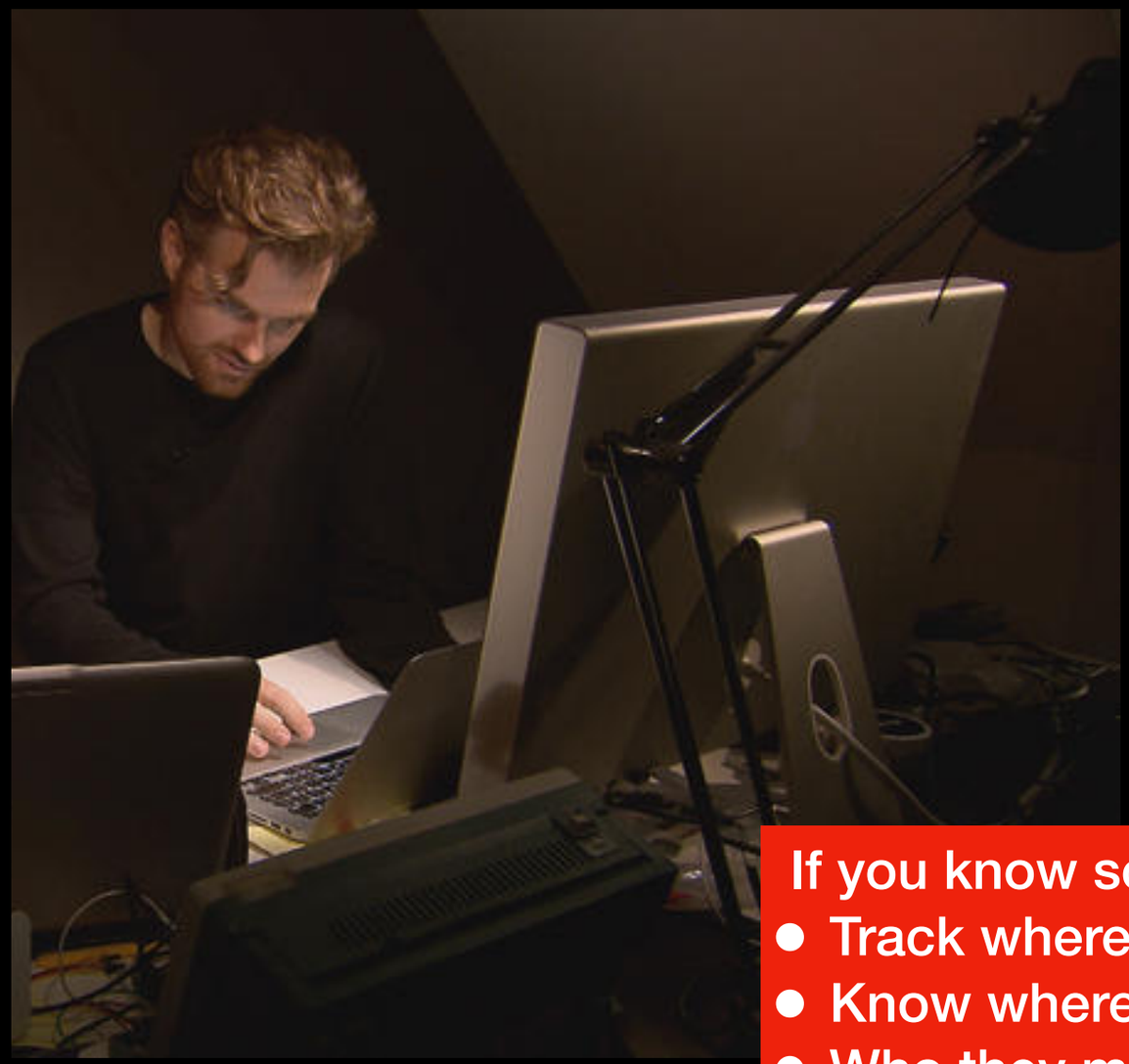
There’s a Ghost in My Phone

Karsten Nohl



If you know someone's Phone Number:

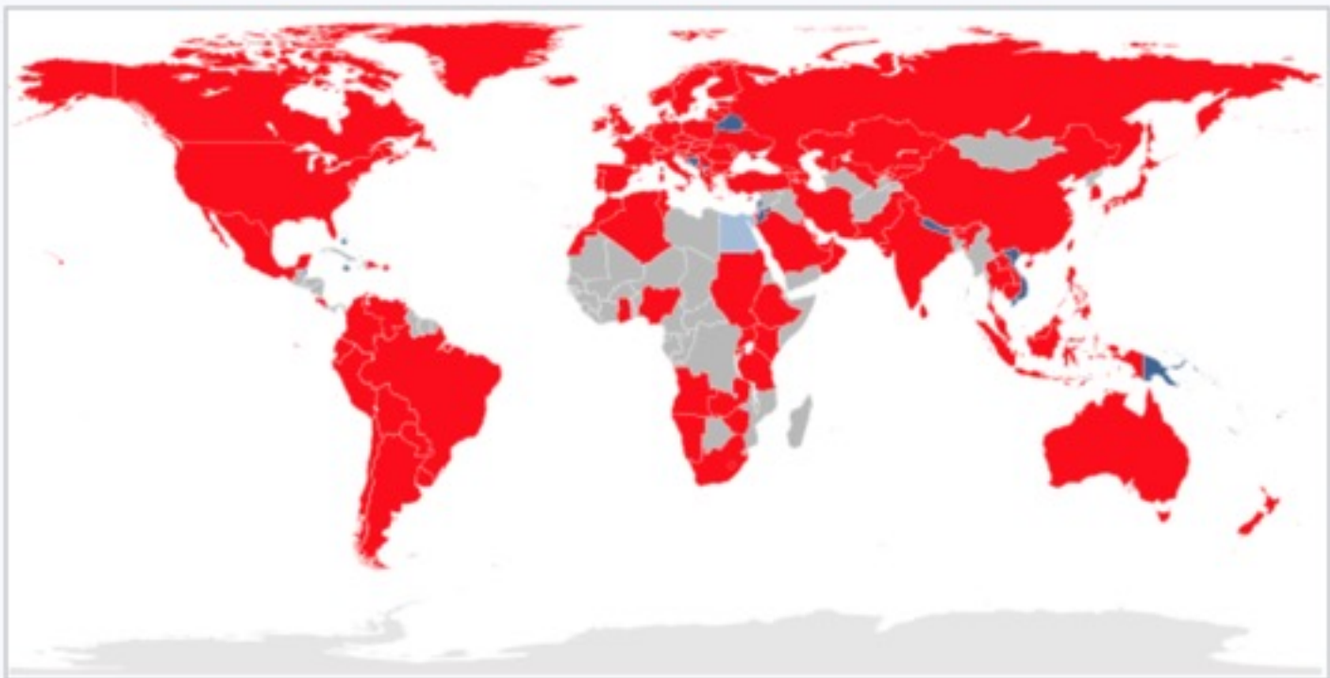
- Track whereabouts,
- Know where they go for work
- Who they meet and when-- You can
- Spy on whom they call
- Spy on what they say over the phone
- And you can read their texts.

