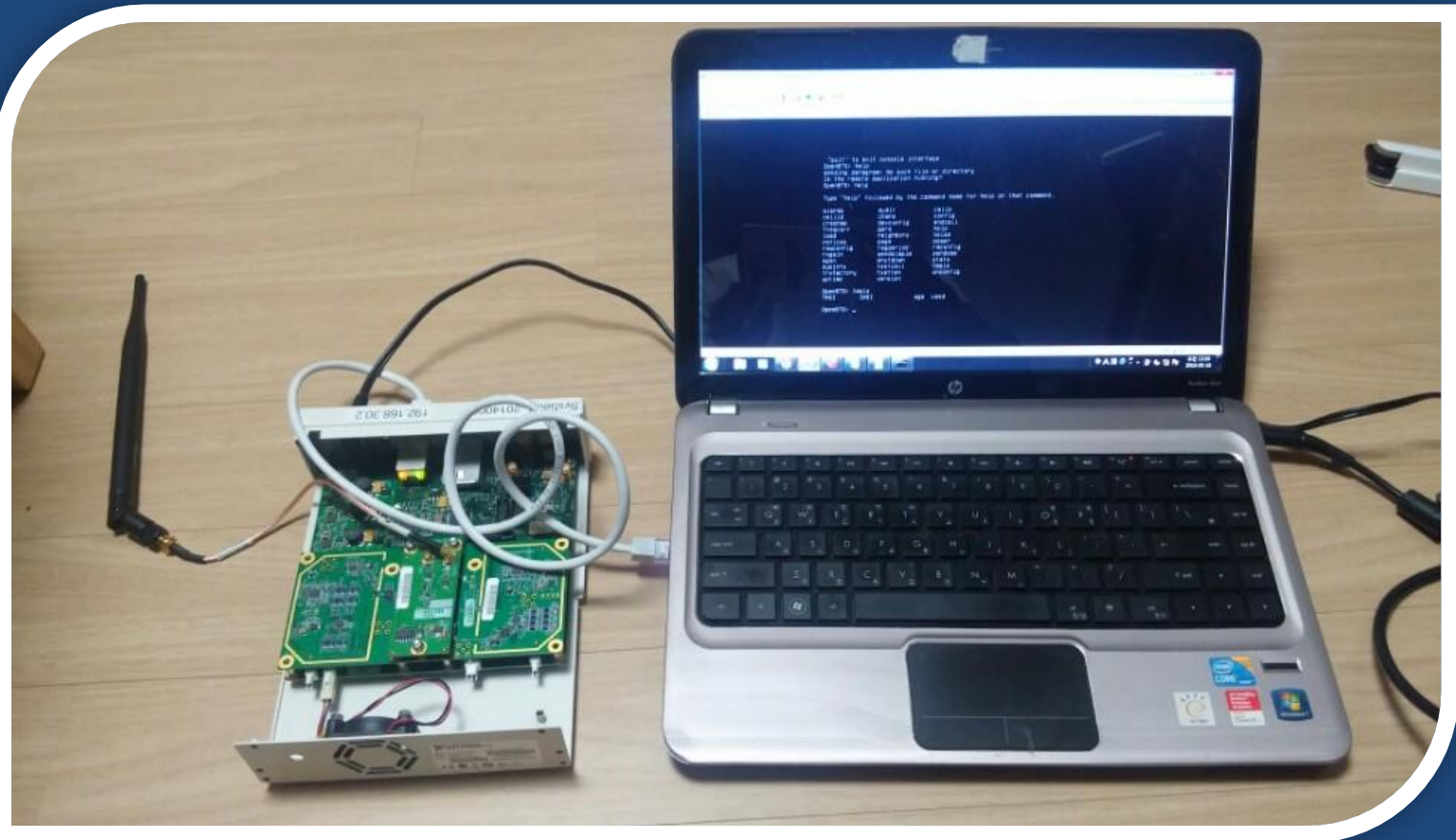
[illegible][illegible]

07919471173254F6440D91947187674523F10000993092516195800B06163C5C5C3F5C25180C

[illegible][illegible][illegible][illegible][illegible]

# 참고 : Fake BTS

- BTS : Base Transceiver Station



# 참고 : Fake BTS

- Software
  - OpenBTS
- Hardware
  - USRP N210
- OS
  - Debian 6.0
- 특징
  - 통신사의 방해를 받지 않음
  - 타겟의 전화번호를 몰라도 공격 가능
  - 차량 근거리에서 공격 가능

# 결론

- SMS를 이용하여 TCU를 원격 장악 가능
- 기능이 다양한 만큼 공격 벡터가 많음
- 후킹을 통해 폰 내에서 SMS Fuzzing 가능
- SMS는 차량에 대한 가장 위험한 공격벡터 중 하나가 될 수 있음

Q/A



**감사합니다!**

# 기타 참고자료

# 송신 SMS vs 수신 SMS

- 송신 SMS (SMS-SUBMIT)
  - 079128012143214301000B811030503184F3000004F4F29C0E
  - “test” 송신
- 수신 SMS (SMS-DELIVER)
  - 0791280192919000040BA11030503184F300007180329175716304F4F29C0E
  - “test 수신”

# SMS-SUBMIT

- 송신 SMS
  - 0791280121432143  
01000B8110305031  
84F3000004F4F29  
C0E
- PDU Header : 0x01
  - TP-MTI : 01
- TP-MR 필드 추가 (1byte)

|                     |                           |
|---------------------|---------------------------|
| Resultcode :        | 10                        |
| Resultmessage:      | Success                   |
| Type:               | SMS-SUBMIT                |
| PDU len:            | 25 bytes                  |
| Recipient:          | 01030513483               |
| Message:            | test                      |
| SMSC:               | +821012341234             |
| Data coding scheme: | SMS Default Alphabet (0)  |
| Message-id:         | 0                         |
| Message-ref:        | 0                         |
| Message-part:       | 1/1                       |
| Validity-format:    | None                      |
| Validity-timestamp: | 0 day(s), 0 hour(s) hours |

## Original values:

|             |                  |
|-------------|------------------|
| SMSC:       | 0791280121432143 |
| PDU-Header: | 01               |
| TP-MTI:     | 01               |
| TP-RD:      | 00               |
| TP-VPF:     |                  |
| TP-SRR:     | 00               |
| TP-UDHI:    | 00               |
| TP-RP:      | 00               |
| TP-MR:      | 00               |
| TP-DA:      | 0B811030503184F3 |
| TP-PID:     | 00               |
| TP-DCS:     | 00               |
| TP-VP:      | 00               |
| TP-UDL:     | 04               |
| TP-UD:      | F4F29C0E         |

# SMS-DELIVER

- 수신 SMS

– 0791280192919000  
040BA1103050318  
4F3000071803291  
75716304F4F29C0  
E

- PDU Header : 0x04

– TP-MTI : 00  
– TP-MMS : 1

|                     |                          |
|---------------------|--------------------------|
| Resultcode :        | 10                       |
| Resultmessage:      | Success                  |
| Type:               | SMS-DELIVER              |
| PDU len:            | 31 bytes                 |
| Originator:         | 01030513483              |
| Message:            | test                     |
| Timestamp:          | 23/08/2017 20:57:17      |
| SMSC:               | +821029190900            |
| Data coding scheme: | SMS Default Alphabet (0) |
| Message-part:       | 1/1                      |

