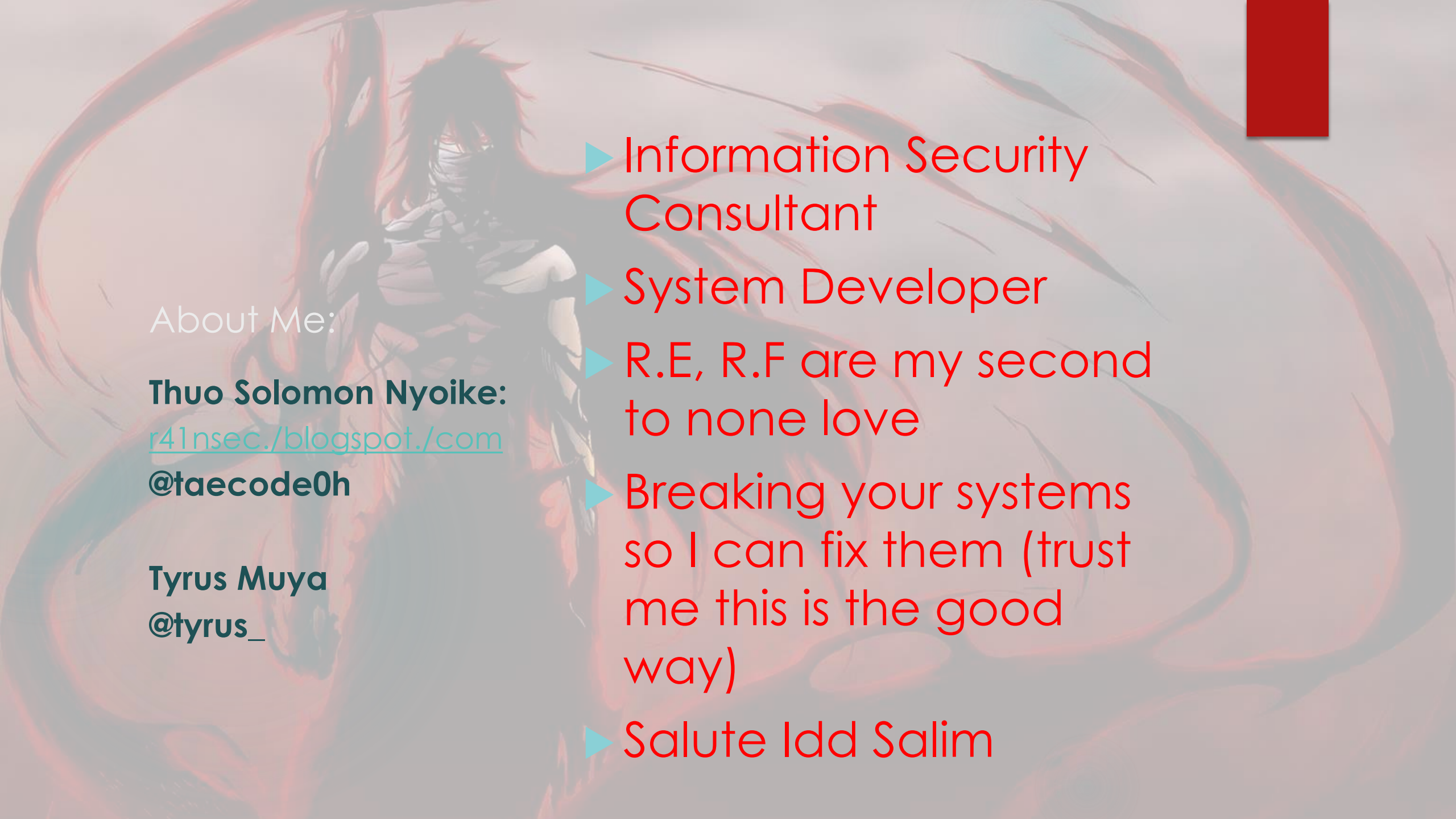
Radio-Frequency Analysis/Hacking and Securing

(GSM) SO YOU CAN QUOTE ME



About Me:

