

Introducing the Microsoft Vista Event Log File Format.



Andreas Schuster
Deutsche Telekom AG
Global Group Security
andreas.schuster@telekom.de



Vista Event Log Files. Agenda.

1. Introduction
2. The Outer Structure
3. The Inner Structure – Binary XML
 - 3.1 Token
 - 3.2 Substitution
 - 3.3 Templates
4. Forensic Practice
 - 4.1 Carving
 - 4.2 Interpretation of a Single Record
5. Conclusion



Vista Event Log Files.

Introduction.

- “Crimson” 2005, now “Windows Event Logging”
- truly new event logging service
- log file format obviously differs from that of NT family
- no parsers available beside the logging service
 - Vista required for analysis
 - doesn't operate on fragments of files



Vista Event Log Files.

Method.

- must not use any material that is under NDA
- no decompilation, restricted by German IP law
- clean-room analysis
 - clean install of Microsoft Vista Ultima RTM
 - normal system activity
 - 17 non-empty files, 2616 records
 - compare binary and textual representation
 - special conditions
 - flooding
 - unclean shutdown

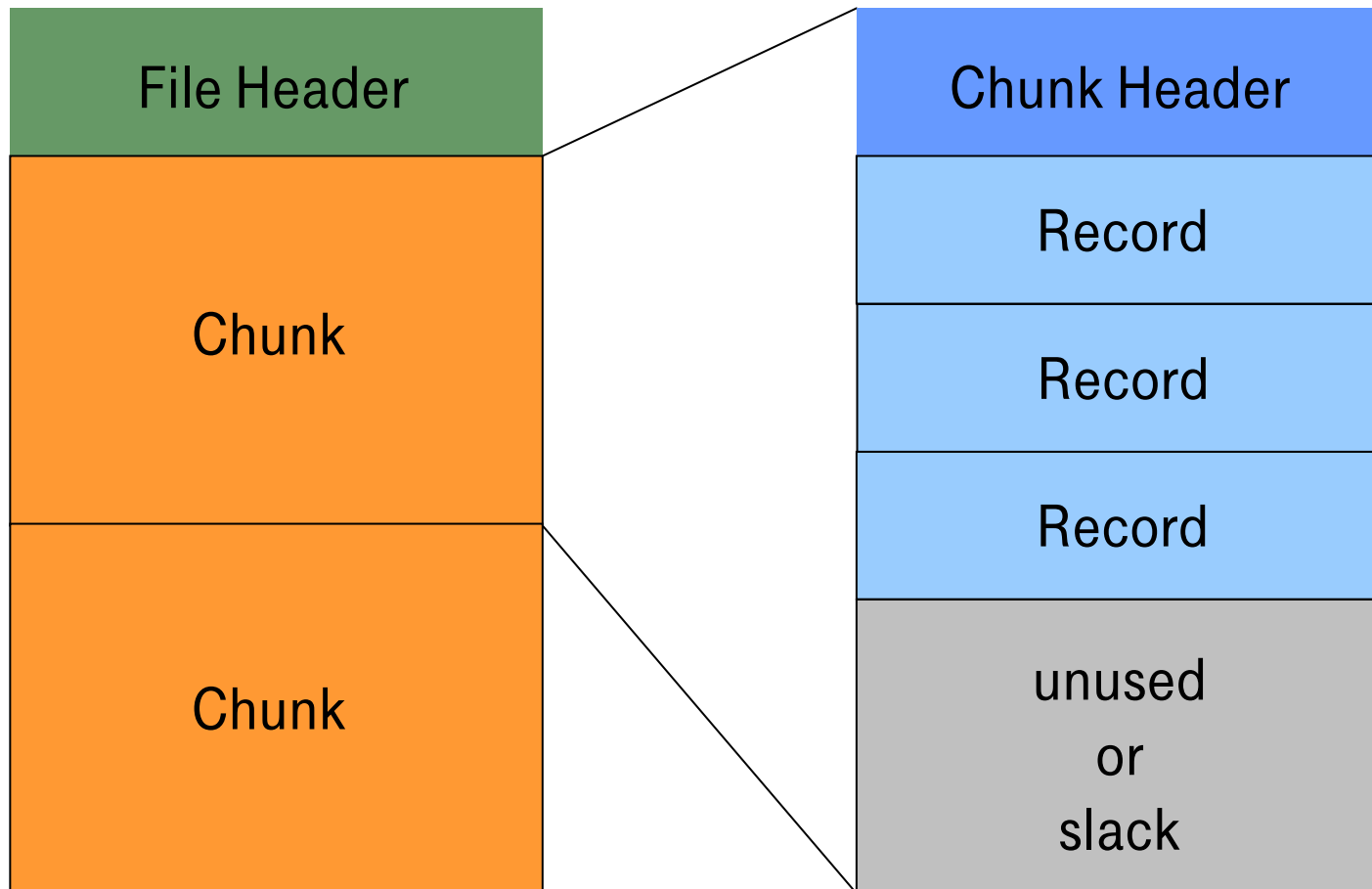


Vista Event Log Files. Tools.