## Original values:

|             |                  |
|-------------|------------------|
| SMSC:       | 0791280192919000 |
| PDU-Header: | 04               |
| TP-MTI:     | 00               |
| TP-MMS:     | 04               |
| TP-SRI:     | 00               |
| TP-RP:      | 00               |
| TP-UDHI:    | 00               |
| TP-OA:      | 0BA11030503184F3 |
| TP-PID:     | 00               |
| TP-DCS:     | 00               |
| TP-SCTS:    | 71803291757163   |
| TP-UDL:     | 04               |
| TP-UD:      | F4F29C0E         |

# PDU-Header in SMS-SUBMIT

- 01 = SMS\_SUBMIT

The First-Octet field format is as follows:

| TP-RP | TP-UDHI | TP-SRR | TP-VPF |   | TP-RD | TP-MTI |   |
|-------|---------|--------|--------|---|-------|--------|---|
| 0     | 0       | 0      | 0      | 0 | 0     | 0      | 1 |

All the value are given for the most simple case, for more details see the GSM 03.40 (section 9.2.3).

**a) TP-Message-Type-Indicator (TP-MTI)**

In the case of a SMS-SUBMIT, the two bits, bit 0 and bit 1, should be set with the values 0 and 1.

**b) TP-Reject-Duplicates (TP-RD)**

The bit 2 is set to 0, indicating the Service Center can accept an SMS-SUBMIT, which has the same TP-MR and the same TP-DA as a previously submitted from the same Originated Address.

**c) TP-Validity-Period-Format (TP-VPF)**

In the case of simplified SMS in PDU mode, we will consider that there is no validity period, in this case the TP-Validity-Period-Format value, represented by the bits 4 and 3, is 0.

**d) TP-Status-Report-Request (TP-SRR)**

To simplify, no status report is requested. In this case the bit 5 within the First-Octet is set to 0.

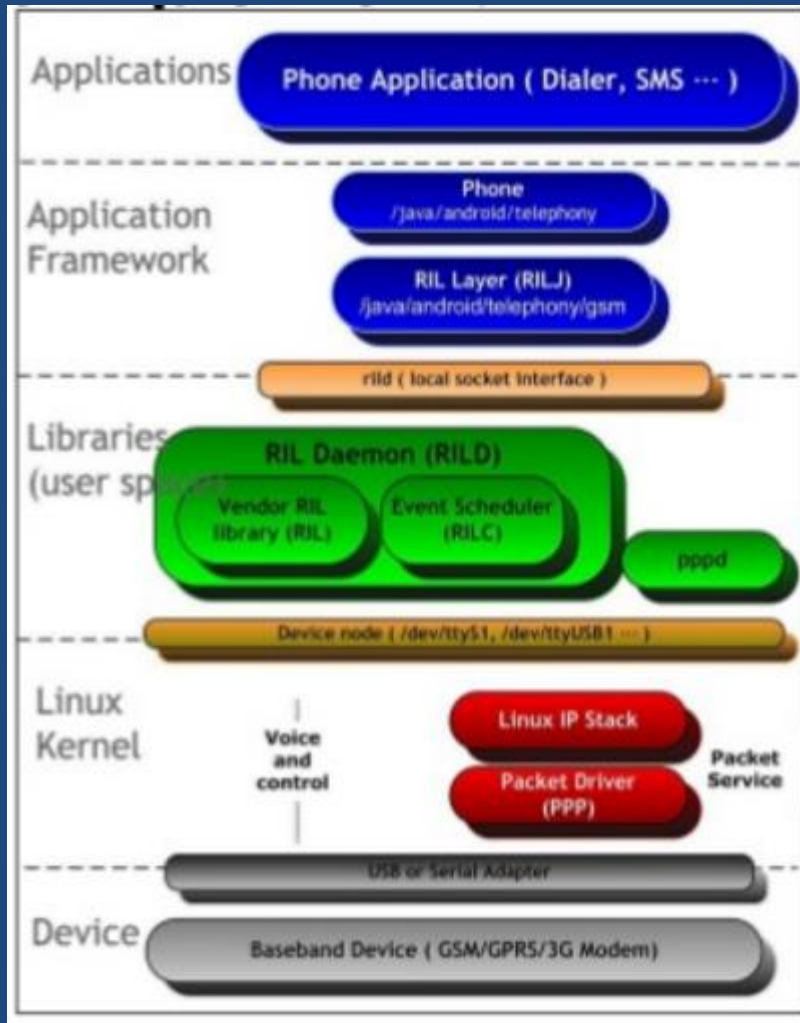
**e) TP-User-Data-Header-Indicator (TP-UDHI)**

To simplify, the PDU does not contain any Header in addition to the short message, also the bit 6 within the First-Octet is set to 0.

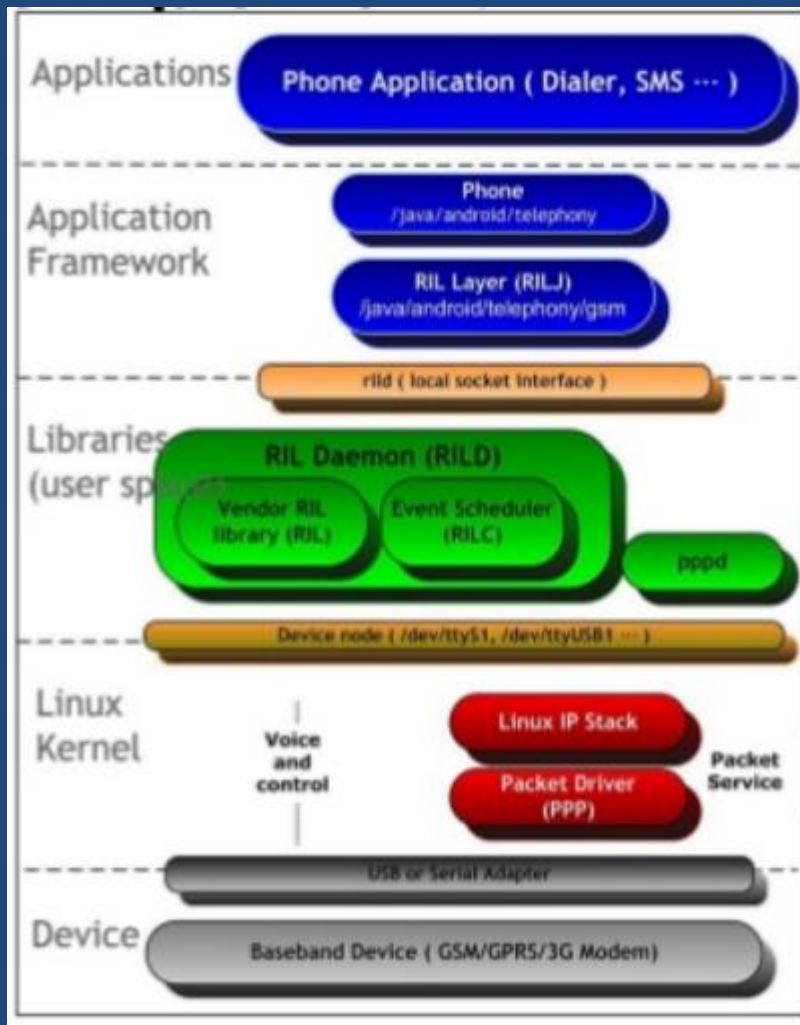
**f) TP-Reply-Path (TP-RP)**

To simplify, the reply path is not specified. In this case the bit 7 within the First-Octet is set to 0.