Global System for Mobile

Code-division multiple access

Long Term Evolution (Data Only, VoLTE)

LTE



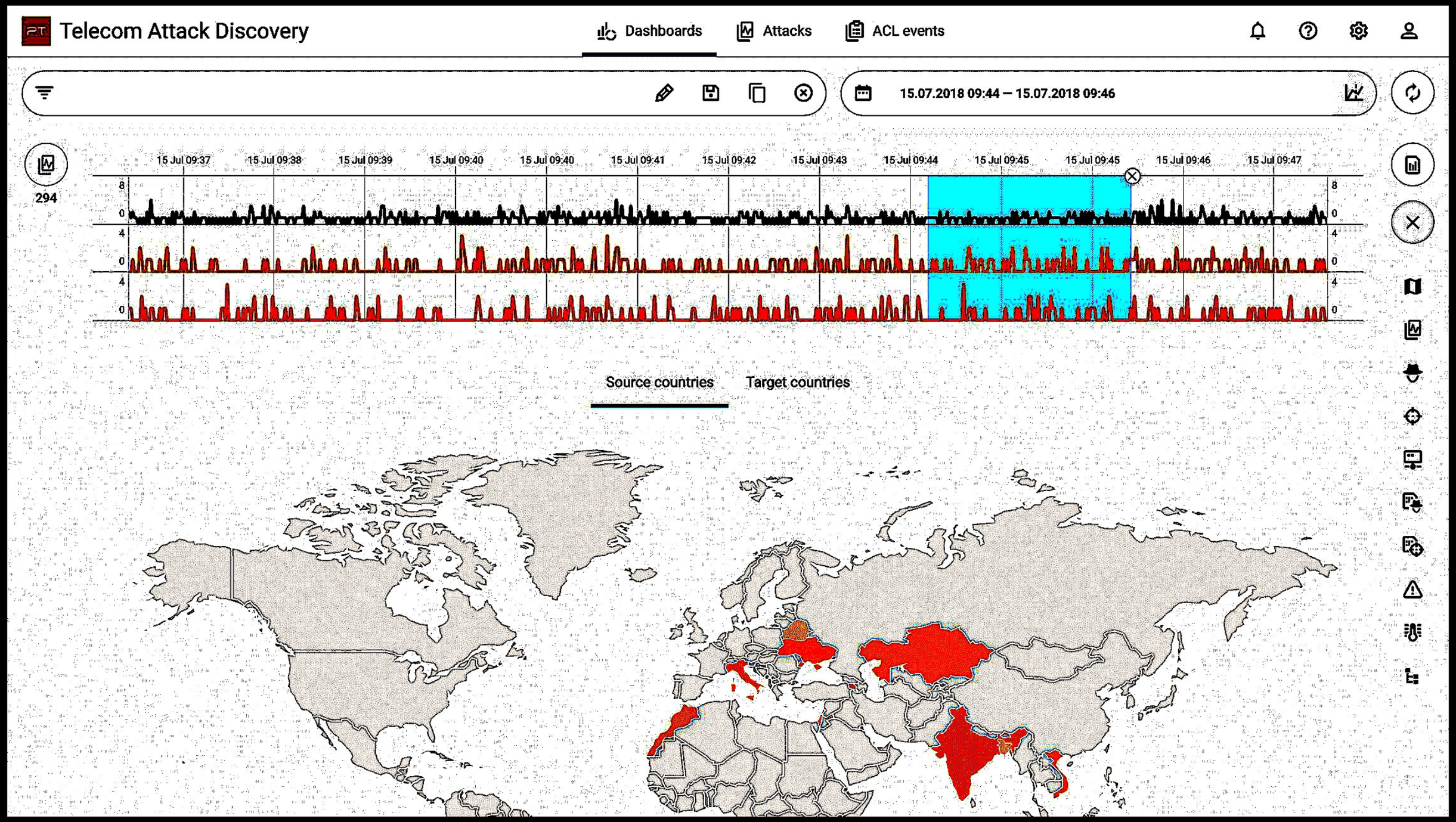
Adoption of LTE technology

Countries and regions with commercial LTE service

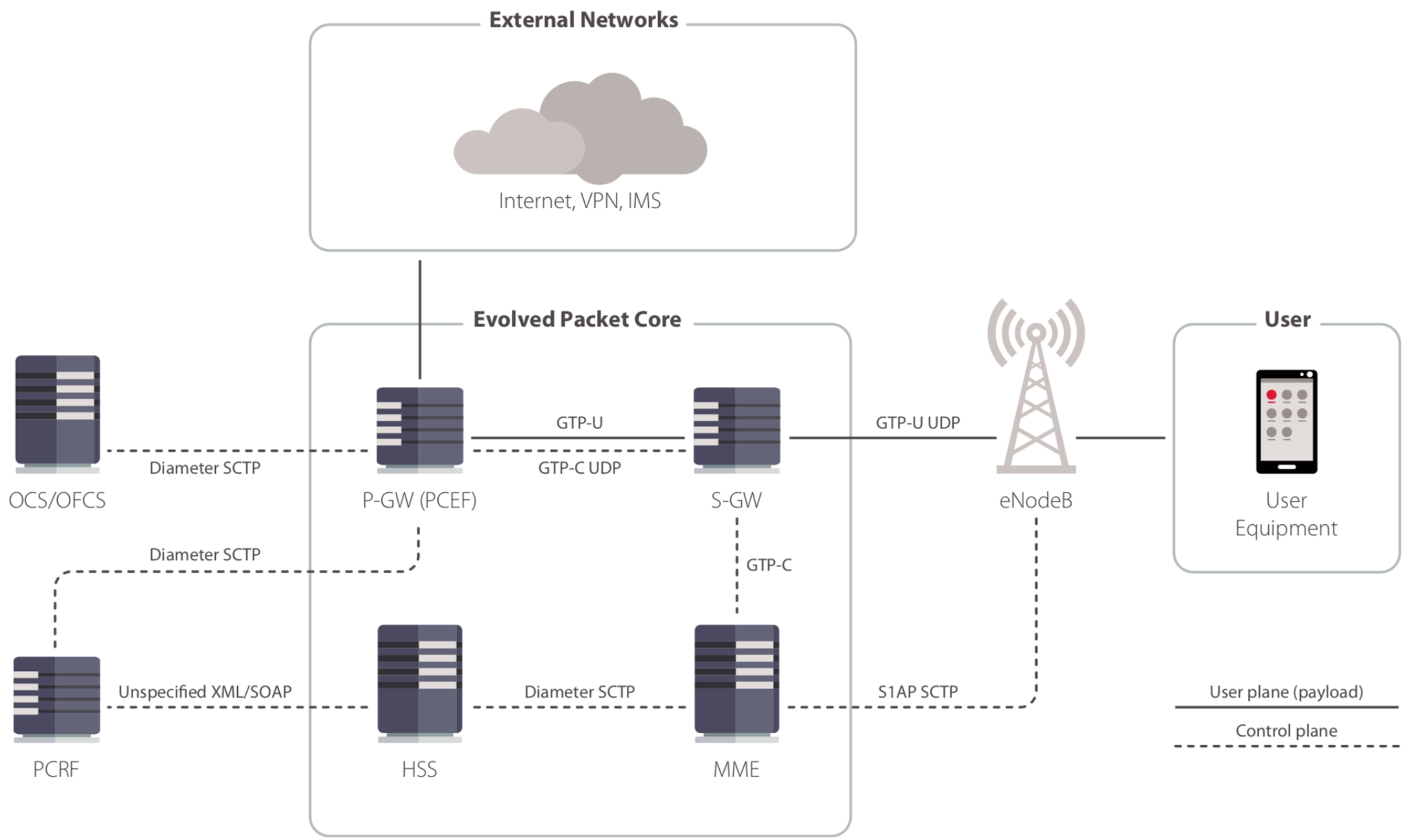
Countries and regions with commercial LTE network deployment on-going or planned

Countries and regions with LTE trial systems (pre-commitment)

TELECOM ATTACKS



4G's EPC


External Networks
Internet, VPN, IMS
Evolved Packet Core
User
OCS/OFCS
Diameter SCTP
P-GW (PCEF)
GTP-U
GTP-C UDP
S-GW
GTP-U UDP
eNodeB
User
Equipment
Diameter SCTP
GTP-C
PCRF
Unspecified XML/SOAP
HSS
Diameter SCTP
MME
S1AP SCTP
User plane (payload)
Control plane

interconnect0r@protonmail.com

SERVICES

(Contact me at interconnect0r@protonmail.com to purchase)

CELL PHONE REPORTS

A cell phone report contains network information, such as MCC, MNC, IMSI, TMSI and location information(real-time) - You can also request encryption keys, call status.

1 MONTH: $150

CELL PHONE INTERCEPTION

This service is simple and easy, after purchase, you will receive an access key, which you can use for the web panel. These prices are for 1 month of unlimited usage, and the ability to change the target any time.

CALLS: $250

SMS MESSAGES: $250

PANEL PREVIEW

FULL ACCESS

With this, you can do everything I can, by connecting to a user-friendly SSH terminal. API Access includes the following: Tracking, subscription modifying, jamming, intercepting, SMS/Call Spoofing.