- Scripts for the 010 Editor
 - outer structure (file to record)
 - SubstitutionArray
 - http://computer.forensikblog.de/files/010_templates/
- Framework (Perl) around a recursive-descent parser
 - outer structure
 - known system tokens, known data types
 - <http://computer.forensikblog.de/files/evtX/EvtXParser-1.0.0.zip>



The Outer Structure. Overview.



The Outer Structure. File.

- file header is permanently mapped into memory
- size 4096 bytes (= 1 physical memory page)
- only 128 Bytes are in use
- magic string “ElfFile”, 0x00
- version 3.1 (NT Event Log uses 1.1, Crimson 2.1)
- count of chunks
number of current chunk
- flags (DIRTY, FULL)
- integrity protected by CRC32 check sum



The Outer Structure. Chunk.

- from all chunks only the current one is mapped into memory
- size 64 kiB
- magic string “ElfChnk”, 0x00
- numbers of first/last event record
- integrity protected by CRC32 check sum



The Outer Structure. Event Record.

- magic string 0x2a 0x2a 0x00 0x00
- length near beginning and at the end
- record number (uint64)
- timestamp (FILETIME, 100ns since Jan 1st, 1601, 00:00:00)
- XML (“inner structure”)



Binary XML. Schema.

XML schema has been published on the MSDN web site.

```
<Events>
  <Event>
    <System>
      <EventID>1</EventID>
      <TimeCreated SystemTime="2006-10-
        08T09:21:28.415Z" />
      <EventRecordID>573</EventRecordID>
      ...
    </System>
    <EventData>
      ...
    </EventData>
  </Event>
</Events>
```



Binary XML.

Problems with Textual XML.

- disk utilization
 - low entropy
- CPU utilization
 - calculating block length
 - check for well-formedness

Solution: binary XML

- commonly found on smartphones



Binary XML. Tokenization.

XML language elements are replaced by tokens.

- system tokens („operators“)
- application tokens („operands“)
 - element/attribute names
 - XML templates



Binary XML. Tokenization.

Encoding of a start element tag:

< EventID >

becomes

#OpenStartElementTag#

EventID

#CloseStartElementTag#



Binary XML. Tokenization.

Encoding of a container element:

<EventID>1234</EventID>

becomes

#OpenStartElementTag#

EventID

#CloseStartElementTag#

1234

#EndElementTag#



Binary XML. Tokenization.

Value	Meaning	Example
0x00	EndOfBXmlStream	
0x01	OpenStartElementTag	< name >
0x02	CloseStartElementTag	< name >
0x03	CloseEmptyElementTag	< name />
0x04	End Element Tag	</ name >
0x05	Value	attribute = "value"
0x06	Attribute	attribute = "value"
0x0c	TemplateInstance	
0x0d	NormalSubstitution	
0x0e	OptionalSubstitution	
0x0f	StartOfBXmlStream	

Binary XML. Substitution.

Separating structure from content:

<EventID> 1234 <EventID/>

becomes

#OpenStartElementTag#

EventID

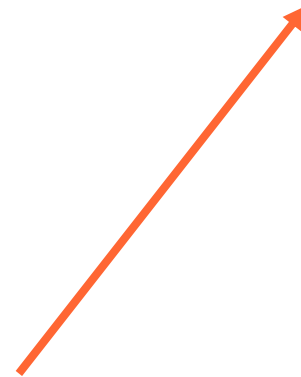
#CloseStartElementTag#

#NormalSubstitution# *Index n*

#EndElementTag#

Index	Length	Type
n-1
n	2	uint16
n+1

...
1234
...



Binary XML. Templates.

After the separation step many records share a common XML structure.
The structure is defined once (“template”) and applied multiple times.

Example:

- the same event message is submitted twice
- only timestamp and record number will differ



Binary XML Templates.

