EXPLORING LTE SECURITY AND PROTOCOL EXPLOITS WITH OPEN SOURCE SOFTWARE AND LOW-COST SOFTWARE RADIO

Roger Piqueras Jover

rpiquerasjov@bloomberg.net

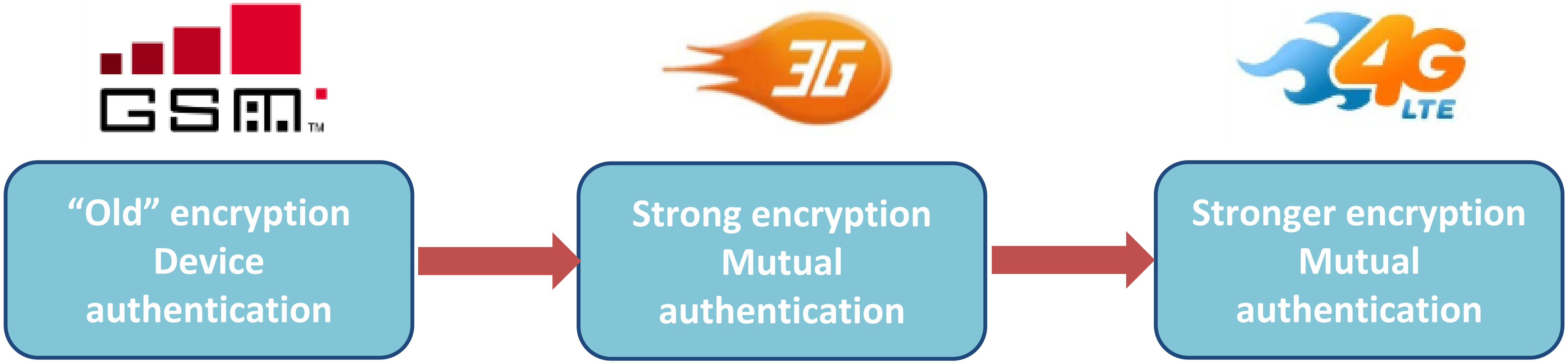
Bloomberg

ABOUT ME

- Wireless Security Researcher (aka Security Architect) at Bloomberg LP
  - http://www.bloomberg.com/company/announcements/mobile-security-a-conversation-with-roger-piqueras-jover/
- Formerly (5 years) Principal Member of Technical Staff at AT&T Security Research
  - http://src.att.com/projects/index.html
- Mobile/wireless network security research
  - LTE security and protocol exploits
  - Advanced radio jamming
  - Control plane signaling scalability in mobile networks
  - 5G mobile networks and new mobile core architectures
- If it communicates wirelessly, I am interested in its security
  - Bluetooth and BLE
  - 802.11
  - Zigbee, Zigwave
  - LoRa, SigFox…
  - GPS spoofing
- More details
  - http://www.ee.columbia.edu/~roger/ @rgoestotheshows

MOBILE NETWORK SECURITY

The first mobile networks were not designed with a strong security focus (no support for encryption in 1G!!!)



"Old" encryption
Device authentication

Strong encryption
Mutual authentication

Stronger encryption
Mutual authentication

Basic security principles

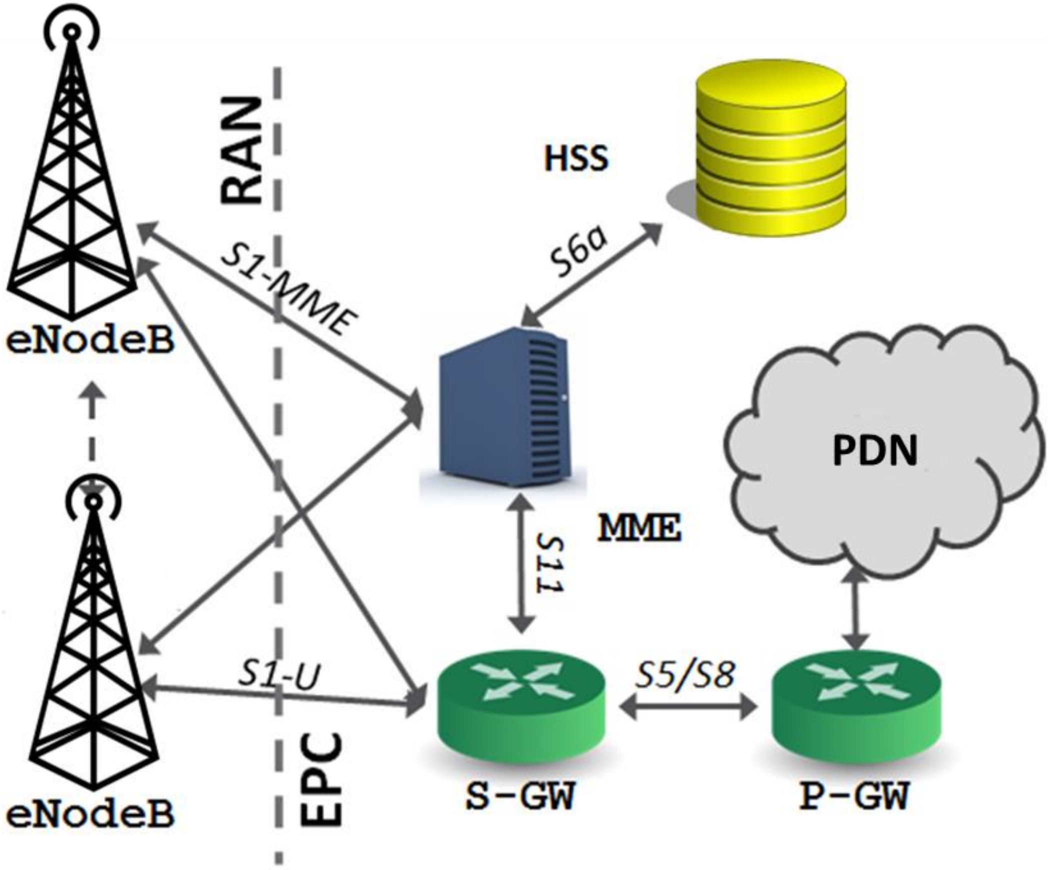
- Confidentiality ✓
- Authentication ✓
- Availability

Protecting user data

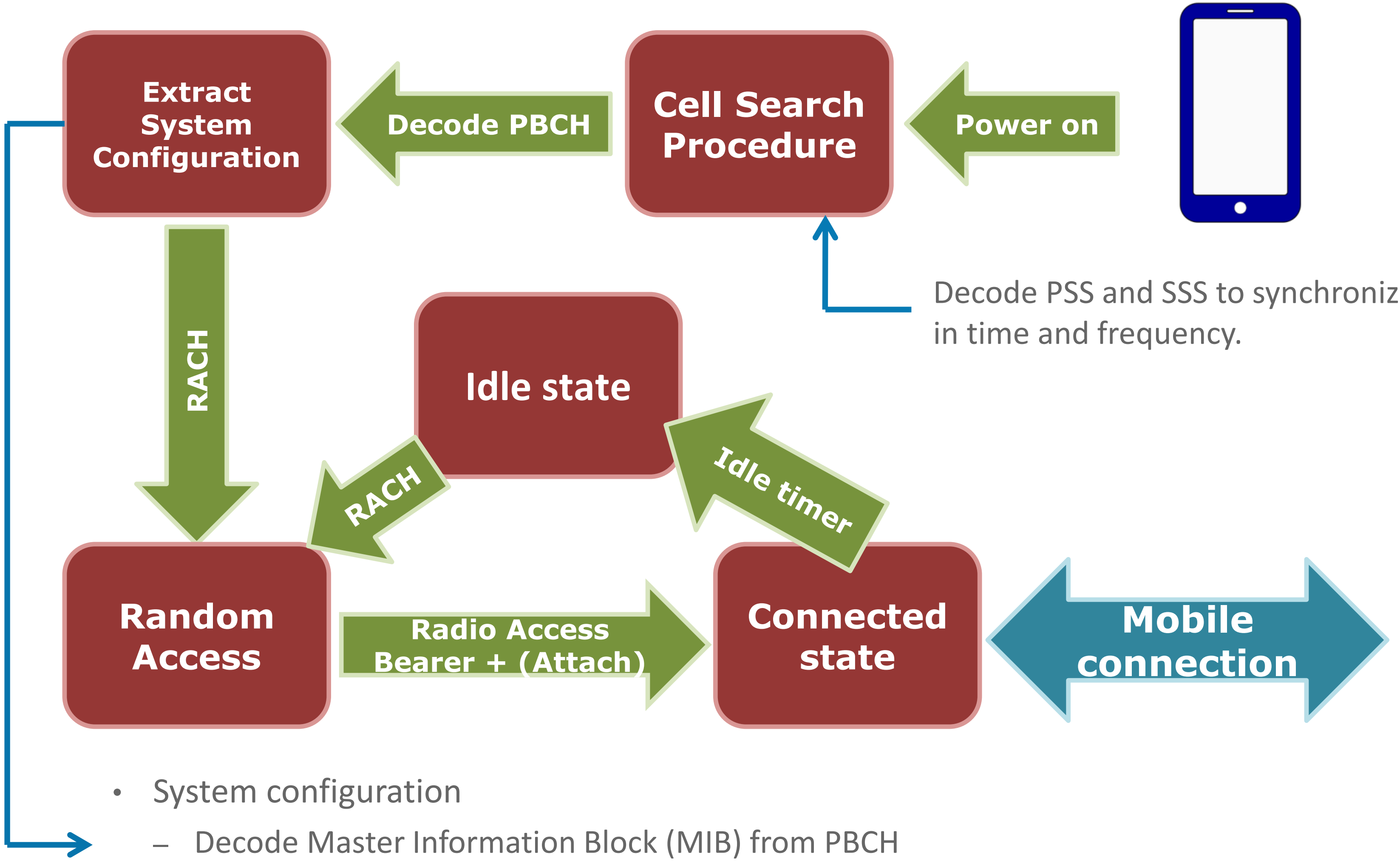
Mobile connectivity availability against security threats

LTE BASICS

LTE MOBILE NETWORK ARCHITECTURE



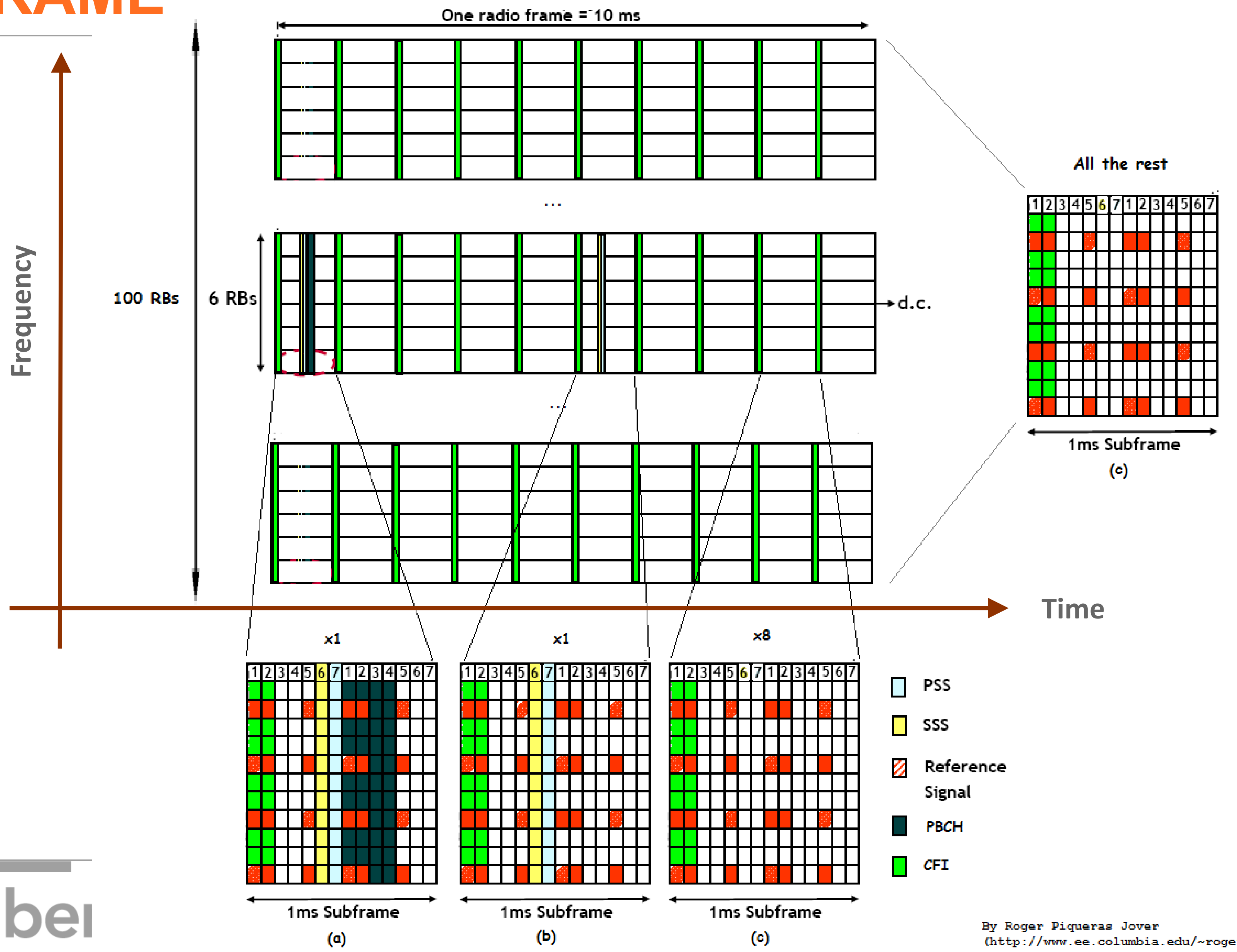
LTE CELL SELECTION AND CONNECTION



Decode PSS and SSS to synchronize in time and frequency.

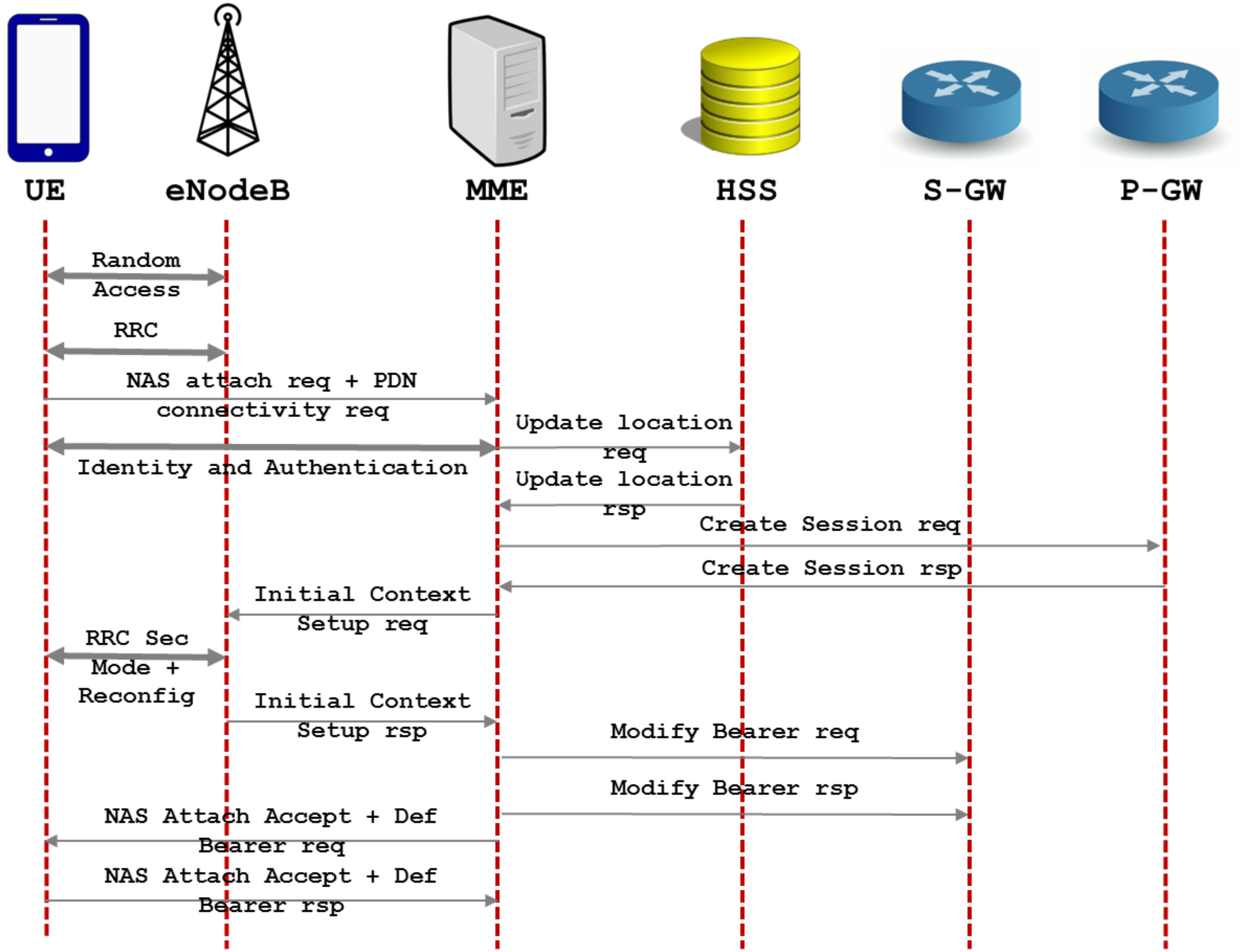
- System configuration
  - Decode Master Information Block (MIB) from PBCH
  - Decode System Information Blocks (SIBs) from PDSCH

LTE FRAME

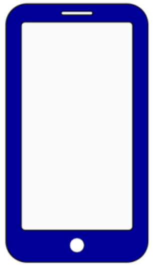


By Roger Piqueras Jover
(http://www.ee.columbia.edu/~roger)

LTE NAS ATTACH PROCEDURE


UE
eNodeB
MME
HSS
S-GW
P-GW
Random Access
RRC
NAS attach req + PDN connectivity req
Identity and Authentication
Update location req
Update location rsp
Create Session req
Create Session rsp
Initial Context Setup req
RRC Sec Mode + Reconfig
Initial Context Setup rsp
Modify Bearer req
Modify Bearer rsp
NAS Attach Accept + Def Bearer req
NAS Attach Accept + Def Bearer rsp

MOBILE NETWORK USER/DEVICE IDENTIFIERS



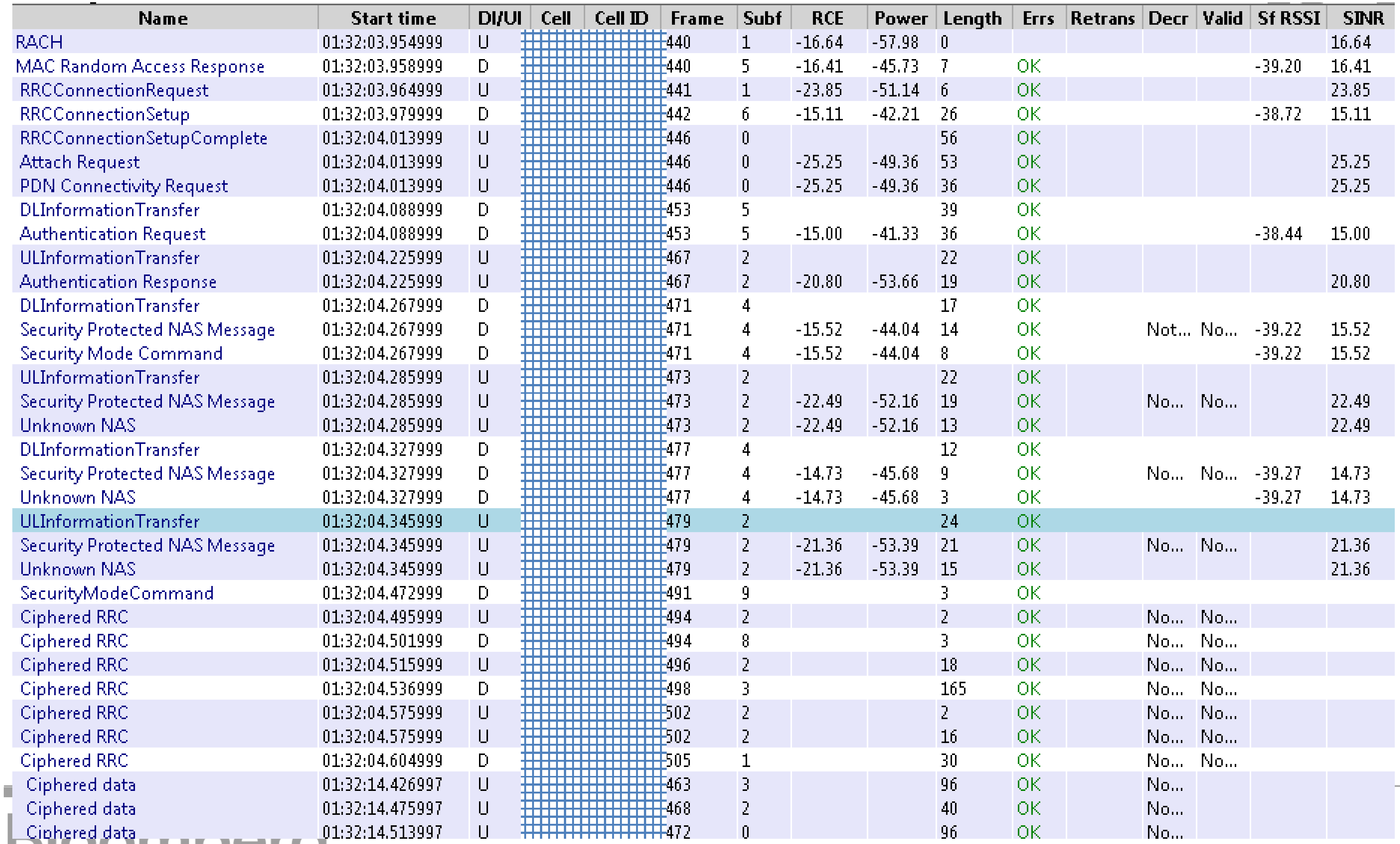
IMEI – “Serial number” of the device

IMSI – secret id of the SIM that should never be disclosed
TMSI – temporary id used by the network once it knows who you are

MSISDN – Your phone number.

