

On Her Majesty's Secret Service - GRX & A spy agency

HITB Amsterdam 2014

Stephen Kho/ Rob Kuiters

29 May 2014



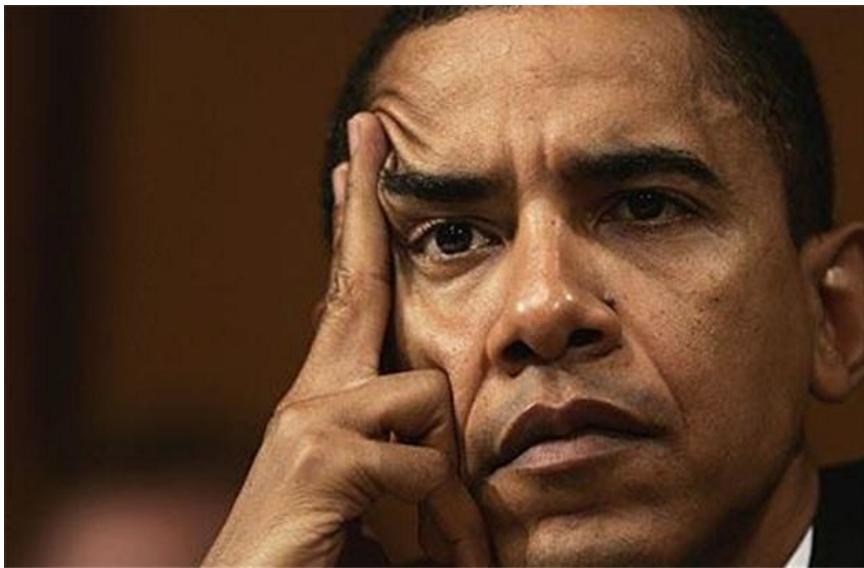
Agenda

- Who we are & why we are giving this talk
- The what, why & who - GRX
- GRX architecture & protocols
- GRX landscape – what we found & why it is interesting
- Vulnerabilities, attack vectors & techniques interesting to spy agencies
- Mitigation & best practises
- Conclusions
- Q&A

Who we are & why this talk

- Stephen Kho & Rob Kuiters
- KPN CISO Team
- KPN-CERT & REDteam
- Penetration Testing & Incident Response
- Overview of GRX & why the interest (from spy agencies)
- Provide understanding of components, protocols, vulnerabilities & attack vectors

Why



This Talk?

Why this talk?

TOP SECRET STRAP 2

One Month Later – OP SOCIALIST

- Scoping session conducted – main focus to be on enabling CNE access to **BELGACOM GRX Operator**
- **Ultimate Goal – enable CNE access to BELGACOM Core GRX Routers from which we can undertake MiTM operations against targets roaming using Smart Phones.**
- Secondary focus – breadth of knowledge on GRX Operators
- Operations Manager assigned, team assembles



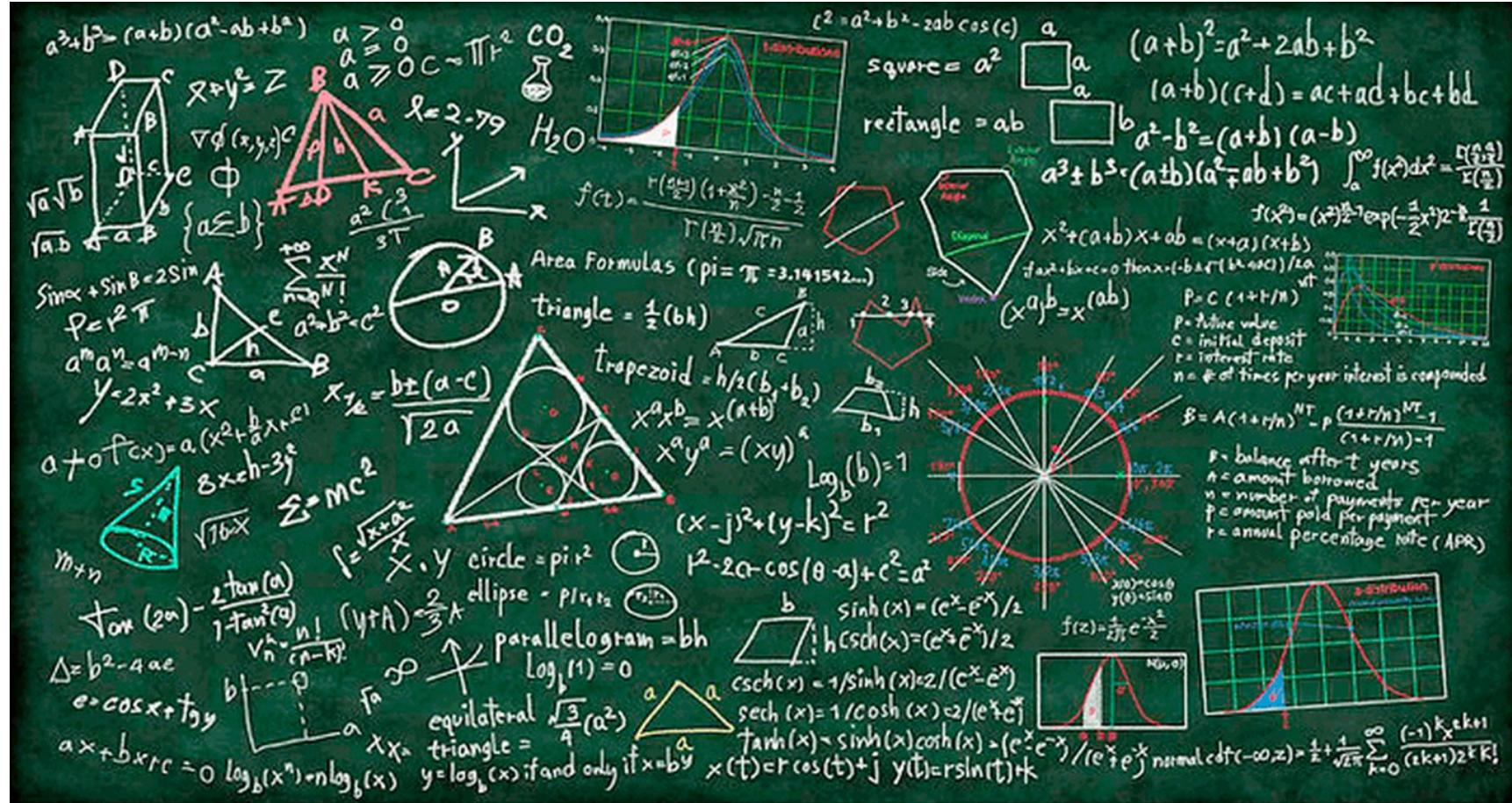
Why this talk?



Why this talk?



The Concept



The Concept Death by abbreviations

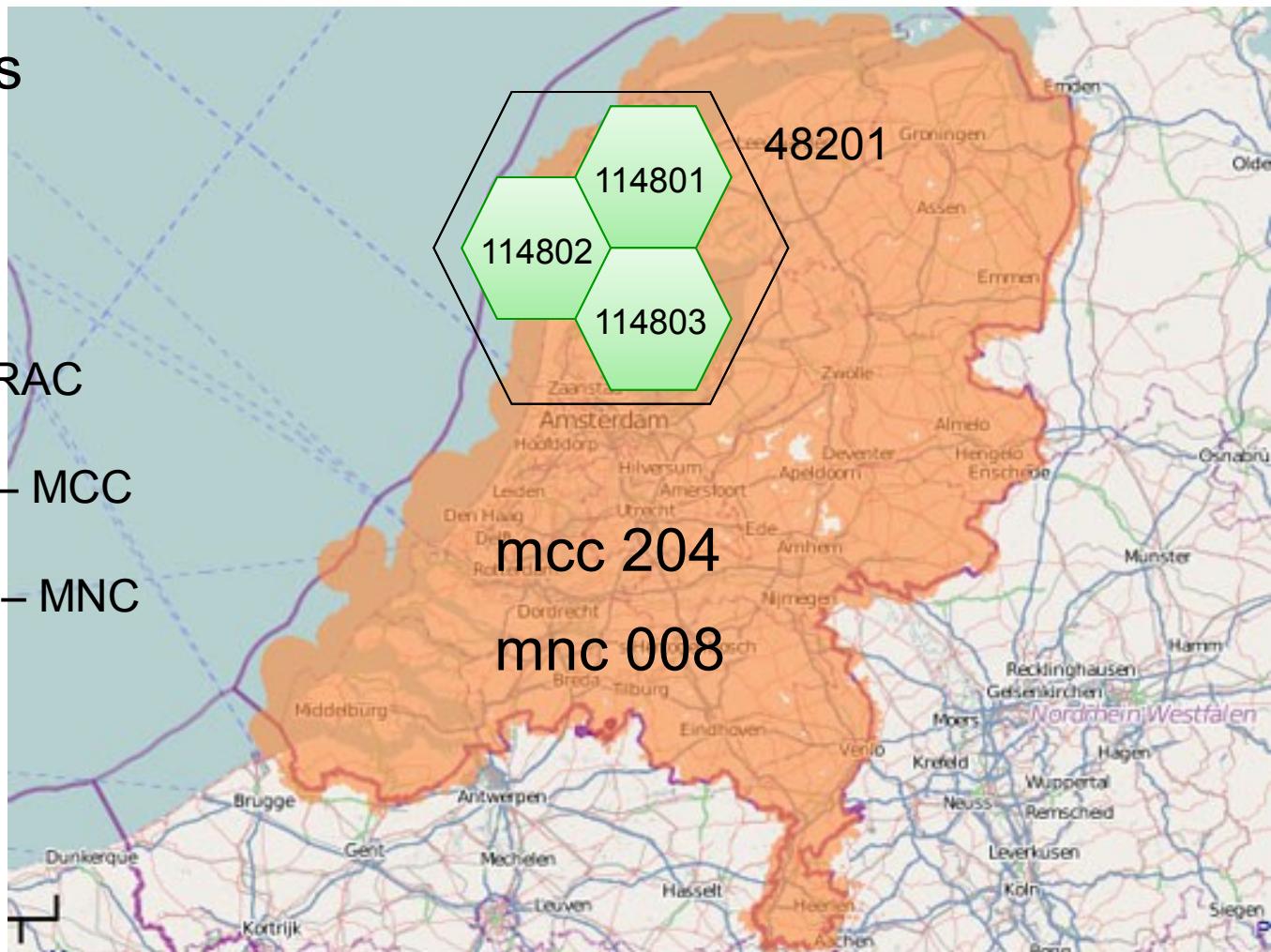
Mobility identifiers

Cell Identifier - CI

Routing Area Code – RAC

Mobile Country Code – MCC

Mobile Network Code – MNC



MCC	MNC	ISO	Country	▲	Country	Network
				Code	Code	
204	14	nl	Netherlands	31	6GMOBILE BV	
204	23	nl	Netherlands	31	Aspider Solutions	
204	05	nl	Netherlands	31	Elephant Talk Communications Premium Rate Services Netherlands BV	
204	17	nl	Netherlands	31	Intercity Mobile Communications BV	
204	10	nl	Netherlands	31	KPN Telecom B.V.	
204	08	nl	Netherlands	31	KPN Telecom B.V.	
204	69	nl	Netherlands	31	KPN Telecom B.V.	
204	12	nl	Netherlands	31	KPN/Telfort	
204	28	nl	Netherlands	31	Lancelot BV	
204	09	nl	Netherlands	31	Lycamobile Ltd	
204	06	nl	Netherlands	31	Mundio/Vectone Mobile	
204	21	nl	Netherlands	31	NS Railinfrabeheer B.V.	
204	24	nl	Netherlands	31	Private Mobility Nederland BV	
204	98	nl	Netherlands	31	T-Mobile B.V.	
204	16	nl	Netherlands	31	T-Mobile B.V.	
204	20	nl	Netherlands	31	Orange/T-mobile	
204	02	nl	Netherlands	31	Tele2	
204	07	nl	Netherlands	31	Teleena Holding BV	
204	68	nl	Netherlands	31	Unify Mobile	
204	18	nl	Netherlands	31	UPC Nederland BV	
204	04	nl	Netherlands	31	Vodafone Libertel	
204	03	nl	Netherlands	31	Voiceworks Mobile BV	
204	15	nl	Netherlands	31	Ziggo BV	