First record

Second record

```
1218h: 0F 01 01 00 0C 01 90 F4 0E 82 26 02 00 00 00 00 .....k.....
1228h: 00 00 90 F4 0E 82 26 0E BD 5D A6 E2 AB 6E 49 D1 .....j.i.b.f.f.
1238h: 00 0E 49 03 00 00 0F 01 01 00 41 13 00 3D 03 00 .....A.....
1248h: 00 4D 02 00 00 00 00 00 00 BA 0C 05 00 45 00 76 .....M.....E.V
1258h: 00 00 0E 08 00 74 00 00 00 87 00 00 06 68 02 .....h.....
1268h: 00 00 00 00 00 00 8C 0F 05 00 78 00 6D 00 6C 00 .....K.M.I.
1278h: 0E 00 73 00 00 00 05 01 35 00 68 00 74 00 74 00 .....S.h.c.t.
1288h: 70 00 3A 00 2E 00 2F 00 73 00 63 00 68 00 65 00 .....P.r.o.f.e.s.s.o.r
1298h: 6D 00 61 00 73 00 2E 00 5D 00 69 00 63 00 72 00 .....a.s.s.e.s.s.i.c.e.
12A8h: 0F 00 73 00 6F 00 66 00 74 00 2E 00 63 00 6F 00 .....O.r.g.a.n.i.z.a.t.i.o.n
12B8h: 6D 00 2F 00 77 00 69 00 6E 08 2F 00 32 00 30 00 .....m.v.w.i.n./2.0.
12C8h: 00 34 00 2E 00 30 00 38 00 2F 00 00 00 76 00 .....O.f.f.i.c.e.
12D8h: 65 0E 6E 74 00 00 00 2E 00 55 00 7E 00 00 00 .....S.o.f.t.w.a.r.e.
12E8h: 0E 00 74 00 02 01 FF FF 8D 02 00 00 F8 02 00 00 .....h.t.t.p.
12F8h: 00 00 00 00 6F 34 06 00 53 00 71 00 73 00 74 00 .....C.o.m.p.a.n.y
1308h: 65 00 6D 00 00 00 D2 41 FF FF 52 00 00 00 1A 03 .....e.m.a.i.l
1318h: 00 00 00 00 00 00 7B 00 00 00 00 00 00 00 00 .....I.P.A.D
1328h: 76 00 69 00 64 00 65 00 72 00 00 00 2F 00 00 00 .....v.i.d.e.o
1338h: 06 00 03 00 00 00 00 00 00 00 00 4E 00 61 00 .....C.o.m.p.a.n.y
1348h: 00 6D 00 65 00 00 00 05 01 0A 00 55 00 73 00 65 .....m.e.s.s.a.g.e
1358h: 00 72 00 20 00 45 00 76 00 65 00 68 00 74 00 03 .....r.e.s.p.o.n.s.e
1368h: 41 03 00 82 00 00 00 73 03 00 00 00 00 00 FF .....A.w.a.r.d
1378h: 61 07 00 45 00 76 00 65 00 68 00 74 00 49 00 44 .....a.s.s.e.s.s.i.c.e
1388h: 00 00 00 27 00 00 06 94 03 00 00 00 00 00 00 .....
1398h: 29 DA 0A 00 51 00 75 00 61 00 6C 00 69 00 66 00 .....C.o.u.s.a.l.i.f.
13A8h: 69 00 65 00 72 00 73 00 00 0E 04 00 06 02 0E .....e.s.s.
13B8h: 03 00 06 04 01 00 00 1E 00 00 00 C7 03 00 00 00 .....
13C8h: 00 00 06 64 C8 05 00 4C 00 65 00 76 00 65 00 6C .....d.i.v.e.r.s.e.
13D8h: 00 00 02 0E 00 00 04 94 03 02 00 1C 00 00 00 .....
13E8h: 2C 03 00 00 00 00 00 45 7B 04 00 54 00 61 00 .....E.T.a.s.
13F8h: 73 00 68 00 00 02 0E 02 00 06 04 01 05 00 24 .....E.M.S.
1408h: 00 00 00 0F 04 00 00 00 00 00 6A CF 08 00 48 .....j.j.k
1418h: 00 65 00 79 00 77 00 6F 00 72 00 64 00 73 00 00 .....S.Y.W.O.R.D.S
1428h: 00 02 0E 05 00 15 04 41 FF FF 50 00 00 00 3A 04 .....A.P.P.
1438h: 00 00 00 00 00 00 2B 8E 08 00 54 00 69 00 6D 00 .....j.j.k
1448h: 65 00 43 00 72 00 65 00 61 00 74 00 65 00 64 00 .....E.V.E.N.T.S
1458h: 00 00 27 00 00 00 06 63 04 00 00 6A 02 00 00 3C .....C.I.P.
1468h: 78 0A 00 53 00 79 00 73 00 74 00 65 00 60 00 54 .....I.M.S.
1478h: 00 69 00 6D 00 65 00 00 00 08 06 00 11 03 01 0A .....I.M.S.
1488h: 00 2E 00 00 00 51 04 00 00 00 00 00 00 00 00 .....E.V.E.N.T.S
1498h: 00 45 00 76 00 65 00 6E 00 74 00 52 00 65 00 63 .....E.V.E.N.T.S
14A8h: 00 6F 00 72 00 64 00 69 00 44 00 00 62 08 0A .....O.V.E.R.I.D
14B8h: 00 DA 04 03 FF FF 38 00 00 00 C6 04 00 00 00 00 .....