LTE (IN)SECURITY

LTE (IN)SECURITY RATIONALE



Name	Start time	DI/UI	Cell	Cell ID	Frame	Subf	RCE	Power	Length	Errs	Retrans	Decr	Valid	Sf RSSI	SINR
RACH	01:32:03.954999	U	[redacted]	[redacted]	440	1	-16.64	-57.98	0						16.64
MAC Random Access Response	01:32:03.958999	D	[redacted]	[redacted]	440	5	-16.41	-45.73	7	OK				-39.20	16.41
RRCConnectionRequest	01:32:03.964999	U	[redacted]	[redacted]	441	1	-23.85	-51.14	6	OK					23.85
RRCConnectionSetup	01:32:03.979999	D	[redacted]	[redacted]	442	6	-15.11	-42.21	26	OK				-38.72	15.11
RRCConnectionSetupComplete	01:32:04.013999	U	[redacted]	[redacted]	446	0			56	OK					
Attach Request	01:32:04.013999	U	[redacted]	[redacted]	446	0	-25.25	-49.36	53	OK					25.25
PDN Connectivity Request	01:32:04.013999	U	[redacted]	[redacted]	446	0	-25.25	-49.36	36	OK					25.25
DLInformationTransfer	01:32:04.088999	D	[redacted]	[redacted]	453	5			39	OK					
Authentication Request	01:32:04.088999	D	[redacted]	[redacted]	453	5	-15.00	-41.33	36	OK				-38.44	15.00
ULInformationTransfer	01:32:04.225999	U	[redacted]	[redacted]	467	2			22	OK					
Authentication Response	01:32:04.225999	U	[redacted]	[redacted]	467	2	-20.80	-53.66	19	OK					20.80
DLInformationTransfer	01:32:04.267999	D	[redacted]	[redacted]	471	4			17	OK					
Security Protected NAS Message	01:32:04.267999	D	[redacted]	[redacted]	471	4	-15.52	-44.04	14	OK		Not...	No...	-39.22	15.52
Security Mode Command	01:32:04.267999	D	[redacted]	[redacted]	471	4	-15.52	-44.04	8	OK				-39.22	15.52
ULInformationTransfer	01:32:04.285999	U	[redacted]	[redacted]	473	2			22	OK					
Security Protected NAS Message	01:32:04.285999	U	[redacted]	[redacted]	473	2	-22.49	-52.16	19	OK		No...	No...		22.49
Unknown NAS	01:32:04.285999	U	[redacted]	[redacted]	473	2	-22.49	-52.16	13	OK					22.49
DLInformationTransfer	01:32:04.327999	D	[redacted]	[redacted]	477	4			12	OK					
Security Protected NAS Message	01:32:04.327999	D	[redacted]	[redacted]	477	4	-14.73	-45.68	9	OK		No...	No...	-39.27	14.73
Unknown NAS	01:32:04.327999	D	[redacted]	[redacted]	477	4	-14.73	-45.68	3	OK				-39.27	14.73
ULInformationTransfer	01:32:04.345999	U	[redacted]	[redacted]	479	2			24	OK					
Security Protected NAS Message	01:32:04.345999	U	[redacted]	[redacted]	479	2	-21.36	-53.39	21	OK		No...	No...		21.36
Unknown NAS	01:32:04.345999	U	[redacted]	[redacted]	479	2	-21.36	-53.39	15	OK					21.36
SecurityModeCommand	01:32:04.472999	D	[redacted]	[redacted]	491	9			3	OK					
Ciphered RRC	01:32:04.495999	U	[redacted]	[redacted]	494	2			2	OK		No...	No...		
Ciphered RRC	01:32:04.501999	D	[redacted]	[redacted]	494	8			3	OK		No...	No...		
Ciphered RRC	01:32:04.515999	U	[redacted]	[redacted]	496	2			18	OK		No...	No...		
Ciphered RRC	01:32:04.536999	D	[redacted]	[redacted]	498	3			165	OK		No...	No...		
Ciphered RRC	01:32:04.575999	U	[redacted]	[redacted]	502	2			2	OK		No...	No...		
Ciphered RRC	01:32:04.575999	U	[redacted]	[redacted]	502	2			16	OK		No...	No...		
Ciphered RRC	01:32:04.604999	D	[redacted]	[redacted]	505	1			30	OK		No...	No...		
Ciphered data	01:32:14.426997	U	[redacted]	[redacted]	463	3			96	OK		No...			
Ciphered data	01:32:14.475997	U	[redacted]	[redacted]	468	2			40	OK		No...			
Ciphered data	01:32:14.513997	U	[redacted]	[redacted]	472	0			96	OK		No...			

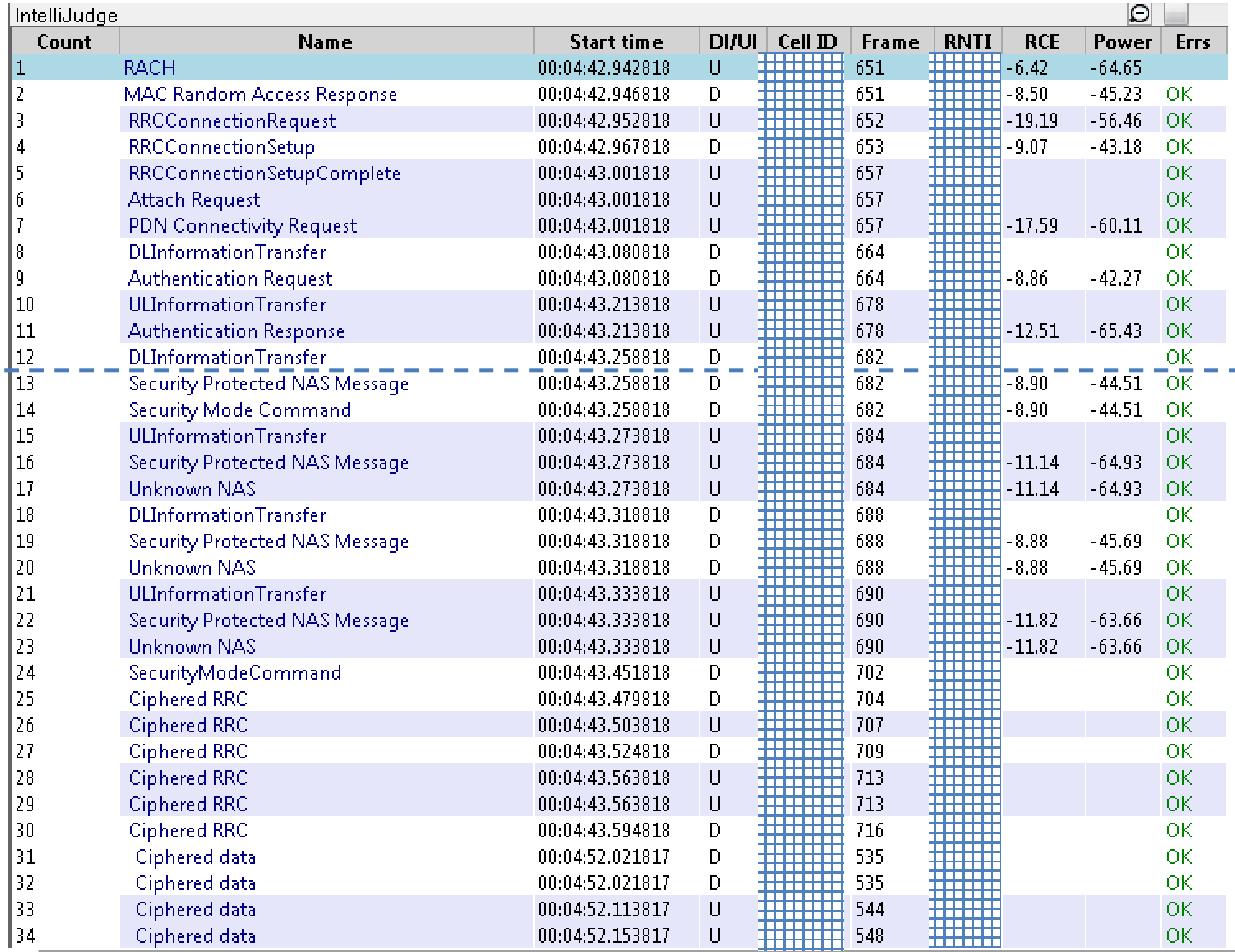
RACH handshake between UE and eNB

RRC handshake between UE and eNB

Connection setup (authentication, set-up of encryption, tunnel set-up, etc)

Encrypted traffic

LTE (IN)SECURITY RATIONALE



IntelliJudge

Count	Name	Start time	Dl/Ul	Cell ID	Frame	RNTI	RCE	Power	Errs
1	RACH	00:04:42.942818	U	[redacted]	651	[redacted]	-6.42	-64.65	
2	MAC Random Access Response	00:04:42.946818	D	[redacted]	651	[redacted]	-8.50	-45.23	OK
3	RRCConnectionRequest	00:04:42.952818	U	[redacted]	652	[redacted]	-19.19	-56.46	OK
4	RRCConnectionSetup	00:04:42.967818	D	[redacted]	653	[redacted]	-9.07	-43.18	OK
5	RRCConnectionSetupComplete	00:04:43.001818	U	[redacted]	657	[redacted]			OK
6	Attach Request	00:04:43.001818	U	[redacted]	657	[redacted]			OK
7	PDN Connectivity Request	00:04:43.001818	U	[redacted]	657	[redacted]	-17.59	-60.11	OK
8	DLInformationTransfer	00:04:43.080818	D	[redacted]	664	[redacted]			OK
9	Authentication Request	00:04:43.080818	D	[redacted]	664	[redacted]	-8.86	-42.27	OK
10	ULInformationTransfer	00:04:43.213818	U	[redacted]	678	[redacted]			OK
11	Authentication Response	00:04:43.213818	U	[redacted]	678	[redacted]	-12.51	-65.43	OK
12	DLInformationTransfer	00:04:43.258818	D	[redacted]	682	[redacted]			OK
13	Security Protected NAS Message	00:04:43.258818	D	[redacted]	682	[redacted]	-8.90	-44.51	OK
14	Security Mode Command	00:04:43.258818	D	[redacted]	682	[redacted]	-8.90	-44.51	OK
15	ULInformationTransfer	00:04:43.273818	U	[redacted]	684	[redacted]			OK
16	Security Protected NAS Message	00:04:43.273818	U	[redacted]	684	[redacted]	-11.14	-64.93	OK
17	Unknown NAS	00:04:43.273818	U	[redacted]	684	[redacted]	-11.14	-64.93	OK
18	DLInformationTransfer	00:04:43.318818	D	[redacted]	688	[redacted]			OK
19	Security Protected NAS Message	00:04:43.318818	D	[redacted]	688	[redacted]	-8.88	-45.69	OK
20	Unknown NAS	00:04:43.318818	D	[redacted]	688	[redacted]	-8.88	-45.69	OK
21	ULInformationTransfer	00:04:43.333818	U	[redacted]	690	[redacted]			OK
22	Security Protected NAS Message	00:04:43.333818	U	[redacted]	690	[redacted]	-11.82	-63.66	OK
23	Unknown NAS	00:04:43.333818	U	[redacted]	690	[redacted]	-11.82	-63.66	OK
24	SecurityModeCommand	00:04:43.451818	D	[redacted]	702	[redacted]			OK
25	Ciphered RRC	00:04:43.479818	D	[redacted]	704	[redacted]			OK
26	Ciphered RRC	00:04:43.503818	U	[redacted]	707	[redacted]			OK
27	Ciphered RRC	00:04:43.524818	D	[redacted]	709	[redacted]			OK
28	Ciphered RRC	00:04:43.563818	U	[redacted]	713	[redacted]			OK
29	Ciphered RRC	00:04:43.563818	U	[redacted]	713	[redacted]			OK
30	Ciphered RRC	00:04:43.594818	D	[redacted]	716	[redacted]			OK
31	Ciphered data	00:04:52.021817	D	[redacted]	535	[redacted]			OK
32	Ciphered data	00:04:52.021817	D	[redacted]	535	[redacted]			OK
33	Ciphered data	00:04:52.113817	U	[redacted]	544	[redacted]			OK
34	Ciphered data	00:04:52.153817	U	[redacted]	548	[redacted]			OK

Unencrypted and unprotected. I can sniff these messages and I can transmit them pretending to be a legitimate base station.

Other things sent in the clear:

- Base station config (broadcast messages)
- Measurement reports
- Measurement report requests
- (Sometimes) GPS coordinates
- HO related messages
- Paging messages
- Etc

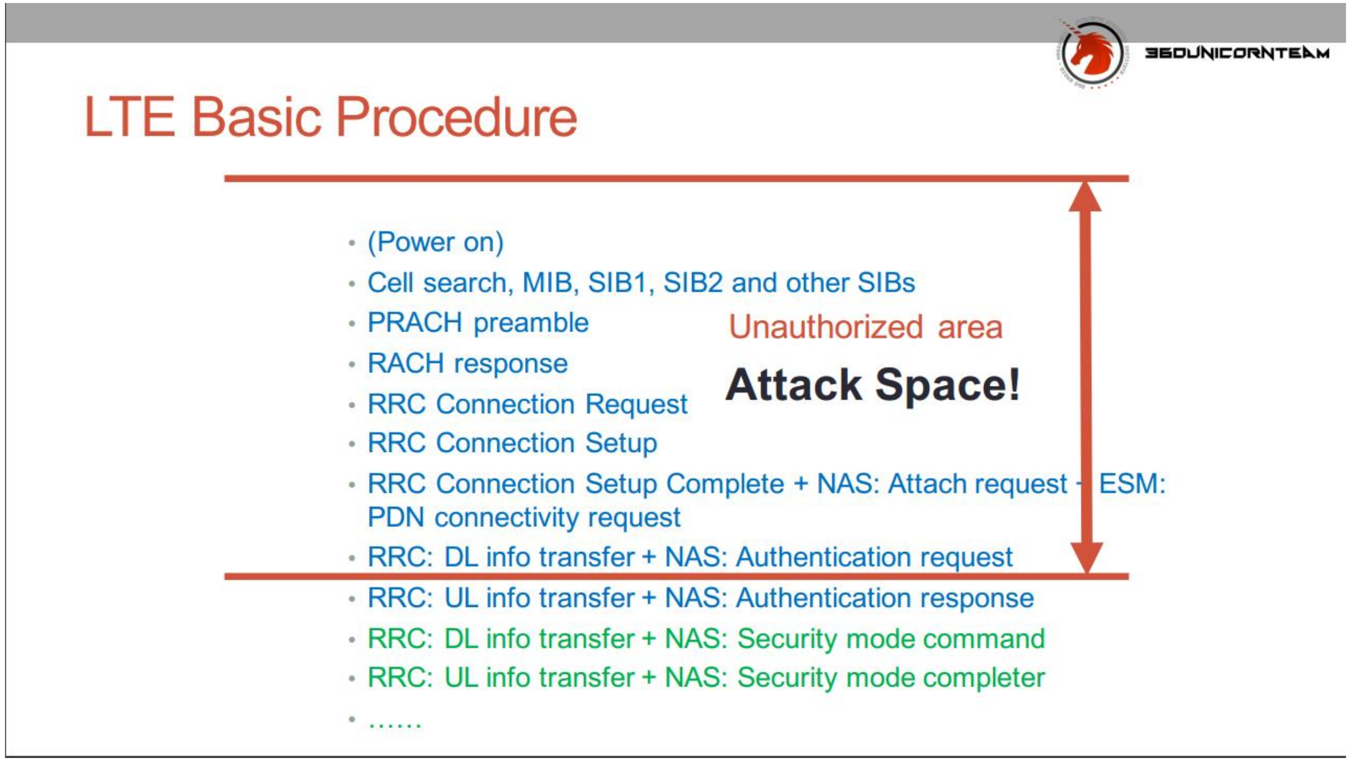
Bloomberg

LTE (IN)SECURITY RATIONALE

Regardless of mutual authentication and strong encryption, a mobile device engages in a substantial exchange of unprotected messages with *any* LTE base station (malicious or not) that advertises itself with the right broadcast information.

LTE (IN)SECURITY RATIONALE

A couple of talks on this at the recent BlackHat and DefCon 2016 conferences…



LTE Basic Procedure

- (Power on)
- Cell search, MIB, SIB1, SIB2 and other SIBs
- PRACH preamble
- RACH response
- RRC Connection Request
- RRC Connection Setup
- RRC Connection Setup Complete + NAS: Attach request + ESM: PDN connectivity request
- RRC: DL info transfer + NAS: Authentication request
- RRC: UL info transfer + NAS: Authentication response
- RRC: DL info transfer + NAS: Security mode command
- RRC: UL info transfer + NAS: Security mode completer
- ……

Unauthorized area

Attack Space!

Haoqi Shan, Wanqiao Zhang (Qihoo 360 Lab). Forcing a Targeted LTE Cellphone into an Unsafe Network. DefCon 24. August 2016.

EXPLORING LTE SECURITY…

TOOLSET

- (Favorite) Fully/partially functional LTE open source implementations
  - OpenLTE – End to end implementation: RAN and "EPC".
    - http://sourceforge.net/projects/openlte/
  - srsLTE – Almost complete implementation.
    - https://github.com/srsLTE
  - srsUE – First available UE stack implementation!
    - https://github.com/srsLTE/srsUE
- HW setup
  - USRP B210 for active rogue base station
  - BUDGET: USRP B210 ($1100) + GPSDO ($625) + LTE Antenna (2x$30) = $1785
  - Machine running Ubunutu
  - US dongles (hackRF, etc) for passive sniffing.

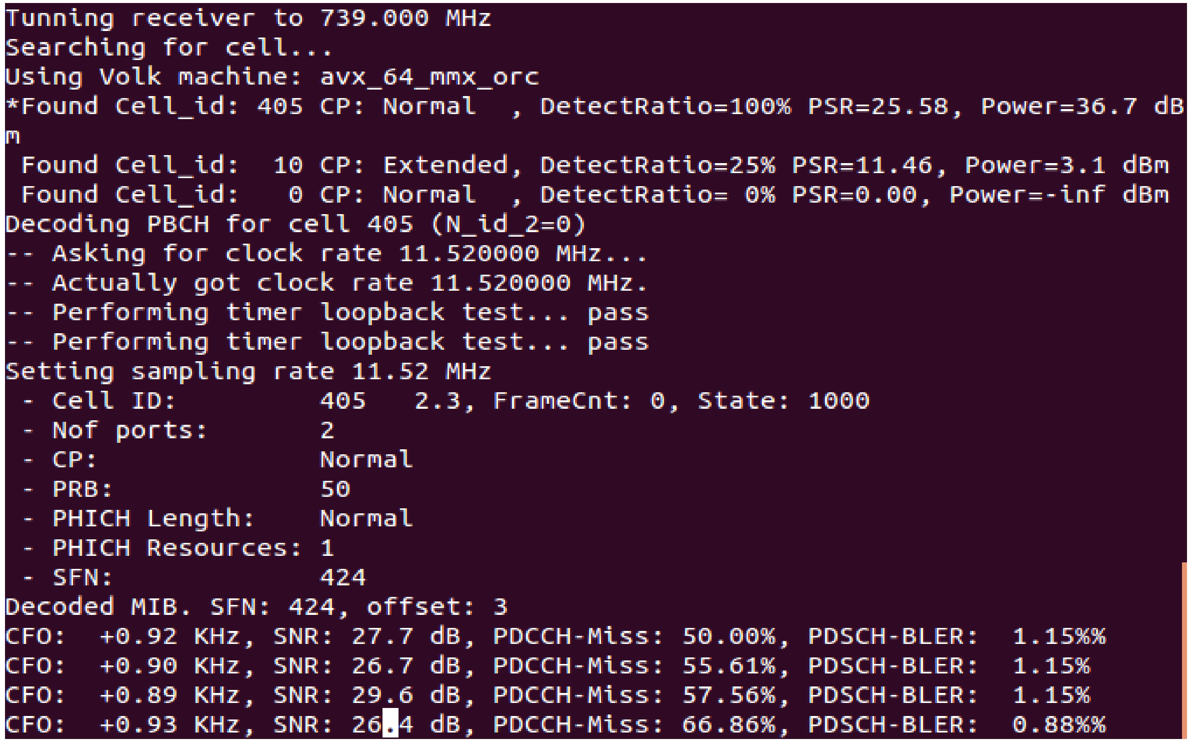
All LTE active radio experiments MUST be performed inside a faraday cage.

