Hacking phone calls and data

Priya Chalakkal

About me : Priya Chalakkal

- Security Researcher at ERNW GmbH, Heidelberg
- Loves telco, pcaps, binaries, logs, protocols and all security stuff in general.
- I am a Blackhoodie
- https://priyachalakkal.wordpress.com/
- https://insinuator.net/

Agenda

- Introduction
- Fundamentals
- Exercise1 : Fun with Base Station
- Exercise 2 : Digging into SIM cards
- Exercise 3 : VoLTE calls
- Hands on time

Introduction - Telephony

Circuit Switched

- PSTN : *Public Switched Telephone Networks*
- Dedicated circuit – "Channel"
- Roots tracked back to 1876
  - Graham Bell got the first patent

Packet Switched

- Data sent as Packets
- Protocol stack: TCP/IP
- Eg:- Internet
- For voice - VoIP

Introduction – VoLTE/VoWiFi

VoLTE

- SK Telecom and LG U+Objective South Korea – 2012
- Vodafone Germany – VoLTE – March 2015

VoWiFi:

- Telekom Germany – VoWiFi – May 2016
- WiFi Calling

History of Mobile Communication

- GSM (2G)
  - Relies on Circuit Switching
  - Supports only Voice and SMS
- GPRS
  - Circuit – voice and SMS
  - Packet – Data
- UMTS (3G)
  - Similar to GPRS
  - Other network elements evolved

ERNW
providing security.

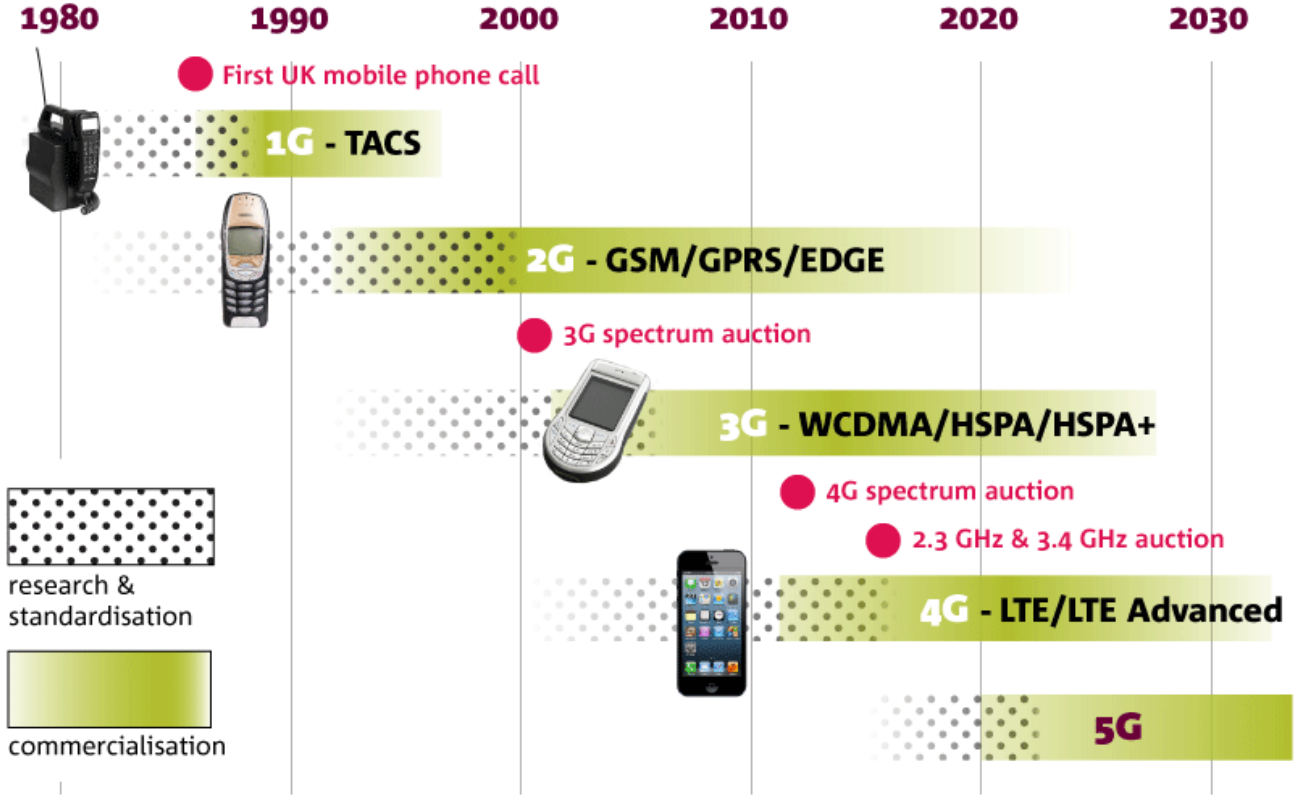
Voice and 4G

- LTE (4G): Supports only packet switching
- Voice - VoLTE
- Circuit Switched Fall Back (CSFB)
  - For voice, fall back to circuit switched networks.
- Other approaches
  - Simultaneous voice and LTE