14C8h: 00 00 83 61 07 00 43 00 68 00 61 00 68 00 68 00 .....C.H.A.N.G.E
14D8h: 65 00 6C 00 00 02 05 01 08 00 41 00 70 00 73 .....E.V.E.N.T.S
14E8h: 00 6C 00 69 00 63 00 61 00 74 00 69 00 6F 00 6E .....I.I.C.A.T.I.O.N
14F8h: 00 04 01 FF FF 36 00 00 05 05 00 3A 04 00 00 .....E.V.E.N.T.S
1508h: 00 3B 6E 08 00 43 00 6F 00 6D 00 70 00 75 00 74 .....j.n.C.o.m.p.u.t.e.r
1518h: 00 65 00 72 00 60 00 02 05 01 09 00 56 00 69 00 .....e.v.e.n.t.s
1528h: 73 00 74 00 63 00 00 00 56 00 54 00 4D 00 04 41 .....E.V.E.N.T.S
1538h: FF FF 42 00 00 00 42 05 00 00 00 00 00 00 A0 2E .....B.....
1548h: 08 00 63 00 65 00 63 00 75 00 72 00 69 00 74 00 .....E.V.E.N.T.S
1558h: 79 00 00 00 1F 00 00 06 65 05 00 00 00 00 00 .....V.....
1568h: 00 66 4C 06 00 55 00 73 00 65 00 72 00 49 00 44 .....I.I.C.A.T.I.O.N
1578h: 00 00 00 0C 00 13 03 04 0E 13 00 21 04 00 14 .....
1588h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1598h: 00 06 00 02 00 06 00 08 00 15 00 08 00 11 00 00 .....
15A8h: 00 00 00 04 00 08 00 04 00 08 00 08 00 0A 00 01 .....
15B8h: 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
15C8h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
15D8h: 00 21 00 04 00 00 98 10 00 00 00 00 00 00 00 .....d.....
15E8h: 00 80 00 00 34 9F 64 1D 90 C7 03 00 00 00 00 00 .....
15F8h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1608h: 0C 01 46 D3 BC 12 06 00 08 00 00 00 00 00 03 46 .....F.....
1618h: D3 BC 25 02 67 38 86 39 D7 78 70 28 1C B9 78 00 .....S.p.r.i.n.g
1628h: 00 00 0F 03 01 01 01 FF FF 6C 00 00 39 0E 00 .....S.....
1638h: 00 00 00 00 44 82 09 00 45 00 76 00 65 00 6E .....D.I.V.E.S.T
1648h: 00 74 00 46 00 61 00 74 00 63 00 00 02 03 00 .....E.V.E.N.T.S
1658h: 00 1C 00 00 00 61 06 00 00 00 00 00 00 8A 6F 04 .....a.....
1668h: 00 44 00 00 00 64 61 00 00 00 02 00 00 81 .....D.A.T.A
1678h: 04 01 02 00 20 00 00 00 84 06 00 00 00 00 00 .....
1688h: 61 98 60 60 60 60 60 60 60 60 60 60 60 60 60 .....
1698h: 00 00 02 08 02 00 0E 04 04 00 03 00 00 00 20 00 .....
16A8h: 81 00 04 00 08 00 00 00 00 54 00 65 00 73 00 .....E.V.E.N.T.S
16B8h: 74 00 20 00 41 00 74 00 6F 00 74 00 6F 00 63 00 .....E.V.E.N.T.S
16C8h: 63 00 69 00 75 00 70 00 00 00 00 00 00 00 00 .....C.K.U.P.
16D8h: 80 A2 76 22 .....*
```

```
16F8h: 0F 01 01 00 0C 01 90 F4 0E 82 26 02 00 00 14 00 .....k.....
1708h: 06 00 02 00 06 00 08 00 15 00 08 00 11 00 00 00 .....
1728h: 00 00 04 00 08 00 04 00 08 00 08 00 0A 00 01 00 .....
1738h: 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1748h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....C.
1758h: 21 00 04 00 00 00 9F 10 00 00 00 00 00 00 00 .....
1768h: 80 00 00 04 9F 64 1D 90 C7 01 00 00 00 00 00 .....
1778h: 00 00 00 00 00 00 00 00 00 00 0F 01 01 00 0C .....C.I.
1788h: 01 01 46 D3 BC 12 06 00 00 03 00 00 20 00 81 .....F.....
1798h: 00 04 00 08 00 00 00 00 54 00 65 00 73 00 74 .....T.E.M.P.
17A8h: 00 20 00 41 00 75 00 74 00 6F 00 42 00 61 00 63 .....A.U.T.H.O.R.I.T.Y
17B8h: 00 68 00 75 00 70 00 00 00 00 00 00 00 00 03 .....k.u.p.
17C8h: 00 17 00 00 .....

