



Introducing the Microsoft Vista Log File Format

By

Andreas Schuster

Presented At

The Digital Forensic Research Conference

DFRWS 2007 USA Pittsburgh, PA (Aug 13th - 15th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

<http://dfrws.org>

Introducing the Microsoft Vista Event Log File Format.



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

.....T

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

..... T



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 2

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 3

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



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 3

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 4

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

..... T



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 4

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 5

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>

..... T

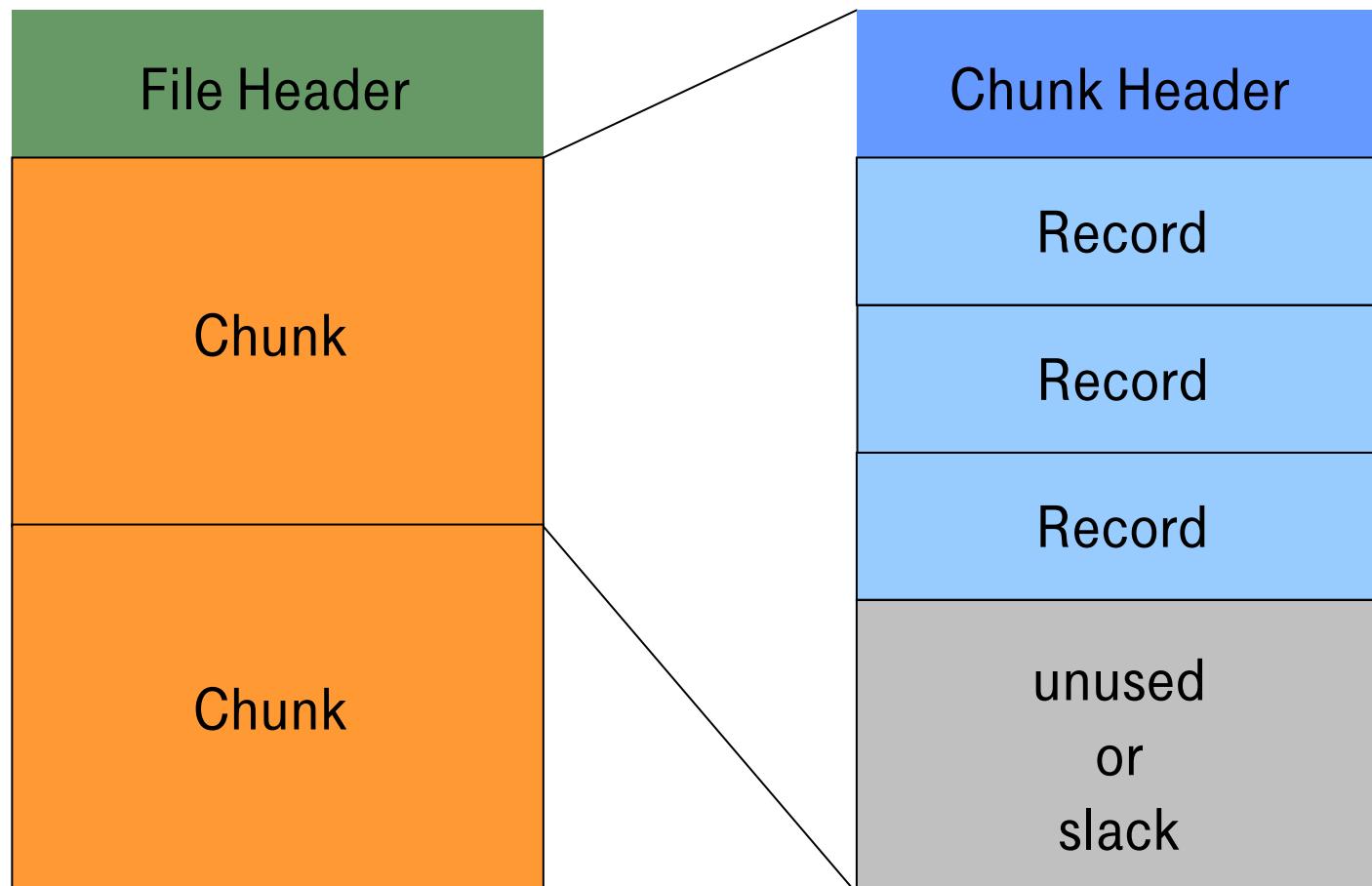


Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 5

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 6

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



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 7

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 8

The Outer Structure.