The Concept Death by Abbreviations

Access Point Name – APN

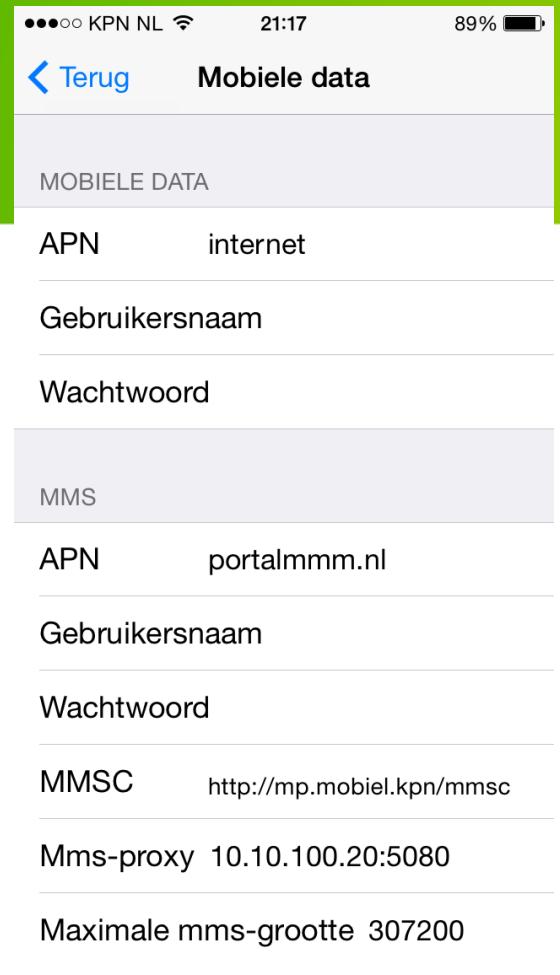
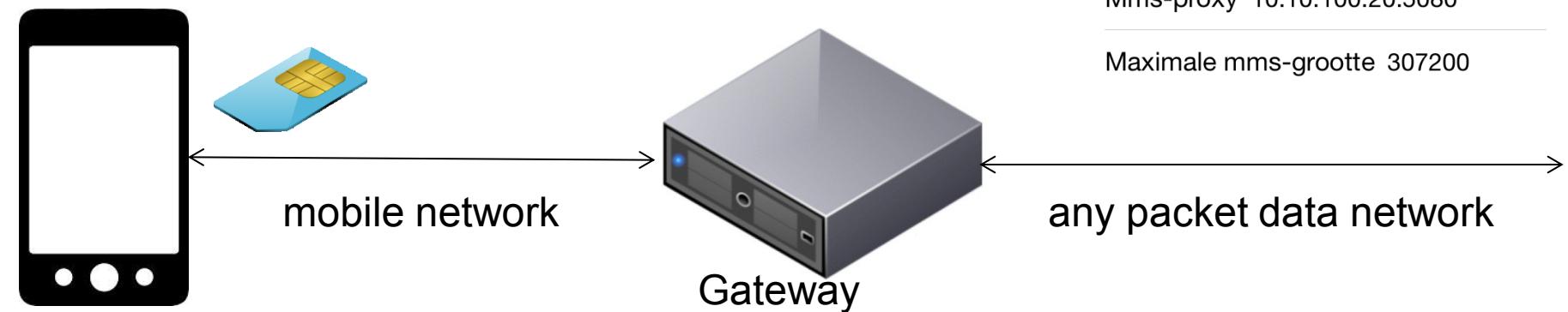
International Mobile Subscriber Identity – IMSI

Universal Integrated Circuit Card – UICC

Packet Data Protocol Context – PDP Context

internet.mnc008.mcc204.gprs

internet.mnc008.mcc204.3gppnetworks.org



The Concept Elements



Radio (BTS / nodeB)



