Tranalyzer2

gsmDecode

Global System for Mobile Communication (GSM)

Tranalyzer Development Team

Contents

1 gsmDecode

1.1 Description

The gsmDecode plugin analyzes GSM traffic.

1.2 Dependencies

1.2.1 External Libraries

This plugin does not require any external library.

1.2.2 Required Files

The file `tacdb.csv` is required.

1.3 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description	Flags
`GSM_ARFCNFILE`	1	Save ARFCN in a separate file	
`GSM_CALLFILE`	1	Save calls in a separate file	
`GSM_CDFILE`	1	Save channels in a separate file	
`GSM_IMSIFILE`	1	Save IMSI/TMSI/IMEI/IMEISV in a separate file	
`GSM_IMMASSFILE`	1	Save Immediate Assignments in a separate file	
`GSM_OPFILE`	1	Save operator names in a separate file	
`GSM_SMSFILE`	1	Save SMS messages in a separate file	
`GSM_ROTATE_TIME`	0	Create new files every *N* seconds (use 0 to deactivate the feature)	
`GSM_SPEECHFILE`	1	Save audio conversations	
`GSM_STATFILE`	1	Save GSM statistics in a separate file	
`GSM_SPEECH_SPLIT`	1	Speech frames handling: 0: Save A and B flows in the same file 1: Create one file per direction	
`GSM_TMSI_FORMAT`	1	Format for TMSI: 0: Integer, 1: Hexadecimal	
`GSM_SPEECH_DIR`	`"/tmp/gsm_speech"`	Folder for extracted audio conversations	`GSM_SPEECHFILE=1`
`GSM_TXT_DIR`	`"/tmp/gsm_txt"`	Folder for output files	
`GSM_RMDIR`	1	Empty `GSM_SPEECH_DIR` before starting	`GSM_SPEECHFILE=1`

The following flag reside in **src/e164_list.h**:

Name	Default	Description	Flags
`GSM_E164_FORMAT`	0	0: Country code, 1: Country name	

Name	Default	Description	Flags
The following flags reside in **src/mcc_list.h**:			
`GSM_MCC_FORMAT`	0	0: Country code, 1: Country name	
`GSM_MNC_FORMAT`	0	0: Operator name, 1: Brand name	
`GSM_NOT_FOUND`	`""`	Value to use when no entry was found	

The suffix of the output files produced is controlled by the following flags:

Name	Default	Description	Flags
GSM_ARFCNFILE_SUFFIX	"_gsm_arfcn"	Suffix for ARFCN file	GSM_ARFCNFILE=1
GSM_CALLFILE_SUFFIX	"_gsm_calls"	Suffix for calls file	GSM_CALLFILE=1
GSM_CDFILE_SUFFIX	"_gsm_channels"	Suffix for channels file	GSM_CDFILE=1
GSM_IMMASSFILE_SUFFIX	"_gsm_imm_ass"	Suffix for Immediate Assignments file	GSM_IMMASSFILE=1
GSM_IMSIFILE_SUFFIX	"_gsm_imsi"	Suffix for IMSI file	GSM_IMSIFILE=1
GSM_OPFILE_SUFFIX	"_gsm_operators"	Suffix for operators file	GSM_OPFILE=1
GSM_SMSFILE_SUFFIX	"_gsm_sms"	Suffix for SMS file	GSM_SMSFILE=1
GSM_FILES_AMR_EXT	".amr"	File extension for audio files	GSM_SPEECHFILE=1
GSM_FILES_TMP_EXT	".tmp"	File extension for temporary files	
GSM_FILES_TXT_EXT	".txt"	File extension for text files	
GSM_STATFILE_SUFFIX	"_gsm_stats.txt"	Suffix for GSM statistics file	GSM_STATFILE=1

The following flags produce a more verbose output and are mostly useful for debugging:

Name	Default	Description	Flags
GSM_DEBUG_A_RP	0	Print debug messages for A-I/F RP layer	
GSM_DEBUG_A_RP_UNK	0	Report unknown values for A-I/F RP layer	GSM_DEBUG_A_RP=1
GSM_DEBUG_DTAP	0	Print debug messages for A-I/F DTAP layer	
GSM_DEBUG_DTAP_UNK	0	Report unknown values for A-I/F DTAP layer	GSM_DEBUG_DTAP=1
GSM_DEBUG_GSMTAP	0	Print debug messages for GSMTAP layer	
GSM_DEBUG_GSMTAP_UNK	0	Report unknown values for GSMTAP layer	GSM_DEBUG_GSMTAP=1
GSM_DEBUG_LAPD	0	Print debug messages for LAPD layer	
GSM_DEBUG_LAPD_UNK	0	Report unknown values for LAPD layer	GSM_DEBUG_LAPD=1
GSM_DEBUG_LAPDM	0	Print debug messages for LAPDm layer	
GSM_DEBUG_LAPDM_UNK	0	Report unknown values for LAPDm layer	GSM_DEBUG_LAPDM=1
GSM_DEBUG_RSL	0	Print debug messages for RSL layer	
GSM_DEBUG_RSL_UNK	0	Report unknown values for RSL layer	GSM_DEBUG_RSL=1
GSM_DEBUG_SMS	0	Print debug messages for SMS layer	
GSM_DEBUG_SMS_UNK	0	Report unknown values for SMS layer	GSM_DEBUG_SMS=1
GSM_DEBUG	0	Print generic debug messages	
GSM_DEBUG_UNK	0	Report unknown values for other messages	GSM_DEBUG=1

1.3.1 Environment Variable Configuration Flags

The following configuration flags can also be configured with environment variables (ENVCNTRL>0):

- GSM_RMDIR
- GSM_SPEECH_DIR
- GSM_TXT_DIR
- GSM_ARFCNFILE_SUFFIX

- GSM_CALLFILE_SUFFIX
- GSM_CDFILE_SUFFIX
- GSM_IMMASSFILE_SUFFIX
- GSM_IMSIFILE_SUFFIX
- GSM_OPFILE_SUFFIX
- GSM_SMSFILE_SUFFIX
- GSM_FILES_AMR_EXT
- GSM_FILES_TMP_EXT
- GSM_FILES_TXT_EXT
- GSM_STATFILE_SUFFIX
- GSM_ROTATE_TIME

1.4 Flow File Output

The gsmDecode plugin outputs the following columns:

Column	Type	Description	Flags
gsmStat	H32	Status	
gsmLapdSAPI	U8	LAPD Service Access Point Identifier (SAPI)	
gsmLapdTEI	U8	LAPD Terminal Endpoint Identifier (TEI)	
gsmRslTN	R(U8)	GSM RSL Timeslot Numbers	
gsmAMRDuration	FLT	GSM Duration of AMR conversation (seconds)	GSM_SPEECHFILE=1
gsmNumAMRGood_bad	U32_U32	GSM Number of AMR good/bad frames	GSM_SPEECHFILE=1

1.4.1 gsmStat

The gsmStat column is to be interpreted as follows:

gsmStat	Description
0x0000 0001	LAPD Radio Signalling Link (RSL, SAPI 0)
0x0000 0002	LAPD O&M link (SAPI 62)
0x0000 0004	LAPD Layer 2 Management (SAPI 63)
0x0000 0008	RSL Radio Link Layer Management (RLM)
0x0000 0010	RSL Dedicated Channel Management (DCM)
0x0000 0020	RSL Common Channel Management (CCM)
0x0000 0040	RSL TRX Management
0x0000 0080	RSL Location Services
0x0000 0100	RSL ip.access Vendor Specific

gsmStat	Description
`0x0000 0200`	RSL HUAWEI Paging Extension
`0x0000 0400`	GSM A-I/F DTAP
`0x0000 0800`	GSM A-I/F DTAP Call Control (CC)
`0x0000 1000`	GSM A-I/F DTAP Mobility Management (MM)
`0x0000 2000`	GSM A-I/F DTAP Radio Resources Management (RR)
`0x0000 4000`	GSM A-I/F DTAP SMS
`0x0000 8000`	GSM A-I/F RP
`0x0001 0000`	GSM SMS TPDU
`0x0002 0000`	GSM Mobile Application (GSM MAP)
`0x0004 0000`	AMR speech
`0x0008 0000`	—
`0x0010 0000`	Uplink
`0x0020 0000`	Downlink
`0x0040 0000`	—
`0x0080 0000`	—
`0x0100 0000`	File I/O error
`0x0200 0000`	—
`0x0400 0000`	LAPD decoding error
`0x0800 0000`	LAPDm decoding error
`0x1000 0000`	RSL decoding error
`0x2000 0000`	DTAP decoding error
`0x4000 0000`	SMS decoding error
`0x8000 0000`	Decoding error

