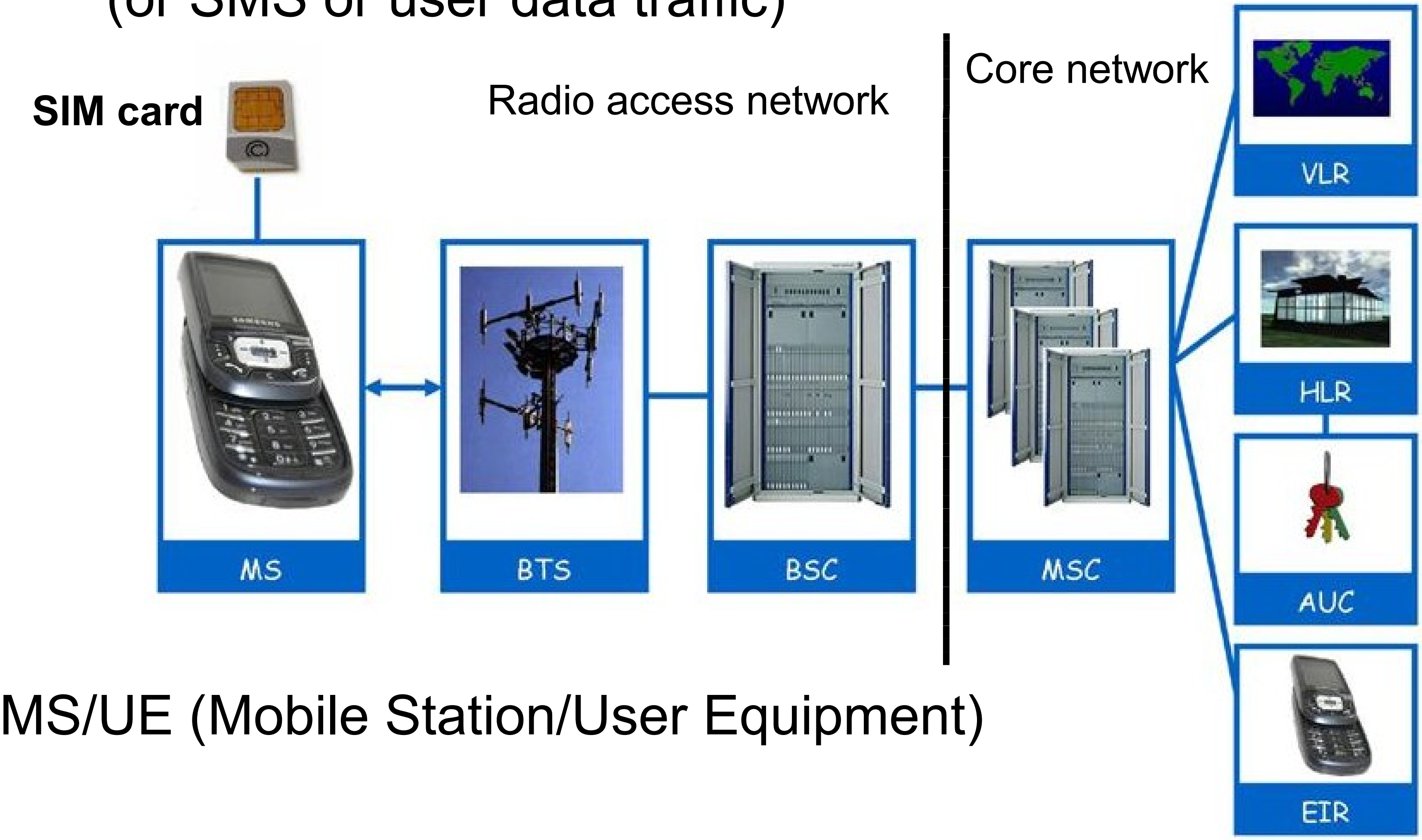
Mobile forensics

SMS (Short Message Service)

EMS, MMS, CBS

How the Mobiles Work

- The Route of a Mobile Phone Telephone Call, (or SMS or user data traffic)



SIM card

Radio access network

Core network

MS

BTS

BSC

MSC

VLR

HLR

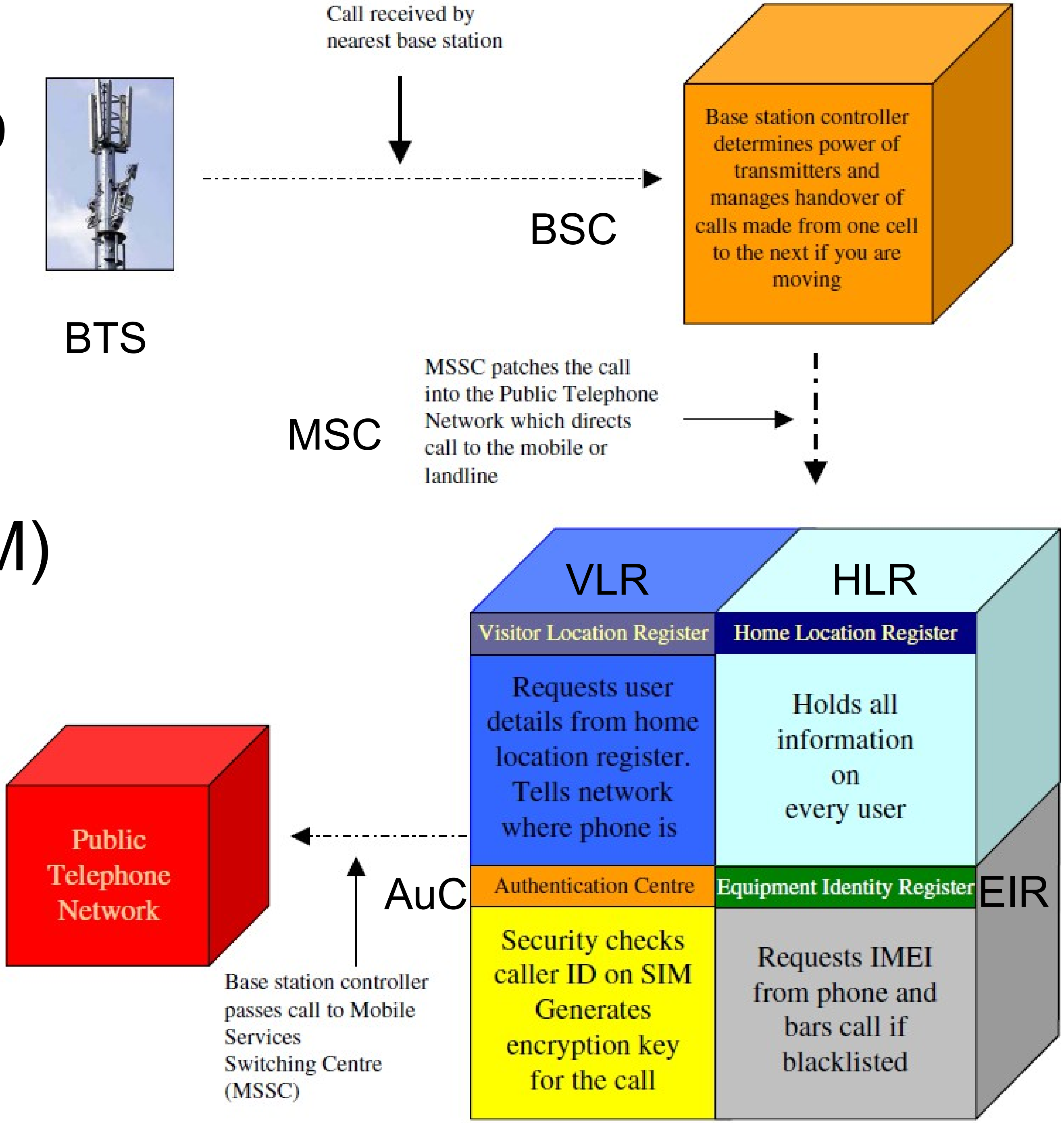
AUC

EIR

MS/UE (Mobile Station/User Equipment)

SMS intro

- How mobile phones work (GSM)