# Android telephony stack



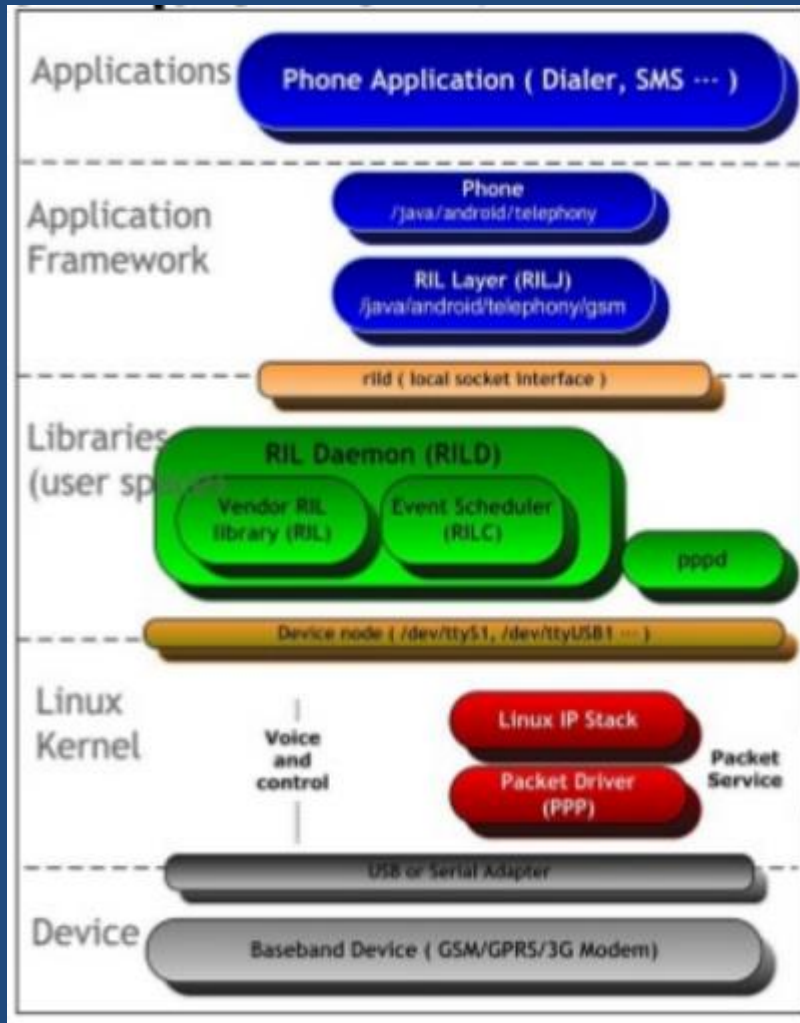
# Android telephony stack



← QUALCOMM MODEM



# Android telephony stack



← /sbin/rild

← QUALCOMM MODEM

# Rild의 socket 분석

```
/ # netstat -anp
...
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags      Type       State      I-Node PID/Program name      Path
unix  3      [ ]          STREAM     CONNECTED  1787 226/atfwd_daemon      /var/qmux_client_socket 226
unix  3      [ ]          STREAM     CONNECTED  1834 259/qmi_shutdown_mo  /var/qmux_client_socket 259
unix  2      [ ACC ]      STREAM     LISTENING  1895 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1927 256/netmgrd           /var/qmux_client_socket 256
unix  2      [ ACC ]      STREAM     LISTENING  1971 329/rild              /var/rild
unix  2      [ ACC ]      STREAM     LISTENING  1972 329/rild              /var/rild-debug
unix  3      [ ]          STREAM     CONNECTED  1973 329/rild              /var/qmux_client_socket 329
unix  2      [ ACC ]      STREAM     LISTENING  1811 250/adbd              @jdpw-control
unix  2      [ ACC ]      STREAM     LISTENING  1906 330/commander         @COMMANDER
unix  4      [ ]          DGRAM      1868 280/syslogd           /dev/log
unix  2      [ ACC ]      STREAM     LISTENING  1908 331/wifi_daemon       /tmp/wifi
unix  2      [ ACC ]      STREAM     LISTENING  1922 338/FOTA_DAEMON       /tmp/ua
unix  2      [ ACC ]      STREAM     LISTENING  1979 327/start             @android
unix  2      [ ACC ]      STREAM     LISTENING  1930 339/debuggerd         @debuggerd
unix  3      [ ]          STREAM     CONNECTED  2040 250/adbd
unix  3      [ ]          STREAM     CONNECTED  2039 250/adbd
unix  2      [ ]          STREAM     CONNECTED  1991 327/start             @android
unix  3      [ ]          STREAM     CONNECTED  1985 329/rild              /var/rild
unix  3      [ ]          STREAM     CONNECTED  1984 363/com.android.phone
unix  2      [ ]          DGRAM      1982 363/com.android.phone
unix  3      [ ]          STREAM     CONNECTED  1976 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1966 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1928 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1925 242/qmuxd             /var/qmux_connect_socket
unix  2      [ ]          DGRAM      1871 286/klogd
unix  3      [ ]          STREAM     CONNECTED  1809 250/adbd
unix  3      [ ]          STREAM     CONNECTED  1808 250/adbd
/ #
```

# Rild의 socket 분석

```
/ # netstat -anp
...
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags      Type       State      I-Node PID/Program name      Path
unix  3      [ ]          STREAM     CONNECTED  1787 226/atfwd_daemon      /var/qmux_client_socket 226
unix  3      [ ]          STREAM     CONNECTED  1834 259/qmi_shutdown_mo  /var/qmux_client_socket 259
unix  2      [ ACC ]      STREAM     LISTENING  1895 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1927 256/netmgrd           /var/qmux_client_socket 256
unix  2      [ ACC ]      STREAM     LISTENING  1971 329/rild              /var/rild
unix  2      [ ACC ]      STREAM     LISTENING  1972 329/rild              /var/rild-debug
unix  3      [ ]          STREAM     CONNECTED  1973 329/rild              /var/qmux_client_socket 329
unix  2      [ ACC ]      STREAM     LISTENING  1811 250/adbd              @jdpw-control
unix  2      [ ACC ]      STREAM     LISTENING  1906 330/commander         @COMMANDER
unix  4      [ ]          DGRAM      1868 280/syslogd           /dev/log
unix  2      [ ACC ]      STREAM     LISTENING  1908 331/wifi_daemon       /tmp/wifi
unix  2      [ ACC ]      STREAM     LISTENING  1922 338/FOTA_DAEMON       /tmp/ua
unix  2      [ ACC ]      STREAM     LISTENING  1979 327/start             @android
unix  2      [ ACC ]      STREAM     LISTENING  1930 339/debuggerd         @debuggerd
unix  3      [ ]          STREAM     CONNECTED  2040 250/adbd
unix  3      [ ]          STREAM     CONNECTED  2039 250/adbd
unix  2      [ ]          STREAM     CONNECTED  1991 327/start             @android
unix  3      [ ]          STREAM     CONNECTED  1985 329/rild              /var/rild
unix  3      [ ]          STREAM     CONNECTED  1984 363/com.android.phone
unix  2      [ ]          DGRAM      1982 363/com.android.phone
unix  3      [ ]          STREAM     CONNECTED  1976 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1966 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1928 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1925 242/qmuxd             /var/qmux_connect_socket
unix  2      [ ]          DGRAM      1871 286/klogd
unix  3      [ ]          STREAM     CONNECTED  1809 250/adbd
unix  3      [ ]          STREAM     CONNECTED  1808 250/adbd
/ #
```

