Systems Applications Proxy Pwnage

ian@sensepost.com

about: us

sensepost

Ian de Villiers

What we're going to talk about

- Why this Talk ?
- The history of decompressing SAP DIAG
- Understanding the fundamentals
- New Attacks
- Conclusion

Why this Talk ?

- SAP systems carry business critical data
  - Root is nice, but it's all about the data… ☺
- Any numbers of attacks against SAP systems
  - This talk is not about them…
- Fundamental security shortcoming in the SAP GUI (DIAG) protocol
  - Unencrypted. By Default
  - Compressed
  - This is old news…

#include <Disclaimer.h>

- SAP is a behemoth
- Very little documentation out there
  - service.sap.com require user accounts ☹
- Documentation for DIAG protocol requires NDA (apparently)… ☹
- Custom toolsets require development
- SAP Basis version used is reasonably outdated..
  - Fine for protocol analysis
  - Some attack scenarios may not be applicable

#include <Disclaimer.h>

- SensePost Assessments
  - Covered a lot of ground…
  - … but virtually impossible to do a complete job on something as complex
  - Research has been on an “as-time-allows” approach between projects
- Releasing tools and research as-is…
  - Let’s see some SAP 0-day in the next couple of months… ☺
- Lack of documentation means analysis is probably not spot-on

#include <Disclaimer.h>

- Planned to present with SAP on second laptop
- Some technical issues yesterday
  - Running SAP in a VM
  - Laptop is a dog in terms of speed at the moment

What we're going to talk about

- ~~Why this Talk ?~~
- The history of decompressing SAP DIAG
- Understanding the fundamentals
- New Attacks
- Conclusion

The History…

- Sniffing SAP GUI Passwords
  - Andreas Baus && René Ledosquet from Securon
  - Published 6th July, 2009
- Dealt with playing back captured packets to SAP GUI
- Decompressed data obtained from SAP GUI memory with debugger

But wait…
There's more…

The History…

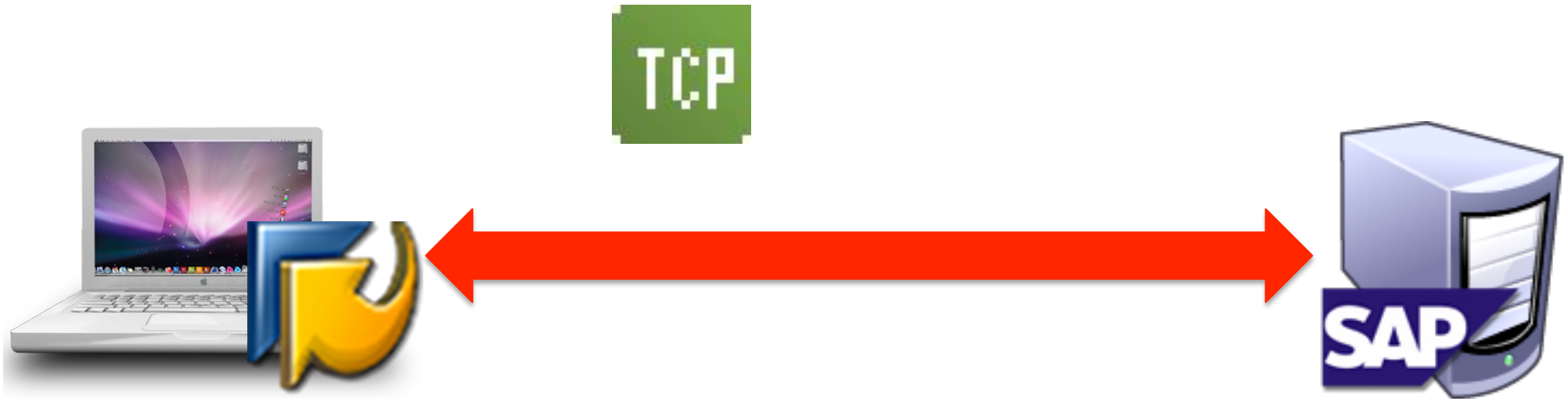
- Dennis Yurichev
  - Published 2nd June, 2010
- Discovered that similar compression method was employed in MaxDB
  - Open Source MaxDB code available
- Wrote utility for decompressing SAP traffic
  - Required manual reassembly of data segments over multiple packets

The History…

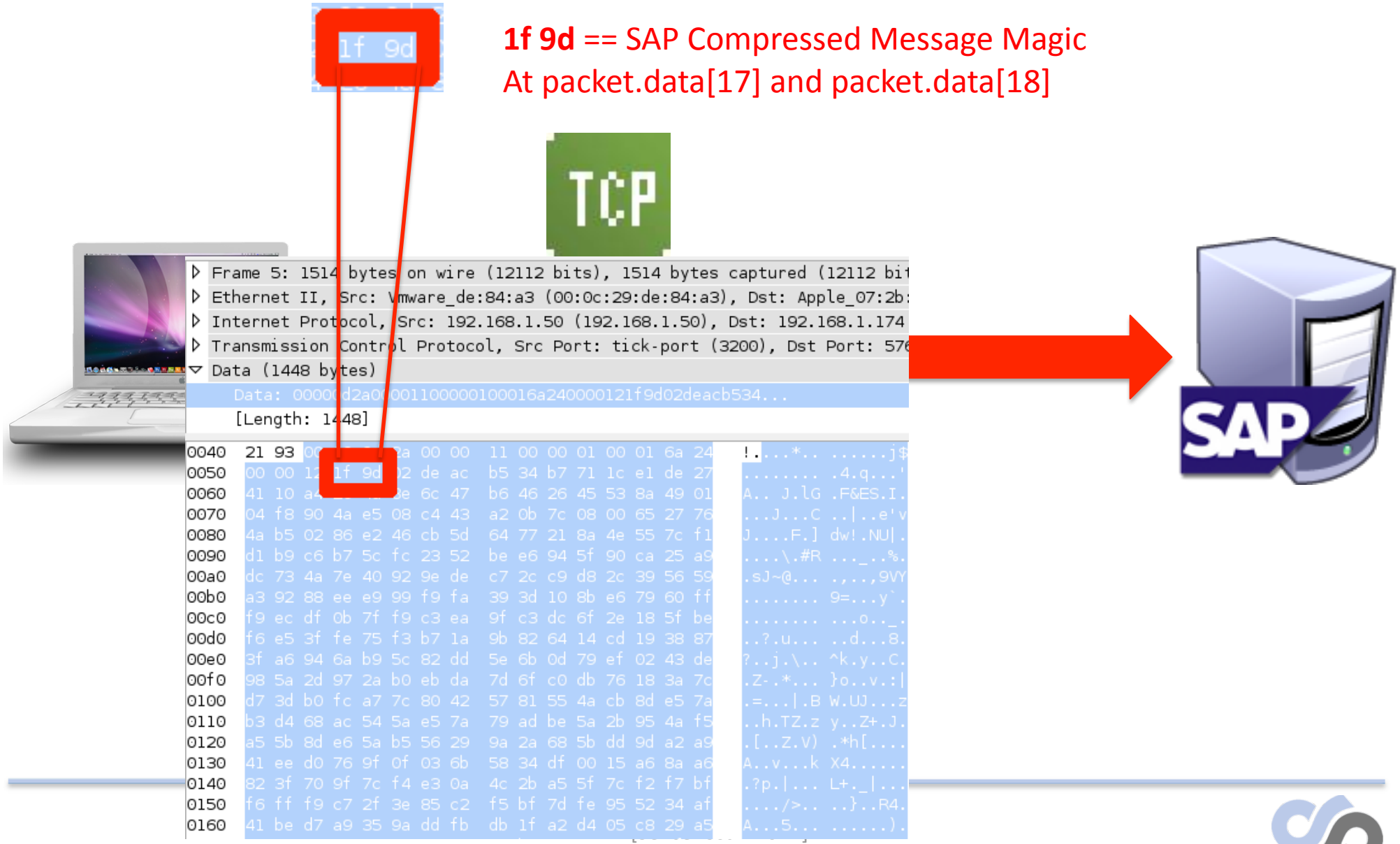
- Dennis' research required:
  - Identification of SAP compressed packets by magic
    - 0x1f @ packet.data[17]
    - 0x9d @ packet.data[18]
  - Stringing together of subsequent packets without magic at 17 and 18
  - Once complete "message" had been assembled, we could decompress the data
    - (Decompression won't work until we have the complete stream)

SAPDecompress – In Pictures

SAPDecompress – In Pictures

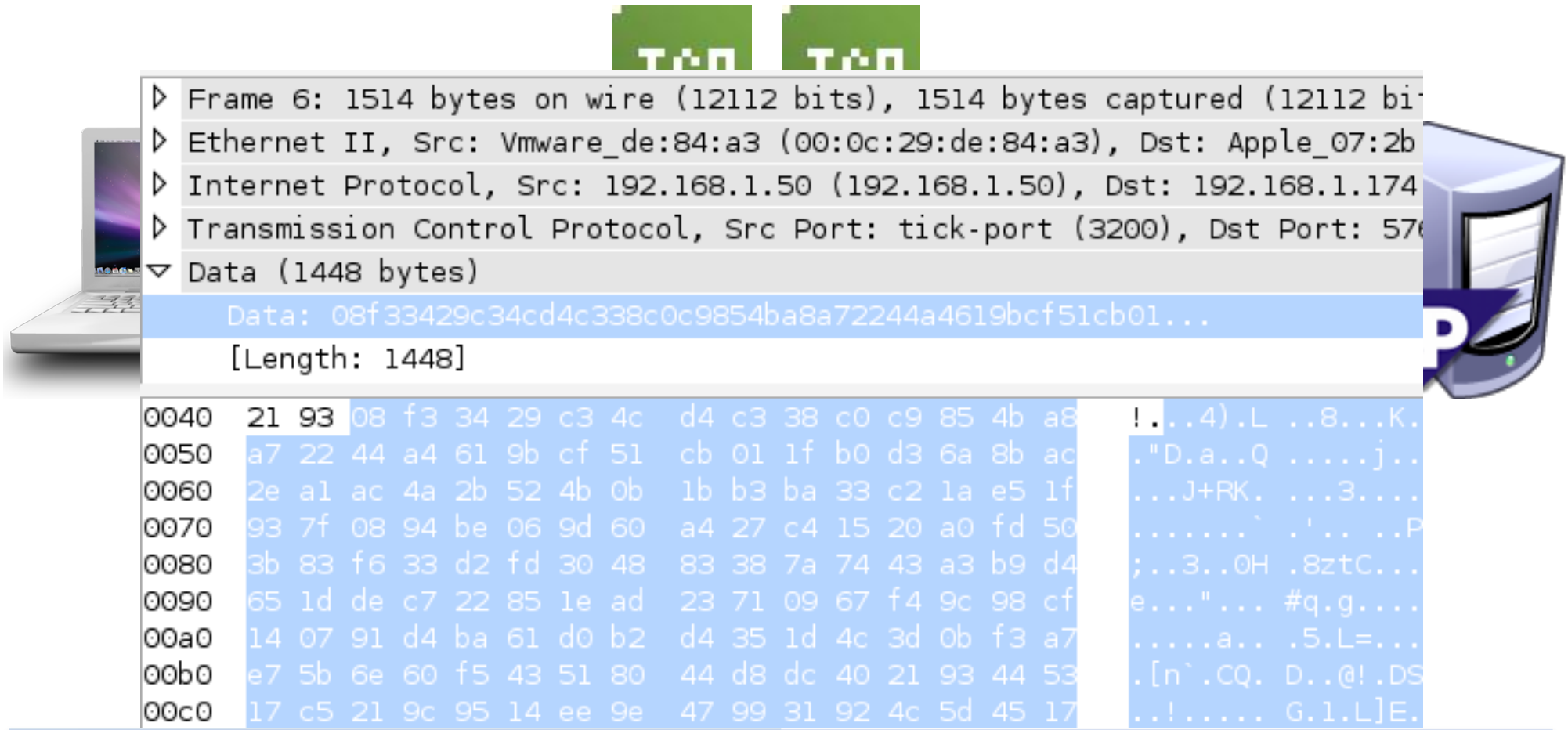


SAPDecompress – In Pictures

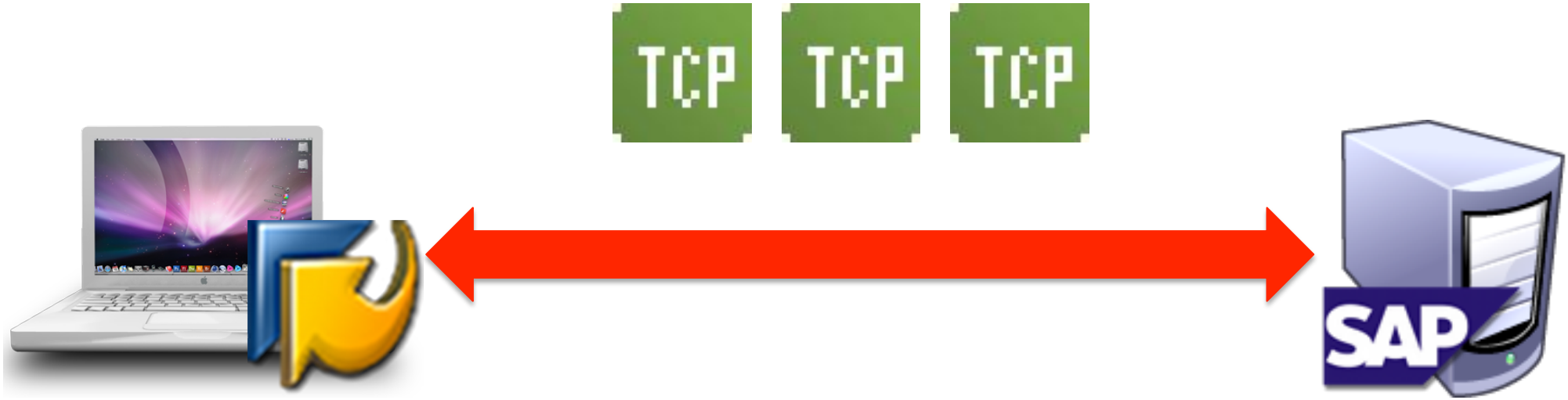


SAPDecompress – In Pictures

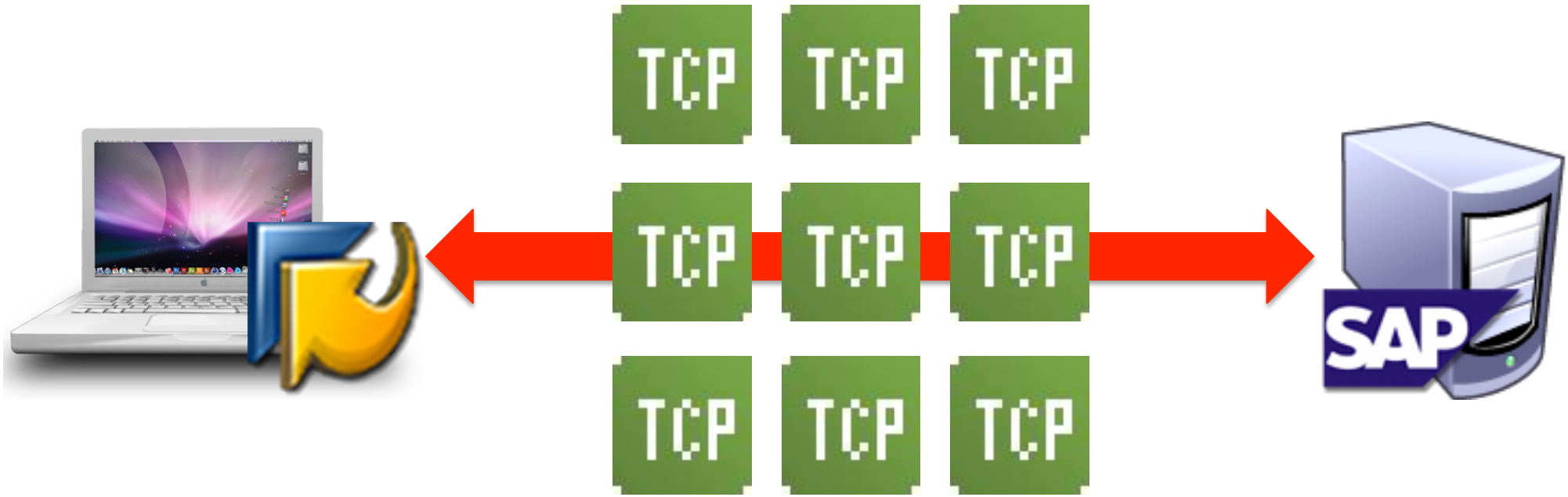
SAPDecompress – In Pictures



SAPDecompress – In Pictures



SAPDecompress – In Pictures



SAPDecompress – In Pictures

SAPDecompress – In Pictures

Compressed Message

SAPDecompress.exe

Decompressed Message

SAPDecompress – In Pictures

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Rå ø ½ $ Eqü \ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £ § n · · Úî 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ¬ ° ŸB ‡ R ‡ VÔ
04.:	db	53	7f	47	e7	ae	2d	f2	c2	e5	0b	9f	f3	3d	e7	fb	ÛS Gç ® - òÂå Ÿó = çû
05.:	65	ac	0a	07	0f	8b	17	40	08	8f	d9	b5	94	36	4c	fd	e ¬ ‹ @ Ùµ " 6Lý
06.:	bb	36	a0	56	81	7c	cb	b1	51	3b	85	1c	cd	aa	0c	10	» 6 V | Ë ± Q ; … Íª
07.:	a0	04	fa	bf	5d	d4	34	28	83	49	14	a1	84	da	09	19	ú ¿] Ô 4 (ƒ I ¡ „ Ú
08.:	cf	50	6b	90	d4	b1	c0	a0	01	05	80	9c	59	73	71	2e	ÏPk Ô ± À œ Ysq.
09.:	11	6a	7f	5b	46	59	9d	ca	7f	d3	b9	38	53	34	8a	70	j [FY Ê Ó ¹ 8S4 Šp
0a.:	4e	c3	cc	25	01	18											
0b.:	ce	e8	be	99	40	65											
0c.:	a3	ed	c6	15	f2	ca											
0d.:	fe	39	be	14	bd	ae											
0e.:	a4	ab	73	de	e9	3f											
0f.:	42	04	87	d3	51	c2											
10.:	7f	4a	06	eb	f0	75											
11.:	d6	cc	71	45	8b	44											
12.:	c7	26	43	40	06	65											
13.:	4d	2a	59	aa	13	55											

Compressed Message

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 431 Bytes
00.:	01	01	0f	00	00	00	00	00	00	00	00	00	00	00	00	00	
01.:	00	10	06	23	00	0f	00	00	10	0e	01	34	31	31	30	00	# 4110
02.:	55	54	46	38	00	10	04	09	00	03	37	32	30	10	04	19	UTF8 720
03.:	00	02	00	00	10	0f	01	00	10	00	00	07	00	0a	0f	00	
04.:	00	00	00	00	00	00	00	00	00	10	04	04	00	08	00	14	
05.:	00	07	00	10	00	07	10	04	17	00	02	00	1f	10	04	16	
06.:	00	02	00	13	10	05	01	00	16	00	05	00	00	02	14	11	
07.:	3d	10	5b	31	10	00	11	00	00	00	00	00	00	00	00	10	= [1
08.:	0c	08	00	10	00	00	03	e6	00	00	07	70	00	00	03	e6	æ p æ
09.:	00	00	07	70	10	0c	06	00	21	00	00	00	11	00	00	00	p !
0a.:	00	00	00	00	31	00	00	01	10	00	00	00	00	00	00	00	1
0b.:	00	00	00	00	13	00	00	00	5b	02	10	09	0b	00	0a	01	[
0c.:	00	02	00	14	00	00	00	00	00	11	00	00	00	e0	3c	3f	à<?
0d.:	78	6d	6c	20	76	65	72	73	69	6f	6e	3d	22	31	2e	30	xml version="1.0
0e.:	22	20	65	6e	63	6f	64	69	6e	67	3d	22	73	61	70	2a	" encoding="sap*
0f.:	22	3f	3e	0a	3c	44	41	54	41	4d	41	4e	41	47	45	52	"?> <DATAMANAGER
10.:	3e	0a	20	20	3c	43	4f	50	59	20	69	64	3d	22	63	6f	> <COPY id="co
11.:	70	79	22	3e	0a	20	20	20	20	3c	47	55	49	20	69	64	py"> <GUI id
12.:	3d	22	67	75	69	22	3e	0a	20	20	20	20	20	20	3c	4d	="gui"> <M
13.:	45	54	52	49	43	53	20	69	64	3d	22	6d	65	74	72	69	ETRICS id="metri
14.:	63	73	22	20	58	33	3d	22	31	39	32	30	22	20	58	32	cs" X3="1920" X2
15.:	3d	22	37	22	20	58	31	3d	22	37	22	20	58	30	3d	22	="7" X1="7" X0="
16.:	32	38	33	22	20	59	33	3d	22	31	32	30	30	22	20	59	283" Y3="1200" Y
17.:	32	3d	22	32	30	22	20	59	31	3d	22	31	32	22	20	59	2="20" Y1="12" Y
18.:	30	3d	22	32	38	33	22	2f	3e	0a	20	20	20	20	3c	2f	0="283"/> </
19.:	47	55	49	3e	0a	20	20	3c	2f	43	4f	50	59	3e	0a	3c	GUI> </COPY> <
1a.:	2f	44	41	54	41	4d	41	4e	41	47	45	52	3e	0a	0c		/DATAMANAGER>

The History…

- Dennis Yurichev's work is *awesome*…
- My work is based very much on his discovery…

What we're going to talk about

- ~~Why this Talk ?~~
- ~~The history of decompressing SAP DIAG~~
- Understanding the fundamentals
- New Attacks
- Conclusion

The Fundamentals

- Understand the compression
- Understand the compressed protocol
  - Simplify the sniffing and decompression
- Recompression
- Understand the application protocol
  - What makes SAP GUI tick ?
- Identify SAP attack vectors not previously considered…

The Compression Algorithm

- Variants of Lempel-Ziv
  - LZC
  - LZH
  - SAP Supports both (tried and tested)

The Compression Algorithm

- Variant of Lempel-Ziv
  - LZC
  - LZH
  - SAP Supports both (tried and tested)
    - Makes one believe that SAP and MaxDB share same compression code-base… ☺

.Compression
.Decompression

==

.Compression
.Decompression

The Compression Algorithm

- Variant of Lempel-Ziv
  - LZC
  - LZH
  - SAP Supports both (tried and tested)
    - Makes one believe that SAP and MaxDB share same compression code-base… ☺
- Version used per message is determined by the Compression Header…
  - This is described in a minute…

The Fundamentals

- ~~Understand the compression~~
- Understand the compressed protocol
  - Simplify the sniffing and decompression
  - Recompression
- Understand the application protocol
  - What makes SAP GUI tick ?
- Identify SAP attack vectors not previously considered…

The Core, Compressed Protocol

- Easy to parse…

The Core, Compressed Protocol

- Easy to parse…

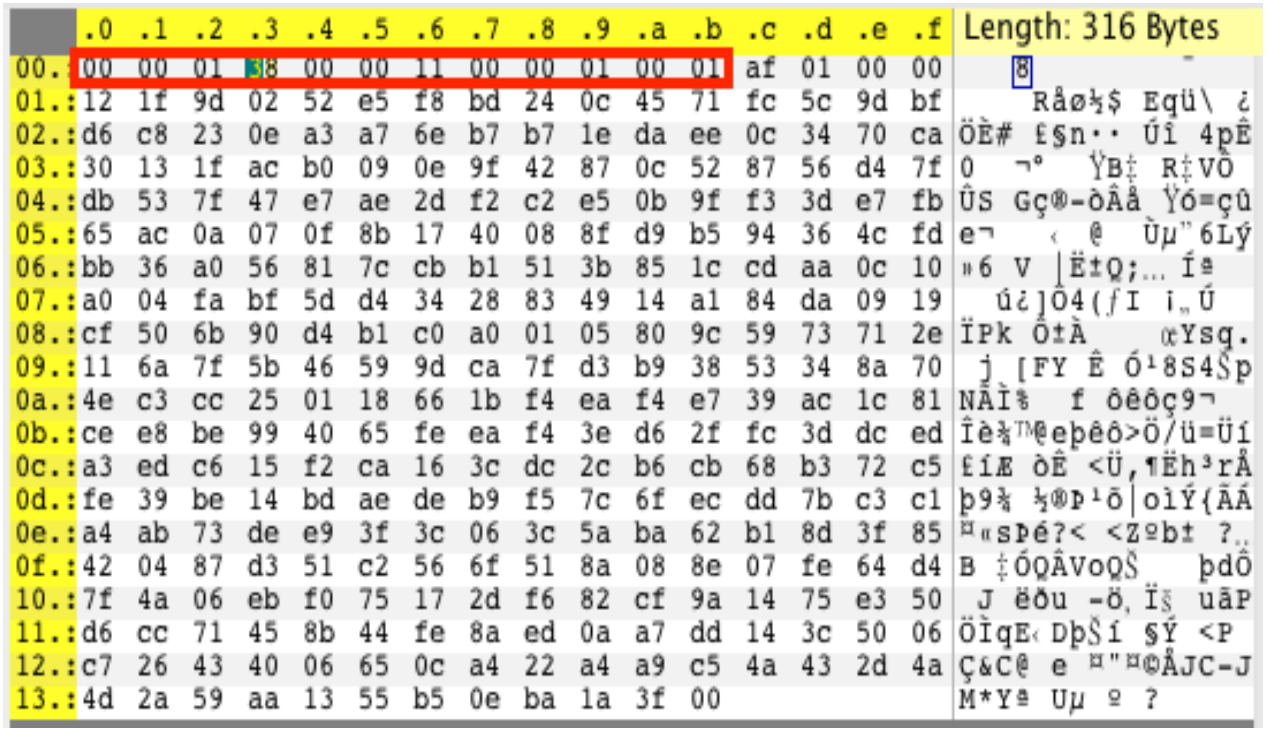
- In the absence of documentation, I've had to make my own names…

The Core, Compressed Protocol

- Easy to parse…

- In the absence of documentation, I've had to make my own names…
  - SAP Header
  - Compression Header
  - Compressed Data

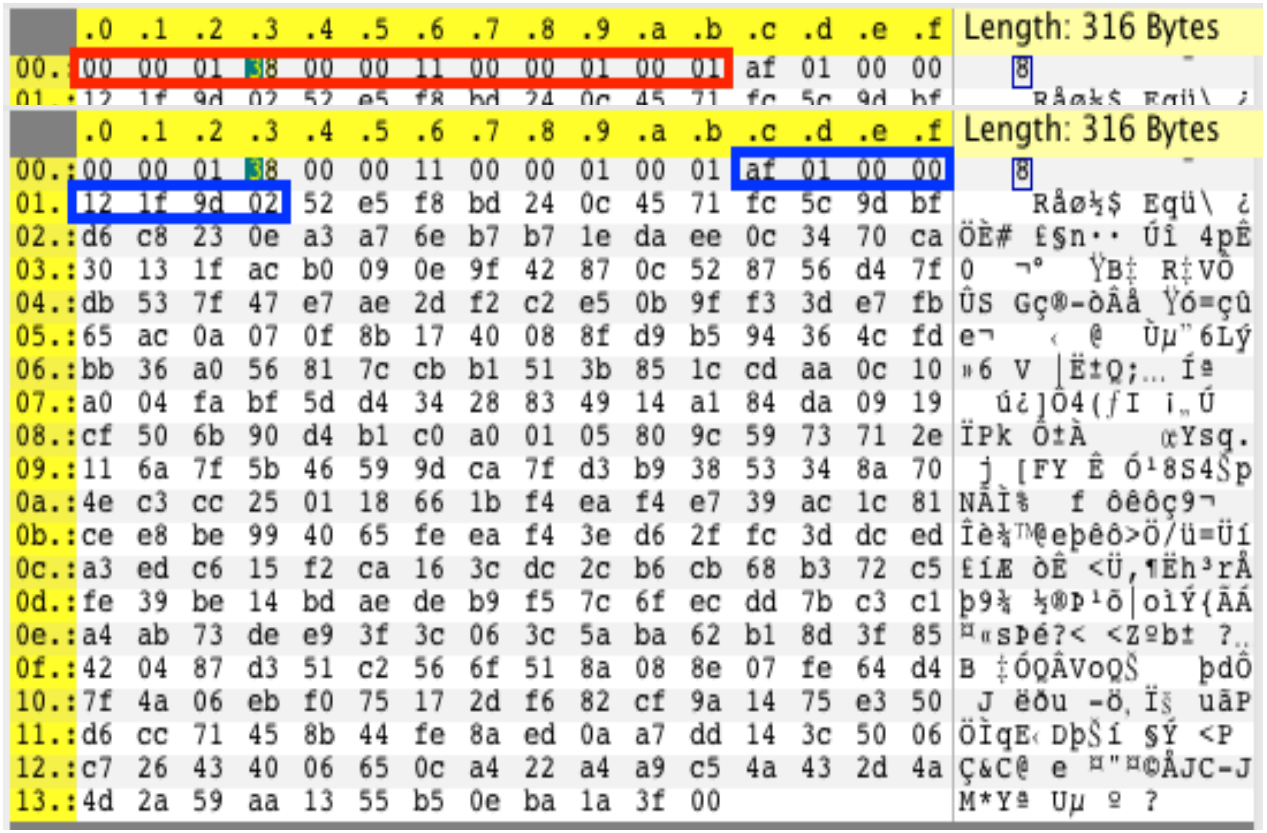
The Core, Compressed Protocol



	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £§n·· Úî 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ¬° ŸB‡ R‡VÔ
04.:	db	53	7f	47	e7	ae	2d	f2	c2	e5	0b	9f	f3	3d	e7	fb	ÛS Gç®-òÂå Ÿó=çû
05.:	65	ac	0a	07	0f	8b	17	40	08	8f	d9	b5	94	36	4c	fd	e¬ ‹ @ Ùµ"6Lý
06.:	bb	36	a0	56	81	7c	cb	b1	51	3b	85	1c	cd	aa	0c	10	»6 V |Ë±Q;… Íª
07.:	a0	04	fa	bf	5d	d4	34	28	83	49	14	a1	84	da	09	19	ú¿]Ô4(ƒI ¡„Ú
08.:	cf	50	6b	90	d4	b1	c0	a0	01	05	80	9c	59	73	71	2e	ÏPk Ô±À œYsq.
09.:	11	6a	7f	5b	46	59	9d	ca	7f	d3	b9	38	53	34	8a	70	j [FY Ê Ó¹8S4Šp
0a.:	4e	c3	cc	25	01	18	66	1b	f4	ea	f4	e7	39	ac	1c	81	NÃÌ% f ôêôç9¬
0b.:	ce	e8	be	99	40	65	fe	ea	f4	3e	d6	2f	fc	3d	dc	ed	Îè¾™@eþêô>Ö/ü=Üí
0c.:	a3	ed	c6	15	f2	ca	16	3c	dc	2c	b6	cb	68	b3	72	c5	£íÆ òÊ <Ü,¶Ëh³rÅ
0d.:	fe	39	be	14	bd	ae	de	b9	f5	7c	6f	ec	dd	7b	c3	c1	þ9¾ ½®Þ¹õ|oìÝ{ÃÁ
0e.:	a4	ab	73	de	e9	3f	3c	06	3c	5a	ba	62	b1	8d	3f	85	¤«sÞé?< <Zºb± ?…
0f.:	42	04	87	d3	51	c2	56	6f	51	8a	08	8e	07	fe	64	d4	B ‡ÓQÂVoQŠ Žþdô
10.:	7f	4a	06	eb	f0	75	17	2d	f6	82	cf	9a	14	75	e3	50	J ëðu -ö‚Ïš uãP
11.:	d6	cc	71	45	8b	44	fe	8a	ed	0a	a7	dd	14	3c	50	06	ÖÌqE‹DþŠí §Ý <P
12.:	c7	26	43	40	06	65	0c	a4	22	a4	a9	c5	4a	43	2d	4a	Ç&C@ e ¤"¤©ÅJC-J
13.:	4d	2a	59	aa	13	55	b5	0e	ba	1a	3f	00					M*Yª Uµ º ?