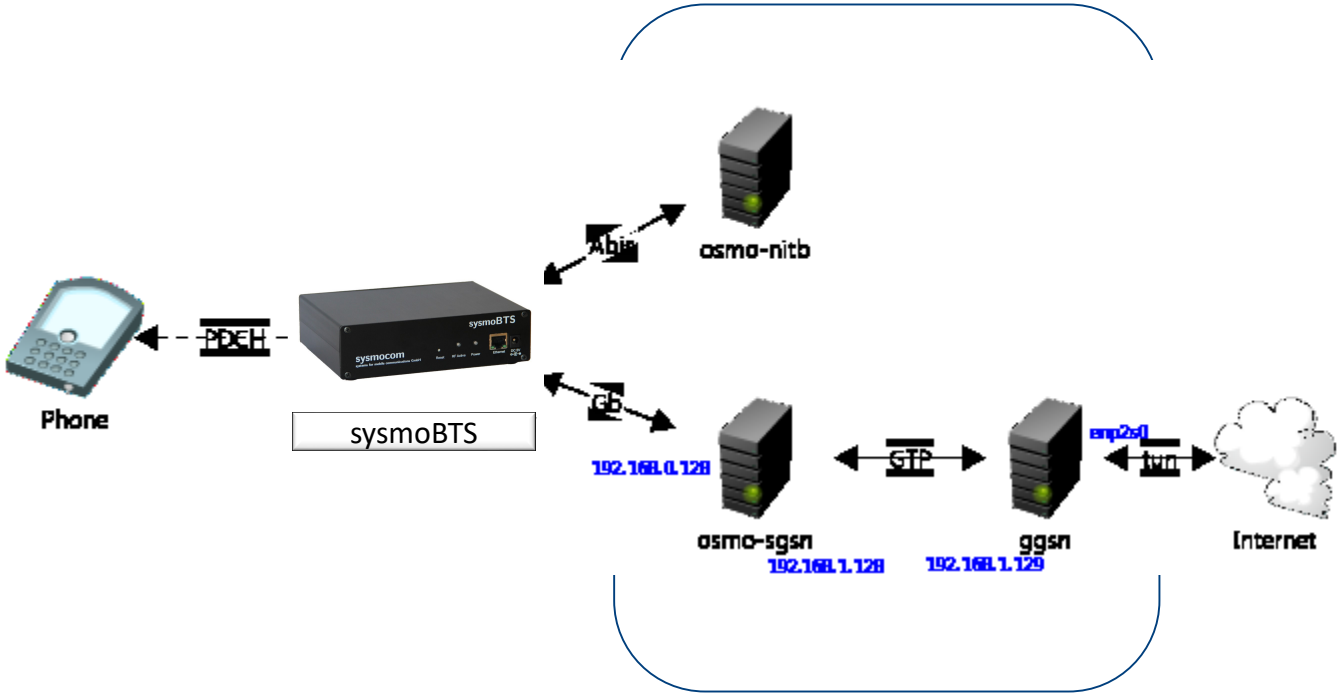
  etc..

ERNW
providing security.

Evolution of mobile phone communications



Exercise1 : Fun with Base Station


Abis
osmo-nitb
PDCH
sysmoBTS
sysmocom
Phone
sysmoBTS
Gb
192.168.0.128
GTP
enp2s0
tun
osmo-sgsn
192.168.1.128
ggsn
192.168.1.129
Internet

ERNW
providing security.

Alternative cheaper solution

Software - OpenBTS:
https://github.com/RangeNetworks/dev/wiki

My blog post:
https://insinuator.net/2018/02/hacking-101-to-mobile-data/

Osmo/nitb

- OsmoNITB implements all parts of a GSM Network (BSC, MSC, VLR, HLR, AUC, SMSC) in the box, i.e. in one element.

GGSN

- The GGSN is responsible for the internetworking between the GPRS network and external packet switched networks, such as the Internet or an X.25 network.

ERNW
providing security.

SGSN

- The Serving GPRS Support Node (SGSN) is the node that is serving the MS/UE.

- The SGSN keeps track of the location of an individual MS/UE and performs security functions and access control.

Building your own fake base station

- Quick look at Exercise

Exercise2 : Digging into SIM cards

ERNW
providing security.

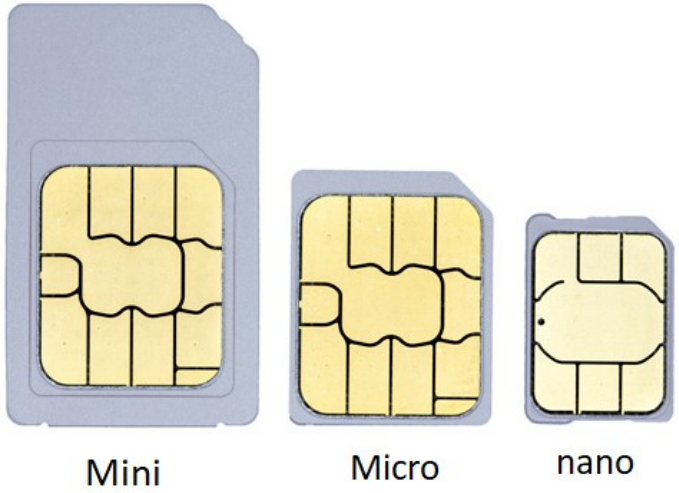
What is a SIM card?

- A **subscriber identity module** or **subscriber identification module** (SIM), widely known as a **SIM card**, is an integrated circuit that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers).

ERNW
providing security.

Universal Integrated Circuit Card

- GSM – SIM
- UMTS – USIM
- IMS- ISIM
- CDMA – CSIM
- UICC contains CPU, ROM, RAM, EEPROM, and I/O circuits
- OS – Java /proprietary



What is inside a SIM?

- IMSI (15 digits, ITU E.212 standard)
- Key for authentication
- SSN – SIM serial number
- Authentication algorithms
- Phone book, SMS
- Location area identiy (LAI)
- etc

ERNW
providing security.

IMSI

- international mobile subscriber identity
- Private identity - IMSI
- Public identity is the phone number

Task – find your IMSI from your phone

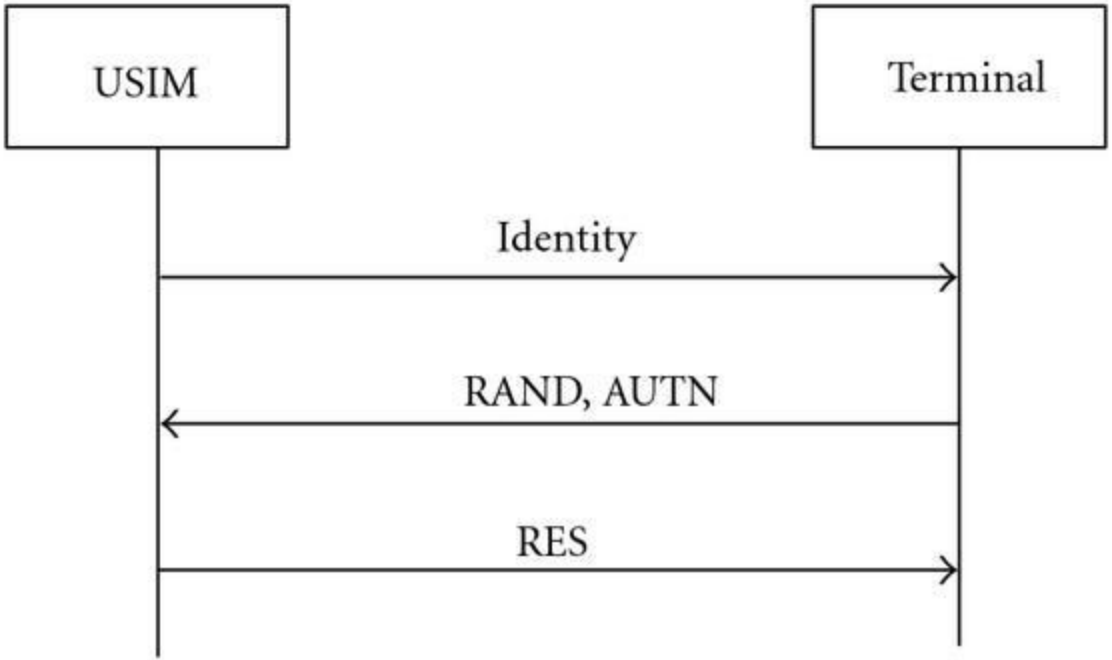
ERNW
providing security.

