DRAFT

Learning from the Past:

Tools and Techniques for Timeline Analysis

Andreas Schuster
andreas.schuster@telekom.de

Life's for Sharing

Agenda

- What can we learn from the past?
- Timestamps
  - Classic data sources
  - Formats
- How to find more timestamps
- Leveraging log2timeline
- Visualization

What can we learn from the past?

- Timeline: a list of events, ordered by their time of occurence

- Analysis of a timeline will help to
  - correlate events
  - find root cause
  - falsify your hypothesis
    - „A happend earlier than B“ rules out that B caused A
    - „A happend earlier than B“ is no proof that A caused B

- Do not jump to conclusions!

Examples of time stamps

Classic sources

- Logfiles, e.g. syslog

```
May  2 19:35:10 mx1dbn exim[5958]: End queue run: pid=5958
```

- MACB times

```
$ fls -m c: myimage.E01 > myimage.body
$ mactime -b myimage.body
...
Fri Aug 20 2004 17:05:58        168 ...b d/drwxrwxrwx 0    0    9947-144-5 c:/Program Files/Cain
                             108544 .a.b r/rrwxrwxrwx 0    0    9950-128-3 c:/Program Files/Cain/UNINSTAL.EXE
                                627 .acb r/rrwxrwxrwx 0    0    9951-128-1 c:/Program Files/Cain/Credits.txt
                            2064384 ...b r/rrwxrwxrwx 0    0    9952-128-3 c:/Program Files/Cain/Cain.exe
Fri Aug 20 2004 17:05:59         66 .acb r/rrwxrwxrwx 0    0    9953-128-1 c:/Program Files/Cain/Cain.exe.sig
                              26413 .acb r/rrwxrwxrwx 0    0    9954-128-3 c:/Program Files/Cain/Whats.new
                             312490 ..cb r/rrwxrwxrwx 0    0    9955-128-3 c:/Program Files/Cain/oui.txt
...
```

Examples of time stamps

- Microsoft Windows SYSTEMTIME

```
typedef struct _SYSTEMTIME {
  WORD wYear;
  WORD wMonth;
  WORD wDayOfWeek;
  WORD wDay;
  WORD wHour;
  WORD wMinute;
  WORD wSecond;
  WORD wMilliseconds;
} SYSTEMTIME, *PSYSTEMTIME;
```

Examples of time stamps

- SQUID HTTP proxy, native format

```
1286536309.450    917 192.168.0.227 TCP_MISS/200 20670 GET http://www.youtube.com/watch? - DIRECT/209.85.231.136 text/html
1286536309.549    172 192.168.0.227 TCP_MISS/204 294 GET http://v15.c.youtube.com/generate_204? - DIRECT/122.160.120.150 text/html
1286536309.845    221 192.168.0.227 TCP_MISS/200 4035 GET http://i1.ytimg.com/vi/LFV2ASSoEHI/default.jpg - DIRECT/209.85.153.118
1286536310.075    452 192.168.0.227 TCP_MISS/200 5067 GET http://i1.ytimg.com/vi/TeYOZBVfnuY/default.jpg - DIRECT/209.85.153.118
1286536310.372    748 192.168.0.227 TCP_MISS/200 5230 GET http://i4.ytimg.com/vi/GldVBAqJHLY/default.jpg - DIRECT/209.85.153.118
```

Format of time stamps

	printable	binary
unpacked	syslog RFC 822 ISO 8601	SYSTEMTIME
packed	SQUID native log files	time_t FILETIME OLETIME

Format of time stamps

Calculation of a packed time value

- $v = (t - t_0) / u$

- v: time value
- t: time to express
- t_0: Epoch
- u: Unit

Format of time stamps

Common packed formats

Name	Epoch	Unit	Data type
Unix/POSIX time	00:00:00 Jan 01, 1970	1 s	signed integer, 32 bit
Apple HFS Plus	00:00:00 Jan 01, 1904	1 s	unsigned integer, 32 bit
Windows .NET Ticks	00:00:00 Jan 01, 0001	100 ns	signed integer, 64 bit
Windows FILETIME	00:00:00 Jan 01, 1601	100 ns	unsigned integer, 64 bit
Windows OLE, Delphi	00:00:00 Dec 30, 1899	1 d	double, 64 bit
Julian Date (JD)	12:00:00 Jan 01, 4713 BC	1 d	real
Reduced Julian Date (RJD)	12:00:00 Nov 16, 1858		

How to find more time stamps?