BTS

Call received by nearest base station

BSC

Base station controller determines power of transmitters and manages handover of calls made from one cell to the next if you are moving

MSC

MSSC patches the call into the Public Telephone Network which directs call to the mobile or landline

VLR

Visitor Location Register

Requests user details from home location register. Tells network where phone is

HLR

Home Location Register

Holds all information on every user

AuC

Authentication Centre

Security checks caller ID on SIM Generates encryption key for the call

EIR

Equipment Identity Register

Requests IMEI from phone and bars call if blacklisted

Public Telephone Network

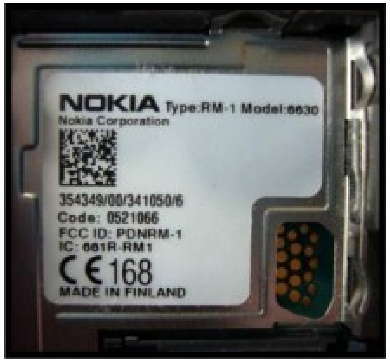
Base station controller passes call to Mobile Services Switching Centre (MSSC)

PSTN
or other
PLMN

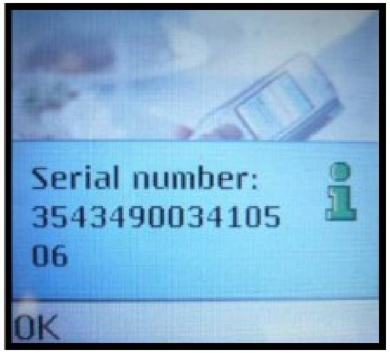
International Mobile Equipment Identifier - IMEI

http://en.wikipedia.org/wiki/IMEI

- 15 digits in length
- Stored digitally in the handset
- Printed on a sticker under the battery
- You can determine make, model and serial from IMEI
- IMEI-number 35-209900-176148-1 means:
  - **TAC** (Type Approval Code): 352099 (allocation number 2099)
  - **FAC** (Final Assembly Code): 00
  - **SNR**: 176148 - uniquely identifying a unit of this model
  - **Control Digit**: 1

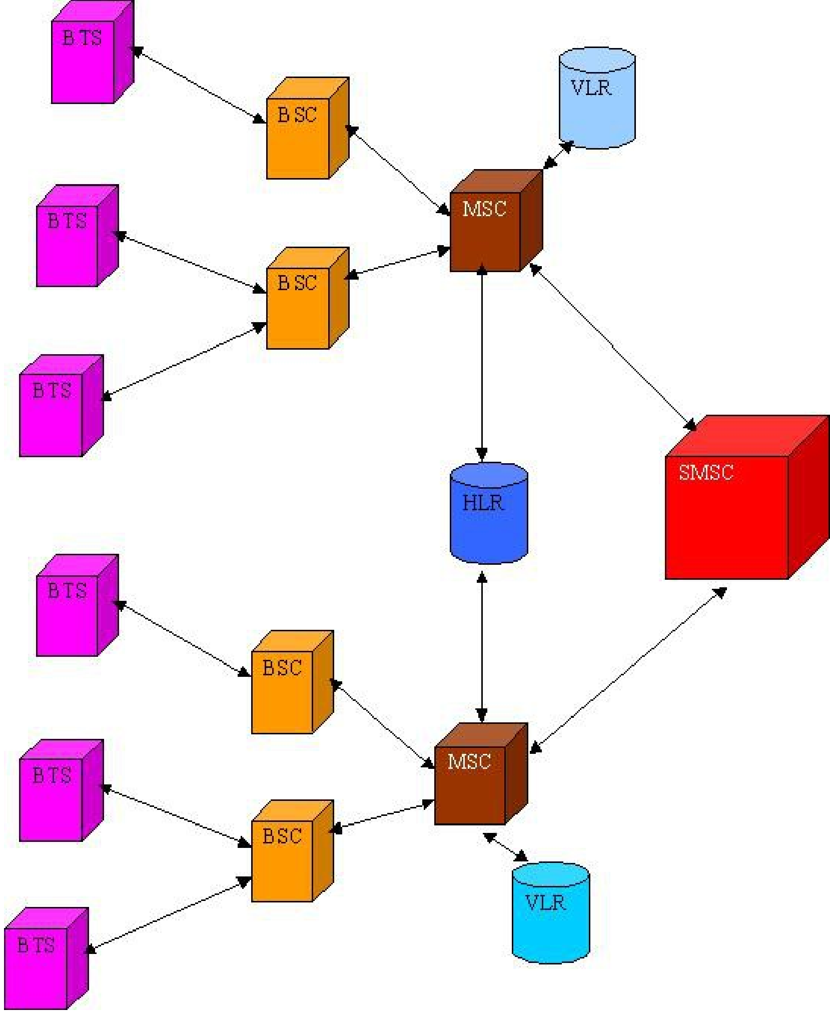


The two versions *should* match…


Serial number:
3543490034105
06

Type *#06#

SMS intro



- BTS - Base Transceiver Station (antenna)
- BSC - Base Station Controller
- MSC - Mobile Switching Center
- HLR- Home Location Register
- VLR - Visitor Location Register
- SMSC - Short Message Service Center
- When a user sends an SMS, the request is placed via the MSC
- The MSC forwards the SMS to the SMSC where it gets stored
- The SMSC queries the HLR to find out where the destination mobile is and forwards the message to the destination MSC if the destination mobile is available
- If the mobile is not available the message gets stored in the current SMSC itself. In most installations If a mobile is not available for SMS delivery the SMSC will not retry. Instead the destination MSC will inform the SMSC when the mobile comes back in range
- http://services.eng.uts.edu.au/userpages/kumbes/public_html/ra/sms/

SMS intro

http://en.wikipedia.org/wiki/Short_message_service

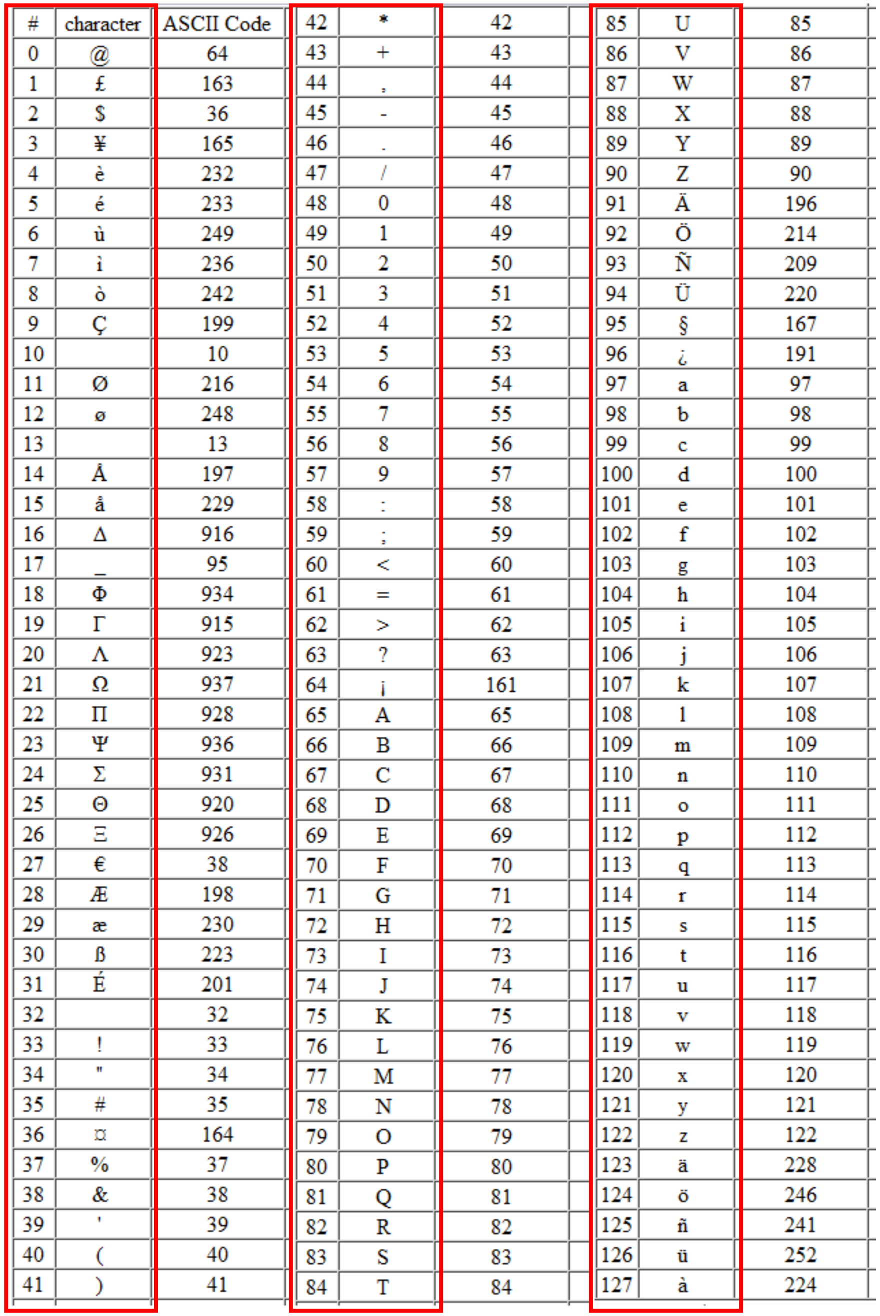
- SMS message is specified by the ETSI (European Telecommunication Standards Institute) organization
  - http://www.etsi.org/ (document GSM 03.40 and GSM 03.38)
- Cell Broadcast Service (CBS) message (GSM 03.49)
  - Carriers version of SMS, only receive, otherwise no difference
  - http://www.cellbroadcastforum.org/
- Enhanced Messaging Service (EMS)
  - An EMS enabled mobile phone can send and receive messages that have special text formatting (such as bold or italic), animations, pictures, icons, sound effects and special ring tones
  - EMS is an intermediate technology, between SMS and MMS
  - http://en.wikipedia.org/wiki/Enhanced_Messaging_Service
- Multimedia Messaging Service (MMS)
  - http://en.wikipedia.org/wiki/Multimedia_Messaging_Service