SIM reader

Pysim tool :
https://osmocom.org/projects/pysim/wiki

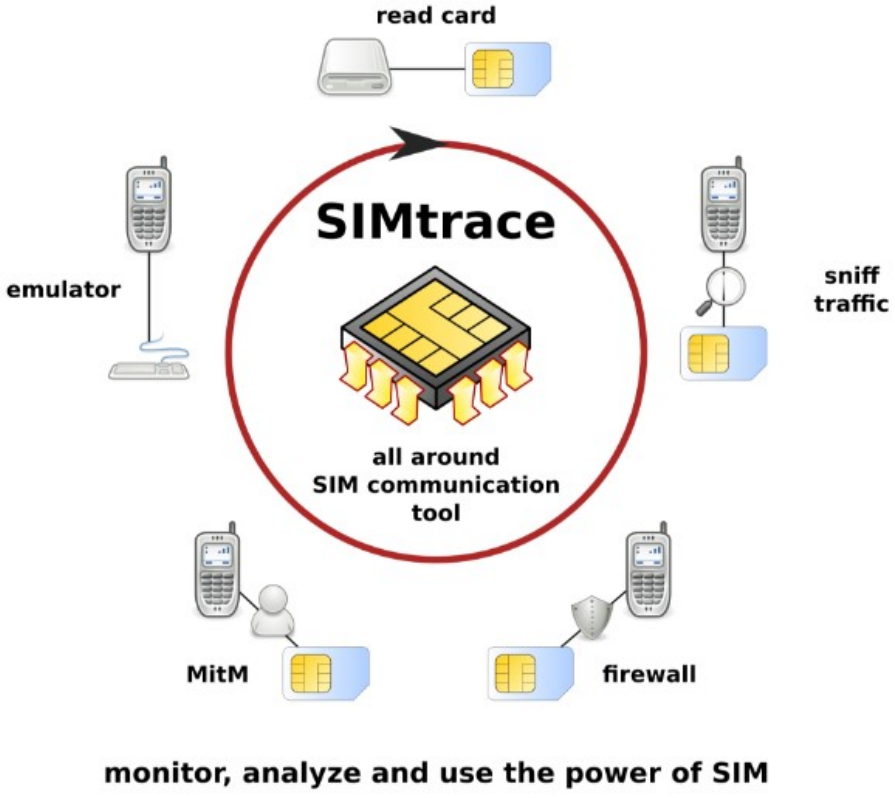
Different types

- sysmoUSIM-SJS1
- GrcardSIM
- GrcardSIM2
- MagicSIM
- More
- https://osmocom.org/projects/pysim/wiki

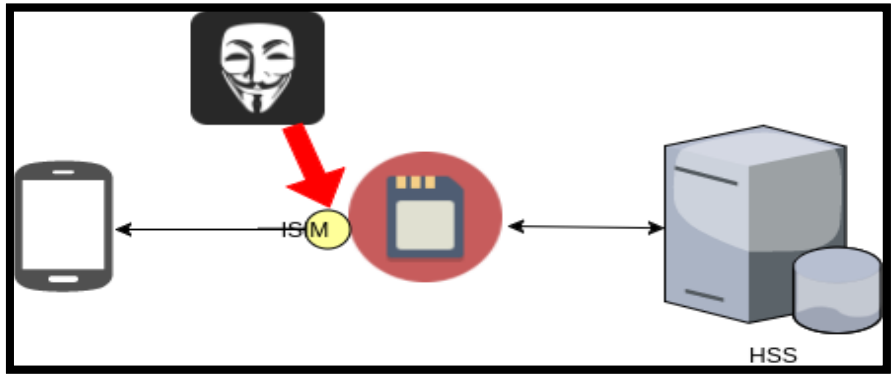

USIM
Terminal
Identity
RAND, AUTN
RES

ERNW
providing security.

SIMTrace



SIM
sniffing with
SIMTrace



SIM sniffing

```
[~/thesis/simtrace/host]> sudo ./simtrace
simtrace - GSM SIM and smartcard tracing
(C) 2010 by Harald Welte <laforge@gnumonks.org>

Entering main loop
ATR APDU: 3b 9f 96 80 1f c6 80 31 e0 73 fe 21 1b 66 d0 02 06 e2 0f 18 01 f0
PPS(Fi=9/Di=6) APDU: 00 a4 00 04 02 3f 00 61 2e
APDU: 00 c0 00 00 2e 62 2c 82 02 78 21 83 02 3f 00 a5 09 80 01 61 83 04 00 00 57 6a 8a 01 05 8b 03
APDU: 00 a4 00 0c 02 2f e2 90 00
APDU: 00 b0 00 00 0a 98 94 20 00 00 21 09 68 85 19 90 00
APDU: 00 a4 00 04 02 2f 05 61 1e
APDU: 00 c0 00 00 1e 62 1c 82 02 41 21 83 02 2f 05 a5 03 80 01 61 8a 01 05 8b 03 2f 04 04 02 00 08
APDU: a4 00 04 02 a4 2f 06
APDU: 61 21 00 c0 00 00 21
APDU: c0 62 1f 82 05 42 21
APDU: 00 38 08 83 02 2f 06
APDU: a5 03 80 01 61 8a 01
APDU: 05 8b 03 2f 06 01 80
APDU: 02 01 c0 88 01 30 90
APDU: 00 00 b2 04 04 38 b2
APDU: 80 01 18 a4 06 83 01
APDU: 0b 95 01 08 80 01 02
APDU: a0 18 a4 06 83 01 01
APDU: 95 01 08 a4 06 83 01
APDU: 0b 95 01 08 a4 06 83
APDU: 01 0c 95 01 08 80 01
APDU: 01 90 00 84 01 d4 a4
APDU: 06 83 01 0b 95 01 08
APDU: 90 00 00 a4 00 04 02
APDU: a4 2f 05 61 1e 00 c0
APDU: 00 00 1e c0 62 1c 82
APDU: 02 41 21 83 02 2f 05
APDU: a5 03 80 01 61 8a 01
APDU: 05 8b 03 2f 06 04 80
APDU: 02 00 08 88 01 28 90
APDU: 00 00 b0 00 00 08 b0
APDU: 64 65 65 6e ff ff ff
APDU: ff 90 00 80 10 00 00
APDU: 20 10 ff ff ff ff 7f
APDU: 9d 00 df ff 00 1f e2 00 00 00 c3 eb 00 00 00 01 48 00 50 00 00 00 00 08 00 00 60 91 0f 00 a4
83 02 2f 00 a5 03 80 01 61 8a 01 05 8b 03 2f 06 07 80 02 00 2c 88 01 f0 91 0f 00 a4 00 04 02 a4 2f
03 80 01 61 8a 01 05 8b 03 2f 06 01 80 02 01 c0 88 01 30 91 0f 00 b2 07 04 38 b2 80 01 1a a4 06 83
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 91 0f 00 a4 00 04 02 a4
```