SAP Header

The Core, Compressed Protocol

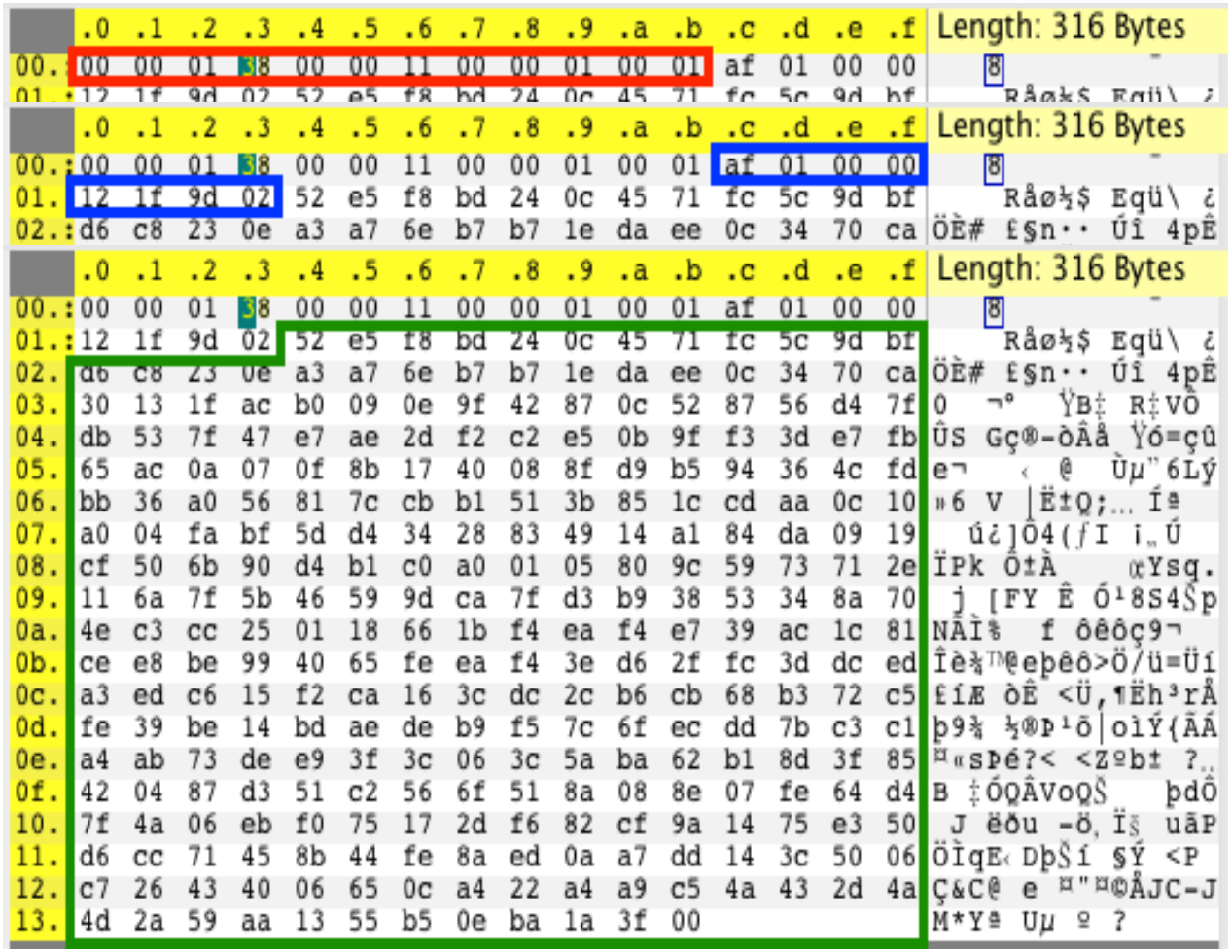


	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £§n·· ÚÎ 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ¬° ŸB‡ R‡VÔ
04.:	db	53	7f	47	e7	ae	2d	f2	c2	e5	0b	9f	f3	3d	e7	fb	ÛS Gç®-òÂå Ÿó=çû
05.:	65	ac	0a	07	0f	8b	17	40	08	8f	d9	b5	94	36	4c	fd	e¬ ‹ @ Ùµ"6Lý
06.:	bb	36	a0	56	81	7c	cb	b1	51	3b	85	1c	cd	aa	0c	10	»6 V |Ë±Q;… Íª
07.:	a0	04	fa	bf	5d	d4	34	28	83	49	14	a1	84	da	09	19	úż]Ô4(ƒI i„Ú
08.:	cf	50	6b	90	d4	b1	c0	a0	01	05	80	9c	59	73	71	2e	ÏPk Ô±À œYsq.
09.:	11	6a	7f	5b	46	59	9d	ca	7f	d3	b9	38	53	34	8a	70	j [FY Ê Ó¹8S4Šp
0a.:	4e	c3	cc	25	01	18	66	1b	f4	ea	f4	e7	39	ac	1c	81	NÃÌ% f ôêôç9¬
0b.:	ce	e8	be	99	40	65	fe	ea	f4	3e	d6	2f	fc	3d	dc	ed	Îè¾™@eþêô>Ö/ü=Üí
0c.:	a3	ed	c6	15	f2	ca	16	3c	dc	2c	b6	cb	68	b3	72	c5	£íÆ òÊ <Ü,¶Ëh³rÅ
0d.:	fe	39	be	14	bd	ae	de	b9	f5	7c	6f	ec	dd	7b	c3	c1	þ9¾ ½®Þ¹õ|oìÝ{ÃÁ
0e.:	a4	ab	73	de	e9	3f	3c	06	3c	5a	ba	62	b1	8d	3f	85	¤«sÞé?< <Zºb± ?…
0f.:	42	04	87	d3	51	c2	56	6f	51	8a	08	8e	07	fe	64	d4	B ‡ÓQÂVoQŠ Žþdô
10.:	7f	4a	06	eb	f0	75	17	2d	f6	82	cf	9a	14	75	e3	50	J ëðu -ö‚Ïš uãP
11.:	d6	cc	71	45	8b	44	fe	8a	ed	0a	a7	dd	14	3c	50	06	ÖÌqE‹ DþŠí §Ý <P
12.:	c7	26	43	40	06	65	0c	a4	22	a4	a9	c5	4a	43	2d	4a	Ç&C@ e ¤"¤©ÅJC-J
13.:	4d	2a	59	aa	13	55	b5	0e	ba	1a	3f	00					M*Yª Uµ º ?

SAP Header

Compression Header

The Core, Compressed Protocol



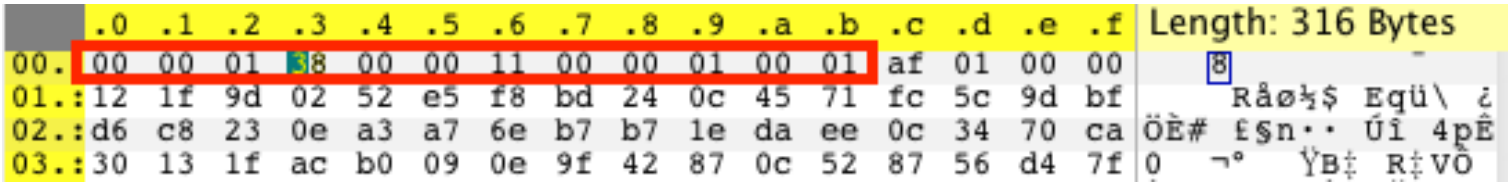
SAP Header

Compression Header

Compressed Data

The SAP Header

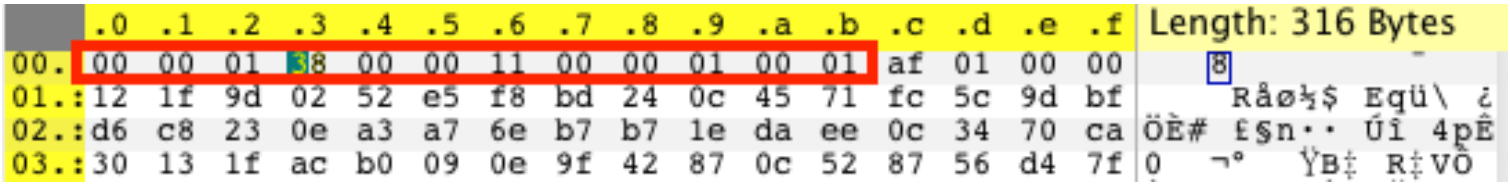
- Bytes [0] – [11]



	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £§n·· Úî 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ¬° ŸB‡ R‡VÔ

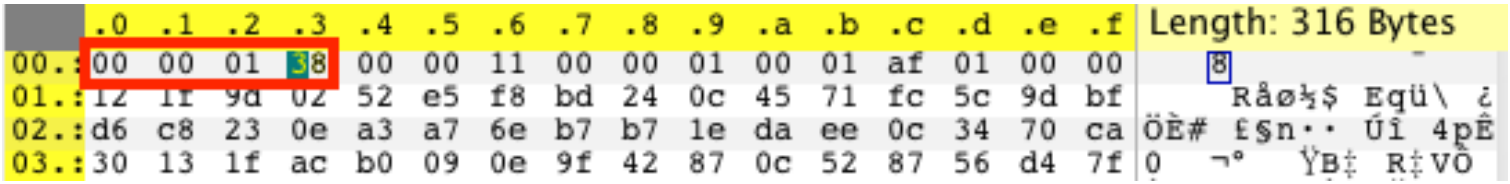
The SAP Header

- Bytes [0] – [11]



	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £§n·· Úî 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ¬° ŸB‡ R‡VÔ

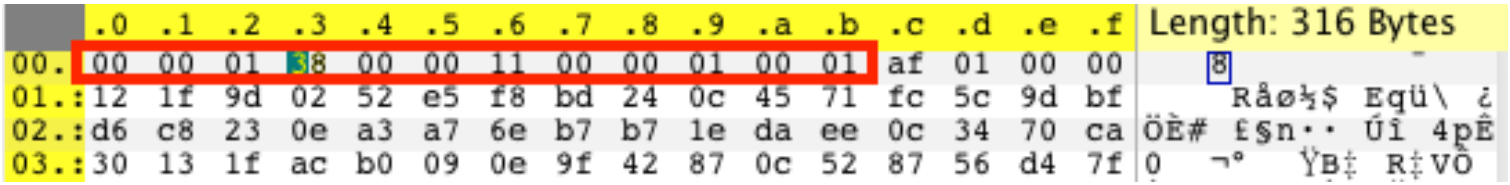
  - Bytes [0] – Bytes [3]
    - Len(Sheader) + Len(Cheader) + Len(Cdata) - 4



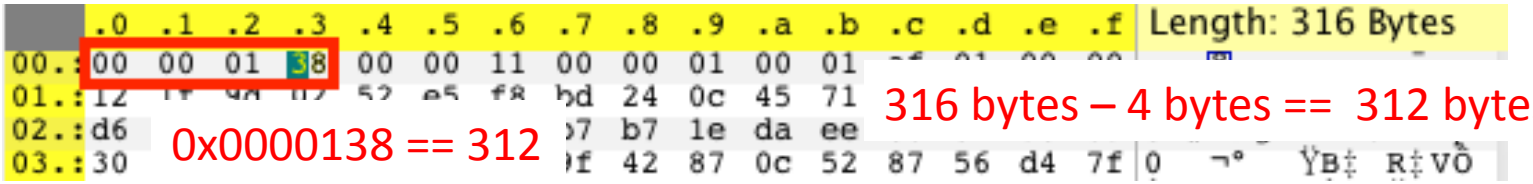
	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £§n·· Úî 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ¬° ŸB‡ R‡VÔ

The SAP Header

- Bytes [0] – [11]

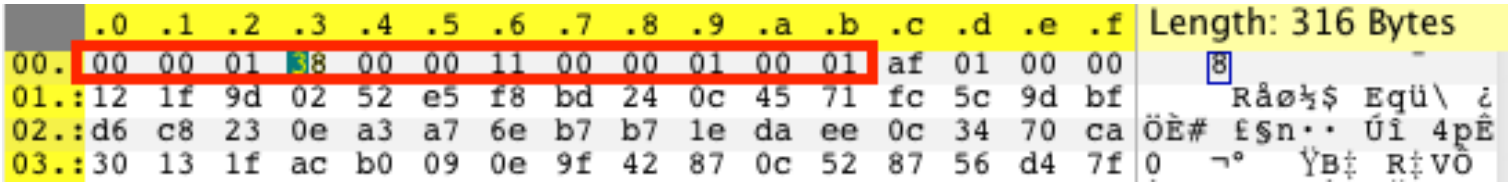


  - Bytes [0] – Bytes [3]
    - Len(Sheader) + Len(Cheader) + Len(Cdata) – 4

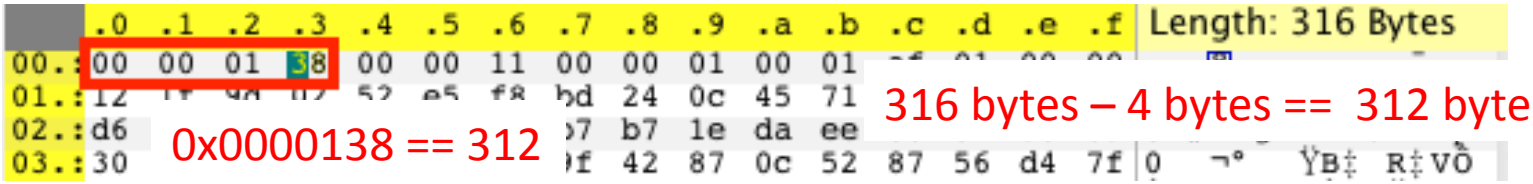


The SAP Header

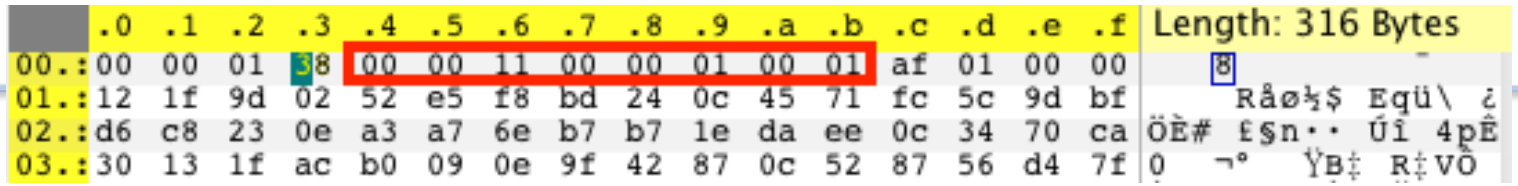
- Bytes [0] – [11]



  - Bytes [0] – Bytes [3]
    - Len(Sheader) + Len(Cheader) + Len(Cdata) – 4

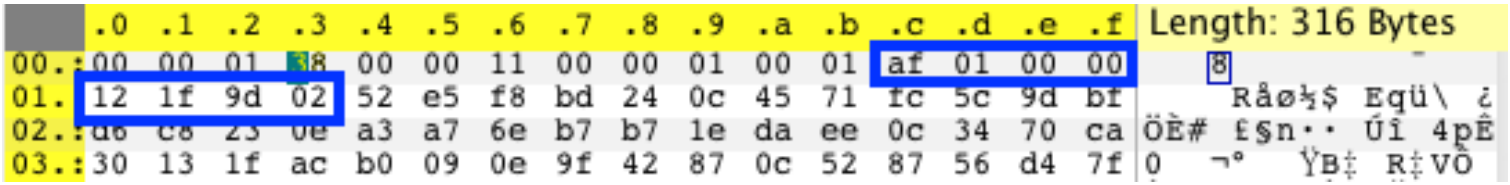


  - Bytes [4] – Bytes [11]
    - Unknown (Tampering makes *no* difference)



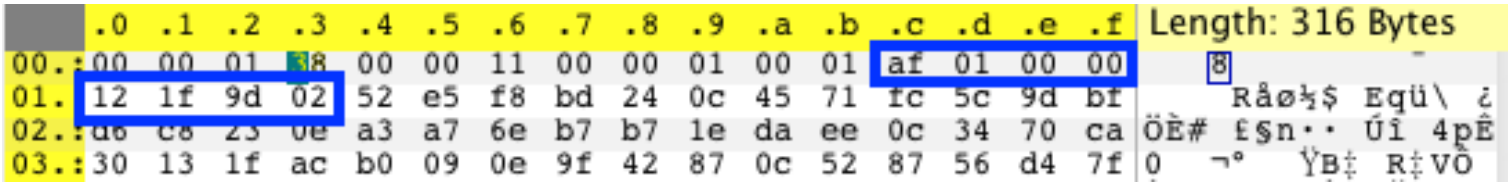
The Compression Header

- Bytes [12] – [19]

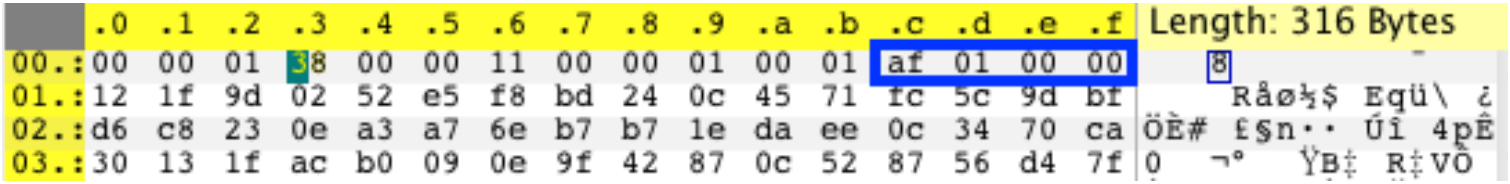


The Compression Header

- Bytes [12] – [19]

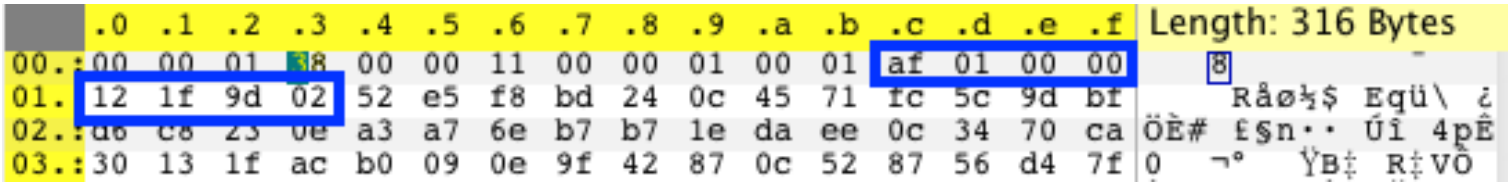


  - Bytes [12] – Bytes [15]
    - Length of decompressed stream
    - Little-Endian

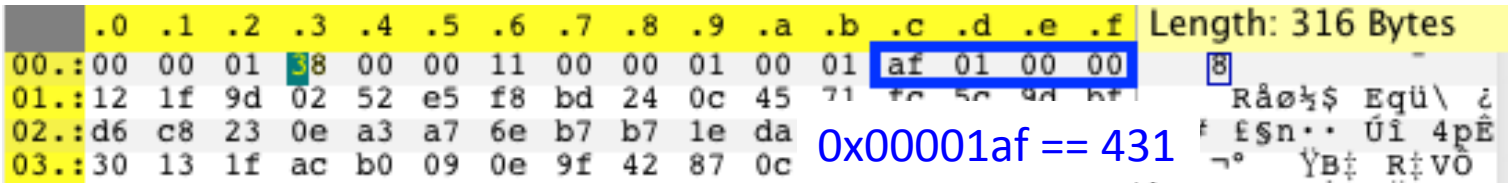


The Compression Header

- Bytes [12] – [19]

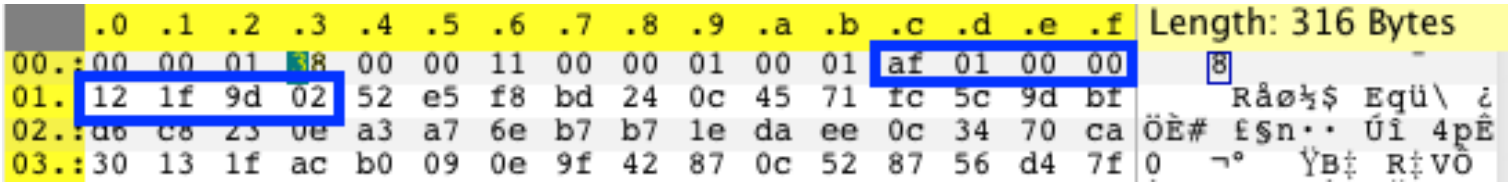


  - Bytes [12] – Bytes [15]
    - Length of decompressed stream
    - Little-Endian

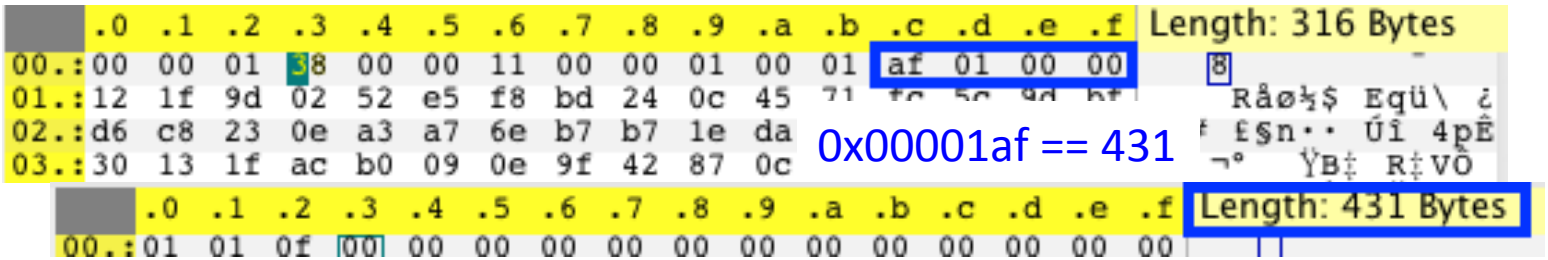


The Compression Header

- Bytes [12] – [19]

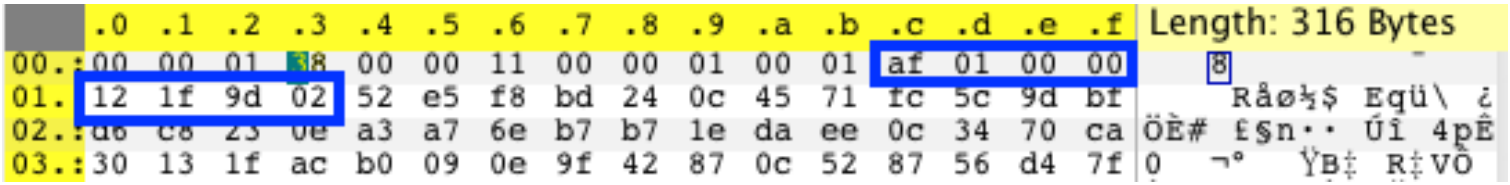


  - Bytes [12] – Bytes [15]
    - Length of decompressed stream
    - Little-Endian



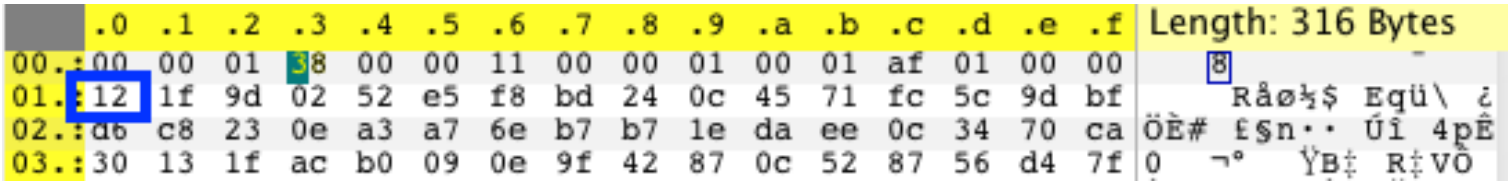
The Compression Header

- Bytes [12] – [19]



	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £§n·· Úî 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ¬° ŸB‡ R‡VÔ

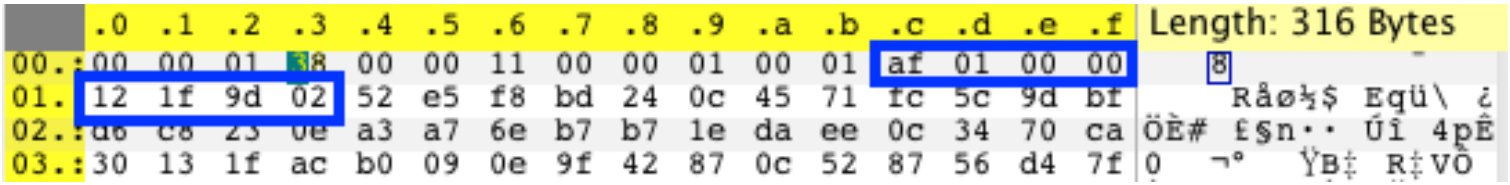
  - Bytes [16]
    - Version of compression (LZH / LZC)
    - LZC == byte & 0x0f = 0x00
    - LZH == byte & 0x0f = 0x02



	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £§n·· Úî 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ¬° ŸB‡ R‡VÔ

The Compression Header

- Bytes [12] – [19]



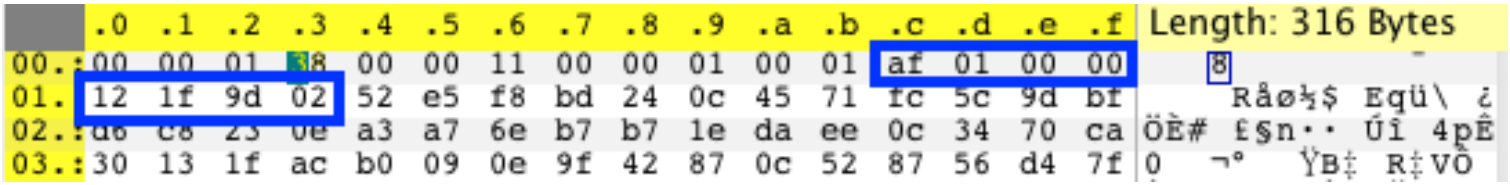
```
    .0 .1 .2 .3 .4 .5 .6 .7 .8 .9 .a .b .c .d .e .f  Length: 316 Bytes
00.:00 00 01 38 00 00 11 00 00 01 00 01 af 01 00 00      8
01. 12 1f 9d 02 52 e5 f8 bd 24 0c 45 71 fc 5c 9d bf     Råø½$ Eqü\ ¿
02.:d6 c8 23 0e a3 a7 6e b7 b7 1e da ee 0c 34 70 ca ÖÈ# £§n·· Úî 4pÊ
03.:30 13 1f ac b0 09 0e 9f 42 87 0c 52 87 56 d4 7f 0  ¬°   ŸB‡ R‡VÔ
```

  - Bytes [16]
    - Version of compression (LZH / LZC)
    - LZC == byte & 0x0f = 0x00
    - MZH == byte & 0x0f = 0x02

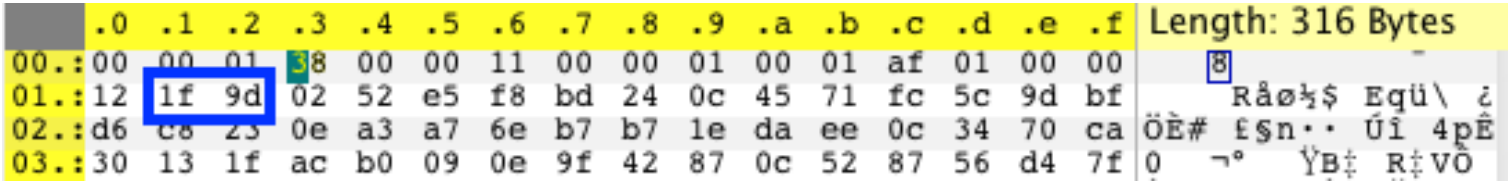
```
#define CS_LZC                          0x0     /* use lzc ....................*/
#define CS_LZH                          0x2     /* use lzh ....................*/
 int CsObjectInt::CsGetAlgorithm(SAP_BYTE * data)
 /*-------------------------------------------------------------------------*/
 /* Get Algorithm number of compressed data                                 */
 /*-------------------------------------------------------------------------*/ {
     return ((int) (data[4] & (unsigned char) 0x0F));
 }
```


The Compression Header

- Bytes [12] – [19]

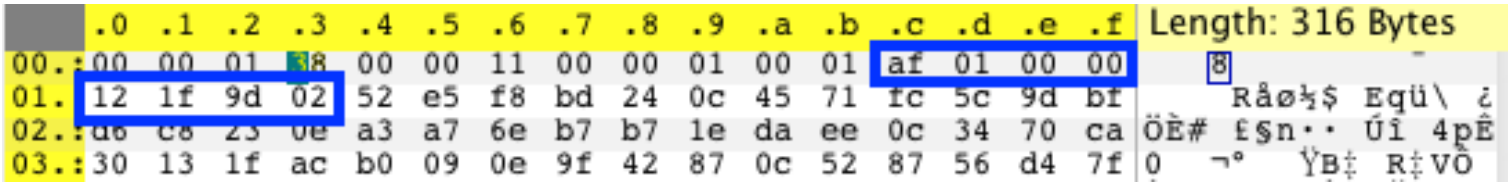


  - Bytes [17] – Bytes [18]
    - Compression Magic
    - Always 1f 9d



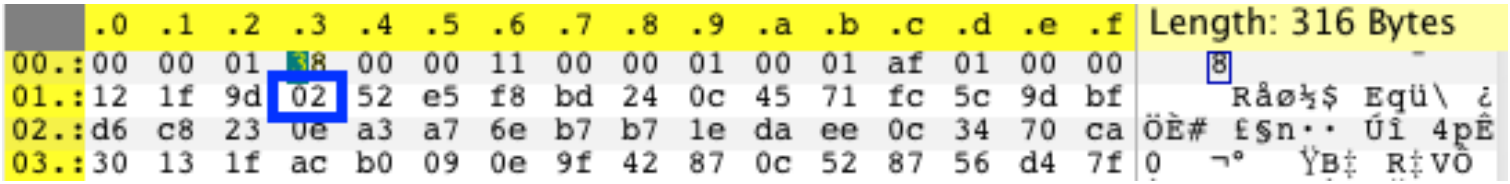
The Compression Header

- Bytes [12] – [19]



	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £§n·· ÚÎ 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ¬° ŸB‡ R‡VÔ

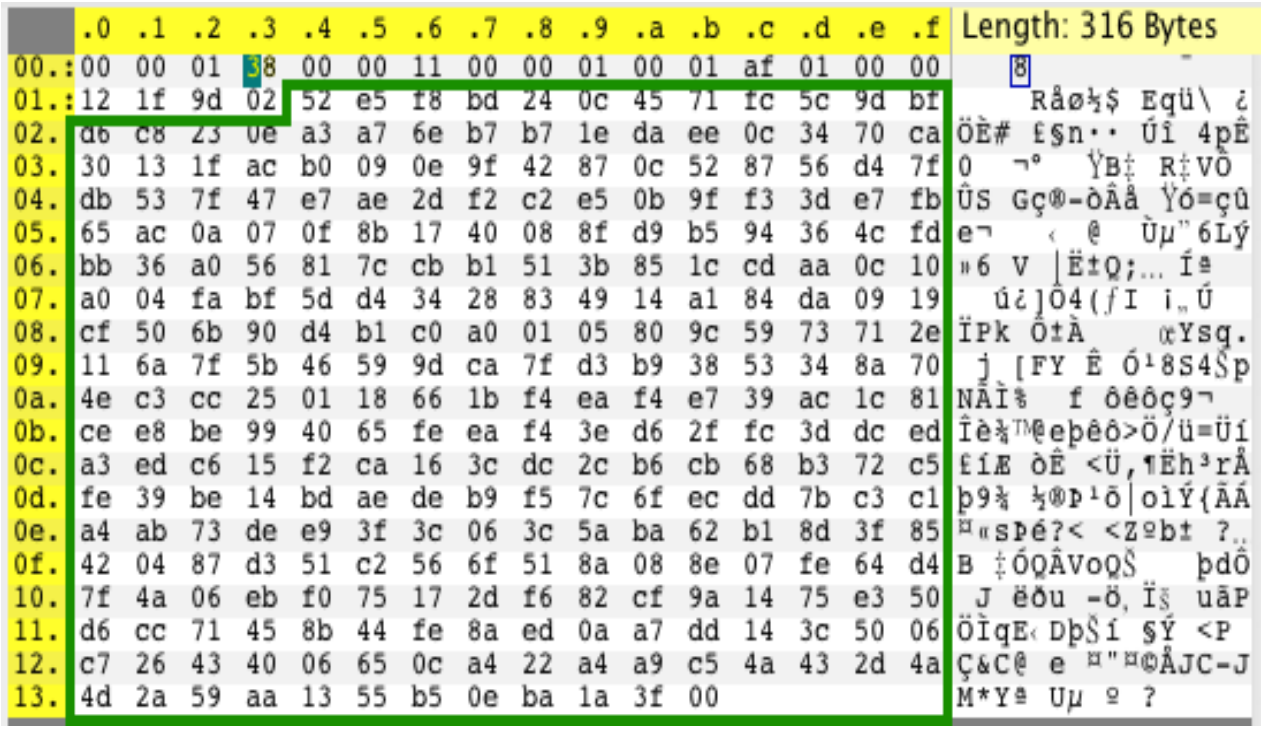
  - Bytes [19]
    - MaxBits



	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £§n·· ÚÎ 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ¬° ŸB‡ R‡VÔ

Compressed Data

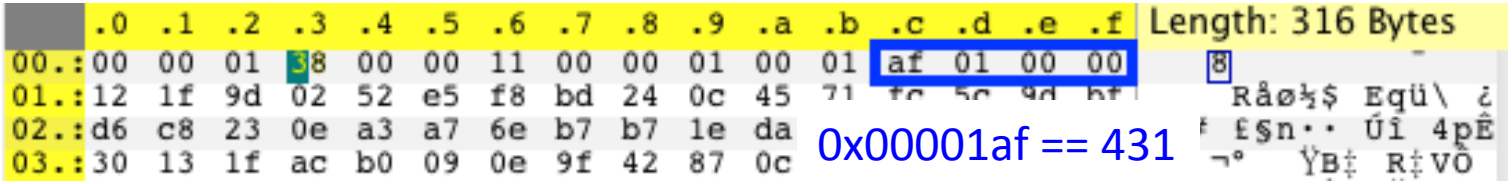
- Bytes [20] – [N]
  - The compressed stream



	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £§n·· Úî 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ¬° ŸB‡ R‡VÔ
04.	db	53	7f	47	e7	ae	2d	f2	c2	e5	0b	9f	f3	3d	e7	fb	ÛS Gç®-òÂå Ÿó=çû
05.	65	ac	0a	07	0f	8b	17	40	08	8f	d9	b5	94	36	4c	fd	e¬ ‹ @ Ùµ"6Lý
06.	bb	36	a0	56	81	7c	cb	b1	51	3b	85	1c	cd	aa	0c	10	»6 V |Ë±Q;… Íª
07.	a0	04	fa	bf	5d	d4	34	28	83	49	14	a1	84	da	09	19	úż]Ô4(ƒI i„Ú
08.	cf	50	6b	90	d4	b1	c0	a0	01	05	80	9c	59	73	71	2e	ÏPk Ô±À œYsq.
09.	11	6a	7f	5b	46	59	9d	ca	7f	d3	b9	38	53	34	8a	70	j [FY Ê Ó¹8S4Šp
0a.	4e	c3	cc	25	01	18	66	1b	f4	ea	f4	e7	39	ac	1c	81	NÃÌ% f ôêôç9¬
0b.	ce	e8	be	99	40	65	fe	ea	f4	3e	d6	2f	fc	3d	dc	ed	Îè¾™@eþêô>Ö/ü=Üí
0c.	a3	ed	c6	15	f2	ca	16	3c	dc	2c	b6	cb	68	b3	72	c5	£íÆ òÊ <Ü,¶Ëh³rÅ
0d.	fe	39	be	14	bd	ae	de	b9	f5	7c	6f	ec	dd	7b	c3	c1	þ9¾ ½®Þ¹õ|oìÝ{ÃÁ
0e.	a4	ab	73	de	e9	3f	3c	06	3c	5a	ba	62	b1	8d	3f	85	¤«sÞé?< <Zºb± ?…
0f.	42	04	87	d3	51	c2	56	6f	51	8a	08	8e	07	fe	64	d4	B ‡ÓQÂVoQŠ Žþdô
10.	7f	4a	06	eb	f0	75	17	2d	f6	82	cf	9a	14	75	e3	50	J ëðu -ö‚ Ïš uãP
11.	d6	cc	71	45	8b	44	fe	8a	ed	0a	a7	dd	14	3c	50	06	ÖÌqE‹ DþŠí §Ý <P
12.	c7	26	43	40	06	65	0c	a4	22	a4	a9	c5	4a	43	2d	4a	Ç&C@ e ¤"¤©ÅJC-J
13.	4d	2a	59	aa	13	55	b5	0e	ba	1a	3f	00					M*Yª Uµ º ?