Home Location Register



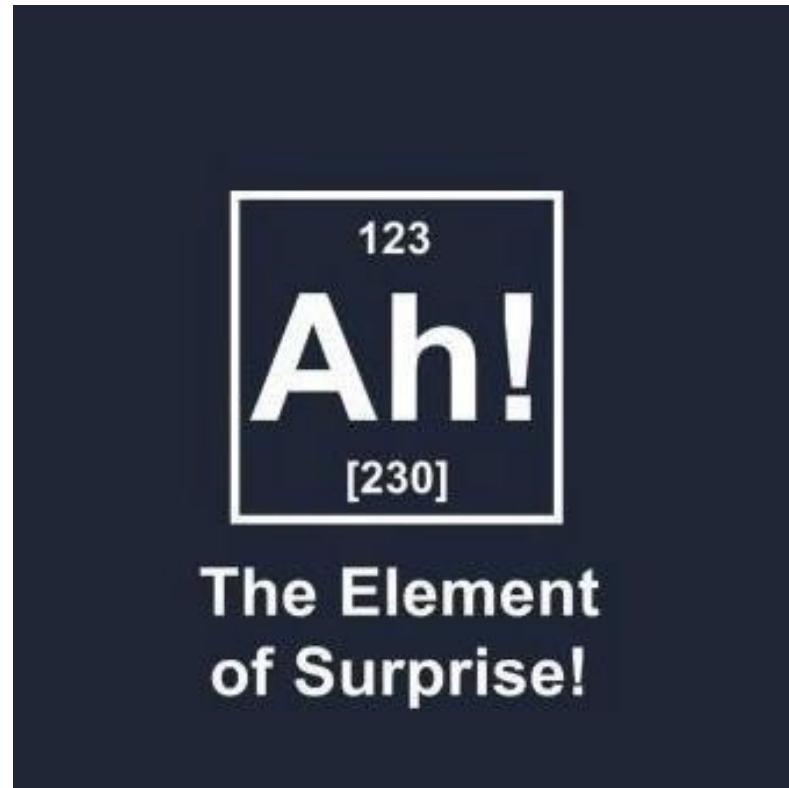
Serving GPRS support node



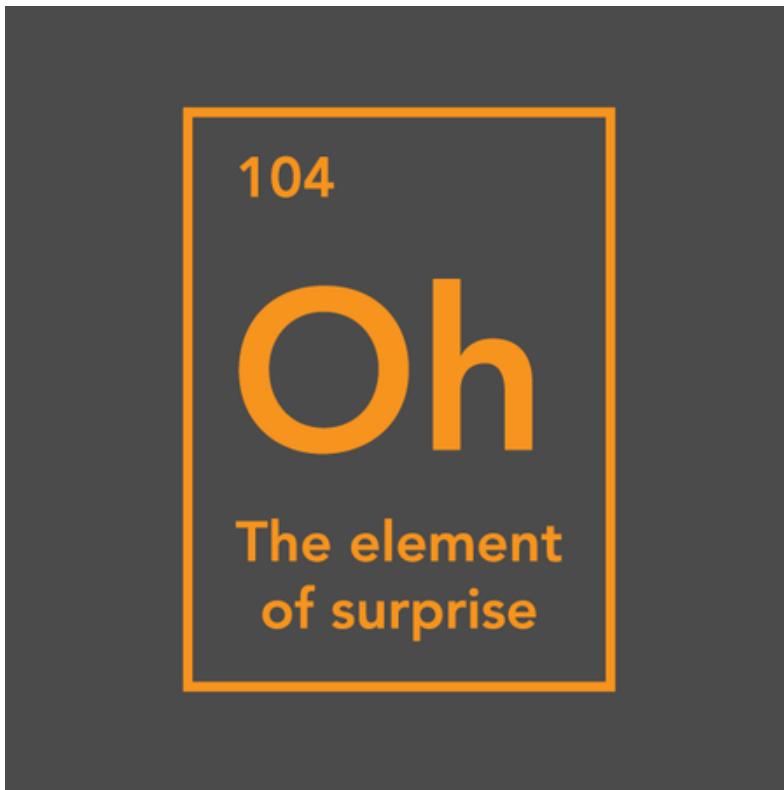
Gateway GPRS support node



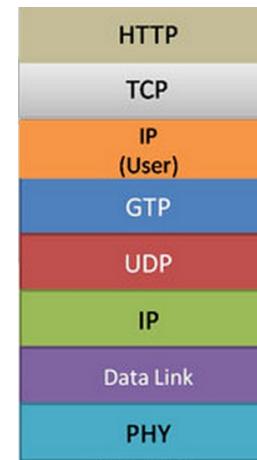
Domain Name Server



The Concept Elements

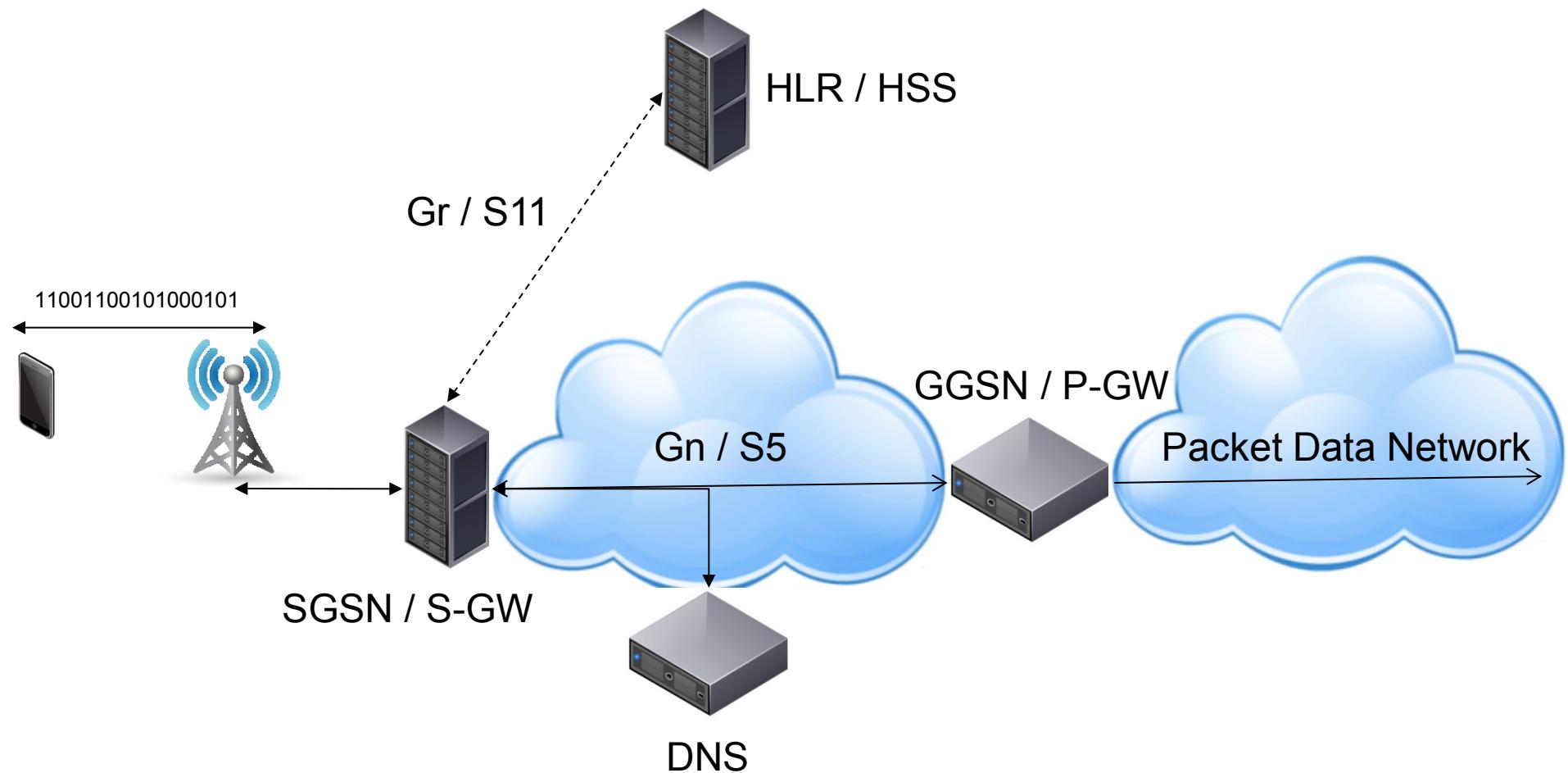


Networks

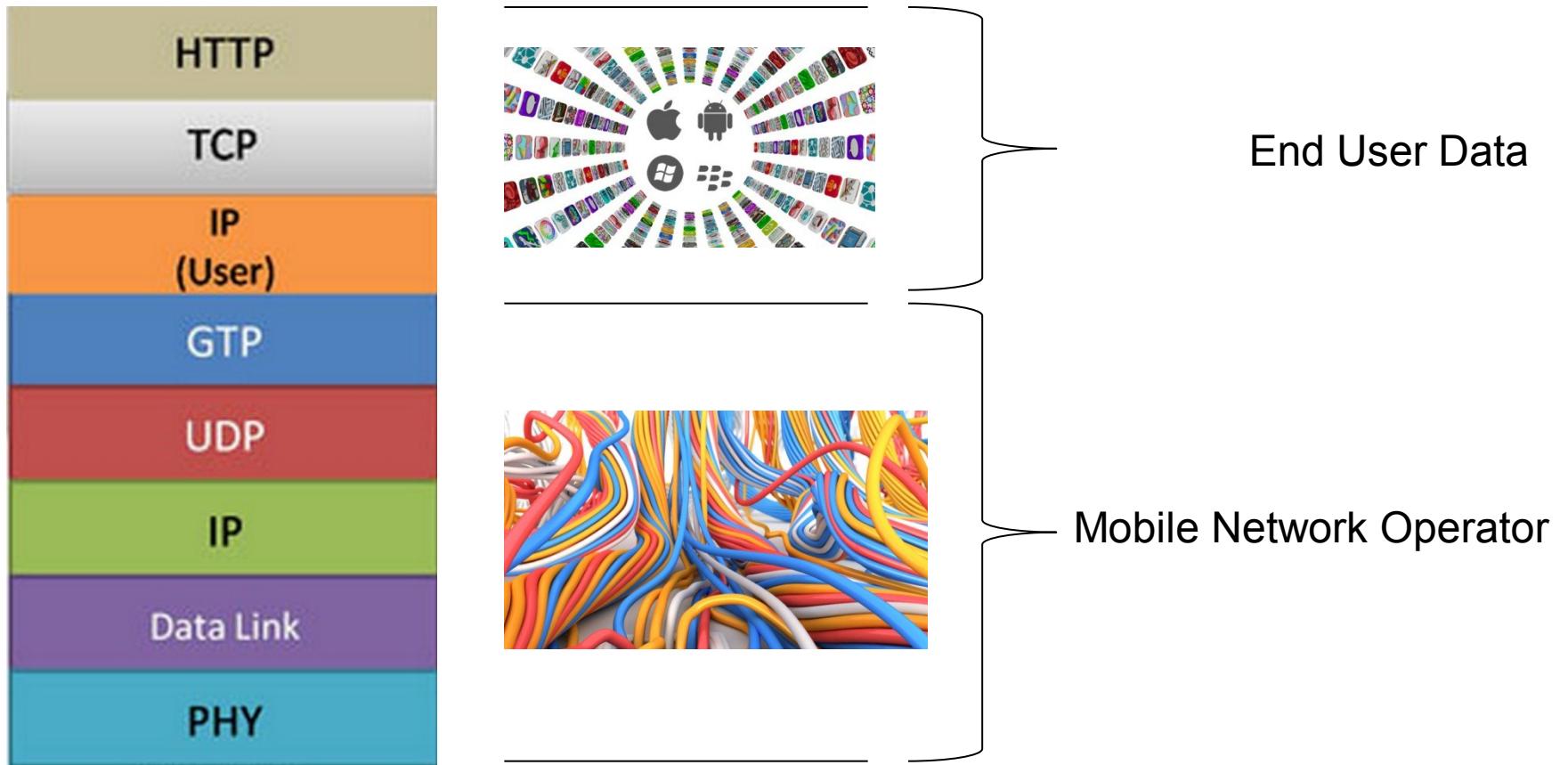


Protocols

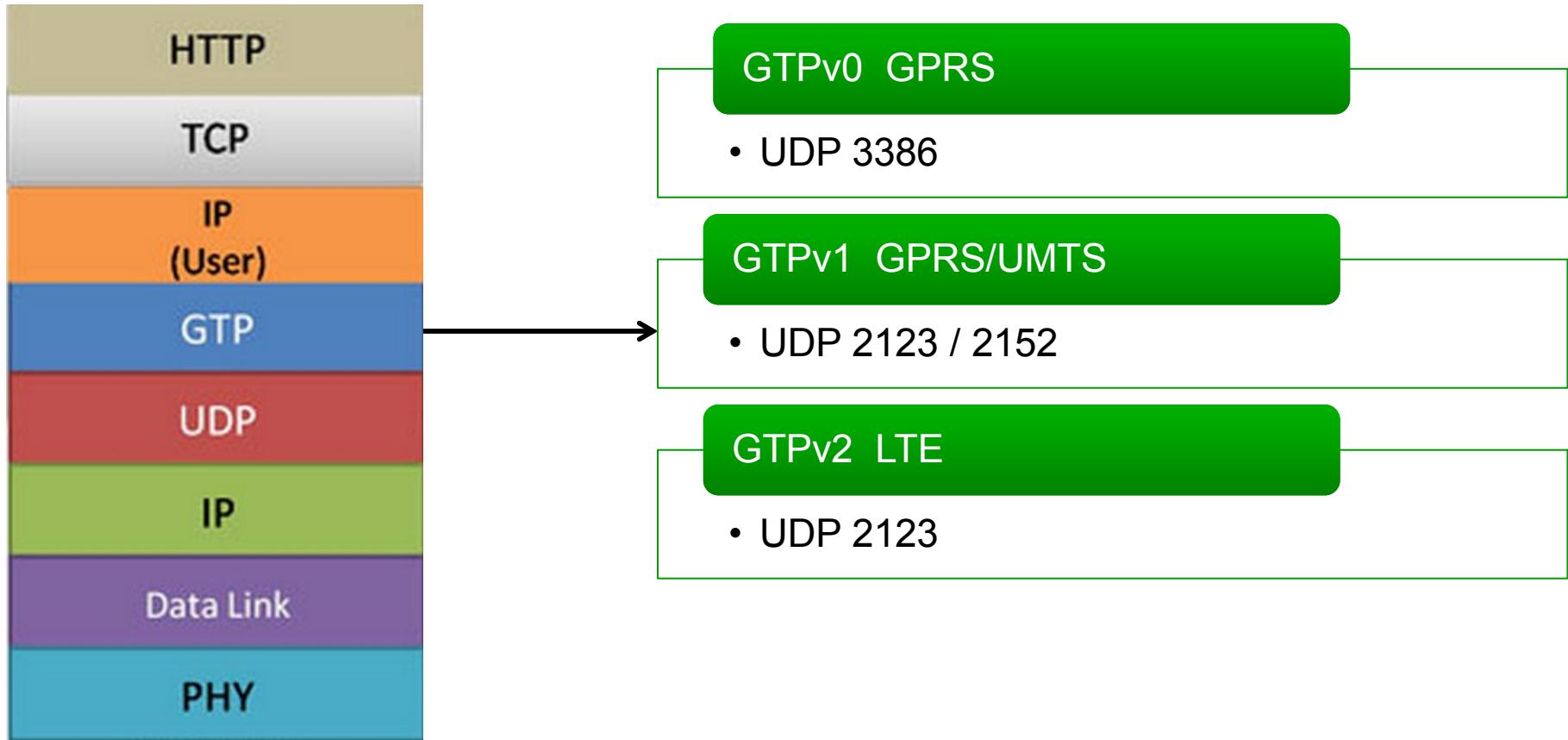
Connecting the Dots



GPRS Tunneling Protocol

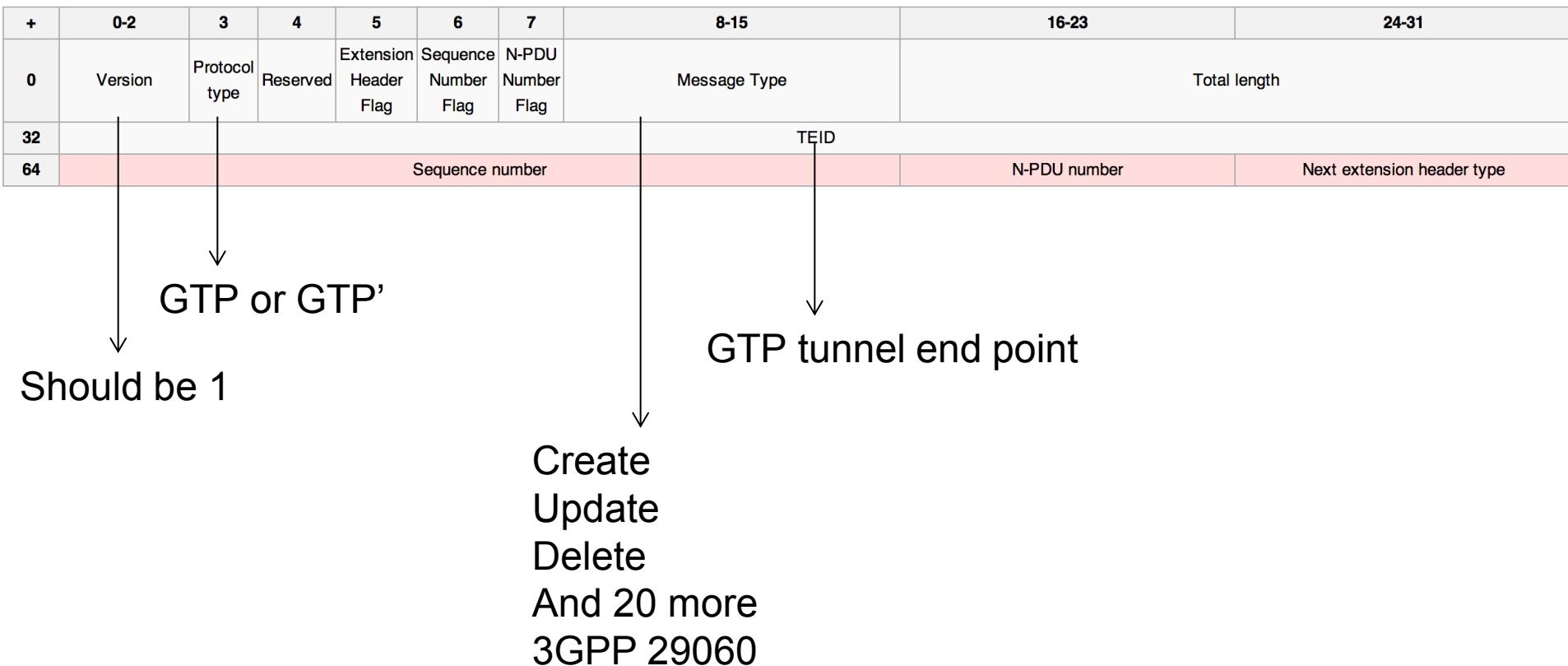


GPRS Tunneling Protocol



GPRS Tunneling protocol Header

GTPv1



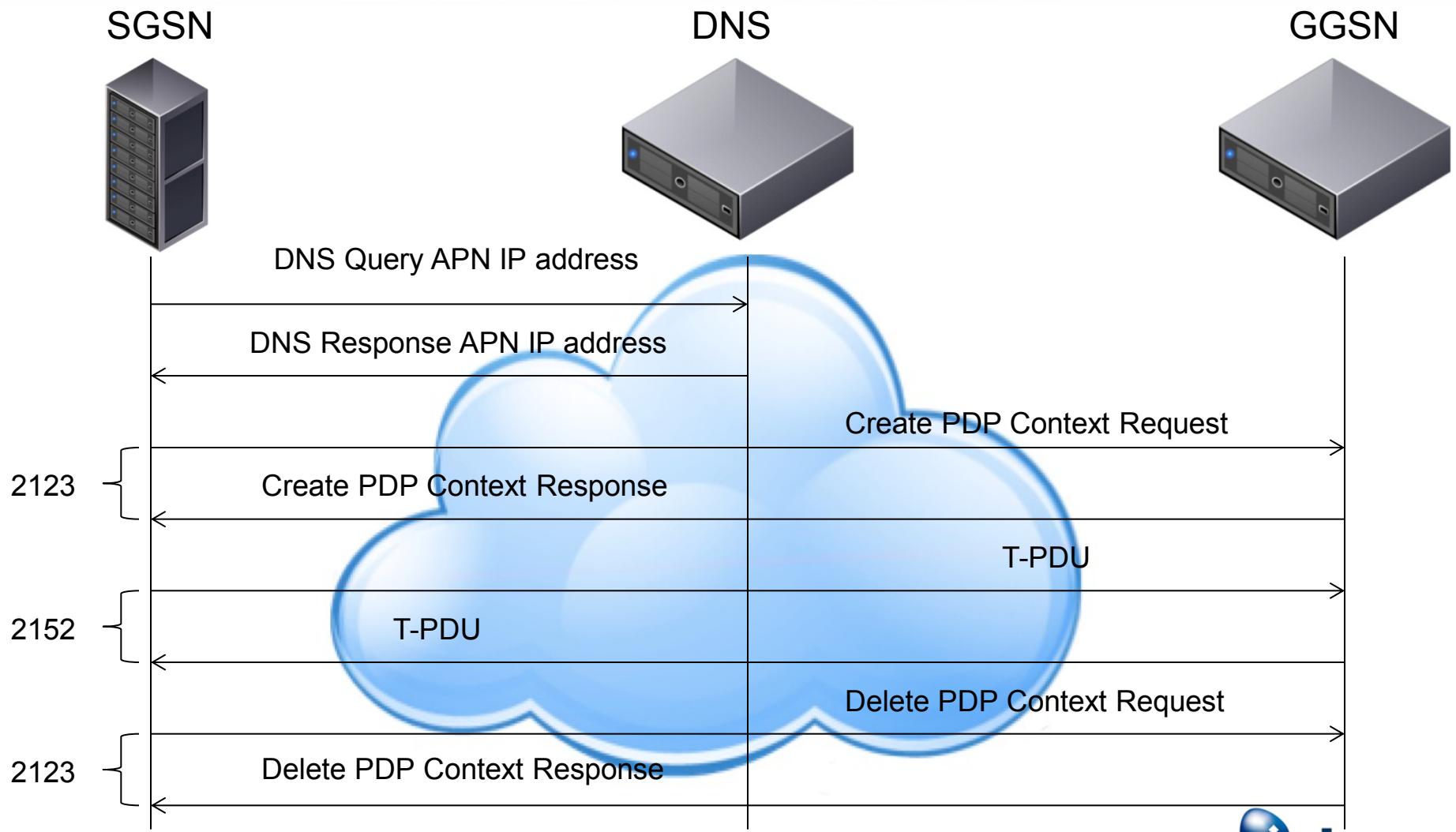
GPRS Tunneling protocol

Information Elements in a Create PDP Context

Information element	Presence requirement	Reference
IMSI	Conditional	7.7.2
Routeing Area Identity (RAI)	Optional	7.7.3
Recovery	Optional	7.7.11
Selection mode	Conditional	7.7.12
Tunnel Endpoint Identifier Data I	Mandatory	7.7.13
Tunnel Endpoint Identifier Control Plane	Conditional	7.7.14
NSAPI	Mandatory	7.7.17
Linked NSAPI	Conditional	7.7.17
Charging Characteristics	Conditional	7.7.23
Trace Reference	Optional	7.7.24
Trace Type	Optional	7.7.25
End User Address	Conditional	7.7.27
Access Point Name	Conditional	7.7.30
Protocol Configuration Options	Optional	7.7.31
SGSN Address for signalling	Mandatory	GSN Address 7.7.32
SGSN Address for user traffic	Mandatory	GSN Address 7.7.32