SMS (1/4)

http://www.dreamfabric.com/sms/

- SMS is a store and forward service
  - Not sent directly from sender to recipient, but always via an SMS Center (SMSC) instead
  - Some SMSCs also provide a "forward and forget“
  - Message delivery is best effort
- Each mobile operator has one or more SMSCs
- Supports ACK of sent message if configured with AT+CSMP
  - Can also sometimes be enabled with a prefix in the SMS user data message body (operator specific) as for example: ”*T#”
- 7-bit default alphabet text messages
  - Up to 160 characters long (since we pack the 7-bits to bytes)

- 7-bits GSM default alphabet
- The corresponding ISO-8859-1 ASCII decimal codes are shown in the right column



#	character	ASCII Code
0	@	64
1	£	163
2	$	36
3	¥	165
4	è	232
5	é	233
6	ù	249
7	ì	236
8	ò	242
9	Ç	199
10		10
11	Ø	216
12	ø	248
13		13
14	Å	197
15	å	229
16	Δ	916
17	_	95
18	Φ	934
19	Γ	915
20	Λ	923
21	Ω	937
22	Π	928
23	Ψ	936
24	Σ	931
25	Θ	920
26	Ξ	926
27	€	38
28	Æ	198
29	æ	230
30	ß	223
31	É	201
32		32
33	!	33
34	"	34
35	#	35
36	¤	164
37	%	37
38	&	38
39	'	39
40	(	40
41	)	41
42	*	42
43	+	43
44	,	44
45	-	45
46	.	46
47	/	47
48	0	48
49	1	49
50	2	50
51	3	51
52	4	52
53	5	53
54	6	54
55	7	55
56	8	56
57	9	57
58	:	58
59	;	59
60	<	60
61	=	61
62	>	62
63	?	63
64	¡	161
65	A	65
66	B	66
67	C	67
68	D	68
69	E	69
70	F	70
71	G	71
72	H	72
73	I	73
74	J	74
75	K	75
76	L	76
77	M	77
78	N	78
79	O	79
80	P	80
81	Q	81
82	R	82
83	S	83
84	T	84
85	U	85
86	V	86
87	W	87
88	X	88
89	Y	89
90	Z	90
91	Ä	196
92	Ö	214
93	Ñ	209
94	Ü	220
95	§	167
96	¿	191
97	a	97
98	b	98
99	c	99
100	d	100
101	e	101
102	f	102
103	g	103
104	h	104
105	i	105
106	j	106
107	k	107
108	l	108
109	m	109
110	n	110
111	o	111
112	p	112
113	q	113
114	r	114
115	s	115
116	t	116
117	u	117
118	v	118
119	w	119
120	x	120
121	y	121
122	z	122
123	ä	228
124	ö	246
125	ñ	241
126	ü	252
127	à	224

- Also here:
- http://www.dreamfabric.com/sms/default_alphabet.html

SMS (2/4)

http://www.dreamfabric.com/sms/

- 8-bit (binary) data messages
  - Max 140 characters long
  - Usually not viewable by the phone as text messages
  - Used for remote control of the phone (if an app can respond)
  - OTA provisioning of WAP settings etc.
- Provisioning is a term often used in the telecommunication field
  - Provisioning refers to the configuration of both hardware and software in order to activate telecommunication service for a customer
  - Provisioning is not equipment. Rather, it consists of commands and controls for specific telecommunication devices
- Flash SMS (aka blinking SMS or alert SMS)
  - A 16-bit text message of class 0, appears on screen at once

SMS (3/4)

http://www.gsm-modem.de/sms.html

- 16-bit messages
  - Max 70 characters long
  - Used for UCS-2 (Universal Character Set coded in 2 octets) messages, http://unicode.org
- Two ways of send and receive SMS
  - PDU (Protocol Description Unit) mode
    - The PDU mode offers to send information in any mode (7/8/16 bit) according to the TP-Data Coding Scheme (DCS) (see a later slide)
    - You can build your own encoding of the characters
  - Text mode (unavailable on some phones) is just an encoding of the bit stream represented by the PDU mode
  - Alphabet differences, the most common encodings are
    - ASCII, PCCP437, PCDN, 8859-1, IRA and GSM
    - Either set by AT command or choosen by phone application

SMS (4/4)

http://www.gsm-modem.de/sms.html

- SMS can be sent and received simultaneously with GSM voice, Data and Fax calls
  - Possible because whereas voice, Data and Fax calls take over a dedicated radio channel for the duration of the call, SMS travel over and above the radio channel using the GSM signaling path (control plane). Similar to what ICMP is for IP?
- Also incorporated into the GSM SMS standards
  - SMS concatenation (appends several short messages together)
    - SMS user data = <UDH> + <Message Body>
  - SMS compression (getting more than 160 characters of information within a single short message)
  - Not all possible features are implemented by all GSM operators worldwide

Concatenated SMS

http://en.wikipedia.org/wiki/Concatenated_SMS

- Larger content (Concatenated SMS, multipart or segmented SMS or "long SMS") can be sent using multiple messages, in which case each message will start with a User Data Header (UDH) containing segmentation information
  - Since UDH is inside the payload, the number of characters per segment is lower: 153 for 7-bit encoding, 134 for 8-bit encoding and 67 for 16-bit encoding
  - Standard theoretically permits up to 255 segments, 6 to 8 segment messages are the practical maximum
- Example of the UDH for a text SMS, split into two parts
  - **Byte 0:** Information Element Identifier, 00 for concatenated SMS with 8-bit and 08 with 16-bit CSMS reference number
  - **Byte 1:** Length of the header, **excluding** these two first bytes; always 3 (8-bit ref number) and 4 (16-bit ref number) for a CSMS
  - **Byte 2:** 00-FF, CSMS reference number, must be same for all the SMS parts in the CSMS
  - **Byte 3:** 00-FF, total number of parts
  - **Byte 4:** 00-FF, this part's number in the sequence