```

binary XML structure

substitution array



Binary XML.

Summary.

- 3-step process
 - tokenization
 - substitution
 - templates
- results in compact binary XML



Forensic Practice.

Carving – Whole File.

- header with magic string „ElfFile“
- no footer
- file size = 4 kiB + chunks * 64 kiB
- use evtxdump.pl or system service to transform the carved (binary) file into text



Forensic Practice.

Carving – Single Chunk.

- header with magic string „ElfChunk“
- no footer
- size = 64 kiB
- use evtxdump.pl to transform into text



Forensic Practice.

Carving – Single Record.

- header with magic string 0x2a 0x2a 0x00 0x00
- no fixed footer
- size is variable, but known



Forensic Practice.

Interpretation of a Single Record.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
2A	2A	00	00	FO	00	00	00	43	21	00	00	00	00	00	00	**
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	
0E	82	26	02	00	00	14	00	00	00	01	00	04	00	01	00	
04	00	02	00	06	00	02	00	06	00	02	00	06	00	08	00	
15	00	08	00	11	00											
08	00	08	00	0A	00											
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	43	00	21	00	04	00	00	00	9F	10	
00	00	00	00	00	00	00	00	80	00	00	E4	9F	64	1D	90	
C7	01	00	00	00	00	00	00	00	00	43	21	00	00	00	00	
00	00	00	0F	01	01	00	0C	01	01	46	D3	EC	12	06	00	
00	03	00	00	00	20	00	81	00	04	00	08	00	00	00	00	
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	
00	00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	
2A	2A	00	00	FO	00	00	00	44	21	00	00	00	00	00	00	**	

magic string

Forensic Practice.

Interpretation of a Single Record.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
2A	2A	00	00	FO	00	00	00	43	21	00	00	00	00	00	00	**
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	
0E	82	26	02	00	00	14	00	00	00	01	00	04	00	01	00	
04	00	02	00	06	00	02	00	06	00	02	00	06	00	08	00	
15	00	08	00	11	00	00	00	00	00	04	00	08	00	04	00	
08	00	08	00	0A	00	01	00	04	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	9F	10	
00	00	00	00	00	00	00	00	00	00	00	00	E4	9F	64	1D	90	
C7	01	00	00	00	00	00	00	00	00	00	43	21	00	00	00	
00	00	00	0F	01	01	00	0C	01	01	46	D3	EC	12	06	00	
00	03	00	00	00	20	00	81	00	04	00	08	00	00	00	00	
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	
00	00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	
2A	2A	00	00	FO	00	00	00	44	21	00	00	00	00	00	00	**	

record length



Forensic Practice.