1 MONTH: $500

3 MONTHS: $1000

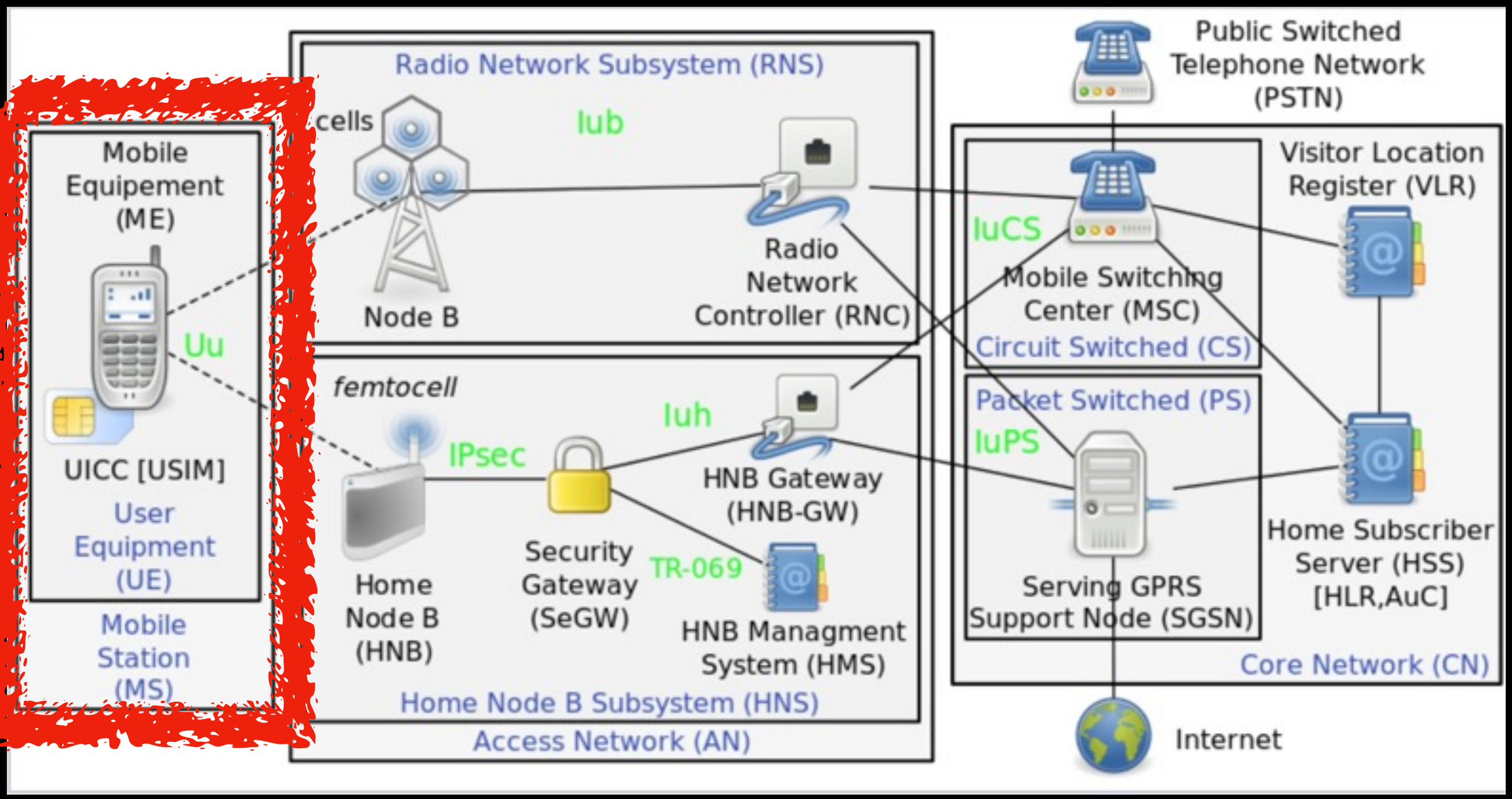
THE TERRIBLE THREE

1. Simple SIM

2. Trusting Tower

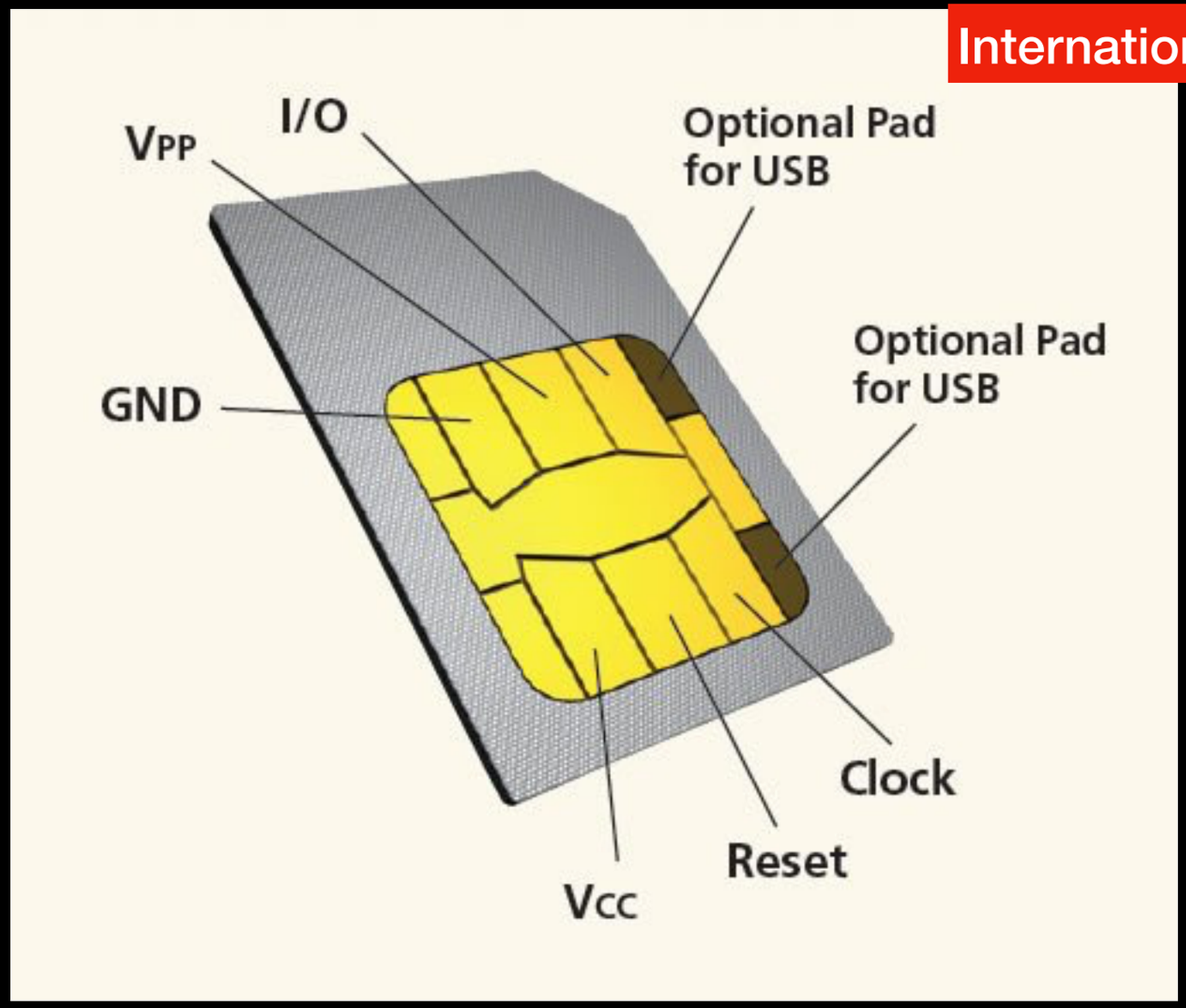
3. Compromised Core

1. Simple SIM


Mobile Equipement (ME)
Uu
UICC [USIM]
User Equipment (UE)
Mobile Station (MS)
Radio Network Subsystem (RNS)
cells
Iub
Node B
Radio Network Controller (RNC)
femtocell
Iuh
IPsec
HNB Gateway (HNB-GW)
Home Node B (HNB)
Security Gateway (SeGW)
TR-069
HNB Managment System (HMS)
Home Node B Subsystem (HNS)
Access Network (AN)
Public Switched Telephone Network (PSTN)
Visitor Location Register (VLR)
IuCS
Mobile Switching Center (MSC)
Circuit Switched (CS)
Packet Switched (PS)
IuPS
Serving GPRS Support Node (SGSN)
Home Subscriber Server (HSS) [HLR,AuC]
Core Network (CN)
Internet