Search for candidates

```
33 // scan file
34 local int64 pos = 0;
35 local int64 nMaxPos = FileSize() - nDateLength;
36 local uint64 probe;
37
38 while (pos <= nMaxPos) {
39     // read data at offset "pos"
40     FSeek(pos);
41     probe = ReadUInt64(pos);
42     if ((probe >= nLowerBound) && (probe <= nUpperBound)) {
43         // create bookmark
44         AddBookmark(
45             pos,
46             "",
47             "FILETIME",
48             -1,
49             cWhite,
50             cRed);
51         // advance the size of data found
52         pos = pos + nDateLength;
53     } else {
54         // advance one byte
55         pos++;
56     }
57 }
```

How to find more time stamps?

Search for candidates

Inspector

Name	Value	Start
FILETIME	05/05/2007 11:54:41	1210h
FILETIME	05/05/2007 11:54:41	15EBh
FILETIME	05/05/2007 11:54:41	16D8h
FILETIME	05/05/2007 11:54:41	1752h
FILETIME	05/05/2007 11:54:41	17B0h
FILETIME	05/05/2007 11:54:41	182Ah
FILETIME	05/05/2007 11:54:41	1888h
FILETIME	05/05/2007 11:54:41	1902h
FILETIME	05/05/2007 11:54:41	1960h
FILETIME	05/05/2007 11:54:41	19DAh
FILETIME	05/05/2007 11:54:41	1A38h
FILETIME	05/05/2007 11:54:41	1AB2h
FILETIME	05/05/2007 11:54:41	1B10h
FILETIME	05/05/2007 11:54:41	1B8Ah
FILETIME	05/05/2007 11:54:41	1BE8h
FILETIME	05/05/2007 11:54:41	1C62h
FILETIME	05/05/2007 11:54:41	1CC0h
FILETIME	05/05/2007 11:54:41	1D3Ah
FILETIME	05/05/2007 11:54:41	1D98h
FILETIME	05/05/2007 11:54:41	1E12h
FILETIME	05/05/2007 11:54:41	1E70h
FILETIME	05/05/2007 11:54:41	1EEAh
FILETIME	05/05/2007 11:54:41	1F48h
FILETIME	05/05/2007 11:54:41	1FC2h
FILETIME	05/05/2007 11:54:41	2020h