Interpretation of a Single Record.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
2A	2A	00	00	FO	00	00	00	43	21	00	00	00	00	00	00	**
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	
0E	82	26	02	00	00	14	00	00	00	00	01	00	04	00	01	
04	00	02	00	06	00	02	00	06	00	02	00	06	00	08	00	
15	00	08	00	11	00	00	00	00	00	04	00	08	00	04	00	
08	00	08	00	0A	00	01	00	04	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	04	00	00	00	00	00	00	00	9F	10	
00	00	00	00	00	00	00	00	80	00	00	E4	9F	64	1D	90	
C7	01	00	00	00	00	00	00	00	00	43	21	00	00	00	00	
00	00	00	0F	01	01	00	0C	01	01	46	D3	EC	12	06	00	
00	03	00	00	00	20	00	81	00	04	00	08	00	00	00	00	
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	
00	00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	
2A	2A	00	00	FO	00	00	00	44	21	00	00	00	00	00	00	**	

start of BXml



Forensic Practice.

Interpretation of a Single Record.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2A	2A	00	00	FO	00	00	00	43	21	00	00	00	00	00	00	**
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	
0E	82	26	02	00	00	14	00	00	00	01	00	04	00	01	00	
04	00	02	00	06	00	02	00	06	00	02	00	06	00	08	00	
15	00	08	00	11	00	00	00	00	00	04	00	08	00	04	00	
08	00	08	00	0A	00	01	00	04	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	03	00	00	00	20	00	81	00	04	00	08	00	00	00	00	
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	
00	00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	
2A	2A	00	00	FO	00	00	00	44	21	00	00	00	00	00	00	**	

create
template
instance



Forensic Practice.

Interpretation of a Single Record.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2A	2A	00	00	FO	00	00	00	43	21	00	00	00	00	00	00	**
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	
0E	82	26	02	00	00	14	00	00	00	01	00	04	00	01	00	
04	00	02	00	06	00	02	00	06	00	02	00	06	00	08	00	
15	00	08	00	11	00	00	00	00	00	04	00	08	00	04	00	
08	00	08	00	0A	00	01	00	04	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	03	00	00	00	20	00	81	00	04	00	08	00	00	00	00		
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74		
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00		
00	00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00		
2A	2A	00	00	FO	00	00	00	44	21	00	00	00	00	00	00	**		

template ID
(DWORD)

Forensic Practice.

Interpretation of a Single Record.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
2A	2A	00	00	FO	00	00	00	43	21	00	00	00	00	00	00	**
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	
0E	82	26	02	00	00	14	00	00	00	01	00	04	00	01	00	
04	00	02	00	06	00	02	00	06	00	02	00	06	00	08	00	
15	00	08	00	11	00	00	00	00	00	04	00	08	00	04	00	
08	00	08	00	0A	00	01	00	04	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	03	00	00	00	20	00	81	00	04	00	08	00	00	00	00	
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	
00	00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	
2A	2A	00	00	FO	00	00	00	44	21	00	00	00	00	00	00	**	

template
offset
(DWORD)

Forensic Practice.

Interpretation of a Single Record.

- Problem: XML template requested, but not available
- XML schema: „System“ is a mandatory element
- observation: static mapping between element/attribute and index into substitution array
- use evttemplates.pl to view:

```
<Event xmlns="...">
  <System>
    <EventID Qualifiers="#4 (type 6, optional)#"
      #3 (type 6, optional)#
    </EventID>
```

Forensic Practice.