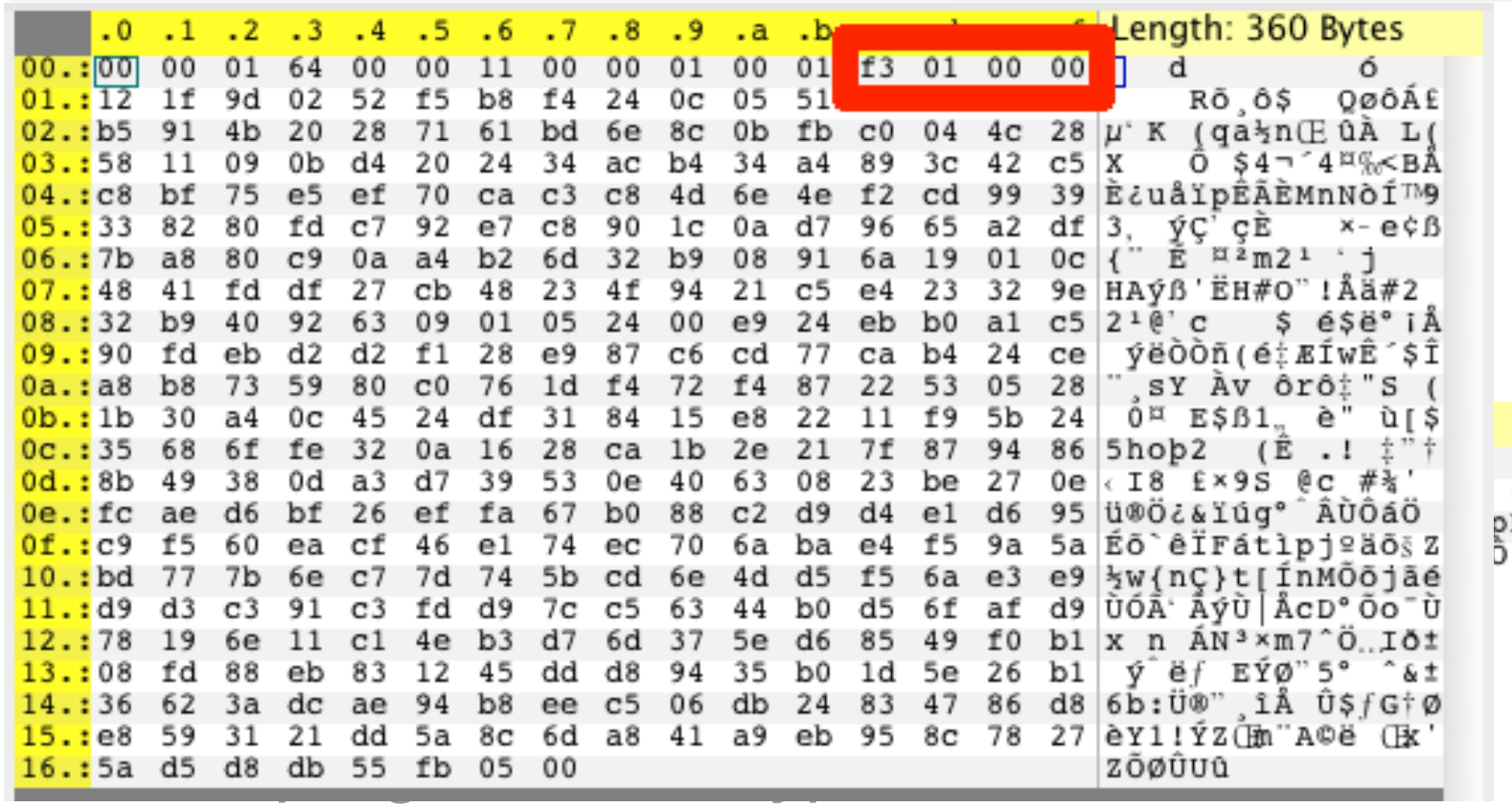
As an Aside…

- Bytes [12] – Bytes [15]
  - Length of decompressed stream
  - Little-Endian



  - Field is user-controlled, but programmatic type is SAP_INT
  - Signed integer
- What if the original length was 0xffffff ?
- (thanks Behrang Fouladi)

As an Aside…



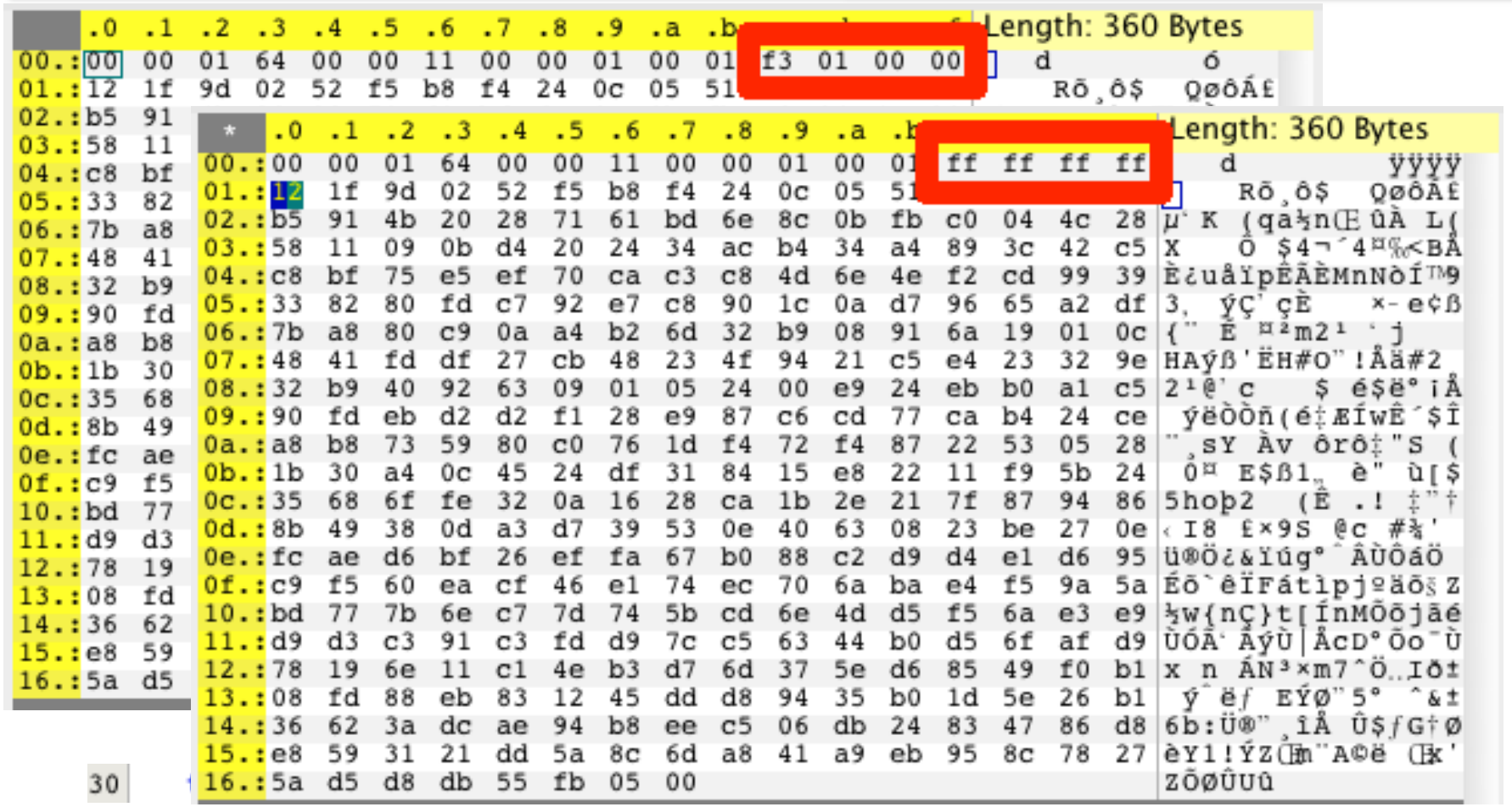
	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f
00.:	00	00	01	64	00	00	11	00	00	01	00	01	f3	01	00	00
01.:	12	1f	9d	02	52	f5	b8	f4	24	0c	05	51				
02.:	b5	91	4b	20	28	71	61	bd	6e	8c	0b	fb	c0	04	4c	28
03.:	58	11	09	0b	d4	20	24	34	ac	b4	34	a4	89	3c	42	c5
04.:	c8	bf	75	e5	ef	70	ca	c3	c8	4d	6e	4e	f2	cd	99	39
05.:	33	82	80	fd	c7	92	e7	c8	90	1c	0a	d7	96	65	a2	df
06.:	7b	a8	80	c9	0a	a4	b2	6d	32	b9	08	91	6a	19	01	0c
07.:	48	41	fd	df	27	cb	48	23	4f	94	21	c5	e4	23	32	9e
08.:	32	b9	40	92	63	09	01	05	24	00	e9	24	eb	b0	a1	c5
09.:	90	fd	eb	d2	d2	f1	28	e9	87	c6	cd	77	ca	b4	24	ce
0a.:	a8	b8	73	59	80	c0	76	1d	f4	72	f4	87	22	53	05	28
0b.:	1b	30	a4	0c	45	24	df	31	84	15	e8	22	11	f9	5b	24
0c.:	35	68	6f	fe	32	0a	16	28	ca	1b	2e	21	7f	87	94	86
0d.:	8b	49	38	0d	a3	d7	39	53	0e	40	63	08	23	be	27	0e
0e.:	fc	ae	d6	bf	26	ef	fa	67	b0	88	c2	d9	d4	e1	d6	95
0f.:	c9	f5	60	ea	cf	46	e1	74	ec	70	6a	ba	e4	f5	9a	5a
10.:	bd	77	7b	6e	c7	7d	74	5b	cd	6e	4d	d5	f5	6a	e3	e9
11.:	d9	d3	c3	91	c3	fd	d9	7c	c5	63	44	b0	d5	6f	af	d9
12.:	78	19	6e	11	c1	4e	b3	d7	6d	37	5e	d6	85	49	f0	b1
13.:	08	fd	88	eb	83	12	45	dd	d8	94	35	b0	1d	5e	26	b1
14.:	36	62	3a	dc	ae	94	b8	ee	c5	06	db	24	83	47	86	d8
15.:	e8	59	31	21	dd	5a	8c	6d	a8	41	a9	eb	95	8c	78	27
16.:	5a	d5	d8	db	55	fb	05	00								

Length: 360 Bytes

```
30    typedef int SAP_INT;                    /* Value range:          */
```

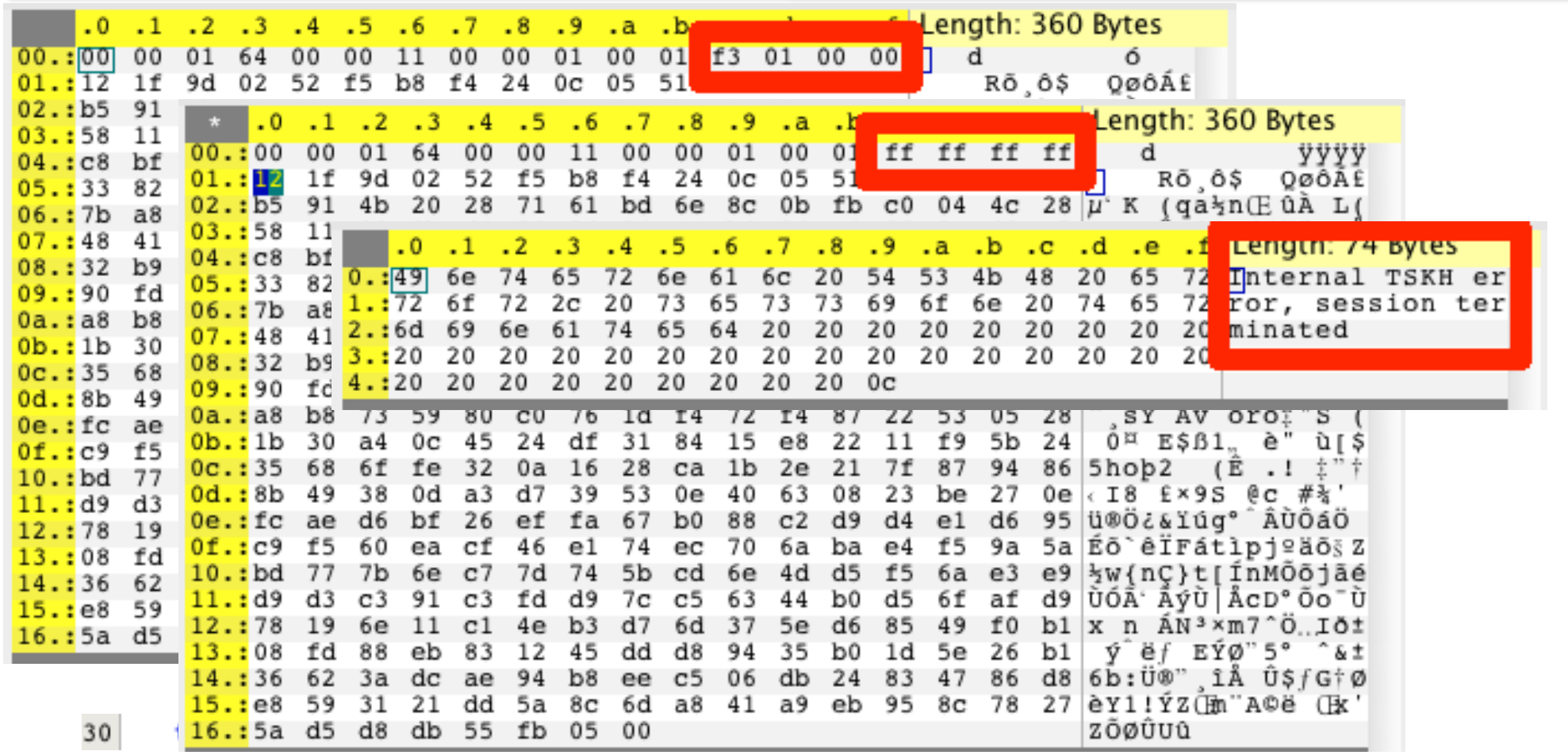
– What if the original length was 0xffffff ?

As an Aside…



– What if the original length was 0xffffff ?

As an Aside…

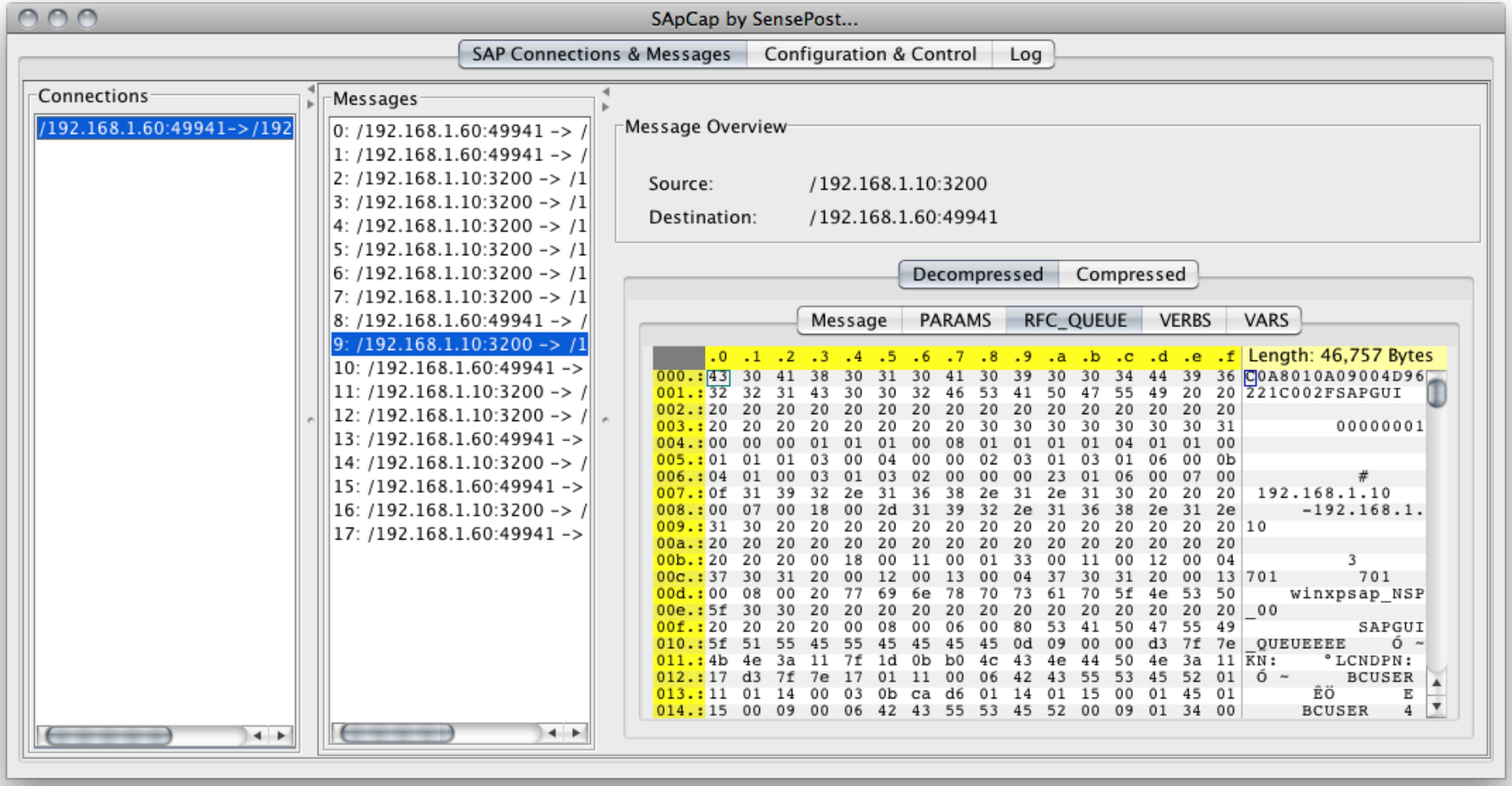


– What if the original length was 0xffffff ?

Sniffing SAP Traffic

- SAP traffic does not lend itself very well to WireShark dissectors…
- Answer was to write a custom protocol analysis tool in Java
- Used 3rd Party pCap JNI interface
  - Allows us to use standard pCap filters / dump files
- Use custom built JNI interface built from MaxDB code

SApCap


SApCap by SensePost...
SAP Connections & Messages
Configuration & Control
Log
Connections
/192.168.1.60:49941->/192
Messages
0: /192.168.1.60:49941 -> /
1: /192.168.1.60:49941 -> /
2: /192.168.1.10:3200 -> /1
3: /192.168.1.10:3200 -> /1
4: /192.168.1.10:3200 -> /1
5: /192.168.1.10:3200 -> /1
6: /192.168.1.10:3200 -> /1
7: /192.168.1.10:3200 -> /1
8: /192.168.1.60:49941 -> /
9: /192.168.1.10:3200 -> /1
10: /192.168.1.60:49941 ->
11: /192.168.1.10:3200 -> /
12: /192.168.1.10:3200 -> /
13: /192.168.1.60:49941 ->
14: /192.168.1.10:3200 -> /
15: /192.168.1.60:49941 ->
16: /192.168.1.10:3200 -> /
17: /192.168.1.60:49941 ->
Message Overview
Source: /192.168.1.10:3200
Destination: /192.168.1.60:49941
Decompressed
Compressed
Message
PARAMS
RFC_QUEUE
VERBS
VARS
Length: 46,757 Bytes

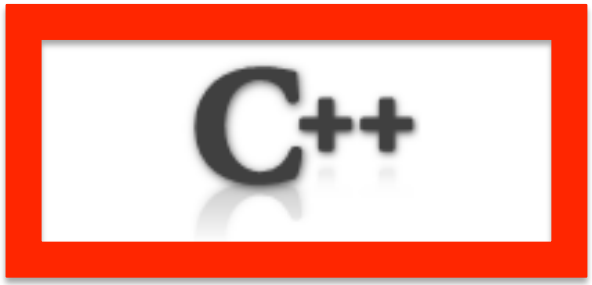
SApCap

- Jpcap
  - JNI interface for pCap
  - Responsible for reading packets
    - pCap dump files
    - Sniffing
  - Filtering packets using standard pCap filters
  - Saving information as pCap dump files

SApCap

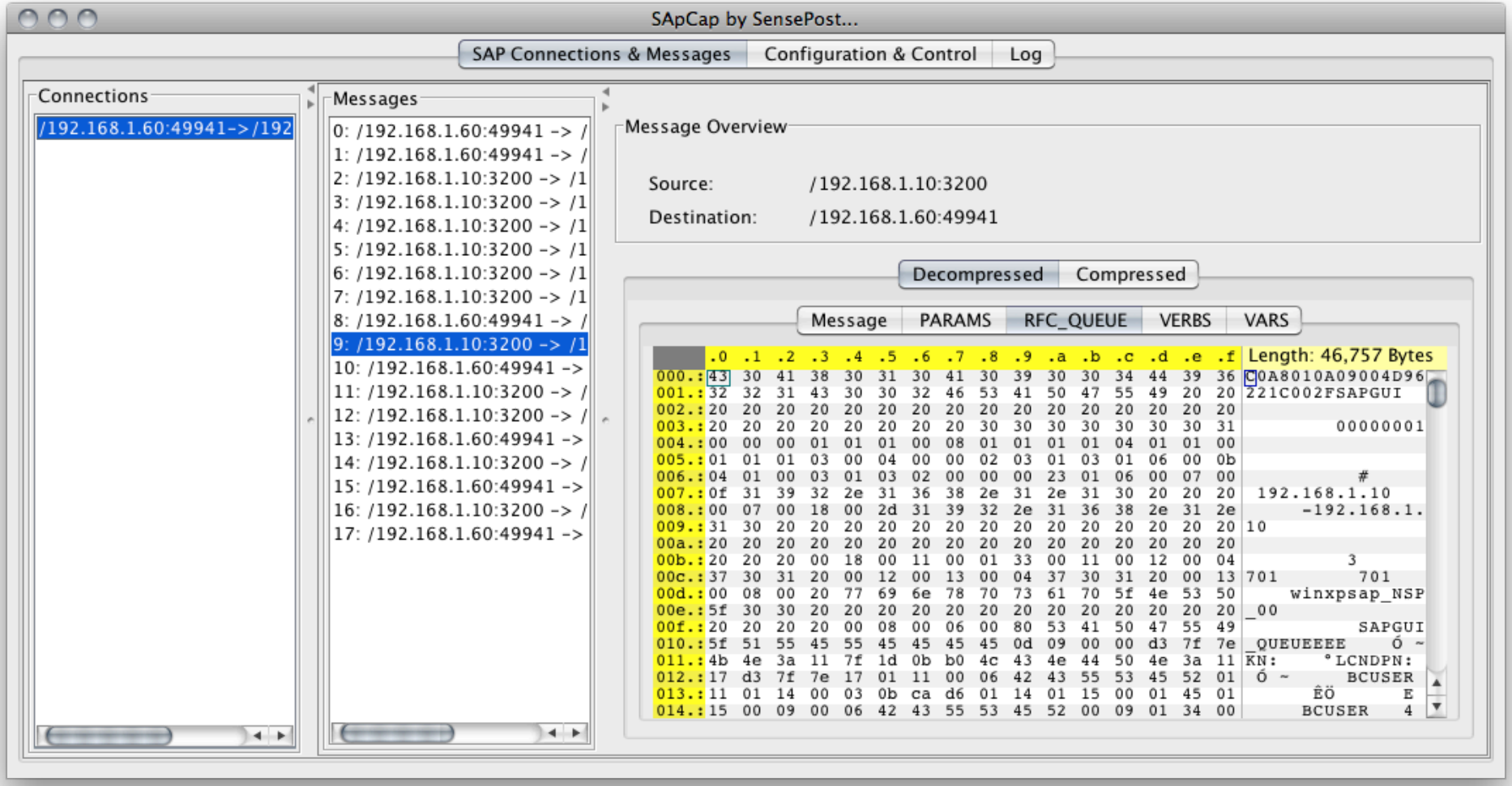
- SApCap
  - Java
  - Responsible for:
    - Parsing packet data
    - Decompressing messages
    - Queue management

SApCap



- SapCompress
  - JNI interface
  - Implements MaxDB functions for decompression
    - int[] doDecompress(int[])

Demo: SApCap


SApCap by SensePost...
SAP Connections & Messages
Configuration & Control
Log
Connections
/192.168.1.60:49941->/192
Messages
0: /192.168.1.60:49941 -> /
1: /192.168.1.60:49941 -> /
2: /192.168.1.10:3200 -> /1
3: /192.168.1.10:3200 -> /1
4: /192.168.1.10:3200 -> /1
5: /192.168.1.10:3200 -> /1
6: /192.168.1.10:3200 -> /1
7: /192.168.1.10:3200 -> /1
8: /192.168.1.60:49941 -> /
9: /192.168.1.10:3200 -> /1
10: /192.168.1.60:49941 ->
11: /192.168.1.10:3200 -> /
12: /192.168.1.10:3200 -> /
13: /192.168.1.60:49941 ->
14: /192.168.1.10:3200 -> /
15: /192.168.1.60:49941 ->
16: /192.168.1.10:3200 -> /
17: /192.168.1.60:49941 ->
Message Overview
Source: /192.168.1.10:3200
Destination: /192.168.1.60:49941
Decompressed
Compressed
Message
PARAMS
RFC_QUEUE
VERBS
VARS
Length: 46,757 Bytes

The Fundamentals

- ~~Understand the compression~~
- ~~Understand the compressed protocol~~
  - ~~Simplify the sniffing and decompression~~
- Recompression
- Understand the application protocol
  - What makes SAP GUI tick ?
- Identify SAP attack vectors not previously considered…

Recompression ?

- Core decompression functions are defined in vpa105CsObjInt.cpp
  - CsDecompr()

```
123  int CsObjectInt::CsDecompr(SAP_BYTE * inbuf, /* ptr input .......*/
124          SAP_INT inlen, /* len of input ....*/
125          SAP_BYTE * outbuf, /* ptr output ......*/
126          SAP_INT outlen, /* len output ......*/
127          SAP_INT option, /* decompr. option  */
128          SAP_INT * bytes_read, /* bytes read ......*/
129          SAP_INT * bytes_decompressed) /* bytes decompr.  */
130  /*------------------------------------------------------------------*/
131  /*     Decompress                                                   */
132  /*                                                                  */
133  /* Adaptive Dictionary Compression                                  */
134  /*   Lempel-Zip                                                     */
```

Recompression ?

- But… vpa105CsObjInt.cpp also contains function for what would appear to be compression…
  - CsCompr()

```
55
56  int CsObjectInt::CsCompr(SAP_INT sumlen,
57          SAP_BYTE * inbuf,
58          SAP_INT inlen,
59          SAP_BYTE * outbuf,
60          SAP_INT outlen,
61          SAP_INT option,
62          SAP_INT * bytes_read,
63          SAP_INT * bytes_written)
64  /*------------------------------------------------------------------*/
65  /* Compress a memory segmented                                      */
66  /*                                                                  */
67  /* Adaptive Dictionary Compression                                  */
68  /*   Lempel-Zip                                                     */
69  /*                                                                  */
```

Recompression ?

- We modify our JNI library to make use of MaxDB code
  - doCompress()
  - doDecompress()

```
1
2   #include <jni.h>
3   #include <stdio.h>
4   #include <stdlib.h>
5   #include <assert.h>
6
7   #include "SapLib.h"
8   #include "hpa101saptype.h"
9   #include "hpa104CsObject.h"
10  #include "hpa106cslzc.h"
11  #include "hpa107cslzh.h"
12  #include "hpa105CsObjInt.h"
13
14  JNIEXPORT jintArray JNICALL Java_com_sensepost_SAPProx_jni_JniInterface__1doDecompress
15  (JNIEnv * env, jobject jobj, jintArray in) {...}
82
83  JNIEXPORT jintArray JNICALL Java_com_sensepost_SAPProx_jni_JniInterface__1doCompress
84  (JNIEnv * env, jobject jbbj, jintArray in) {...}
```

Recompression ?