Thuo Solomon Nyoike:
r41nsec./blogspot./com
@taecode0h

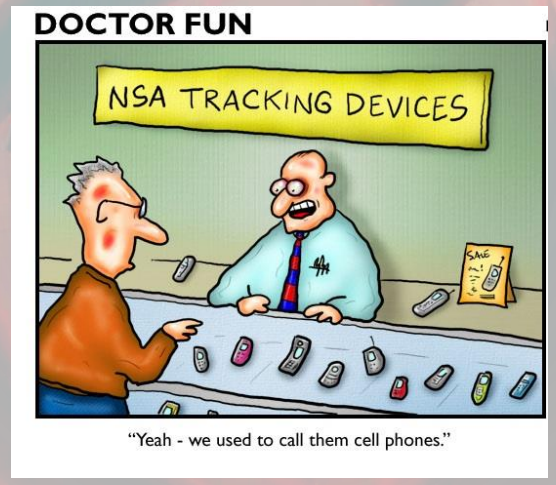
Tyrus Muya
@tyrus_

- Information Security Consultant
- System Developer
- R.E, R.F are my second to none love
- Breaking your systems so I can fix them (trust me this is the good way)
- Salute Idd Salim

GSM-Security: THE PERKS (WHEN YOU ~~HACK~~ ANALYSIS

CELL TRACKING

Can I show you how to track a person/suspect via GSM (this is also like the best way considering some of the phones don't have Wi-Fi or GPS)



DATA SNIFFING

Ok now after we find the Guy can we listen to his conversations? SMS, Voice ,GPRS

MITM Attacks

Ok good, now what about a little Attack say MITM? Spoof Data, Impersonation? I don know….umm update the STA

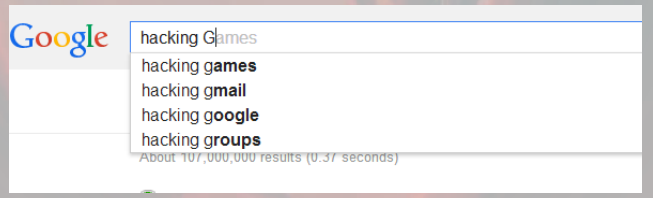
Where to start: Well Mostly

RF Security is not so common doubt me ask google

WHY : COZ TOOLS ARE EXPENSIVE AND NOT EASY TO PROCURE:

AND THE KNOWLEDGE NOT SO COMMON OR USER FRIENDLY

WORST BIT , LICENCES NOT CHEAP/ NOT EASY FOR DEVELOPERS AND RESEARCHERS



HOW BIG IS RF SPECIFICALLY GSM

GSM is used by ove 70% of the worlds mobile communication platform hence a span of nearly 3 billion users globally… big number?

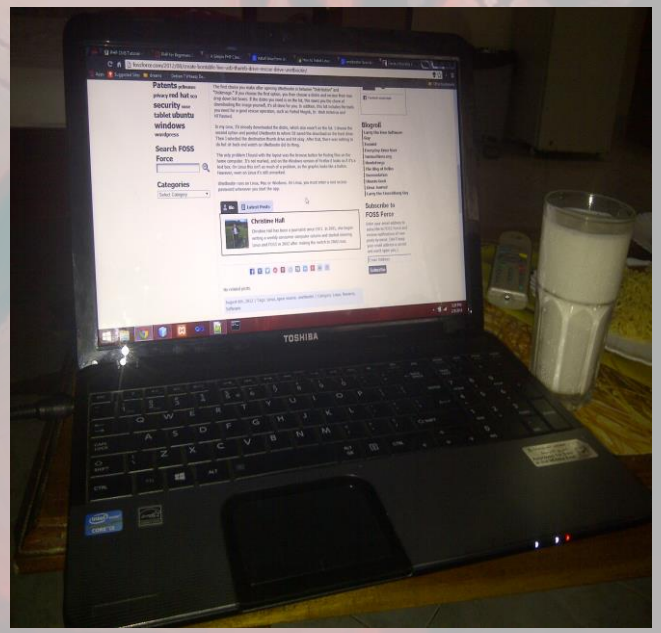
Hence a very huge impact if anything insecure was to happen.