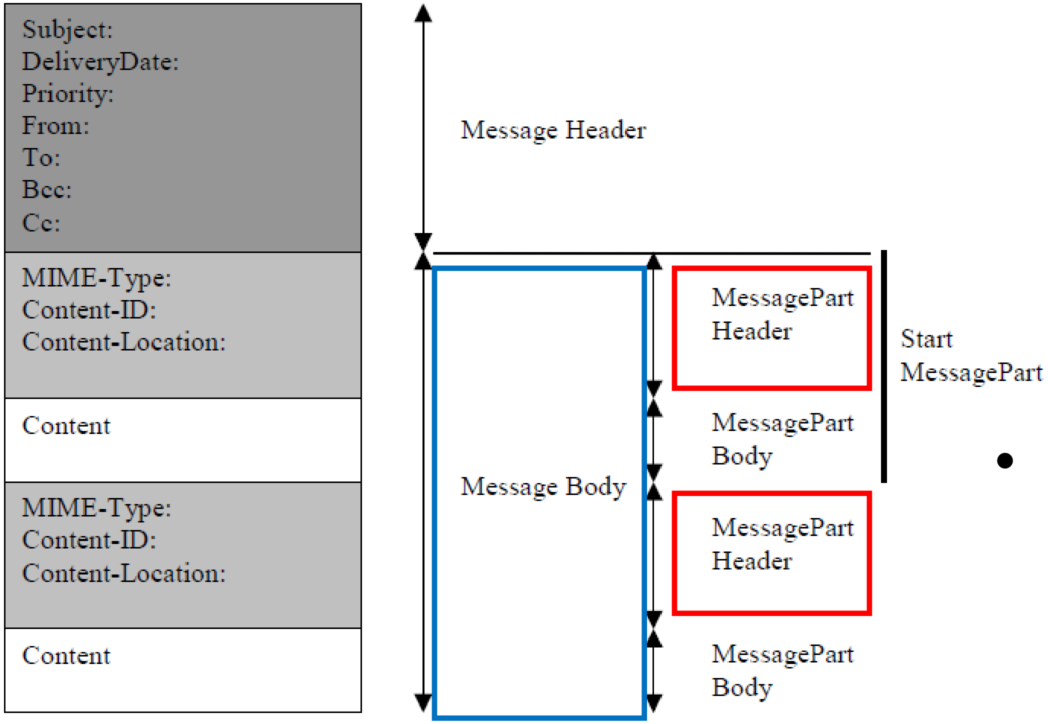
```
00 03 CC 02 00 [ message ]
00 03 CC 02 01 [ message ]
```

MMS 1

http://en.wikipedia.org/wiki/Multimedia_Messaging_Service

- An extension to the SMS standard
  - The standard is developed by the Open Mobile Alliance (OMA), although during development it was part of the 3GPP and WAP groups
- Multimedia content are encoded and inserted into a message in a similar way to MIME types in an e-mail
- The message is forwarded to the carriers MMS store and forward server (MMSC) and then over Internet to recipients carriers MMS relay
- When reached correct MMS relay the message is extracted and viewable via HTTP
- A control message (binary SMS) is sent to the recipient with an URL to the content which the recipient can open up in his WAP browser
- Some installations perform content adaption making it suitable for the receiver UE (User Equipment)
- E-mail and web-based gateways to the MMS (and SMS) systems are common

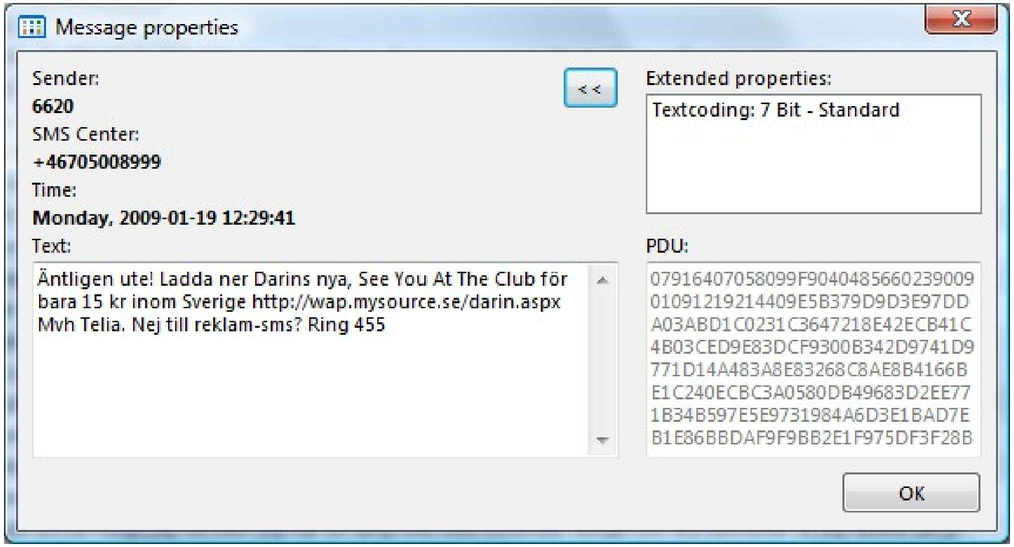
MMS 2



- The content of each message can have its own MIME-Type, ID and Location
  - Location may point to URL
  - Usually script etc. to start presentation
- Do not depend on more than (3 segments)
  - 189 characters, depending on encoding (as UCS-2), segments and port info?
  - 381 bytes for binary message?

MyPhoneExplorer

- Received SMS
  - Sender
  - SMS center
  - Time
  - PDU
    - 7bit
- Sent SMS
  - Recipient
  - Time
  - 2 SMS
  - Validity period
  - PDU
    - 7bit



Message properties

Sender:
6620
SMS Center:
+46705008999
Time:
Monday, 2009-01-19 12:29:41
Text:

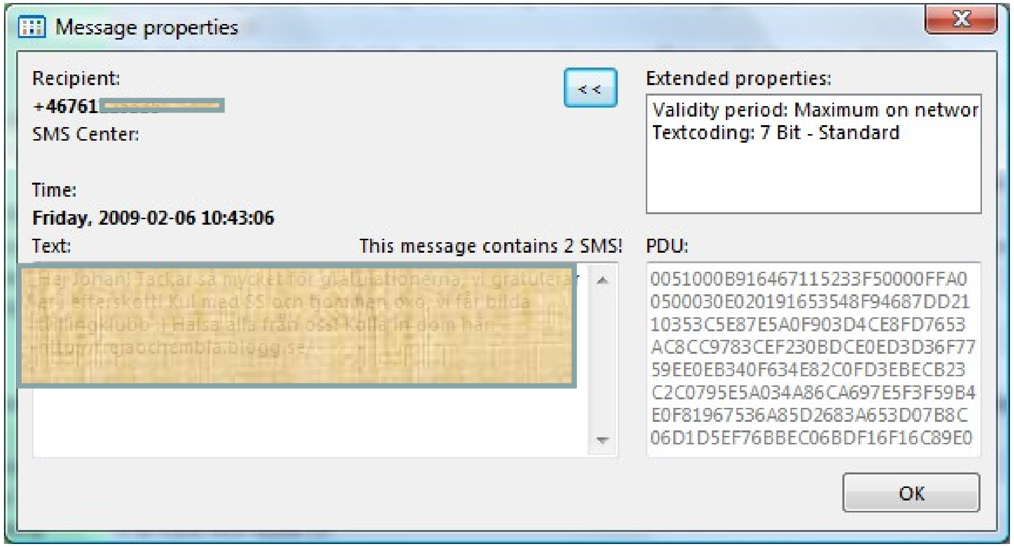
Äntligen ute! Ladda ner Darins nya, See You At The Club för bara 15 kr inom Sverige http://wap.mysource.se/darin.aspx Mvh Telia. Nej till reklam-sms? Ring 455

Extended properties:

Textcoding: 7 Bit - Standard

PDU:

```
07916407058099F9040485660239009
01091219214409E5B379D9D3E97DD
A03ABD1C0231C3647218E42ECB41C
4B03CED9E83DCF9300B342D9741D9
771D14A483A8E83268C8AE8B4166B
E1C240ECBC3A0580DB49683D2EE77
1B34B597E5E9731984A6D3E1BAD7E
B1E86BBDAF9F9BB2E1F975DF3F28B
```



Message properties

Recipient:
+46761[redacted]
SMS Center:

Time:
Friday, 2009-02-06 10:43:06
Text: This message contains 2 SMS!