Chunk.

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

..... T



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 8

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 9

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”)

..... T



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 9

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 10

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>
```



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 10

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 11

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



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 11

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 12

Binary XML.

Tokenization.

XML language elements are replaced by tokens.

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



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 12

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 13

Binary XML. Tokenization.

Encoding of a start element tag:

< EventID >

becomes

#OpenStartElementTag#

EventID

#CloseStartElementTag#



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 13

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 14

Binary XML. Tokenization.

Encoding of a container element:

<EventID>1234</EventID>

becomes

#OpenStartElementTag#

EventID

#CloseStartElementTag#

1234

#EndElementTag#



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 14

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 15

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

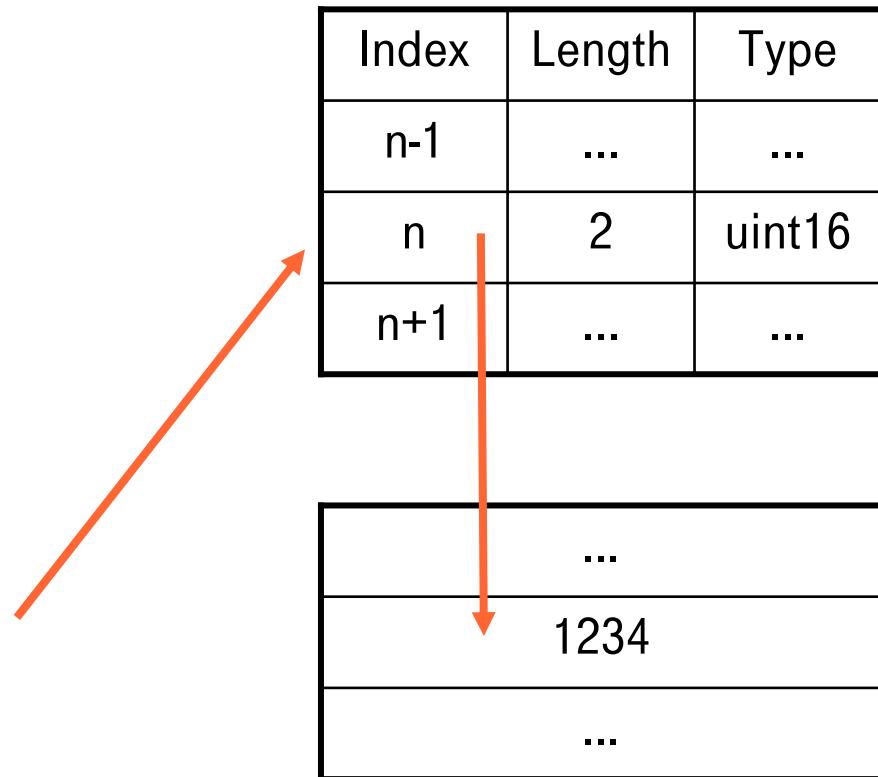
#OpenStartElementTag#

EventID

#CloseStartElementTag#

#NormalSubstitution# *Index n*

#EndElementTag#



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 16

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 17

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



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 17

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 18

Binary XML. Templates.

First record

Second record

binary XML structure

substitution
array



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 18

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 19

Binary XML.

Summary.

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

..... T



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 19

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 20

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

..... T



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 20

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 21

Forensic Practice.

Carving – Single Chunk.

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

..... T



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 21

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 22

Forensic Practice.

Carving – Single Record.

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

..... T



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 22

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 23

Forensic Practice.

Interpretation of a Single Record.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