# Rild의 socket 분석

```
/ # netstat -anp
...
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags      Type      State      I-Node PID/Program name      Path
unix  3      [ ]          STREAM    CONNECTED  1787 226/atfwd_daemon      /var/qmux_client_socket 226
unix  3      [ ]          STREAM    CONNECTED  1834 259/qmi_shutdown_mo  /var/qmux_client_socket 259
unix  2      [ ACC ]      STREAM    LISTENING  1895 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM    CONNECTED  1927 256/netmgrd           /var/qmux_client_socket 256
unix  2      [ ACC ]      STREAM    LISTENING  1971 329/rild              /var/rild
unix  2      [ ACC ]      STREAM    LISTENING  1972 329/rild              /var/rild-debug
unix  3      [ ]          STREAM    CONNECTED  1973 329/rild              /var/qmux_client_socket 329
unix  2      [ ACC ]      STREAM    LISTENING  1811 250/adbd              @jdpw-control
unix  2      [ ACC ]      STREAM    LISTENING  1906 330/commander         @COMMANDER
unix  4      [ ]          DGRAM     1868 280/syslogd           /dev/log
unix  2      [ ACC ]      STREAM    LISTENING  1908 331/wifi_daemon       /tmp/wifi
unix  2      [ ACC ]      STREAM    LISTENING  1922 338/FOTA_DAEMON       /tmp/ua
unix  2      [ ACC ]      STREAM    LISTENING  1979 327/start             @android
unix  2      [ ACC ]      STREAM    LISTENING  1930 339/debuggerd        @debuggerd
unix  3      [ ]          STREAM    CONNECTED  2040 250/adbd
unix  3      [ ]          STREAM    CONNECTED  2039 250/adbd
unix  2      [ ]          STREAM    CONNECTED  1991 327/start             @android
unix  3      [ ]          STREAM    CONNECTED  1985 329/rild              /var/rild
unix  3      [ ]          STREAM    CONNECTED  1984 363/com.android.phone
unix  2      [ ]          DGRAM     1982 363/com.android.phone
unix  3      [ ]          STREAM    CONNECTED  1976 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM    CONNECTED  1966 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM    CONNECTED  1928 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM    CONNECTED  1925 242/qmuxd             /var/qmux_connect_socket
unix  2      [ ]          DGRAM     1871 286/klogd
unix  3      [ ]          STREAM    CONNECTED  1809 250/adbd
unix  3      [ ]          STREAM    CONNECTED  1808 250/adbd
/ #
```

# Rild의 socket 분석

```
/ # netstat -anp
...
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags      Type       State      I-Node PID/Program name      Path
unix  3      [ ]          STREAM     CONNECTED  1787 226/atfwd_daemon      /var/qmux_client_socket 226
unix  3      [ ]          STREAM     CONNECTED  1834 259/qmi_shutdown_mo  /var/qmux_client_socket 259
unix  2      [ ACC ]      STREAM     LISTENING  1895 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1927 256/netmgrd           /var/qmux_client_socket 256
unix  2      [ ACC ]      STREAM     LISTENING  1971 329/rild              /var/rild
unix  2      [ ACC ]      STREAM     LISTENING  1972 329/rild              /var/rild-debug
unix  3      [ ]          STREAM     CONNECTED  1973 329/rild              /var/qmux_client_socket 329
unix  2      [ ACC ]      STREAM     LISTENING  1811 250/adbd              @jdpw-control
unix  2      [ ACC ]      STREAM     LISTENING  1906 330/commander         @COMMANDER
unix  4      [ ]          DGRAM      1868 280/syslogd           /dev/log
unix  2      [ ACC ]      STREAM     LISTENING  1908 331/wifi_daemon       /tmp/wifi
unix  2      [ ACC ]      STREAM     LISTENING  1922 338/FOTA_DAEMON       /tmp/ua
unix  2      [ ACC ]      STREAM     LISTENING  1979 327/start             @android
unix  2      [ ACC ]      STREAM     LISTENING  1930 339/debuggerd        @debuggerd
unix  3      [ ]          STREAM     CONNECTED  2040 250/adbd
unix  3      [ ]          STREAM     CONNECTED  2039 250/adbd
unix  2      [ ]          STREAM     CONNECTED  1991 327/start             @android
unix  3      [ ]          STREAM     CONNECTED  1985 329/rild              /var/rild
unix  3      [ ]          STREAM     CONNECTED  1984 363/com.android.phone
unix  2      [ ]          DGRAM      1982 363/com.android.phone
unix  3      [ ]          STREAM     CONNECTED  1976 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1966 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1928 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1925 242/qmuxd             /var/qmux_connect_socket
unix  2      [ ]          DGRAM      1871 286/klogd
unix  3      [ ]          STREAM     CONNECTED  1809 250/adbd
unix  3      [ ]          STREAM     CONNECTED  1808 250/adbd
/ #
```

# Rild의 socket 분석

```
/ # netstat -anp
...
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags      Type       State      I-Node PID/Program name      Path
unix  3      [ ]          STREAM     CONNECTED  1787 226/atfwd_daemon      /var/qmux_client_socket 226
unix  3      [ ]          STREAM     CONNECTED  1834 259/qmi_shutdown_mo  /var/qmux_client_socket 259
unix  2      [ ACC ]      STREAM     LISTENING  1895 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1927 256/netmgrd           /var/qmux_client_socket 256
unix  2      [ ACC ]      STREAM     LISTENING  1971 329/rild              /var/rild
unix  2      [ ACC ]      STREAM     LISTENING  1972 329/rild              /var/rild-debug
unix  3      [ ]          STREAM     CONNECTED  1973 329/rild              /var/qmux_client_socket 329
unix  2      [ ACC ]      STREAM     LISTENING  1811 250/adbd              @jdpw-control
unix  2      [ ACC ]      STREAM     LISTENING  1906 330/commander         @COMMANDER
unix  4      [ ]          DGRAM      1868 280/syslogd           /dev/log
unix  2      [ ACC ]      STREAM     LISTENING  1908 331/wifi_daemon       /tmp/wifi
unix  2      [ ACC ]      STREAM     LISTENING  1922 338/FOTA_DAEMON       /tmp/ua
unix  2      [ ACC ]      STREAM     LISTENING  1979 327/start             @android
unix  2      [ ACC ]      STREAM     LISTENING  1930 339/debuggerd        @debuggerd
unix  3      [ ]          STREAM     CONNECTED  2040 250/adbd
unix  3      [ ]          STREAM     CONNECTED  2039 250/adbd
unix  2      [ ]          STREAM     CONNECTED  1991 327/start             @android
unix  3      [ ]          STREAM     CONNECTED  1985 329/rild              /var/rild
unix  3      [ ]          STREAM     CONNECTED  1984 363/com.android.phone
unix  2      [ ]          DGRAM      1982 363/com.android.phone
unix  3      [ ]          STREAM     CONNECTED  1976 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1966 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1928 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1925 242/qmuxd             /var/qmux_connect_socket
unix  2      [ ]          DGRAM      1871 286/klogd
unix  3      [ ]          STREAM     CONNECTED  1809 250/adbd
unix  3      [ ]          STREAM     CONNECTED  1808 250/adbd
/ #
```