MSISDN	Conditional	7.7.33
Quality of Service Profile	Mandatory	7.7.34
TFT	Conditional	7.7.36
Trigger Id	Optional	7.7.41
OMC Identity	Optional	7.7.42
Common Flags	Optional	7.7.48
APN Restriction	Optional	7.7.49
RAT Type	Optional	7.7.50
User Location Information	Optional	7.7.51
MS Time Zone	Optional	7.7.52
IMEI(SV)	Conditional	7.7.53
CAMEL Charging Information Container	Optional	7.7.54
Additional Trace Info	Optional	7.7.62
Correlation-ID	Optional	7.7.82
Evolved Allocation/Retention Priority I	Optional	7.7.91
Extended Common Flags	Optional	7.7.93
User CSG Information	Optional	7.7.94
APN-AMBR	Optional	7.7.98
Signalling Priority Indication	Optional	7.7.103
Private Extension	Optional	7.7.46

- APN
- IMSI
- End User Address
- User Location Information
- IMEI

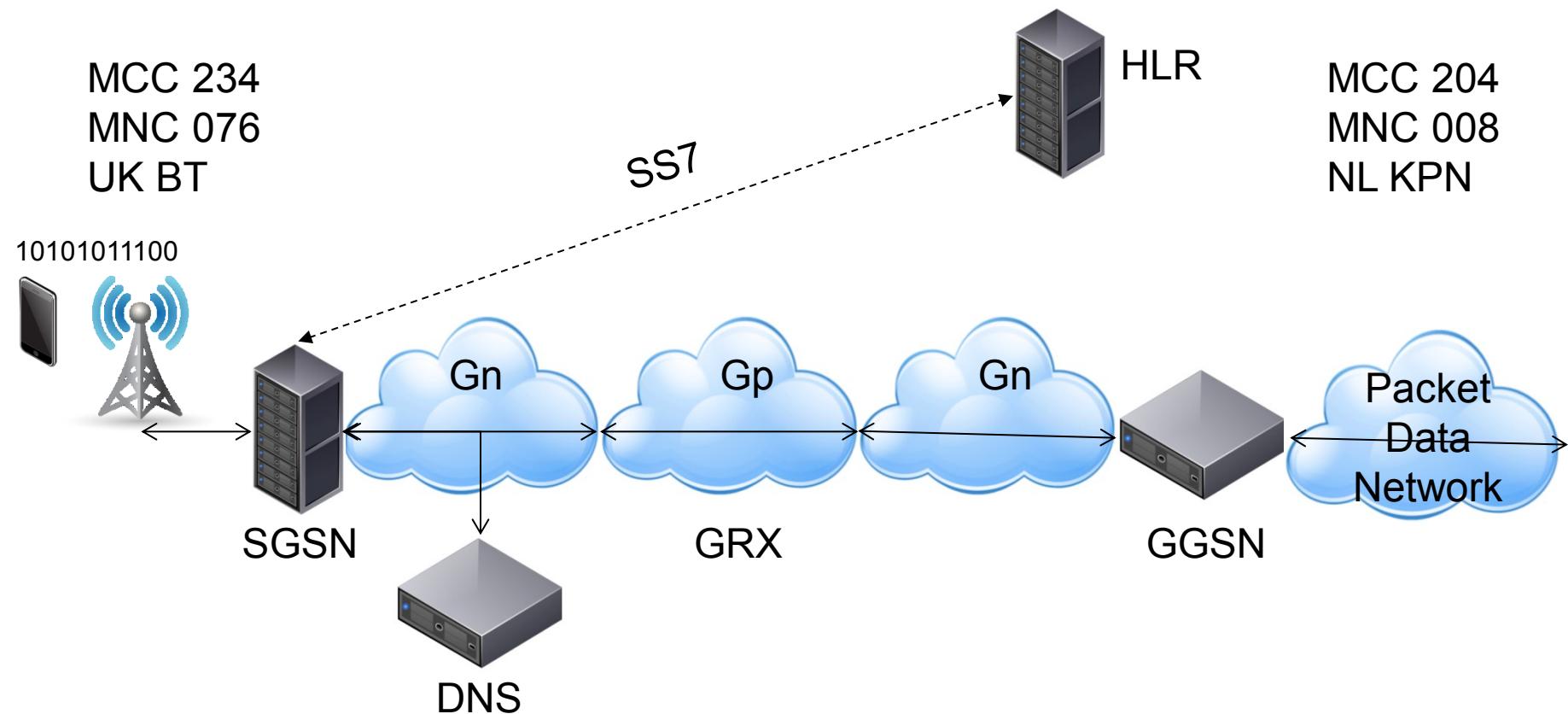
GPRS Tunneling protocol



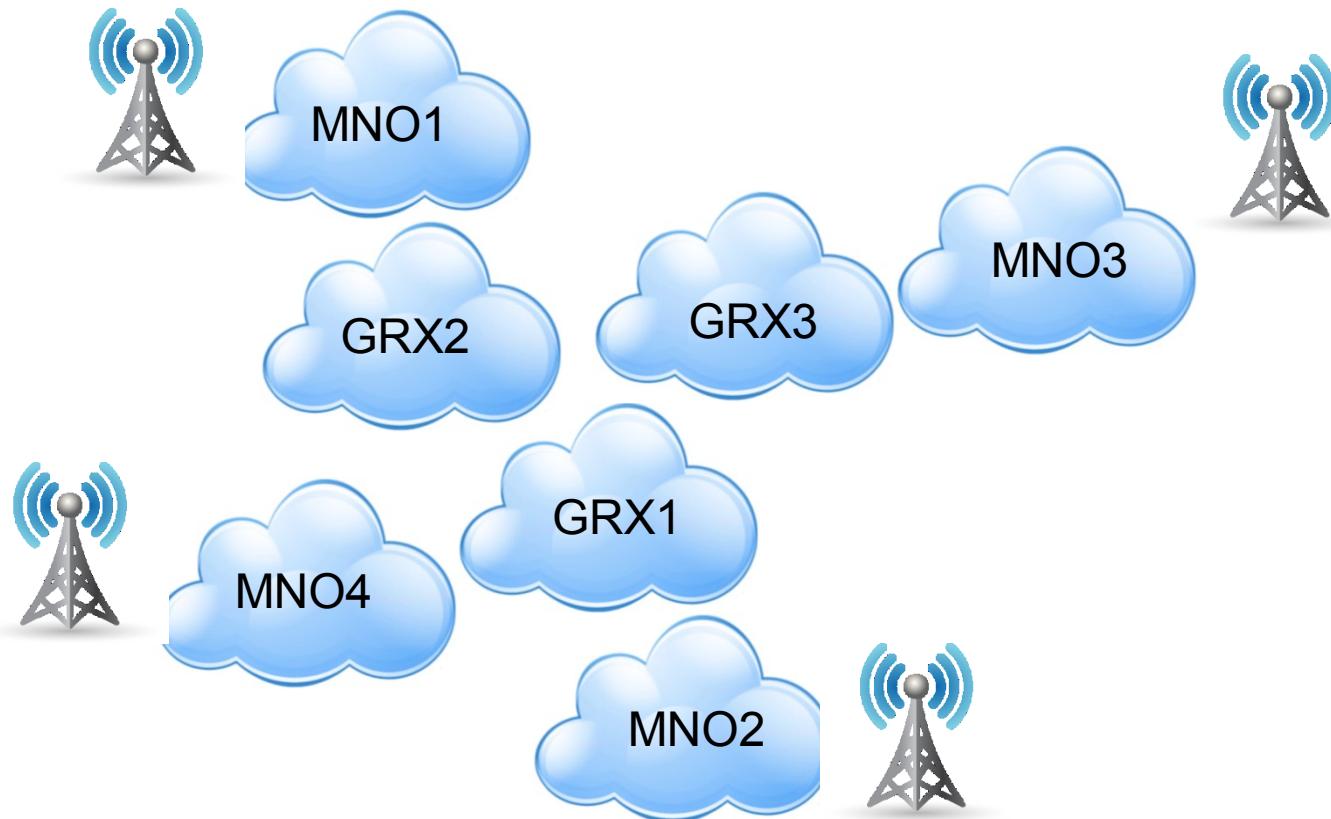
GPRS Roaming eXchange



GPRS Roaming eXchange

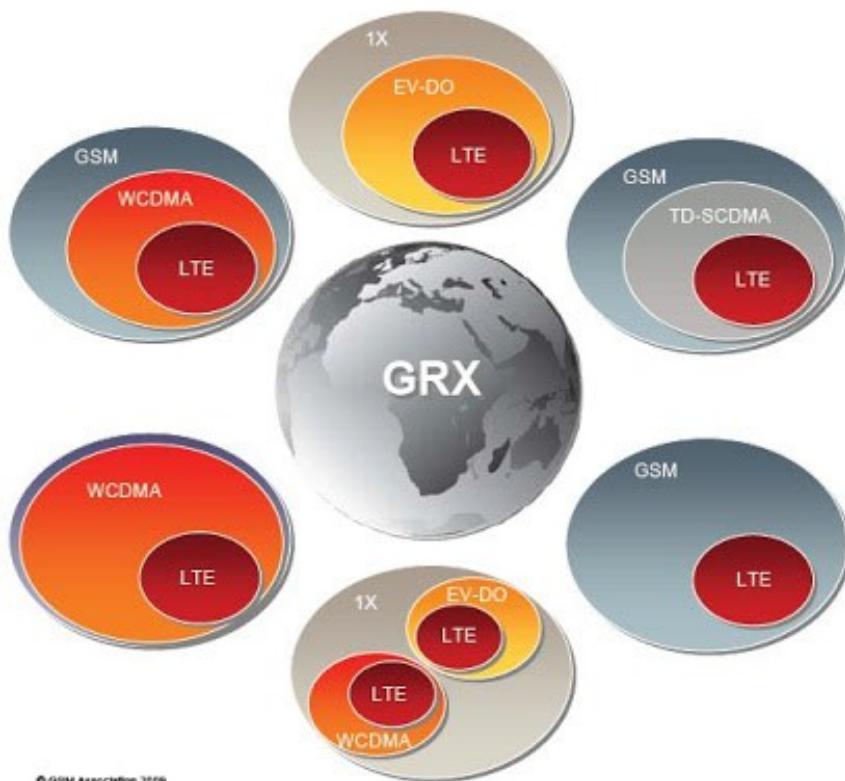


GRX architecture & protocols



GRX architecture & protocols

Linking the “islands” – backwards compatibility & roaming



- GRX will support LTE/EPC Roaming
- Including support for GTPv2, MIP, Diameter
- GSMA Project will deliver Next Gen. roaming capability on time for service launch
- Work carried out by existing GSMA expert working groups