LTE TRAFFIC ANALYSIS – LTE SNIFFER!!!

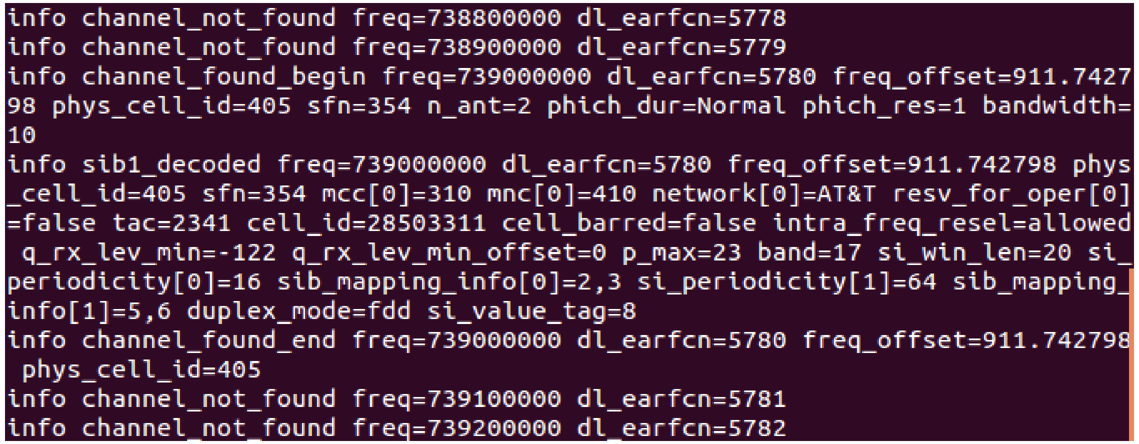
- srsLTE - AirScope
  - New LTE sniffer tool
  - Full LTE traffic sniffing and analysis
  - Pcap dumps compatible with Wireshark LTE dissector
  - Custom traffic log analysis

SNIFFING BASE STATION CONFIGURATION

- Base station configuration broadcasted in the clear in MIB and SIB messages.
- Open source tools available to scan for LTE base stations
  - My setup: USRP B210 + Ubuntu machine + modified openLTE
  - Alternative setup: European USB LTE dongle (GT-B3740) + modified Kalmia driver
  - New setup: srsLTE + USRP mini

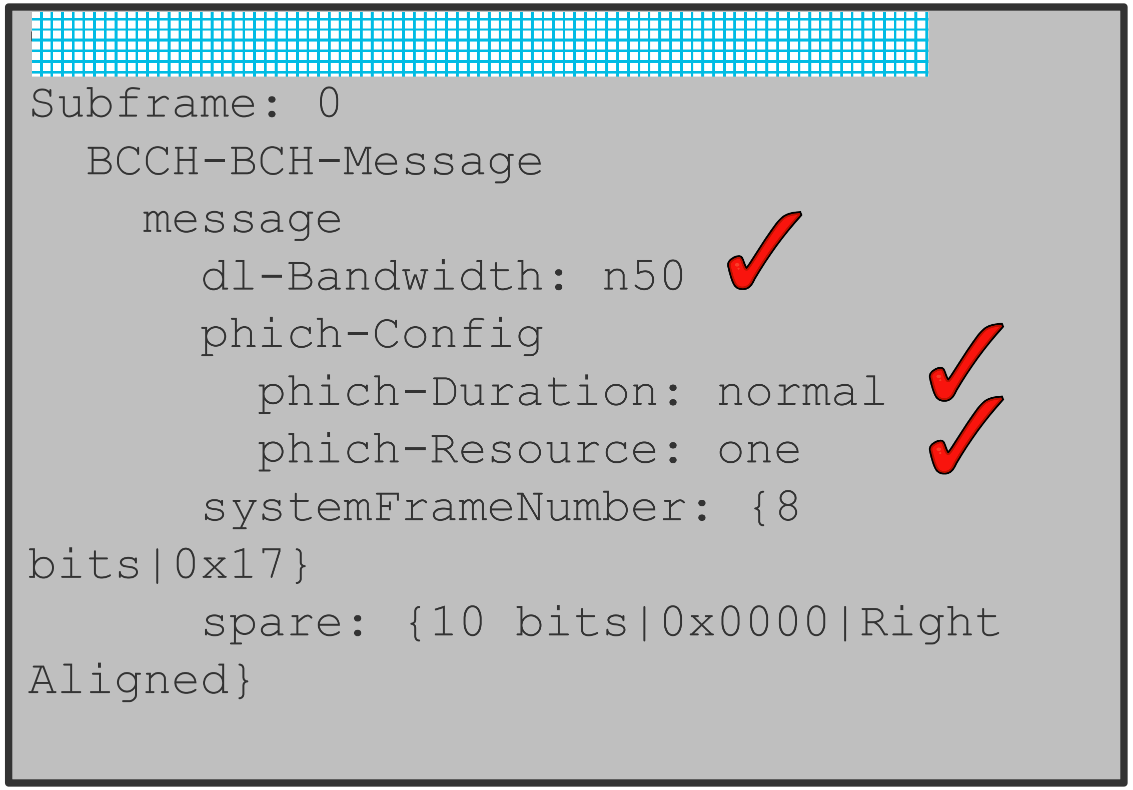


```
Tunning receiver to 739.000 MHz
Searching for cell...
Using Volk machine: avx_64_mmx_orc
*Found Cell_id: 405 CP: Normal   , DetectRatio=100% PSR=25.58, Power=36.7 dB
m
 Found Cell_id:  10 CP: Extended, DetectRatio=25% PSR=11.46, Power=3.1 dBm
 Found Cell_id:   0 CP: Normal   , DetectRatio= 0% PSR=0.00, Power=-inf dBm
Decoding PBCH for cell 405 (N_id_2=0)
-- Asking for clock rate 11.520000 MHz...
-- Actually got clock rate 11.520000 MHz.
-- Performing timer loopback test... pass
-- Performing timer loopback test... pass
Setting sampling rate 11.52 MHz
 - Cell ID:          405   2.3, FrameCnt: 0, State: 1000
 - Nof ports:        2
 - CP:               Normal
 - PRB:              50
 - PHICH Length:     Normal
 - PHICH Resources: 1
 - SFN:              424
Decoded MIB. SFN: 424, offset: 3
CFO:  +0.92 KHz, SNR: 27.7 dB, PDCCH-Miss: 50.00%, PDSCH-BLER:  1.15%%
CFO:  +0.90 KHz, SNR: 26.7 dB, PDCCH-Miss: 55.61%, PDSCH-BLER:  1.15%
CFO:  +0.89 KHz, SNR: 29.6 dB, PDCCH-Miss: 57.56%, PDSCH-BLER:  1.15%
CFO:  +0.93 KHz, SNR: 26.4 dB, PDCCH-Miss: 66.86%, PDSCH-BLER:  0.88%%
```



```
info channel_not_found freq=738800000 dl_earfcn=5778
info channel_not_found freq=738900000 dl_earfcn=5779
info channel_found_begin freq=739000000 dl_earfcn=5780 freq_offset=911.7427
98 phys_cell_id=405 sfn=354 n_ant=2 phich_dur=Normal phich_res=1 bandwidth=
10
info sib1_decoded freq=739000000 dl_earfcn=5780 freq_offset=911.742798 phys
_cell_id=405 sfn=354 mcc[0]=310 mnc[0]=410 network[0]=AT&T resv_for_oper[0]
=false tac=2341 cell_id=28503311 cell_barred=false intra_freq_resel=allowed
 q_rx_lev_min=-122 q_rx_lev_min_offset=0 p_max=23 band=17 si_win_len=20 si_
periodicity[0]=16 sib_mapping_info[0]=2,3 si_periodicity[1]=64 sib_mapping_
info[1]=5,6 duplex_mode=fdd si_value_tag=8
info channel_found_end freq=739000000 dl_earfcn=5780 freq_offset=911.742798
 phys_cell_id=405
info channel_not_found freq=739100000 dl_earfcn=5781
info channel_not_found freq=739200000 dl_earfcn=5782
```

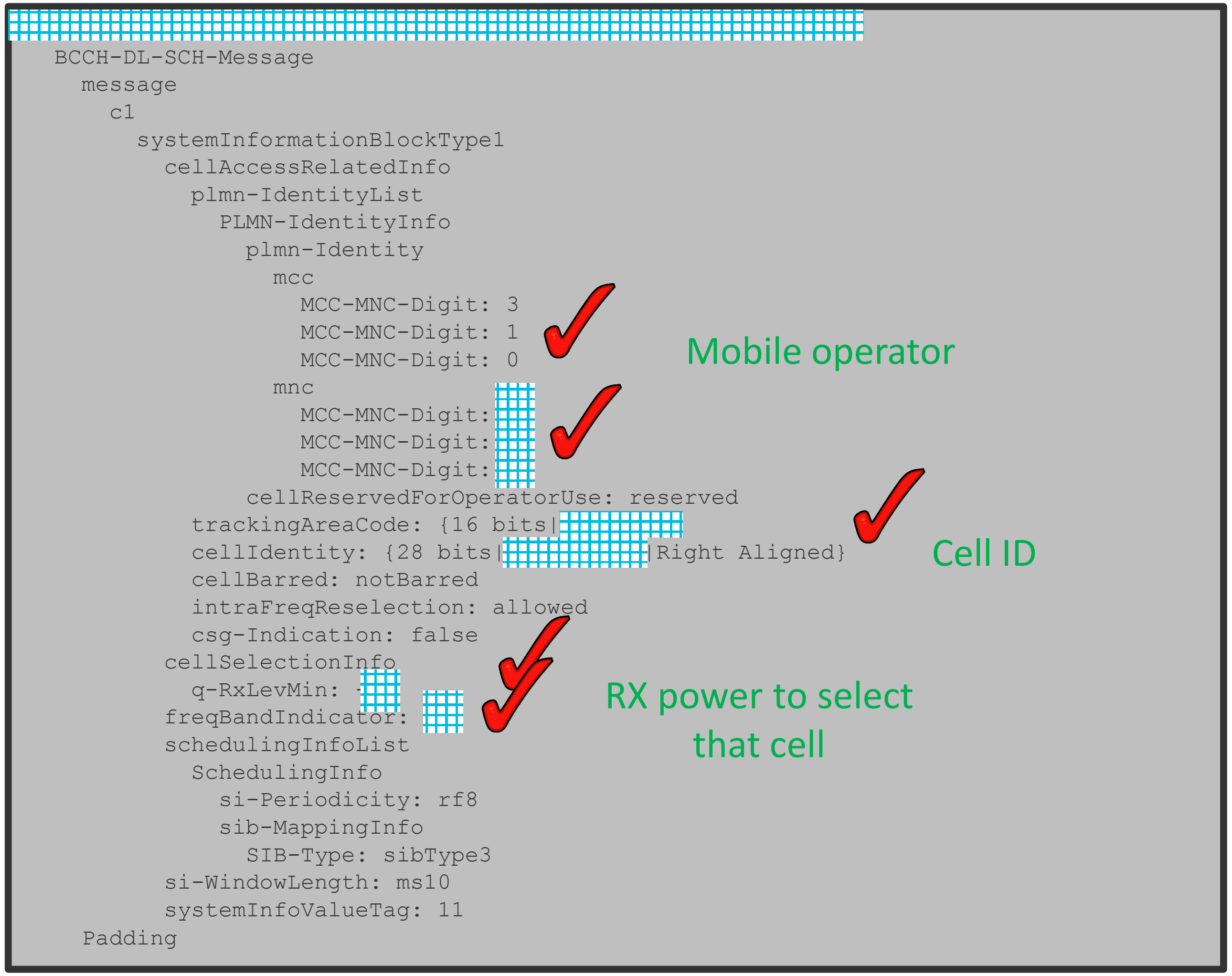
SNIFFING BASE STATION CONFIGURATION



```
[redacted]
Subframe: 0
  BCCH-BCH-Message
    message
      dl-Bandwidth: n50 ✓
      phich-Config
        phich-Duration: normal ✓
        phich-Resource: one    ✓
      systemFrameNumber: {8
bits|0x17}
      spare: {10 bits|0x0000|Right
Aligned}
```

LTE PBCH MIB packet

SNIFFING BASE STATION CONFIGURATION



```
[redacted]
  BCCH-DL-SCH-Message
    message
      c1
        systemInformationBlockType1
          cellAccessRelatedInfo
            plmn-IdentityList
              PLMN-IdentityInfo
                plmn-Identity
                  mcc
                    MCC-MNC-Digit: 3
                    MCC-MNC-Digit: 1
                    MCC-MNC-Digit: 0
                  mnc
                    MCC-MNC-Digit: [redacted]
                    MCC-MNC-Digit:
                    MCC-MNC-Digit:
                cellReservedForOperatorUse: reserved
            trackingAreaCode: {16 bits|[redacted]
            cellIdentity: {28 bits|[redacted]|Right Aligned}
            cellBarred: notBarred
            intraFreqReselection: allowed
            csg-Indication: false
          cellSelectionInfo
            q-RxLevMin: [redacted]
          freqBandIndicator: [redacted]
          schedulingInfoList
            SchedulingInfo
              si-Periodicity: rf8
              sib-MappingInfo
                SIB-Type: sibType3
          si-WindowLength: ms10
          systemInfoValueTag: 11
    Padding
```

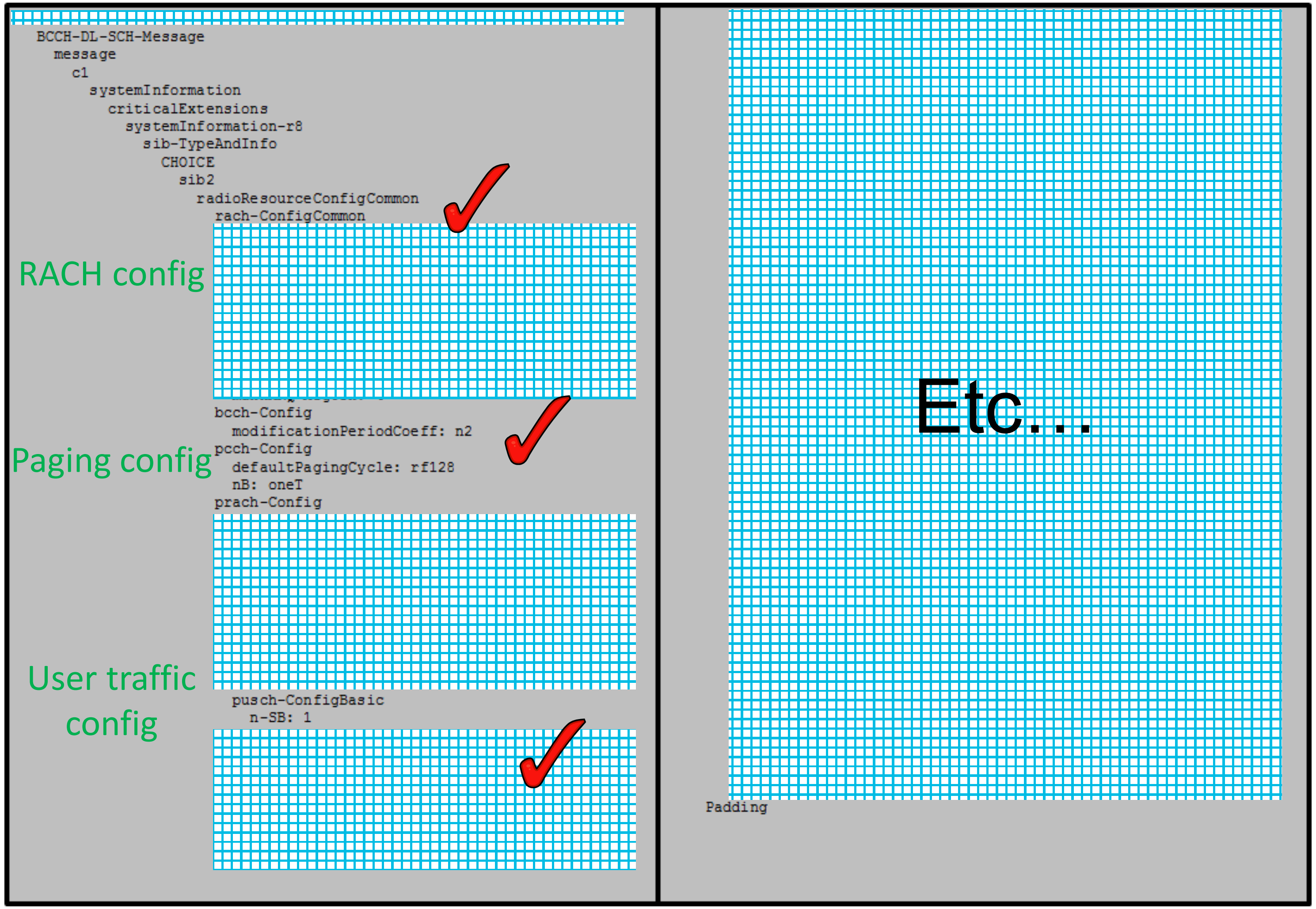
Mobile operator

Cell ID

RX power to select that cell

LTE PDSCH SIB1 packet

SNIFFING BASE STATION CONFIGURATION



```
[redacted]
  BCCH-DL-SCH-Message
    message
      c1
        systemInformation
          criticalExtensions
            systemInformation-r8
              sib-TypeAndInfo
                CHOICE
                  sib2
                    radioResourceConfigCommon
                      rach-ConfigCommon
                      [redacted]
                      bcch-Config
                        modificationPeriodCoeff: n2
                      pcch-Config
                        defaultPagingCycle: rf128
                        nB: oneT
                      prach-Config
                      [redacted]
                        pusch-ConfigBasic
                          n-SB: 1
                      [redacted]
```

```
[redacted]
Padding
```