[redacted]

Extended properties:

Validity period: Maximum on networ
Textcoding: 7 Bit - Standard

PDU:

```
0051000B916467115233F50000FFA0
0500030E02019165354 8F94687DD21
10353C5E87E5A0F903D4CE8FD7653
AC8CC9783CEF230BDCE0ED3D36F77
59EE0EB340F634E82C0FD3EBECB23
C2C0795E5A034A86CA697E5F3F59B4
E0F81967536A85D2683A653D07B8C
06D1D5EF76BBEC06BDF16F16C89E0
```

PDU (Protocol Description Unit) format

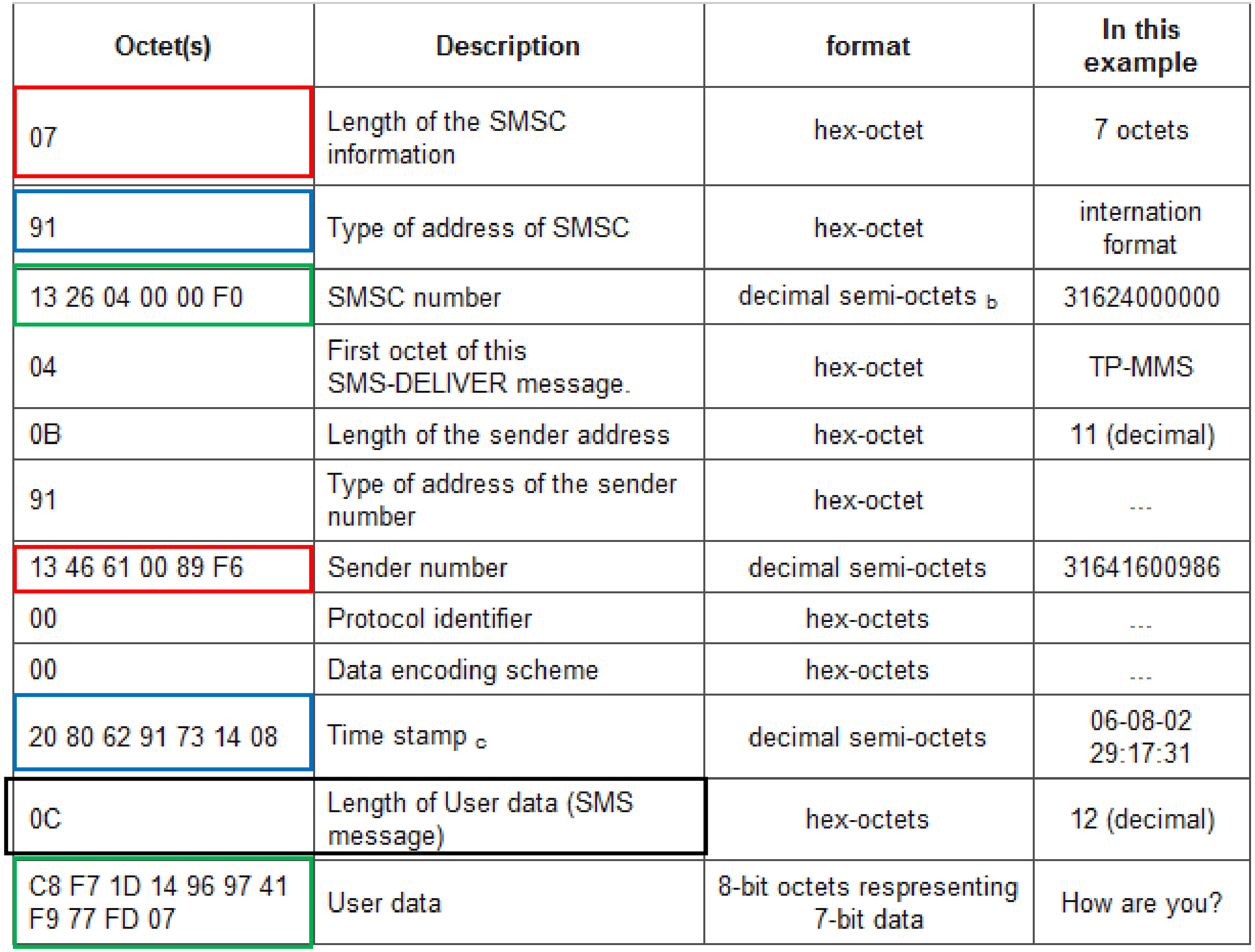
- Note that some hex-octets or decimal semi-octets must be read in reverse order
- Example of received PDU string and its decoding

07911326040000F0040B911346610089F60000208062917314080CC8F71D14969741F977FD07

The status number is not shown. Sent (05), not sent (07), received (01), received unread (03), etc.

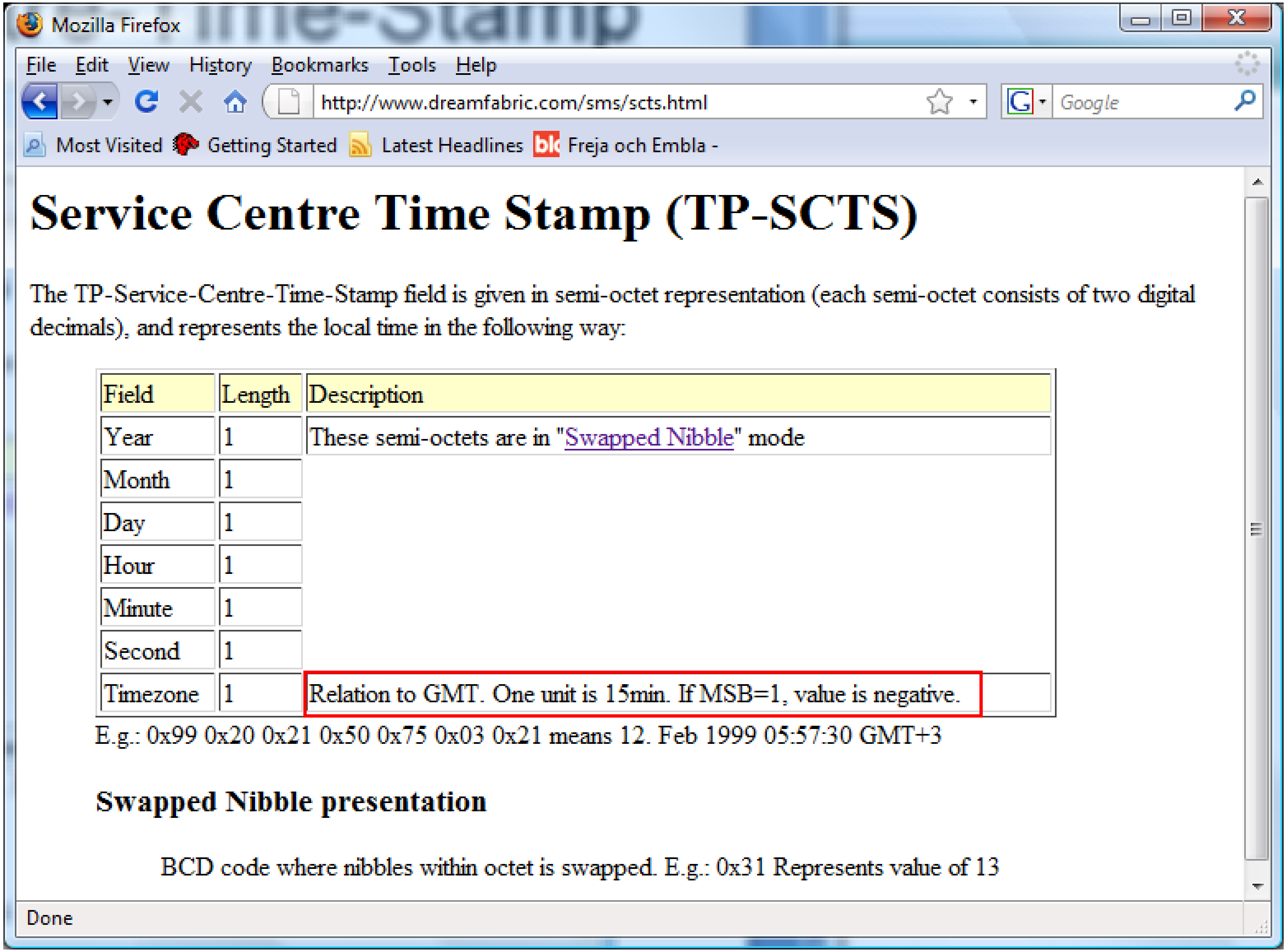
Decimal semi-octet = only 0-9 is used
nibble = semi-octet

yymmddhhmmsstz
020826-193741-80
GMT+0 (negative)