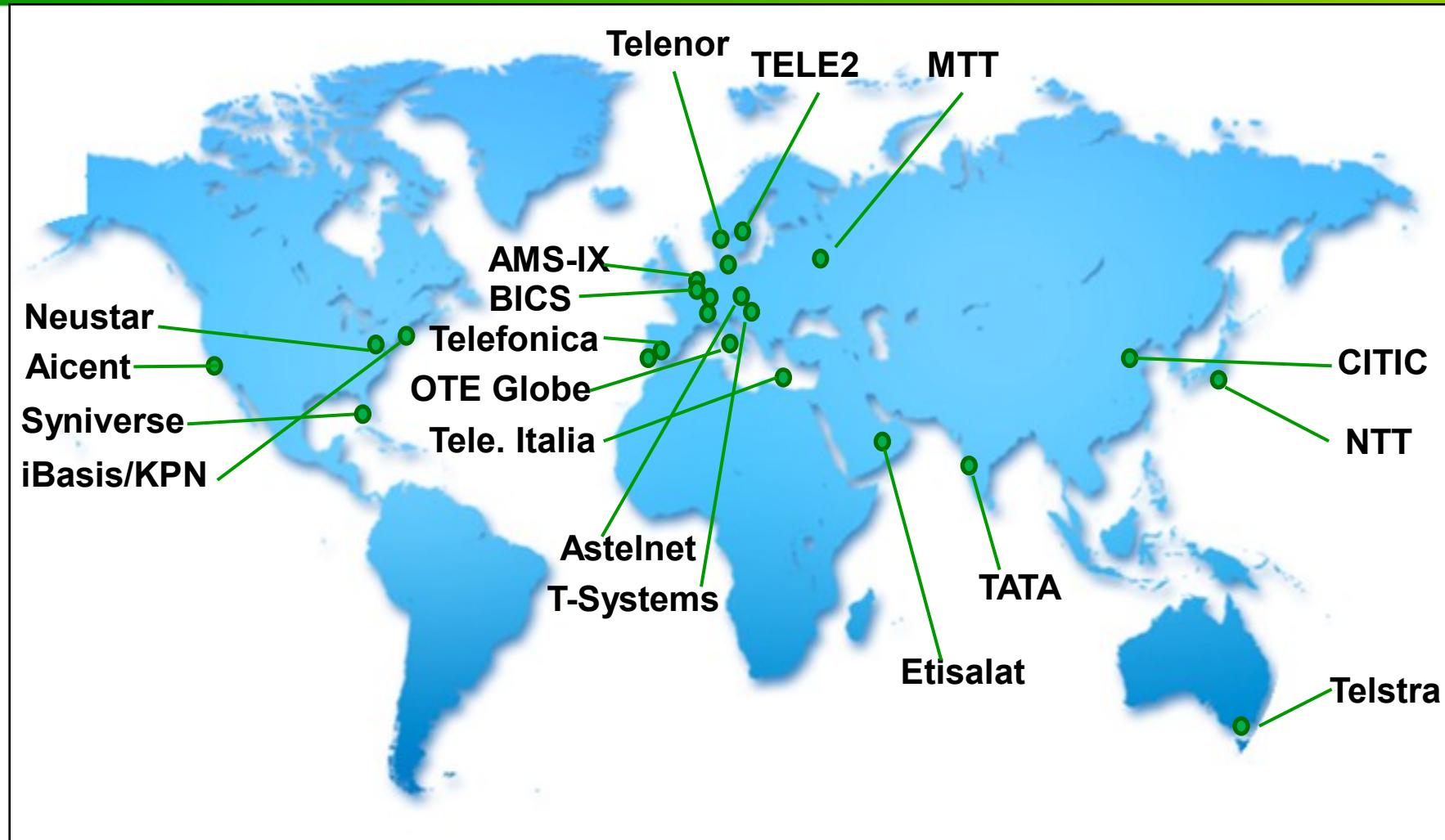


15

GRX providers

<u>Name</u>	<u>City/Country</u>
AMS-IX	Amsterdam/Netherlands
Astelnet	Prague, Czech Republic
Telefonica Spain	Madrid, Spain
NTT	Tokyo, Japan
Neustar	Sterling, VA, USA
TELE2	Stockholm, Sweden
Etisalat	Abu Dhabi, UAE
Telenor	Oslo, Norway
Telecom-Austria	Vienna, Austria
Comfone	Bern, Switzerland
Syniverse	Florida, USA
Citic	Beijing, China
Telecom Italia Sparkle	Rome, Italy
Aicent	California, USA
Portugal Telecom	Lisbon, Portugal
T-Systems	Frankfurt, Germany
TDC	Copenhagen, Denmark
Telstra/Reach	Melbourne, Australia
OTE Globe	Athens, Greece
TATA	Mumbai, India
MTT	Moscow, Russia
iBasis/KPN	Burlington, USA
BICS	Brussels, Belgium

GRX providers - HQ



GTP Traffic – why the interest?

- GTP traffic captured from GRX router: looks like this in Wireshark:

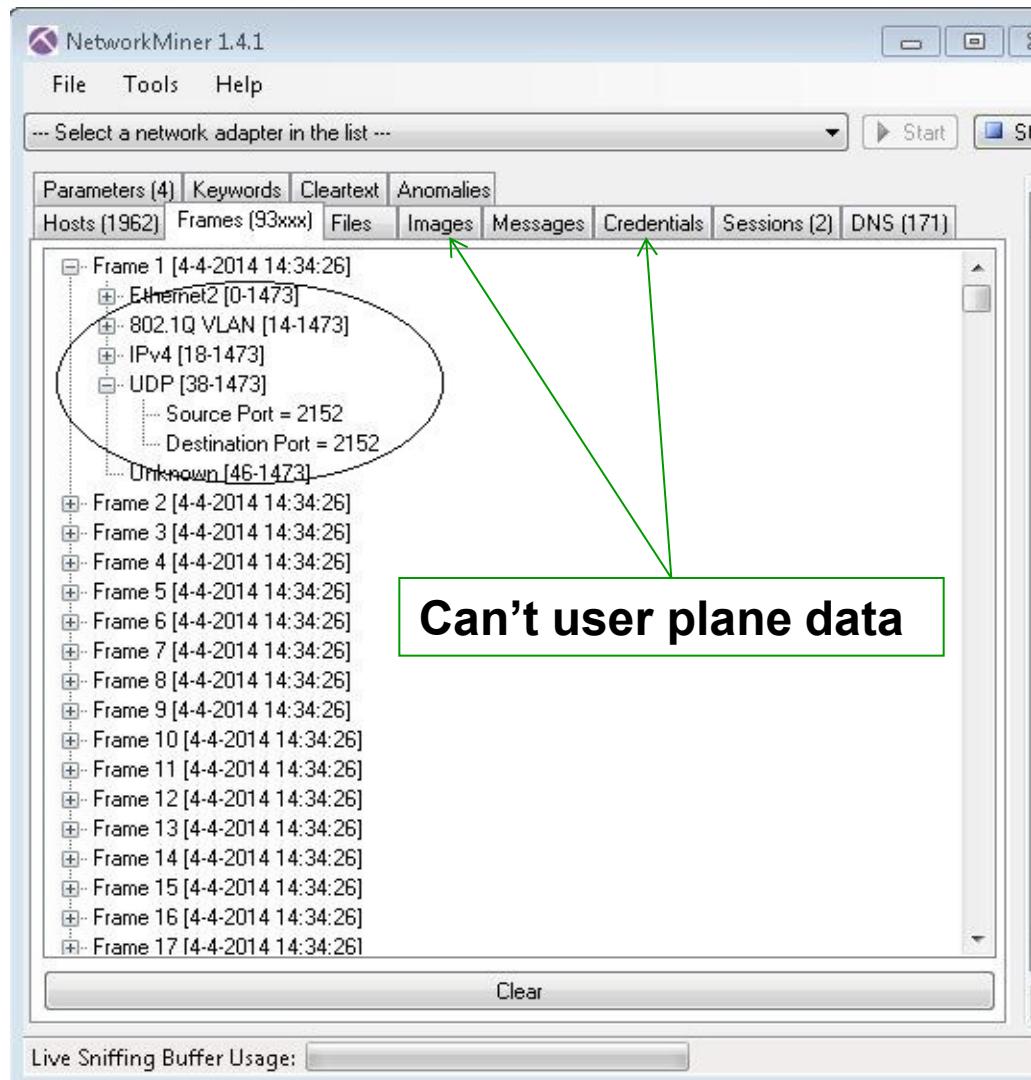
No.	Time	Source	Destination	Protocol	Info
146	2014-04-04 14:34:26.354	10.243.21.226	66.28.0.45	GTP <DNS>	Standard query
▶ Frame 146: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)					
▶ Ethernet II, Src: JuniperN_a3:18:5d (00:1f:12:a3:18:5d), Dst: Cisco_40:f2:40 (00:1e:f7:40:f2:40)					
▶ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 304					
▶ Internet Protocol Version 4, Src: 145.7.████ (145.7.████), Dst: 83.137.████ (83.137.████)					
▶ User Datagram Protocol, Src Port: gtp-user (2152), Dst Port: gtp-user (2152)					
▶ GPRS Tunneling Protocol					
T-PDU Data 64 bytes					
▶ Internet Protocol Version 4, Src: 10.243.21.226 (10.243.21.226), Dst: 66.28.0.45 (66.28.0.45)					
▶ User Datagram Protocol, Src Port: 58238 (58238), Dst Port: domain (53)					
▶ Domain Name System (query)					
[Response In: 2467]					
Transaction ID: 0xf402					
▶ Flags: 0x0100 Standard query					
Questions: 1					
Answer RRs: 0					
Authority RRs: 0					
Additional RRs: 0					
▶ Queries					
▶ www.sanomamedia.nl: type A, class IN					

UE End points

GTP tunnel end points

User plane traffic

GTP Traffic – why the interest?



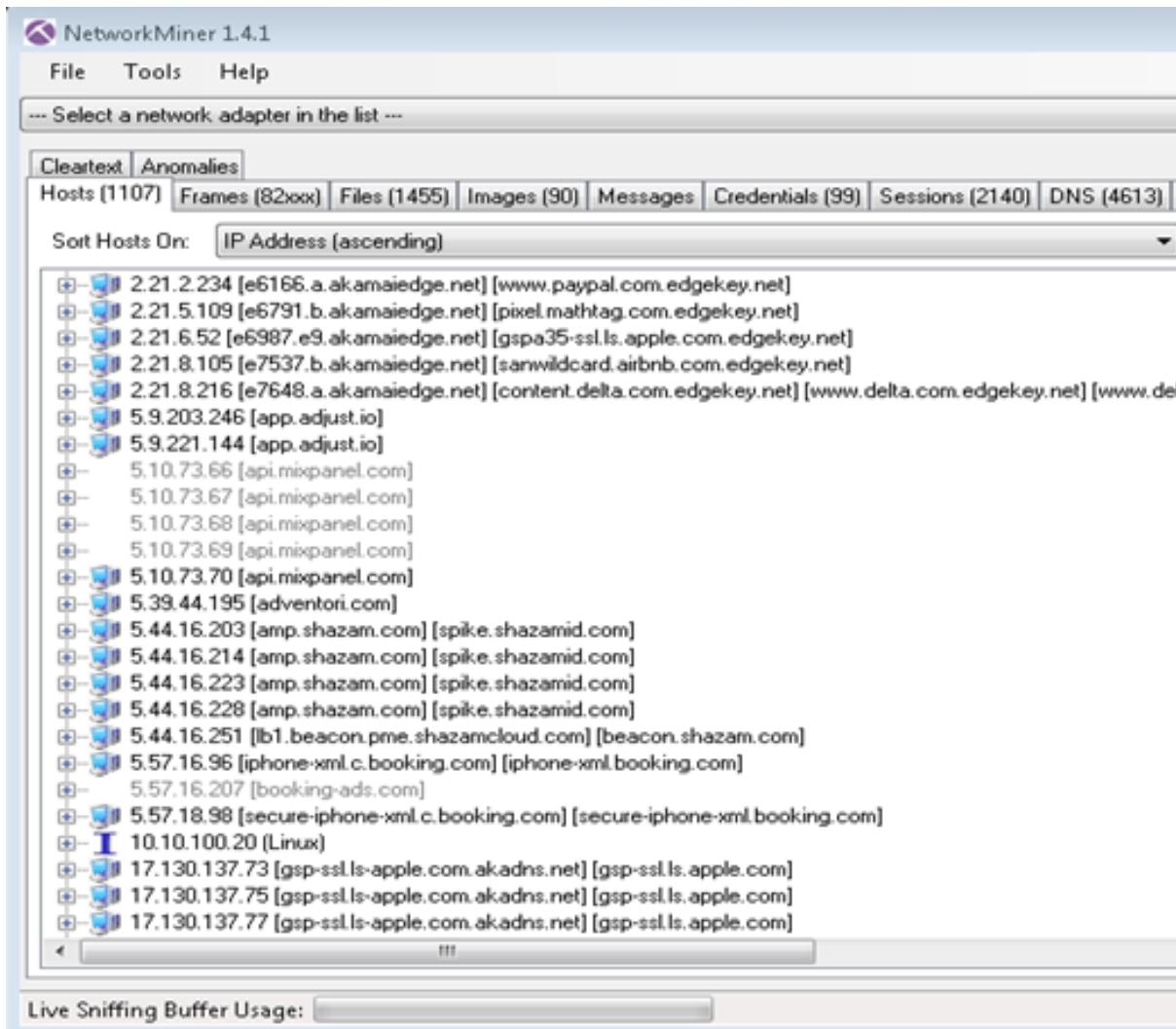
- Network forensics
- NetworkMiner, Explico
- Frames loaded but...