RACH config ✓

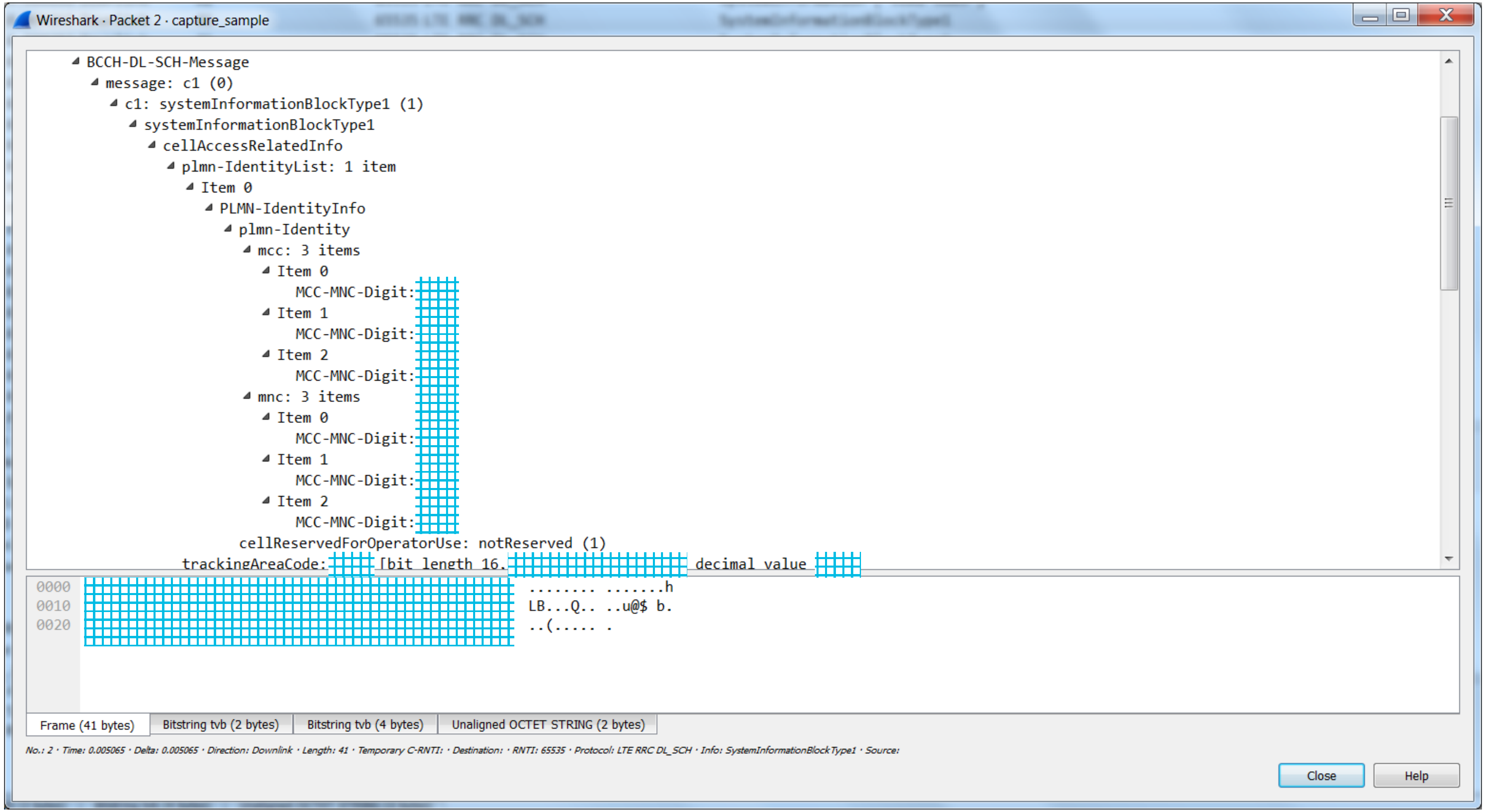
Paging config ✓

User traffic config ✓

Etc…

LTE PDSCH SIB2/3 packet

THE SAME WITH OPEN-SOURCE AND WIRESHARK



Wireshark · Packet 2 · capture_sample [redacted]

```
◢ BCCH-DL-SCH-Message
  ◢ message: c1 (0)
    ◢ c1: systemInformationBlockType1 (1)
      ◢ systemInformationBlockType1
        ◢ cellAccessRelatedInfo
          ◢ plmn-IdentityList: 1 item
            ◢ Item 0
              ◢ PLMN-IdentityInfo
                ◢ plmn-Identity
                  ◢ mcc: 3 items
                    ◢ Item 0
                        MCC-MNC-Digit: [redacted]
                    ◢ Item 1
                        MCC-MNC-Digit: [redacted]
                    ◢ Item 2
                        MCC-MNC-Digit: [redacted]
                  ◢ mnc: 3 items
                    ◢ Item 0
                        MCC-MNC-Digit: [redacted]
                    ◢ Item 1
                        MCC-MNC-Digit: [redacted]
                    ◢ Item 2
                        MCC-MNC-Digit: [redacted]
                cellReservedForOperatorUse: notReserved (1)
          trackingAreaCode: [redacted] [bit length 16, [redacted] decimal value [redacted]
```

```
0000  [redacted]  ........ .......h
0010              LB...Q.. ..u@$ b.
0020              ..(..... .
```

Frame (41 bytes) | Bitstring tvb (2 bytes) | Bitstring tvb (4 bytes) | Unaligned OCTET STRING (2 bytes)

No.: 2 · Time: 0.005065 · Delta: 0.005065 · Direction: Downlink · Length: 41 · Temporary C-RNTI: · Destination: · RNTI: 65535 · Protocol: LTE RRC DL_SCH · Info: SystemInformationBlockType1 · Source:

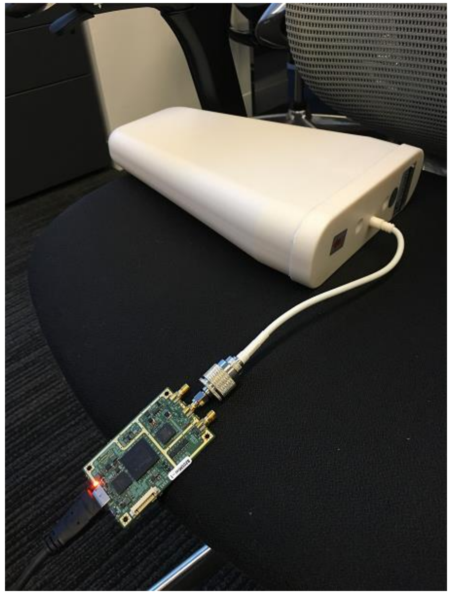
SNIFFING BASE STATION CONFIGURATION

- MIB/SIB messages are necessary for the operation of the network
  - Some things must be sent in the clear (i.e. a device connecting for the first time)
  - But perhaps not everything
- Things an attacker can learn from MIB and SIB messages
  - Optimal tx power for a rogue base station (no need to set up your USRP to its max tx power)
  - High priority frequencies to force priority cell reselection
  - Mobile operator who owns that tower
  - Tracking Area of the legitimate cell (use a different one in your rogue eNodeB to force TAU update messages)
  - Mapping of signaling channels
  - Paging channel mapping and paging configuration
  - Etc
- **I can use the data in the SIB messages to optimize a rogue base station setup…**

LTE/LTE-A Jamming, Spoofing and Sniffing: Threat Assessment and Mitigation. Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, Jeffrey H. Reed. **IEEE Communications Magazine.** Special issue on Critical Communications and Public Safety Networks. April 2016.

SNIFFING BASE STATION CONFIGURATION

- New project → **LTE eNB database + rogue eNB setup tool**
  - Small form-factor portable MIB/SIB scanner
    - RaspberryPi 3 + RTL-SDR
    - Android phone + RTL-SDR
    - Latest configuration: Android phone + USRP B200-mini
  - Modified srsLTE scanner



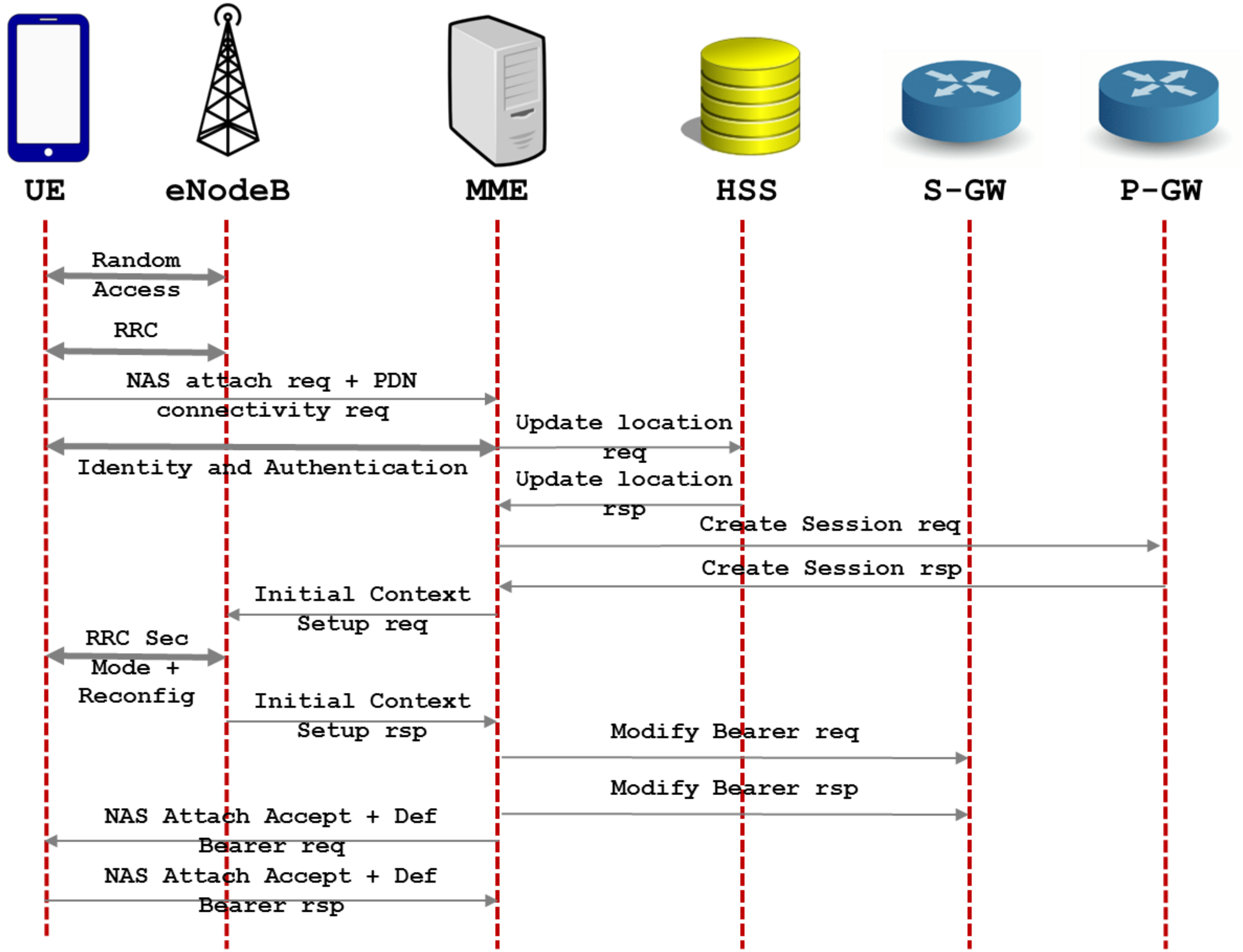
- Step 1 - Scan for eNBs and collect MIB/SIBs
  - Generate a database of everything I see while hanging out in NYC

- Step 2 – Build a rogue base station configuration tool for openLTE
  - Input – {where are you, mobile operator}
  - Output – Start openLTE rogue eNodeB with optimal configuration for maximum impact

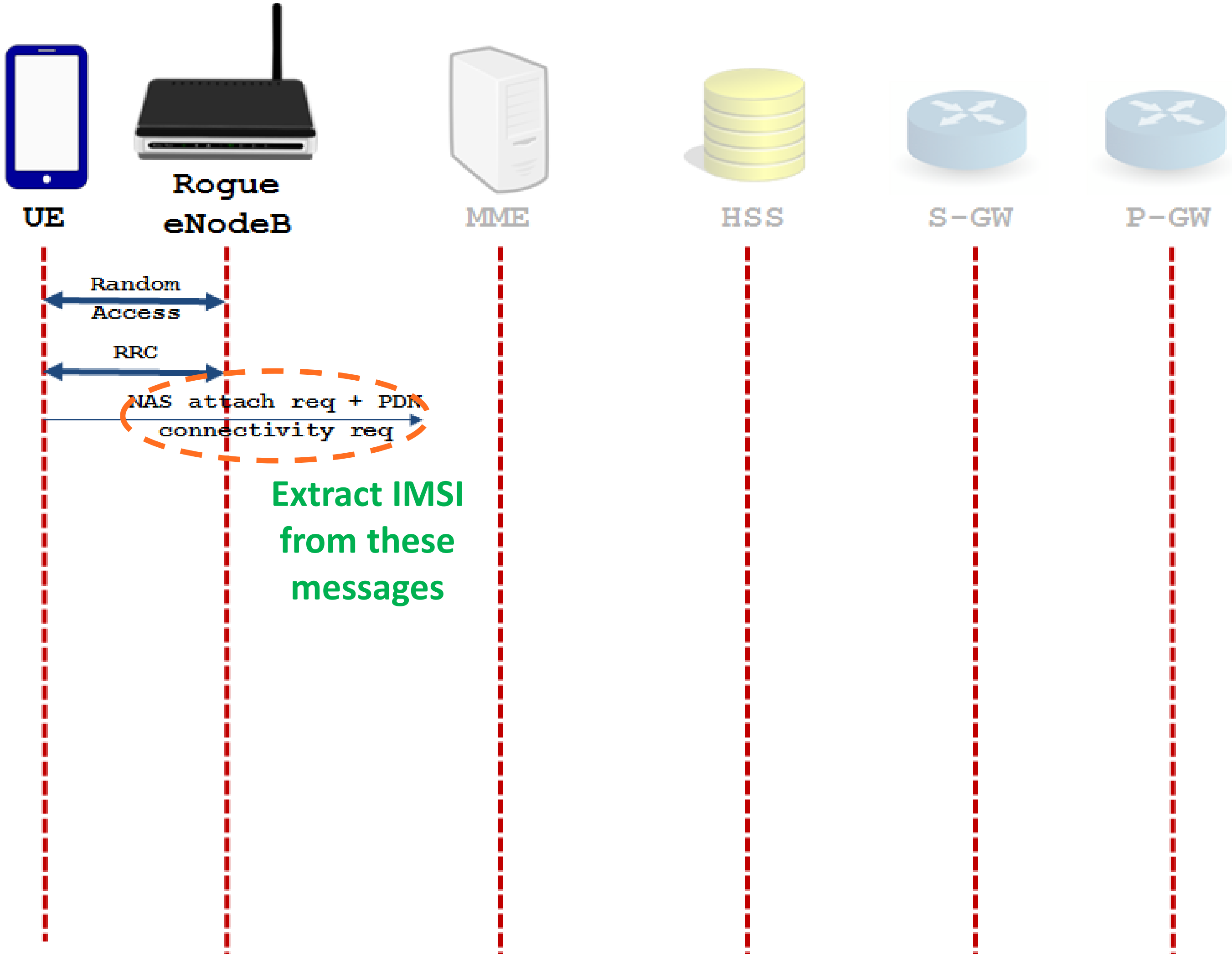
LOW-COST LTE IMSI CATCHER (STINGRAY)

- Despite common assumptions, in LTE the IMSI is always transmitted in the clear at least once
  - If the network has never seen that UE, it must use the IMSI to claim its identity
  - A UE will trust *any* eNodeB that claims it has never seen that device (pre-authentication messages)
  - IMSI can also be transmitted in the clear in error recovery situations (very rare)
- Implementation
  - USRP B210
  - LTE base station – OpenLTE (modified LTE_fdd_eNodeB)
    - Added feature to record IMSI from Attach Request messages
  - Send attach reject after IMSI collection
  - Tested with my phone and 2 LTE USB dongles
    - Experiments in controlled environment
- **Stingrays also possible in LTE without need to downgrade connection to GSM**
  - Low-cost IMSI catcher (under $2000)

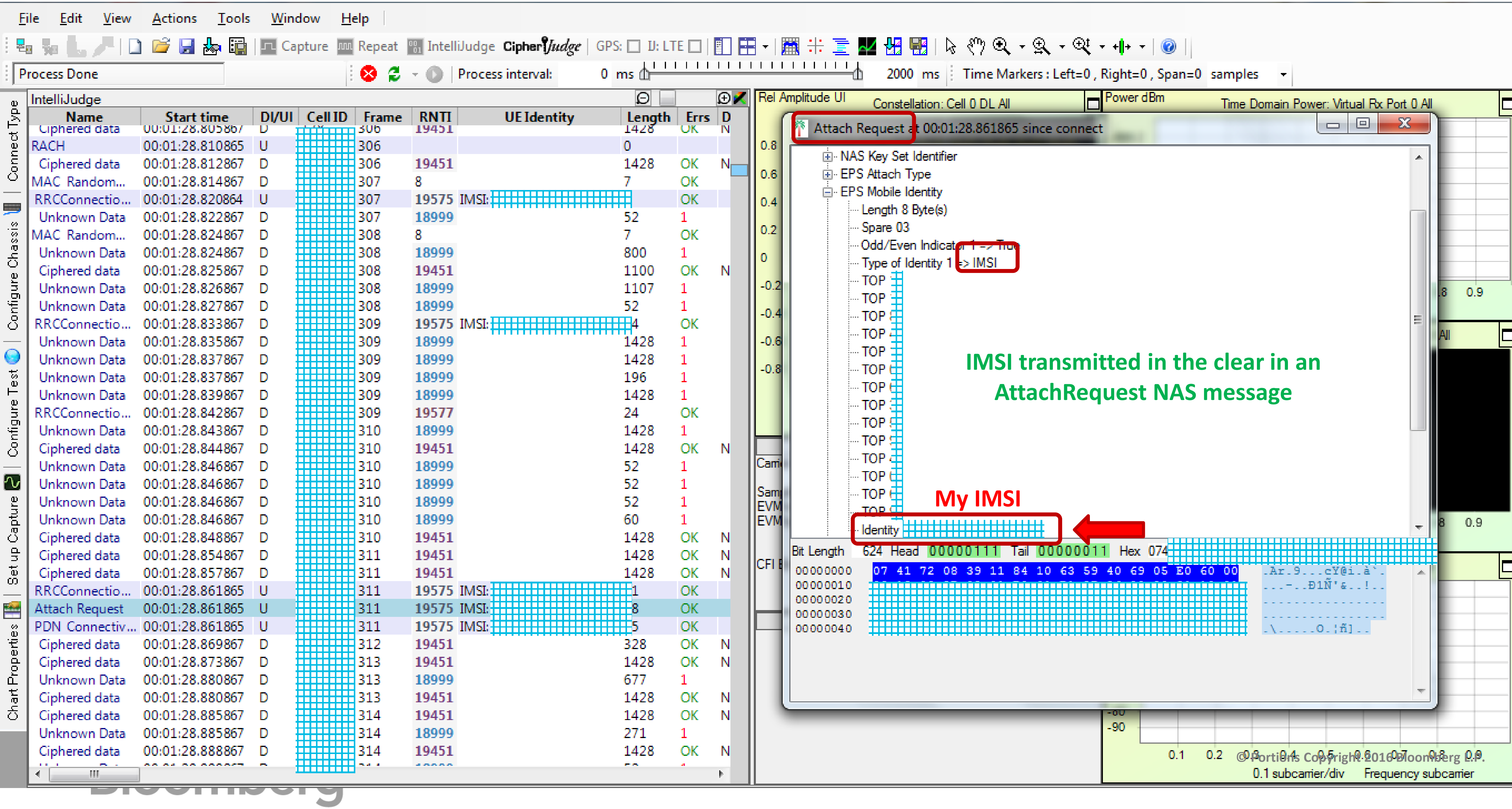
IMSI CATCHERS(STINGRAY)


UE
eNodeB
MME
HSS
S-GW
P-GW
Random Access
RRC
NAS attach req + PDN connectivity req
Identity and Authentication
Update location req
Update location rsp
Create Session req
Create Session rsp
Initial Context Setup req
RRC Sec Mode + Reconfig
Initial Context Setup rsp
Modify Bearer req
Modify Bearer rsp
NAS Attach Accept + Def Bearer req
NAS Attach Accept + Def Bearer rsp

IMSI CATCHERS(STINGRAY)



Extract IMSI from these messages



IntelliJudge

Name	Start time	DI/UI	Cell ID	Frame	RNTI	UE Identity	Length	Errs	D
Ciphered data	00:01:28.805867	D	[redacted]	306	19451		1428	OK	N
RACH	00:01:28.810865	U	[redacted]	306			0		
Ciphered data	00:01:28.812867	D	[redacted]	306	19451		1428	OK	N
MAC Random...	00:01:28.814867	D	[redacted]	307	8		7	OK	
RRCConnectio...	00:01:28.820864	U	[redacted]	307	19575	IMSI:[redacted]		OK	
Unknown Data	00:01:28.822867	D	[redacted]	307	18999		52	1	
MAC Random...	00:01:28.824867	D	[redacted]	308	8		7	OK	
Unknown Data	00:01:28.824867	D	[redacted]	308	18999		800	1	
Ciphered data	00:01:28.825867	D	[redacted]	308	19451		1100	OK	N
Unknown Data	00:01:28.826867	D	[redacted]	308	18999		1107	1	
Unknown Data	00:01:28.827867	D	[redacted]	308	18999		52	1	
RRCConnectio...	00:01:28.833867	D	[redacted]	309	19575	IMSI:[redacted]	4	OK	
Unknown Data	00:01:28.835867	D	[redacted]	309	18999		1428	1	
Unknown Data	00:01:28.837867	D	[redacted]	309	18999		1428	1	
Unknown Data	00:01:28.837867	D	[redacted]	309	18999		196	1	
Unknown Data	00:01:28.839867	D	[redacted]	309	18999		1428	1	
RRCConnectio...	00:01:28.842867	D	[redacted]	309	19577		24	OK	
Unknown Data	00:01:28.843867	D	[redacted]	310	18999		1428	1	
Ciphered data	00:01:28.844867	D	[redacted]	310	19451		1428	OK	N
Unknown Data	00:01:28.846867	D	[redacted]	310	18999		52	1	
Unknown Data	00:01:28.846867	D	[redacted]	310	18999		52	1	
Unknown Data	00:01:28.846867	D	[redacted]	310	18999		52	1	
Unknown Data	00:01:28.846867	D	[redacted]	310	18999		60	1	
Ciphered data	00:01:28.848867	D	[redacted]	310	19451		1428	OK	N
Ciphered data	00:01:28.854867	D	[redacted]	311	19451		1428	OK	N
Ciphered data	00:01:28.857867	D	[redacted]	311	19451		1428	OK	N
RRCConnectio...	00:01:28.861865	U	[redacted]	311	19575	IMSI:[redacted]	1	OK	
Attach Request	00:01:28.861865	U	[redacted]	311	19575	IMSI:[redacted]	8	OK	
PDN Connectiv...	00:01:28.861865	U	[redacted]	311	19575	IMSI:[redacted]	5	OK	
Ciphered data	00:01:28.869867	D	[redacted]	312	19451		328	OK	N
Ciphered data	00:01:28.873867	D	[redacted]	313	19451		1428	OK	N
Unknown Data	00:01:28.880867	D	[redacted]	313	18999		677	1	
Ciphered data	00:01:28.880867	D	[redacted]	313	19451		1428	OK	N
Ciphered data	00:01:28.885867	D	[redacted]	314	19451		1428	OK	N
Unknown Data	00:01:28.885867	D	[redacted]	314	18999		271	1	
Ciphered data	00:01:28.888867	D	[redacted]	314	19451		1428	OK	N