Octet(s)	Description	format	In this example
07	Length of the SMSC information	hex-octet	7 octets
91	Type of address of SMSC	hex-octet	internation format
13 26 04 00 00 F0	SMSC number	decimal semi-octets [b]	31624000000
04	First octet of this SMS-DELIVER message.	hex-octet	TP-MMS
0B	Length of the sender address	hex-octet	11 (decimal)
91	Type of address of the sender number	hex-octet	...
13 46 61 00 89 F6	Sender number	decimal semi-octets	31641600986
00	Protocol identifier	hex-octets	...
00	Data encoding scheme	hex-octets	...
20 80 62 91 73 14 08	Time stamp [c]	decimal semi-octets	06-08-02 29:17:31
0C	Length of User data (SMS message)	hex-octets	12 (decimal)
C8 F7 1D 14 96 97 41 F9 77 FD 07	User data	8-bit octets respresenting 7-bit data	How are you?

TP-Service-Centre-Time-Stamp



Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.dreamfabric.com/sms/scts.html
Google
Most Visited Getting Started Latest Headlines Freja och Embla -
Done

Service Centre Time Stamp (TP-SCTS)

The TP-Service-Centre-Time-Stamp field is given in semi-octet representation (each semi-octet consists of two digital decimals), and represents the local time in the following way:

Field	Length	Description
Year	1	These semi-octets are in "Swapped Nibble" mode
Month	1	
Day	1	
Hour	1	
Minute	1	
Second	1	
Timezone	1	Relation to GMT. One unit is 15min. If MSB=1, value is negative.

E.g.: 0x99 0x20 0x21 0x50 0x75 0x03 0x21 means 12. Feb 1999 05:57:30 GMT+3

Swapped Nibble presentation

BCD code where nibbles within octet is swapped. E.g.: 0x31 Represents value of 13

Send a message in PDU mode (1/2)

http://www.dreamfabric.com/sms/

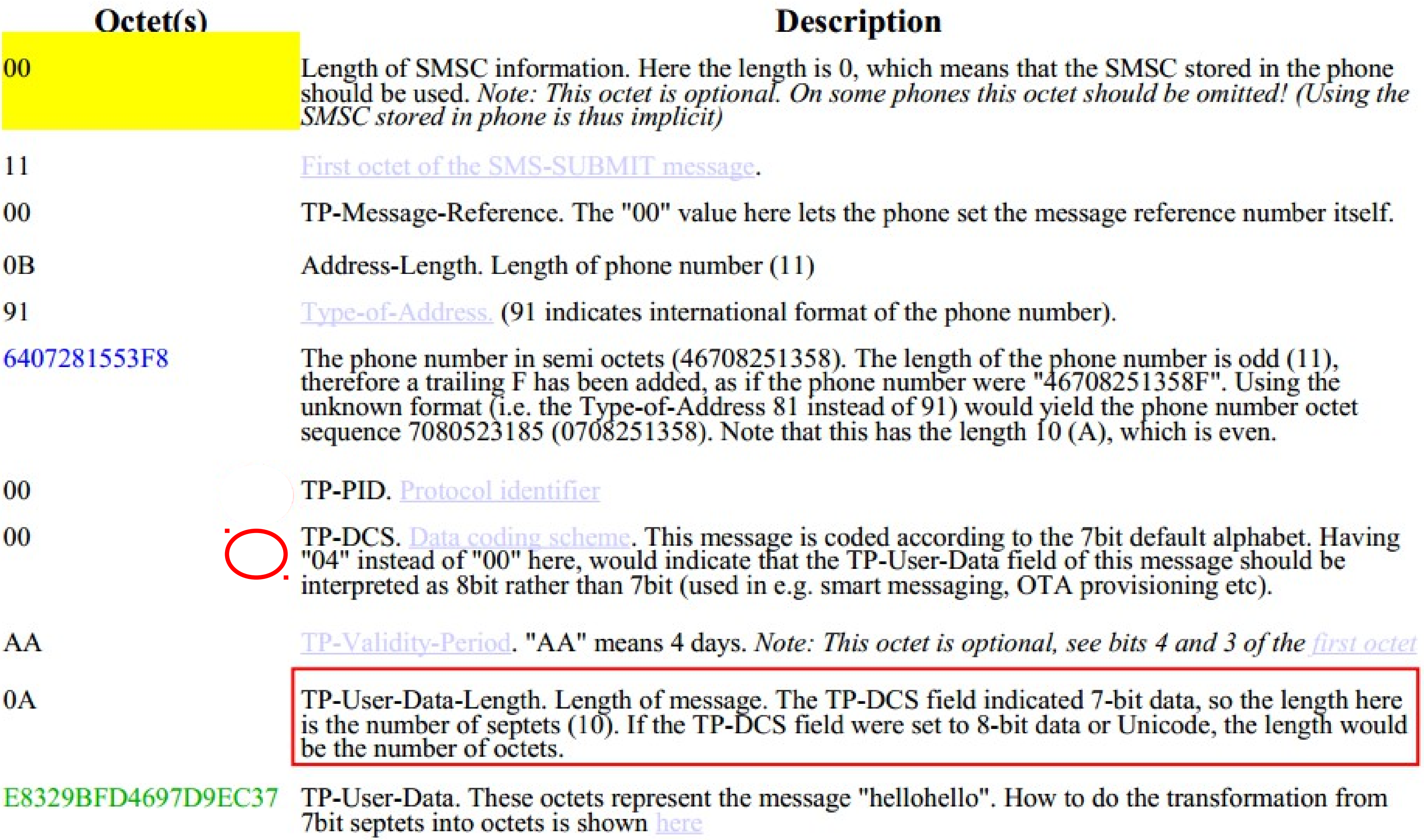
- The following example shows how to send the message "hellohello" in the PDU mode from a Nokia 6110

  ```
  AT+CMGF=0 //Set PDU mode
  AT+CSMS=0 //Check if modem supports SMS commands
  AT+CMGS=23 //Send message, 23 octets (excluding the two initial
  zeros)
  >0011000B916407281553F80000AA0AE8329BFD4697D9EC37
  <ctrl-z>
  ```

- There are 23 octets in this message (46 'characters')
  - The first octet ("00") doesn't count, it is only an indicator of the length of the SMSC information supplied (0)
- Se next slide for explanation of the PDU string