GTP Traffic – why the interest?

- Need to remove GTP headers
- Here's Wesley - CERT team
- Cool shirts
(<http://en.wikipedia.org/wiki/Brainfuck>)
- gtpstrip.c
 - identifies link layer header
 - detects VLAN tag
 - checks for IP header
 - checks for UDP header
 - confirms GTP user plane traffic
 - removes IP, UDP & GTP headers
 - re-write frame



GTP Traffic – why the interest?



- Re-load stripped PCAP file
- Now can see info:
- **Hosts details**

GTP Traffic – why the interest?

- Now can see info: **Sessions**

The screenshot shows the NetworkMiner 1.4.1 interface. The main window displays a table of network sessions. The columns include Frame nr., Client host, C. port, Server host, S. port, Protocol (application), and Start time. Most entries show HTTP traffic between various IP addresses and ports. A 'Case Panel' on the right lists a single file entry: KoenBos... with MD5 6a4d92... and a 'Reload Case Files' button at the bottom.

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application)	Start time
51	100.104.246.65	54465	194.221.65.73 [a1441.g4.akamai.net] [init-p...]	80	Http	20-5-2014 20:58:...
348	100.104.246.65	54472	162.217.102.127 [ads.mopub.com]	80	Http	20-5-2014 20:58:...
353	100.104.246.65	54473	216.52.203.13 [data.flurry.com]	80	Http	20-5-2014 20:58:...
421	100.104.246.65	54475	74.217.75.7 [data.flurry.com]	80	Http	20-5-2014 20:58:...
425	100.104.246.65	54476	162.217.102.228 [ads.mopub.com]	80	Http	20-5-2014 20:58:...
434	100.104.246.65	54477	216.52.203.13 [data.flurry.com]	80	Http	20-5-2014 20:58:...
502	100.104.246.65	54479	74.125.136.102 [www.google-analytics.l.go...]	80	Http	20-5-2014 20:58:...
501	100.104.246.65	54480	23.52.59.27 [e8218.ce.akamaiedge.net] [oc...]	80	Http	20-5-2014 20:58:...
804	100.104.246.65	54497	74.125.136.139 [www.google-analytics.l.go...]	80	Http	20-5-2014 20:59:...
992	100.104.246.65	54499	93.184.220.29 [cs9.wac.edgecastcdn.net] [...]	80	Http	20-5-2014 20:59:...
991	100.104.246.65	54498	93.184.220.29 [cs9.wac.edgecastcdn.net] [...]	80	Http	20-5-2014 20:59:...
1052	100.104.246.65	54501	216.52.203.13 [data.flurry.com]	80	Http	20-5-2014 20:59:...
1172	100.104.246.65	54503	23.52.59.27 [e8218.ce.akamaiedge.net] [oc...]	80	Http	20-5-2014 20:59:...
1707	100.104.246.65	54508	17.254.32.16 [wu.apple.com] [iphone-wu.ap...]	80	Http	20-5-2014 20:59:...
1708	100.104.246.65	54509	98.137.205.233 [any-appleweather-cache.i...]	80	Http	20-5-2014 20:59:...
3308	100.104.246.65	54529	95.101.0.83 [a675.da1.akamai.net] [a675.p...]	80	Http	20-5-2014 21:00:...
3310	100.104.246.65	54530	95.101.0.97 [a986.da1.akamai.net] [a986.p...]	80	Http	20-5-2014 21:00:...
3449	100.104.246.65	54533	95.101.1.208 [a442.w45.akamai.net] [gspa...]	80	Http	20-5-2014 21:00:...
3451	100.104.246.65	54534	95.101.1.208 [a442.w45.akamai.net] [gspa...]	80	Http	20-5-2014 21:00:...
3453	100.104.246.65	54535	95.101.1.208 [a442.w45.akamai.net] [gspa...]	80	Http	20-5-2014 21:00:...
3471	100.104.246.65	54538	95.101.1.208 [a442.w45.akamai.net] [gspa...]	80	Http	20-5-2014 21:00:...
3726	100.104.246.65	54545	74.125.136.100 [www.google-analytics.l.go...]	80	Http	20-5-2014 21:01:...
3769	100.104.246.65	54546	95.101.0.96 [a1412.gi3.akamai.net] [gspa2...]	80	Http	20-5-2014 21:01:...
3938	100.104.246.65	54553	162.217.102.42 [ads.mopub.com]	80	Http	20-5-2014 21:01:...
3939	100.104.246.65	54554	216.52.203.13 [data.flurry.com]	80	Http	20-5-2014 21:01:...

GTP Traffic – why the interest?

- Now can see info: **Images**

NetworkMiner 1.4.1

File Tools Help

... Select a network adapter in the list ...

Cleartext Anomalies

Hosts (1107) Frames (82xxx) Files (1455) Images (90) Messages Credentials (99) Sessions (2140) DNS (4613) Parameters (5561) Keywords

Case Panel

Filename	MD5
KoenBos...	6a4d92...

Live Sniffing Buffer Usage:

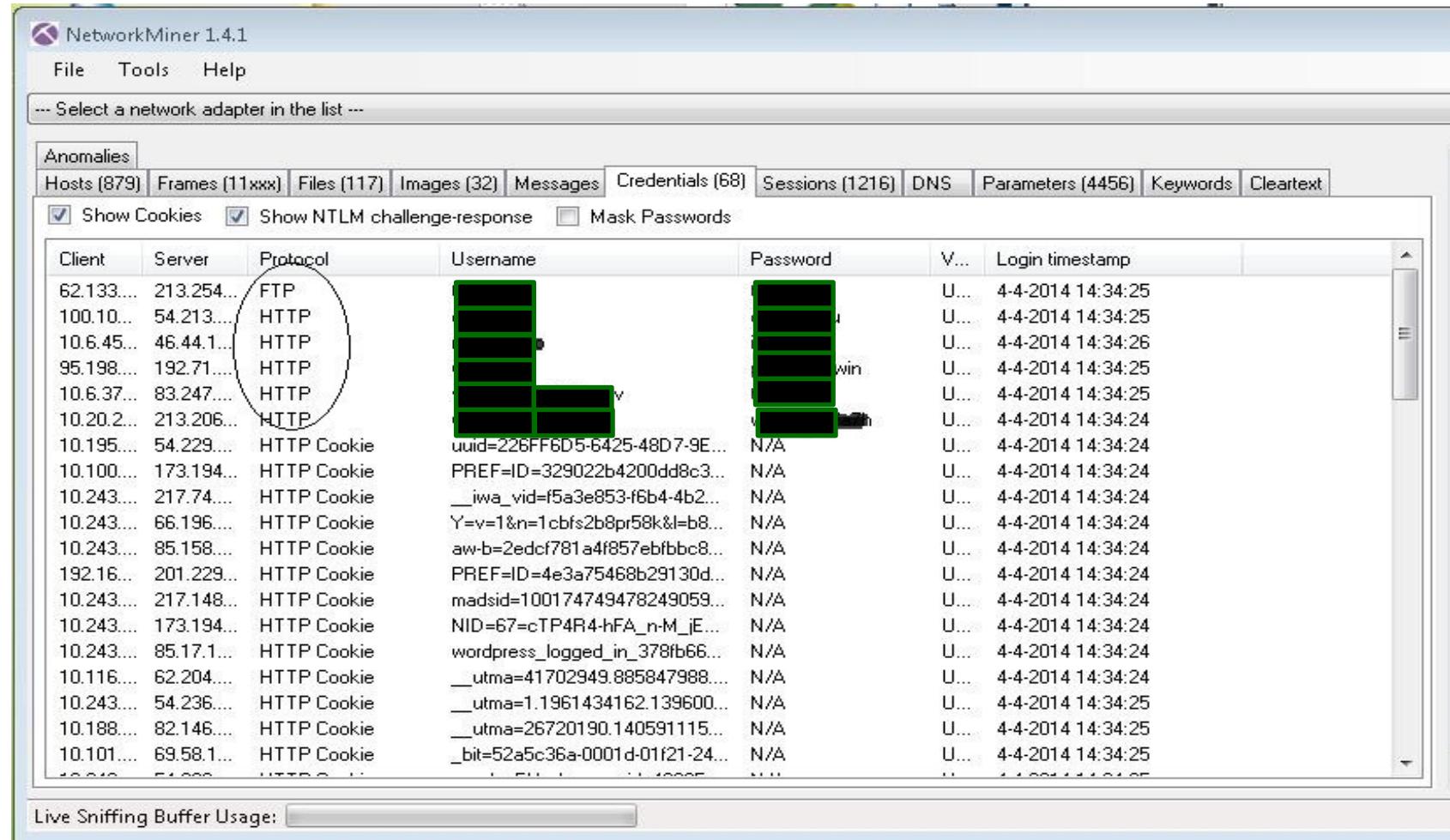
Images (90)

File Name	Size
s.169AB41C[3].gif	1x1, 43 B
s.5A420325[3].gif	1x1, 43 B
s.FD625210[3].gif	1x1, 43 B
__utm.gif.45733E7C[3].gif	1x1, 35 B
Default[3].jpg	480x270, 4 758 B
p2.BCDC5A9D[3].gif	1x1, 43 B
imp.FADDAD64[3].gif	1x1, 43 B
MV5BMTc2NjM1OTU2[3]...	176x262, 5 377 B
MV5BMTQzMzc5NDkx[3]...	144x144, 2 677 B
p2.CFE921DC[3].gif	1x1, 43 B
iui3.1625A77D[3].gif	1x1, 43 B
iui3.1FF26209[3].gif	1x1, 43 B
trackMyBags_thumb_2x[3]...	250x110, 2 130 B
__utm.gif.FF071A96[3].gif	1x1, 35 B
5679440[3].jpeg	88x88, 2 925 B
21915427[3].jpeg	88x88, 1 362 B
MSP6031ha19.7D0971B8[...]	351x34, 2 301 B
collect[21].gif	1x1, 35 B
collect[22].gif	1x1, 35 B
m1mxmtnacchf_wd320[3].jpg	320x180, 7 055 B

GTP Traffic – why the interest?

- Now can see info:

Credentials



The screenshot shows the NetworkMiner 1.4.1 interface with the 'Credentials' tab selected. A circular selection highlights a group of entries in the table, specifically focusing on the first six rows which show multiple instances of the same client-server pair (62.133.1.1 and 213.254.1.1) using the FTP protocol.

Client	Server	Protocol	Username	Password	V...	Login timestamp
62.133....	213.254....	FTP	[REDACTED]	[REDACTED]	U...	4-4-2014 14:34:25
100.10....	54.213....	HTTP	[REDACTED]	[REDACTED]	U...	4-4-2014 14:34:25
10.6.45....	46.44.1....	HTTP	[REDACTED]	[REDACTED]	U...	4-4-2014 14:34:26
95.198....	192.71....	HTTP	[REDACTED]	[REDACTED]	U...	4-4-2014 14:34:25
10.6.37....	83.247....	HTTP	[REDACTED]	[REDACTED]	U...	4-4-2014 14:34:25
10.20.2....	213.206....	HTTP	[REDACTED]	[REDACTED]	U...	4-4-2014 14:34:24
10.195....	54.229....	HTTP Cookie	uuid=226FF6D5-6425-48D7-9E...	N/A	U...	4-4-2014 14:34:24
10.100....	173.194....	HTTP Cookie	PREF=ID=329022b42000dd8c3...	N/A	U...	4-4-2014 14:34:24
10.243....	217.74....	HTTP Cookie	_iwa_vid=f5a3e853-f6b4-4b2...	N/A	U...	4-4-2014 14:34:24
10.243....	66.196....	HTTP Cookie	Y=v=1&n=1cbfs2b8pr58k&l=b...	N/A	U...	4-4-2014 14:34:24
10.243....	85.158....	HTTP Cookie	aw-b=2edcf781a4f857ebfbcc8...	N/A	U...	4-4-2014 14:34:24
192.16....	201.229....	HTTP Cookie	PREF=ID=4e3a75468b29130d...	N/A	U...	4-4-2014 14:34:24
10.243....	217.148....	HTTP Cookie	madsid=100174749478249059...	N/A	U...	4-4-2014 14:34:24
10.243....	173.194....	HTTP Cookie	NID=67=cTP4R4-hFA_n-M_jE...	N/A	U...	4-4-2014 14:34:24
10.243....	85.17.1....	HTTP Cookie	wordpress_logged_in_378fb66...	N/A	U...	4-4-2014 14:34:24
10.116....	62.204....	HTTP Cookie	_utma=41702949.885847988...	N/A	U...	4-4-2014 14:34:24
10.243....	54.236....	HTTP Cookie	_utma=1.1961434162.139600...	N/A	U...	4-4-2014 14:34:25
10.188....	82.146....	HTTP Cookie	_utma=26720190.140591115...	N/A	U...	4-4-2014 14:34:25
10.101....	69.58.1....	HTTP Cookie	_bit=52a5c36a-0001d-01f21-24...	N/A	U...	4-4-2014 14:34:25
10.243....	51.222....	HTTP Cookie	..._F..._L..._I..._H..._O..._N...	N/A	U...	4-4-2014 14:34:25

GTP Traffic – why the interest?