Attach Request at 00:01:28.861865 since connect

```
+ NAS Key Set Identifier
+ EPS Attach Type
- EPS Mobile Identity
    Length 8 Byte(s)
    Spare 03
    Odd/Even Indicator 1 -> True
    Type of Identity 1 => IMSI
    TOP [redacted]
    TOP [redacted]
    TOP [redacted]
    TOP [redacted]
    TOP [redacted]
    TOP [redacted]
    TOP [redacted]
    TOP [redacted]
    TOP [redacted]
    TOP [redacted]
    TOP [redacted]
    TOP [redacted]
    TOP [redacted]
    TOP [redacted]
    Identity [redacted]
```

```
Bit Length  624  Head 00000111  Tail 00000011  Hex 074[redacted]
00000000  07 41 72 08 39 11 84 10 63 59 40 69 05 E0 60 00   .Ar.9...cY@i.à`.
00000010  [redacted]                                         ...-..ÐlÑ'&..!..
00000020  [redacted]
00000030  [redacted]
00000040  [redacted]                                         .\.....O.¦ñ]..
```

IMSI transmitted in the clear in an AttachRequest NAS message

My IMSI

INTERMISSION – EXCELLENT RELATED WORK

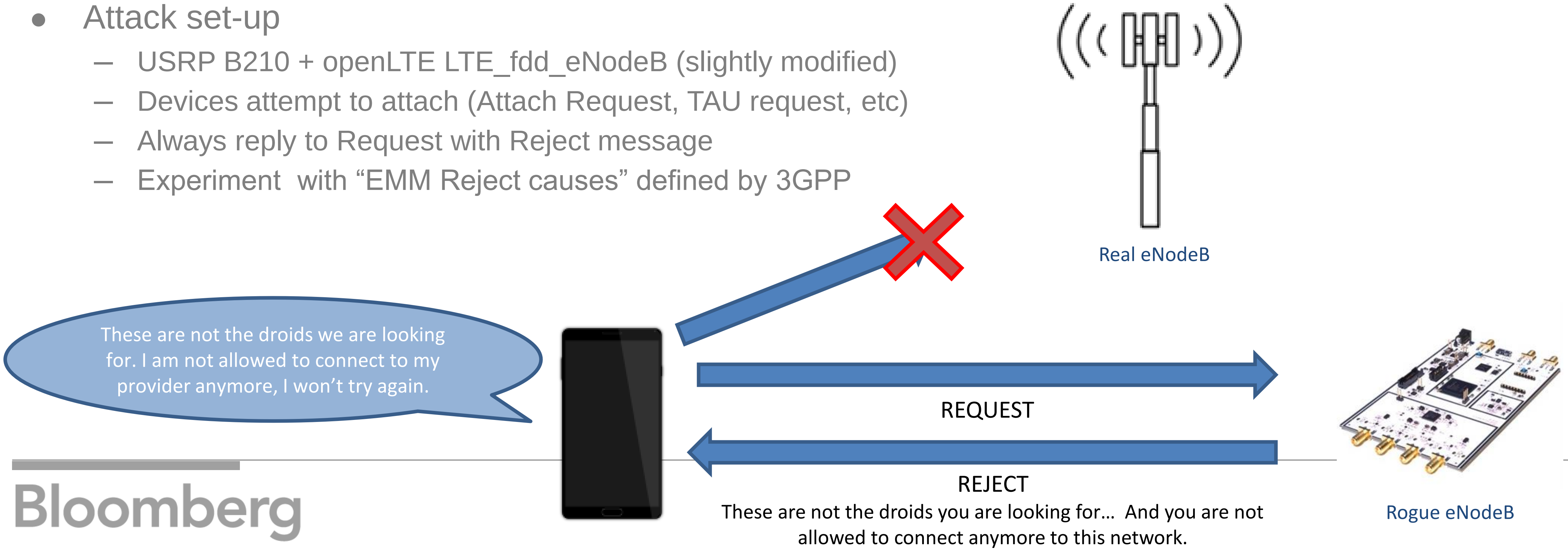
- I was hoping to be the first to publish but…

- A team at TU Berlin, University of Helsinki and Aalto University doing excellent work in the same area
  - More results on SIM/device bricking with Attach/TAU reject messages
  - LTE location leaks
  - Detailed implementation and results
  - Paper presented at NDSS 2016: http://arxiv.org/abs/1510.07563

- Prof. Seifert's team at TU Berlin responsible for other previous VERY COOL projects

DEVICE AND SIM TEMPORARY LOCK

- Attach reject and TAU (Tracking Area Update) reject messages not encrypted/integrity-protected
- Spoofing this messages one can trick a device to
  - Believe it is not allowed to connect to the network (blocked)
  - Believe it is supposed to downgrade to or only allowed to connect to GSM
- Attack set-up
  - USRP B210 + openLTE LTE_fdd_eNodeB (slightly modified)
  - Devices attempt to attach (Attach Request, TAU request, etc)
  - Always reply to Request with Reject message
  - Experiment with "EMM Reject causes" defined by 3GPP


Real eNodeB
These are not the droids we are looking for. I am not allowed to connect to my provider anymore, I won't try again.
REQUEST
REJECT
These are not the droids you are looking for… And you are not allowed to connect anymore to this network.
Rogue eNodeB

DEVICE AND SIM TEMPORARY LOCK

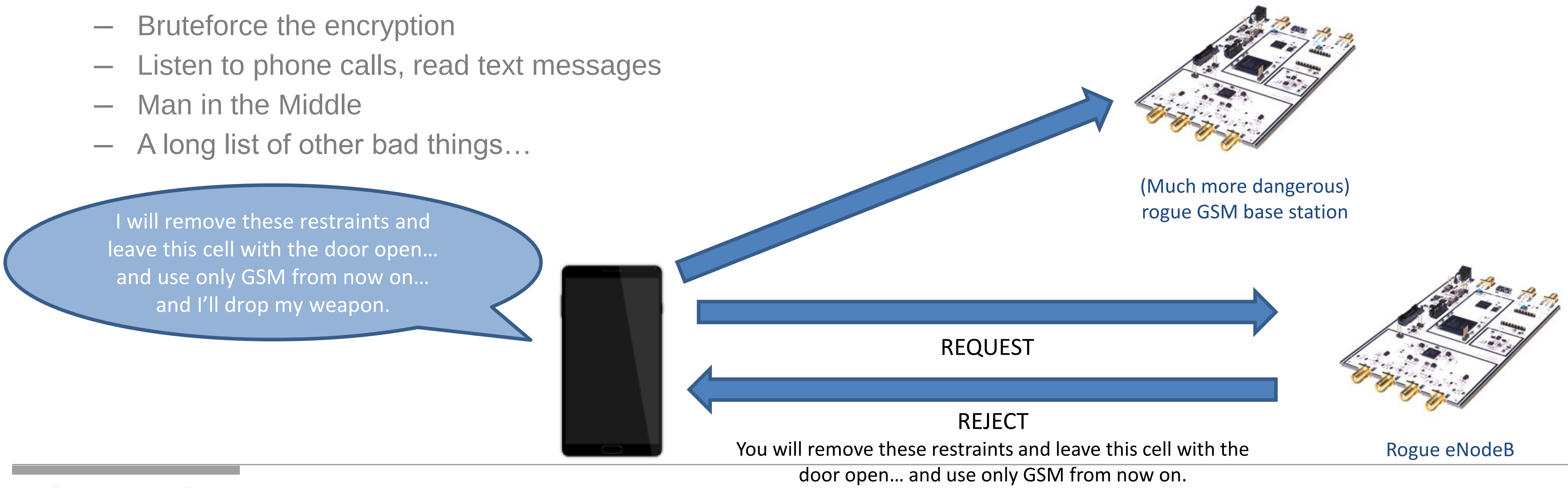
- Some results
  - Tested with my phone and 2 USB LTE dongles
  - The blocking of the device/SIM is only temporary
  - Device won't connect until rebooted
  - SIM won't connect until reboot
  - SIM/device bricked until timer T3245 expires (24 to 48 hours!)
    - I did not test this because I cannot go by without phone for 24h!
    - See related work for much more and better results on this…
  - Downgrade device to GSM and get it to connect to a rogue BS

- If the target is an M2M device, it could be a semi-persistent attack
  - Reboot M2M device remotely?
  - Send a technician to reset SIM?
  - Or just wait 48 hours for your M2M device to come back online…

SOFT DOWNGRADE TO GSM

- Use similar techniques to “instruct” the phone to downgrade to GSM
  - Only GSM services allowed OR LTE and 3G not allowed
  - Tested with my phone and 2 LTE USB dongles

- Once at GSM, the phone to connects to your rogue base station
  - Bruteforce the encryption
  - Listen to phone calls, read text messages
  - Man in the Middle
  - A long list of other bad things…



I will remove these restraints and leave this cell with the door open… and use only GSM from now on… and I’ll drop my weapon.

(Much more dangerous) rogue GSM base station

REQUEST

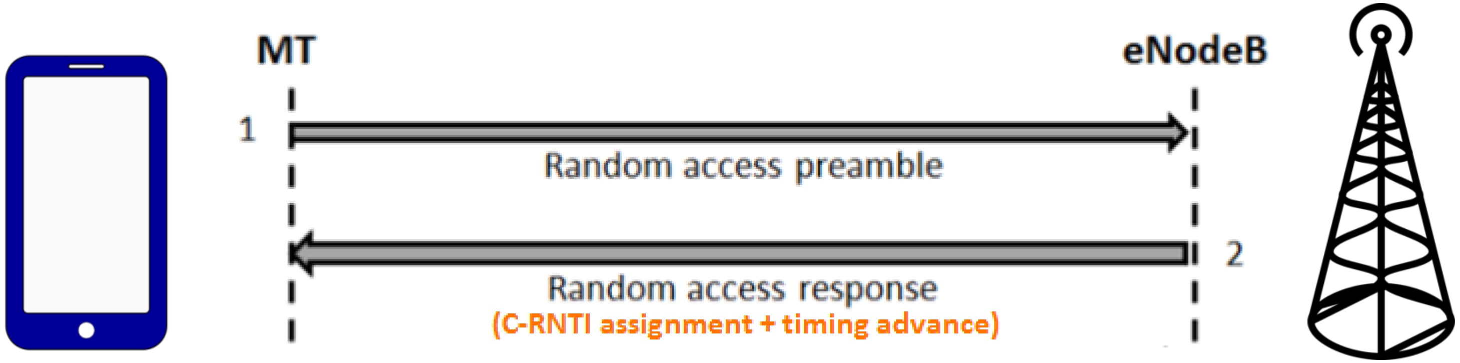
REJECT

You will remove these restraints and leave this cell with the door open… and use only GSM from now on.

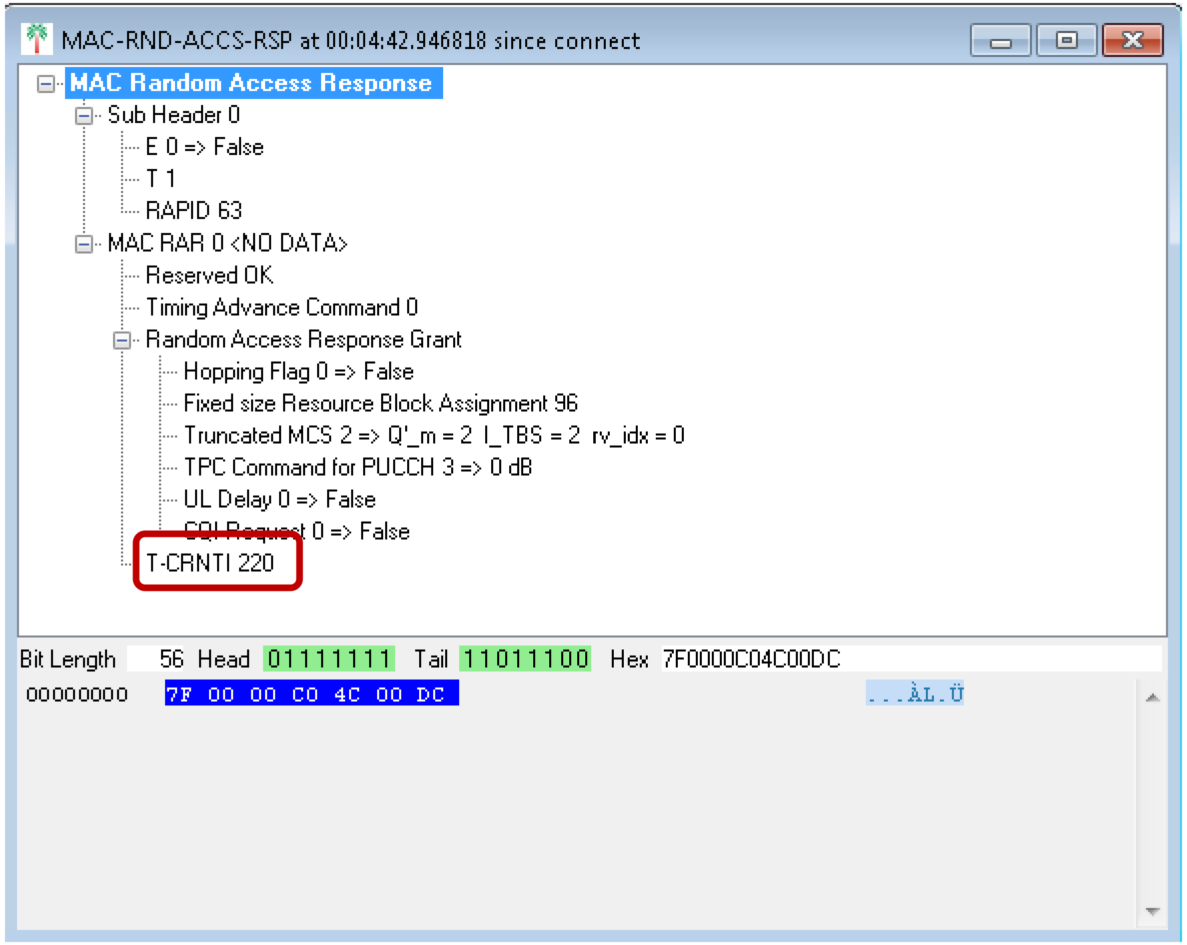
Rogue eNodeB

LOCATION LEAKS AND DEVICE TRACKING

- RNTI
  - PHY layer id sent in the clear in EVERY SINGLE packet, both UL and DL
  - Identifies uniquely every UE within a cell
    - Changes infrequently
    - Based on several captures in the NYC and Honolulu areas
  - No distinguishable behavior per operator or per base station manufacturer
  - Assigned by the network in the MAC RAR response to the RACH preamble



LOCATION LEAKS AND DEVICE TRACKING



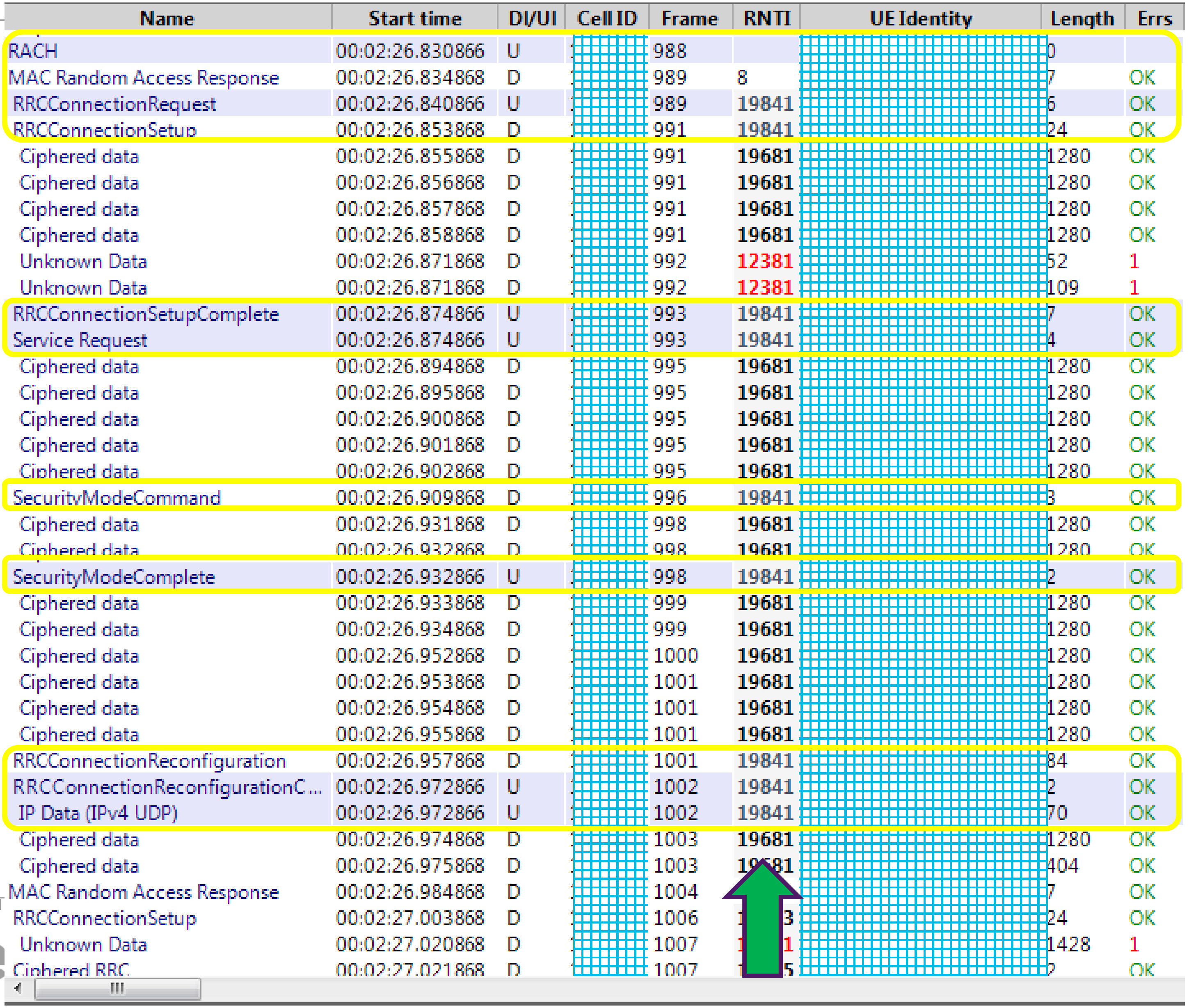
MAC-RND-ACCS-RSP at 00:04:42.946818 since connect

```
MAC Random Access Response
  Sub Header 0
    E 0 => False
    T 1
    RAPID 63
  MAC RAR 0 <NO DATA>
    Reserved OK
    Timing Advance Command 0
    Random Access Response Grant
      Hopping Flag 0 => False
      Fixed size Resource Block Assignment 96
      Truncated MCS 2 => Q'_m = 2  I_TBS = 2  rv_idx = 0
      TPC Command for PUCCH 3 => 0 dB
      UL Delay 0 => False
      CQI Request 0 => False
    T-CRNTI 220
```

```
Bit Length    56  Head  01111111   Tail  11011100   Hex  7F0000C04C00DC
00000000      7F 00 00 C0 4C 00 DC                       ...ÀL.Ü
```