	2A	2A	00	00	F0	00	00	00	43	21	00	00	00	00	00	00	* * C !
	00	E4	9F	54	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	. . . d
	DE	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							00	00	00	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	80	00	00	E4	9F	64	1D	90	 d . .	
	C7	01	00	00	00	00	00	00	00	43	21	00	00	00	00	 C ! . . .
	00	00	00	0F	01	01	00	0C	01	01	46	D3	EC	12	06	00 F
	00	03	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	. T.e.s.t. . A.u.t
	00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	. o.B.a.c.k.u.p..
	00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	
	2A	2A	00	00	F0	00	00	00	44	21	00	00	00	00	00	00	* * D !



Forensic Practice.

Interpretation of a Single Record.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
2A	2A	00	00	F0	00	00	00	43	21	00	00	00	00	00	00	**...C!....
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	...d.....
DE	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 10C.!....
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00d..
C7	01	00	00	00	00	00	00	00	00	43	21	00	00	00	00C!....
00	00	0F	01	01	00	0C	01	01	46	D3	EC	12	06	00	00F....
00	03	00	00	20	00	81	00	04	00	08	00	00	00	00	00
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	.T.e.s.t. .A.u.t
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	.o.B.a.c.k.u.p..
00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	00
2A	2A	00	00	F0	00	00	00	44	21	00	00	00	00	00	00	**...D!....



Forensic Practice.

Interpretation of a Single Record.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
2A	2A	00	00	F0	00	00	00	43	21	00	00	00	00	00	00	**...C!....
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	...d.....
DE	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	0	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	4	start of BXml	00	00	00	00	00	9F	10C.!....
00	00	00	00	00	00	00	00	80	00	00	E4	9F	64	1D	90d..
C7	01	00	00	00	00	00	00	00	00	43	21	00	00	00	00C!....
00	00	0F	01	01	00	0C	01	01	46	D3	EC	12	06	00	00F....
00	03	00	00	20	00	81	00	04	00	08	00	00	00	00	00
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	.T.e.s.t. .A.u.t
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	.o.B.a.c.k.u.p..
00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	00
2A	2A	00	00	F0	00	00	00	44	21	00	00	00	00	00	00	**...D!....



Forensic Practice.

Interpretation of a Single Record.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
2A	2A	00	00	F0	00	00	00	43	21	00	00	00	00	00	00	**...C!....
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	...d.....
DE	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	0	create template instance				00	00	00	00
00	00	00	00	00	00	04					00	00	00	9F	10C!....
00	00	00	00	00	00	00					E4	9F	64	1D	90d..
C7	01	00	00	00	00	00					21	00	00	00	00C!....
00	00	00	0F	01	01	00					D3	EC	12	06	00F....
00	03	00	00	20	00	81	00	04	00	08	00	00	00	00	00
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	.T.e.s.t. .A.u.t
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	.o.B.a.c.k.u.p..
00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	00
2A	2A	00	00	F0	00	00	00	44	21	00	00	00	00	00	00	**...D!....