SIM locking

- PIN – 4-8 digits
- 3 failed attempts, locks SIM
- PUK – personal unblocking code
- 10 failed attempts locks the SIM card

Task: SIMtrace – VERIFY pcap for PIN

GSM SIM authenticate while Registration

Source	Destination	sport	dport	Protocol	Info
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 UPDATE BINARY Offset=35072
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 SELECT File DF.GSM-ACCESS
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 SELECT File 4f52
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 GET RESPONSE
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 UPDATE BINARY Offset=0
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 SELECT File ADF
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 SELECT File EF.PSLOCI
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 GET RESPONSE
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 UPDATE BINARY Offset=0
127.0.0.1	127.0.1.1	49482	53	DNS	Standard query 0x5e58 A prx1.ernw.net
127.0.1.1	127.0.0.1	53	49482	DNS	Standard query response 0x5e58 A prx1.ernw.net A 62.159.96.83
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 UPDATE BINARY Offset=36608
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 UPDATE BINARY Offset=36608
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 SELECT /ADF
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 RUN GSM ALGORITHM / AUTHENTICATE
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 GET RESPONSE
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 UPDATE BINARY Offset=40448
127.0.0.1	127.0.0.1	42129	4729	GSM SIM	ISO/IEC 7816-4 UPDATE BINARY Offset=35584

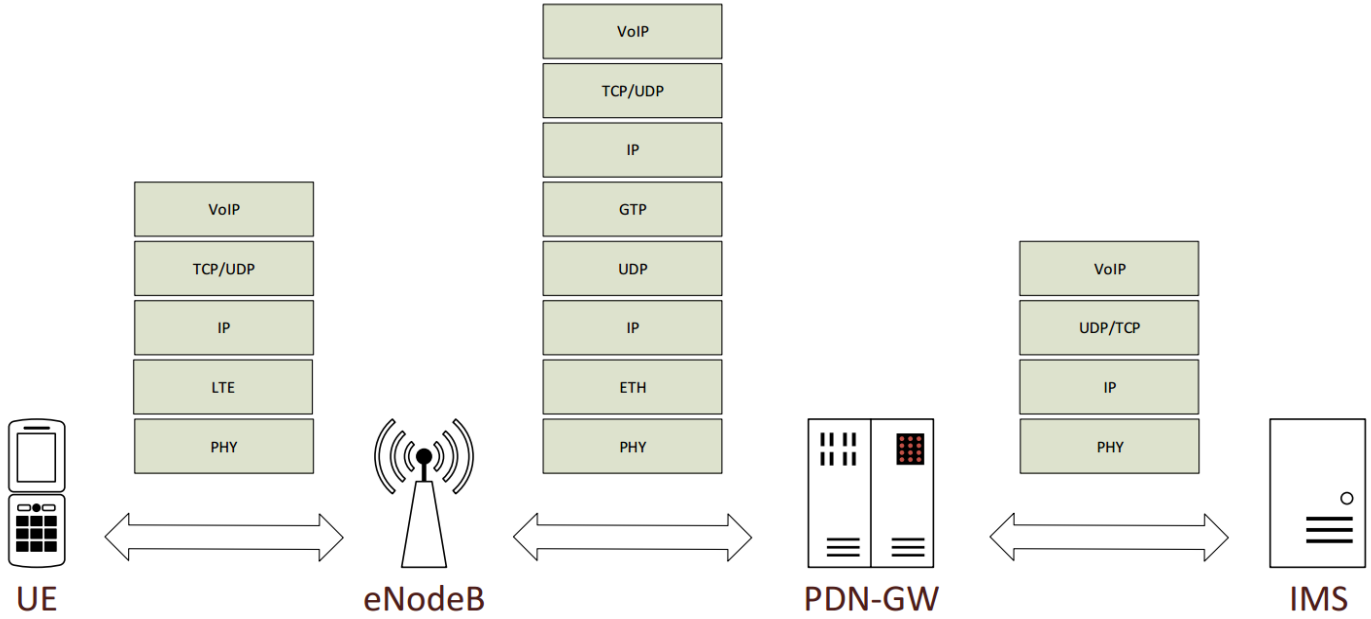
Exercise3 : 4G calls

Voice and 4G

- LTE (4G): Supports only packet switching
- **Voice - VoLTE**
- **Circuit Switched Fall Back (CSFB)**
  - For voice, fall back to circuit switched networks.
- Other approaches
  - Simultaneous voice and LTE