Auto | Variables | Bookmarks

FindTimestamps.1sc | sample1.evtx

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
17C0h: 0E 82 26 02 00 00 14 00 00 00 01 00 04 00 01 00   .‚&.............
17D0h: 04 00 02 00 06 00 02 00 06 00 02 00 06 00 08 00   ................
17E0h: 15 00 08 00 11 00 00 00 00 00 04 00 08 00 04 00   ................
17F0h: 08 00 08 00 0A 00 01 00 04 00 00 00 00 00 00 00   ................
1800h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1810h: 00 00 00 00 00 00 2D 00 21 00 04 00 00 00 03 00   ......-.!.......
1820h: 00 00 00 00 00 00 00 00 80 00 80 56 FA 29 0C 8F   .........€.€Vú)..
1830h: C7 01 00 00 00 00 00 00 00 00 E0 00 00 00 00 00   Ç.........à.....
1840h: 00 00 00 0F 01 01 00 0C 01 01 46 D3 EC 12 06 00   ..........FÓì...
1850h: 00 03 00 00 00 0A 00 81 00 04 00 08 00 00 00 00   ................
1860h: 00 54 00 65 00 73 00 74 00 00 00 00 00 00 00 00   .T.e.s.t........
1870h: 00 04 04 00 D8 00 00 00 2A 2A 00 00 D8 00 00 00   ....Ø...**..Ø...
1880h: 04 00 00 00 00 00 00 00 80 56 FA 29 0C 8F C7 01   .........€Vú)..Ç.
1890h: 0F 01 01 00 0C 01 90 F4 0E 82 26 02 00 00 14 00   .......ô.‚&.....
18A0h: 00 00 01 00 04 00 01 00 04 00 02 00 06 00 02 00   ................
18B0h: 06 00 02 00 06 00 08 00 15 00 08 00 11 00 00 00   ................
18C0h: 00 00 04 00 08 00 04 00 08 00 08 00 0A 00 01 00   ................
18D0h: 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
18E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2D 00   ..............-.
18F0h: 21 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00   !...............
1900h: 80 00 80 56 FA 29 0C 8F C7 01 00 00 00 00 00 00   €.€Vú)..Ç.......
1910h: 00 00 E1 00 00 00 00 00 00 00 00 0F 01 01 00 0C   ..á.............
1920h: 01 01 46 D3 EC 12 06 00 00 03 00 00 00 0A 00 81   ..FÓì...........
1930h: 00 04 00 08 00 00 00 00 00 54 00 65 00 73 00 74   .........T.e.s.t
1940h: 00 00 00 00 00 00 00 00 00 00 2E 00 D8 00 00 00   ............Ø...
1950h: 2A 2A 00 00 D8 00 00 00 05 00 00 00 00 00 00 00   **..Ø...........
```

How to find more time stamps?

Analyze applications

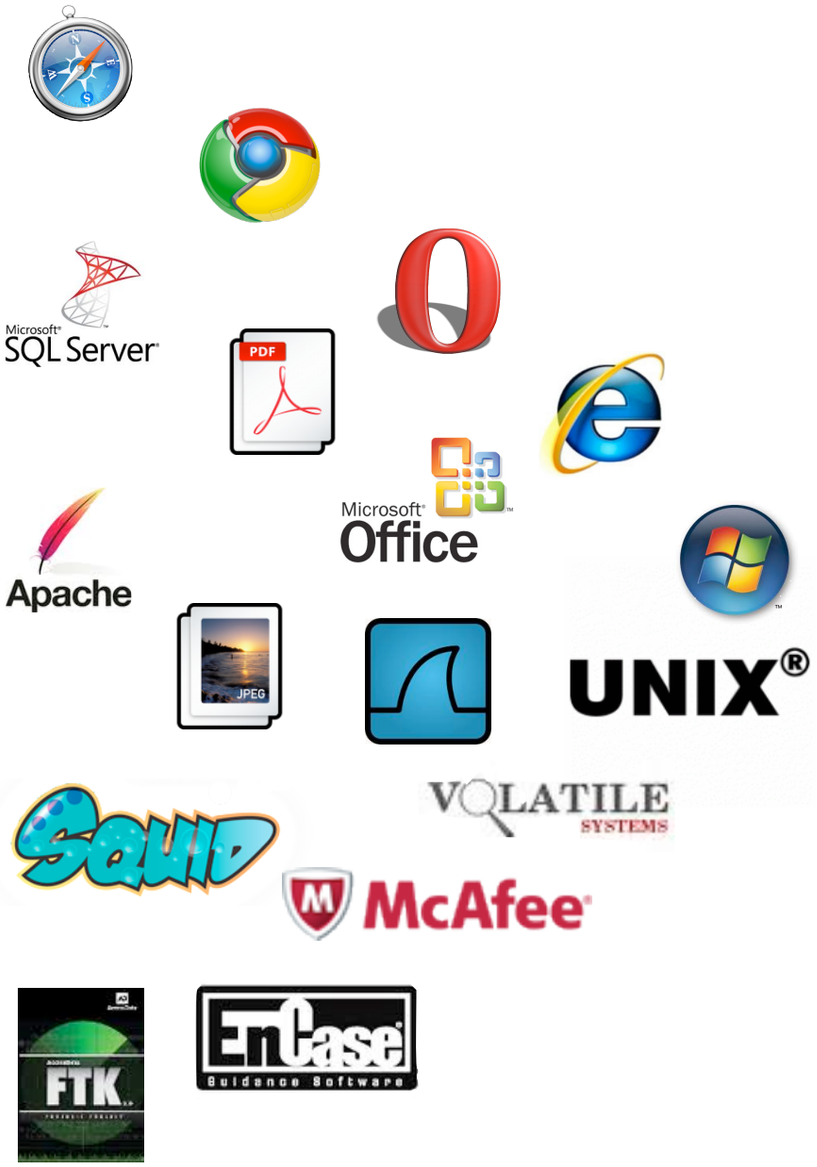
IDA View-A | Hex View-A | Structures | Enums | Imports | Exports