Forensic Practice.

Interpretation of a Single Record.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
2A	2A	00	00	F0	00	00	00	43	21	00	00	00	00	00	00	**...C!....
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	...d.....
DE	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	0	template ID (DWORD)				00	00	00	00
00	00	00	00	00	00	00	4					00	00	00	9F 10C!....
00	00	00	00	00	00	00	0					E4	9F	64	1D 90d....
C7	01	00	00	00	00	00	00	43	21	00	00	00	00	00	00C!....
00	00	0F	01	01	00	0C	01	01	46	D3	EC	12	06	00	00F....
00	03	00	00	20	00	81	00	04	00	08	00	00	00	00	00
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	.T.e.s.t. .A.u.t
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	.o.B.a.c.k.u.p..
00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	00
2A	2A	00	00	F0	00	00	00	44	21	00	00	00	00	00	00	**...D!....



Forensic Practice.

Interpretation of a Single Record.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
2A	2A	00	00	F0	00	00	00	43	21	00	00	00	00	00	00	**...C!....
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	...d.....
DE	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	0	template offset (DWORD)				00	00	00	00
00	00	00	00	00	00	04					00	00	00	9F	10C!....
00	00	00	00	00	00	00					E4	9F	64	1D	90d..
C7	01	00	00	00	00	00					21	00	00	00	00C!....
00	00	0F	01	01	0					D3	EC	12	06	00F....	
00	03	00	00	20	00	81	00	04	00	08	00	00	00	00	00
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	.T.e.s.t. .A.u.t
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	.o.B.a.c.k.u.p..
00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	00
2A	2A	00	00	F0	00	00	00	44	21	00	00	00	00	00	00	**...D!....



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 evtxtemplates.pl to view:

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



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 29

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 30

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	0123456789ABCDEF
2A	2A	00	00	F0	00	00	00	43	21	00	00	00	00	00	**...C!....	
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	
DE	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	0	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	4	start of substitution array				00	00	00	9F 10	
00	00	00	00	00	00	00	0	E4	9F	64	1D	90	21	00	00	
C7	01	00	00	00	00	00	0	00	00	00	00	00	00	00	00	
00	00	00	0F	01	01	0	00	03	EC	12	06	00	00	00	00	
00	03	00	00	20	00	81	00	04	00	08	00	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	03	00	17	00	00	FO	00	00	00	00	
2A	2A	00	00	F0	00	00	00	44	21	00	00	00	00	00	00	



Forensic Practice.

Interpretation of a Single Record.

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 EvtVariant_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 EvtVariant_e Type	VarTypeSid (19)
+ struct SID_t data	S-1-5-18
+ struct Element_t slot13	

..... T



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 31

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 32

Forensic Practice.

Interpretation of a Single Record - Validation.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