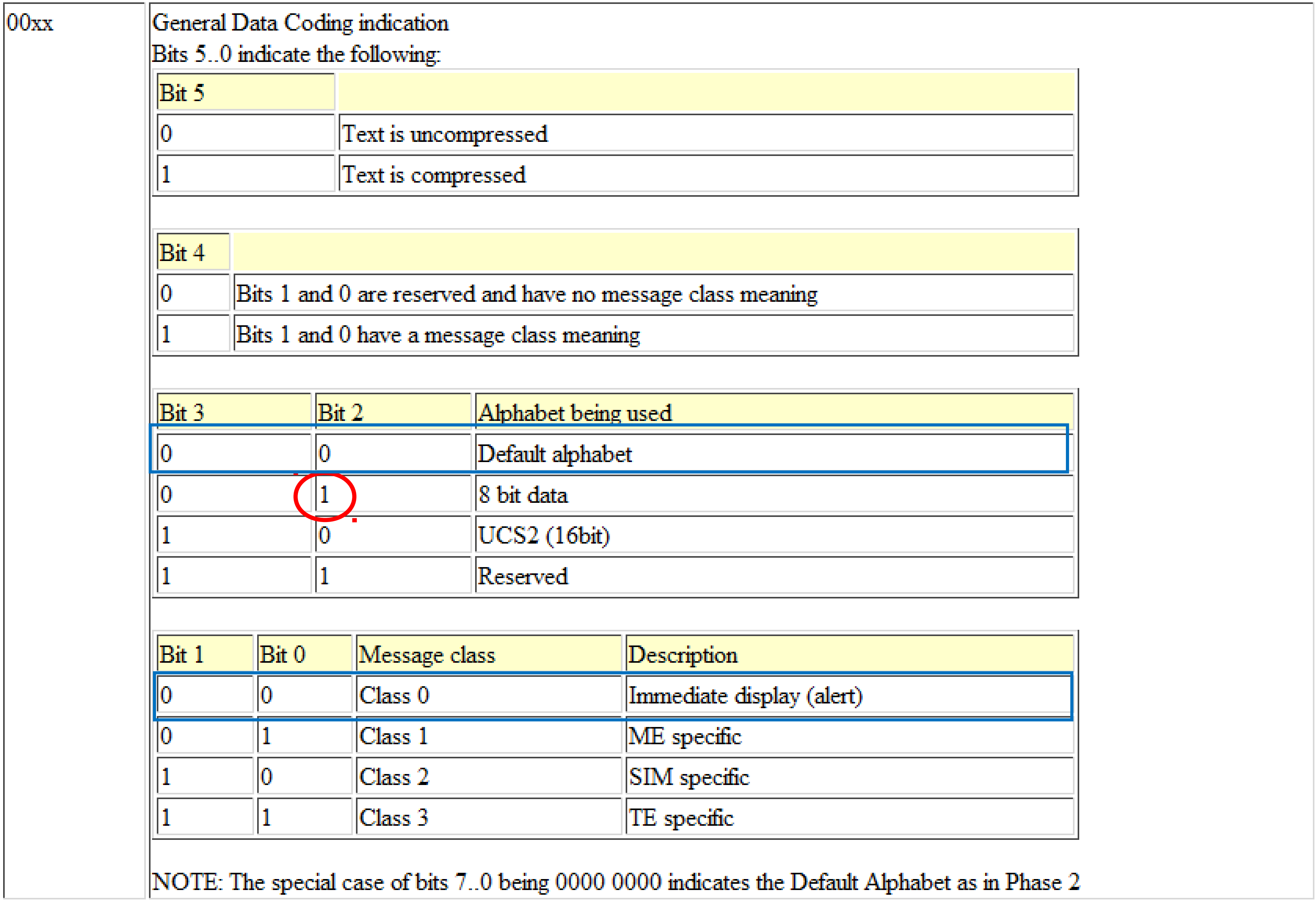
Send a message in PDU mode (2/2)

0011000B916407281553F80000AA0AE8329BFD4697D9EC37



Octet(s)	Description
00	Length of SMSC information. Here the length is 0, which means that the SMSC stored in the phone should be used. *Note: This octet is optional. On some phones this octet should be omitted! (Using the SMSC stored in phone is thus implicit)*
11	First octet of the SMS-SUBMIT message.
00	TP-Message-Reference. The "00" value here lets the phone set the message reference number itself.
0B	Address-Length. Length of phone number (11)
91	Type-of-Address. (91 indicates international format of the phone number).
6407281553F8	The phone number in semi octets (46708251358). The length of the phone number is odd (11), therefore a trailing F has been added, as if the phone number were "46708251358F". Using the unknown format (i.e. the Type-of-Address 81 instead of 91) would yield the phone number octet sequence 7080523185 (0708251358). Note that this has the length 10 (A), which is even.
00	TP-PID. Protocol identifier
00	TP-DCS. Data coding scheme. This message is coded according to the 7bit default alphabet. Having "04" instead of "00" here, would indicate that the TP-User-Data field of this message should be interpreted as 8bit rather than 7bit (used in e.g. smart messaging, OTA provisioning etc).
AA	TP-Validity-Period. "AA" means 4 days. *Note: This octet is optional, see bits 4 and 3 of the* first octet
0A	TP-User-Data-Length. Length of message. The TP-DCS field indicated 7-bit data, so the length here is the number of septets (10). If the TP-DCS field were set to 8-bit data or Unicode, the length would be the number of octets.
E8329BFD4697D9EC37	TP-User-Data. These octets represent the message "hellohello". How to do the transformation from 7bit septets into octets is shown here

Data Coding Scheme (TP-DCS)



00xx

General Data Coding indication
Bits 5..0 indicate the following:

Bit 5	
0	Text is uncompressed
1	Text is compressed

Bit 4	
0	Bits 1 and 0 are reserved and have no message class meaning
1	Bits 1 and 0 have a message class meaning

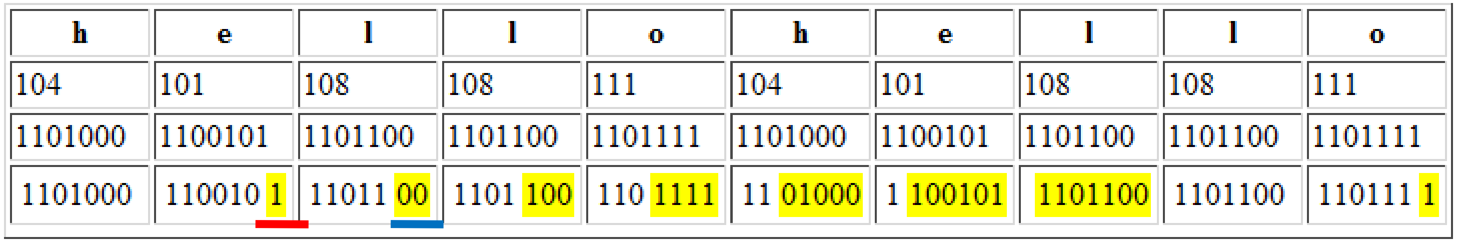
Bit 3	Bit 2	Alphabet being used
0	0	Default alphabet
0	1	8 bit data
1	0	UCS2 (16bit)
1	1	Reserved

Bit 1	Bit 0	Message class	Description
0	0	Class 0	Immediate display (alert)
0	1	Class 1	ME specific
1	0	Class 2	SIM specific
1	1	Class 3	TE specific

NOTE: The special case of bits 7..0 being 0000 0000 indicates the Default Alphabet as in Phase 2

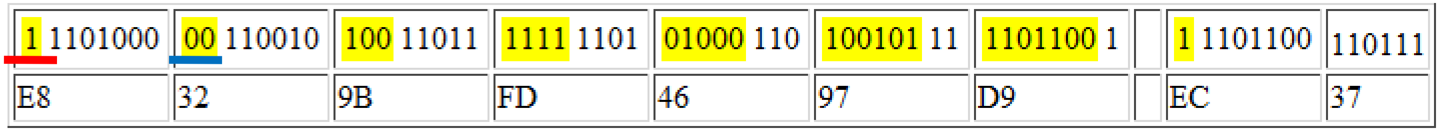
Coding 7-bit data (septets) into octets

- The message "hellohello" consists of 10 characters, called septets when represented by 7 bits each. These septets need to be transformed into octets for the SMS transfer.



h	e	l	l	o	h	e	l	l	o
104	101	108	108	111	104	101	108	108	111
1101000	1100101	1101100	1101100	1101111	1101000	1100101	1101100	1101100	1101111
1101000	110010 1	11011 00	1101 100	110 1111	11 01000	1 100101	1101100	1101100	110111 1