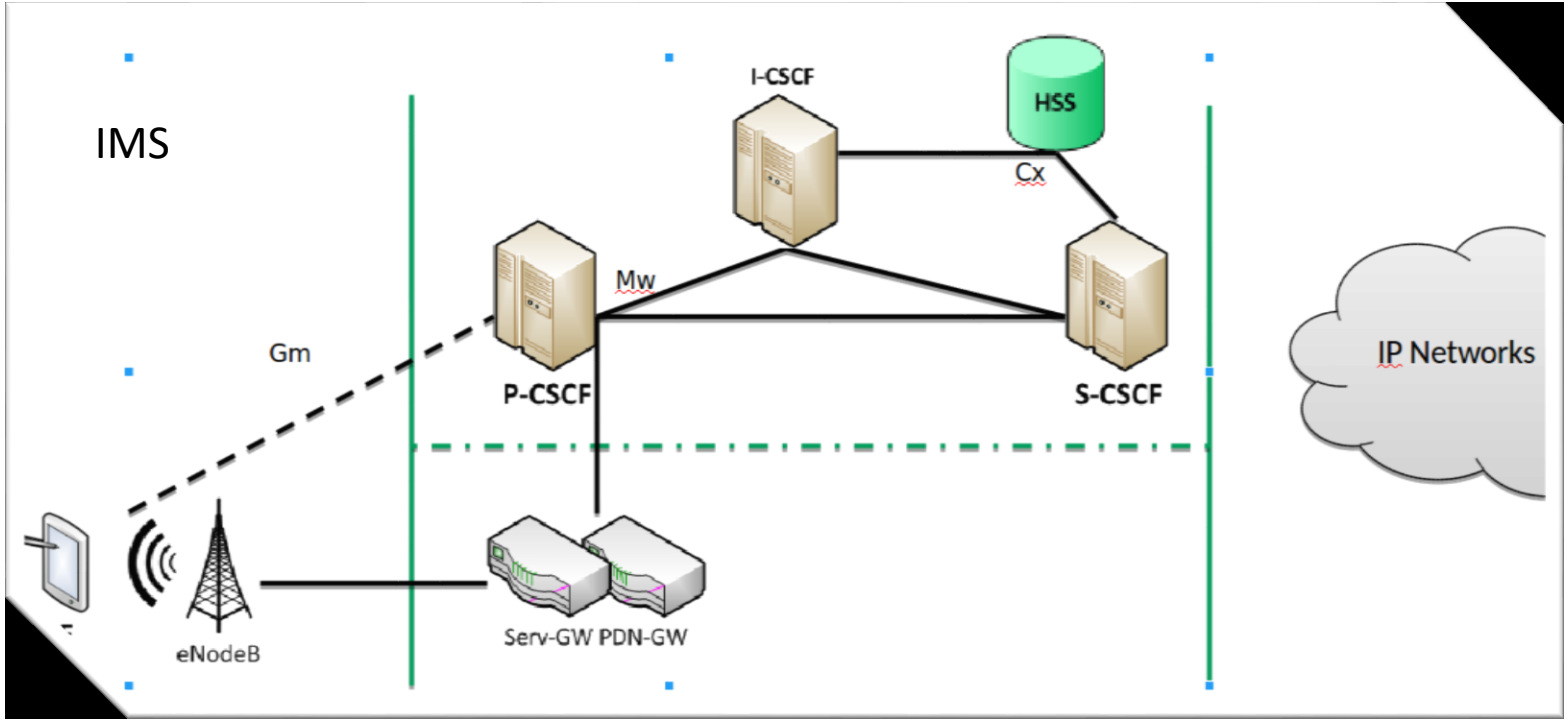
  etc..

VoLTE Stack


VoIP
TCP/UDP
IP
LTE
PHY
VoIP
TCP/UDP
IP
GTP
UDP
IP
ETH
PHY
VoIP
UDP/TCP
IP
PHY
UE
eNodeB
PDN-GW
IMS

IMS – IP Multimedia Subsystem

- Backend: IMS Core
  - *IP Multimedia Subsystem*
  - Call session control functions (CSCF)
    - P-CSCF
    - S-CSCF
    - I-CSCF

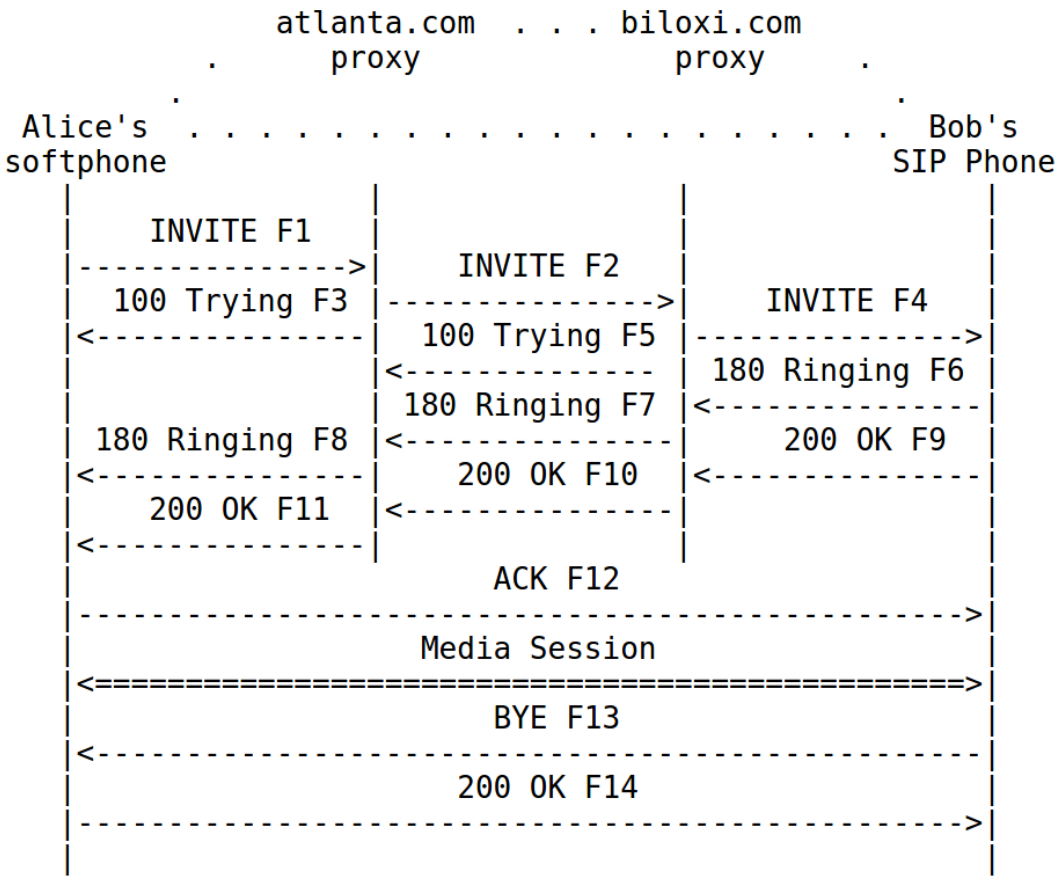

IMS
I-CSCF
HSS
Cx
Mw
Gm
P-CSCF
S-CSCF
IP Networks
eNodeB
Serv-GW PDN-GW

IMS Signaling

SIP - Session Initiation Protocol

- Similar to HTTP (text based)
- TCP or UDP
- Contains SDP
  - Session Description Protocol
  - Describing multimedia session
  - Eg:- audio/video type