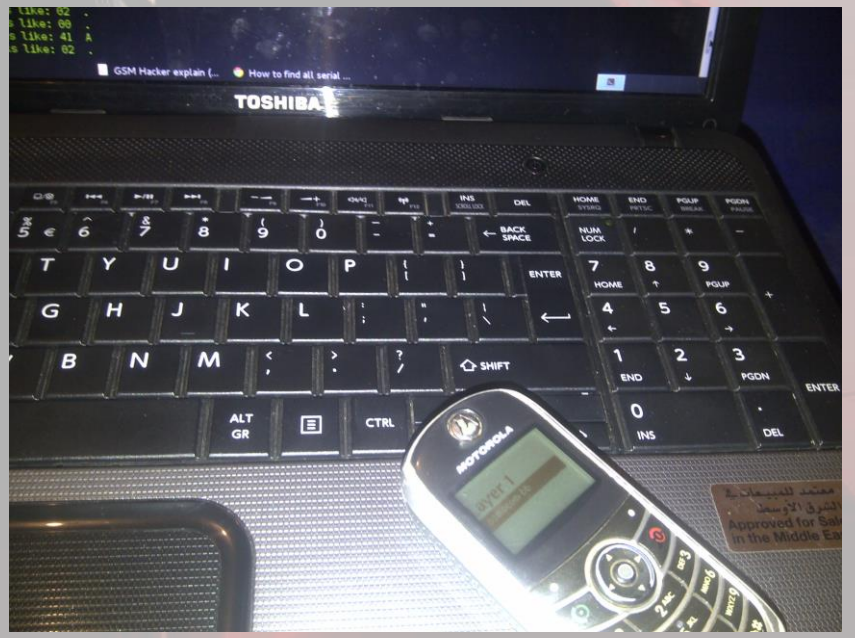
Lets start hacking and forget the boring talk.

So Tools

- A laptop
- Software----- Any Linux/BSD Variant, OsmocomBB Firmware
- A calypso based device e.g