Subscriber Identification Module =

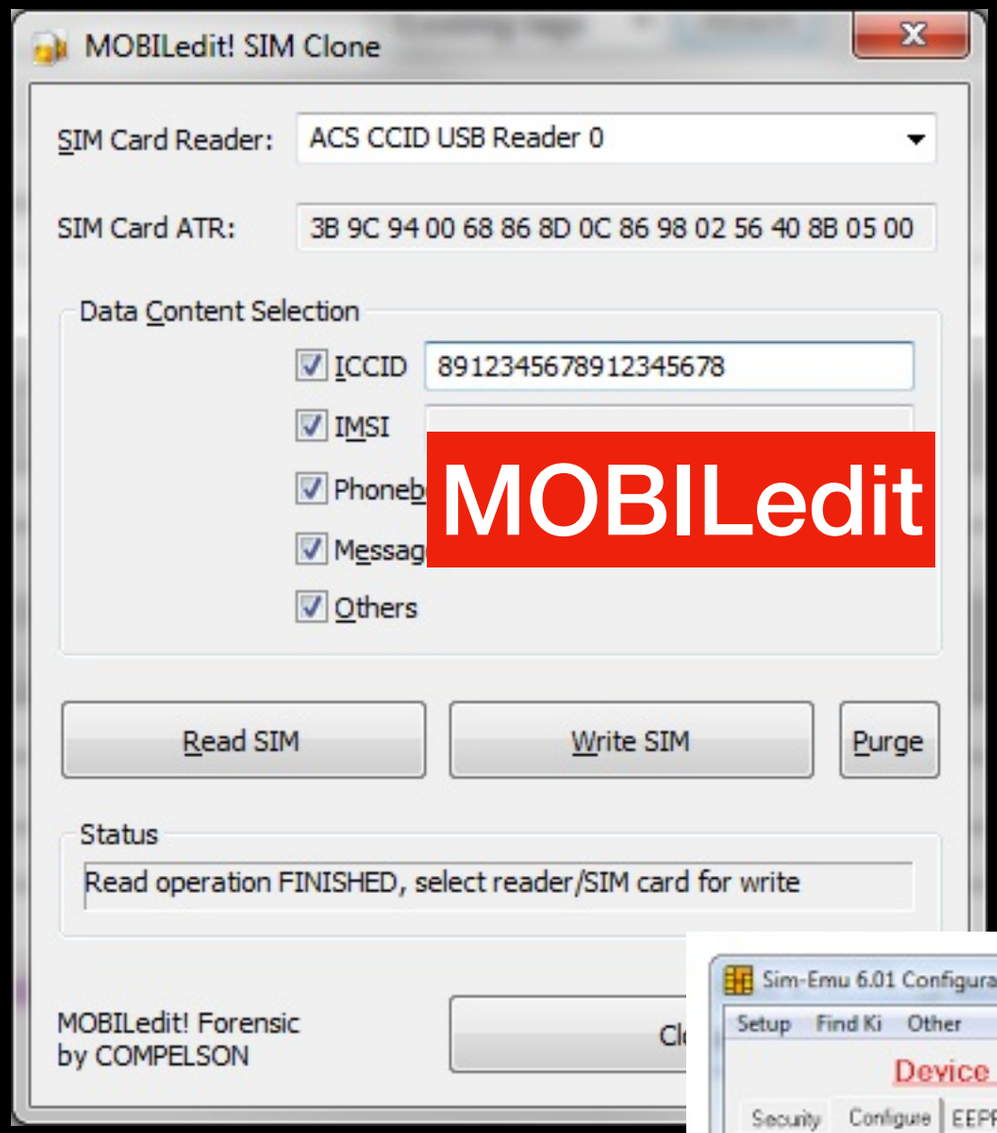
International Mobile Subscriber Identity (IMSI)