- We now have programmatic interface to:
  - Decompress SAP traffic
    - doDecompress()
    - Useful for interception and sniffing
  - Compress SAP traffic
    - doCompress()
    - Useful for MiTM attacks
    - Useful for assessment of SAP Gui Applications

The Fundamentals

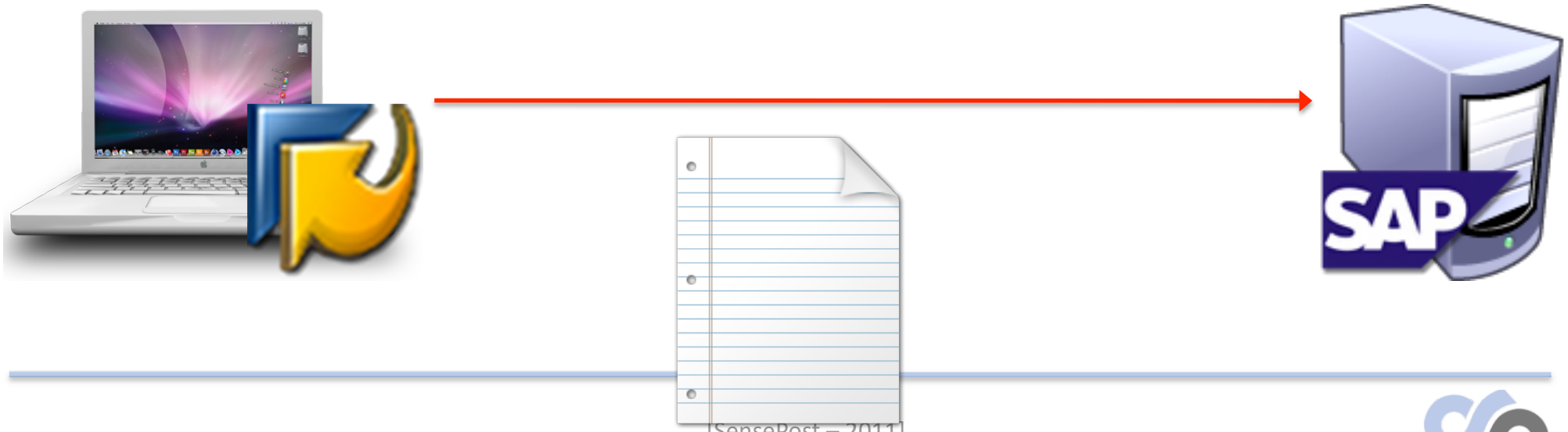
- ~~Understand the compression~~
- ~~Understand the compressed protocol~~
  - ~~Simplify the sniffing and decompression~~
- ~~Recompression~~
- Understand the application protocol
  - What makes SAP GUI tick ?
- Identify SAP attack vectors not previously considered…

The Application Protocol

- Multiplexed
  - Single connection per-user per-location per-host

The Application Protocol

- Multiplexed
  - Single connection per-user per-location per-host
- Initial hand-shake is uncompressed



[SensePost – 2011]

The Application Protocol

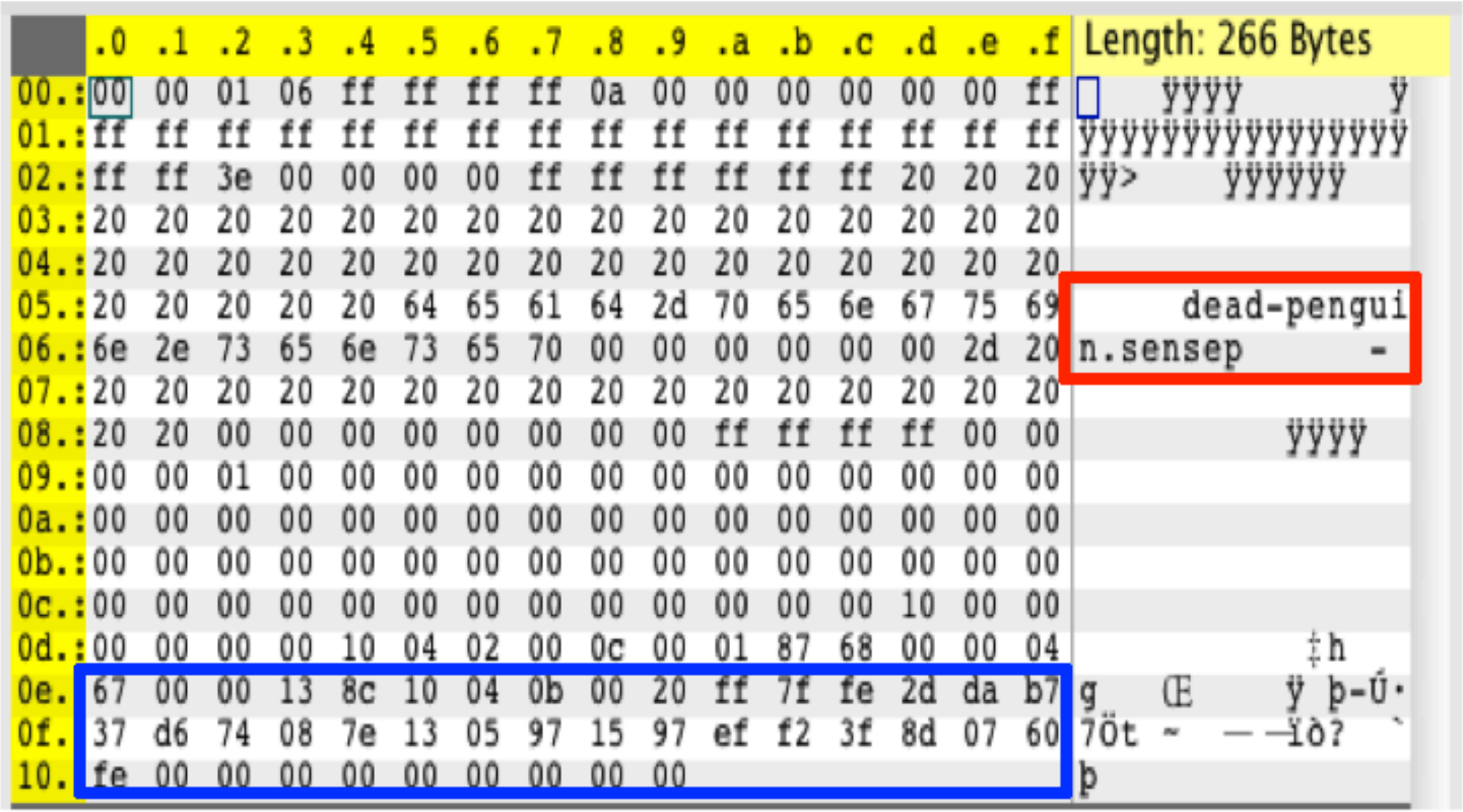
- Multiplexed
  - Single connection per-user per-location per-host
- Initial hand-shake is uncompressed
- Server response is compressed

[SensePost – 2011]

The Application Protocol

- Multiplexed
  - Single connection per-user per-location per-host
- Initial hand-shake is uncompressed
- Server response is compressed
- Uncompressed component is static
  - Terminal name
  - Options change depending on capabilities of SAP GUI (support bits)

The Application Protocol



	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 266 Bytes
00.:	00	00	01	06	ff	ff	ff	ff	0a	00	00	00	00	00	00	ff	ÿÿÿÿ ÿ
01.:	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
02.:	ff	ff	3e	00	00	00	00	ff	ff	ff	ff	ff	ff	20	20	20	ÿÿ> ÿÿÿÿÿÿ
03.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
04.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
05.:	20	20	20	20	20	64	65	61	64	2d	70	65	6e	67	75	69	dead-pengui
06.:	6e	2e	73	65	6e	73	65	70	00	00	00	00	00	00	2d	20	n.sensep -
07.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
08.:	20	20	00	00	00	00	00	00	00	00	ff	ff	ff	ff	00	00	ÿÿÿÿ
09.:	00	00	01	00	00	00	00	00	00	00	00	00	00	00	00	00	
0a.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0b.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0c.:	00	00	00	00	00	00	00	00	00	00	00	00	00	10	00	00	
0d.:	00	00	00	00	10	04	02	00	0c	00	01	87	68	00	00	04	‡h
0e.	67	00	00	13	8c	10	04	0b	00	20	ff	7f	fe	2d	da	b7	g Œ ÿ þ-Ú·
0f.	37	d6	74	08	7e	13	05	97	15	97	ef	f2	3f	8d	07	60	7Öt ~ — —ïò? `
10.	fe	00	00	00	00	00	00	00	00	00							þ

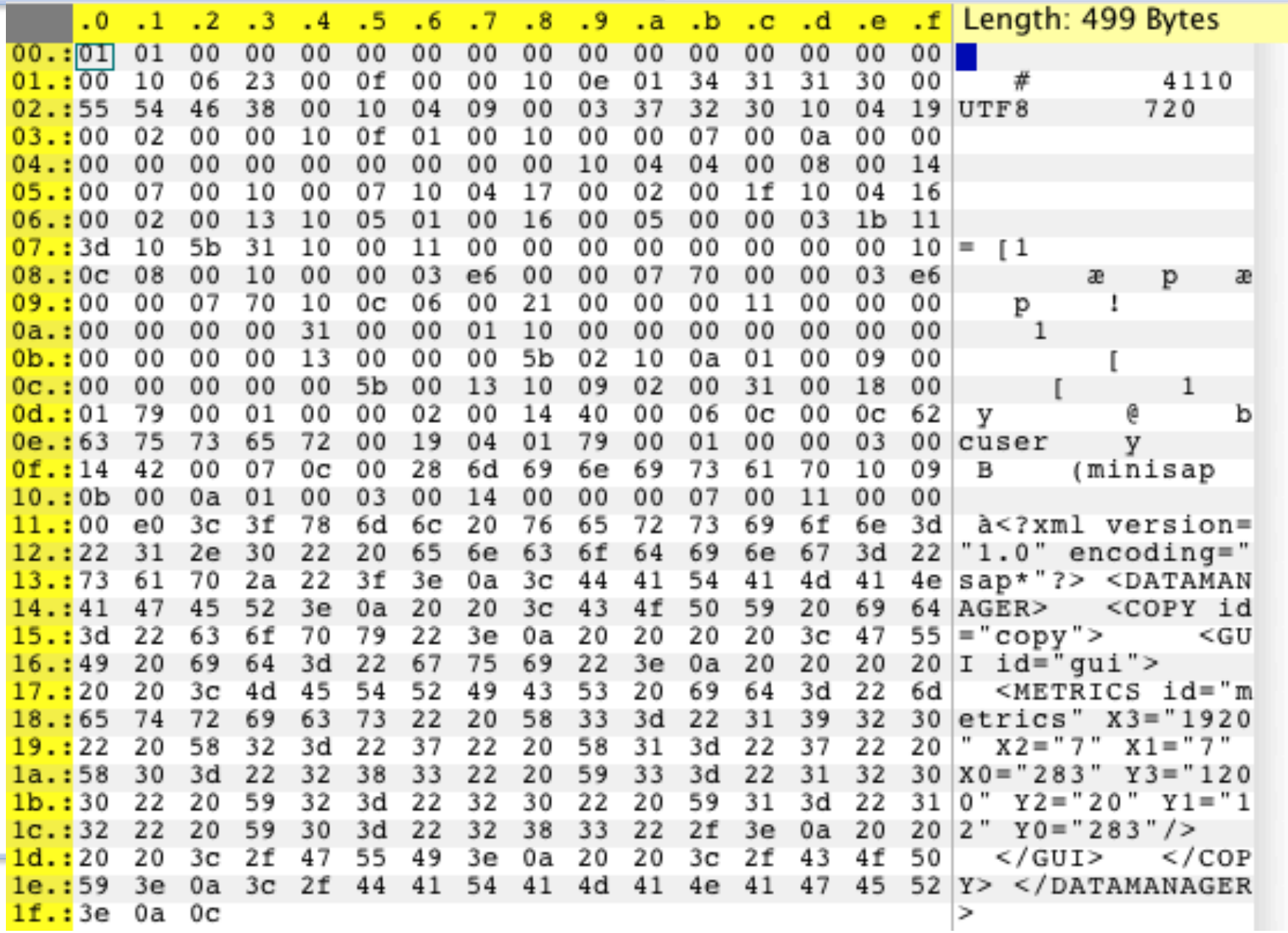
Message Types

- Two basic Types of Messages
  - Simple Messages
  - Complex Messages
- Message structures differ in terms of direction
  - GUI -> Server
  - Server -> GUI

Simple Messages : GUI -> SAP

- Header
  - "OK Code"
  - Character Encoding
  - GUI Version
- Data
  - Input values
  - XML Stream defining screen metrics

Simple Messages : GUI -> SAP



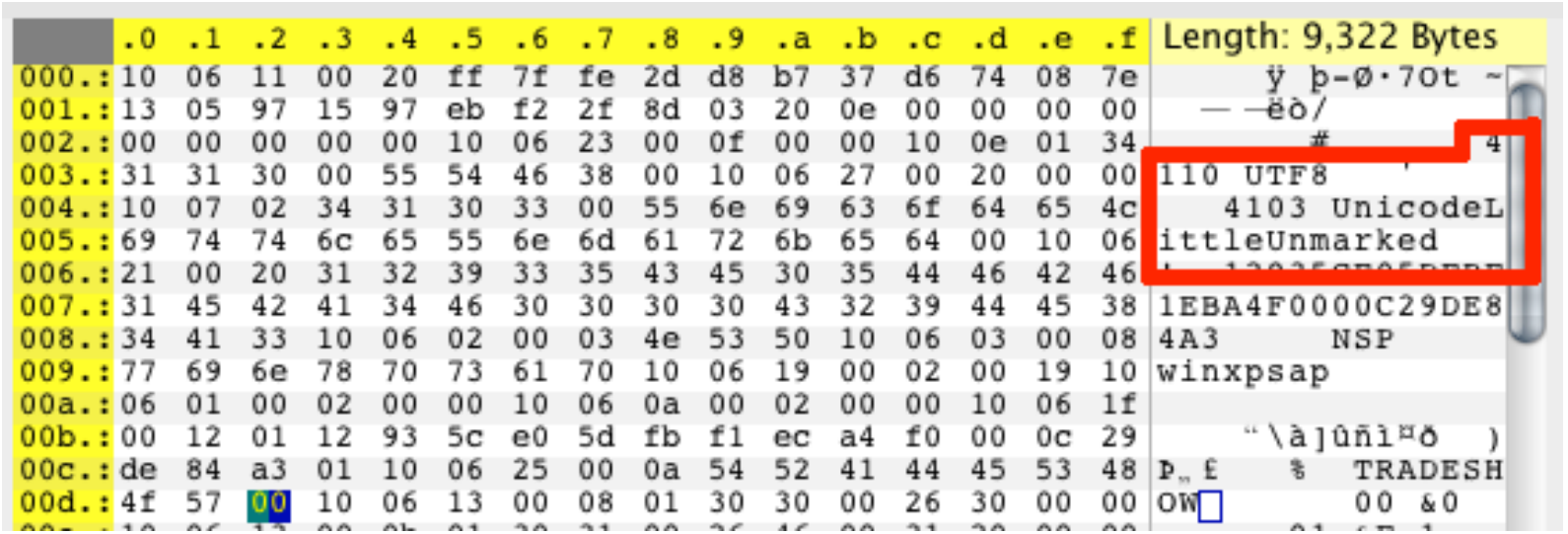
	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 499 Bytes
00.:	01	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01.:	00	10	06	23	00	0f	00	00	10	0e	01	34	31	31	30	00	# 4110
02.:	55	54	46	38	00	10	04	09	00	03	37	32	30	10	04	19	UTF8 720
03.:	00	02	00	00	10	0f	01	00	10	00	00	07	00	0a	00	00	
04.:	00	00	00	00	00	00	00	00	00	10	04	04	00	08	00	14	
05.:	00	07	00	10	00	07	10	04	17	00	02	00	1f	10	04	16	
06.:	00	02	00	13	10	05	01	00	16	00	05	00	00	03	1b	11	
07.:	3d	10	5b	31	10	00	11	00	00	00	00	00	00	00	00	10	= [1
08.:	0c	08	00	10	00	00	03	e6	00	00	07	70	00	00	03	e6	æ p æ
09.:	00	00	07	70	10	0c	06	00	21	00	00	00	11	00	00	00	p !
0a.:	00	00	00	00	31	00	00	01	10	00	00	00	00	00	00	00	1
0b.:	00	00	00	00	13	00	00	00	5b	02	10	0a	01	00	09	00	[
0c.:	00	00	00	00	00	5b	00	13	10	09	02	00	31	00	18	00	[1
0d.:	01	79	00	01	00	00	02	00	14	40	00	06	0c	00	0c	62	y @ b
0e.:	63	75	73	65	72	00	19	04	01	79	00	01	00	00	03	00	cuser y
0f.:	14	42	00	07	0c	00	28	6d	69	6e	69	73	61	70	10	09	B (minisap
10.:	0b	00	0a	01	00	03	00	14	00	00	00	07	00	11	00	00	
11.:	00	e0	3c	3f	78	6d	6c	20	76	65	72	73	69	6f	6e	3d	à<?xml version=
12.:	22	31	2e	30	22	20	65	6e	63	6f	64	69	6e	67	3d	22	"1.0" encoding="
13.:	73	61	70	2a	22	3f	3e	0a	3c	44	41	54	41	4d	41	4e	sap*"?> <DATAMAN
14.:	41	47	45	52	3e	0a	20	20	3c	43	4f	50	59	20	69	64	AGER> <COPY id
15.:	3d	22	63	6f	70	79	22	3e	0a	20	20	20	20	3c	47	55	="copy"> <GU
16.:	49	20	69	64	3d	22	67	75	69	22	3e	0a	20	20	20	20	I id="gui">
17.:	20	20	3c	4d	45	54	52	49	43	53	20	69	64	3d	22	6d	<METRICS id="m
18.:	65	74	72	69	63	73	22	20	58	33	3d	22	31	39	32	30	etrics" X3="1920
19.:	22	20	58	32	3d	22	37	22	20	58	31	3d	22	37	22	20	" X2="7" X1="7"
1a.:	58	30	3d	22	32	38	33	22	20	59	33	3d	22	31	32	30	X0="283" Y3="120
1b.:	30	22	20	59	32	3d	22	32	30	22	20	59	31	3d	22	31	0" Y2="20" Y1="1
1c.:	32	22	20	59	30	3d	22	32	38	33	22	2f	3e	0a	20	20	2" Y0="283"/>
1d.:	20	20	3c	2f	47	55	49	3e	0a	20	20	3c	2f	43	4f	50	</GUI> </COP
1e.:	59	3e	0a	3c	2f	44	41	54	41	4d	41	4e	41	47	45	52	Y> </DATAMANAGER
1f.:	3e	0a	0c														>

Simple Messages : SAP -> GUI

- Header
- Data
- “TH”

Simple Messages : SAP -> GUI

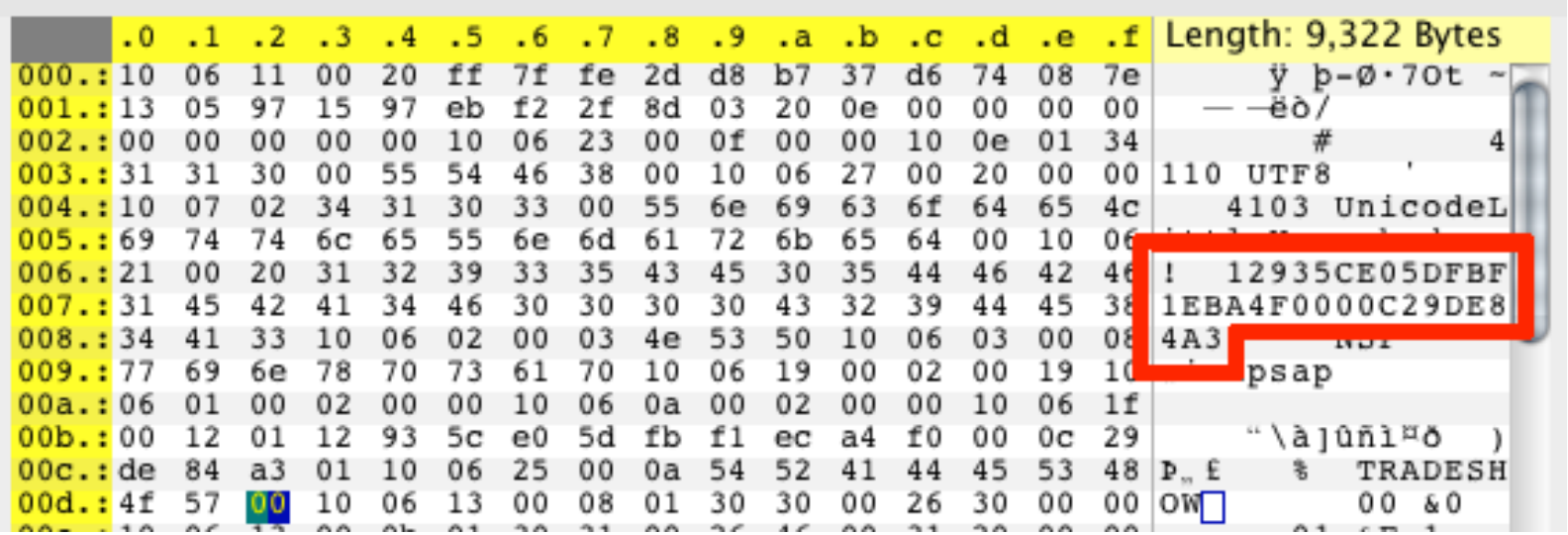
- Header
  - Encoding



	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 9,322 Bytes
000.:	10	06	11	00	20	ff	7f	fe	2d	d8	b7	37	d6	74	08	7e	ÿ þ-Ø·7Ot ~
001.:	13	05	97	15	97	eb	f2	2f	8d	03	20	0e	00	00	00	00	— —ëò/
002.:	00	00	00	00	00	10	06	23	00	0f	00	00	10	0e	01	34	# 4
003.:	31	31	30	00	55	54	46	38	00	10	06	27	00	20	00	00	110 UTF8 '
004.:	10	07	02	34	31	30	33	00	55	6e	69	63	6f	64	65	4c	4103 UnicodeL
005.:	69	74	74	6c	65	55	6e	6d	61	72	6b	65	64	00	10	06	ittleUnmarked
006.:	21	00	20	31	32	39	33	35	43	45	30	35	44	46	42	46	! 12935CE05DFBF
007.:	31	45	42	41	34	46	30	30	30	30	43	32	39	44	45	38	1EBA4F0000C29DE8
008.:	34	41	33	10	06	02	00	03	4e	53	50	10	06	03	00	08	4A3 NSP
009.:	77	69	6e	78	70	73	61	70	10	06	19	00	02	00	19	10	winxpsap
00a.:	06	01	00	02	00	00	10	06	0a	00	02	00	00	10	06	1f	
00b.:	00	12	01	12	93	5c	e0	5d	fb	f1	ec	a4	f0	00	0c	29	"\à]ûñì¤ð)
00c.:	de	84	a3	01	10	06	25	00	0a	54	52	41	44	45	53	48	Þ„£ % TRADESH
00d.:	4f	57	00	10	06	13	00	08	01	30	30	00	26	30	00	00	OW 00 &0

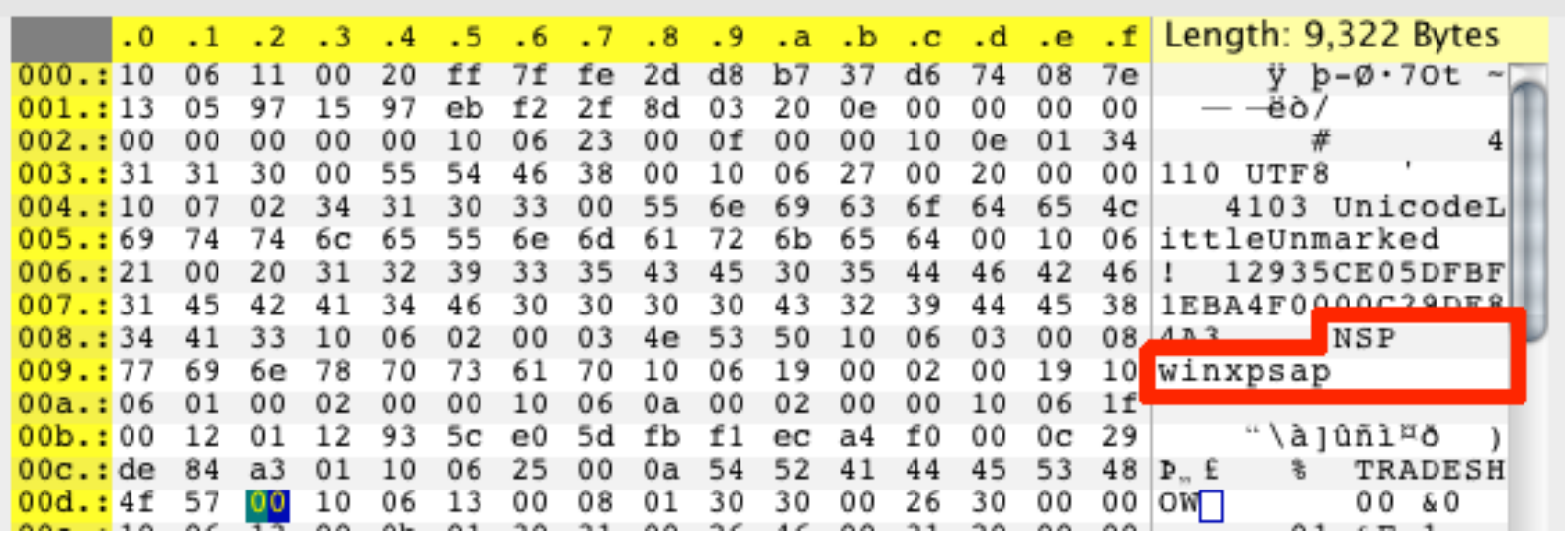
Simple Messages : SAP -> GUI

- Header
  - Encoding
  - Transaction ID



Simple Messages : SAP -> GUI

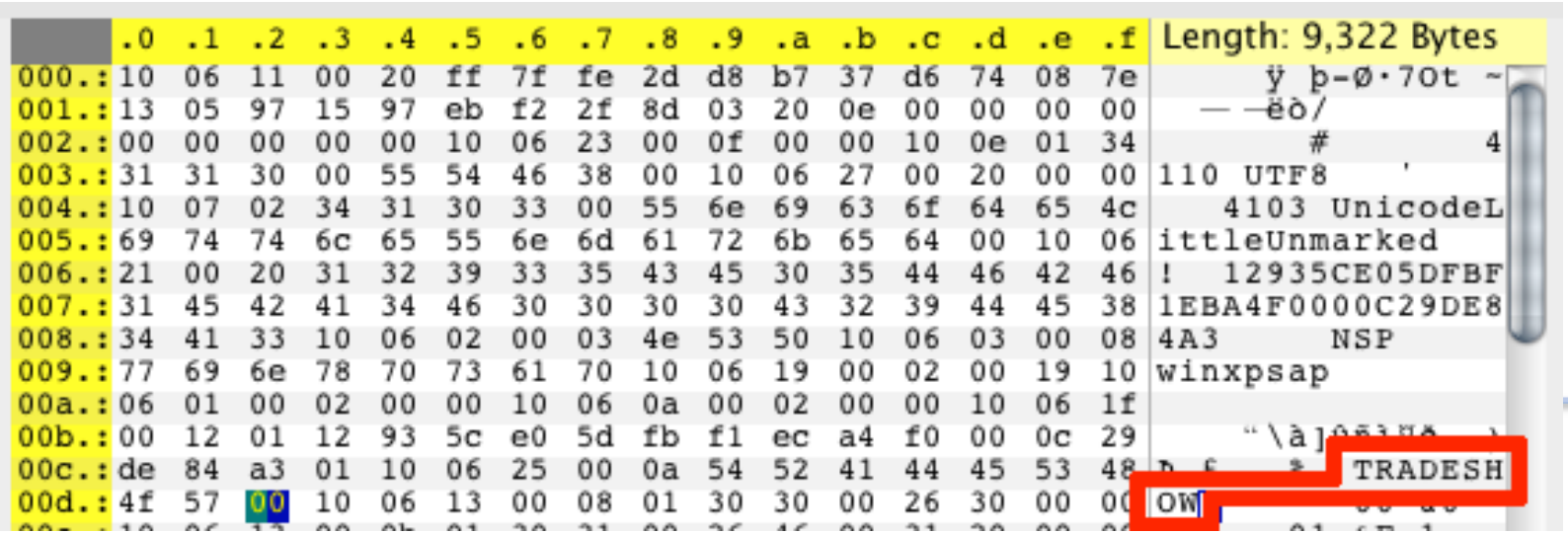
- Header
  - Encoding
  - Transaction ID
  - System & Hostname



```
      .0 .1 .2 .3 .4 .5 .6 .7 .8 .9 .a .b .c .d .e .f  Length: 9,322 Bytes
000.: 10 06 11 00 20 ff 7f fe 2d d8 b7 37 d6 74 08 7e       ÿ þ-Ø·7Ot ~
001.: 13 05 97 15 97 eb f2 2f 8d 03 20 0e 00 00 00 00    — —ëò/
002.: 00 00 00 00 00 10 06 23 00 0f 00 00 10 0e 01 34          #         4
003.: 31 31 30 00 55 54 46 38 00 10 06 27 00 20 00 00 110 UTF8    '
004.: 10 07 02 34 31 30 33 00 55 6e 69 63 6f 64 65 4c     4103 UnicodeL
005.: 69 74 74 6c 65 55 6e 6d 61 72 6b 65 64 00 10 06 ittleUnmarked
006.: 21 00 20 31 32 39 33 35 43 45 30 35 44 46 42 46 !  12935CE05DFBF
007.: 31 45 42 41 34 46 30 30 30 30 43 32 39 44 45 38 1EBA4F0000C29DE8
008.: 34 41 33 10 06 02 00 03 4e 53 50 10 06 03 00 08 4A3     NSP
009.: 77 69 6e 78 70 73 61 70 10 06 19 00 02 00 19 10 winxpsap
00a.: 06 01 00 02 00 00 10 06 0a 00 02 00 00 10 06 1f
00b.: 00 12 01 12 93 5c e0 5d fb f1 ec a4 f0 00 0c 29      "\à]ûñì¤ð   )
00c.: de 84 a3 01 10 06 25 00 0a 54 52 41 44 45 53 48 Þ„£    %  TRADESH
00d.: 4f 57 00 10 06 13 00 08 01 30 30 00 26 30 00 00 OW        00 &0
```

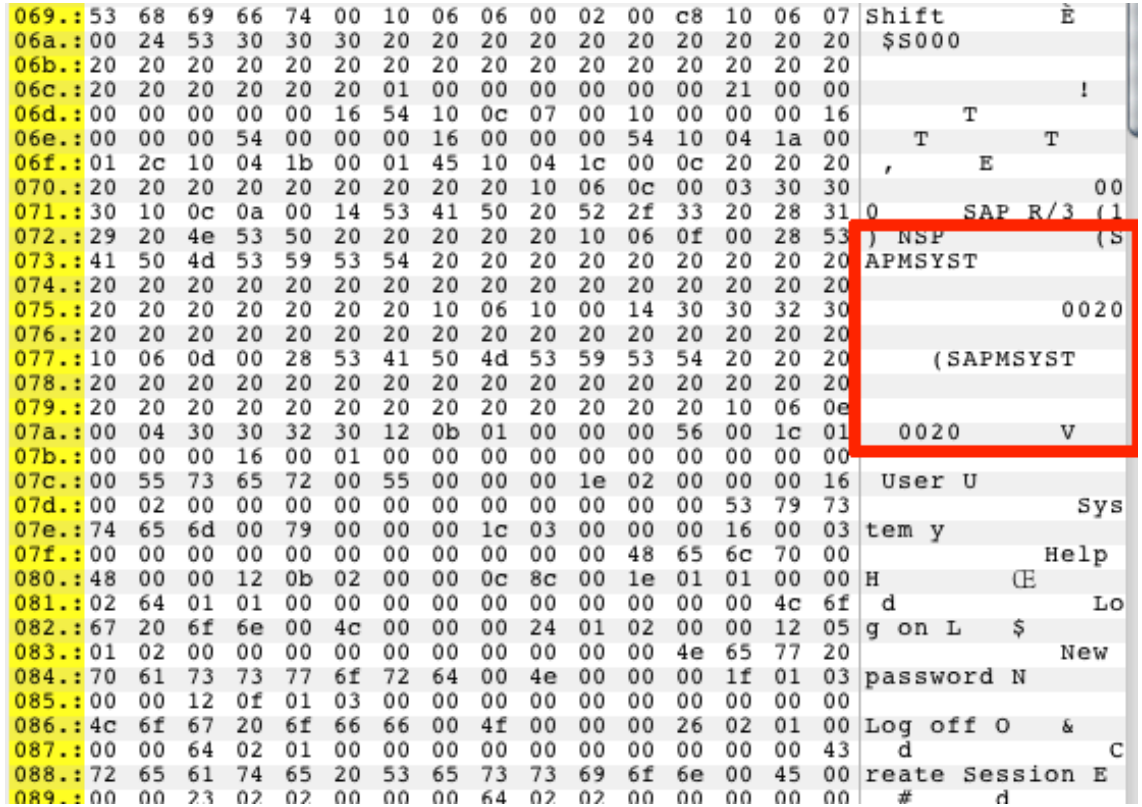
Simple Messages : SAP -> GUI

- Header
  - Encoding
  - Transaction ID
  - System Name
  - Host name
  - Theme



Simple Messages : SAP -> GUI

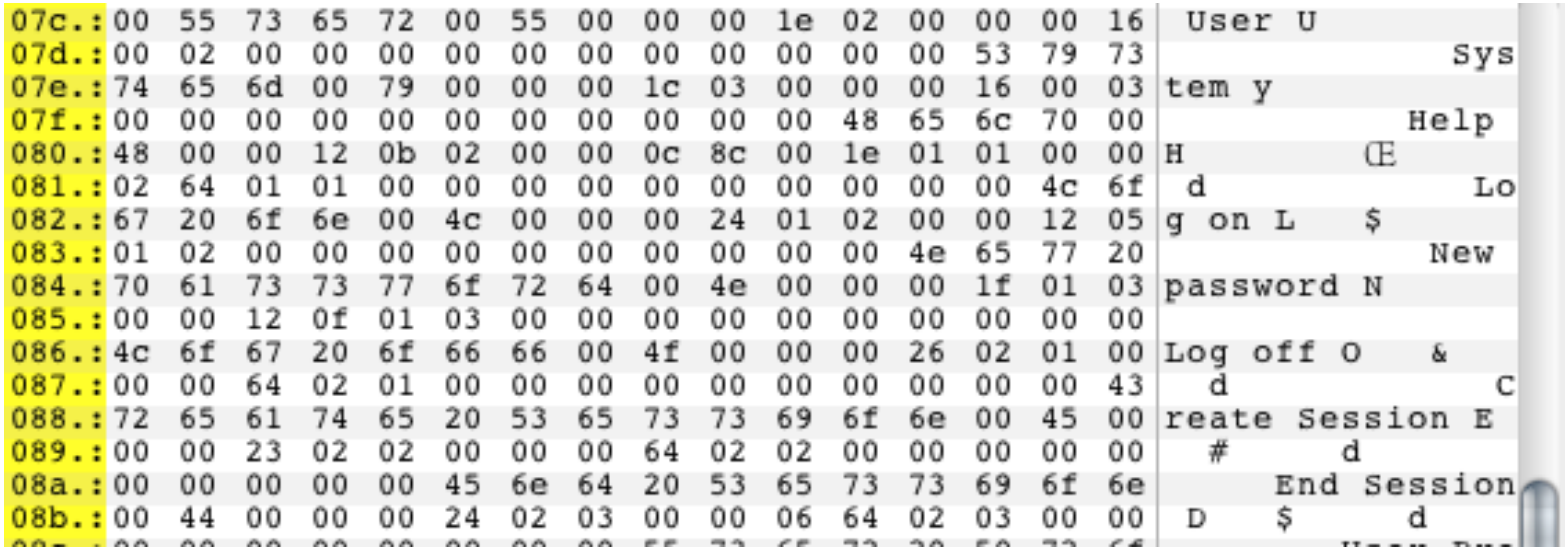
- Data
  - SAP Program Context & SAP Screen



```
069.:53 68 69 66 74 00 10 06 06 00 02 00 c8 10 06 07 Shift        È
06a.:00 24 53 30 30 30 20 20 20 20 20 20 20 20 20 20  $S000
06b.:20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
06c.:20 20 20 20 20 20 01 00 00 00 00 00 00 21 00 00                !
06d.:00 00 00 00 00 16 54 10 0c 07 00 10 00 00 00 16       T
06e.:00 00 00 54 00 00 00 16 00 00 00 54 10 04 1a 00    T        T
06f.:01 2c 10 04 1b 00 01 45 10 04 1c 00 0c 20 20 20  ,     E
070.:20 20 20 20 20 20 20 20 20 10 06 0c 00 03 30 30                 00
071.:30 10 0c 0a 00 14 53 41 50 20 52 2f 33 20 28 31 0      SAP R/3 (1
072.:29 20 4e 53 50 20 20 20 20 20 10 06 0f 00 28 53 ) NSP          (S
073.:41 50 4d 53 59 53 54 20 20 20 20 20 20 20 20 20 APMSYST
074.:20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
075.:20 20 20 20 20 20 20 10 06 10 00 14 30 30 32 30               0020
076.:20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
077.:10 06 0d 00 28 53 41 50 4d 53 59 53 54 20 20 20     (SAPMSYST
078.:20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
079.:20 20 20 20 20 20 20 20 20 20 20 20 20 10 06 0e
07a.:00 04 30 30 32 30 12 0b 01 00 00 00 56 00 1c 01   0020       V
07b.:00 00 00 16 00 01 00 00 00 00 00 00 00 00 00 00
07c.:00 55 73 65 72 00 55 00 00 00 1e 02 00 00 00 16  User U
07d.:00 02 00 00 00 00 00 00 00 00 00 00 00 53 79 73                Sys
07e.:74 65 6d 00 79 00 00 00 1c 03 00 00 00 16 00 03 tem y
07f.:00 00 00 00 00 00 00 00 00 00 00 48 65 6c 70 00                Help
080.:48 00 00 12 0b 02 00 00 0c 8c 00 1e 01 01 00 00 H         Œ
081.:02 64 01 01 00 00 00 00 00 00 00 00 00 00 4c 6f  d              Lo
082.:67 20 6f 6e 00 4c 00 00 00 24 01 02 00 00 12 05 g on L   $
083.:01 02 00 00 00 00 00 00 00 00 00 00 4e 65 77 20                New
084.:70 61 73 73 77 6f 72 64 00 4e 00 00 00 1f 01 03 password N
085.:00 00 12 0f 01 03 00 00 00 00 00 00 00 00 00 00
086.:4c 6f 67 20 6f 66 66 00 4f 00 00 00 26 02 01 00 Log off O   &
087.:00 00 64 02 01 00 00 00 00 00 00 00 00 00 00 43   d             C
088.:72 65 61 74 65 20 53 65 73 73 69 6f 6e 00 45 00 reate Session E
089.:00 00 23 02 02 00 00 00 64 02 02 00 00 00 00 00   #      d
```