- The first septet (h) is turned into an octet by adding the rightmost bit of the second septet. This bit is inserted to the left which yields 1 + 1101000 = 11101000 ("E8").
- The rightmost bit of the second character is then consumed, so the second character (septet) needs two bits (yellow) of the third character to make an 8bit octet. This process goes on and on yielding the following octets:



1 1101000	00 110010	100 11011	1111 1101	01000 110	100101 11	1101100 1		1 1101100	110111
E8	32	9B	FD	46	97	D9		EC	37

- The 9 octets from "hellohello" are E8 32 9B FD 46 97 D9 EC 37

Receive a message in PDU mode (1/3)

http://www.dreamfabric.com/sms/

- PDU string contains not only the message, but also a lot of meta-information about the sender as
  - Senders SMS service center
  - The time stamp etc.
- Example
  - Sent from an operator SMS service www-page
  - String "hellohello”
  - Received on a Nokia 6110
- PDU string
  - It is all in the form of hexa-decimal *octets* or decimal *semi-octets*
  - This octet sequence consists of three parts:
  - 07 917283010010F5 040BC87238880900F10000993092516195800AE8329BFD4697D9EC37
  - An initial octet indicating the length of the SMSC information ("07")
  - The SMSC information itself ("917283010010F5")
  - And the SMS_DELIVER part (specified by ETSI in GSM 03.40)

Receive a message in PDU mode (2/3)

http://www.dreamfabric.com/sms/

07917283010010F5040BC87238880900F10000993092516195800AE8329BFD4697D9EC37

Octet(s)	Description
07	Length of the SMSC information (in this case 7 octets)
91	Type-of-address of the SMSC. (91 means international format of the phone number)
72 83 01 00 10 F5	Service center number(in decimal semi-octets). The length of the phone number is odd (11), so a trailing F has been added to form proper octets. The phone number of this service center is "+27381000015".
04	First octet of this SMS-DELIVER message.
0B	Address-Length. Length of the sender number (0B hex = 11 dec)
C8	Type-of-address of the sender number
72 38 88 09 00 F1	Sender number (decimal semi-octets), with a trailing F
00	TP-PID. Protocol identifier.
00	TP-DCS Data coding scheme
99 30 92 51 61 95 80	TP-SCTS. Time stamp (semi-octets)
0A	TP-UDL. User data length, length of message. The TP-DCS field indicated 7-bit data, so the length here is the number of septets (10). If the TP-DCS field were set to indicate 8-bit data or Unicode, the length would be the number of octets (9).
E8329BFD4697D9EC37	TP-UD. Message "hellohello" , 8-bit octets representing 7-bit data.

Receive a message in PDU mode (3/3)

- All the octets are hexa-decimal 8-bit octets, except the Service center number, the sender number and the time-stamp; they are decimal semi-octets. The message part in the end of the PDU string consists of hexa-decimal 8-bit octets, but these octets represent 7-bit data
- The semi-octets are decimal, and e.g. the sender number is obtained by performing internal swapping within the semi-octets from "72 38 88 09 00 F1" to "27 83 88 90 00 1F". The length of the phone number is odd, so a proper octet sequence cannot be formed by this number. This is the reason why the trailing F has been added. The time stamp, when parsed, equals "99 03 29 15 16 59 08", where the 6 first characters represent date, the following 6 represents time, and the last two represents time-zone related to GMT.
- Interpreting 8-bit octets as 7-bit messages
  - This transformation is described in detail in GSM 03.38, and an example of the "hellohello" transformation is shown here. The transformation is based on the 7 bit default alphabet , but an application built on the PDU mode can use any character encoding.

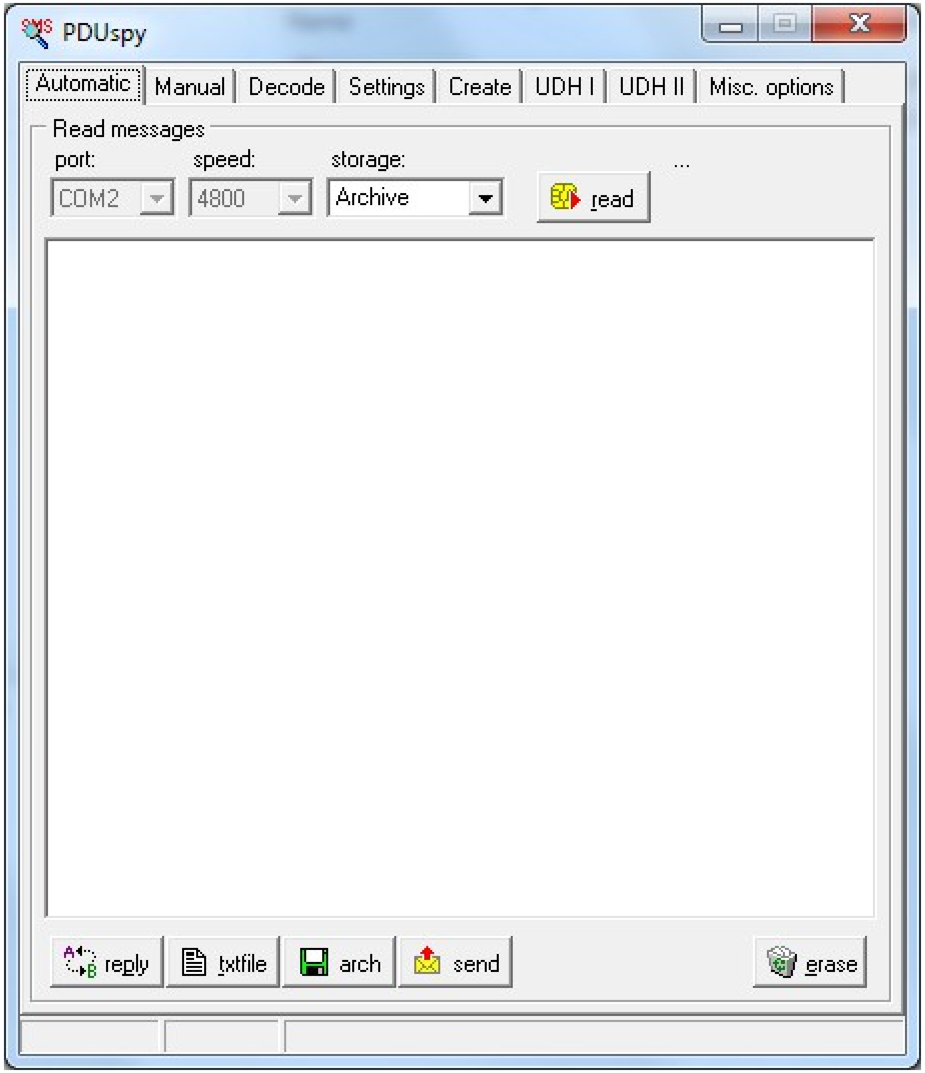
PDUspy

- PDUSpy is a tool to that can be used to:
- Send SMS through your GSM modem or cellphone
- Encode/decode PDU string found in GSM SMS
- Read SMS message from your GSM modem or cellphone
- Set UDH options etc.
- Very technical tool

http://www.nobbi.com/download.html

Manual

http://www.nobbi.com/pduspy.html



SMS further digging

- Python
  - https://github.com/pmarti/python-messaging
  - https://github.com/rapidsms/pygsm
- Perl modules
  - http://www.umts-tools.org/
  - http://cpan.uwinnipeg.ca/htdocs/GSM-Nbit/GSM/Nbit.html
- C/C++ code
  - PDU lib under STL for SMS
  - http://www.codeproject.com/KB/mobile/PDU_lib.aspx
- SMS, EMS, MMS Tutorials and FAQs
  - http://www.palowireless.com/sms/tutorials.asp
- Online PDU Encoder and Decoder (.NET)
  - http://twit88.com/home/utility/sms-pdu-encode-decode
- Using VB.NET to Encode/Decode SMS and EMS
  - http://www.codeproject.com/KB/IP/PDUEncoder.aspx
  - http://www.codeproject.com/KB/IP/PDUDecoder.aspx