SIP call session



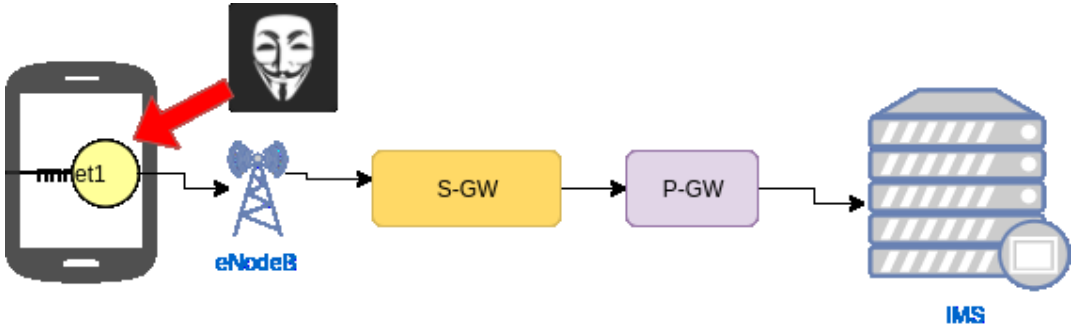

```
INVITE sip: jennifer@csp.com SIP/2.0
Via: SIP/2.0/UDP [5555::a:b:c:d]:1400; branch=abc123
Max-Forwards:70
Route: <sip:[5555::55:66:77:88]:7531;lr>,< sip:orig@scscf1.home.fi;lr>
P-Access-Network-Info:3GPP-E-UTRAN-TDD;utran-cell-id-3gpp=244005F3F5F7
P-Preferred-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel
Privacy: none
From: <sip:kristiina@example.com>;tag=171828
To: <sip:jennifer@csp.com>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: sec-agree
Proxy-Require: sec-agree
Supported: precondition, 100rel, 199
Security-Verify: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=98765432;
spi-s=87654321; port-c=8642; port-s=7531
Contact: <sip:[5555::a:b:c:d]:1400;+g.3gpp.icsi-ref="urn%3Aurn-7%
3gpp-service.ims.icsi.mmtel"
Accept-Contact: *;+g.3gpp.icsi-ref="urn%3Aurn-7%
3gpp-service.ims.icsi.mmtel"
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE, OPTIONS
Accept:application/sdp, application/3gpp-ims+xml
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2890844526 2890842807 IN IP6 5555::a:b:c:d
s=-
c=IN IP6 5555::a:b:c:d
t=0 0
m=audio 49152 RTP/AVP 97 98
a=rtpmap:97 AMR/8000/1
a=fmtp:97 mode-change-capability=2; max-red=220
b=AS:30
b=RS:0
b=RR:0
a=rtpmap:98 telephone-event/8000/1
a=fmtp:98 0-15
a=ptime:20
a=maxptime:240
a=inactive
a=curr:qos local none
```

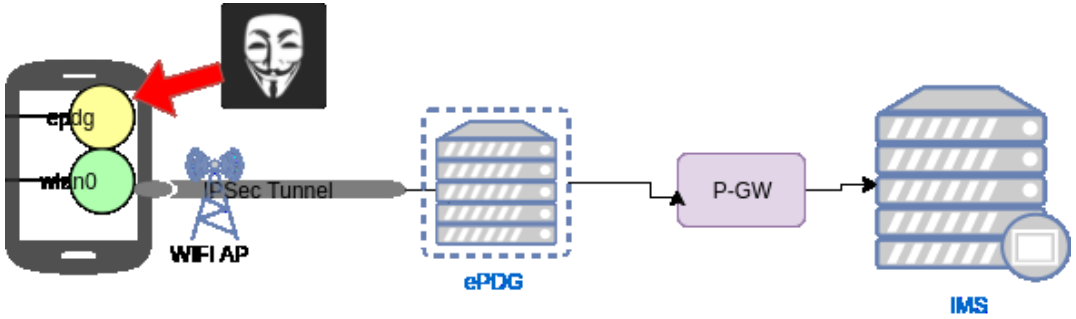
SIP

SDP

VoLTE sniffing



VoWiFi sniffing



Sniffing VoLTE/VoWiFi Interfaces

- VoLTE – rmnet1/rmnet0

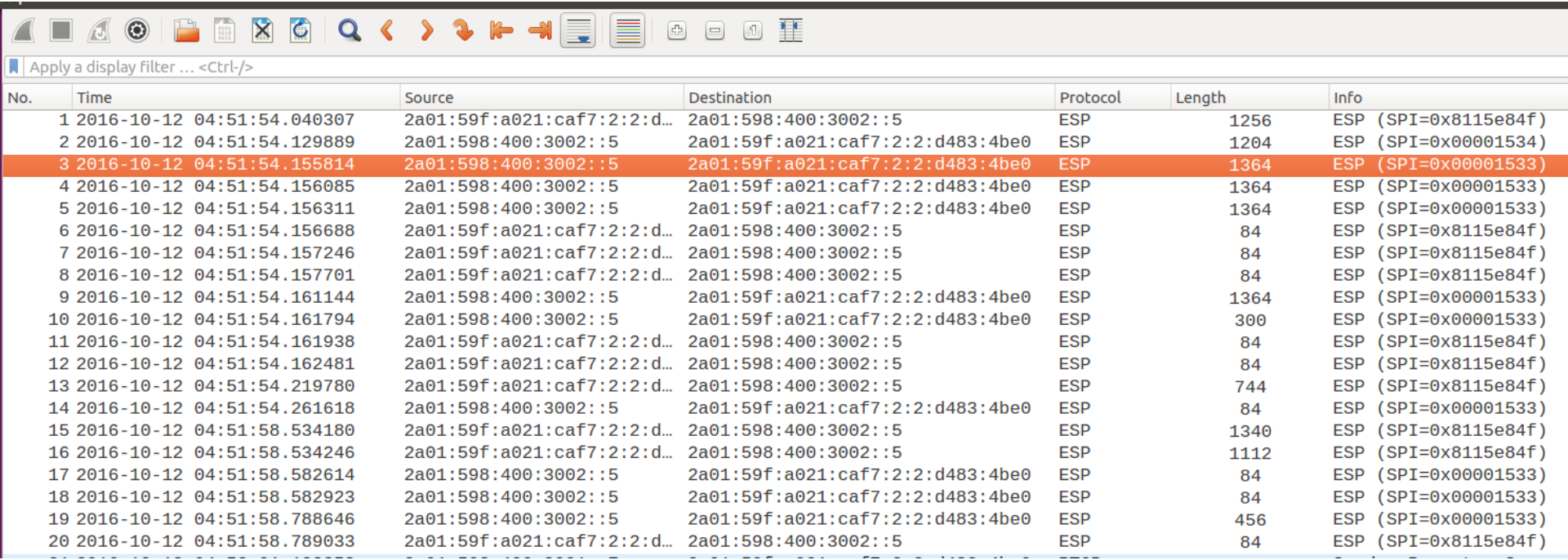
```
Sniffing VoLTE interface :
$ adb shell
$ tcpdump -i rmnet1 -n -s 0 -w - | nc -l 127.0.0.1 -p 11233
$ adb forward tcp:11233 tcp:11233 && nc 127.0.0.1 11233 | wireshark -k -S -i -
```