2A	2A	00	00	F0	00	00	00	43	21	00	00	00	00	00	00	**...C!....
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	...d.....
DE	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	EventRecordId			
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	SF	10C.!....
00	00	00	00	00	00	80	00	00	E4	9F	64	1D	90	00	00d..
C7	01	00	00	00	00	00	00	00	00	43	21	00	00	00	00C!....
00	00	0F	01	01	00	0C	01	01	46	D3	EC	12	06	00	00F....
00	03	00	00	20	00	81	00	04	00	08	00	00	00	00	00
00	54	00	65	00	73	00	74	00	20	00	41	00	75	00	74	.T.e.s.t. .A.u.t
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	.o.B.a.c.k.u.p..
00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	00
2A	2A	00	00	FO	00	00	00	44	21	00	00	00	00	00	00	**...D!....



Forensic Practice.

Interpretation of a Single Record - Validation.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
2A	2A	00	00	F0	00	00	00	43	21	00	00	00	00	00	00	**...C!....
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	...d.....
DE	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	43	00	21	00	04	00	00	00	00	9F	10C!....
00	00	00	00	00	80	00	00	E4	9F	64	1D	90			d..
C7	01	00	00	00	00	00	00	00	43	21	00	00	00	00	C!....
00	00	0F	01	01	00	0C	01	01	46	D3	EC	12	06	00	F....
00	03	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	.T.e.s.t. .A.u.t
00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00	00	.o.B.a.c.k.u.p..
00	00	00	00	00	00	03	00	17	00	00	FO	00	00	00	
2A	2A	00	00	F0	00	00	00	44	21	00	00	00	00	00	00	**...D!....



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



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 34

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 35

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.



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 35

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 36

Conclusion. Parsers.

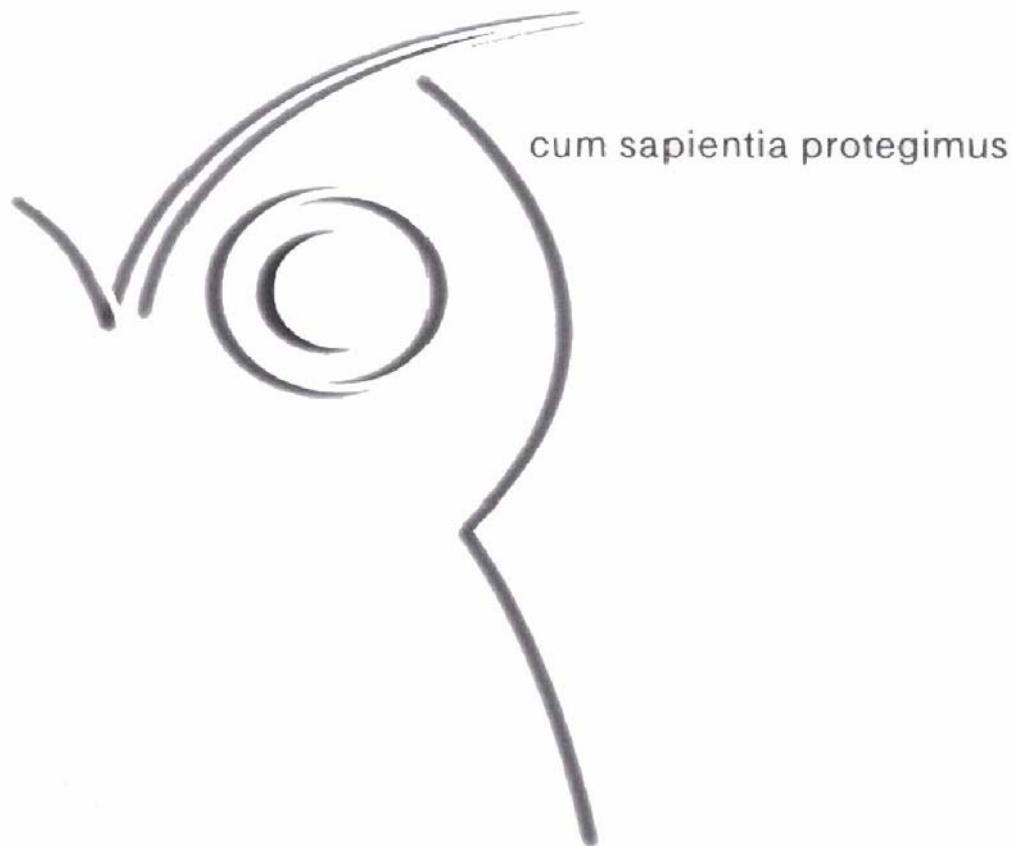
- Vista Event Viewer Applet by Microsoft for uncorrupted files.
- EvtxParser
 - platform-independent (Perl)
 - works on corrupted files
 - some data types are missing
 - some system tokens are missing
CDATA, PI, EntityRef?



Microsoft Vista Event Log File Format
Andreas Schuster
2007-08-14, slide 36

Patent Owner Centripetal Networks, Inc. - Ex. 2014, p. 37

Questions?



cum sapientia protegimus

.....T

Thank You for Your Attention.



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

.....T

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	0123456789ABCDEF	
2A	2A	00	00	E0	04	00	00	42	21	00	00	00	00	00	00	* * B !	
00	E4	9F	64	1D	90	C7	01	0F	01	01	00	0C	01	90	F4	. . . d.	
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	D8	49	03	00	00	0F	01	. (J) . b . f I . . . I . . .	
01	00	41	13	00	3D	03						0	00	00	00	. . A . . = . . M	
00	BA	0C	05	00	45	00						0	74	00	00 E . v . e . n . t . .	
06	65	05	00	00	00	00	00	00	00	00	00	55	00	73		. e f L . . U . s	
00	65	00	72	00	49	00	44	00	00	00	0E	0C	00	13	03		. e . r . I . D
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		. . T . e . s . t . . A . u .
74	00	6F	00	42	00	61	00	63	00	6B	00	75	00	70	00		t . o . B . a . c . k . u . p .
00	00	00	00	00	00	00	00	80	A2	76	22	E0	04	00	00	 v "