▽ GPRS Tunneling Protocol

- ▷ Flags: 0x32
- Message Type: Create PDP context request (0x10)
- Length: 160
- TEID: 0x00000000
- Sequence number: 0x2519
- N-PDU Number: 0x00
- IMSI: 204091004 [REDACTED]
-00 = Selection mode: MS or network provided APN, subscribed verified (0)
- TEID Data I: 0x384d6bfe
- TEID Control Plane: 0x9cf72016
- ▷ NSAPI: 5
- ▷ End user address (IETF/IPv4)
- ▷ Access Point Name: data.lycamobile.nl
- ▷ Protocol configuration options
- ▷ GSN address : 145.7.1 [REDACTED]
- ▷ GSN address : 145.7.1 [REDACTED]
- ▷ MS international PSTN/ISDN number
- ▷ Quality of Service
- ▷ Common Flags :
- ▷ RAT Type: GERAN
- ▽ User Location Information
 - Length: 8
 - Geographic Location Type: 0
 - Mobile Country Code (MCC): Netherlands (Kingdom of the) (204)
 - Mobile Network Code (MNC): KPN Mobile The Netherlands B.V. (08)
 - Cell LAC: 0xc62 (3170)
 - Cell CI: 0xc09c (49308)
- ▷ MS Time Zone: GMT + 1 hours 0 minutes
- ▷ IMEI(SV): 0114720062758705

[\[Response In: 41370\]](#)

IMSI

MCC
MNC
LAC
CI

IMEI

- What else?
- Location details
- Device detail

GTP Traffic – why the interest? MCC, MNC, LAC, CI = your location

- <http://unwiredlabs.com/api>

The screenshot shows the unwiredlabs Location API interface. On the left, a code editor displays a JSON request:

```
1 {  
2     "token": "216071648",  
3     "radio": "gsm",  
4     "mcc": 204,  
5     "mnc": 08,  
6     "cells": [  
7         {"lac": 3170,  
8          "cid": 49308  
9     }],  
10    "address": 1  
11 }
```

In the center, a code editor displays the JSON response:

```
1 {  
2     "status": "ok",  
3     "balance": 49,  
4     "lat": 51.92552,  
5     "lon": 4.49542,  
6     "accuracy": 1379,  
7     "address": "Willem Sch\u00fclinkstraat 1, 3170 VZ Rotterdam, Noord-Holland, Nederland"  
8 }
```

On the right, a map of Rotterdam shows a red dot indicating the location, with a blue circle representing the accuracy radius.

GTP Traffic – why the interest? MCC, MNC, LAC, CI = your location

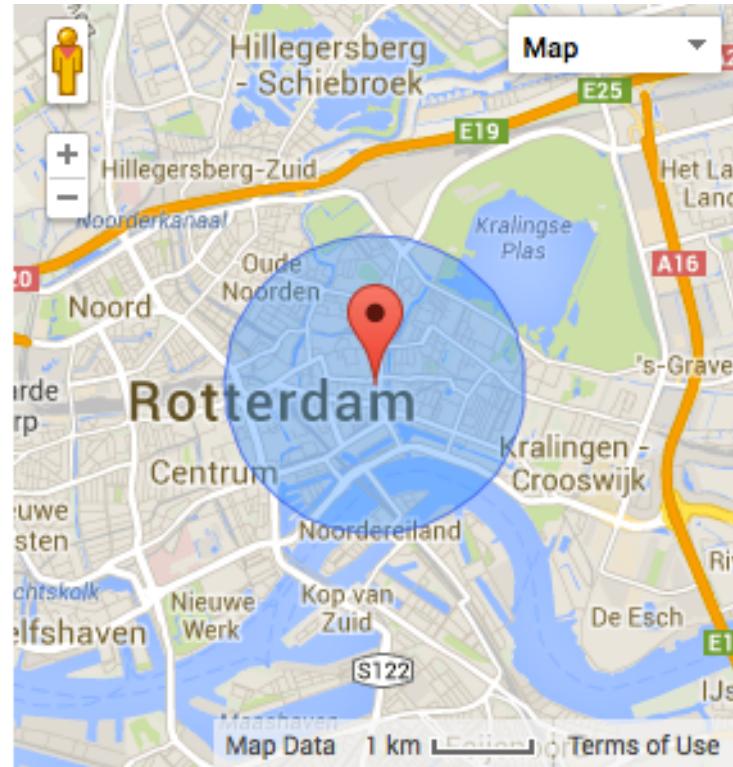
Request

```
{  
  "token": "216071648",  
  "radio": "gsm",  
  "mcc": 204,  
  "mnc": 08,  
  "cells": [  
    {"lac": 3170,  
     "cid": 49308  
    }],  
  "address": 1  
}
```

GPS coordinates

Response

```
{  
  "status": "ok",  
  "balance": 49,  
  "lat": 51.92552,  
  "lon": 4.49542,  
  "accuracy": 1379,  
  "address": "Willem  
Schurmannstraat, Rotterdam,  
Stadsregio Rotterdam, South  
Holland, Kingdom of the  
Netherlands, 3061CT, The  
Netherlands, European Union"
```



GTP Traffic – why the interest? IMEI – International Mobile Equipment Identity

The screenshot shows a web browser window with the URL www.numberingplans.com/?page=analysis&sub=imeinr. The page title is "INTERNATIONAL NUMBERING PLANS". On the left, a sidebar lists services like "Services", "Subscriptions", "Numbering plans", etc. A "Grammarly Checker" sidebar is also present. The main content area is titled "Analysis of IMEI numbers". It includes a tip about displaying IMEI on handsets, an input field for "Enter IMEI number below" containing "357634-05-291395-6", and an "analyse" button. To the right, there's a section titled "It's gone. Undo" with a question "What was wrong with this ad?" and three radio buttons for "Inappropriate", "Repetitive", or "Irrelevant". Below this is a "Google" logo. The main analysis results for IMEI 357634052913956 are listed under "Information on IMEI 357634052913956", including the Type Allocation Holder (Samsung), Mobile Equipment Type (Samsung I9505 Galaxy S4), GSM Implementation Phase (2/2+), and IMEI Validity Assessment (Very likely). Further down are sections for "Information on range assignment" and "Information on number format", both listing "Full IMEI Presentation" as 357634-05-291395-6.

- <http://www.numberingplans.com/>

IMEI

Samsung I9505
Galaxy S4

Handset
specific
payload?

GRX landscape – overview

- Now we know the **what, who, why**
- Now need to find and work out **How** to get unauthorised access?
- Kill Chain (Reconnaissance → Weaponization)
 - Identify hosts, enumerate service ONLY
- GRX BGP routing table (MNOs)
 - Total number of subnets: 4.8K
 - Total IP address space: 320K
- Host discovery - limited port scan & GTP ping

```
./masscan <target> p21,22,23,25,80,139,443,445,3868,1433 -oB out-$b.bin --ping
```
- Approximate live hosts: 42K



GRX landscape – Looking for GGSNs

- Search for GTP ports: UDP 2152 & UDP 2123
- GTP echo request looks like this:

No.	Time	Source	Destination	Protocol	Info
13352	2014-04-04 14:34:26.570	212.23.██████	145.7.██████	GTP	Echo request
.....					
▷ Frame 13352: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)					
▷ Ethernet II, Src: Cisco_40:f2:40 (00:1e:f7:40:f2:40), Dst: JuniperN_a3:18:5d (00:1f:12:a3:18:5d)					
▷ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 304					
▷ Internet Protocol Version 4, Src: 212.23.██████ (212.23.██████), Dst: 145.7.██████ [145.7.██████]					
▷ User Datagram Protocol, Src Port: gtp-control (2123), Dst Port: gtp-control (2123)					
▽ GPRS Tunneling Protocol					
▽ Flags: 0x32					
001. = Version: GTP release 99 version (1)					
...1 = Protocol type: GTP (1)					
.... 0... = Reserved: 0					
.... .0.. = Is Next Extension Header present?: No					
.... ..1. = Is Sequence Number present?: Yes					
.... ...0 = Is N-PDU number present?: No					
Message Type: Echo request (0x01)					
Length: 4					
TEID: 0x00000000					
Sequence number: 0x05ad					
N-PDU Number: 0x00					
[Response In: 13708]					
.....					

GRX landscape – Looking for GGSNs

- GTP echo response looks like this:

No.	Time	Source	Destination	Protocol	Info
13357	2014-04-04 14:34:26.570	145.7 [REDACTED]	193.254. [REDACTED]	GTP	Echo response
Frame 13357: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)					
Ethernet II, Src: JuniperN_a3:18:5d (00:1f:12:a3:18:5d), Dst: Cisco_40:f2:40 (00:1e:f7:40:f2:40)					
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 304					
Internet Protocol Version 4, Src: 145.7.4 [REDACTED] (145.7.4 [REDACTED]), Dst: 193.254. [REDACTED] (193.254. [REDACTED])					
User Datagram Protocol, Src Port: gtp-control (2123), Dst Port: gtp-control (2123)					
GPRS Tunneling Protocol					
Flags: 0x32					
001. = Version: GTP release 99 version (1)					
...1 = Protocol type: GTP (1)					
.... 0... = Reserved: 0					
.... .0.. = Is Next Extension Header present?: No					
.... ..1. = Is Sequence Number present?: Yes					
.... ...0 = Is N-PDU number present?: No					
Message Type: Echo response (0x02)					
Length: 6					
TEID: 0x000000000					
Sequence number: 0x5623					
N-PDU Number: 0x00					
Recovery: 12					

GRX landscape – Looking for GGSNs

- Scan for GTP ports
 - zmap (<https://zmap.io/>)
 - Async & fast – ICMP, TCP, UDP
 - Can scale up to 1.4 million packets/sec, good idea to rate limit
- zmap -M udp -p 2123 <IP> --probe-args=file:GTP-2123-echo.pkt -o GTP-2123-<IP>.csv -B 1G
- Now you've found a GTP port, then what?
 - Send PDP context request to confirm active GGSN
 - OpenGGSN project (<http://sourceforge.net/projects/ggsn/>)

GRX landscape – Talking to GGSNs

- SGSNEMU (part of OpenGGSN)
 - connections to the GGSN
 - ping request, create PDP context
 - forward packets to connections on Gn/Gp interface.

```
# sgsnemu --listen 192.168.253.249 --remote xx.xx.xx.xx --timelimit 10 --contexts 1 1 --apn internet --imsi 240011234567890 --msisdn 46702123456 --create
```

<snip>

Initialising GTP library

```
openggsn[21672]: GTP: gtp_newgsm() started
```

Setting up interface

```
Done initialising GTP library
```

Sending off echo request

Setting up PDP context #0

```
Waiting for response from ggsn.....
```

Received echo response

```
Received create PDP context response.
```

GTP daemon ready to talk!



GRX landscape threat profile – DNS servers

- DNS on GRX used for resolving APNs to set up GTP tunnel
- Typical query for KPN looks like this:
 - dig **internet.mnc008.mcc204.gprs** @ <DNS IP>

DNS response:

```
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26251  
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 8  
  
;; QUESTION SECTION:  
;internet.mnc008.mcc204.gprs. IN A  
  
;; ANSWER SECTION:  
internet.mnc008.mcc204.gprs. 300 IN A 145.7.xx.xx  
internet.mnc008.mcc204.gprs. 300 IN A 145.7.xx.xx  
internet.mnc008.mcc204.gprs. 300 IN A 145.7.xx.xx  
internet.mnc008.mcc204.gprs. 300 IN A 145.7.xx.xx
```

globally agreed APN

GRX landscape threat profile— DNS servers

- Enumerate versions of DNS
- Command to get Bind version:
 - *dig chaos txt version.bind @<DNS IP>*
 - BIND versions 9.2.3 to 9.8.1-P1
 - Microsoft DNS 6.0.6002
 - Outdated versions with publicly known vulnerabilities

- Bind version 9.2.3
- Bind 9.8.1-P1

- Aside from GTP & DNS – what else?