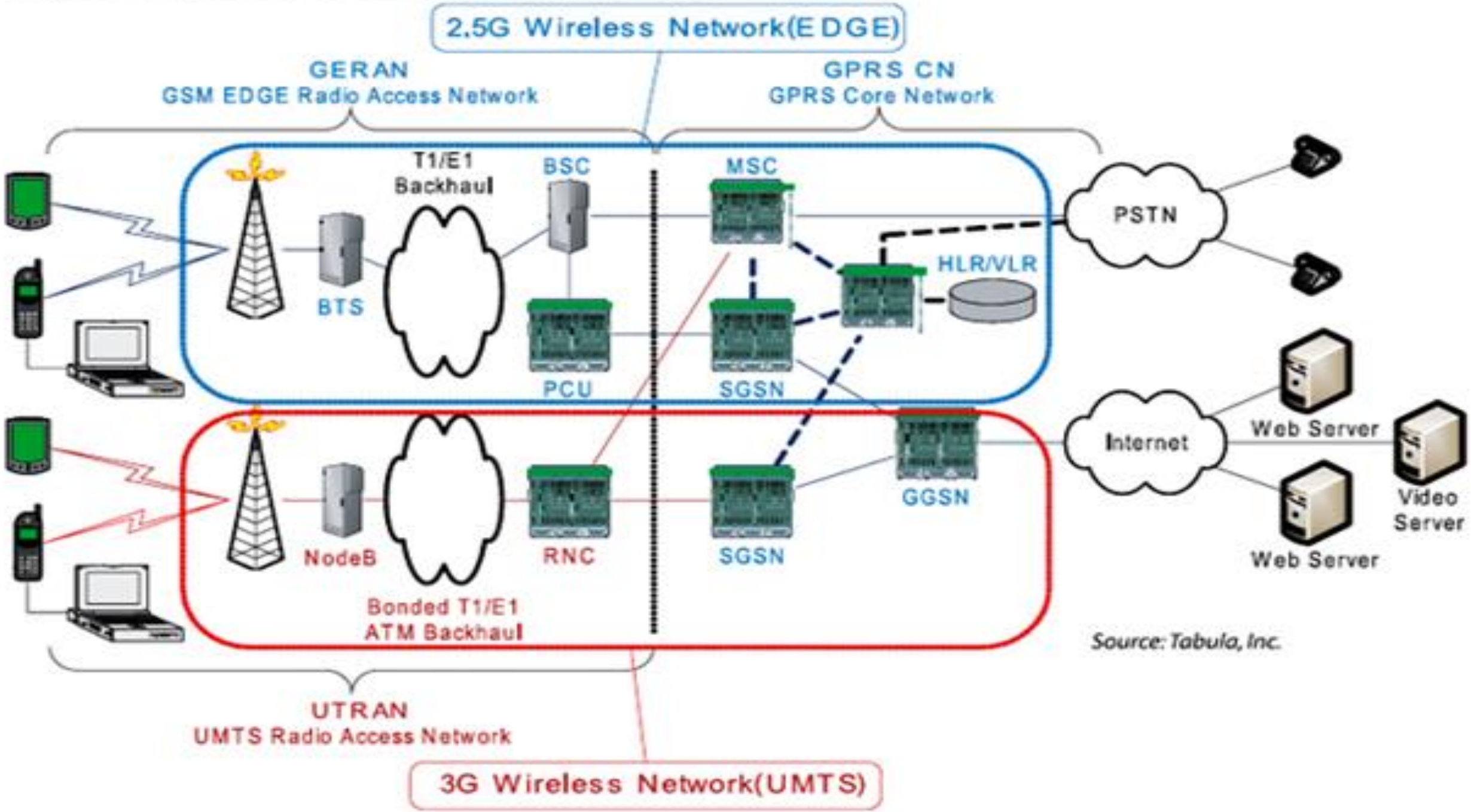
Motorola C113,C115,C118,C123,C126





Your Brain Goes Here

Figure 2: Wireless Network transition from 2.5G to 3G



So Locating our Victim

- First things first
- MS-Mobile Station
- BTS-Base Transmission Station
- ARFCN-absolute radio-frequency channel number
- IMSI-International mobile Subscriber Identity
- TMSI-Temporary Mobile Subscriber Identity

So What we will be Seeing

- The Phone Number (well not really) But we can resolve an IMSI or a TMSI to that

- AN IMSI ☺
- 639020987654321
- Very unique* and is specific to every SIM (Mobile Subscribers)