Getting the key

- Use SIMTrace to get the GSM Authenticate message
- In S6 Samsung, another trick

```
$ ip xfrm state
```

ESP Packets



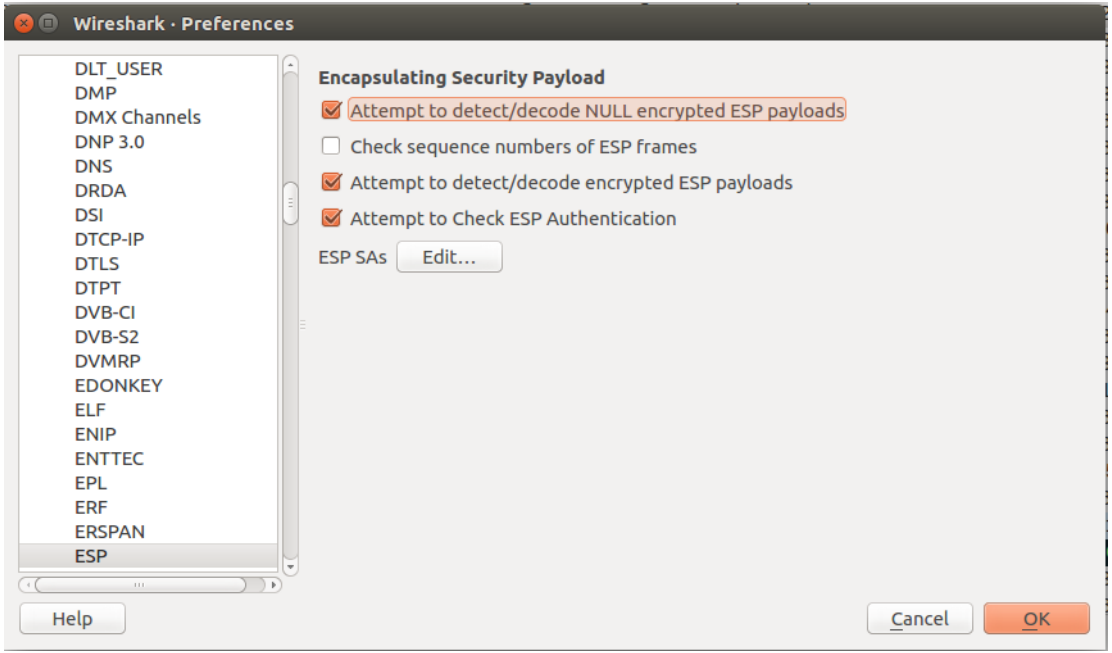
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	2016-10-12 04:51:54.040307	2a01:59f:a021:caf7:2:2:d…	2a01:598:400:3002::5	ESP	1256	ESP (SPI=0x8115e84f)
2	2016-10-12 04:51:54.129889	2a01:598:400:3002::5	2a01:59f:a021:caf7:2:2:d483:4be0	ESP	1204	ESP (SPI=0x00001534)
3	2016-10-12 04:51:54.155814	2a01:598:400:3002::5	2a01:59f:a021:caf7:2:2:d483:4be0	ESP	1364	ESP (SPI=0x00001533)
4	2016-10-12 04:51:54.156085	2a01:598:400:3002::5	2a01:59f:a021:caf7:2:2:d483:4be0	ESP	1364	ESP (SPI=0x00001533)
5	2016-10-12 04:51:54.156311	2a01:598:400:3002::5	2a01:59f:a021:caf7:2:2:d483:4be0	ESP	1364	ESP (SPI=0x00001533)
6	2016-10-12 04:51:54.156688	2a01:59f:a021:caf7:2:2:d…	2a01:598:400:3002::5	ESP	84	ESP (SPI=0x8115e84f)
7	2016-10-12 04:51:54.157246	2a01:59f:a021:caf7:2:2:d…	2a01:598:400:3002::5	ESP	84	ESP (SPI=0x8115e84f)
8	2016-10-12 04:51:54.157701	2a01:59f:a021:caf7:2:2:d…	2a01:598:400:3002::5	ESP	84	ESP (SPI=0x8115e84f)
9	2016-10-12 04:51:54.161144	2a01:598:400:3002::5	2a01:59f:a021:caf7:2:2:d483:4be0	ESP	1364	ESP (SPI=0x00001533)
10	2016-10-12 04:51:54.161794	2a01:598:400:3002::5	2a01:59f:a021:caf7:2:2:d483:4be0	ESP	300	ESP (SPI=0x00001533)
11	2016-10-12 04:51:54.161938	2a01:59f:a021:caf7:2:2:d…	2a01:598:400:3002::5	ESP	84	ESP (SPI=0x8115e84f)
12	2016-10-12 04:51:54.162481	2a01:59f:a021:caf7:2:2:d…	2a01:598:400:3002::5	ESP	84	ESP (SPI=0x8115e84f)
13	2016-10-12 04:51:54.219780	2a01:59f:a021:caf7:2:2:d…	2a01:598:400:3002::5	ESP	744	ESP (SPI=0x8115e84f)
14	2016-10-12 04:51:54.261618	2a01:598:400:3002::5	2a01:59f:a021:caf7:2:2:d483:4be0	ESP	84	ESP (SPI=0x00001533)
15	2016-10-12 04:51:58.534180	2a01:59f:a021:caf7:2:2:d…	2a01:598:400:3002::5	ESP	1340	ESP (SPI=0x8115e84f)
16	2016-10-12 04:51:58.534246	2a01:59f:a021:caf7:2:2:d…	2a01:598:400:3002::5	ESP	1112	ESP (SPI=0x8115e84f)
17	2016-10-12 04:51:58.582614	2a01:598:400:3002::5	2a01:59f:a021:caf7:2:2:d483:4be0	ESP	84	ESP (SPI=0x00001533)
18	2016-10-12 04:51:58.582923	2a01:598:400:3002::5	2a01:59f:a021:caf7:2:2:d483:4be0	ESP	84	ESP (SPI=0x00001533)
19	2016-10-12 04:51:58.788646	2a01:598:400:3002::5	2a01:59f:a021:caf7:2:2:d483:4be0	ESP	456	ESP (SPI=0x00001533)
20	2016-10-12 04:51:58.789033	2a01:59f:a021:caf7:2:2:d…	2a01:598:400:3002::5	ESP	84	ESP (SPI=0x8115e84f)