# Rild의 socket 분석

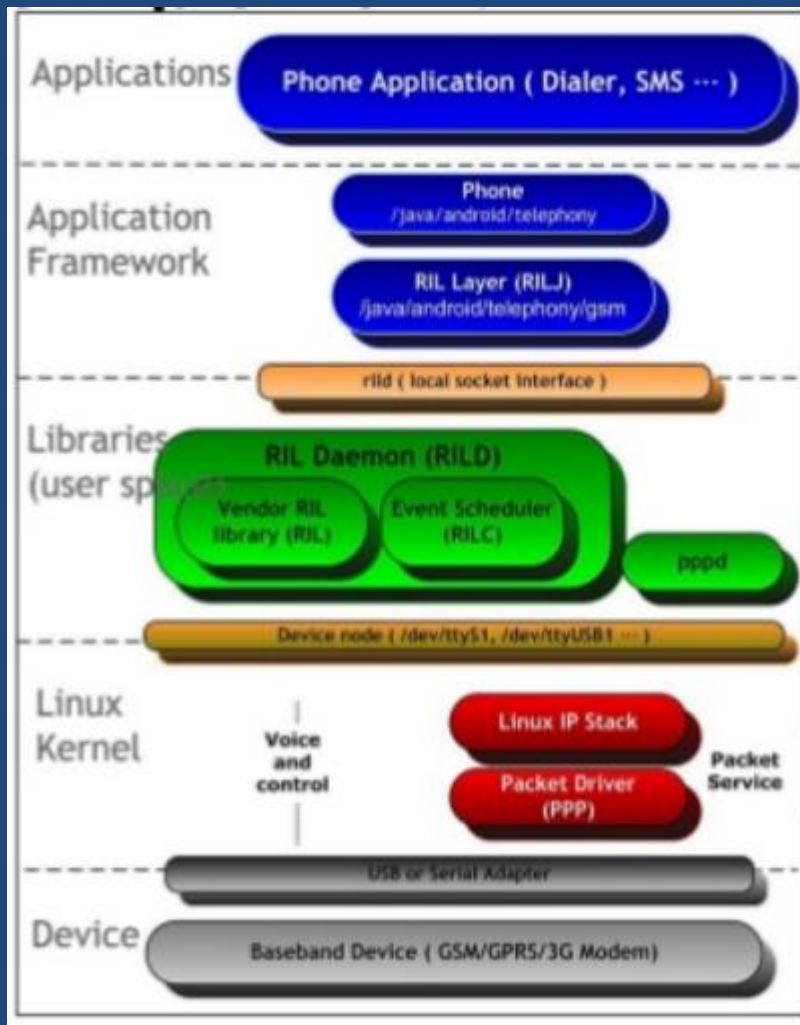
```
/ # netstat -anp
...
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags      Type       State      I-Node PID/Program name      Path
unix  3      [ ]          STREAM     CONNECTED  1787 226/atfwd_daemon      /var/qmux_client_socket 226
unix  3      [ ]          STREAM     CONNECTED  1834 259/qmi_shutdown_mo  /var/qmux_client_socket 259
unix  2      [ ACC ]      STREAM     LISTENING  1895 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1927 256/netmg             /var/qmux_client_socket 256
unix  2      [ ACC ]      STREAM     LISTENING  1971 329/rild               bind()
unix  2      [ ACC ]      STREAM     LISTENING  1972 329/rild               /var/rild_debug
unix  3      [ ]          STREAM     CONNECTED  1973 329/rild               /var/qmux_client_socket 329
unix  2      [ ACC ]      STREAM     LISTENING  1811 250/adbd              @jdpw-control
unix  2      [ ACC ]      STREAM     LISTENING  1906 330/commander         @COMMANDER
unix  4      [ ]          DGRAM      1868 280/syslogd           /dev/log
unix  2      [ ACC ]      STREAM     LISTENING  1908 331/wifi_daemon        /tmp/wifi
unix  2      [ ACC ]      STREAM     LISTENING  1922 338/FOTA_DAEMON        /tmp/ua
unix  2      [ ACC ]      STREAM     LISTENING  1979 327/start              @android
unix  2      [ ACC ]      STREAM     LISTENING  1930 339/debuggerd         @debuggerd
unix  3      [ ]          STREAM     CONNECTED  2040 250/adbd
unix  3      [ ]          STREAM     CONNECTED  2039 250/adbd
unix  2      [ ]          STREAM     CONNECTED  1991 327/start
unix  3      [ ]          STREAM     CONNECTED  1985 329/rild               /var/rild
unix  3      [ ]          STREAM     CONNECTED  1984 363/com.android.phone
unix  2      [ ]          DGRAM      1982 363/com.a
unix  3      [ ]          STREAM     CONNECTED  1976 242/qmuxd
unix  3      [ ]          STREAM     CONNECTED  1966 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1928 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1925 242/qmuxd             /var/qmux_connect_socket
unix  2      [ ]          DGRAM      1871 286/klogd
unix  3      [ ]          STREAM     CONNECTED  1809 250/adbd
unix  3      [ ]          STREAM     CONNECTED  1808 250/adbd
/ #
```

bind()

client\_fd = accept()

connect()