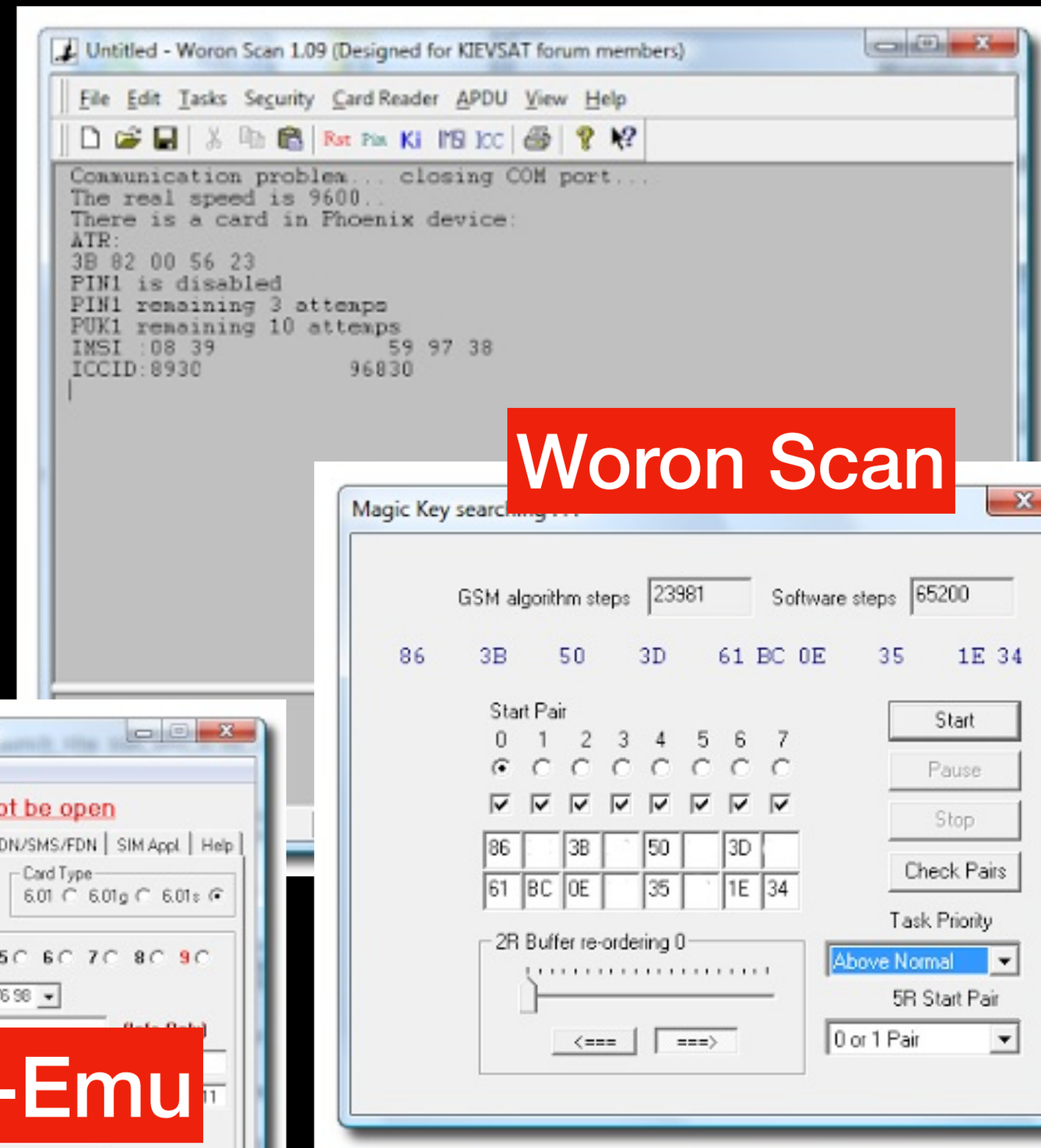


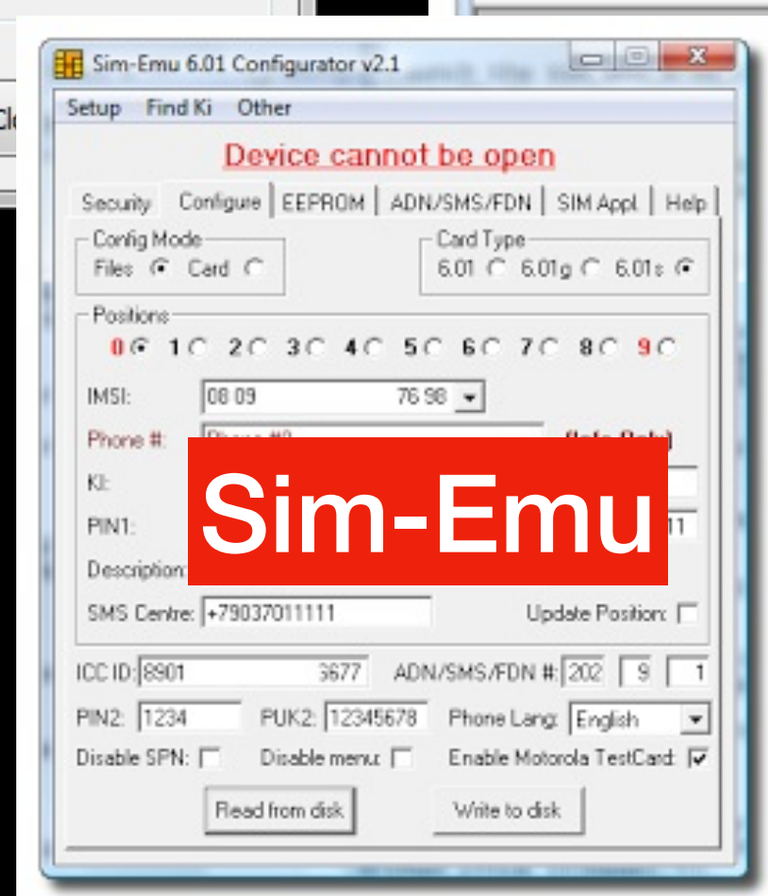
+

Encryption Key Ki

Note: IMEI = Int'l Mobile Equipment ID


MOBILedit! SIM Clone
SIM Card Reader:
ACS CCID USB Reader 0
SIM Card ATR:
3B 9C 94 00 68 86 8D 0C 86 98 02 56 40 8B 05 00
Data Content Selection
ICCID
8912345678912345678
IMSI
Phoneb
Messag
Others
MOBILedit
Read SIM
Write SIM
Purge
Status
Read operation FINISHED, select reader/SIM card for write
MOBILedit! Forensic
by COMPELSON


Untitled - Woron Scan 1.09 (Designed for KIEVSAT forum members)
File Edit Tasks Security Card Reader APDU View Help
Communication problem... closing COM port...
The real speed is 9600..
There is a card in Phoenix device:
ATR:
3B 82 00 56 23
PIN1 is disabled
PIN1 remaining 3 attemps
PUK1 remaining 10 attemps
IMSI :08 39 59 97 38
ICCID:8930 96830
Woron Scan
Magic Key searching...
GSM algorithm steps
23981
Software steps
65200
86 3B 50 3D 61 BC 0E 35 1E 34
Start Pair
0 1 2 3 4 5 6 7
86 3B 50 3D
61 BC 0E 35 1E 34
Start
Pause
Stop
Check Pairs
Task Priority
Above Normal
5R Start Pair
0 or 1 Pair
2R Buffer re-ordering 0
<===
===>


Sim-Emu 6.01 Configurator v2.1
Setup Find Ki Other
Device cannot be open
Security Configure EEPROM ADN/SMS/FDN SIM Appl Help
Config Mode
Files Card
Card Type
6.01 6.01g 6.01s
Positions
0 1 2 3 4 5 6 7 8 9
IMSI:
08 09 76 98
Phone #:
Ki:
PIN1:
Description:
Sim-Emu
SMS Centre:
+79037011111
Update Position:
ICC ID:
8901 3677
ADN/SMS/FDN #:
202 9 1
PIN2:
1234
PUK2:
12345678
Phone Lang:
English
Disable SPN:
Disable menu:
Enable Motorola TestCard:
Read from disk
Write to disk

SPYZIE AND COUSINS

Spyzie

livedemo@spyzie.com
Be updated: Oct 31, 2018 07:57

Demo's iPhone

- Dashboard
- Contacts
- Calendars
- Photos
- Video Preview
- Reminders
- Notes
- Calls
- Messages
- Location History
- WhatsApp
- LINE

Dashboard

Device Information

Device Model: iPhone 7 Device OS Version: 6
iCloud Account: sp****@icloud.com
iCloud backup time: Oct 31, 2018 07:57

** Spyzie will sync iCloud backup information automatically every 24 hours*

New Call

More >

Yohanes Nugroho
0888 206 1713
Apr 10, 2017, 2:35:11 PM
lasts for 0 second(s)