Simple Messages : SAP -> GUI

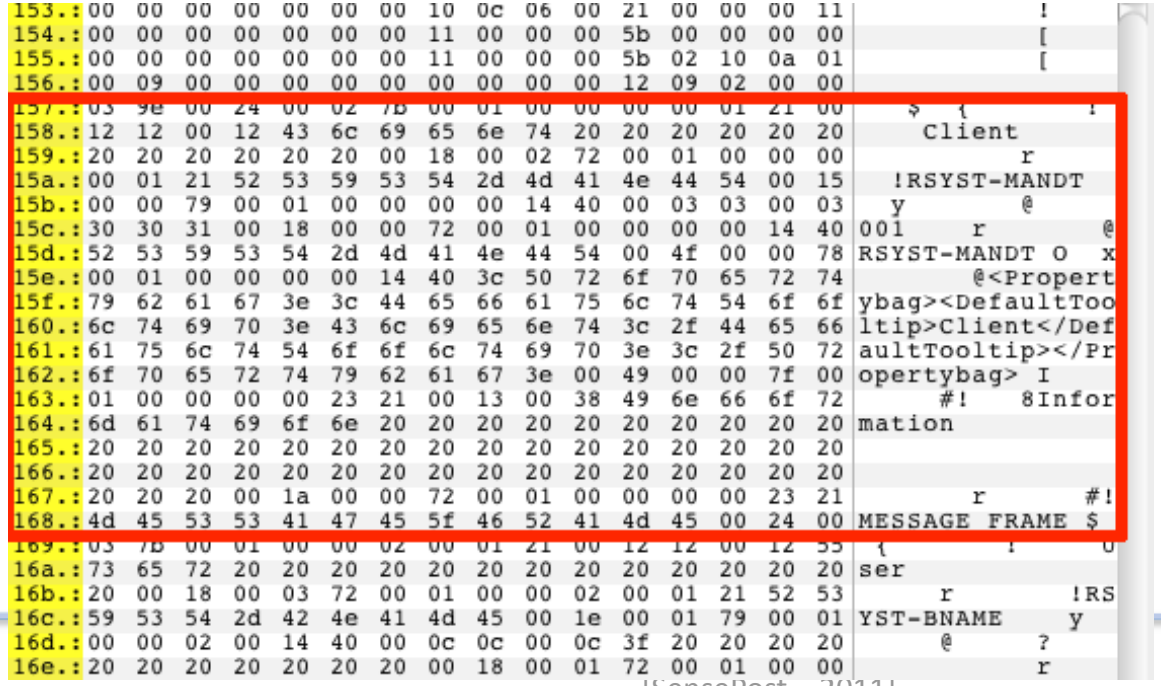
- Data
  - SAP Program Context & SAP Screen
  - Menus & Keyboard Accelerators



```
07c.:00 55 73 65 72 00 55 00 00 00 1e 02 00 00 00 16  User U
07d.:00 02 00 00 00 00 00 00 00 00 00 00 00 53 79 73                Sys
07e.:74 65 6d 00 79 00 00 00 1c 03 00 00 00 16 00 03 tem y
07f.:00 00 00 00 00 00 00 00 00 00 00 48 65 6c 70 00             Help
080.:48 00 00 12 0b 02 00 00 0c 8c 00 1e 01 01 00 00 H         Œ
081.:02 64 01 01 00 00 00 00 00 00 00 00 00 00 4c 6f  d              Lo
082.:67 20 6f 6e 00 4c 00 00 00 24 01 02 00 00 12 05 g on L   $
083.:01 02 00 00 00 00 00 00 00 00 00 00 4e 65 77 20                New
084.:70 61 73 73 77 6f 72 64 00 4e 00 00 00 1f 01 03 password N
085.:00 00 12 0f 01 03 00 00 00 00 00 00 00 00 00 00
086.:4c 6f 67 20 6f 66 66 00 4f 00 00 00 26 02 01 00 Log off O   &
087.:00 00 64 02 01 00 00 00 00 00 00 00 00 00 00 43   d             C
088.:72 65 61 74 65 20 53 65 73 73 69 6f 6e 00 45 00 reate Session E
089.:00 00 23 02 02 00 00 00 64 02 02 00 00 00 00 00   #     d
08a.:00 00 00 00 00 45 6e 64 20 53 65 73 73 69 6f 6e      End Session
08b.:00 44 00 00 00 24 02 03 00 00 06 64 02 03 00 00  D   $     d
```

Simple Messages : SAP -> GUI

- Data
  - SAP Program Context & SAP Screen
  - Menus & Keyboard Accelerators
  - Input dialogs



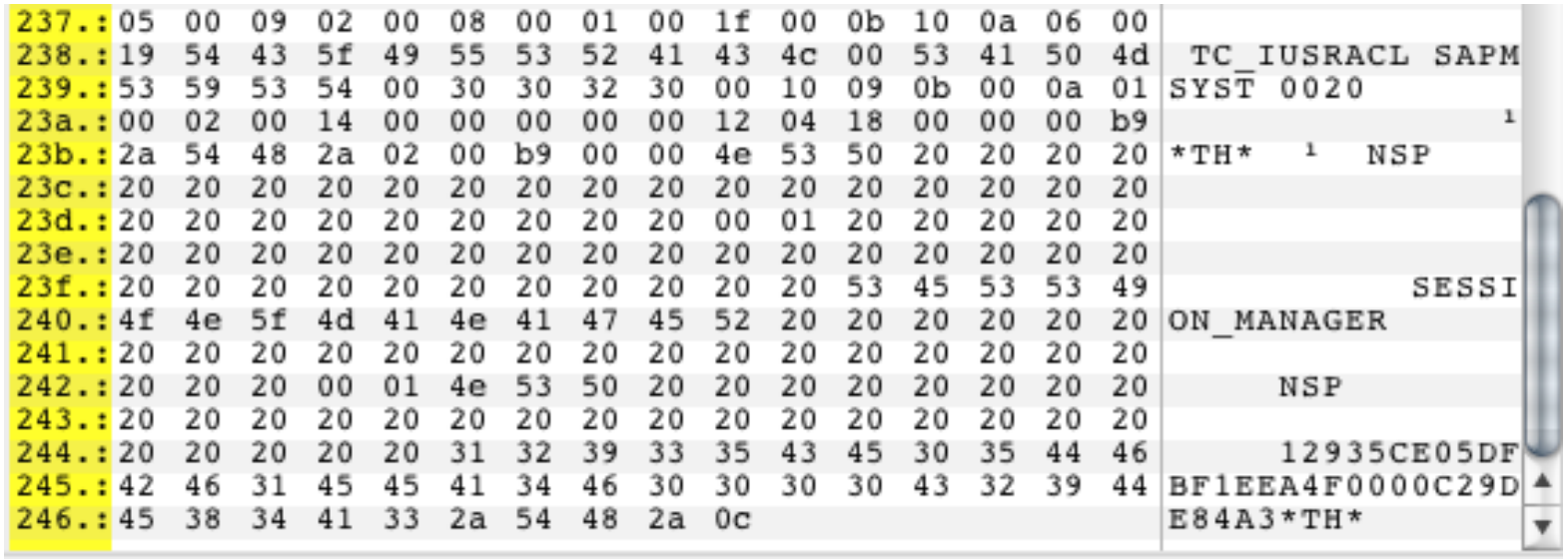
Simple Messages : SAP -> GUI

- Data
  - SAP Program Context & SAP Screen
  - Menus & Keyboard Accelerators
  - Input dialogs
  - Screen Data

```
1cf.: 04 00 7a 01 07 00 00 06 00 00 21 00 84 36 00 84   z        ! „6 „
1d0.: 54 68 72 65 65 20 63 6c 69 65 6e 74 73 3a 20 30 Three clients: 0
1d1.: 30 30 2c 20 30 30 31 20 61 6e 64 20 30 36 36 2e 00, 001 and 066.
1d2.: 20 20 46 6f 72 20 61 6c 6c 20 70 75 72 70 6f 73   For all purpos
1d3.: 65 73 2c 20 30 30 31 20 73 68 6f 75 6c 64 20 62 es, 001 should b
1d4.: 65 20 75 73 65 64 2e 20 20 20 20 20 20 20 20 20 e used.
1d5.: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
1d6.: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
```

Simple Messages : SAP -> GUI

- "TH"
  - System Name
  - Transaction
  - Transaction ID



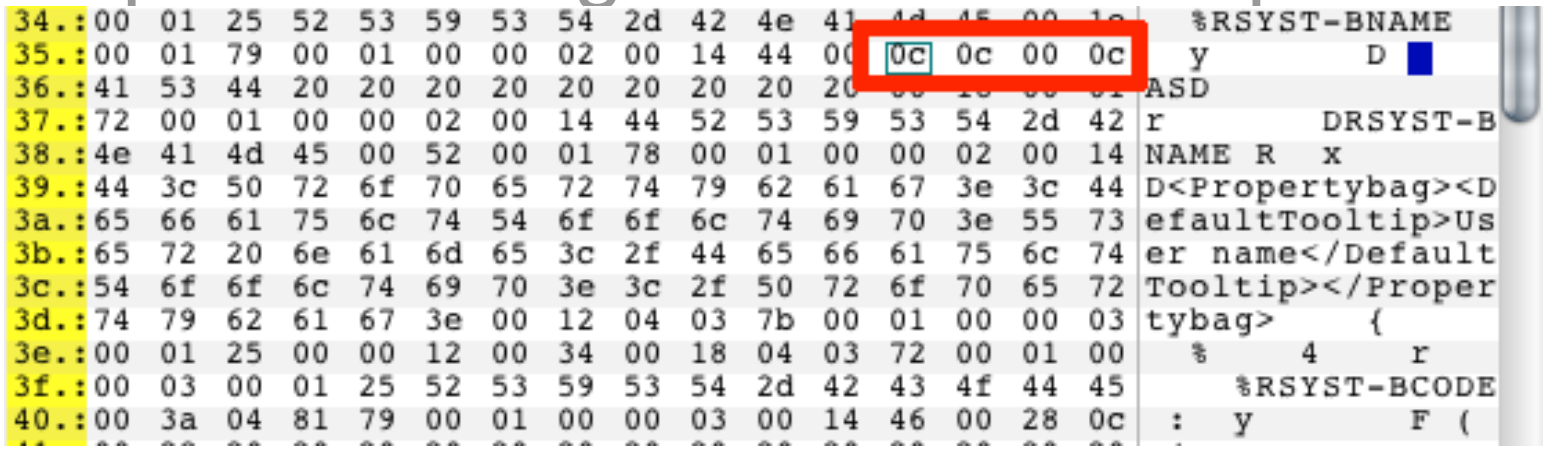
```
237.:05 00 09 02 00 08 00 01 00 1f 00 0b 10 0a 06 00
238.:19 54 43 5f 49 55 53 52 41 43 4c 00 53 41 50 4d  TC_IUSRACL SAPM
239.:53 59 53 54 00 30 30 32 30 00 10 09 0b 00 0a 01 SYST 0020
23a.:00 02 00 14 00 00 00 00 00 12 04 18 00 00 00 b9                 ¹
23b.:2a 54 48 2a 02 00 b9 00 00 4e 53 50 20 20 20 20 *TH*  ¹  NSP
23c.:20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
23d.:20 20 20 20 20 20 20 20 20 00 01 20 20 20 20 20
23e.:20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
23f.:20 20 20 20 20 20 20 20 20 20 20 53 45 53 53 49             SESSI
240.:4f 4e 5f 4d 41 4e 41 47 45 52 20 20 20 20 20 20 ON_MANAGER
241.:20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
242.:20 20 20 00 01 4e 53 50 20 20 20 20 20 20 20 20      NSP
243.:20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
244.:20 20 20 20 20 31 32 39 33 35 43 45 30 35 44 46      12935CE05DF
245.:42 46 31 45 45 41 34 46 30 30 30 30 43 32 39 44 BF1EEA4F0000C29D
246.:45 38 34 41 33 2a 54 48 2a 0c                    E84A3*TH*
```

Dialogs

- All input fields accept strings
  - No client-side validation
  - Data is validated on the server
- Input field lengths can be manipulated

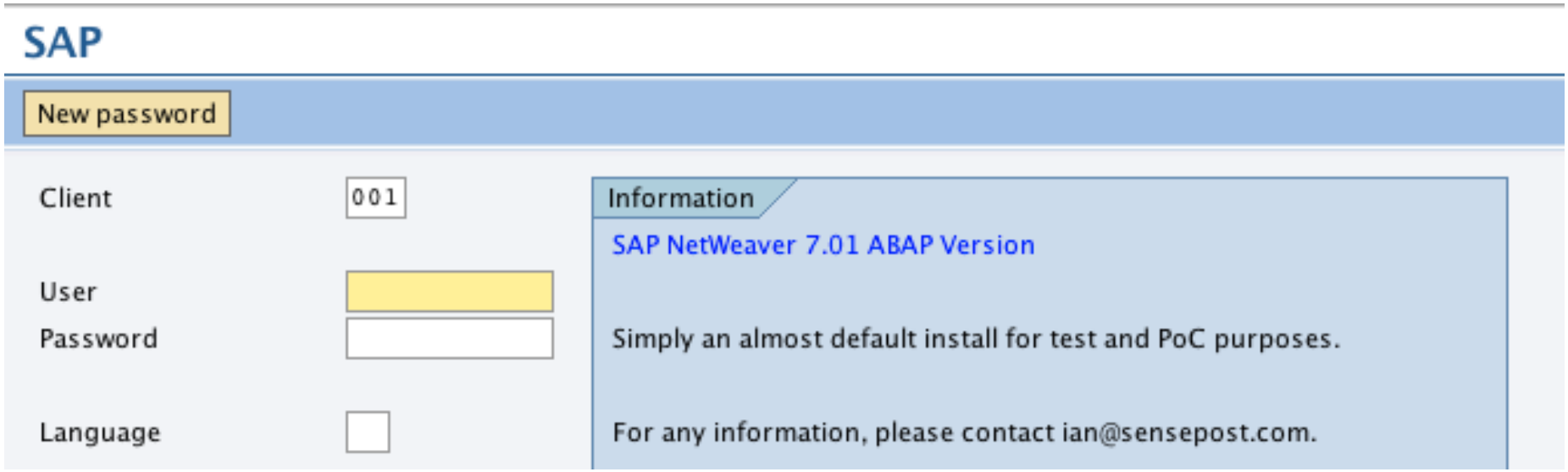
Dialogs

- All input fields accept strings
  - No client-side validation
  - Data is validated on the server
- Input field lengths can be manipulated



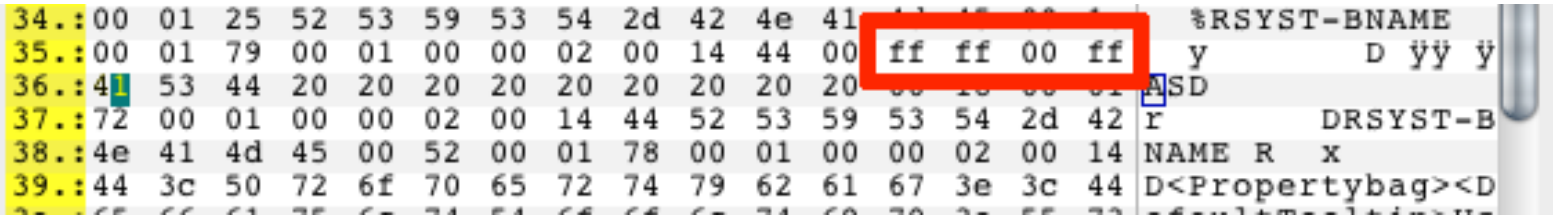
Dialogs

- All input fields accept strings
  - No client-side validation
  - Data is validated on the server
- Input field lengths can be manipulated



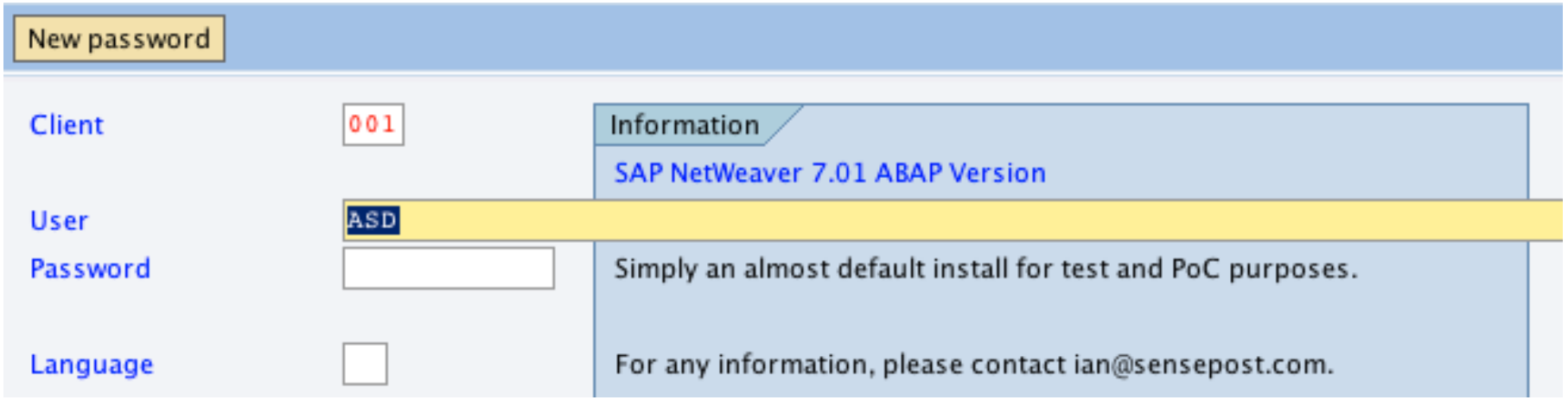
Dialogs

- All input fields accept strings
  - No client-side validation
  - Data is validated on the server
- Input field lengths can be manipulated



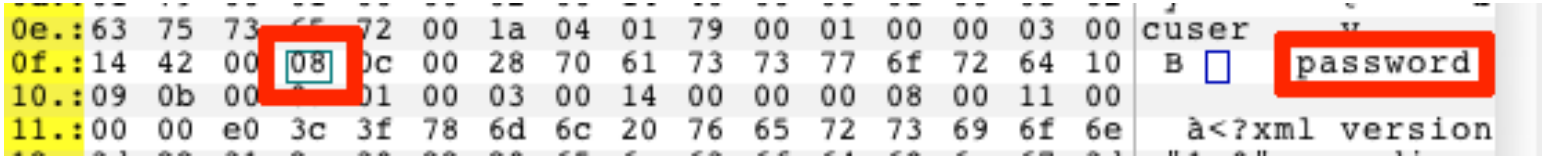
Dialogs

- All input fields accept strings
  - No client-side validation
  - Data is validated on the server
- Input field lengths can be manipulated



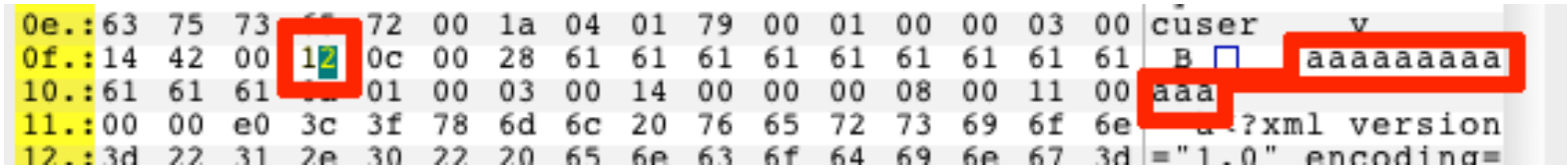
Dialogs

- Length of submitted strings can be adjusted in a similar fashion…



Dialogs

- Length of submitted strings can be adjusted in a similar fashion…



Complex Messages

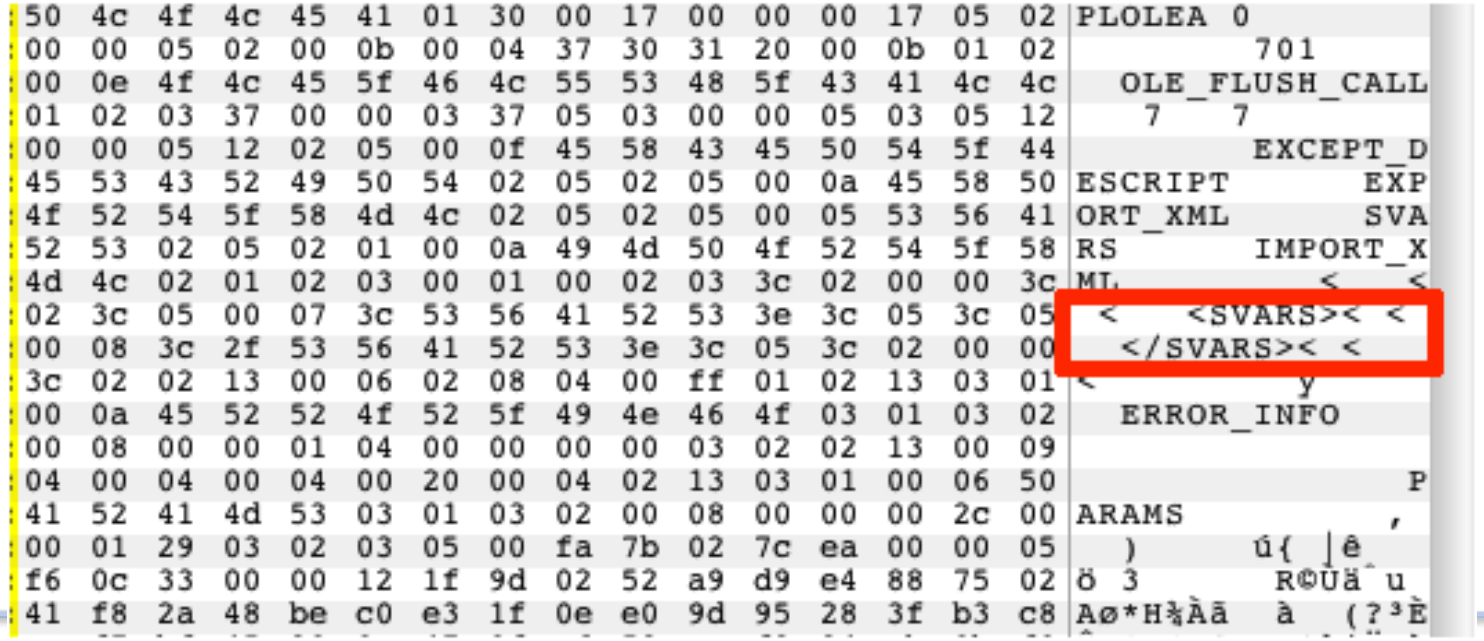
- Contain the same structures as simple messages…

Complex Messages

- Contain the same structures as simple messages…
- … But include XML structure:
  - <SVARS>

Complex Messages

- Contain the same structures as simple messages…
- … But include XML structure:
  - <SVARS>



```
50 4c 4f 4c 45 41 01 30 00 17 00 00 00 17 05 02 PLOLEA 0
00 00 05 02 00 0b 00 04 37 30 31 20 00 0b 01 02         701
00 0e 4f 4c 45 5f 46 4c 55 53 48 5f 43 41 4c 4c   OLE_FLUSH_CALL
01 02 03 37 00 00 03 37 05 03 00 00 05 03 05 12    7   7
00 00 05 12 02 05 00 0f 45 58 43 45 50 54 5f 44         EXCEPT_D
45 53 43 52 49 50 54 02 05 02 05 00 0a 45 58 50 ESCRIPT       EXP
4f 52 54 5f 58 4d 4c 02 05 02 05 00 05 53 56 41 ORT_XML       SVA
52 53 02 05 02 01 00 0a 49 4d 50 4f 52 54 5f 58 RS       IMPORT_X
4d 4c 02 01 02 03 00 01 00 02 03 3c 02 00 00 3c ML           <    <
02 3c 05 00 07 3c 53 56 41 52 53 3e 3c 05 3c 05  <    <SVARS>< <
00 08 3c 2f 53 56 41 52 53 3e 3c 05 3c 02 00 00   </SVARS>< <
3c 02 02 13 00 06 02 08 04 00 ff 01 02 13 03 01 <          y
00 0a 45 52 52 4f 52 5f 49 4e 46 4f 03 01 03 02   ERROR_INFO
00 08 00 00 01 04 00 00 00 00 03 02 02 13 00 09
04 00 04 00 04 00 20 00 04 02 13 03 01 00 06 50                P
41 52 41 4d 53 03 01 03 02 00 08 00 00 00 2c 00 ARAMS           ,
00 01 29 03 02 03 05 00 fa 7b 02 7c ea 00 00 05   )      ú{ |ê
f6 0c 33 00 00 12 1f 9d 02 52 a9 d9 e4 88 75 02 ö 3       R©Ùä u
41 f8 2a 48 be c0 e3 1f 0e e0 9d 95 28 3f b3 c8 Aø*H¾Àã   à   (?³È
```

Complex Messages

- Contain the same structures as simple messages…
- … But include XML structure:
  - <SVARS>
- Include compressed streams:
  - PARAMS

Complex Messages

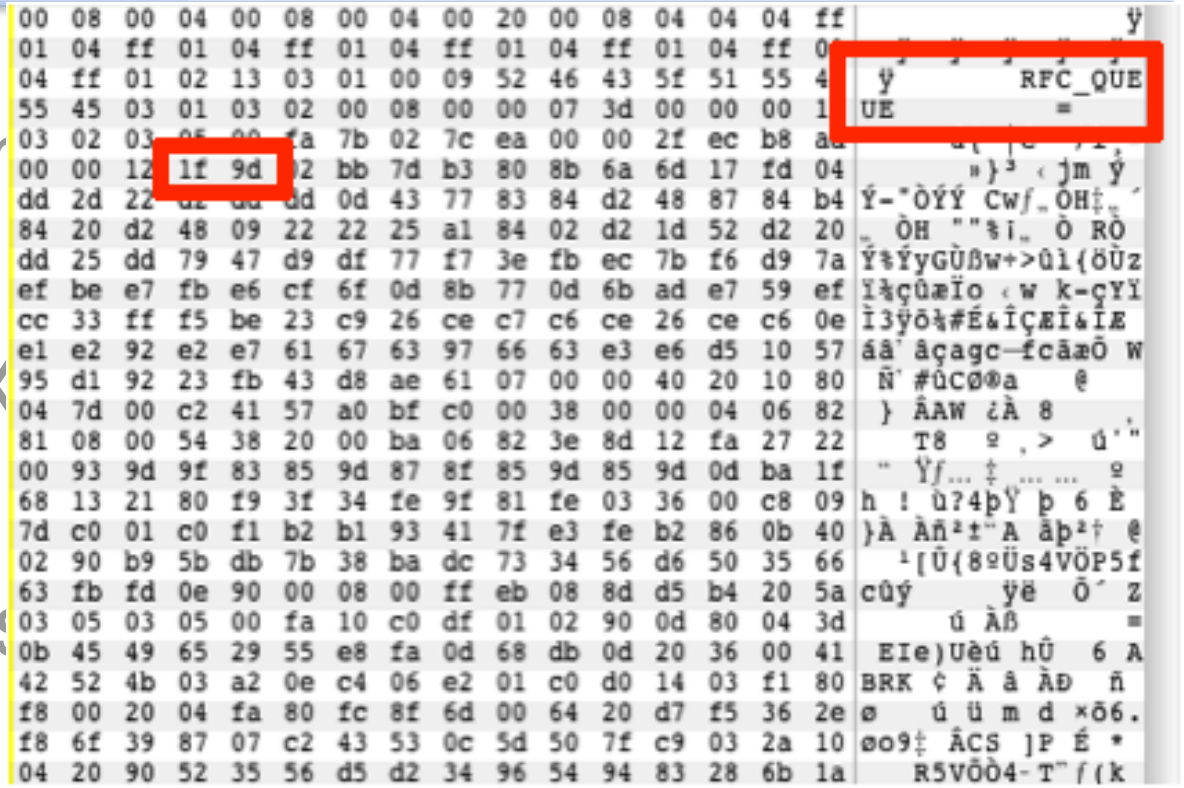
- Contain the messages…
- … But inclu
  - <SVARS>
- Include com
  - PARAMS

Complex Messages

- Contain the same structures as simple messages…
- … But include XML structure:
  - <SVARS>
- Include compressed streams:
  - PARAMS
  - RFC_QUEUE

Complex Messages

- Contain the sam
  messages…
- … But include X
  - <SVARS>
- Include compres
  - PARAMS
  - RFC_QUEUE