# Android telephony stack



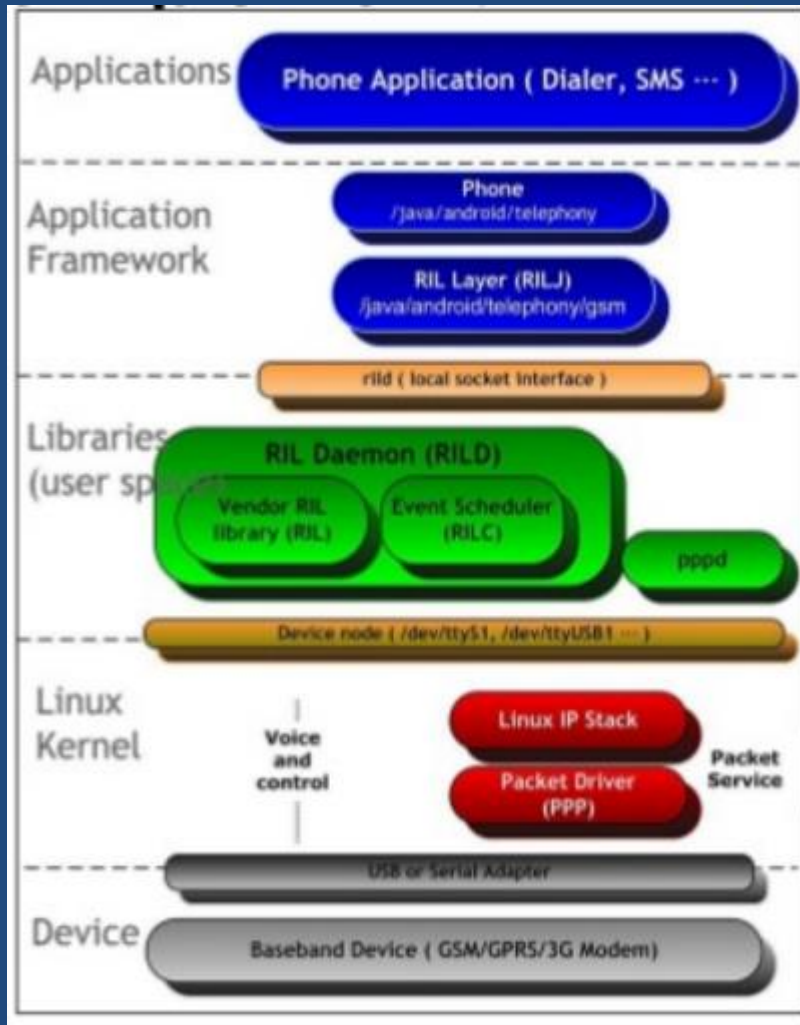
← /var/rild 소켓

← /sbin/rild

← QUALCOMM MODEM



# Android telephony stack



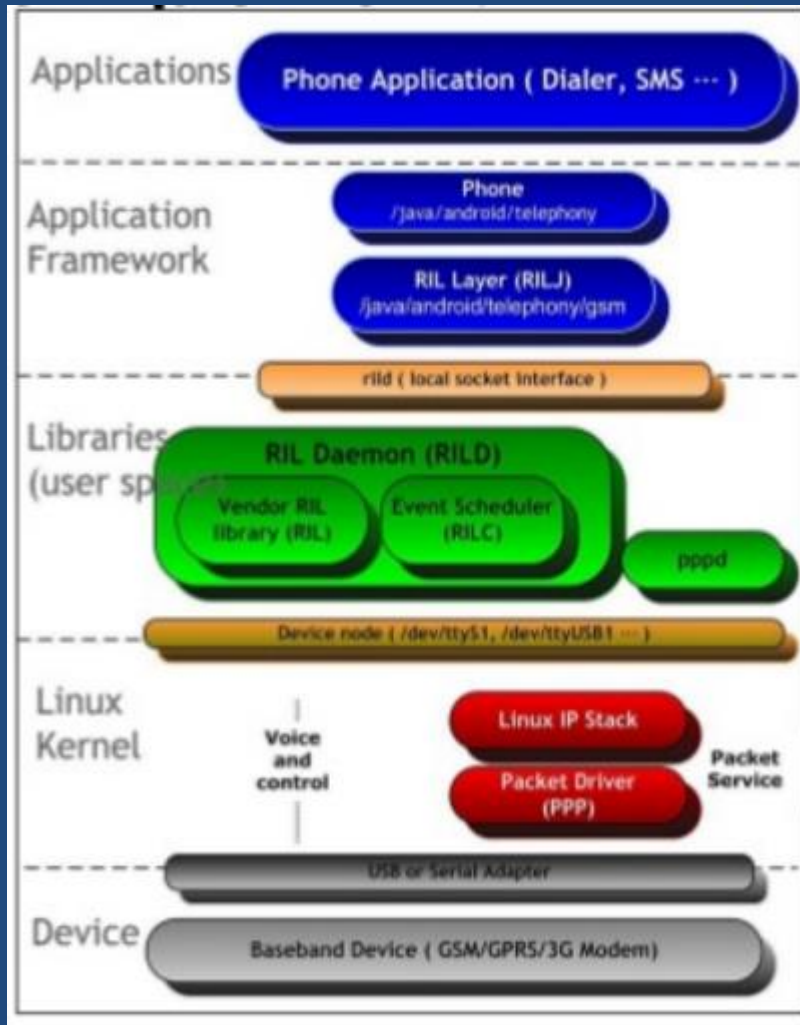
← **com.android.phone**

← /var/rild 소켓

← /sbin/rild

← QUALCOMM MODEM

# Android telephony stack



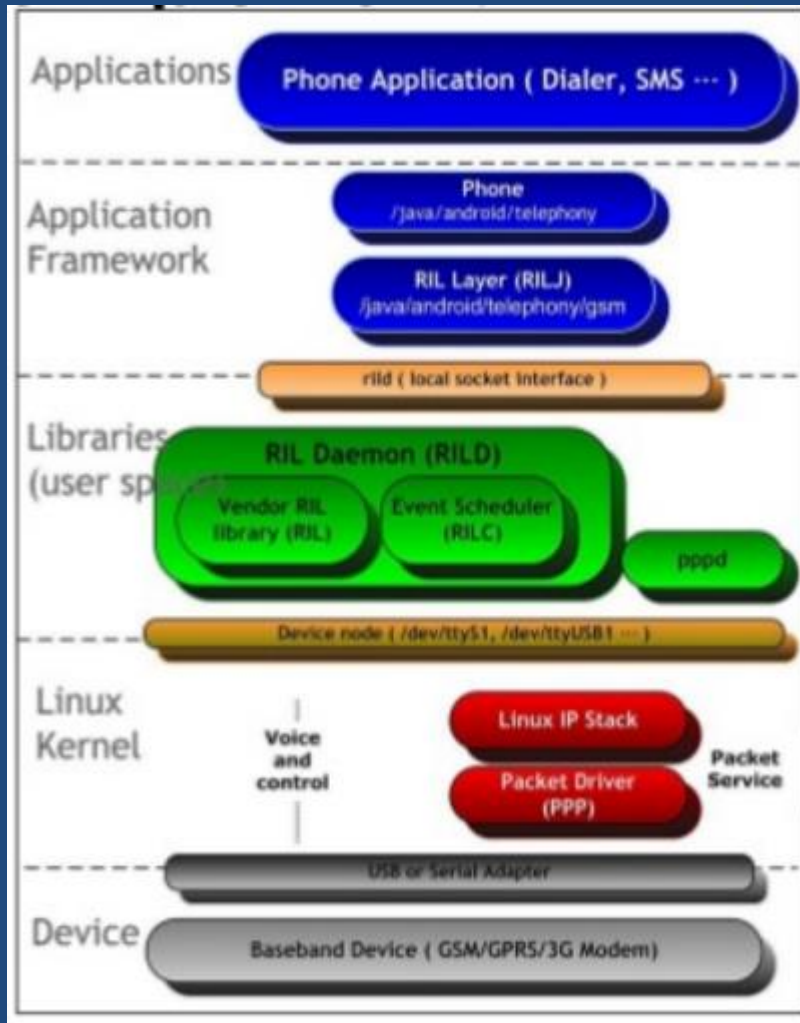
← `com.android.phone` (client)

← `/var/rild` 소켓

← `/sbin/rild` (server)

← QUALCOMM MODEM

# Android telephony stack



← `com.android.phone` (client)



← `/var/rild` 소켓



← `/sbin/rild` (server)

← ???