Bloomberg

LOCATION LEAKS AND DEVICE TRACKING



Name	Start time	DI/UI	Cell ID	Frame	RNTI	UE Identity	Length	Errs
RACH	00:02:26.830866	U	[redacted]	988		[redacted]	0	
MAC Random Access Response	00:02:26.834868	D	[redacted]	989	8	[redacted]	7	OK
RRCConnectionRequest	00:02:26.840866	U	[redacted]	989	19841	[redacted]	6	OK
RRCConnectionSetup	00:02:26.853868	D	[redacted]	991	19841	[redacted]	24	OK
Ciphered data	00:02:26.855868	D	[redacted]	991	19681	[redacted]	1280	OK
Ciphered data	00:02:26.856868	D	[redacted]	991	19681	[redacted]	1280	OK
Ciphered data	00:02:26.857868	D	[redacted]	991	19681	[redacted]	1280	OK
Ciphered data	00:02:26.858868	D	[redacted]	991	19681	[redacted]	1280	OK
Unknown Data	00:02:26.871868	D	[redacted]	992	12381	[redacted]	52	1
Unknown Data	00:02:26.871868	D	[redacted]	992	12381	[redacted]	109	1
RRCConnectionSetupComplete	00:02:26.874866	U	[redacted]	993	19841	[redacted]	7	OK
Service Request	00:02:26.874866	U	[redacted]	993	19841	[redacted]	4	OK
Ciphered data	00:02:26.894868	D	[redacted]	995	19681	[redacted]	1280	OK
Ciphered data	00:02:26.895868	D	[redacted]	995	19681	[redacted]	1280	OK
Ciphered data	00:02:26.900868	D	[redacted]	995	19681	[redacted]	1280	OK
Ciphered data	00:02:26.901868	D	[redacted]	995	19681	[redacted]	1280	OK
Ciphered data	00:02:26.902868	D	[redacted]	995	19681	[redacted]	1280	OK
SecurityModeCommand	00:02:26.909868	D	[redacted]	996	19841	[redacted]	3	OK
Ciphered data	00:02:26.931868	D	[redacted]	998	19681	[redacted]	1280	OK
Ciphered data	00:02:26.932868	D	[redacted]	998	19681	[redacted]	1280	OK
SecurityModeComplete	00:02:26.932866	U	[redacted]	998	19841	[redacted]	2	OK
Ciphered data	00:02:26.933868	D	[redacted]	999	19681	[redacted]	1280	OK
Ciphered data	00:02:26.934868	D	[redacted]	999	19681	[redacted]	1280	OK
Ciphered data	00:02:26.952868	D	[redacted]	1000	19681	[redacted]	1280	OK
Ciphered data	00:02:26.953868	D	[redacted]	1001	19681	[redacted]	1280	OK
Ciphered data	00:02:26.954868	D	[redacted]	1001	19681	[redacted]	1280	OK
Ciphered data	00:02:26.955868	D	[redacted]	1001	19681	[redacted]	1280	OK
RRCConnectionReconfiguration	00:02:26.957868	D	[redacted]	1001	19841	[redacted]	84	OK
RRCConnectionReconfigurationC...	00:02:26.972866	U	[redacted]	1002	19841	[redacted]	2	OK
IP Data (IPv4 UDP)	00:02:26.972866	U	[redacted]	1002	19841	[redacted]	70	OK
Ciphered data	00:02:26.974868	D	[redacted]	1003	19681	[redacted]	1280	OK
Ciphered data	00:02:26.975868	D	[redacted]	1003	19681	[redacted]	404	OK
MAC Random Access Response	00:02:26.984868	D	[redacted]	1004	[illegible]	[redacted]	7	OK
RRCConnectionSetup	00:02:27.003868	D	[redacted]	1006	[illegible]	[redacted]	24	OK
Unknown Data	00:02:27.020868	D	[redacted]	1007	[illegible]	[redacted]	1428	1
Ciphered RRC	00:02:27.021868	D	[redacted]	1007	[illegible]	[redacted]	2	OK

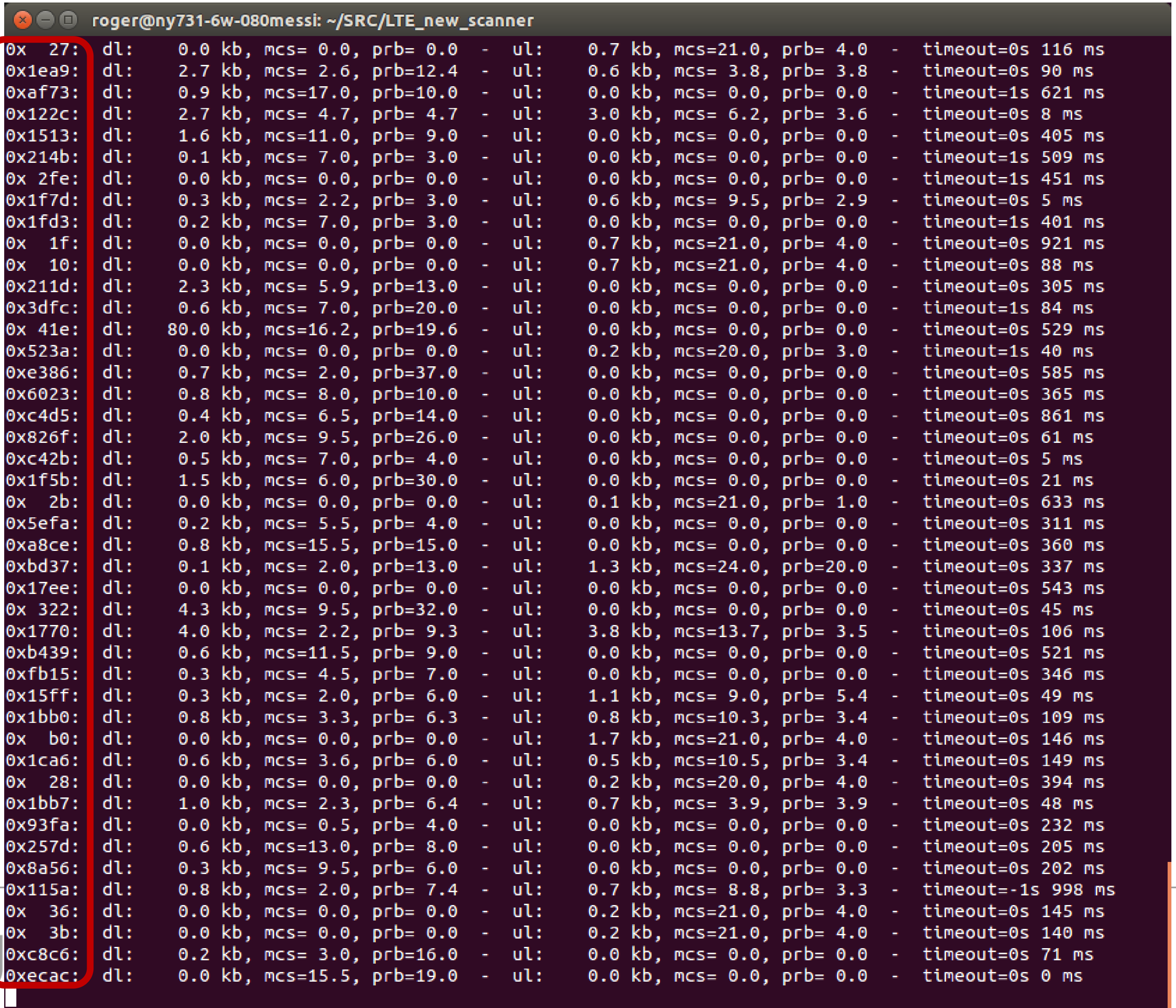
LOCATION LEAKS AND DEVICE TRACKING

- Potential RNTI tracking use cases
  - Know how long you stay at a given location
    - and meanwhile someone robs your house…
  - Estimate the UL and DL load of a given device
    - Signaling traffic on the air interface << Data traffic on the air interface
  - Potentially identify the hot-spot/access point in an LTE-based ad-hoc network

- Phone # - TMSI – RNTI mapping is trivial
  - If the passive sniffer is within the same cell/sector as the target

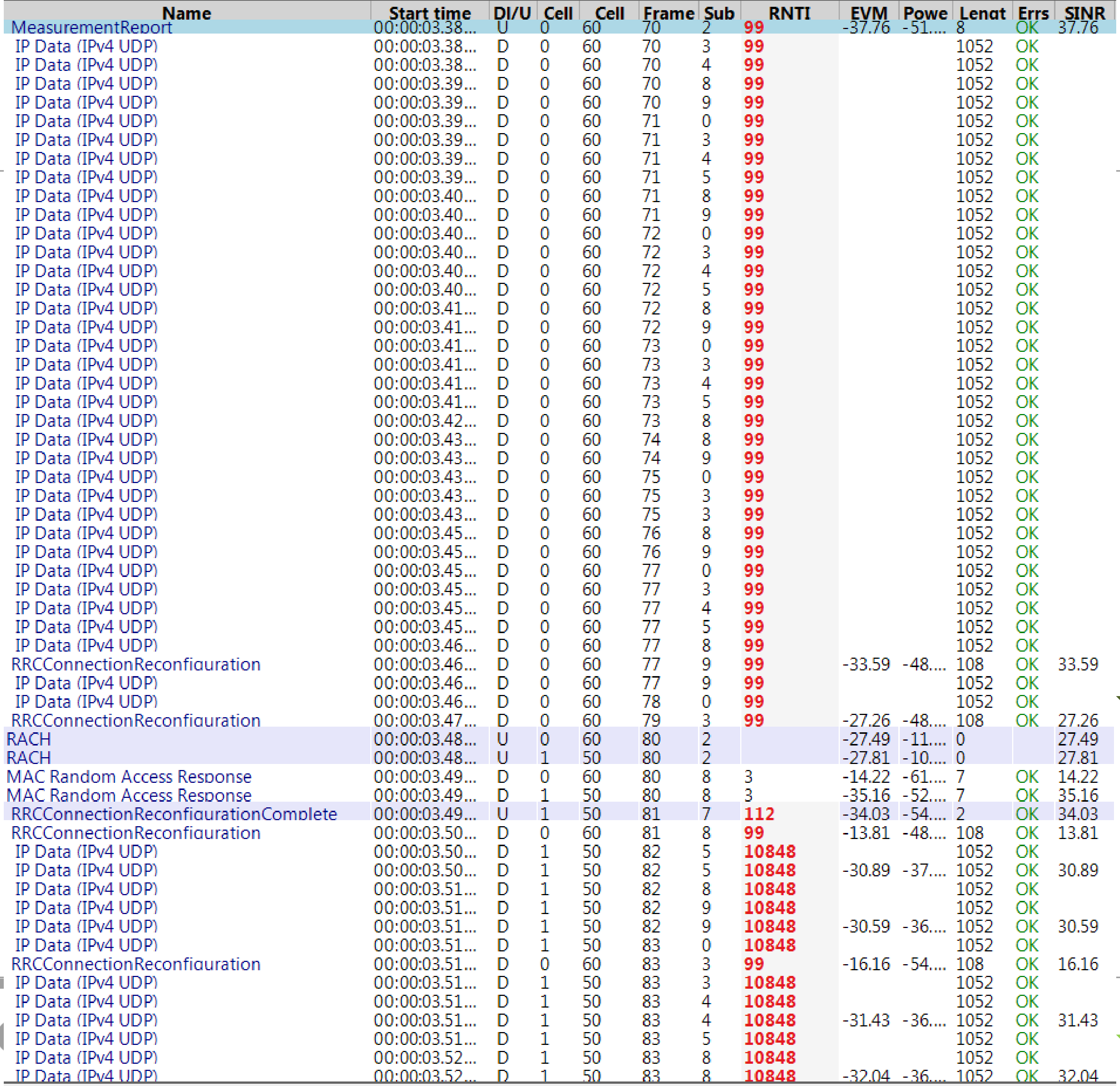
RNTI TRACKING WITH OPEN SOURCE TOOLS

RNTIs being tracked within this cell



roger@ny731-6w-080messi: ~/SRC/LTE_new_scanner

```
0x  27:  dl:    0.0 kb, mcs= 0.0, prb= 0.0  -  ul:    0.7 kb, mcs=21.0, prb= 4.0  -  timeout=0s 116 ms
0x1ea9:  dl:    2.7 kb, mcs= 2.6, prb=12.4  -  ul:    0.6 kb, mcs= 3.8, prb= 3.8  -  timeout=0s 90 ms
0xaf73:  dl:    0.9 kb, mcs=17.0, prb=10.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=1s 621 ms
0x122c:  dl:    2.7 kb, mcs= 4.7, prb= 4.7  -  ul:    3.0 kb, mcs= 6.2, prb= 3.6  -  timeout=0s 8 ms
0x1513:  dl:    1.6 kb, mcs=11.0, prb= 9.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 405 ms
0x214b:  dl:    0.1 kb, mcs= 7.0, prb= 3.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=1s 509 ms
0x 2fe:  dl:    0.0 kb, mcs= 0.0, prb= 0.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=1s 451 ms
0x1f7d:  dl:    0.3 kb, mcs= 2.2, prb= 3.0  -  ul:    0.6 kb, mcs= 9.5, prb= 2.9  -  timeout=0s 5 ms
0x1fd3:  dl:    0.2 kb, mcs= 7.0, prb= 3.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=1s 401 ms
0x  1f:  dl:    0.0 kb, mcs= 0.0, prb= 0.0  -  ul:    0.7 kb, mcs=21.0, prb= 4.0  -  timeout=0s 921 ms
0x  10:  dl:    0.0 kb, mcs= 0.0, prb= 0.0  -  ul:    0.7 kb, mcs=21.0, prb= 4.0  -  timeout=0s 88 ms
0x211d:  dl:    2.3 kb, mcs= 5.9, prb=13.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 305 ms
0x3dfc:  dl:    0.6 kb, mcs= 7.0, prb=20.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=1s 84 ms
0x 41e:  dl:   80.0 kb, mcs=16.2, prb=19.6  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 529 ms
0x523a:  dl:    0.0 kb, mcs= 0.0, prb= 0.0  -  ul:    0.2 kb, mcs=20.0, prb= 3.0  -  timeout=1s 40 ms
0xe386:  dl:    0.7 kb, mcs= 2.0, prb=37.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 585 ms
0x6023:  dl:    0.8 kb, mcs= 8.0, prb=10.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 365 ms
0xc4d5:  dl:    0.4 kb, mcs= 6.5, prb=14.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 861 ms
0x826f:  dl:    2.0 kb, mcs= 9.5, prb=26.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 61 ms
0xc42b:  dl:    0.5 kb, mcs= 7.0, prb= 4.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 5 ms
0x1f5b:  dl:    1.5 kb, mcs= 6.0, prb=30.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 21 ms
0x  2b:  dl:    0.0 kb, mcs= 0.0, prb= 0.0  -  ul:    0.1 kb, mcs=21.0, prb= 1.0  -  timeout=0s 633 ms
0x5efa:  dl:    0.2 kb, mcs= 5.5, prb= 4.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 311 ms
0xa8ce:  dl:    0.8 kb, mcs=15.5, prb=15.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 360 ms
0xbd37:  dl:    0.1 kb, mcs= 2.0, prb=13.0  -  ul:    1.3 kb, mcs=24.0, prb=20.0  -  timeout=0s 337 ms
0x17ee:  dl:    0.0 kb, mcs= 0.0, prb= 0.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 543 ms
0x 322:  dl:    4.3 kb, mcs= 9.5, prb=32.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 45 ms
0x1770:  dl:    4.0 kb, mcs= 2.2, prb= 9.3  -  ul:    3.8 kb, mcs=13.7, prb= 3.5  -  timeout=0s 106 ms
0xb439:  dl:    0.6 kb, mcs=11.5, prb= 9.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 521 ms
0xfb15:  dl:    0.3 kb, mcs= 4.5, prb= 7.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 346 ms
0x15ff:  dl:    0.3 kb, mcs= 2.0, prb= 6.0  -  ul:    1.1 kb, mcs= 9.0, prb= 5.4  -  timeout=0s 49 ms
0x1bb0:  dl:    0.8 kb, mcs= 3.3, prb= 6.3  -  ul:    0.8 kb, mcs=10.3, prb= 3.4  -  timeout=0s 109 ms
0x  b0:  dl:    0.0 kb, mcs= 0.0, prb= 0.0  -  ul:    1.7 kb, mcs=21.0, prb= 4.0  -  timeout=0s 146 ms
0x1ca6:  dl:    0.6 kb, mcs= 3.6, prb= 6.0  -  ul:    0.5 kb, mcs=10.5, prb= 3.4  -  timeout=0s 149 ms
0x  28:  dl:    0.0 kb, mcs= 0.0, prb= 0.0  -  ul:    0.2 kb, mcs=20.0, prb= 4.0  -  timeout=0s 394 ms
0x1bb7:  dl:    1.0 kb, mcs= 2.3, prb= 6.4  -  ul:    0.7 kb, mcs= 3.9, prb= 3.9  -  timeout=0s 48 ms
0x93fa:  dl:    0.0 kb, mcs= 0.5, prb= 4.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 232 ms
0x257d:  dl:    0.6 kb, mcs=13.0, prb= 8.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 205 ms
0x8a56:  dl:    0.3 kb, mcs= 9.5, prb= 6.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 202 ms
0x115a:  dl:    0.8 kb, mcs= 2.0, prb= 7.4  -  ul:    0.7 kb, mcs= 8.8, prb= 3.3  -  timeout=-1s 998 ms
0x  36:  dl:    0.0 kb, mcs= 0.0, prb= 0.0  -  ul:    0.2 kb, mcs=21.0, prb= 4.0  -  timeout=0s 145 ms
0x  3b:  dl:    0.0 kb, mcs= 0.0, prb= 0.0  -  ul:    0.2 kb, mcs=21.0, prb= 4.0  -  timeout=0s 140 ms
0xc8c6:  dl:    0.2 kb, mcs= 3.0, prb=16.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 71 ms
0xecac:  dl:    0.0 kb, mcs=15.5, prb=19.0  -  ul:    0.0 kb, mcs= 0.0, prb= 0.0  -  timeout=0s 0 ms
```

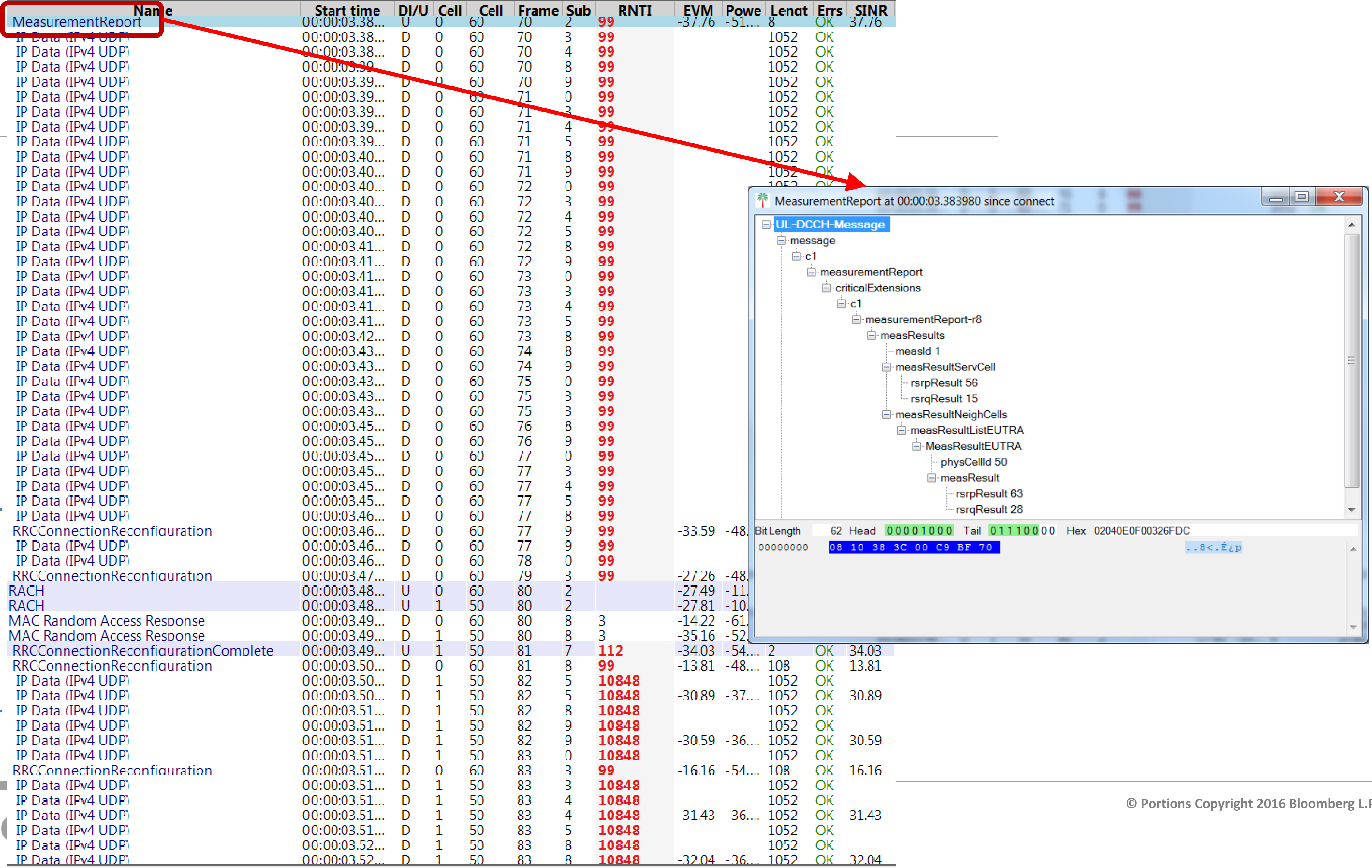


Name	Start time	Dl/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lengt	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	99	-37.76	-51....	8	OK	37.76
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	5	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	5	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	5	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.42...	D	0	60	73	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	5	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	8	99			1052	OK	
RRCConnectionReconfiguration	00:00:03.46...	D	0	60	77	9	99	-33.59	-48....	108	OK	33.59
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	78	0	99			1052	OK	
RRCConnectionReconfiguration	00:00:03.47...	D	0	60	79	3	99	-27.26	-48....	108	OK	27.26
RACH	00:00:03.48...	U	0	60	80	2		-27.49	-11....	0		27.49
RACH	00:00:03.48...	U	1	50	80	2		-27.81	-10....	0		27.81
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-14.22	-61....	7	OK	14.22
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52....	7	OK	35.16
RRCConnectionReconfigurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiguration	00:00:03.50...	D	0	60	81	8	99	-13.81	-48....	108	OK	13.81
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-30.89	-37....	1052	OK	30.89
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiguration	00:00:03.51...	D	0	60	83	3	99	-16.16	-54....	108	OK	16.16
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848	-31.43	-36....	1052	OK	31.43
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848	-32.04	-36....	1052	OK	32.04