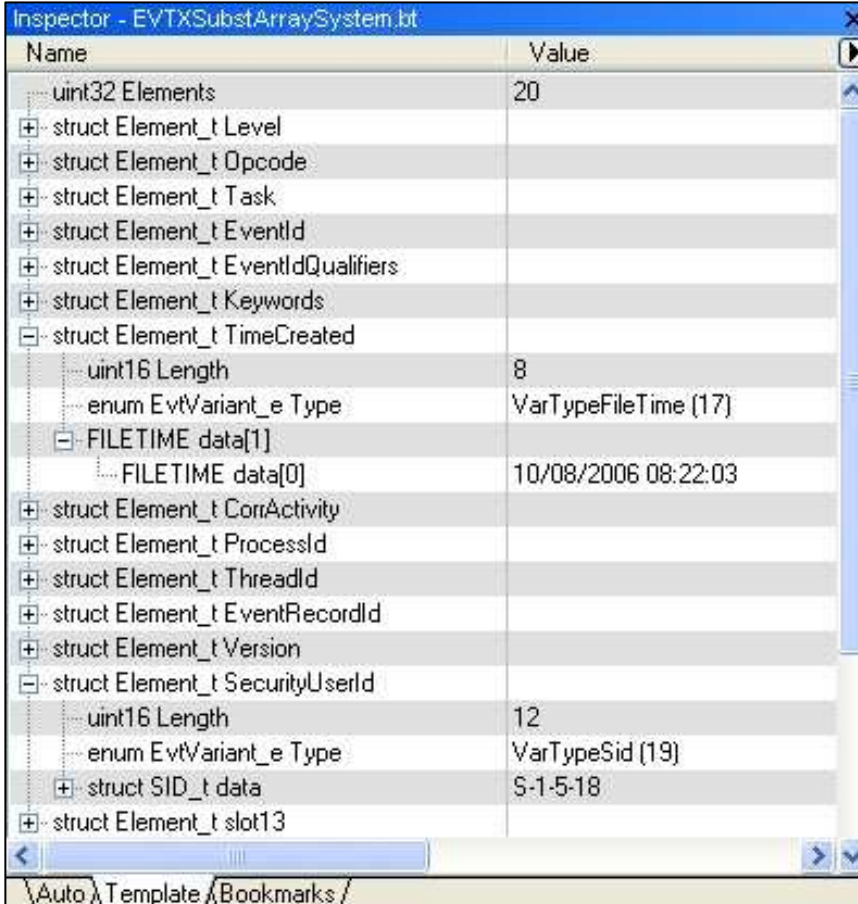
Interpretation of a Single Record - Locate SubstitutionArray.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
2A	2A	00	00	FO	00	00	00	43	21	00	00	00	00	00	00	**
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	
0E	82	26	02	00	00	14	00	00	00	01	00	04	00	01	00	
04	00	02	00	06	00	02	00	06	00	02	00	06	00	08	00	
15	00	08	00	11	00	00	00	00	00	04	00	08	00	04	00	
08	00	08	00	0A	00	01	00	04	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	03	00	00	00	20	00	81	00	04	00	08	00	00	00	00	
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	
00	00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	
2A	2A	00	00	FO	00	00	00	44	21	00	00	00	00	00	00	**	

start of substitution array

Forensic Practice.

Interpretation of a Single Record.



The screenshot shows the 'Inspector' window for an event log record. The window title is 'Inspector - EVT_XSubstArraySystem.bt'. It displays a tree view of the record's structure with two columns: 'Name' and 'Value'. The structure is as follows:

Name	Value
uint32 Elements	20
struct Element_t Level	
struct Element_t Opcode	
struct Element_t Task	
struct Element_t EventId	
struct Element_t EventIdQualifiers	
struct Element_t Keywords	
struct Element_t TimeCreated	
uint16 Length	8
enum EvVariant_e Type	VarTypeFileTime (17)
FILETIME data[1]	
FILETIME data[0]	10/08/2006 08:22:03
struct Element_t CorrActivity	
struct Element_t ProcessId	
struct Element_t ThreadId	
struct Element_t EventRecordId	
struct Element_t Version	
struct Element_t SecurityUserId	
uint16 Length	12
enum EvVariant_e Type	VarTypeSid (19)
struct SID_t data	S-1-5-18
struct Element_t slot13	

Forensic Practice.

Interpretation of a Single Record - Validation.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
2A	2A	00	00	FO	00	00	00	43	21	00	00	00	00	00	00	**
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	
0E	82	26	02	00	00	14	00	00	00	01	00	04	00	01	00	
04	00	02	00	06	00	02	00	06	00	02	00	06	00	08	00	
15	00	08	00	11	00	00	00	00	00	04	00	08	00	00	00	
08	00	08	00	0A	00	01	00	04	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	43	00	21	00	04	00	00	00	9F	10	
00	00	00	00	00	00	00	00	80	00	00	E4	9F	64	1D	90	
C7	01	00	00	00	00	00	00	00	00	43	21	00	00	00	00	
00	00	00	0F	01	01	00	0C	01	01	46	D3	EC	12	06	00	
00	03	00	00	00	20	00	81	00	04	00	08	00	00	00	00	
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	
00	00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	
2A	2A	00	00	FO	00	00	00	44	21	00	00	00	00	00	00	**	

EventRecordId

Forensic Practice.