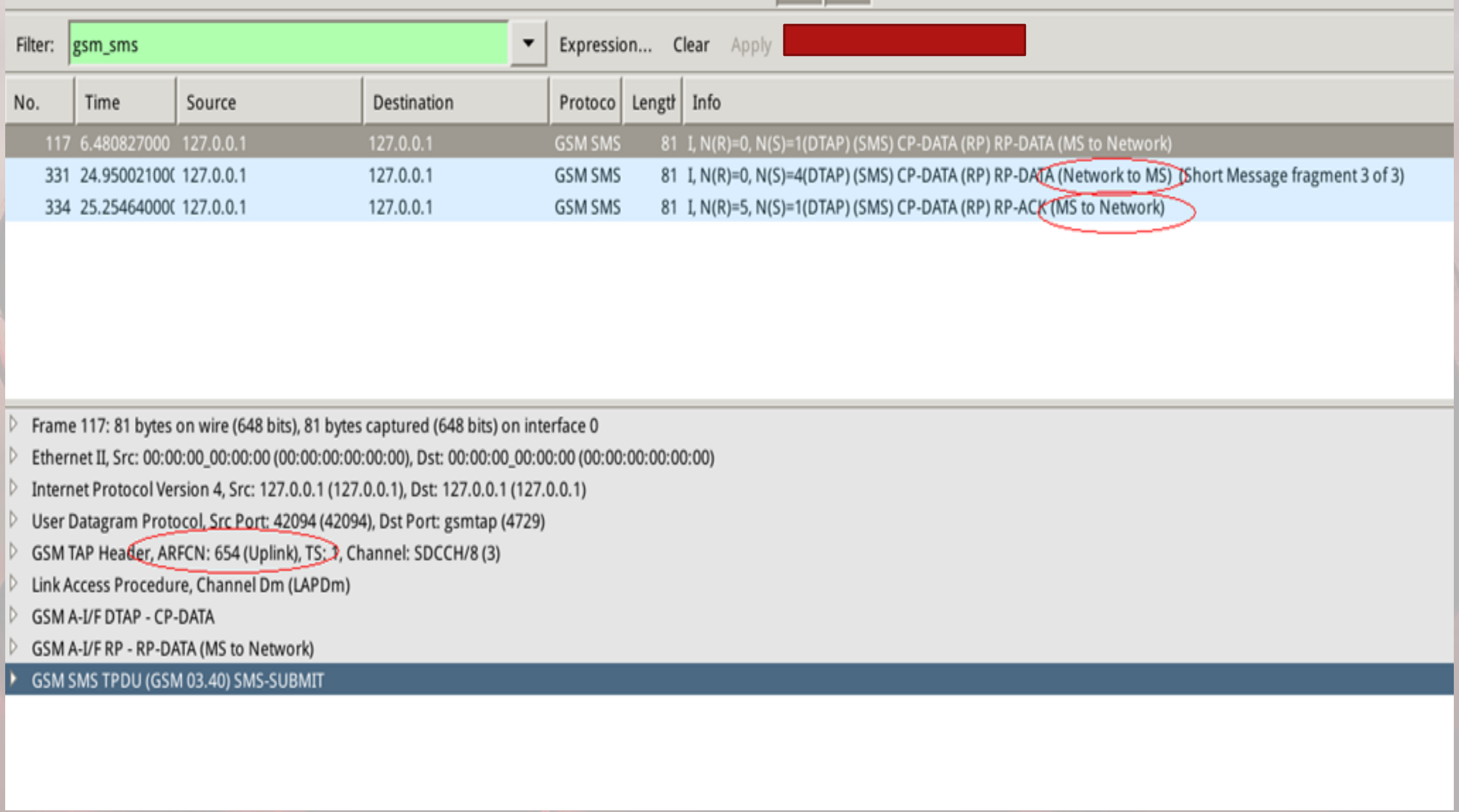
- So our modified version of the very expensive* device.

PRACTICAL BIT

Capturing Data

- **Capturing SMS**
- **Capturing Voice**
- **Capturing GPRS data**

- **Well am not going to show you that ☺**
- **Ok maybe let me show you one that I did on MY phone**


Filter: gsm_sms
Expression... Clear Apply
No. Time Source Destination Protoco Lengtl Info
117 6.480827000 127.0.0.1 127.0.0.1 GSM SMS 81 I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
331 24.95002100(127.0.0.1 127.0.0.1 GSM SMS 81 I, N(R)=0, N(S)=4(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS) (Short Message fragment 3 of 3)
334 25.25464000(127.0.0.1 127.0.0.1 GSM SMS 81 I, N(R)=5, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-ACK (MS to Network)
Frame 117: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
User Datagram Protocol, Src Port: 42094 (42094), Dst Port: gsmtap (4729)
GSM TAP Header, ARFCN: 654 (Uplink), TS: 1, Channel: SDCCH/8 (3)
Link Access Procedure, Channel Dm (LAPDm)
GSM A-I/F DTAP - CP-DATA
GSM A-I/F RP - RP-DATA (MS to Network)
GSM SMS TPDU (GSM 03.40) SMS-SUBMIT

IMPLICATIONS

- I KNOW WHERE YOU ARE
- I KNOW WHAT YOU ARE SAYING
- I CAN IMERSONATE YOU
- I CAN DO AN MITM
- In short YOU are NOT SECURE

Remediation

- **Talk to us ☺**