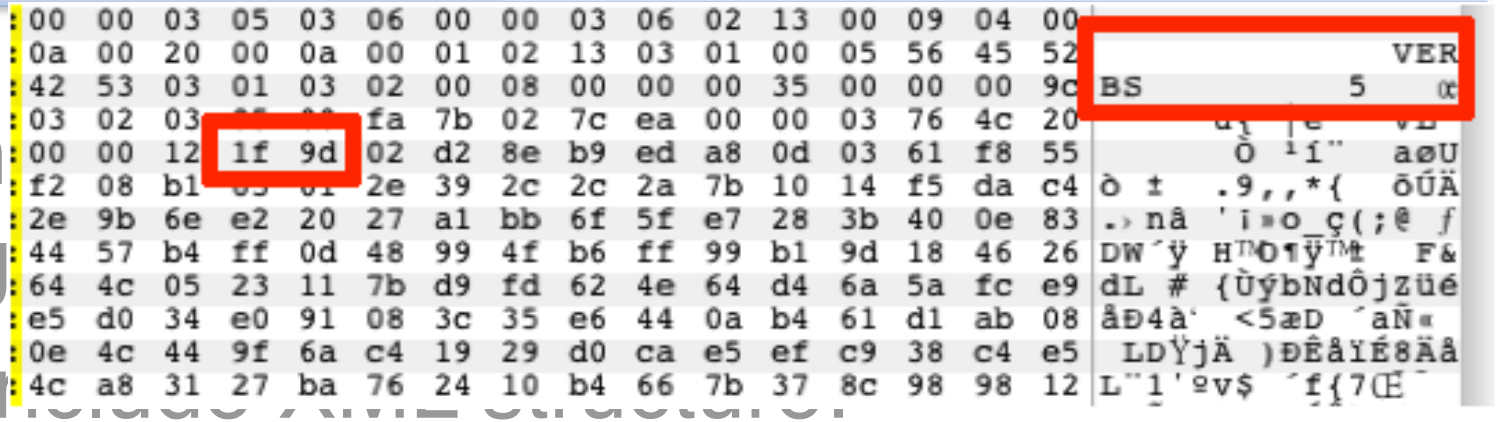


Complex Messages

- Contain the same structures as simple messages…
- … But include XML structure:
  - <SVARS>
- Include compressed streams:
  - PARAMS
  - RFC_QUEUE
  - VERBS

Complex Messages

- Contain
  messag
- … But i
  - <SVARS>
- Include compressed streams:
  - PARAMS
  - RFC_QUEUE
  - VERBS

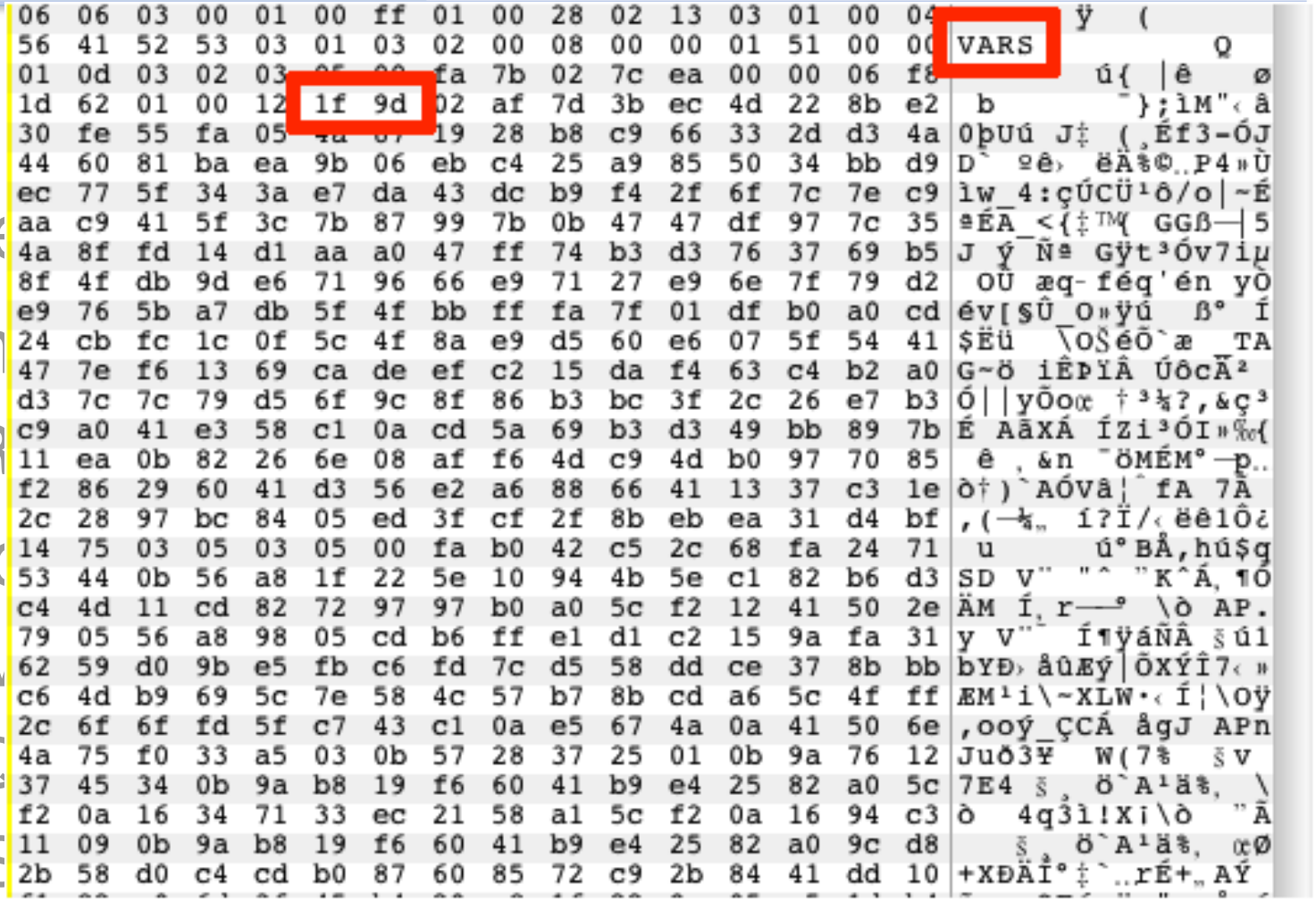


Complex Messages

- Contain the same structures as simple messages…
- … But include XML structure:
  - <SVARS>
- Include compressed streams:
  - PARAMS
  - RFC_QUEUE
  - VERBS
  - VARS

Complex Messages

- Contain
  message
- … But in
  - <SVAR
- Include
  - PARAM
  - RFC_C
  - VERBS
  - VARS

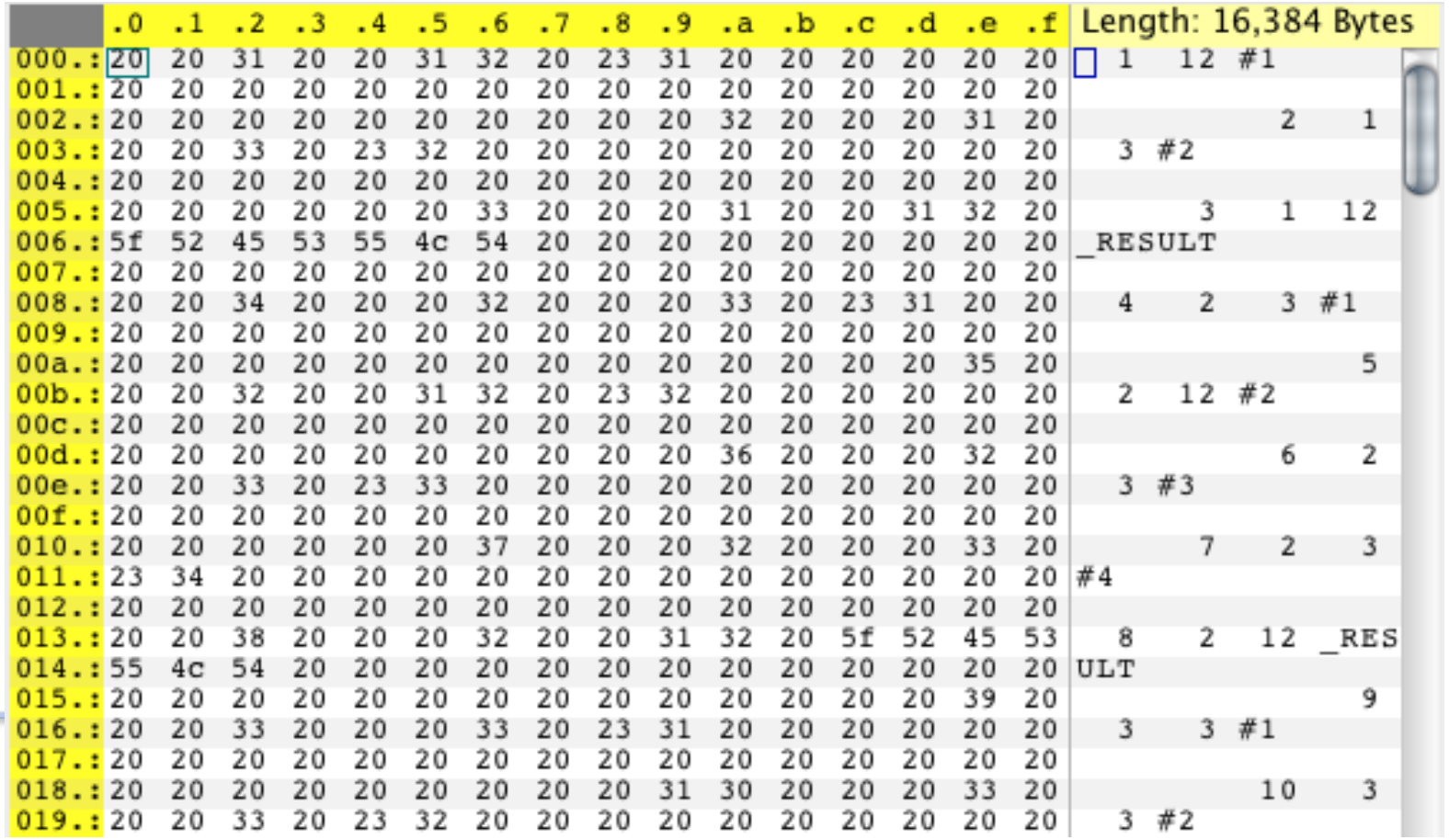


PARAMS, VARS and VERBS

- Work in conjunction
- Define actions to be performed on / by objects on the GUI / Server
- Lists of “indexed data” are decompressed and parsed by ABAP to various fixed-length data structures

PARAMS, VARS and VERBS

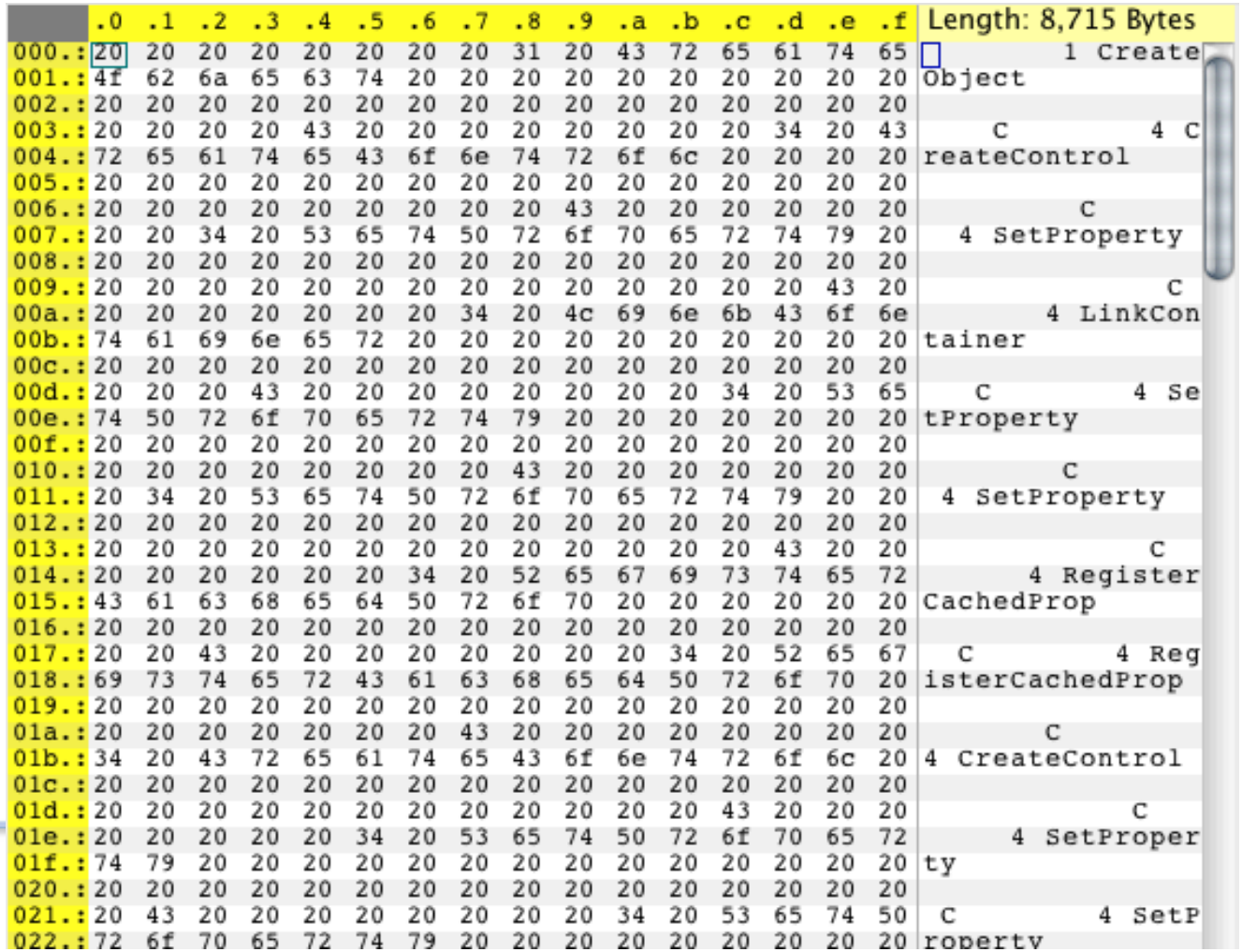
- Decompressed, they look as follows:
  - PARAMS:



	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 16,384 Bytes
000.:	20	20	31	20	20	31	32	20	23	31	20	20	20	20	20	20	1 12 #1
001.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
002.:	20	20	20	20	20	20	20	20	20	20	32	20	20	20	31	20	2 1
003.:	20	20	33	20	23	32	20	20	20	20	20	20	20	20	20	20	3 #2
004.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
005.:	20	20	20	20	20	20	33	20	20	20	31	20	20	31	32	20	3 1 12
006.:	5f	52	45	53	55	4c	54	20	20	20	20	20	20	20	20	20	_RESULT
007.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
008.:	20	20	34	20	20	20	32	20	20	20	33	20	23	31	20	20	4 2 3 #1
009.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00a.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	35	20	5
00b.:	20	20	32	20	20	31	32	20	23	32	20	20	20	20	20	20	2 12 #2
00c.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00d.:	20	20	20	20	20	20	20	20	20	20	36	20	20	20	32	20	6 2
00e.:	20	20	33	20	23	33	20	20	20	20	20	20	20	20	20	20	3 #3
00f.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
010.:	20	20	20	20	20	20	37	20	20	20	32	20	20	20	33	20	7 2 3
011.:	23	34	20	20	20	20	20	20	20	20	20	20	20	20	20	20	#4
012.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
013.:	20	20	38	20	20	20	32	20	20	31	32	20	5f	52	45	53	8 2 12 _RES
014.:	55	4c	54	20	20	20	20	20	20	20	20	20	20	20	20	20	ULT
015.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	39	20	9
016.:	20	20	33	20	20	20	33	20	23	31	20	20	20	20	20	20	3 3 #1
017.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
018.:	20	20	20	20	20	20	20	20	20	31	30	20	20	20	33	20	10 3
019.:	20	20	33	20	23	32	20	20	20	20	20	20	20	20	20	20	3 #2

PARAMS, VARS and VERBS

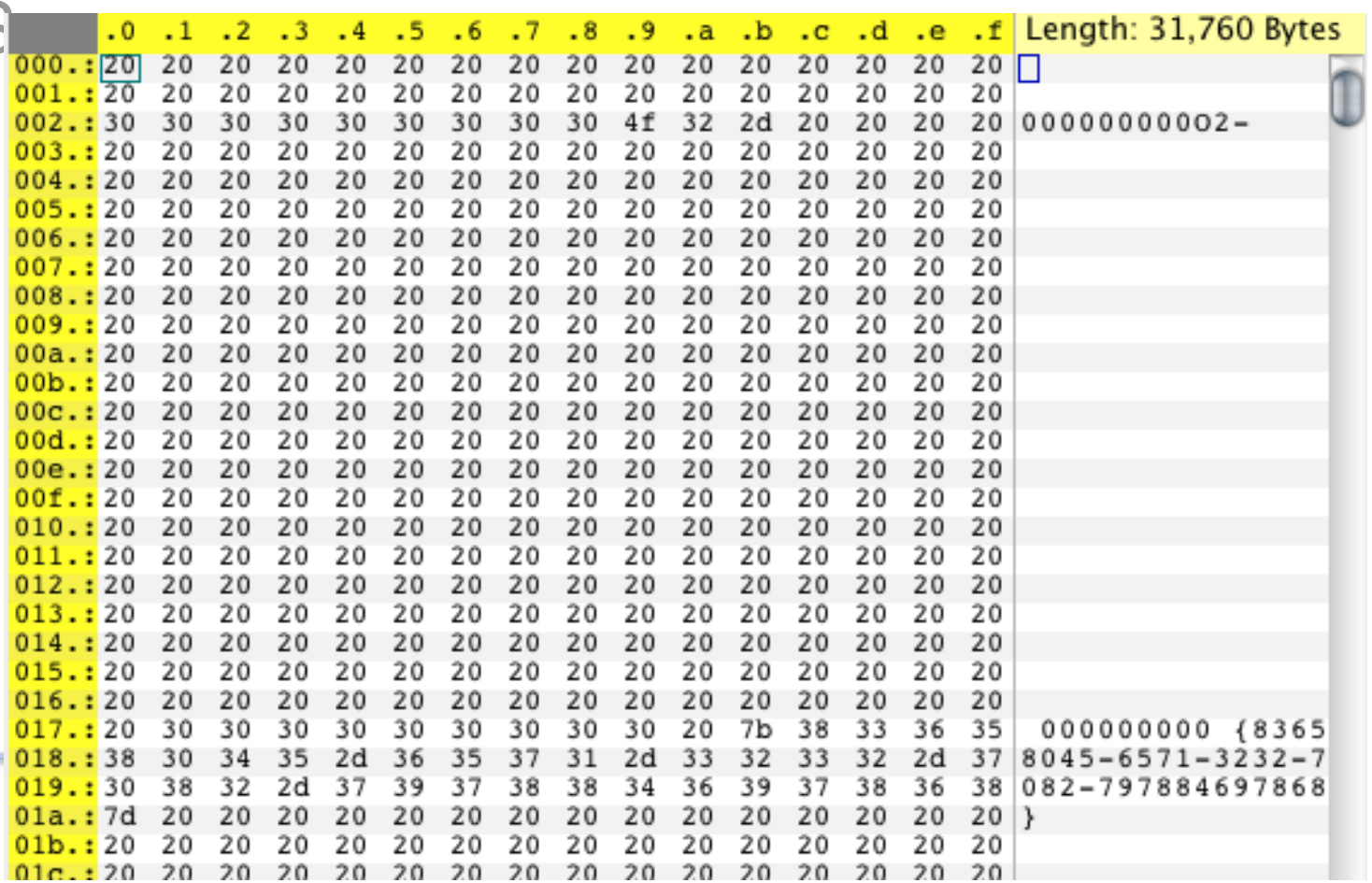
- Decompressed, they look as follows:
  - PARAMS:
  - VERBS:



	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 8,715 Bytes
000.:	20	20	20	20	20	20	20	20	31	20	43	72	65	61	74	65	1 Create
001.:	4f	62	6a	65	63	74	20	20	20	20	20	20	20	20	20	20	Object
002.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
003.:	20	20	20	20	43	20	20	20	20	20	20	20	20	34	20	43	C 4 C
004.:	72	65	61	74	65	43	6f	6e	74	72	6f	6c	20	20	20	20	reateControl
005.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
006.:	20	20	20	20	20	20	20	20	20	43	20	20	20	20	20	20	C
007.:	20	20	34	20	53	65	74	50	72	6f	70	65	72	74	79	20	4 SetProperty
008.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
009.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	43	20	C
00a.:	20	20	20	20	20	20	20	34	20	4c	69	6e	6b	43	6f	6e	4 LinkCon
00b.:	74	61	69	6e	65	72	20	20	20	20	20	20	20	20	20	20	tainer
00c.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00d.:	20	20	20	43	20	20	20	20	20	20	20	20	34	20	53	65	C 4 Se
00e.:	74	50	72	6f	70	65	72	74	79	20	20	20	20	20	20	20	tProperty
00f.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
010.:	20	20	20	20	20	20	20	20	43	20	20	20	20	20	20	20	C
011.:	20	34	20	53	65	74	50	72	6f	70	65	72	74	79	20	20	4 SetProperty
012.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
013.:	20	20	20	20	20	20	20	20	20	20	20	20	20	43	20	20	C
014.:	20	20	20	20	20	20	34	20	52	65	67	69	73	74	65	72	4 Register
015.:	43	61	63	68	65	64	50	72	6f	70	20	20	20	20	20	20	CachedProp
016.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
017.:	20	20	43	20	20	20	20	20	20	20	20	34	20	52	65	67	C 4 Reg
018.:	69	73	74	65	72	43	61	63	68	65	64	50	72	6f	70	20	isterCachedProp
019.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
01a.:	20	20	20	20	20	20	20	43	20	20	20	20	20	20	20	20	C
01b.:	34	20	43	72	65	61	74	65	43	6f	6e	74	72	6f	6c	20	4 CreateControl
01c.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
01d.:	20	20	20	20	20	20	20	20	20	20	20	20	43	20	20	20	C
01e.:	20	20	20	20	20	34	20	53	65	74	50	72	6f	70	65	72	4 SetProper
01f.:	74	79	20	20	20	20	20	20	20	20	20	20	20	20	20	20	ty
020.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
021.:	20	43	20	20	20	20	20	20	20	20	34	20	53	65	74	50	C 4 SetP
022.:	72	6f	70	65	72	74	79	20	20	20	20	20	20	20	20	20	roperty

PARAMS, VARS and VERBS

- Decompressed, they look as follows:
  - PARAMS:
  - VERBS:
  - VARS:



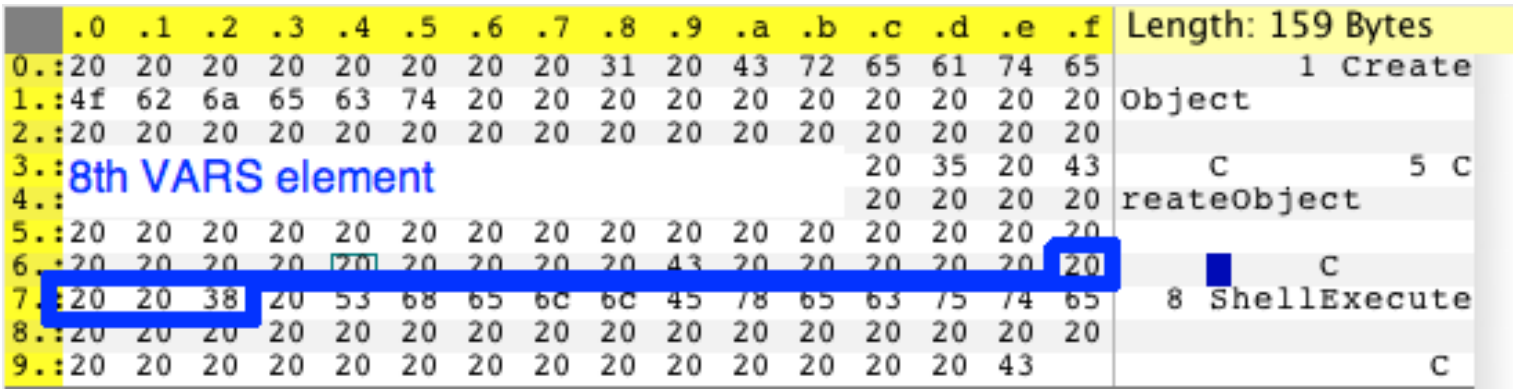
	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 31,760 Bytes
000.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
001.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
002.:	30	30	30	30	30	30	30	30	30	4f	32	2d	20	20	20	20	00000000O2-
003.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
004.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
005.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
006.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
007.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
008.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
009.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00a.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00b.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00c.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00d.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00e.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00f.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
010.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
011.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
012.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
013.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
014.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
015.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
016.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
017.:	20	30	30	30	30	30	30	30	30	30	20	7b	38	33	36	35	000000000 {8365
018.:	38	30	34	35	2d	36	35	37	31	2d	33	32	33	32	2d	37	8045-6571-3232-7
019.:	30	38	32	2d	37	39	37	38	38	34	36	39	37	38	36	38	082-797884697868
01a.:	7d	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	}
01b.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
01c.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	

PARAMS, VARS and VERBS

- Parsed by ABAP into structured variables
- CASE ABAP PARAM-TYP.
  - WHEN ‘S’:
    - Set Value Of
  - WHEN ‘G’:
    - Get Value Of
  - WHEN ‘C’:
    - Call Method Of
- Thoughts of eval() spring to mind…☺

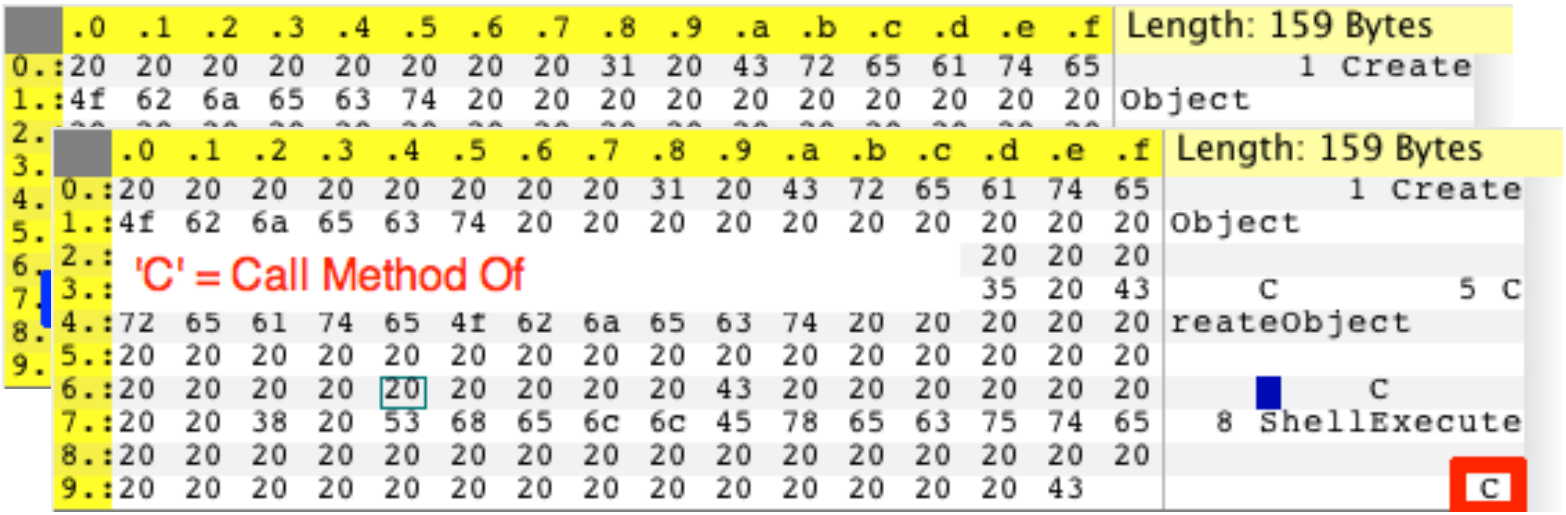
PARAMS, VARS and VERBS

- Graphic example:



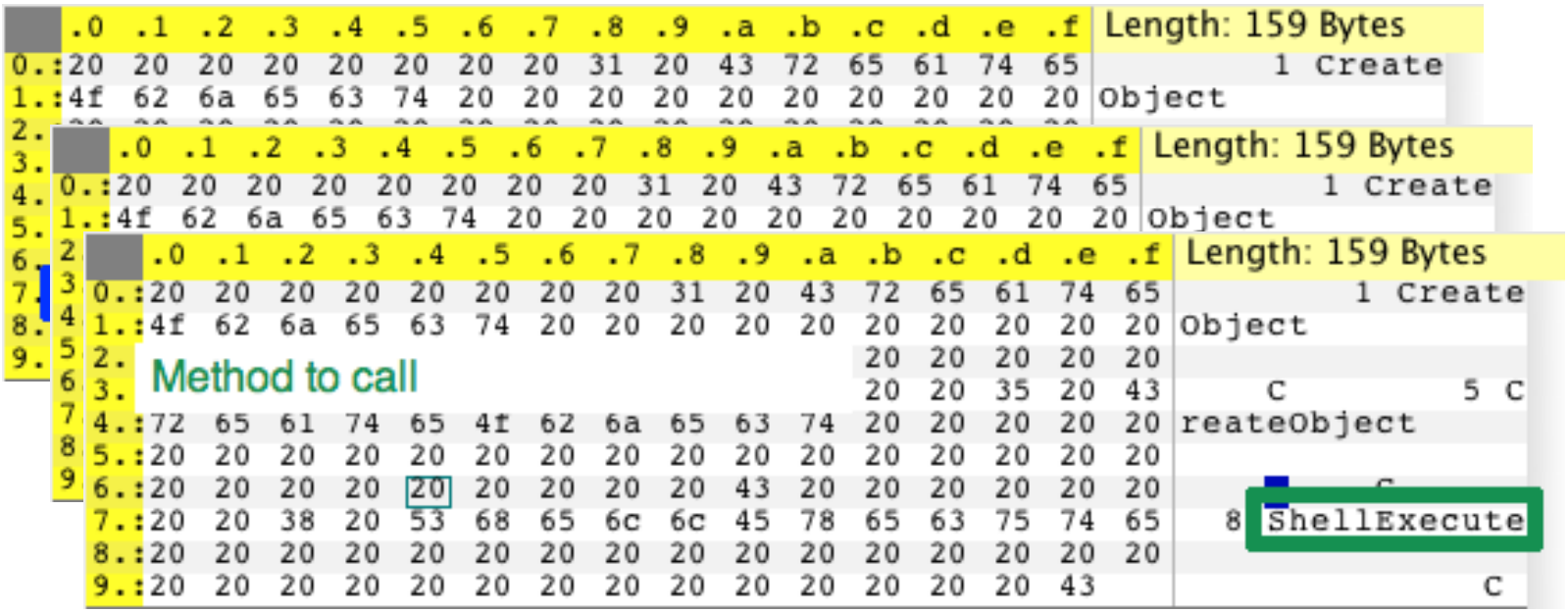
PARAMS, VARS and VERBS

- Graphic example:



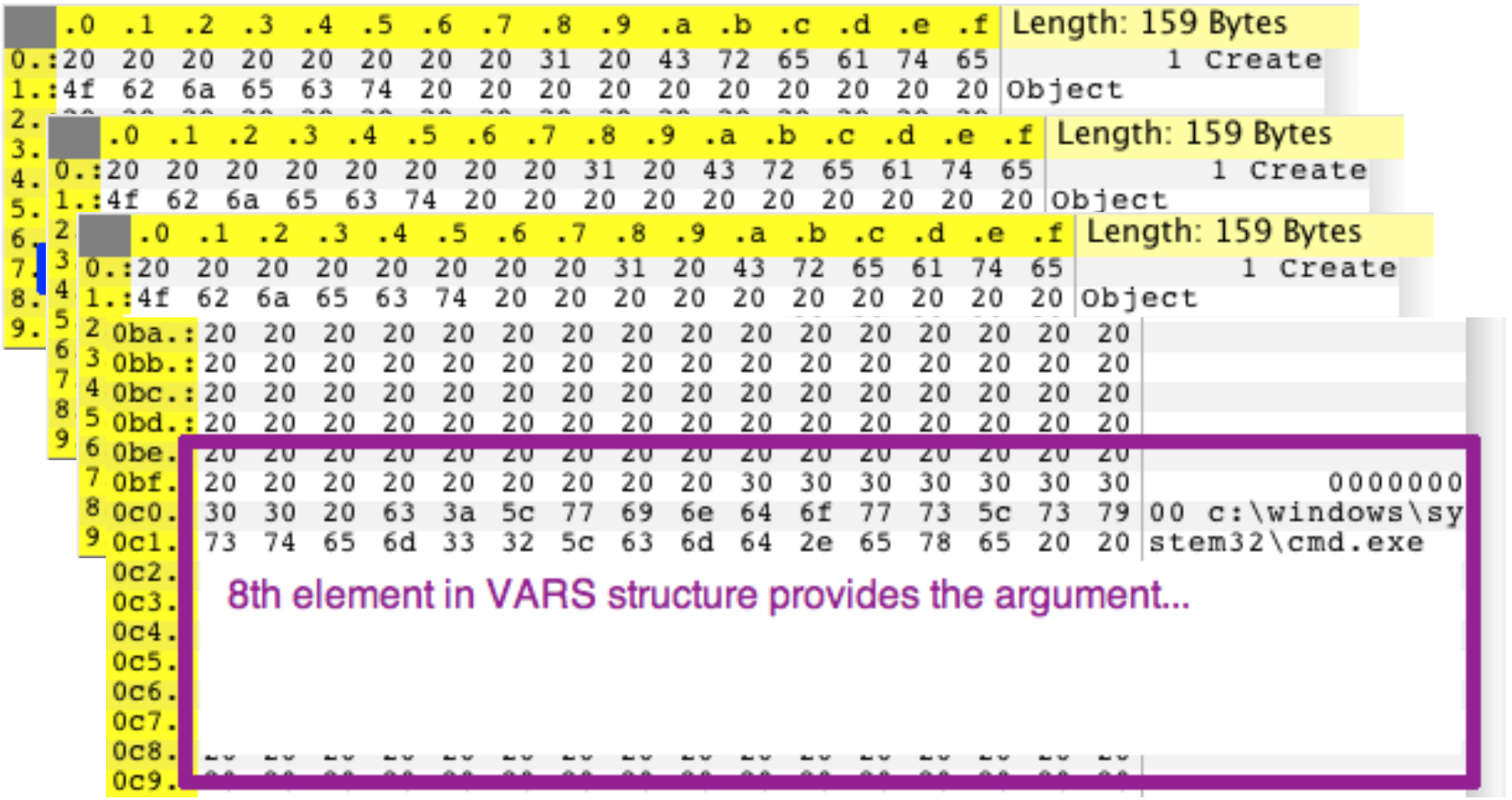
PARAMS, VARS and VERBS

- Graphic example:



PARAMS, VARS and VERBS

- Graphic example:



PARAMS, VARS and VERBS

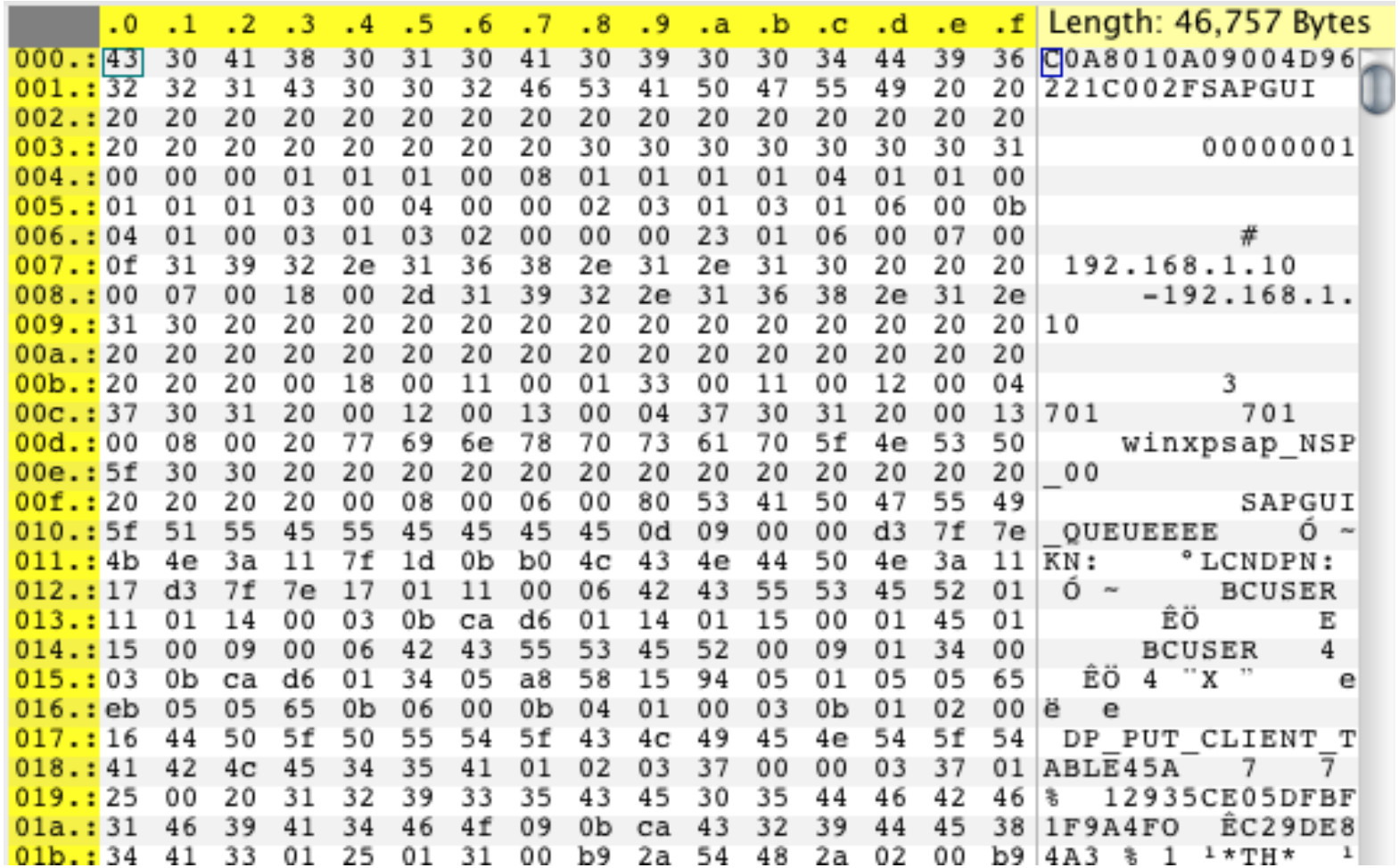
- Details on these structures can be found in ABAP code…
- Refer to ABAP Structures && where used:
  - OLE_PA
  - OLE_VERBS
  - SWCBCONT

RFC_QUEUE

- Contains META and internal table data in use by the current application / screen
- Only ever seems to appear in SAP responses
  - This assumption may be incorrect

RFC_QUEUE

- in
-

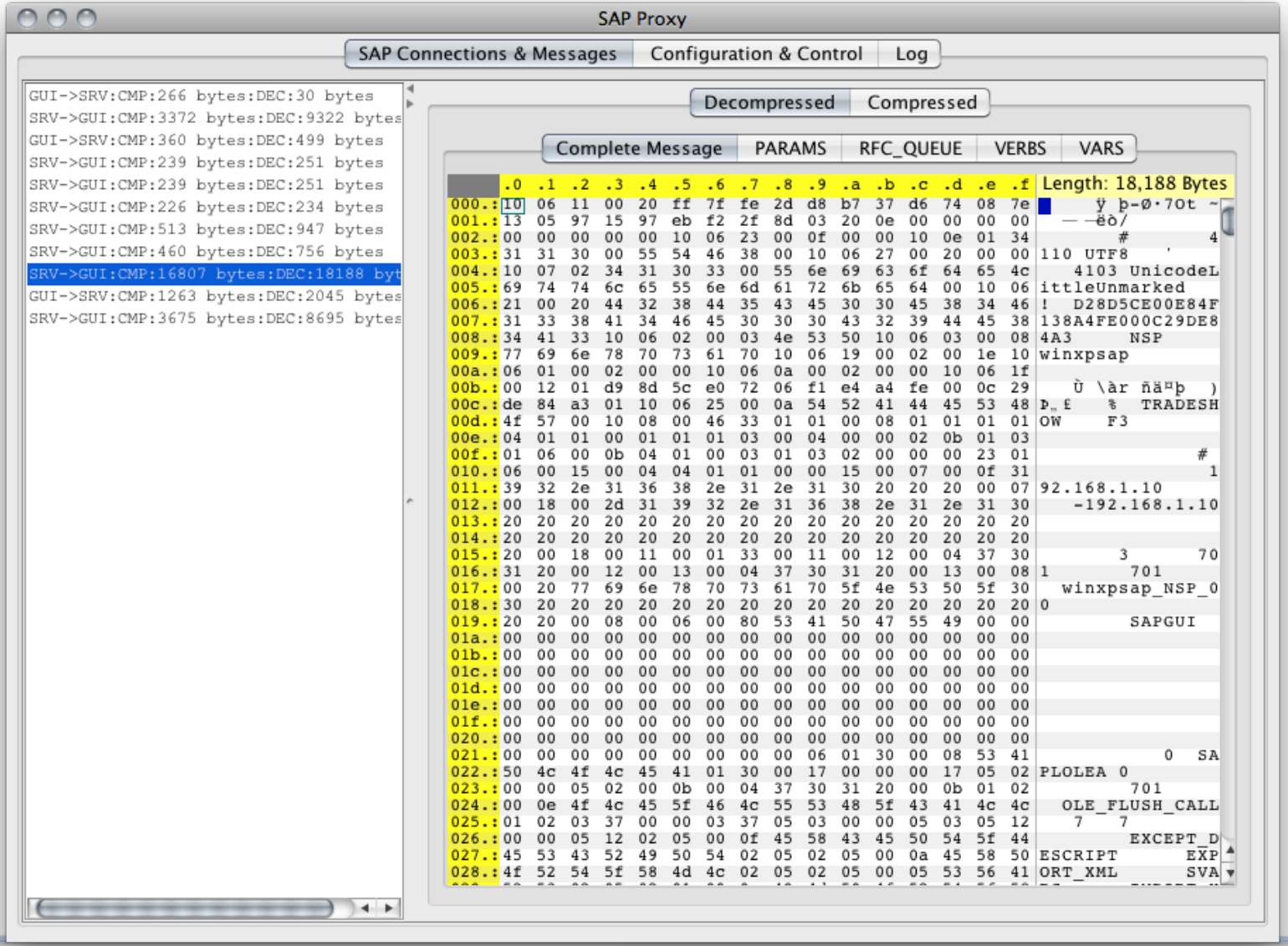


	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 46,757 Bytes
000.:	43	30	41	38	30	31	30	41	30	39	30	30	34	44	39	36	C0A8010A09004D96
001.:	32	32	31	43	30	30	32	46	53	41	50	47	55	49	20	20	221C002FSAPGUI
002.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
003.:	20	20	20	20	20	20	20	20	30	30	30	30	30	30	30	31	00000001
004.:	00	00	00	01	01	01	00	08	01	01	01	01	04	01	01	00	
005.:	01	01	01	03	00	04	00	00	02	03	01	03	01	06	00	0b	
006.:	04	01	00	03	01	03	02	00	00	00	23	01	06	00	07	00	#
007.:	0f	31	39	32	2e	31	36	38	2e	31	2e	31	30	20	20	20	192.168.1.10
008.:	00	07	00	18	00	2d	31	39	32	2e	31	36	38	2e	31	2e	-192.168.1.
009.:	31	30	20	20	20	20	20	20	20	20	20	20	20	20	20	20	10
00a.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00b.:	20	20	20	00	18	00	11	00	01	33	00	11	00	12	00	04	3
00c.:	37	30	31	20	00	12	00	13	00	04	37	30	31	20	00	13	701 701
00d.:	00	08	00	20	77	69	6e	78	70	73	61	70	5f	4e	53	50	winxpsap_NSP
00e.:	5f	30	30	20	20	20	20	20	20	20	20	20	20	20	20	20	_00
00f.:	20	20	20	20	00	08	00	06	00	80	53	41	50	47	55	49	SAPGUI
010.:	5f	51	55	45	55	45	45	45	45	0d	09	00	00	d3	7f	7e	_QUEUEEEE Ó ~
011.:	4b	4e	3a	11	7f	1d	0b	b0	4c	43	4e	44	50	4e	3a	11	KN: °LCNDPN:
012.:	17	d3	7f	7e	17	01	11	00	06	42	43	55	53	45	52	01	Ó ~ BCUSER
013.:	11	01	14	00	03	0b	ca	d6	01	14	01	15	00	01	45	01	ÊÖ E
014.:	15	00	09	00	06	42	43	55	53	45	52	00	09	01	34	00	BCUSER 4
015.:	03	0b	ca	d6	01	34	05	a8	58	15	94	05	01	05	05	65	ÊÖ 4 ¨X ¨ e
016.:	eb	05	05	65	0b	06	00	0b	04	01	00	03	0b	01	02	00	ë e
017.:	16	44	50	5f	50	55	54	5f	43	4c	49	45	4e	54	5f	54	DP_PUT_CLIENT_T
018.:	41	42	4c	45	34	35	41	01	02	03	37	00	00	03	37	01	ABLE45A 7 7
019.:	25	00	20	31	32	39	33	35	43	45	30	35	44	46	42	46	% 12935CE05DFBF
01a.:	31	46	39	41	34	46	4f	09	0b	ca	43	32	39	44	45	38	1F9A4FO ÊC29DE8
01b.:	34	41	33	01	25	01	31	00	b9	2a	54	48	2a	02	00	b9	4A3 % 1 ¹*TH* ¹

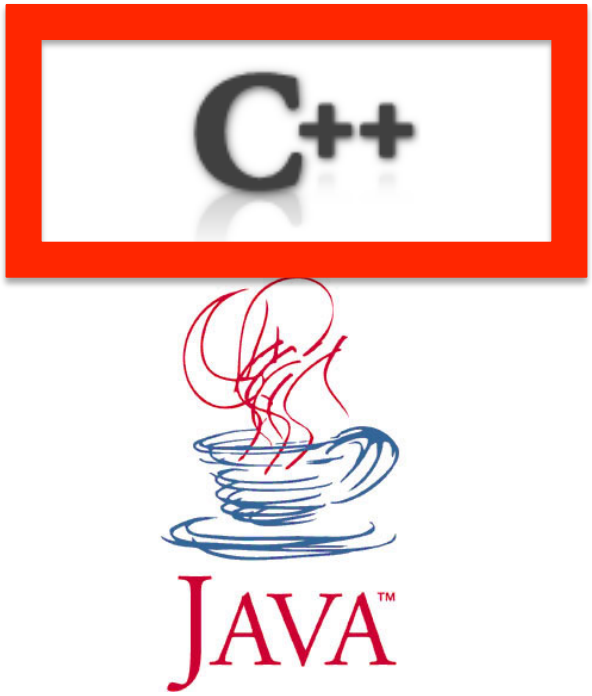
The Fundamentals

- ~~Understand the compression~~
- ~~Understand the compressed protocol~~
  - ~~Simplify the sniffing and decompression~~
- ~~Recompression~~
- ~~Understand the application protocol~~
  - ~~What makes SAP Gui tick ?~~
- Identify SAP attack vectors not previously considered…

SAPProx


SAP Proxy
SAP Connections & Messages
Configuration & Control
Log
GUI->SRV:CMP:266 bytes:DEC:30 bytes
SRV->GUI:CMP:3372 bytes:DEC:9322 bytes
GUI->SRV:CMP:360 bytes:DEC:499 bytes
SRV->GUI:CMP:239 bytes:DEC:251 bytes
SRV->GUI:CMP:239 bytes:DEC:251 bytes
SRV->GUI:CMP:226 bytes:DEC:234 bytes
SRV->GUI:CMP:513 bytes:DEC:947 bytes
SRV->GUI:CMP:460 bytes:DEC:756 bytes
SRV->GUI:CMP:16807 bytes:DEC:18188 byt
GUI->SRV:CMP:1263 bytes:DEC:2045 bytes
SRV->GUI:CMP:3675 bytes:DEC:8695 bytes
Decompressed
Compressed
Complete Message
PARAMS
RFC_QUEUE
VERBS
VARS
Length: 18,188 Bytes

SAPProx

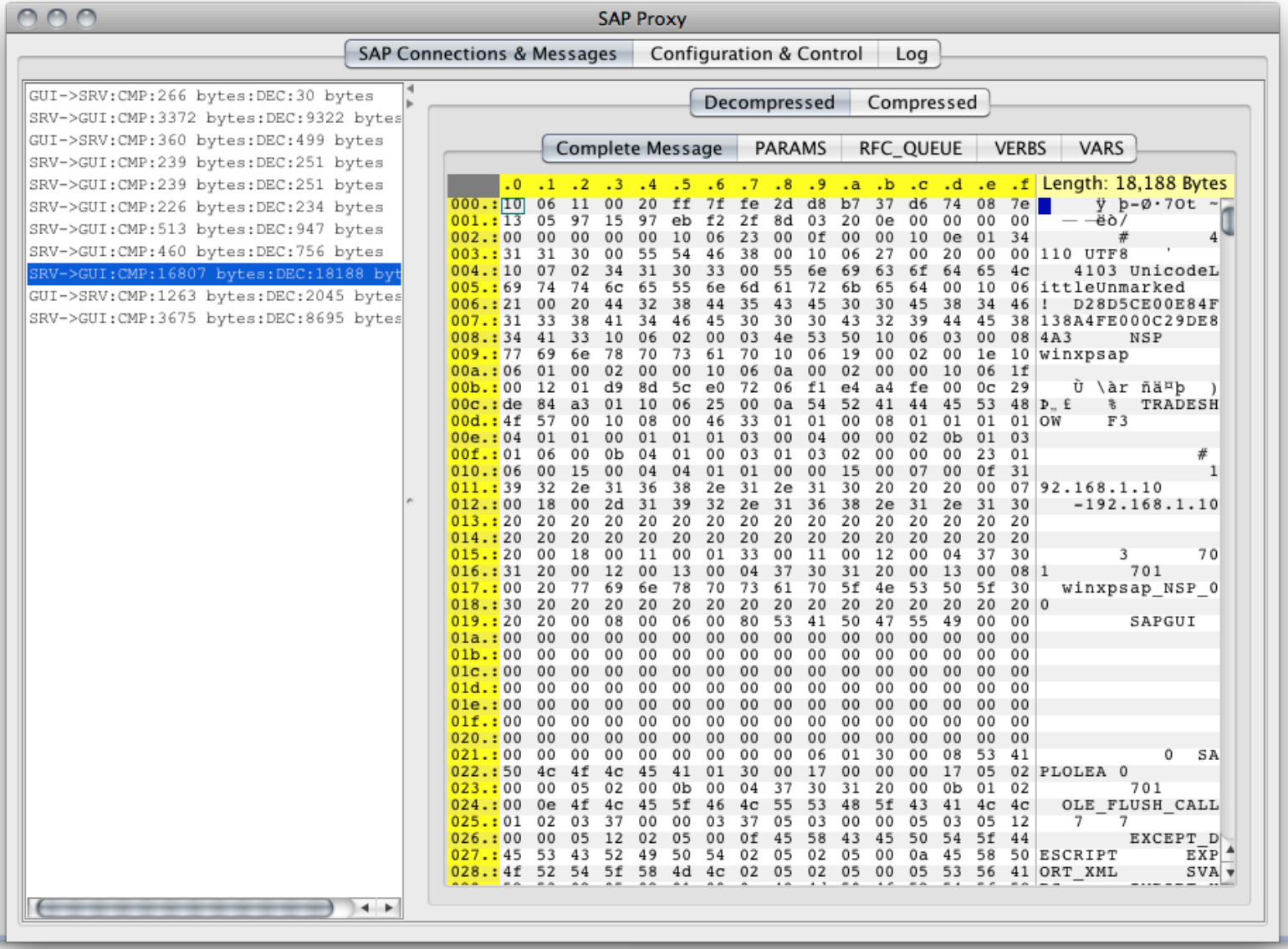


- SapCompress
  - JNI interface
  - Implements MaxDB functions for decompression && compression
    - int[] doDecompress(int[])
    - Int[] doCompress(int[])

SAPProx

- SAPProx
  - Java
  - Responsible for:
    - Parsing packet data
    - Decompressing messages
    - Interception
    - Compressing modified messages
    - Queue management

Demo: SAPProx



Attack API

- Users can write their own exploits
- In a scripting language of their choice…
  - Jython
  - Groovy
  - Jruby
  - *
- Script locations specified in configuration
- Allow for canned exploits
- (thanks Willem Mouton)

Demo: Attacks / Scripting

```
print "START : COMMAND EXEC SCRIPT"
# The saved packet
b = [16, 6, 17, 0, 32, 255, 127, 254, 45, 2
0, 0, 0, 16, 6, 35, 0, 15, 0, 0, 16, 14, 1,
105, 99, 111, 100, 101, 76, 105, 116, 116,
56, 57, 48, 54, 70, 49, 56, 49, 65, 52, 70,
119, 105, 110, 120, 112, 115, 97, 112, 16,
224, 139, 63, 241, 32, 164, 252, 0, 12, 41,
126, 92, 224, 140, 114, 241, 34, 164, 252,
2, 0, 200, 16, 6, 7, 0, 20, 83, 69, 56, 48,
0, 0, 0, 49, 255, 16, 12, 7, 0, 16, 0, 0, 0
12, 66, 67, 85, 83, 69, 82, 32, 32, 32, 32,
32, 78, 83, 80, 32, 32, 32, 32, 32, 16, 6,
32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32,
32, 32, 32, 32, 32, 32, 32, 16, 6, 13, 0, 4
32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32,
55, 0, 0, 16, 6, 39, 0, 32, 0, 0, 16, 7, 2,
114, 107, 101, 100, 0, 16, 2, 5, 0, 223, 4,
print " + SET Message:1"
c = api.getStringInput("C:\PATH\COMMAND")
print " + GET Command : " + c
```


What we're going to talk about

- ~~Why this Talk ?~~
- ~~The history of decompressing SAP DIAG~~
- ~~Understanding the fundamentals~~
- New Attacks
- Conclusion

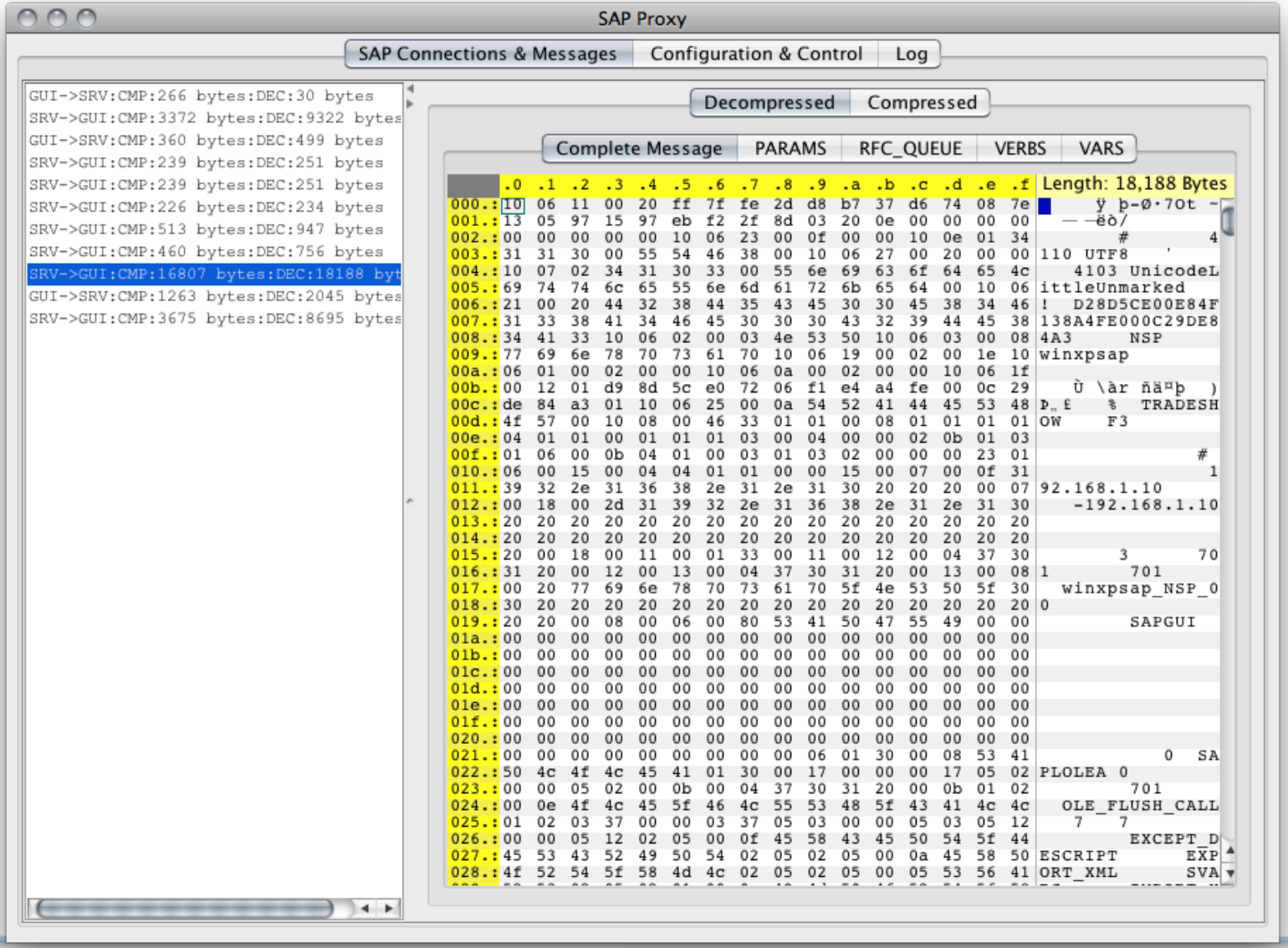
New (Old) Attacks ?

- We now have a proxy for SAP GUI
  - WebScarab for SAP
- For what I believe is the first time, we get an unprecedented view into SAP GUI applications…
- … and we know where that left us with web applications …

New (Old) Attacks ?

- Authorisation
- Authentication

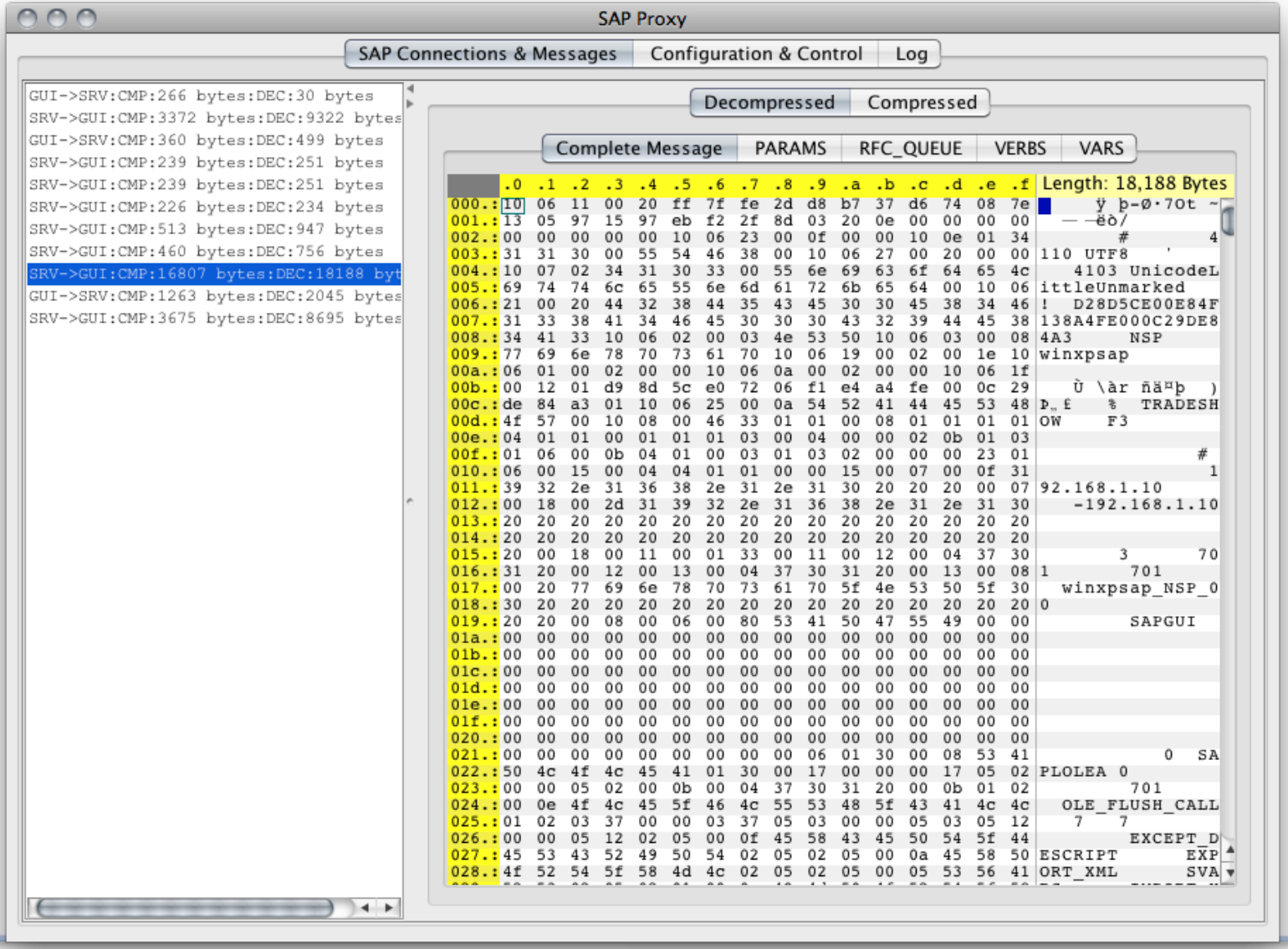
Demo: Auth*


SAP Proxy
SAP Connections & Messages
Configuration & Control
Log
GUI->SRV:CMP:266 bytes:DEC:30 bytes
SRV->GUI:CMP:3372 bytes:DEC:9322 bytes
GUI->SRV:CMP:360 bytes:DEC:499 bytes
SRV->GUI:CMP:239 bytes:DEC:251 bytes
SRV->GUI:CMP:239 bytes:DEC:251 bytes
SRV->GUI:CMP:226 bytes:DEC:234 bytes
SRV->GUI:CMP:513 bytes:DEC:947 bytes
SRV->GUI:CMP:460 bytes:DEC:756 bytes
SRV->GUI:CMP:16807 bytes:DEC:18188 byt
GUI->SRV:CMP:1263 bytes:DEC:2045 bytes
SRV->GUI:CMP:3675 bytes:DEC:8695 bytes
Decompressed
Compressed
Complete Message
PARAMS
RFC_QUEUE
VERBS
VARS
Length: 18,188 Bytes

New (Old) Attacks ?

- Authorisation
- Authentication
- State Management
- Business Logic

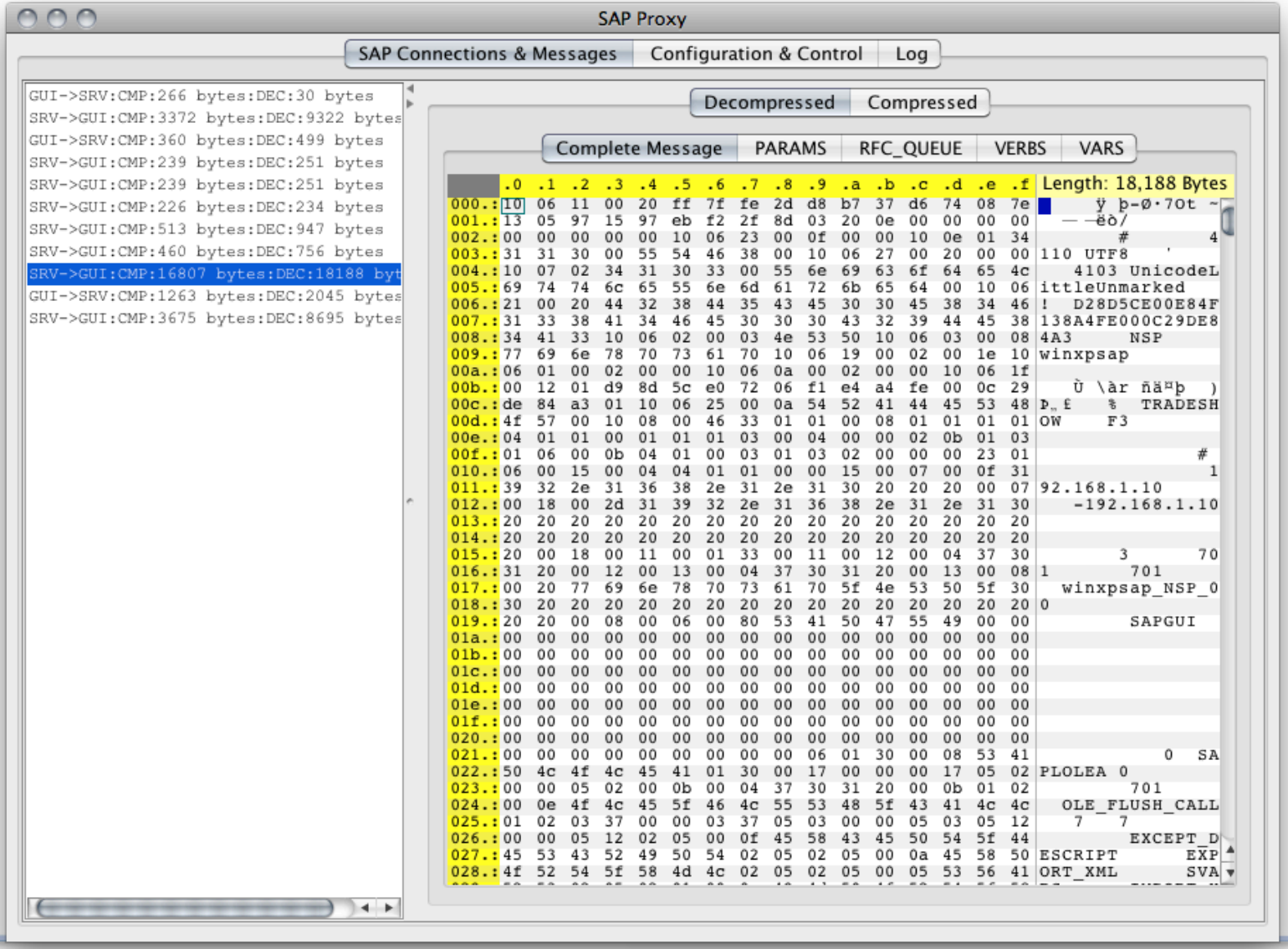
Demo: State & Business Logic



New (Old) Attacks ?