1.4.2 gsmTSC

The `gsmTSC` (Training Sequence Code) column is to be interpreted as follows:

gsmTSC	Description
0	`00100101110000100010010111`
1	`00101101110111100010110111`
2	`01000011101110100100001110`
3	`01000111101101000100011110`
4	`00011010111001000001101011`
5	`01001110101100000100111010`
6	`10100111110110001010011111`
7	`11101111000100101110111100`

1.5 Packet File Output

In packet mode (`-s` option), the gsmDecode plugin outputs the following columns:

Column	Type	Description	Flags
gsmStat	H32	Status	
gsmLapdSAPI	U8	LAPD Service Access Point Identifier (SAPI)	
gsmLapdTEI	U8	LAPD Terminal Endpoint Identifier (TEI)	
gsmRslMsgType	S	GSM RSL Message type	
gsmRslTN	U8	GSM RSL Timeslot Number	
gsmRslSubCh	U8	GSM RSL Subchannel Number	
gsmRslChannel	S	GSM RSL Channel	
gsmDtapTN	U8	GSM A-I/F DTAP Timeslot Number	
gsmDtapChannel	S	GSM A-I/F DTAP Channel	
gsmHandoverRef	U8	Handover reference	
gsmLAIMCC	S	LAI: Mobile Country Code (MCC)	
gsmLAIMCCCountry	S	LAI: MCC Country	
gsmLAIMNC	S	LAI: Mobile Network Code (MNC)	
gsmLAIMNCOperator	S	LAI: MNC Operator	
gsmLAILAC	H16	LAI: Location Area Code (LAC)	
gsmEncryption	SC	Encryption algorithm	
gsmContent	S	Content (voice or signalling)	
gsmAMRCMR	S	AMR codec mode request (CMR)	GSM_SPEECHFILE=1
gsmAMRFrameType	S	AMR frame type	GSM_SPEECHFILE=1
gsmAMRFrameQ	SC	AMR frame quality	GSM_SPEECHFILE=1

1.6 Plugin Report Output

The following information is reported:

- Aggregated gsmStat
- Number of GSMTAP packets
- Number of GSM RSL packets
- Number of GSM DTAP packets
- Number of GSM DTAP CC packets
- Number of GSM DTAP MM packets
- Number of GSM DTAP RR packets
- Number of GSM DTAP SMS packets
- Number of GSM DTAP SS packets
- Number of SMS messages

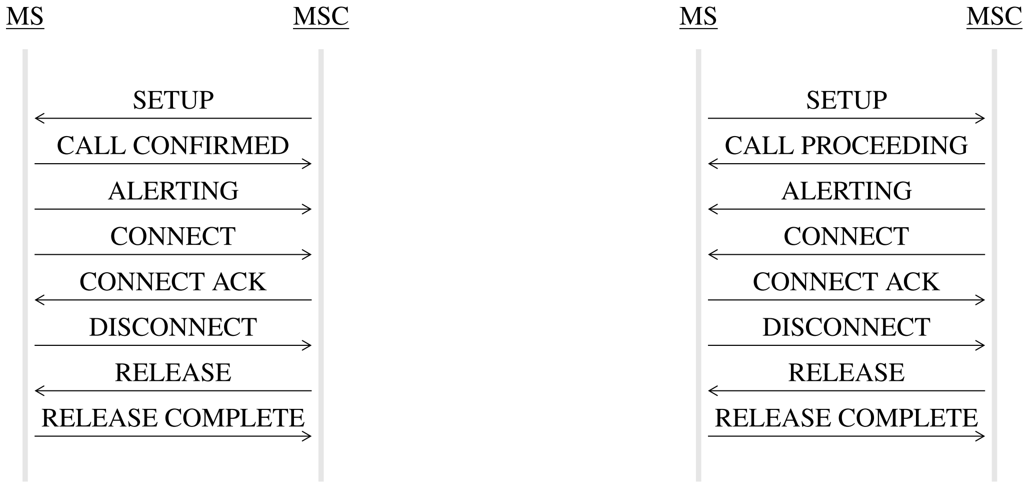
1.7 Additional Output

Non-standard output:

- PREFIX_gsm_arfcn.txt: list of ARFCN, GSM band, up/down frequencies

- `PREFIX_gsm_calls.txt`: list of calls with numbers, countries, ...
- `PREFIX_gsm_channels.txt`: list of channels and their content (speech/signalling)
- `PREFIX_gsm_imm_ass.txt`: list of immediate assignments
- `PREFIX_gsm_imsi.txt`: list of IMSI/TMSI/IMEI/IMEISV, with manufacturers, models, countries and operators.
- `PREFIX_gsm_operators.txt`: list of network operators names and time zones
- `PREFIX_gsm_sms.txt`: list of extracted SMS messages with numbers and countries

1.8 GSM Mobile Terminating and Mobile Originating Call Call Flow Procedures



1.9 Post-Processing

1.9.1 AMR Conversion

The `utils/amr_conv.sh` script can be used to convert extracted AMR conversations to MP3, OGA or WAV files. In addition, the same script can be used to merge two mono AMR files into one stereo MP3, OGA or WAV file. Try `utils/amr_conv.sh --help` for more information

1.9.2 Concatenated SMS messages

The concatenated SMS messages are currently not reassembled. They can be grouped in post-processing with the following `tawk` command:

```
$ tawk 't2rsort(flowInd ";" smsMsgId ";" smsMsgPart)' file_gsm_sms.txt
```

1.10 Acronyms

Acronym	Definition
ACCH	Associated Control Channel
AGCH	Access Grant Channel
AMR	Adaptive Multi-Rate
ARFCN	Absolute Radio-Frequency Channel Number
AuC	Authentication Center
BCCH	Broadcast Control Channel
BSC	Base Station Controller
BSS	Base Station Subsystem (BTS + BSC)

Acronym	Definition
BTS	Base Transceiver Station
CC	Call Control
CBCH	Cell Broadcast Channel
CCCH	Common Control Channel
CCH	Control Channel
CM	Connection Management
DCCH	Dedicated Control Channel
DL	Downlink
DTAP	Direct Transfer Application Part
EIR	Equipment Identity Register
FACCH	Fast Associated Control Channel
FCCH	Frequency Correction Channel
GSM	Global System for Mobile Communication
HLR	Home Location Register
HSN	Hopping Sequence Number
IMEI	International Mobile Equipment Identity
IMEISV	International Mobile Equipment Identity Software Version
IMSI	International Mobile Subscriber Identity
LAC	Location Area Code
LAI	Location Area Identification
LAPD	Link Access Protocol for D Channel
MAIO	Mobile Allocation Index Offset
MCC	Mobile Country Code
MM	Mobility Management
MNC	Mobile Network Code
MS	Mobile Station
MSC	Mobile Switching Center
NMC	Network Management Center
NSS	Network Subsystem
O&M	Operation & Maintenance
OMC	Operation & Maintenance Center
OMS	Operation & Maintenance Subsystem
PCH	Paging Channel

Acronym	Definition
RACH	Random Access Channel
RR	Radio Resource
RSL	Radio Signalling Link
SACCH	Slow Associated Control Channel
SAPI	Service Access Point Identifier
SC	Service Centre
SCH	Synchronization Channel
SDCCH	Standalone Dedicated Control Channel
SMS	Short Message Service
SMSC	Short Message Service Center
SS	Supplementary Services
TAC	Type Allocation Code
TC	Transcoder
TCH	Traffic Channel
TCH/F	Full Rate Traffic Channel
TCH/H	Half Rate Traffic Channel
TEI	Terminal Endpoint Identifier
TMSI	Temporary Mobile Subscriber Identity
TN	Timeslot Number
TRX	Transceiver
TSC	Training Sequence Code
UL	Uplink
VLR	Visitors Location Register

1.11 References

- GSM 04.07: Mobile radio interface signalling layer 3 general aspects
- GSM 04.08: Mobile radio interface layer 3 specification
- GSM 08.56: BSC-BTS interface layer 2 specification
- GSM 08.58: BSC-BTS interface layer 3 specification