Interpretation of a Single Record - Validation.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
2A	2A	00	00	FO	00	00	00	43	21	00	00	00	00	00	00	**
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	
0E	82	26	02	00	00	14	00	00	00	01	00	04	00	01	00	
04	00	02	00	06	00	02	00	06	00	02	00	06	00	08	00	
15	00	08	00	11	00	00						08	00	04	00	
08	00	08	00	0A	00	01						00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	43	00	21	00	04	00	00	00	9F	10	
00	00	00	00	00	00	00	00	80	00	00	E4	9F	64	1D	90	
C7	01	00	00	00	00	00	00	00	00	43	21	00	00	00	00	
00	00	00	0F	01	01	00	0C	01	01	46	D3	EC	12	06	00	
00	03	00	00	00	20	00	81	00	04	00	08	00	00	00	00	
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	
00	00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	
2A	2A	00	00	FO	00	00	00	44	21	00	00	00	00	00	00	**	

TimeCreated

Forensic Practice.

Interpretation of a Single Record.

Recovered data:

- EventID
- Keywords
- TimeCreated
- ProcessID
- ThreadID
- User SID
- Level, Task, Opcode
- Version

Lost data:

- XML namespace
- provider (data source)
- channel
- computer name



Conclusion.

Improvements.

- low memory load, only 68 kiB per log
 - the old service keeps the whole file in memory
- rich set of data types (strings, numbers, special types)
 - the old service only supports strings and binary
- XPath queries

- It's less likely that administrators turn logging off.
- It's more likely that programmers instrument their code for logging.



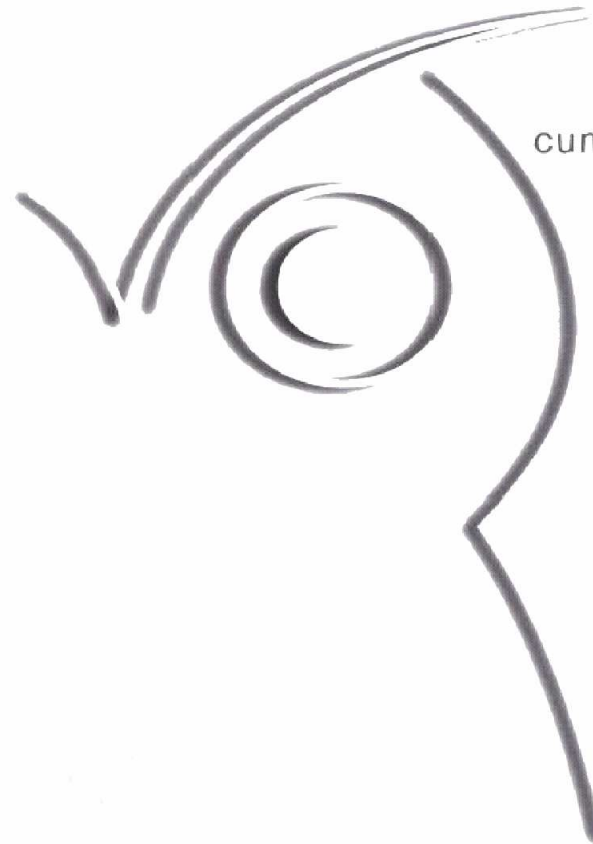
Conclusion.

Parsers.

- Vista Event Viewer Applet by Microsoft for uncorrupted files.
- EvtxParser
 - platform-independent (Perl)
 - works on corrupted files
 - some data types are missing
 - some system tokens are missing
CDATA, PI, EntityRef?



Questions?



cum sapientia protegimus

Thank You for Your Attention.



Andreas Schuster
Deutsche Telekom AG
Global Group Security
andreas.schuster@telekom.de



Forensic Practice.

Interpretation of a Single Record - Locate SubstitutionArray.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
2A	2A	00	00	EO	04	00	00	42	21	00	00	00	00	00	00	**
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	
0E	82	26	02	00	00	00	00	00	00	90	F4	0E	82	3B	8E	
BD	(5D)	A6	62	AB	66	49	D1	10	DB	49	03	00	00	0F	01	
01	00	41	13	00	3D	03										
00	BA	0C	05	00	45	00										
06	65	05	00	00	00	00										
00	65	00	72	00	49	00	44	00	00	00	0E	0C	00	13	03	
04	0E	13	00	21	04	00	14	00	00	00	01	00	04	00	01	
00	04	00	02	00	06	00	02	00	06	00	02	00	06	00	08
00	15	00	08	00	11	00	00	00	00	00	04	00	08	00	04
00	00	54	00	65	00	73	00	74	00	20	00	41	00	75	00
74	00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00
00	00	00	00	00	00	00	00	80	A2	76	22	EO	04	00	00

repeated
template ID