← QUALCOMM MODEM

# 모뎀 <-> RILD 통신 분석

- AT command VS QMI
  - QMI : Qualcomm MSM Interface

## What is QMI?

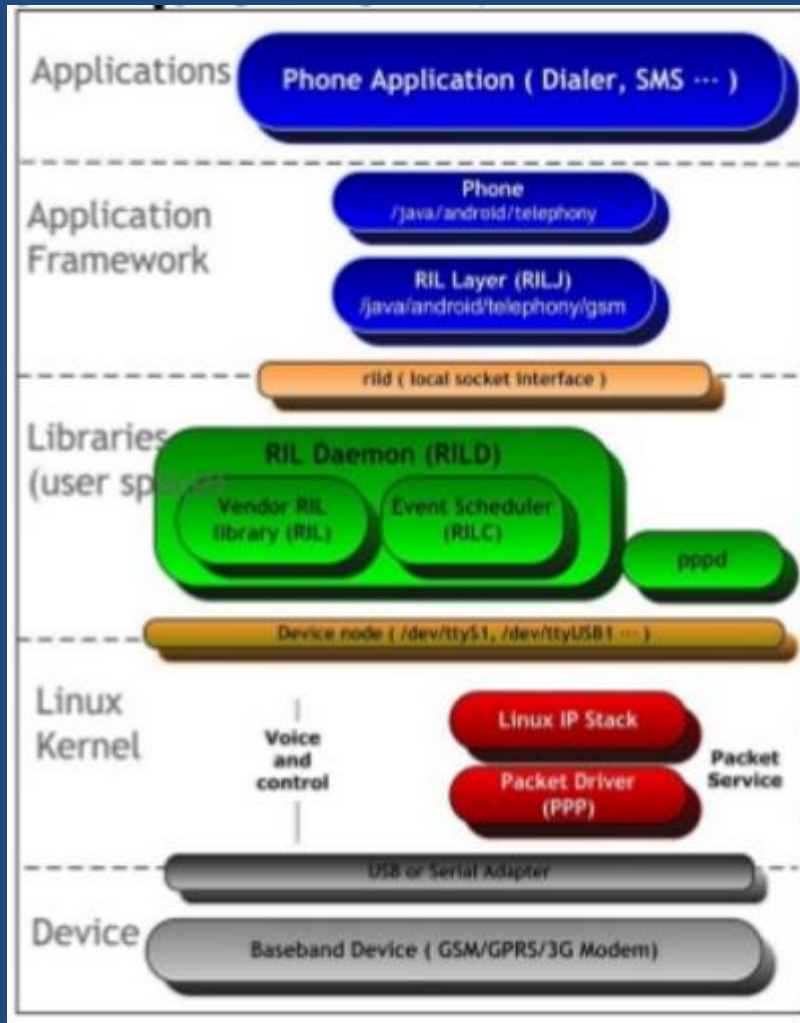
QMI is a binary protocol designed to replace the AT command based communication with modems, and is available in devices with Qualcomm chipsets from multiple vendors (Novatel, Huawei, Sierra Wireless, ZTE... and of course Qualcomm itself).

The protocol defines different 'services', each of them related to different actions that may be requested to the modem. For example, the 'DMS' (Device Management) service provides actions to load device information; while the 'NAS' (Network Access) service provides actions to register in the network. Similarly, other services will allow the user to request data connections (WDS), setup GPS location reporting (PDS), or manage internals of the user identity module (UIM service). The user needs to handle the creation of 'clients' for those services by allocating/deallocating 'client IDs' using the generic always-on 'control' (CTL) service.

# /dev/smdcntl0

```
/ # cat /dev/smdcntl0 | xxd
0000000: 013b 0080 0501 0400 0001 002f 0016 0100  .;...../....
0000010: 0011 1d00 0015 0000 0006 1500 040b a110  .....
0000020: 9036 2321 f100 0861 4031 1024 2163 0200  .6#!...a@1.$!c..
0000030: 6715 0800 0791 2801 0219 4139 011d 0080  g.....( ...A9....
0000040: 0301 0400 0051 0011 0011 0800 8305 0008  .....Q.....
0000050: 96ff ffff 1303 00a9 0700 011d 0080 0301  .....
0000060: 0400 0051 0011 0011 0800 8305 0008 96ff  ...Q.....
0000070: ffff 1303 00a2 0700 013b 0080 0501 0400  .....;.....
0000080: 0001 002f 0016 0100 0011 1d00 0016 0000  .../.....
0000090: 0006 1500 040b a110 9036 2321 f100 0861  .....6#!...a
00000a0: 4031 1024 2163 0200 6715 0800 0791 2801  @1.$!c..g.....(
/ #
```