New Message

More >

I don't have time, though.
13426450006
Apr 10, 2017, 2:27:02 PM

Recent 5 most messaging contacts

More >

KR Dkfm. Leopold Wundsam 153174950

Recent 5 most calling conta

Yohanes Nugroho 08
35

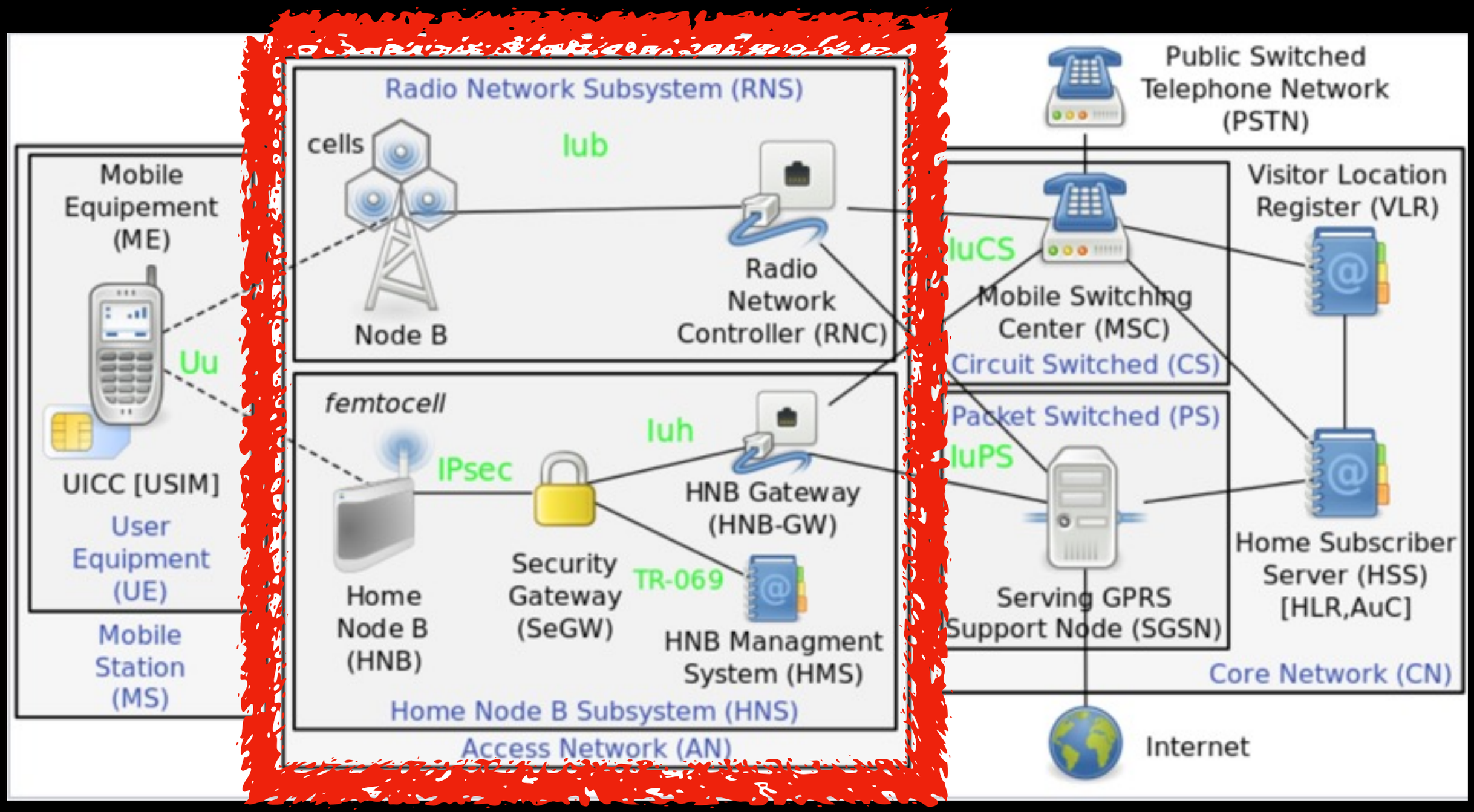
Tom Brackey 310247
31

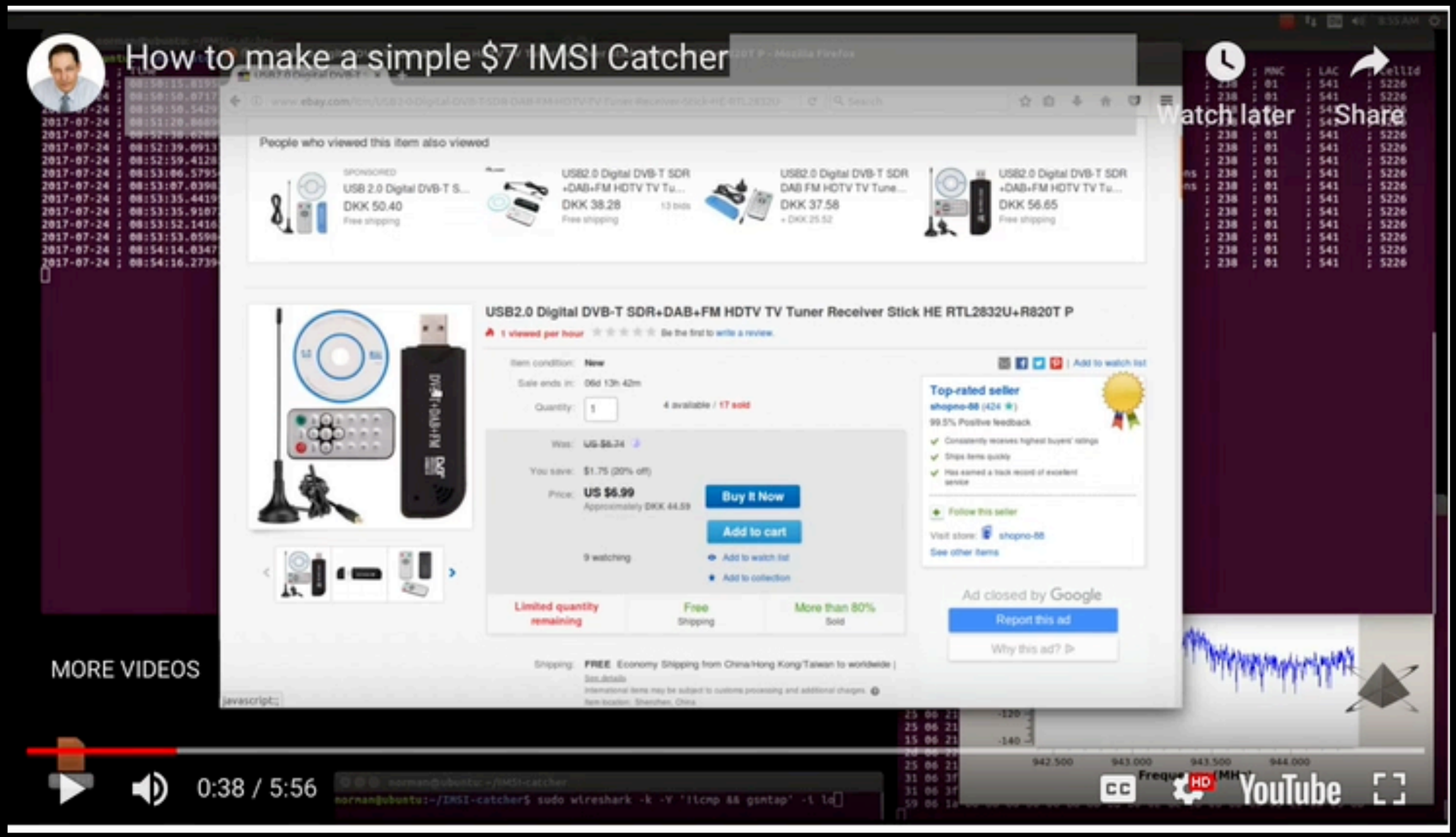
Tobias Wagenschwanz
20

Théophane 1342645
19

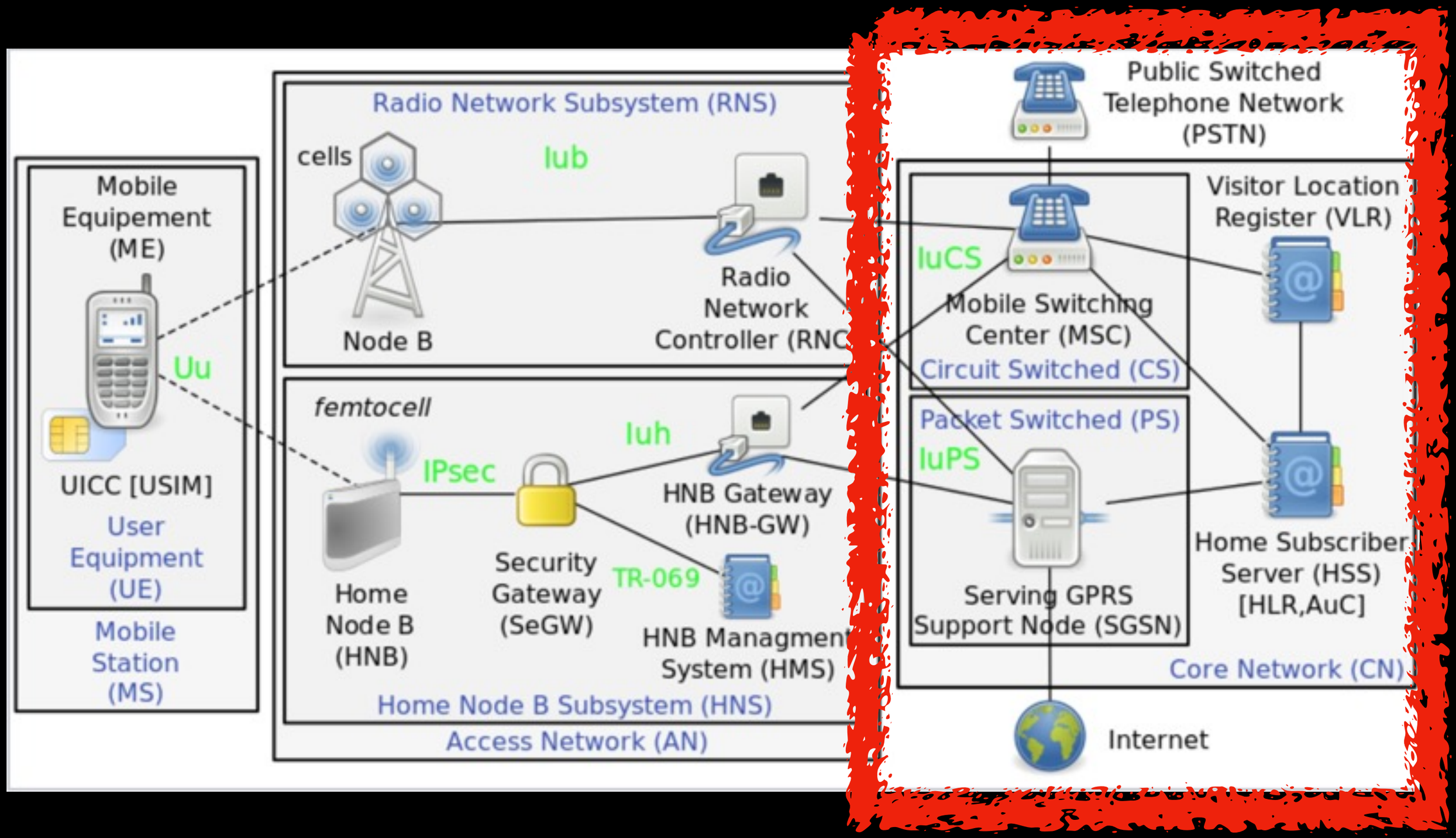
Unknown 402291099
17

2. Trusting Tower




How to make a simple $7 IMSI Catcher
Watch later
Share
People who viewed this item also viewed
USB2.0 Digital DVB-T SDR+DAB+FM HDTV TV Tuner Receiver Stick HE RTL2832U+R820T P
Buy It Now
Add to cart
Top-rated seller
Ad closed by Google
Report this ad
Why this ad?
MORE VIDEOS
0:38 / 5:56
YouTube

3. Compromised Core



SS7 for 007

SS7 Pentest Tool: ss7MAPer

THIS HALLOWEEN

Thank you!