```
.text:0001CF76                call    _PsGetCurrentProcessId@0 ; PsGetCurrentProcessId()
.text:0001CF76
.text:0001CF7B                mov     [esi+TCPA.ProcessID], eax
.text:0001CF81                lea     eax, [esi+TCPA.TimeCreated]
.text:0001CF87                push    eax             ; CurrentTime
.text:0001CF88                call    ds:__imp__KeQuerySystemTime@4 ; KeQuerySystemTime(x)
.text:0001CF88
.text:0001CF8E                mov     eax, [ebp+var_1C]
.text:0001CF91                cmp     eax, 3
.text:0001CF94                jbe     loc_38E5B
.text:0001CF94
.text:0001CF9A                cmp     byte ptr [ebp+arg_pOptions+3], 0 ; End of Options?
.text:0001CF9E                jz      loc_1F53E
.text:0001CF9E
.text:0001CFA4                add     eax, 0FFFFFFFDh
.text:0001CFA7                push    eax             ; int
.text:0001CFA8                lea     eax, [ebp+Source1]
.text:0001CFA8
.text:0001CFAB
.text:0001CFAB loc_1CFAB:                             ; CODE XREF: TdiOpenAddress(x,x,x,x,x,x)+281C↓j
.text:0001CFAB                push    eax             ; Source1
.text:0001CFAC                push    offset _TcpipStackBacktraceTable ; int
.text:0001CFB1                call    _TcpipFindOrCreateBacktraceStack@12 ; TcpipFindOrCreateBacktraceStack(x,x,x)
.text:0001CFB1
.text:0001CFB6                mov     [esi+TCPA.BacktraceStack], eax
.text:0001CFB6
.text:0001CFBC
.text:0001CFBC loc_1CFBC:                             ; CODE XREF: TdiOpenAddress(x,x,x,x,x,x)+1C13C↓j
.text:0001CFBC                push    esi
.text:0001CFBD                call    _InsertAddrObj@4 ; InsertAddrObj(x)
```

0000CF88 | 0001CF88: TdiOpenAddress(x,x,x,x,x,x)+262

log2timeline

Data sources and output formats



log2timeline

TSK mactime body file

ASCII Timeline, TLN

XML Timeline, TLNX

Comma/Tab Separated Value

SIMILE

BeeDocs

CyberForensics TimeLab