# Android telephony stack



← **com.android.phone (client)**

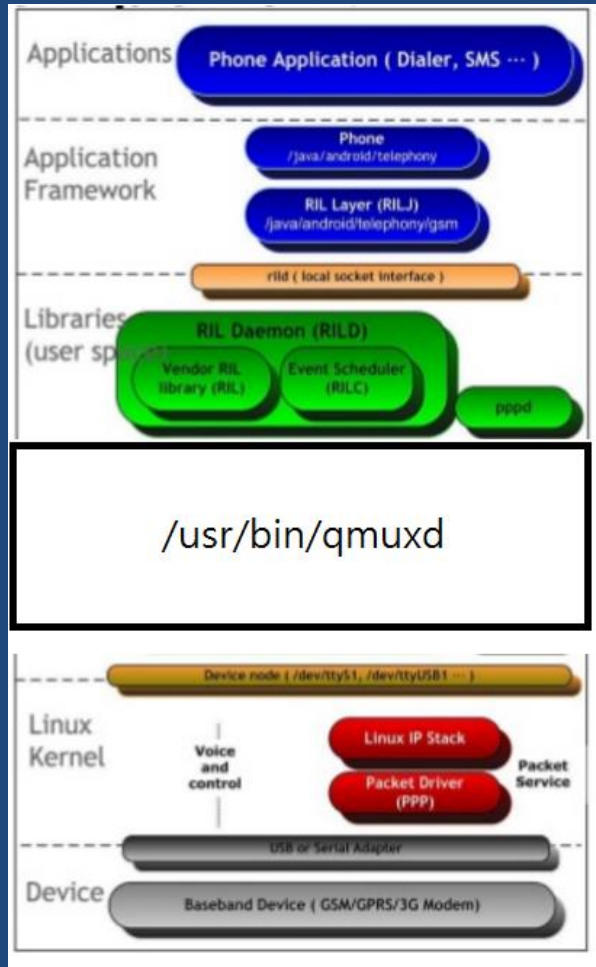
← **/var/rild 소켓**

← **/sbin/rild (server)**

← **/dev/smdctl0**

← **QUALCOMM MODEM**

# Android telephony stack



← `com.android.phone`

← `/var/rild` 소켓

← `/sbin/rild`

← `/usr/bin/qmuxd`

← `/dev/smdctl0`

← QUALCOMM MODEM

# qmuxd <-> rild 연결

```
/ # netstat -anp
...
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags      Type       State      I-Node PID/Program name      Path
unix  3      [ ]          STREAM     CONNECTED  1787 226/atfwd_daemon      /var/qmux_client_socket 226
unix  3      [ ]          STREAM     CONNECTED  1834 259/qmi_shutdown_mo  /var/qmux_client_socket 259
unix  2      [ ACC ]      STREAM     LISTENING  1895 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1927 256/netmgrd           /var/qmux_client_socket 256
unix  2      [ ACC ]      STREAM     LISTENING  1971 329/rild              /var/rild
unix  2      [ ACC ]      STREAM     LISTENING  1972 329/rild              /var/rild-debug
unix  3      [ ]          STREAM     CONNECTED  1973 329/rild              /var/qmux_client_socket 329
unix  2      [ ACC ]      STREAM     LISTENING  1811 250/adbd              @jdpw-control
unix  2      [ ACC ]      STREAM     LISTENING  1906 330/commander         @COMMANDER
unix  4      [ ]          DGRAM      1868 280/syslogd           /dev/log
unix  2      [ ACC ]      STREAM     LISTENING  1908 331/wifi_daemon       /tmp/wifi
unix  2      [ ACC ]      STREAM     LISTENING  1922 338/FOTA_DAEMON       /tmp/ua
unix  2      [ ACC ]      STREAM     LISTENING  1979 327/start             @android
unix  2      [ ACC ]      STREAM     LISTENING  1930 339/debuggerd        @debuggerd
unix  3      [ ]          STREAM     CONNECTED  2040 250/adbd
unix  3      [ ]          STREAM     CONNECTED  2039 250/adbd
unix  2      [ ]          STREAM     CONNECTED  1991 327/start             @android
unix  3      [ ]          STREAM     CONNECTED  1985 329/rild              /var/rild
unix  3      [ ]          STREAM     CONNECTED  1976 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1966 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1928 242/qmuxd             /var/qmux_connect_socket
unix  3      [ ]          STREAM     CONNECTED  1925 242/qmuxd             /var/qmux_connect_socket
unix  2      [ ]          DGRAM      1871 286/klogd
unix  3      [ ]          STREAM     CONNECTED  1809 250/adbd
unix  3      [ ]          STREAM     CONNECTED  1808 250/adbd
/ #
```



# qmuxd <-> rild 연결

```
/ # netstat -anp
...
```

Active UNIX domain sockets (servers and established)

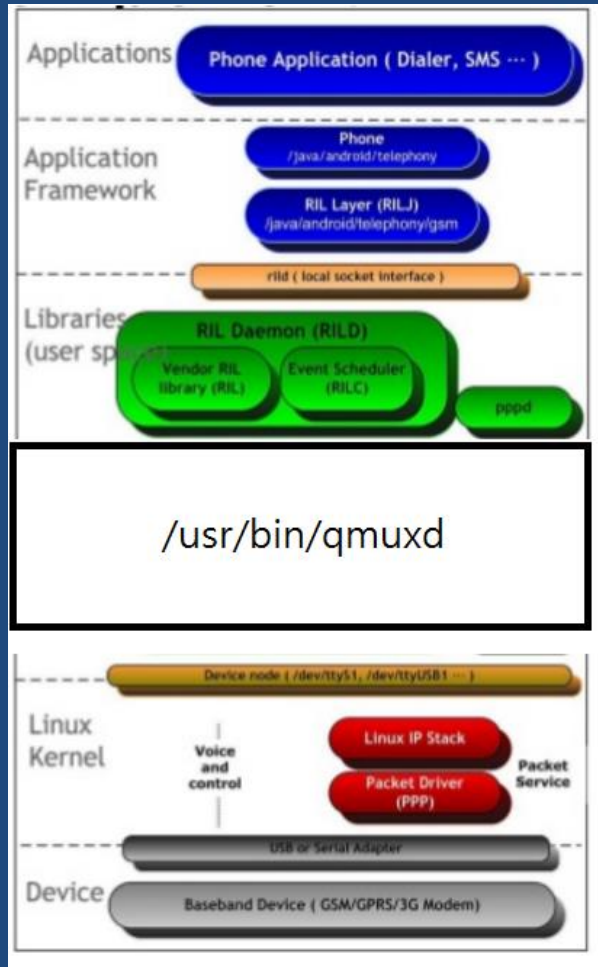
| Proto | RefCnt | Flags   | Type   | State     | I-Node | PID/Program name    | Path                     |
|-------|--------|---------|--------|-----------|--------|---------------------|--------------------------|
| unix  | 3      | [ ]     | STREAM | CONNECTED | 1787   | 226/atfwd_daemon    | /var/                    |
| unix  | 3      | [ ]     | STREAM | CONNECTED | 1834   | 259/qmi_shutdown_mo | /var/                    |
| unix  | 2      | [ ACC ] | STREAM | LISTENING | 1895   | 242/qmuxd           | /var/qmux_connect_socket |
| unix  | 3      | [ ]     | STREAM | CONNECTED | 1927   | 256/netmgrd         | /var/qmux_client_socket  |
| unix  | 2      | [ ACC ] | STREAM | LISTENING | 1971   | 329/rild            | /var/rild                |
| unix  | 2      | [ ACC ] | STREAM | LISTENING | 1972   | 329/rild            | /var/rild-debug          |
| unix  | 3      | [ ]     | STREAM | CONNECTED | 1973   | 329/rild            | /var/qmux_client_socket  |
| unix  | 2      | [ ACC ] | STREAM | LISTENING | 1811   | 250/adbd            | @jdpw-control            |
| unix  | 2      | [ ACC ] | STREAM | LISTENING | 1906   | 330/commander       | @COMMANDER               |
| unix  | 4      | [ ]     | DGRAM  |           | 1868   | 280/syslogd         | /dev/log                 |
| unix  | 2      | [ ACC ] | STREAM | LISTENING | 1908   | 331/wifi_daemon     | /tmp/wifi                |
| unix  | 2      | [ ACC ] | STREAM | LISTENING | 1922   | 338/FOTA_DAEMON     | /tmp/ua                  |
| unix  | 2      | [ ACC ] | STREAM | LISTENING | 1979   | 327/start           | @android                 |
| unix  | 2      | [ ACC ] | STREAM | LISTENING | 1930   | 339/debuggerd       | @debuggerd               |
| unix  | 3      | [ ]     | STREAM | CONNECTED | 2040   | 250/adbd            |                          |
| unix  | 3      | [ ]     | STREAM | CONNECTED | 2039   | 250/adbd            |                          |
| unix  | 2      | [ ]     | STREAM | CONNECTED | 1991   | 327/start           | @android                 |
| unix  | 3      | [ ]     | STREAM | CONNECTED | 1985   | 329/rild            | /var/rild                |
| unix  | 3      | [ ]     | STREAM | CONNECTED | 1976   | 242/qmuxd           |                          |
| unix  | 3      | [ ]     | STREAM | CONNECTED | 1966   | 242/qmuxd           |                          |
| unix  | 3      | [ ]     | STREAM | CONNECTED | 1928   | 242/qmuxd           | /var/qmux_connect_socket |
| unix  | 3      | [ ]     | STREAM | CONNECTED | 1925   | 242/qmuxd           | /var/qmux_connect_socket |
| unix  | 2      | [ ]     | DGRAM  |           | 1871   | 286/klogd           |                          |
| unix  | 3      | [ ]     | STREAM | CONNECTED | 1809   | 250/adbd            |                          |
| unix  | 3      | [ ]     | STREAM | CONNECTED | 1808   | 250/adbd            |                          |

bind()

connect()

client\_fd = accept()

# Android telephony stack



← `com.android.phone`

← `/var/rild` 소켓

← `/sbin/rild`

← `/var/qmux_connect_socket`

← `/usr/bin/qmuxd`

← `/dev/smdctl0`

← QUALCOMM MODEM