Handoff between cell 60 and cell 50

Cell ID = 60

Cell ID = 50



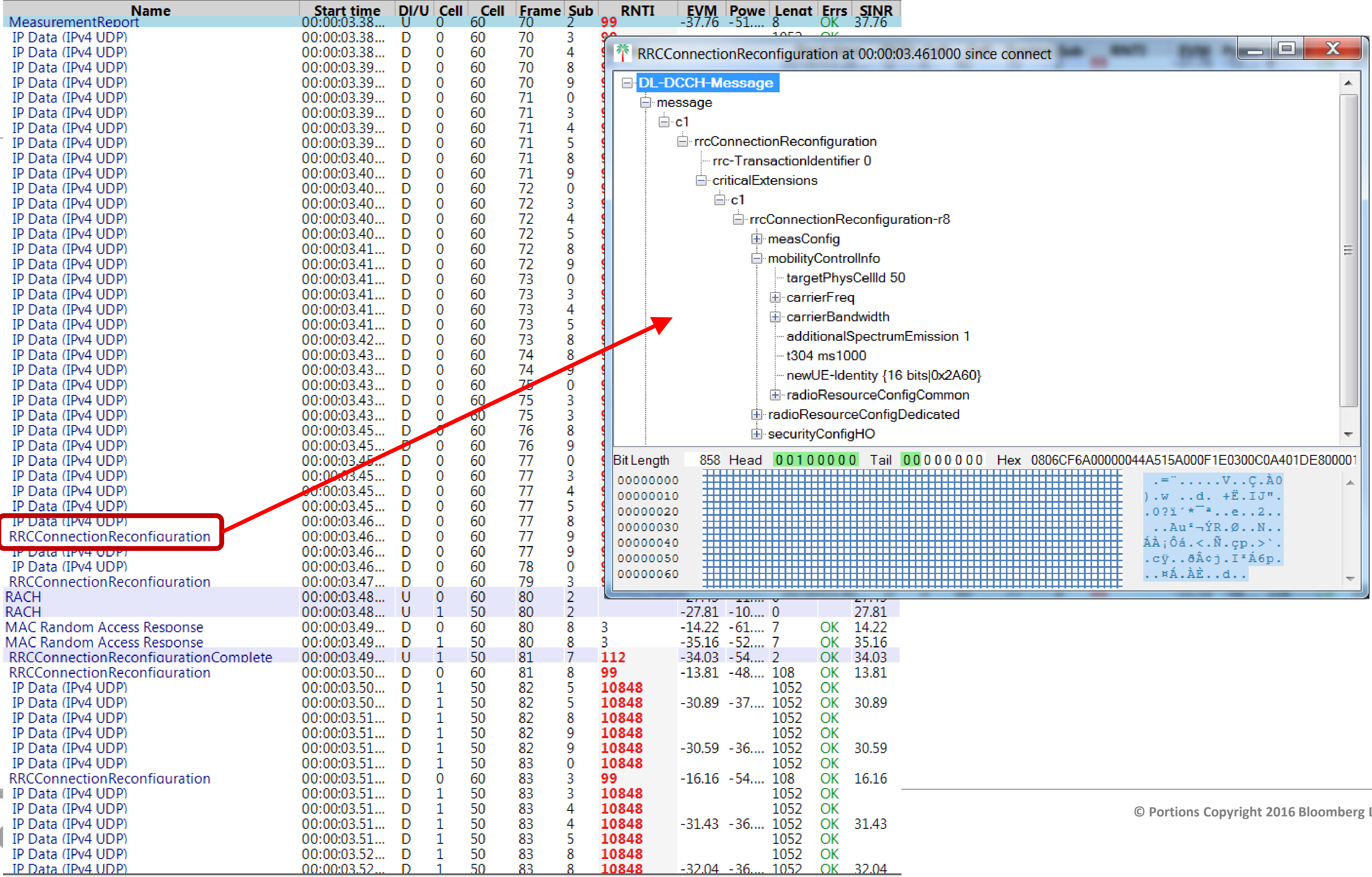
Name	Start time	Dl/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lengt	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	99	-37.76	-51....	8	OK	37.76
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39	D	0	60	70	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	5	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	3	99					
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	4	99					
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	5	99					
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	8	99					
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	9	99					
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	0	99					
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	3	99					
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	4	99					
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	5	99					
IP Data (IPv4 UDP)	00:00:03.42...	D	0	60	73	8	99					
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	8	99					
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	9	99					
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	0	99					
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3	99					
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3	99					
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	8	99					
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	9	99					
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	0	99					
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	3	99					
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	4	99					
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	5	99					
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	8	99					
RRCConnectionReconfiguration	00:00:03.46...	D	0	60	77	9	99	-33.59	-48.			
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	9	99					
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	78	0	99					
RRCConnectionReconfiguration	00:00:03.47...	D	0	60	79	3	99	-27.26	-48.			
RACH	00:00:03.48...	U	0	60	80	2		-27.49	-11.			
RACH	00:00:03.48...	U	1	50	80	2		-27.81	-10.			
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-14.22	-61.			
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52.			
RRCConnectionReconfigurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiguration	00:00:03.50...	D	0	60	81	8	99	-13.81	-48....	108	OK	13.81
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-30.89	-37....	1052	OK	30.89
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiguration	00:00:03.51...	D	0	60	83	3	99	-16.16	-54....	108	OK	16.16
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848	-31.43	-36....	1052	OK	31.43
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848	-32.04	-36....	1052	OK	32.04

MeasurementReport at 00:00:03.383980 since connect

```
UL-DCCH-Message
  message
    c1
      measurementReport
        criticalExtensions
          c1
            measurementReport-r8
              measResults
                measId 1
                measResultServCell
                  rsrpResult 56
                  rsrqResult 15
                measResultNeighCells
                  measResultListEUTRA
                    MeasResultEUTRA
                      physCellId 50
                      measResult
                        rsrpResult 63
                        rsrqResult 28
```

```
Bit Length   62  Head 00001000  Tail 01110000  Hex 02040E0F00326FDC
00000000   08 10 38 3C 00 C9 BF 70        ..8<.É¿p
```

Handoff between cell 60 and cell 50



Handoff between cell 60 and cell 50

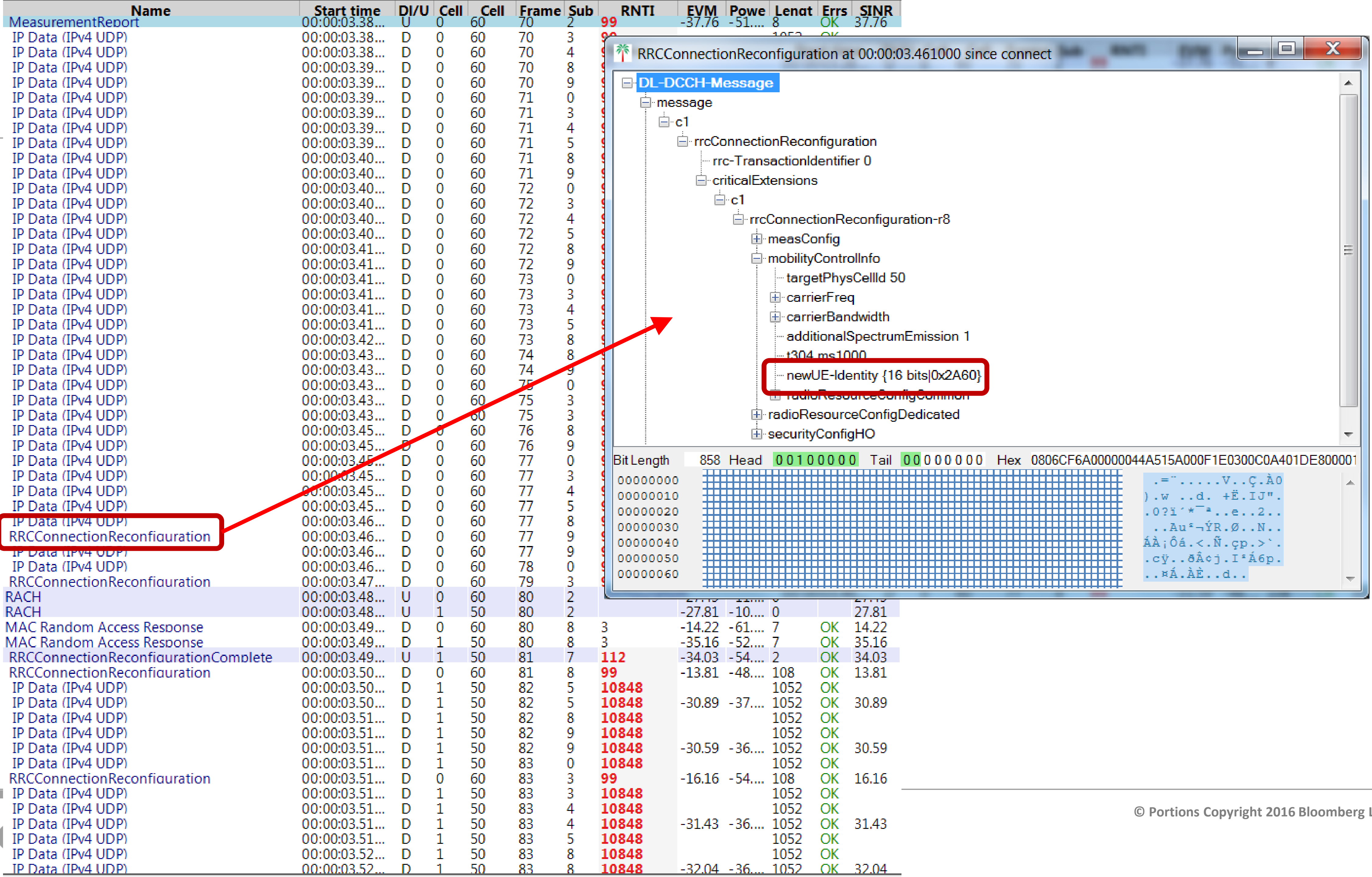
Name	Start time	Dl/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lengt	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	99	-37.76	-51....	8	OK	37.76
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	3						
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	4						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	8						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	9						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	0						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	3						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	4						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	5						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	8						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	9						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	0						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	3						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	4						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	5						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	8						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	9						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	0						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	3						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	4						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	5						
IP Data (IPv4 UDP)	00:00:03.42...	D	0	60	73	8						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	8						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	9						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	0						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	8						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	9						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	0						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	3						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	4						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	5						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	8						
RRCConnectionReconfiguration	00:00:03.46...	D	0	60	77	9						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	9						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	78	0						
RRCConnectionReconfiguration	00:00:03.47...	D	0	60	79	3						
RACH	00:00:03.48...	U	0	60	80	2						
RACH	00:00:03.48...	U	1	50	80	2		-27.81	-10....	0		27.81
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-14.22	-61....	7	OK	14.22
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52....	7	OK	35.16
RRCConnectionReconfigurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiguration	00:00:03.50...	D	0	60	81	8	99	-13.81	-48....	108	OK	13.81
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-30.89	-37....	1052	OK	30.89
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiguration	00:00:03.51...	D	0	60	83	3	99	-16.16	-54....	108	OK	16.16
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848	-31.43	-36....	1052	OK	31.43
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848	-32.04	-36....	1052	OK	32.04

RRCConnectionReconfiguration at 00:00:03.461000 since connect

```
DL-DCCH-Message
  message
    c1
      rrcConnectionReconfiguration
        rrc-TransactionIdentifier 0
        criticalExtensions
          c1
            rrcConnectionReconfiguration-r8
              measConfig
              mobilityControlInfo
                targetPhysCellId 50
                carrierFreq
                carrierBandwidth
                additionalSpectrumEmission 1
                t304 ms1000
                newUE-Identity {16 bits|0x2A60}
                radioResourceConfigCommon
              radioResourceConfigDedicated
              securityConfigHO
```

```
Bit Length   858  Head 00100000  Tail 00000000  Hex 0806CF6A00000044A515A000F1E0300C0A401DE800001
00000000    .=¨.....V..Ç.À0
00000010   ).w ..d. +Ë.IJ".
00000020   .0?ï´*¯ª..e..2..
00000030    ..Au²¬ÝR.Ø..N..
00000040   ÁÀ¡Ôá.<.Ñ.çp.>`.
00000050   .cÿ..ðÂ¢j.I²Á6p.
00000060   ..¤Á.ÀÈ..d..
```

Handoff between cell 60 and cell 50



Name	Start time	DI/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lenqt	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	99	-37.76	-51....	8	OK	37.76
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	3						
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	4						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	8						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	9						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	0						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	3						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	4						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	5						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	8						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	9						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	0						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	3						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	4						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	5						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	8						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	9						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	0						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	3						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	4						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	5						
IP Data (IPv4 UDP)	00:00:03.42...	D	0	60	73	8						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	8						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	9						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	0						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	8						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	9						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	0						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	3						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	4						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	5						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	8						
RRCConnectionReconfiguration	00:00:03.46...	D	0	60	77	9						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	9						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	78	0						
RRCConnectionReconfiguration	00:00:03.47...	D	0	60	79	3						
RACH	00:00:03.48...	U	0	60	80	2						
RACH	00:00:03.48...	U	1	50	80	2		-27.81	-10....	0		27.81
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-14.22	-61....	7	OK	14.22
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52....	7	OK	35.16
RRCConnectionReconfigurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiguration	00:00:03.50...	D	0	60	81	8	99	-13.81	-48....	108	OK	13.81
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-30.89	-37....	1052	OK	30.89
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiguration	00:00:03.51...	D	0	60	83	3	99	-16.16	-54....	108	OK	16.16
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848	-31.43	-36....	1052	OK	31.43
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848	-32.04	-36....	1052	OK	32.04

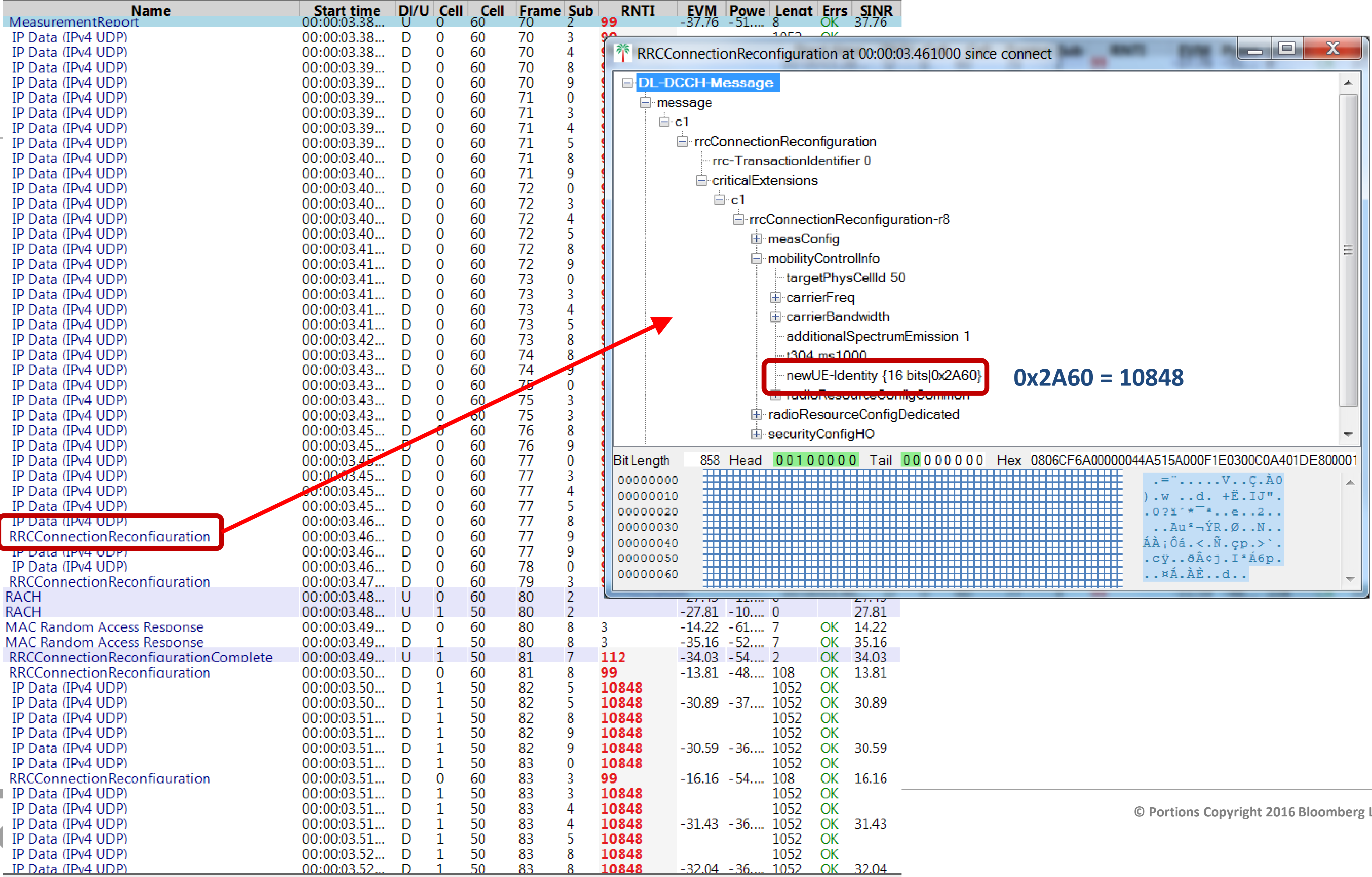
RRCConnectionReconfiguration at 00:00:03.461000 since connect

```
DL-DCCH-Message
  message
    c1
      rrcConnectionReconfiguration
        rrc-TransactionIdentifier 0
        criticalExtensions
          c1
            rrcConnectionReconfiguration-r8
              measConfig
              mobilityControlInfo
                targetPhysCellId 50
                carrierFreq
                carrierBandwidth
                additionalSpectrumEmission 1
                t304 ms1000
                newUE-Identity {16 bits|0x2A60}
                radioResourceConfigCommon
              radioResourceConfigDedicated
              securityConfigHO
```

Bit Length 858 Head 0 0 1 0 0 0 0 0 Tail 0 0 0 0 0 0 0 0 Hex 0806CF6A00000044A515A000F1E0300C0A401DE800001

```
00000000   .=¨.....V..Ç.À0
00000010  ).w ..d. +Ë.IJ".
00000020  .0?ï´*¯ª..e..2..
00000030   ..Auª¬ÝR.Ø..N..
00000040  ÁÀ¡Ôá.<.Ñ.çp.>`.
00000050  .cÿ..ðÂ¢j.I³Á6p.
00000060  ..¤Á.ÀÈ..d..
```