DoS
CVE-2012-516
CVE-2012-4244

DoS & Buffer Overflow
CVE-2013-4854
CVE-2013-3919
CVE-2013-2266

GRX landscape threat profile – SMTP

- Cisco PIX sanitized smtpd
 - Exim smtpd 4.63
 - Microsoft ESMTP 5.0.2195.6713
 - Postfix smtpd
 - Sendmail 1.0, 2.5.3
 - Sendmail 8.11.1, 8.11.6+Sun, 8.11.7p1+Sun/8.11.7
 - Sendmail 8.12.9+Sun/8.12.9, 8.13.3 rev 1.001
 - Sendmail 8.13.7+Sun, 8.13.8+Sun/8.13.8, 8.14.1/8.14.1, 8.14.5+Sun/8.13.4
 - Sendmail 8.9.3
 - netqmail smtpd 1.04
 - qmail smtpd
-
- The diagram illustrates the relationship between various SMTP implementations and known vulnerabilities. Green arrows point from specific implementation names to their corresponding exploit boxes. For example, 'Exim smtpd 4.63' points to 'Remote Root Exploit CVE-2010-4344'. 'Sendmail 8.11.1, 8.11.6+Sun, 8.11.7p1+Sun/8.11.7' points to both 'Remote Code Execution CVE-2006-0058' and 'Remote Code Exec CVE-2003-0694'. 'Sendmail 8.9.3' points to 'Remote Code Exec CVE-2003-0694'. 'netqmail smtpd 1.04' and 'qmail smtpd' point to 'Buffer Overflow CVE-2002-1337'.

GRX landscape threat profile – FTP servers

- BSD ftpd 6.00
- Cisco ftpd 5.3.1
- HP-UX ftpd 1.1.214.8
- Microsoft ftpd 5.0
- OpenBSD ftpd 6.4 (Linux port 6.4)
- Sun Solaris 8 ftpd
- TopLayer/Alcatel ftpd
- VxWorks ftpd 5.4
- WU-FTPD 2.6.1 (revision 4.0), wu-2.6.1-16
- vsftpd 2.0.4, 2.0.5, 2.0.7, 2.2.2

Buffer Overflow
CVE 2001-0053

Buffer Overflow
CVE-2003-0466

BoF/DoS
CVE-2002-2300

DoS
CVE-2011-0762

- 3Com 3CDaemon ftpd
- Axis 211M Network
- BulletProof FTPd
- FileZilla ftpd 0.9.33, 0.9.40
- ProFTPD 1.3.0, 1.3.1
- Pure-FTPd
- Serv-U ftpd 6.0

Remote Code Exec
CVE-2006-5815

Banner based only!

GRX landscape threat profile – Web servers

- Apache Tomcat/Coyote JSP engine 1.0, 1.1
- Apache httpd 2.0.59, 2.2.14 (Ubuntu)
- Apache httpd 2.2.14 (Win32)
- Apache httpd 2.2.15 (Red Hat)
- Apache httpd 2.2.21 (Unix)
- Apache httpd 2.2.22 (FreeBSD)
- Apache httpd 2.2.26 (Unix)
- Apache httpd 2.2.3 (CentOS)
- Apache httpd 2.2.9 (Debian)
- Cisco ASA firewall http,Cisco IOS administrative httpd
- Microsoft IIS webserver 5.0, 6.0, 7.5
- MiniServ (Webmin httpd)
- Netscreen administrative web server (Virata-EmWeb/R6_0_1)
- Oracle HTTP Server Powered by Apache 1.3.22
- lighttpd 1.4.13

Remote Code Exec
CVE-2010-0425

Remote Code Exec
CVE-2013-1862

Remote Code Exec
CVE-2008-1446

DoS/Code Exec
CVE-2002-0392

Why are these servers even here??

GRX landscape threat profile – Telnet daemons

- Alcatel 7750 SR router telnetd
- BSD-derived telnetd
- Cisco IOS telnetd
- Cisco PIX 500 series telnetd
- Cisco or Edge-core switch telnetd
- Cisco router
- HP-UX telnetd
- Huawei Quidway Eudemon firewall telnetd
- Linux telnetd
- Microsoft Windows 2000 telnetd
- Microsoft Windows XP telnetd
- Netscreen ScreenOS telnetd
- Nortel Extranet Contivity Secure IP Services telnetd
- Openwall GNU/*/Linux telnetd
- Sun Solaris telnetd

DoS
CVE-2001-0348

Remote Code Exec
MS01-031

Login Bypass
CVE-2007-0882

Seriously?!

GRX landscape threat profile – SMB (Server Message Block)

- Mainly used for providing shared access to files
 - directly over TCP/445
 - via the NetBIOS API (TCP/139)
- SMB null sessions = blank username & password
 - ./smbclient -N -L //<IP>

**Remote Code Exec
CVE-2012-1182**

Some OS seen:

- Domain=[WORKGROUP] OS=[Unix] Server=[**Samba 3.6.3**]
- Domain=[XX] OS=[Windows 5.0] Server=[**Windows 2000 LAN Manager**]
- Domain=[WORKGROUP] OS=[**Windows Server 2008 R2 Standard 7601 Service Pack 1**] Server=[Windows Server 2008 R2 Standard 6.1]
- Domain=[WORKGROUP] OS=[**Windows Server 2003 3790 Service Pack 2**] Server=[Windows Server 2003 5.2]

**Remote Code Exec
CVE-2008-4835
CVE-2012-1182**

Looks like people are mixing GRX and office network!

GRX landscape threat profile – SMB

- Information disclosure via null session

```
#winfo XX.XX.XX.XX -n  
winfo 1.6 - copyright (c) 1999-2002, Arne Vidstrom  
- http://www.ntsecurity.nu/toolbox/winfo/
```

Trying to establish null session...
Null session established.

USER ACCOUNTS:

- * *udadmin*
(This account is the built-in guest account)
- * *udadmin*
- * *root*
- * *ftpuser1*

PASSWORD POLICY:

min pw length: 5
min pw age: 0 (in days)
max pw age: forever.
pw hist len: 0

No account lockout.

SHARES:

- * *IPC\$*
- * *DataDisk2*
- * *DataDisk1*

GRX landscape – SNMP (UDP/161)

- Default community strings: PUBLIC & PRIVATE
 - Possibly execute arbitrary commands
 - Shutdown machines
 - Stop & start tasks, change settings
 - Gain valuable information

sysDescr.0 = STRING: AGENT++v3.5.27 ATM Simulation Agent

- sysDes **Cisco IOS C2600** are, 1841 Software (C1841-IPBASE-M), Vers
- sysDes **Cisco IOS C2900** are, 2800 Software (C2800NM-ADVIPSERVI
- sysDes **Cisco IOS C3560** are, 3800 Software (C3825-IPBASE-M), Vers
- sysDes **Cisco IOS C3900** are, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 12.4(4)T1
- sysDes **Cisco IOS C1900** are, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4
- sysDes **Cisco IOS C2600** are, C2600 Software (C2600-IPVOICE_IVS-M), Version 12.4(9)T
- sysDes **Cisco IOS C2900** are, C2900 Software (C2900-UNIVERSALK9_NPE-M), Version 15.1(4)M3
- sysDescr.0 = STRING: Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M) Version 12.2(50)SF2
- sysDescr.0 = STRING: Cisco IOS Software, C3900e Software (C3900e-UNIV
- sysDescr.0 = STRING: Cisco IOS Software, c7600rsp72043_rp Software (c7
15.1(3)S5
- sysDescr.0 = STRING: Cisco IOS Software, C880 Software (C880DATA-UNI
- sysDescr.0 = STRING: Cisco IOS Software, IOS-XE Software (PPC_LINUX_
- sysDescr.0 = STRING: Cisco IOS Software, MWAM Software (MWAM-G8IS-
- sysDescr.0 = STRING: CSP CSP VPN Gate 3.1.10330
- sysDescr.0 = STRING: DrayTek Corporation
- sysDescr.0 = STRING: DT 815
- sysDescr.0 = STRING: Ericsson IPOS-12.1.109.8p1-Release

Cisco IOS 1841
Cisco IOS 2800
Cisco IOS 3800
Cisco IOS 7200

Cisco IOS C7600
Cisco IOS-XE
Cisco CSP VPN Gate 3.1
DrayTek Corp
Ericsson IPOS-12.1

GRX landscape – SNMP

- **SNMP UDP/161**
- **Default community strings: PUBLIC & PRIVATE**

Windows 2000

Windows 2003

Hexabyte ADSL

Huawei VRP router

Linux ADSL2PlusRouter

6 Family 15 Model 4 Stepping 8 AT/AT COMPATIBLE - Software: Windows Version

6 Family 6 Model 11 S

or Free)

SL

atile Routing Platform S

PlusRouter 2.6.19 #2 V

• sysDescr.0 = STRING: Linux ADSL2PlusRouter 2.6.19 #2 V

• sysDescr.0 = STRING: Linux iTOP-01 2.6.32.59-0.7-default

• sysDescr.0 = STRING: Product: MG 2K;SW Version: 5.60.0

• sysDescr.0 = STRING: Quidway E300 Firewall, Huawei Ve

• sysDescr.0 = STRING: Redback Networks SmartEdge OS ver

• sysDescr.0 = STRING: RouterOS CCR1036-12G-4S

• sysDescr.0 = STRING: SUN NETRA X4250, ILOM v3.0.3.30, r47608

• sysDescr.0 = STRING: SunOS dpireport 5.10 Generic_127128-11 i86pc

• sysDescr.0 = STRING: Sun SNMP Agent

• sysDescr.0 = STRING: TANDBERG C

• sysDescr.0 = STRING: ucd-snmp-4.1.2

• sysDescr.0 = STRING: ZXR10 ROS Ver

V2.8.01.C.27.P06 Copyright (c) 2001-2

• sysDescr.0 = STRING: ZXR10 xGW-16

• sysDescr.0 = STRING: ZyXEL MAX-20

Huawei Quidway E300 FW/VRP Router

Redback Networks SmartEdge OS

SUN NETRA X4250

SunOS 5.10

Sun Netra-240

TANDBERG Codec

RedHat eCOs

ZTE ZXR10 ROS V4.8.11.01

ZTE ZXR10 GGSN V4.10.10

ZyXEL MAX-207HW2

n ZXR10 G-Series&8900&6900

17:15:50

GSN)V4.10.10(1.0.0)

GRX landscape – the numbers

- Summary of open ports on GRX hosts found during this “light” survey

Service	Open port	Number
DNS	UDP/53	413
	UDP/2152	1042
Diameter	TCP/3868	177
SMB	TCP/139	208
	TCP/445	115
SNMP	UDP/161	219

These were found from the Internet!

**Out of the 42K GRX live hosts
5.5K hosts from 15 operators were reachable from the
Internet!**

May not need to be in GRX to access GRX

On Her Majesty's Secret Service - GRX & A spy agency - Conclusion

- **GRX traffic is interesting (and definitely for spy agencies!)**
- **GRX is not a closed off network as was agreed**
- **15 operators distribute BGP route prefixes to both GRX & Internet**
- **5.5K GRX hosts reachable from the Internet**
- **Misconfigurations, vulnerable & unnecessary services running**
- **Security best practices such as ingress filtering not commonly adopted**
- **Mobile operators need more security awareness & testing**

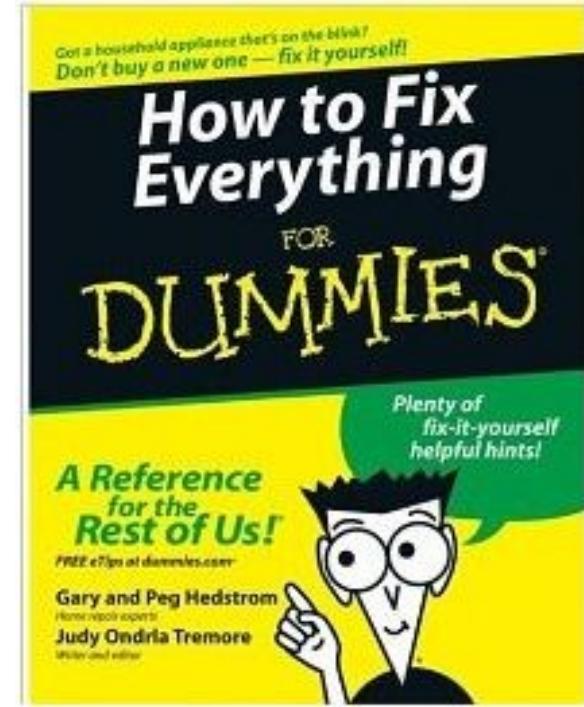
Mitigation & best practises

All systems

- Update & apply security patch
- Harden and remove all unnecessary services

BGP

- Remove GRX prefixes from Internet routers
- Use BGP authentication
- Routers import only specific prefixes from specific AS numbers with roaming agreements
- Ingress filtering
 - permit BGP sessions
 - block spoofed IP addresses (RFC1918,3330 & own IPs)
 - permit GTP (v1&2) towards GGSNs
 - permit DNS traffic to DNS systems
 - permit ICMP echo-reply & request from upstream interface
 - **block all others**



Thank you!

Resource list



rob.kuiters@kpn.com
stephen.kho@kpn.com

OpenGGSN project

<http://sourceforge.net/projects/ggsn/>

Location API

<http://unwiredlabs.com/api>

Network Miner

<http://www.netresec.com/?page=NetworkMiner>

ZMAP

<https://zmap.io>

Masscan

<https://github.com/robertdavidgraham/masscan>

GTP specification

<http://www.3gpp.org/DynaReport/29060.htm>