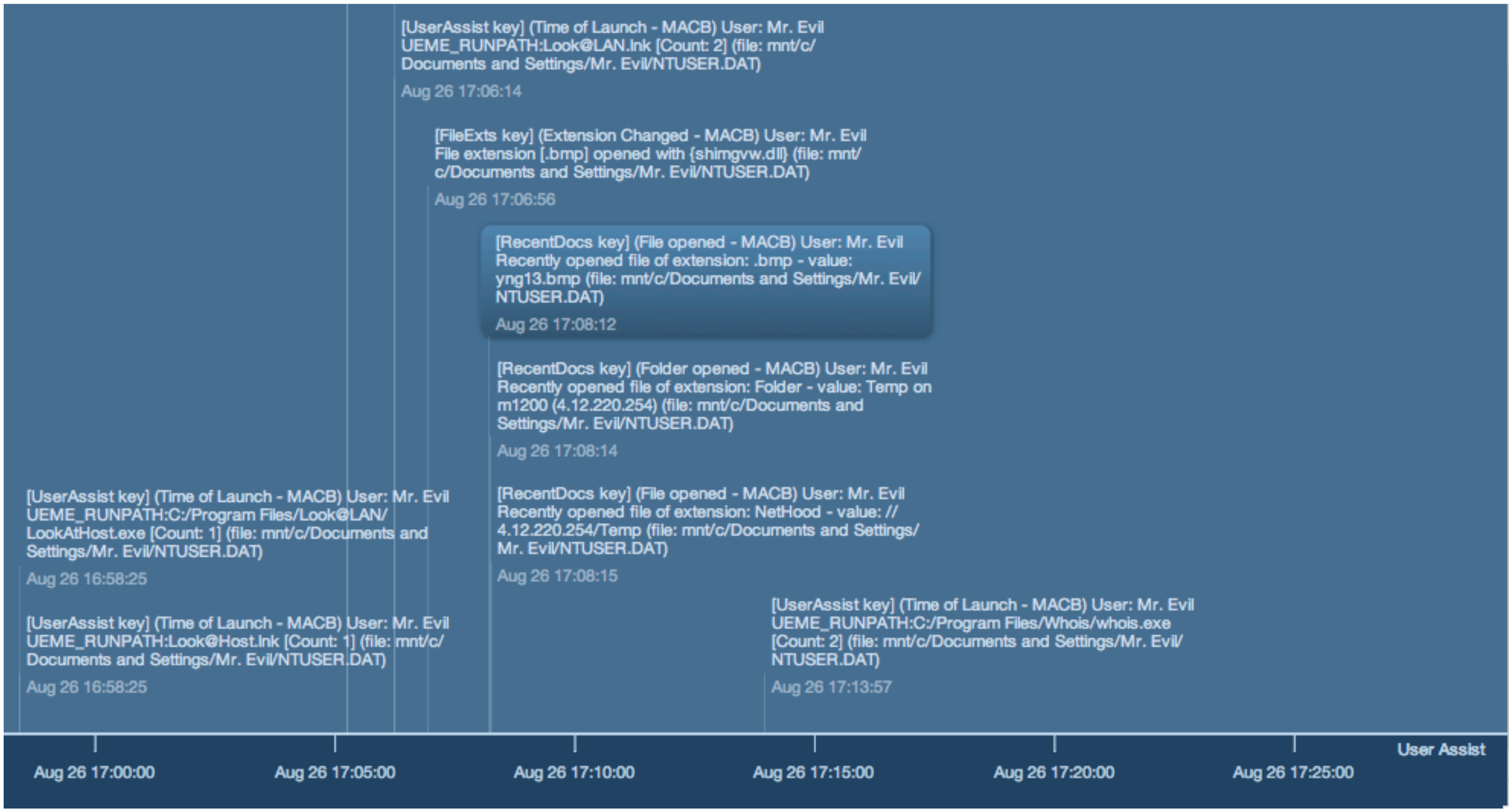
log2timeline

Usage

- get help
  `log2timeline -h`
- get list of input/output/timezone options:
  `log2timeline -f list`
  `log2timeline -o list`
  `log2timeline -z list`
- common invocation:
  `log2timeline -z UTC -f evt -o sqlite -w example.db3 mnt/c/WINDOWS/system32/config`
- to scan a whole file system:
  `timescanner -z UTC -f winxp -o simile -w example.xml -d mnt/c`

Visualization

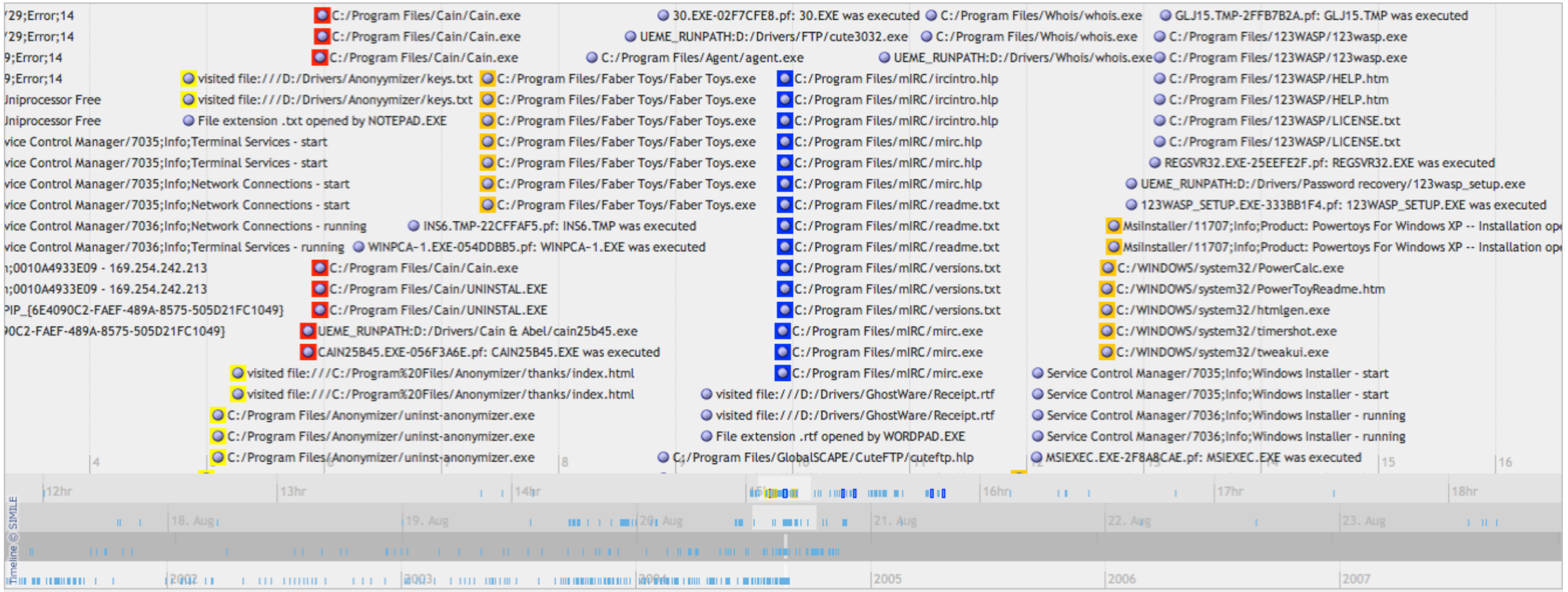
BeeDocs Timeline 3D



Visualization

SIMILE

This timeline was rendered from data of the CFREDS Schardt hacking case using SIMILE Timeline version 2.3.1 (with Ajax lib 2.2.1).



All times are in UTC

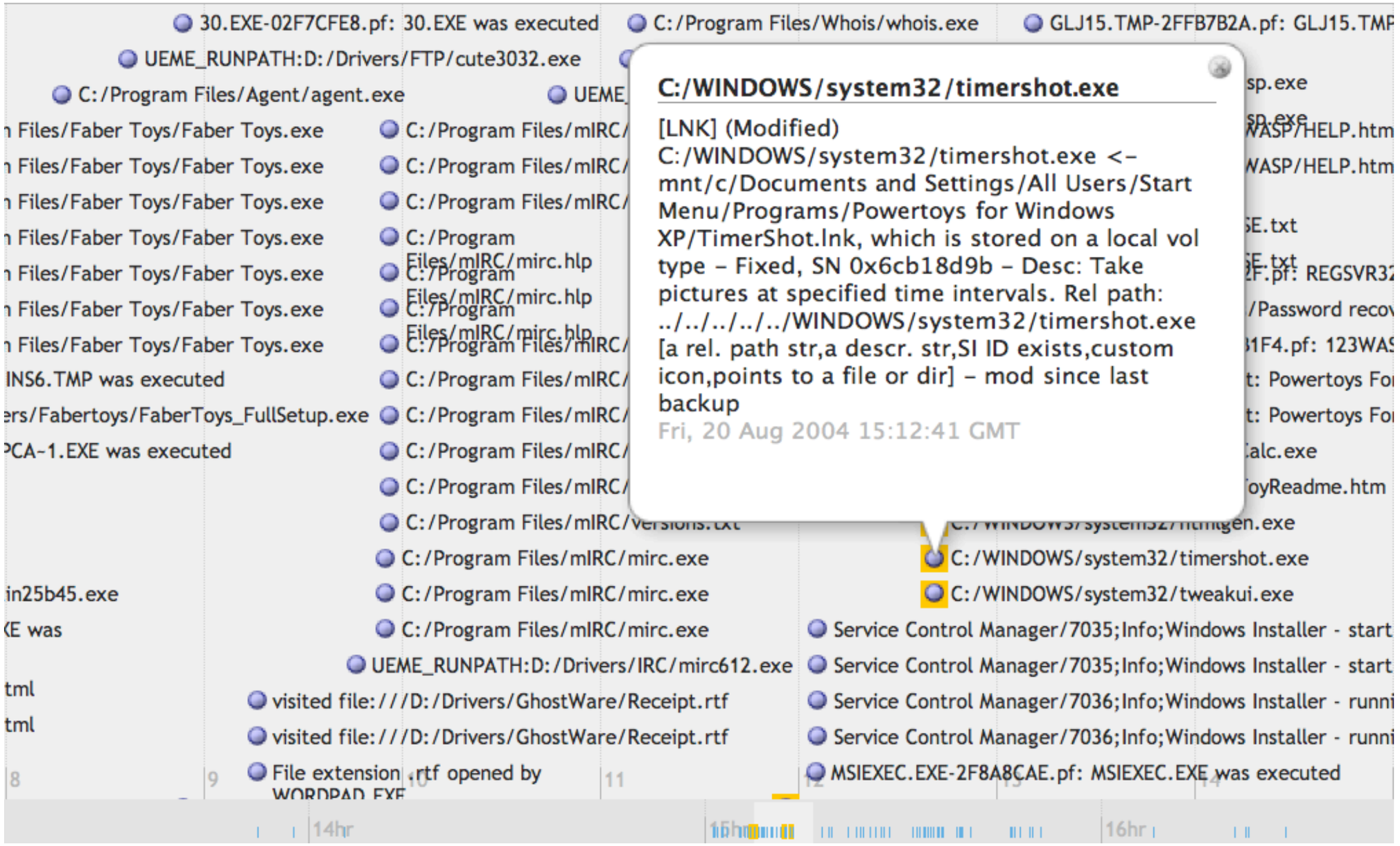
Filter:

Highlight:

anon | toy | cain | mIRC | Clear All

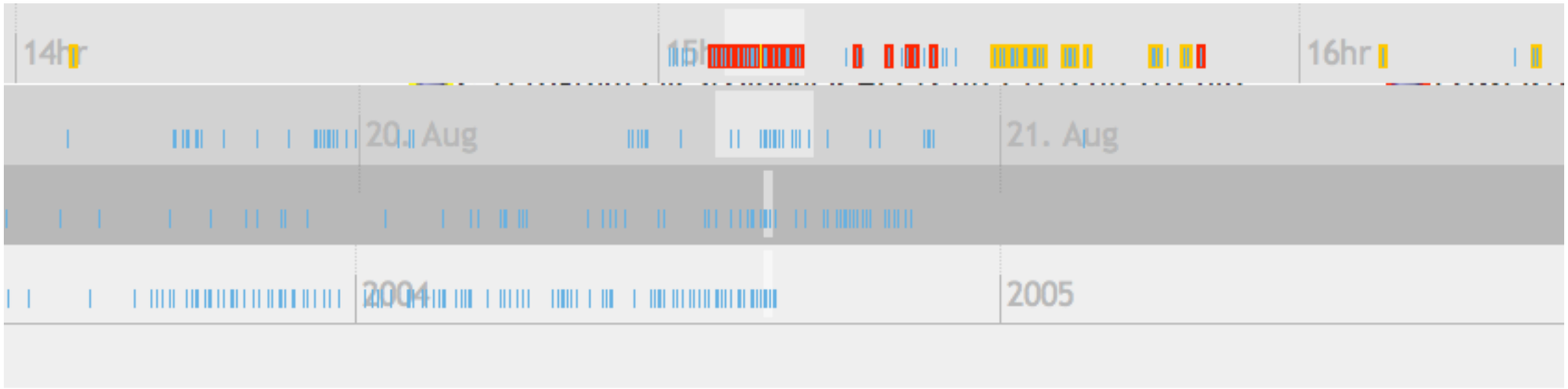
Visualization

SIMILE



Visualization

SIMILE



Highlight:

	http	.EXE	

Visualization

SIMILE

```
function onLoad() {
    var eventSource = new Timeline.DefaultEventSource();
    var theme = Timeline.ClassicTheme.create();
    theme.event.bubble.width = 250;

    var date = "Fri 20 Aug 2004 15:09:56 GMT"
    var bandInfos = [
        Timeline.createBandInfo({
            width:          "85%",
            intervalUnit:   Timeline.DateTime.HOUR,
            date:           date,
            intervalPixels: 200,
            eventSource:    eventSource,
        }),
        Timeline.createBandInfo({
            width:          "5%",
            intervalUnit:   Timeline.DateTime.DAY,
            date:           date,
            intervalPixels: 200,
            eventSource:    eventSource,
            overview:       true,
        }),
        Timeline.createBandInfo({
            width:          "5%",
            intervalUnit:   Timeline.DateTime.MONTH,
```

DRAFT

Thank you for your attention!

Andreas Schuster
andreas.schuster@telekom.de

Life's for Sharing