- Authorisation
- Authentication
- State Management
- Business Logic
- Validation

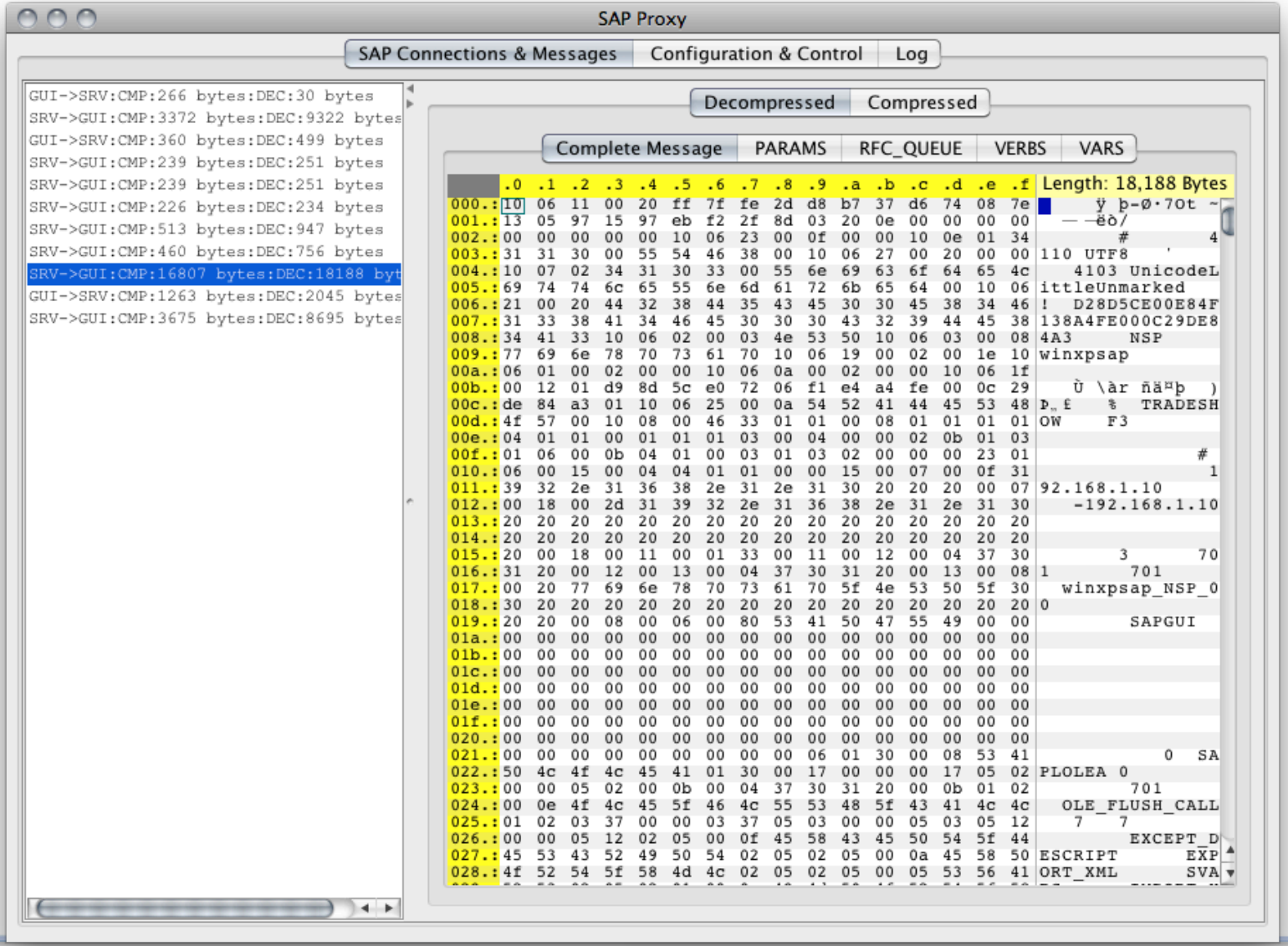
Demo: Validation



New (Old) Attacks ?

- Authorisation
- Authentication
- State Management
- Business Logic
- Validation
- Replay

Demo: Replay


SAP Proxy
SAP Connections & Messages
Configuration & Control
Log
GUI->SRV:CMP:266 bytes:DEC:30 bytes
SRV->GUI:CMP:3372 bytes:DEC:9322 bytes
GUI->SRV:CMP:360 bytes:DEC:499 bytes
SRV->GUI:CMP:239 bytes:DEC:251 bytes
SRV->GUI:CMP:239 bytes:DEC:251 bytes
SRV->GUI:CMP:226 bytes:DEC:234 bytes
SRV->GUI:CMP:513 bytes:DEC:947 bytes
SRV->GUI:CMP:460 bytes:DEC:756 bytes
SRV->GUI:CMP:16807 bytes:DEC:18188 byt
GUI->SRV:CMP:1263 bytes:DEC:2045 bytes
SRV->GUI:CMP:3675 bytes:DEC:8695 bytes
Decompressed
Compressed
Complete Message
PARAMS
RFC_QUEUE
VERBS
VARS
Length: 18,188 Bytes

New (Old) Attacks ?

- Authorisation
- Authentication
- State Management
- Business Logic
- Validation
- Replay
- Client-Side attacks

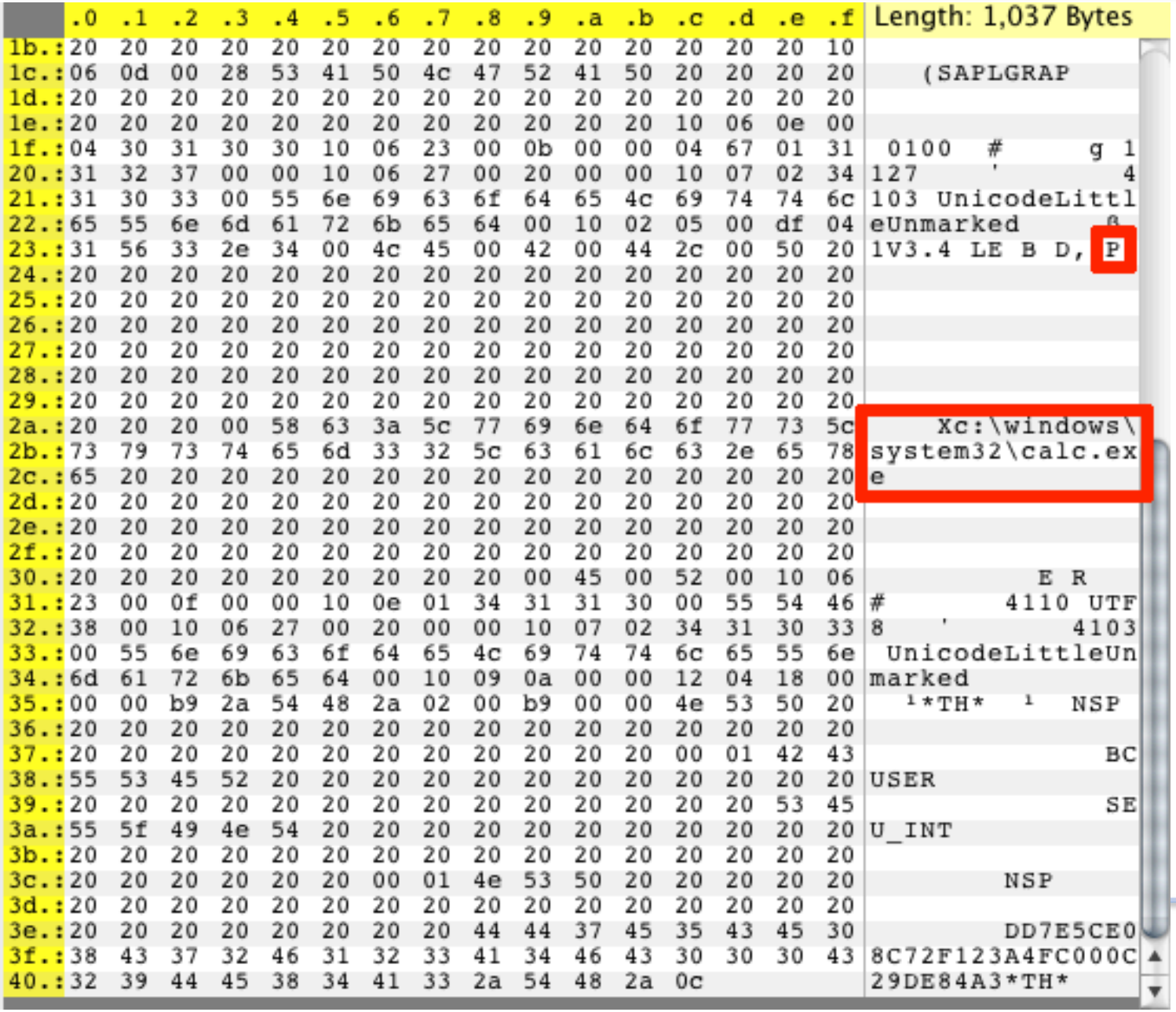
Client-Side Attacks

- Many business cases require the execution of applications on the client.
  - Provided for by ABAP
- Deprecated: GUI_RUN or WS_EXECUTE
- Current: cl_gui_frontend_services
- Newer clients still support old methods
  - Backwards compatibility
  - Do prompt when applications execute
- (thanks Steve Lord)

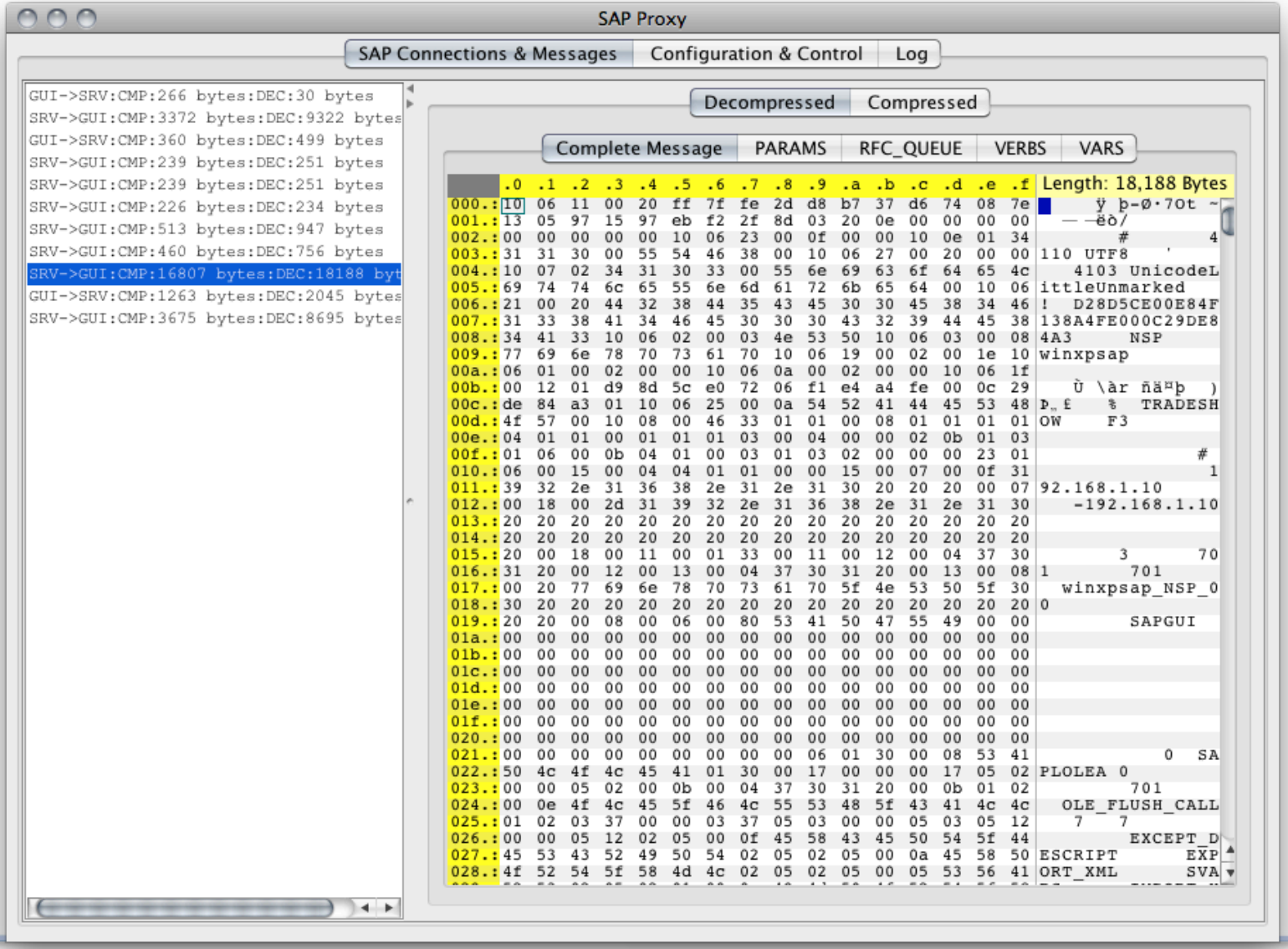
Client-Side Attacks

- WS_EXECUTE / GUI_RUN

Client-Side Attacks

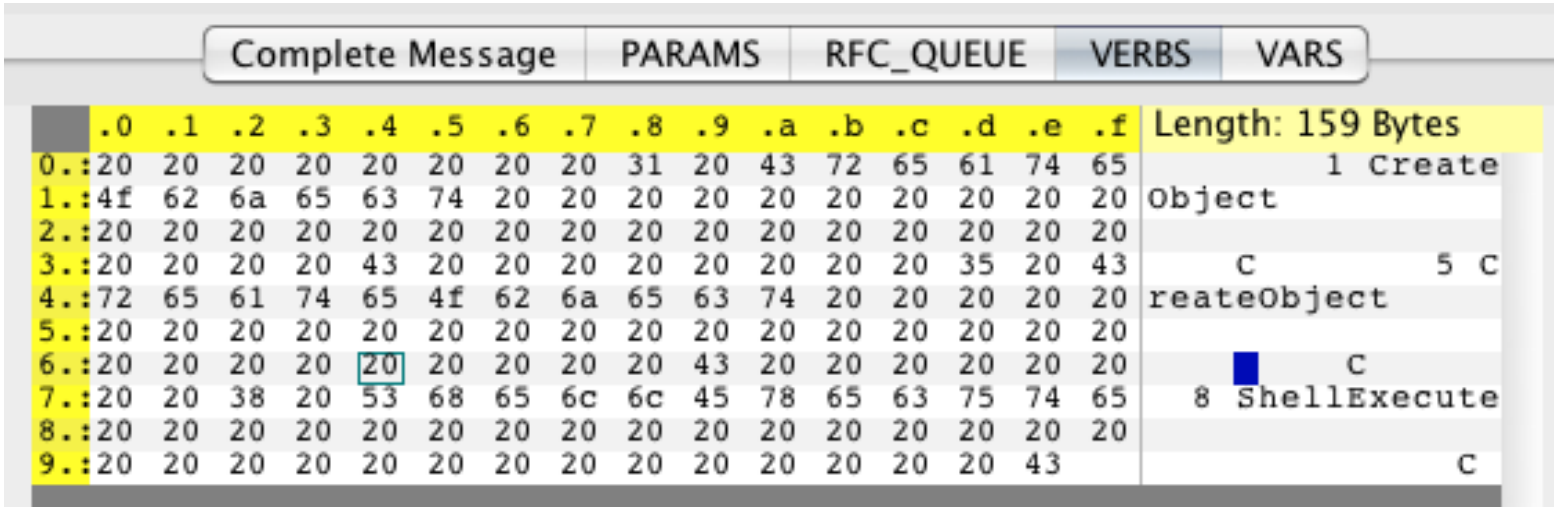


Demo: Client-Side Attacks



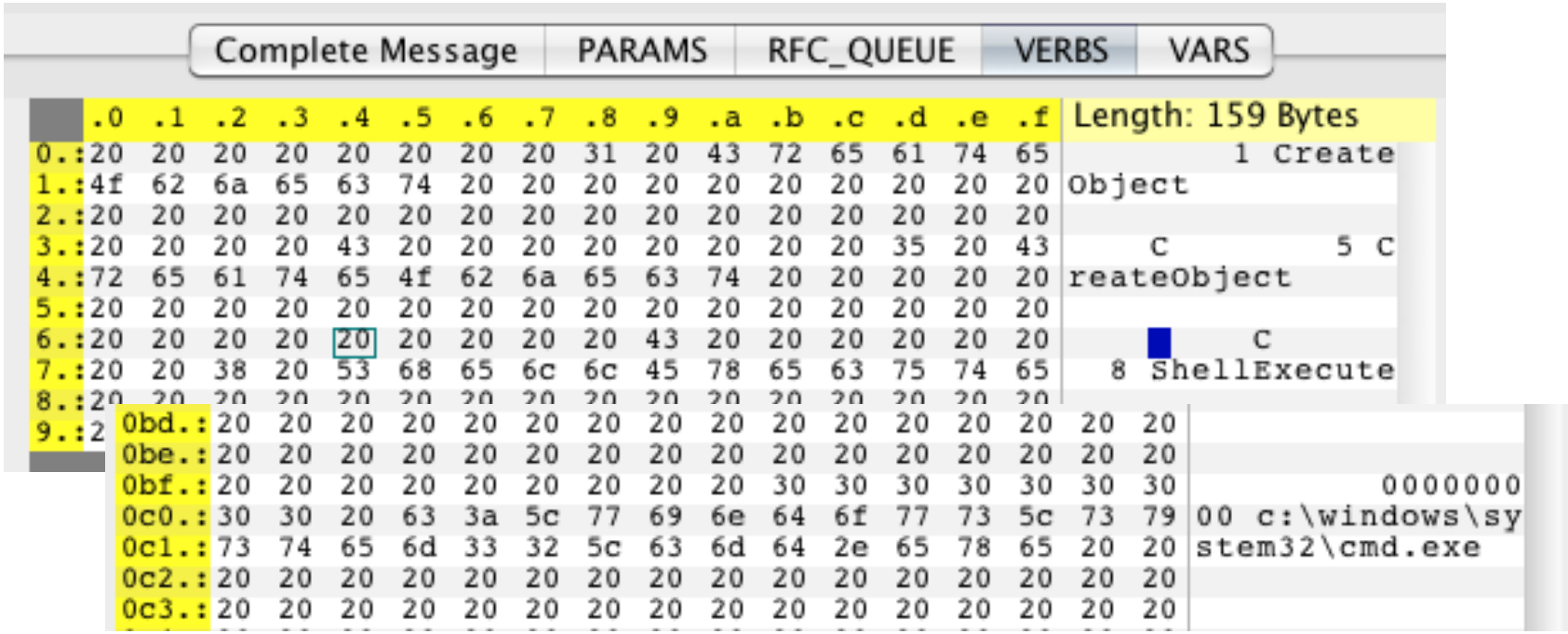
Client-Side Attacks

- cl_gui_frontend_services
  - Makes use of OLE



Client-Side Attacks

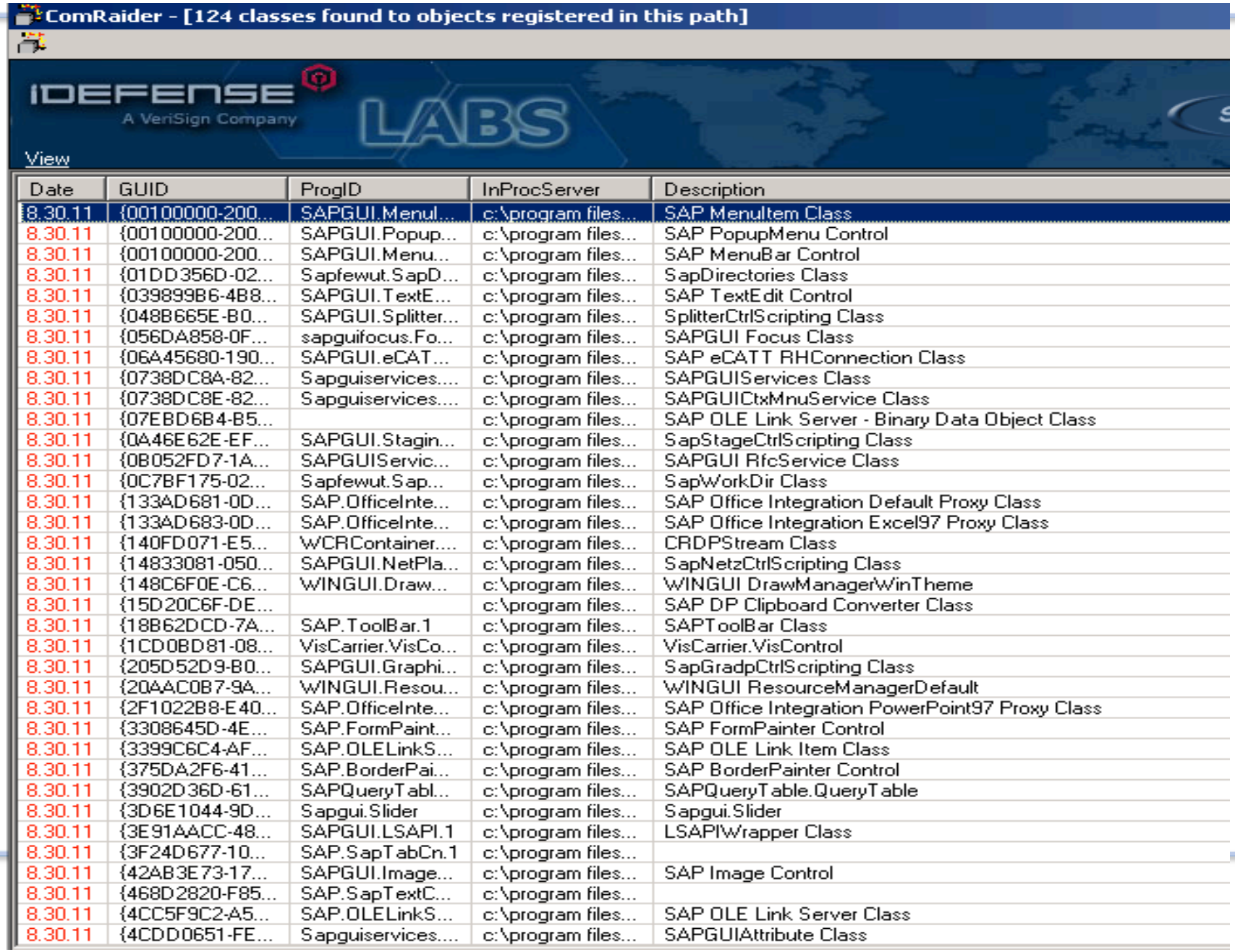
- cl_gui_frontend_services
  - Makes use of OLE



Client-Side Attacks

- SAP GUI provides number of COM libraries with potentially exploitable functions
  - Saved by the fact that the controls are not marked “Safe for Scripting”

Client-Side Attacks



Date	GUID	ProgID	InProcServer	Description
8.30.11	{00100000-200...	SAPGUI.Menul...	c:\program files...	SAP MenuItem Class
8.30.11	{00100000-200...	SAPGUI.Popup...	c:\program files...	SAP PopupMenu Control
8.30.11	{00100000-200...	SAPGUI.Menu...	c:\program files...	SAP MenuBar Control
8.30.11	{01DD356D-02...	Sapfewut.SapD...	c:\program files...	SapDirectories Class
8.30.11	{039899B6-4B8...	SAPGUI.TextE...	c:\program files...	SAP TextEdit Control
8.30.11	{048B665E-B0...	SAPGUI.Splitter...	c:\program files...	SplitterCtrlScripting Class
8.30.11	{056DA858-0F...	sapguifocus.Fo...	c:\program files...	SAPGUI Focus Class
8.30.11	{06A45680-190...	SAPGUI.eCAT...	c:\program files...	SAP eCATT RHConnection Class
8.30.11	{0738DC8A-82...	Sapguiservices....	c:\program files...	SAPGUIServices Class
8.30.11	{0738DC8E-82...	Sapguiservices....	c:\program files...	SAPGUICtxMnuService Class
8.30.11	{07EBD6B4-B5...		c:\program files...	SAP OLE Link Server - Binary Data Object Class
8.30.11	{0A46E62E-EF...	SAPGUI.Stagin...	c:\program files...	SapStageCtrlScripting Class
8.30.11	{0B052FD7-1A...	SAPGUIServic...	c:\program files...	SAPGUI RfcService Class
8.30.11	{0C7BF175-02...	Sapfewut.Sap...	c:\program files...	SapWorkDir Class
8.30.11	{133AD681-0D...	SAP.OfficeInte...	c:\program files...	SAP Office Integration Default Proxy Class
8.30.11	{133AD683-0D...	SAP.OfficeInte...	c:\program files...	SAP Office Integration Excel97 Proxy Class
8.30.11	{140FD071-E5...	WCRContainer....	c:\program files...	CRDPStream Class
8.30.11	{14833081-050...	SAPGUI.NetPla...	c:\program files...	SapNetzCtrlScripting Class
8.30.11	{148C6F0E-C6...	WINGUI.Draw...	c:\program files...	WINGUI DrawManagerWinTheme
8.30.11	{15D20C6F-DE...		c:\program files...	SAP DP Clipboard Converter Class
8.30.11	{18B62DCD-7A...	SAP.ToolBar.1	c:\program files...	SAPToolBar Class
8.30.11	{1CD0BD81-08...	VisCarrier.VisCo...	c:\program files...	VisCarrier.VisControl
8.30.11	{205D52D9-B0...	SAPGUI.Graphi...	c:\program files...	SapGradpCtrlScripting Class
8.30.11	{20AAC0B7-9A...	WINGUI.Resou...	c:\program files...	WINGUI ResourceManagerDefault
8.30.11	{2F1022B8-E40...	SAP.OfficeInte...	c:\program files...	SAP Office Integration PowerPoint97 Proxy Class
8.30.11	{3308645D-4E...	SAP.FormPaint...	c:\program files...	SAP FormPainter Control
8.30.11	{3399C6C4-AF...	SAP.OLELinkS...	c:\program files...	SAP OLE Link Item Class
8.30.11	{375DA2F6-41...	SAP.BorderPai...	c:\program files...	SAP BorderPainter Control
8.30.11	{3902D36D-61...	SAPQueryTabl...	c:\program files...	SAPQueryTable.QueryTable
8.30.11	{3D6E1044-9D...	Sapgui.Slider	c:\program files...	Sapgui.Slider
8.30.11	{3E91AACC-48...	SAPGUI.LSAPI.1	c:\program files...	LSAPIWrapper Class
8.30.11	{3F24D677-10...	SAP.SapTabCn.1	c:\program files...	
8.30.11	{42AB3E73-17...	SAPGUI.Image...	c:\program files...	SAP Image Control
8.30.11	{468D2820-F85...	SAP.SapTextC...	c:\program files...	
8.30.11	{4CC5F9C2-A5...	SAP.OLELinkS...	c:\program files...	SAP OLE Link Server Class
8.30.11	{4CDD0651-FE...	Sapguiservices....	c:\program files...	SAPGUIAttribute Class

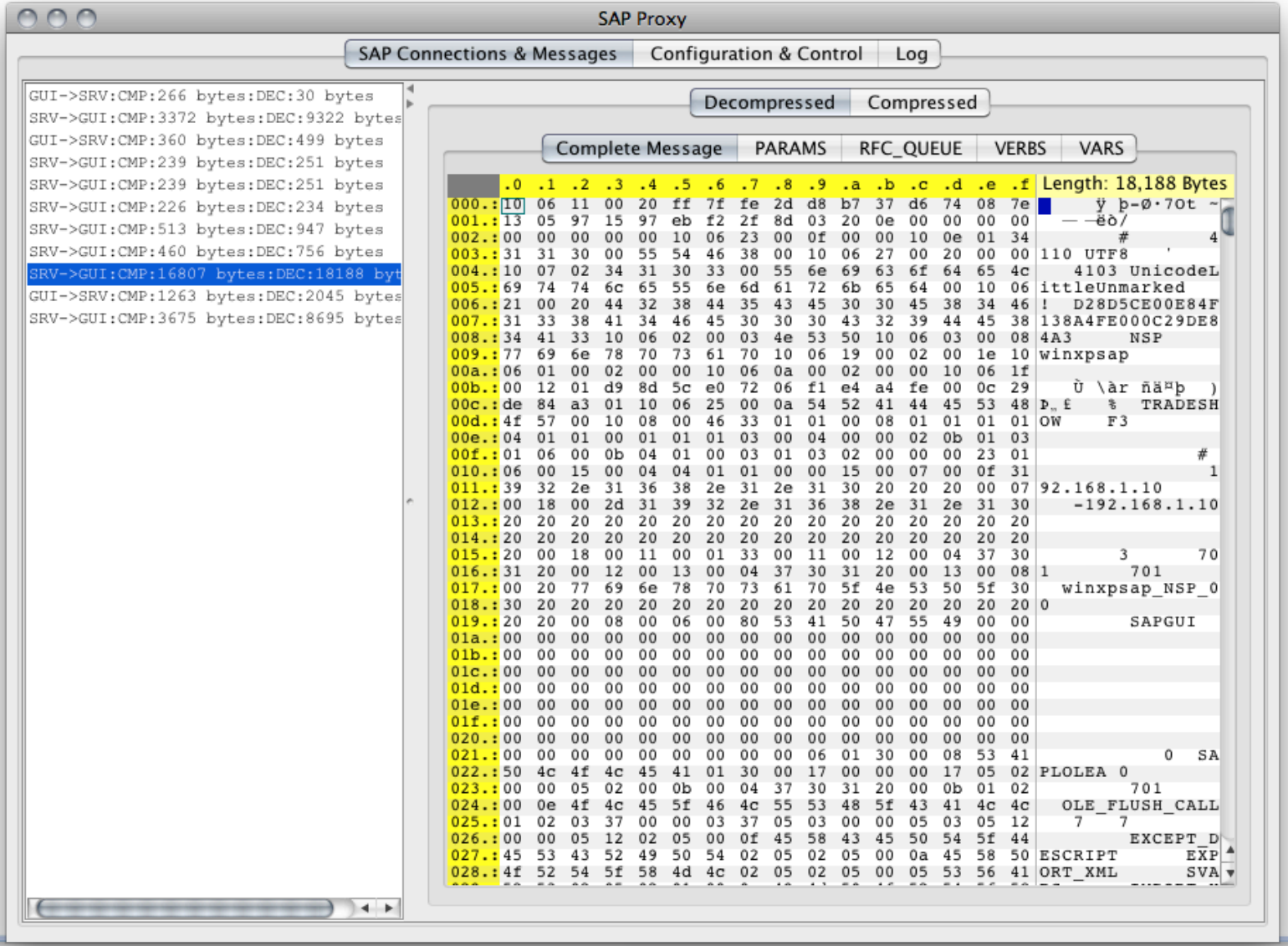
Client-Side Attacks

- SAP GUI provides number of COM libraries with potentially exploitable functions
  - Saved by the fact that the controls are not marked “Safe for Scripting”
- With SAPProxy we can potentially instantiate diverse COM objects

New (Old) Attacks ?

- Authorisation
- Authentication
- State Management
- Business Logic
- Validation
- Replay
- Client-Side attacks
- DoS

Demo: DoS


SAP Proxy
SAP Connections & Messages
Configuration & Control
Log
GUI->SRV:CMP:266 bytes:DEC:30 bytes
SRV->GUI:CMP:3372 bytes:DEC:9322 bytes
GUI->SRV:CMP:360 bytes:DEC:499 bytes
SRV->GUI:CMP:239 bytes:DEC:251 bytes
SRV->GUI:CMP:239 bytes:DEC:251 bytes
SRV->GUI:CMP:226 bytes:DEC:234 bytes
SRV->GUI:CMP:513 bytes:DEC:947 bytes
SRV->GUI:CMP:460 bytes:DEC:756 bytes
SRV->GUI:CMP:16807 bytes:DEC:18188 byt
GUI->SRV:CMP:1263 bytes:DEC:2045 bytes
SRV->GUI:CMP:3675 bytes:DEC:8695 bytes
Decompressed
Compressed
Complete Message
PARAMS
RFC_QUEUE
VERBS
VARS
Length: 18,188 Bytes

New (Old) Attacks ?

- Authorisation
- Authentication
- State Management
- Business Logic
- Validation
- Replay
- Client-Side attacks
- DoS
- *

What we're going to talk about

- ~~Why this Talk ?~~
- ~~The history of decompressing SAP DIAG~~
- ~~Understanding the fundamentals~~
- ~~New Attacks~~
- Conclusion

Conclusion

- A couple of factors have been common security knowledge for years…
  - Plain-text communication == #fail
  - Security by obscurity == #fail
- We now have a toolset and programmatic interface into SAP DIAG protocol
  - Game Changer
  - Change the way we look at ABAP
  - Happy Haxoring

Conclusion

- SAP provides encryption for client components in the form of Secure Network Communications
  - Provided by 3rd Parties
  - Provided by SAP
- SAP Clients should ensure the use of SNC is enabled and enforced

Questions ?

- www.sensepost.com/blog

ian@sensepost.com