Handoff between cell 60 and cell 50



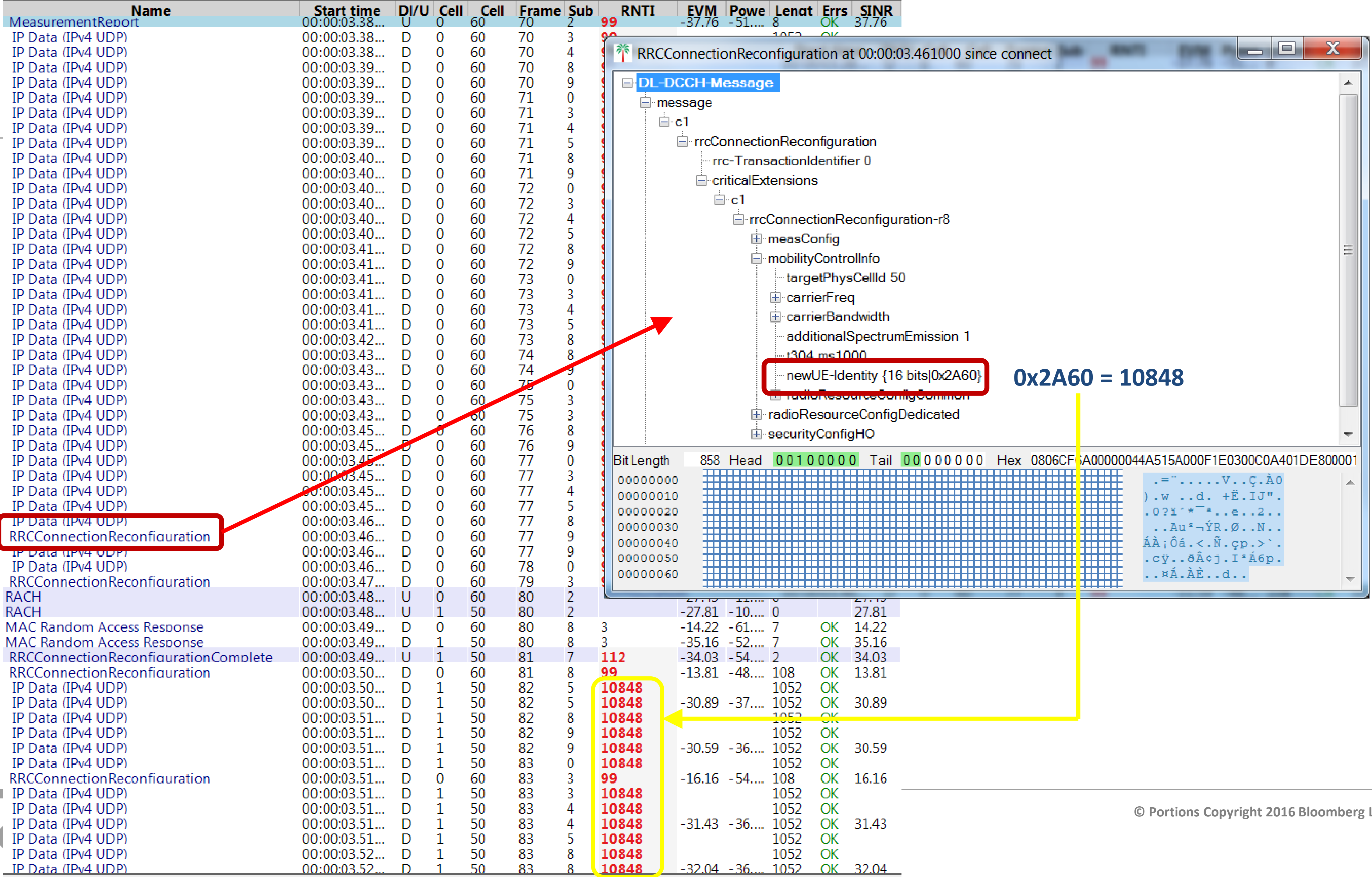
Name	Start time	Dl/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lengt	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	99	-37.76	-51....	8	OK	37.76
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	4						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	8						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	9						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	0						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	3						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	4						
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	5						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	8						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71	9						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	0						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	3						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	4						
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72	5						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	8						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72	9						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	0						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	3						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	4						
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73	5						
IP Data (IPv4 UDP)	00:00:03.42...	D	0	60	73	8						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	8						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74	9						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	0						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3						
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75	3						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	8						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76	9						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	0						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	3						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	4						
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77	5						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	8						
RRCConnectionReconfiguration	00:00:03.46...	D	0	60	77	9						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77	9						
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	78	0						
RRCConnectionReconfiguration	00:00:03.47...	D	0	60	79	3						
RACH	00:00:03.48...	U	0	60	80	2						
RACH	00:00:03.48...	U	1	50	80	2		-27.81	-10....	0		27.81
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-14.22	-61....	7	OK	14.22
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52....	7	OK	35.16
RRCConnectionReconfigurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiguration	00:00:03.50...	D	0	60	81	8	99	-13.81	-48....	108	OK	13.81
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-30.89	-37....	1052	OK	30.89
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiguration	00:00:03.51...	D	0	60	83	3	99	-16.16	-54....	108	OK	16.16
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848	-31.43	-36....	1052	OK	31.43
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848	-32.04	-36....	1052	OK	32.04

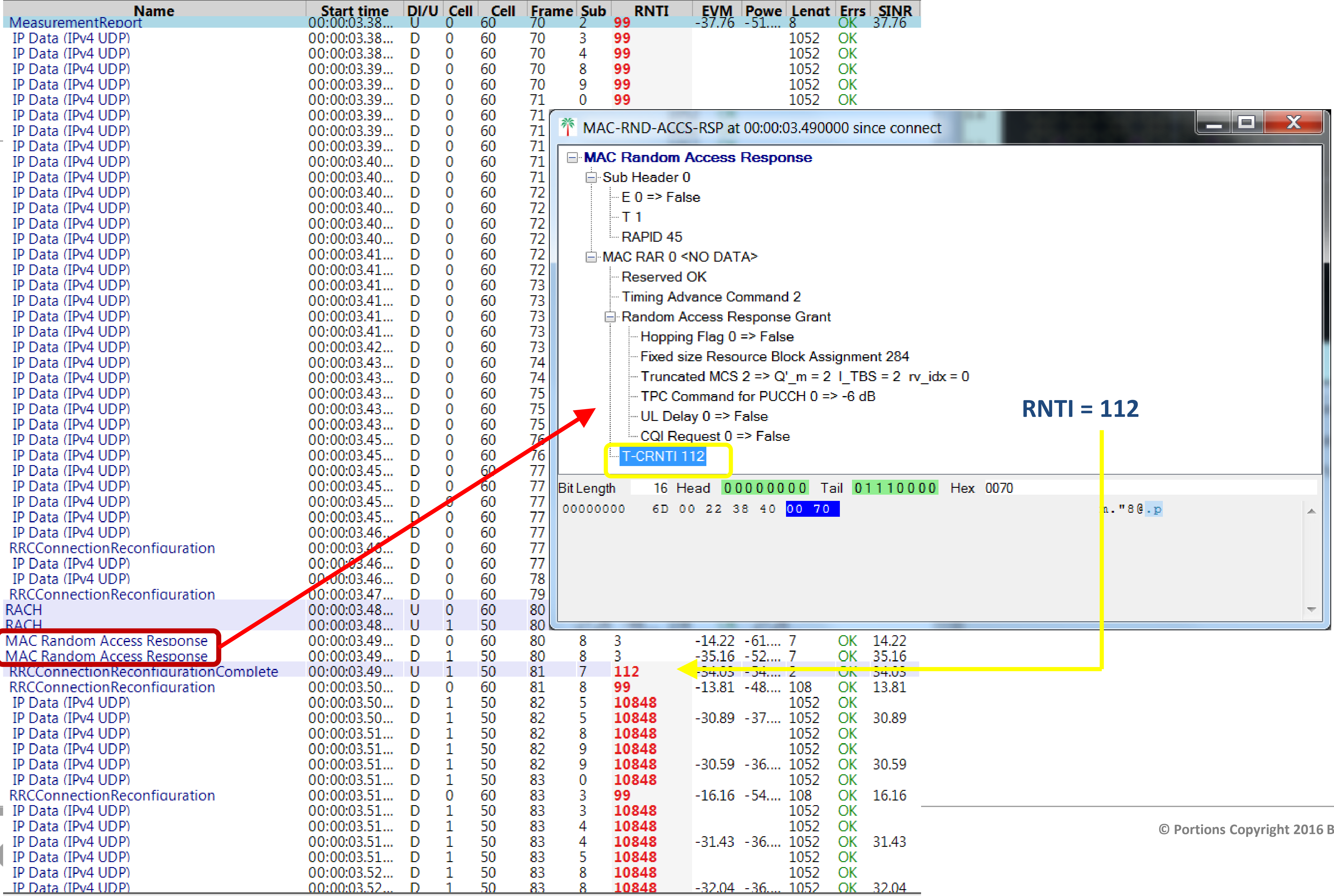
RRCConnectionReconfiguration at 00:00:03.461000 since connect

```
DL-DCCH-Message
  message
    c1
      rrcConnectionReconfiguration
        rrc-TransactionIdentifier 0
        criticalExtensions
          c1
            rrcConnectionReconfiguration-r8
              measConfig
              mobilityControlInfo
                targetPhysCellId 50
                carrierFreq
                carrierBandwidth
                additionalSpectrumEmission 1
                t304 ms1000
                newUE-Identity {16 bits|0x2A60}
                radioResourceConfigCommon
              radioResourceConfigDedicated
              securityConfigHO
```

```
Bit Length   858  Head 0 0 1 0 0 0 0 0   Tail 0 0 0 0 0 0 0 0   Hex 0806CF6A00000044A515A000F1E0300C0A401DE800001
00000000   .=¨.....V..Ç.À0
00000010   ).w ..d. +Ë.IJ".
00000020   .0?ï´*¯ª..e..2..
00000030   ..Au²¬ÝR.Ø..N..
00000040   ÁÀ¡Ôá.<.Ñ.çp.>`.
00000050   .cÿ..ðÂ¢j.I²Á6p.
00000060   ..¤Á.ÀÈ..d..
```

0x2A60 = 10848





Name	Start time	Dl/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lenat	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	99	-37.76	-51....	8	OK	37.76
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	9	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71	0	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.42...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77							
RRCConnectionReconfiguration	00:00:03.46...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	78							
RRCConnectionReconfiguration	00:00:03.47...	D	0	60	79							
RACH	00:00:03.48...	U	0	60	80							
RACH	00:00:03.48...	U	1	50	80							
MAC Random Access Response	00:00:03.49...	D	0	60	80	8	3	-14.22	-61....	7	OK	14.22
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52....	7	OK	35.16
RRCConnectionReconfigurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-34....	2	OK	34.03
RRCConnectionReconfiguration	00:00:03.50...	D	0	60	81	8	99	-13.81	-48....	108	OK	13.81
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-30.89	-37....	1052	OK	30.89
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiguration	00:00:03.51...	D	0	60	83	3	99	-16.16	-54....	108	OK	16.16
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848	-31.43	-36....	1052	OK	31.43
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848	-32.04	-36....	1052	OK	32.04

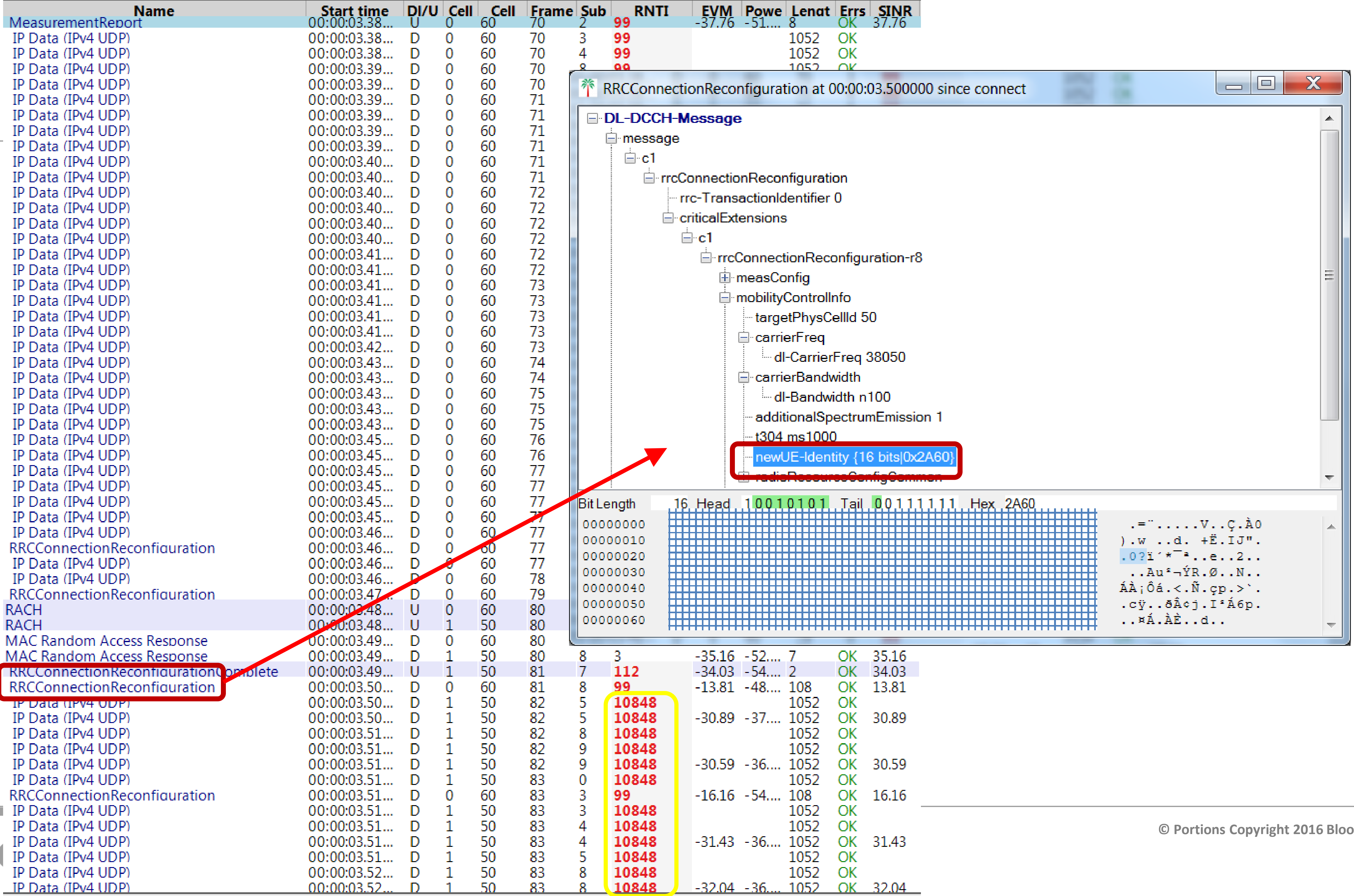
MAC-RND-ACCS-RSP at 00:00:03.490000 since connect

```
MAC Random Access Response
  Sub Header 0
    E 0 => False
    T 1
    RAPID 45
  MAC RAR 0 <NO DATA>
    Reserved OK
    Timing Advance Command 2
    Random Access Response Grant
      Hopping Flag 0 => False
      Fixed size Resource Block Assignment 284
      Truncated MCS 2 => Q'_m = 2  I_TBS = 2  rv_idx = 0
      TPC Command for PUCCH 0 => -6 dB
      UL Delay 0 => False
      CQI Request 0 => False
    T-CRNTI 112
```

```
Bit Length   16  Head  00000000   Tail  01110000   Hex  0070
00000000   6D 00 22 38 40 00 70                    m."8@.p
```

Handoff between cell 60 and cell 50

Handoff between cell 60 and cell 50



Name	Start time	DI/U	Cell	Cell	Frame	Sub	RNTI	EVM	Powe	Lengt	Errs	SINR
MeasurementReport	00:00:03.38...	U	0	60	70	2	99	-37.76	-51....	8	OK	37.76
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	3	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.38...	D	0	60	70	4	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70	8	99			1052	OK	
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	70							
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.39...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	71							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.40...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	72							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.41...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.42...	D	0	60	73							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	74							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75							
IP Data (IPv4 UDP)	00:00:03.43...	D	0	60	75							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	76							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.45...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77							
RRCConnectionReconfiguration	00:00:03.46...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	77							
IP Data (IPv4 UDP)	00:00:03.46...	D	0	60	78							
RRCConnectionReconfiguration	00:00:03.47...	D	0	60	79							
RACH	00:00:03.48...	U	0	60	80							
RACH	00:00:03.48...	U	1	50	80							
MAC Random Access Response	00:00:03.49...	D	0	60	80							
MAC Random Access Response	00:00:03.49...	D	1	50	80	8	3	-35.16	-52....	7	OK	35.16
RRCConnectionReconfigurationComplete	00:00:03.49...	U	1	50	81	7	112	-34.03	-54....	2	OK	34.03
RRCConnectionReconfiguration	00:00:03.50...	D	0	60	81	8	99	-13.81	-48....	108	OK	13.81
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.50...	D	1	50	82	5	10848	-30.89	-37....	1052	OK	30.89
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	82	9	10848	-30.59	-36....	1052	OK	30.59
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	0	10848			1052	OK	
RRCConnectionReconfiguration	00:00:03.51...	D	0	60	83	3	99	-16.16	-54....	108	OK	16.16
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	3	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	4	10848	-31.43	-36....	1052	OK	31.43
IP Data (IPv4 UDP)	00:00:03.51...	D	1	50	83	5	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848			1052	OK	
IP Data (IPv4 UDP)	00:00:03.52...	D	1	50	83	8	10848	-32.04	-36....	1052	OK	32.04

RRCConnectionReconfiguration at 00:00:03.500000 since connect

```
DL-DCCH-Message
  message
    c1
      rrcConnectionReconfiguration
        rrc-TransactionIdentifier 0
        criticalExtensions
          c1
            rrcConnectionReconfiguration-r8
              measConfig
              mobilityControlInfo
                targetPhysCellId 50
                carrierFreq
                  dl-CarrierFreq 38050
                carrierBandwidth
                  dl-Bandwidth n100
                additionalSpectrumEmission 1
                t304 ms1000
                newUE-Identity {16 bits|0x2A60}
              radioResourceConfigCommon
```

```
Bit Length   16  Head  1 0 0 1 0 1 0 1  Tail  0 0 1 1 1 1 1 1  Hex  2A60

00000000      .=¨.....V..Ç.À0
00000010     ).w  ..d. +Ë.IJ".
00000020     .0?ï´*¯ª..e..2..
00000030      ..Auª¬ÝR.Ø..N..
00000040     ÁÀ¡Ôá.<.Ñ.çp.>`.
00000050     .cÿ..ðÂ¢j.IªÁ6p.
00000060     ..¤Á.ÀÈ..d..
```

© Portions Copyright 2016 Bloomberg L.P.

LOCATION LEAKS AND DEVICE TRACKING

- According to 3GPP TS 36.300, 36.331, 36.211, 36.212, 36.213, 36.321
  - C-RNTI is a unique identification used for identifying RRC Connection and scheduling which is dedicated to a particular UE.
  - After connection establishment or re-establishment the Temporary C-RNTI (as explained above) is promoted to C-RNTI.
  - During Handovers within E-UTRA or from other RAT to E-UTRA, C-RNTI is explicitly provided by the eNB in MobilityControlInfo container with IE newUE-Identity.

- No specific guidelines on how often to refresh the RNTI and how to assign it
  - In my passive analysis I have seen RNTIs unchanged for long periods of time
  - Often RNTI_new_user = RNTI_assigned_last + 1

CHALLENGES AND SOLUTIONS

- Potential solutions
  - Refresh the RNTI each time the UE goes from idle to connected
  - Randomize RNTI
  - Analyze the necessity of explicitly indicating the RNTI in the handover message
- If RNTI is not refreshed rather frequently
  - MIT+Bell Labs work - LTE Radio Analytics Made Easy and Accessible (SigComm'14)
  - Track a device and map measurements to it based on RNTI (paper's section 8.7)
  - When RNTI changes, PHY layer measurements still allow to map it to a given UE (SINR, RSSI, etc)
    - MIMO measurements and metrics
- Recent discussion with GSMA
  - The RRC Connection Reconfiguration message should be sent encrypted – This would make tracking more difficult
  - But one could monitor traffic from adjacent cells and wait to see new RNTI with similar RF/traffic signature
  - Ongoing discussions to address these potential issues

WRAP UP

LTE SECURITY AND PROTOCOL EXPLOITS

- Mobile network security is fun
- Mobile network security is IMPORTANT
- The more people working on this the better
- Academia and grad students
  - Very HOT research topic
  - Open source tools + low cost software-radio
  - A grad student has way more time to work on this than me
- My goal – Raise awareness, trigger conversations at 3GPP/GSMA/ETSI/etc and help improve the security of mobile networks

Q&A

http://www.ee.columbia.edu/~roger/ ---- 🐦 @rgoestotheshows