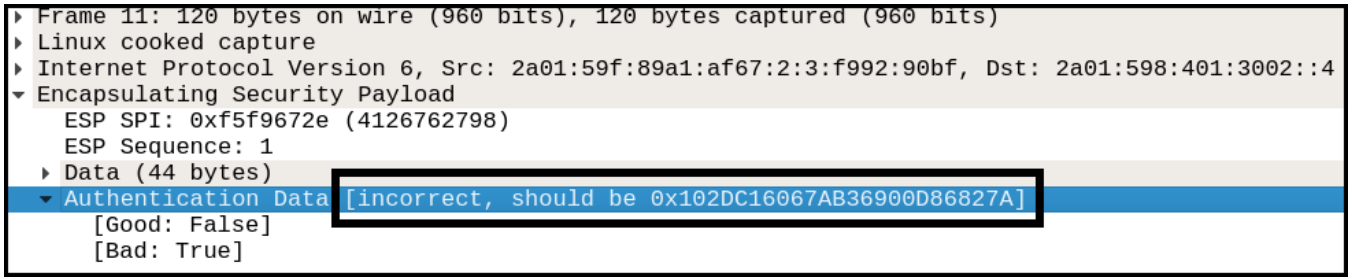
Decode ESP integrity check

- With the key obtained, verify if it the right key used in the packets

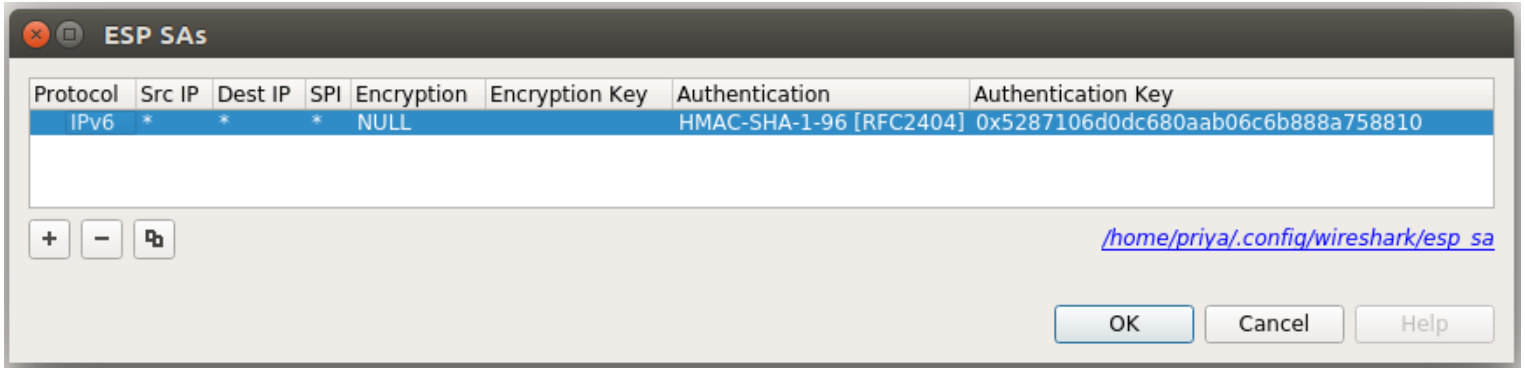
Are the keys used in ESP?



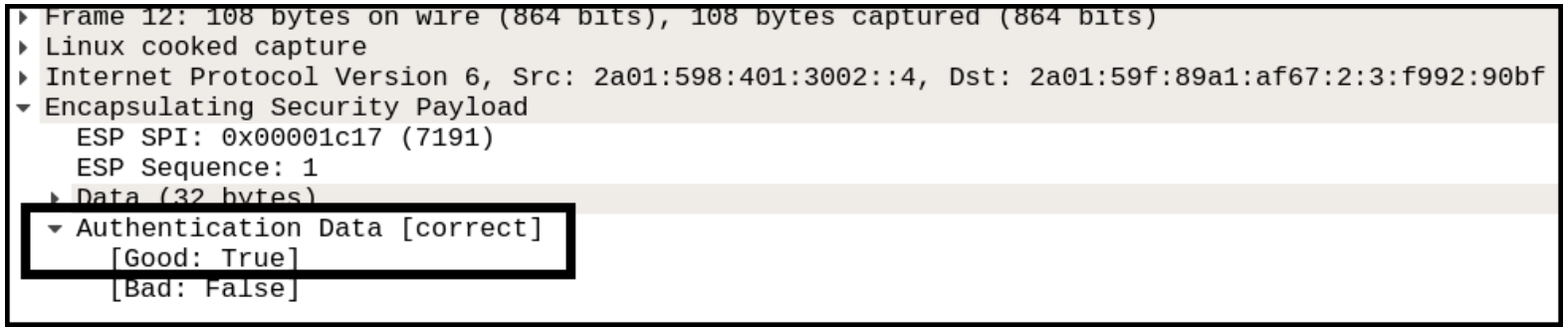
Failed authentication



Set up SA with obtained IK



Success: Key validation



ERNW
providing security.

schalakkal@ernw.de

www.ernw.de

@priyachalakkal

www.insinuator.net


```
##IPTABLES ON ANDROID TO ROUTE TRAFFIC TO LAPTOP AND BACK

iptables -F
iptables -t nat -F
echo 1 > /proc/sys/net/ipv4/ip_forward
RMNET=`ip addr show dev rmnet1 |grep -oE "([0-9]{1,3}\.){3}[0-9]{1,3}"`
WLAN=`ip addr show dev wlan0 | grep inet | grep -oE "([0-9]{1,3}\.){3}[0-9]{1,3}" | grep -v 255`
IMS="10.0.0.1"
MITM="192.168.0.2"
iptables -t nat -A OUTPUT -d $IMS -j DNAT  --to-destination $MITM
iptables -t nat -A POSTROUTING -o wlan0 -d $MITM   -j SNAT --to-source $WLAN
iptables -t nat -A POSTROUTING -o rmnet1 -s $MITM  -d $IMS -j SNAT --to-source $RMNET
iptables -t nat -L -vn
```

ERNW
providing security.

Security protocol: EAP-AKA