Automated Windows Event Log Forensics

By

Rich Murphey

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.

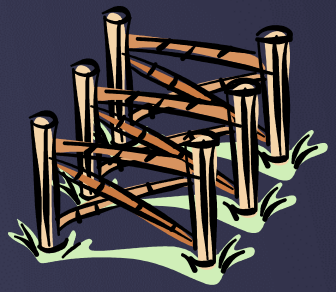
http:/dfrws.org

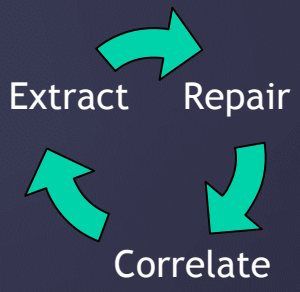
Automated Windows event log forensics

Rich Murphey

ACS

- Case Study
  - Engagement
  - Preliminary Results
  - Final Report
- Log Analysis
  - Extract
  - Repair
  - Correlate
  - Interpret





DFRWS Aug 13, 2007

Special Thanks To

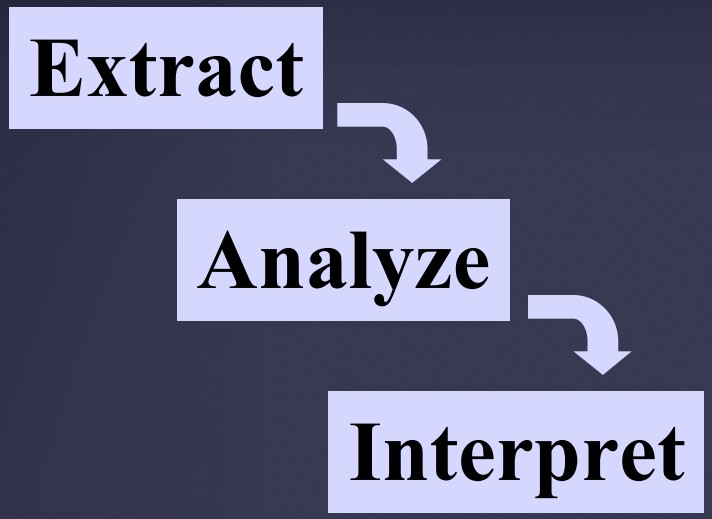
Sponsor:

- Digital Forensic Services
  - In-depth Analysis, Testimony
- Data Recovery Services
  - Complex RAID, Exotic File Systems
- Technology Consulting

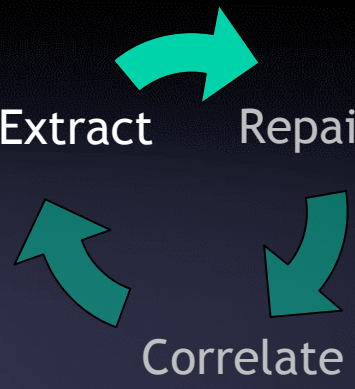
Reviewers: Matthew Geiger, CERT

Jerlyn Mardis, ACS

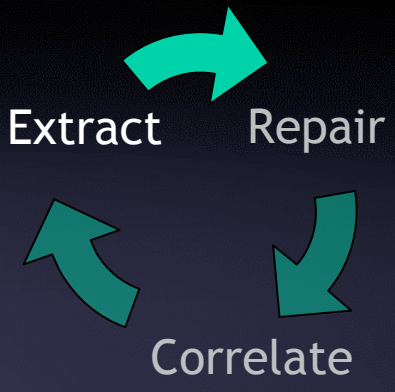
Forensic Process Models



Log Forensics Process



Forensic Process Models



Recover:

Step 1 – Extract
- Data Carve for Logs, etc.

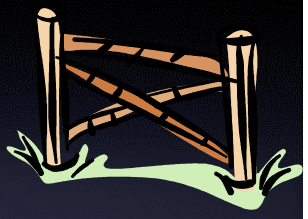
Step 2 – Repair and Validate
- Obtain valid log files.

Step 3 – Correlate
- time, files, paths,…

Analyze

Interpret

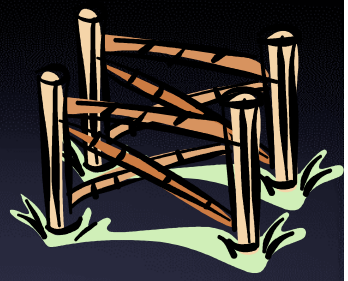
- Officer/Director calls
  - Something bad happened….
  - Possible contract violation.
  - *Outgoing transfer* of proprietary documents.



#1: Define a scope of work.

- Can we identify file transfer?
- Examine hard drives
- Email attachments
- File transfer, uploads
- Anything else?

Good news:



- We know what to look for.
- Well defined keywords, file names

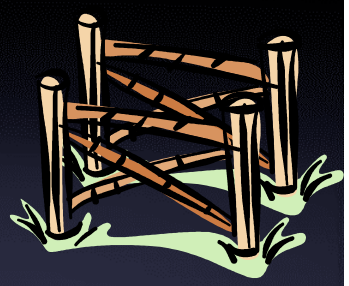
#2: Preliminary Report

- D:\OfInterest.doc
- In unallocated space….

Bad News:

- IT deleted the user profile, and gave laptop to a new employee, six months ago, after they reformatted and reinstalled Windows XP.

#2: Preliminary Report



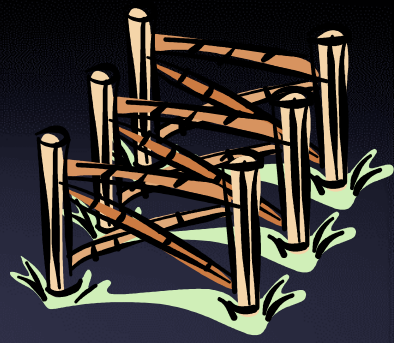
- D:\OfInterest.doc
  - In unallocated space….
- Surrounding data looks like a shortcut.

- Shortcuts contain a *snapshot* of:
  - MAC timestamps
  - Filename
  - Absolute Path, Relative Path
  - Kind of Device (Hard disk/CD-ROM)
  - Partition's Volume Serial Number

- Shortcuts may contain IDs, label, size
  - A snapshot of file's attributes, media's attributes

Link target information	
Local Path	D:\OfInterest.doc
Volume Type	CD-ROM
Volume Label	Nov 11 2006
Volume Serial Number	E2C3-F184
File size	1643743
Creation time (UTC)	11/11/2006 3:21:14 PM
Last write time (UTC)	11/3/2006 10:12:34 AM
Last access time (UTC)	N/A
File attributes	
Read-only	

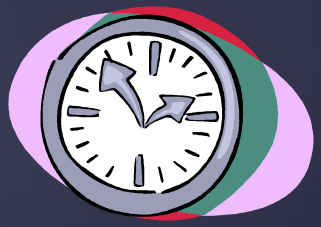
How to identify *outgoing* file transfer?



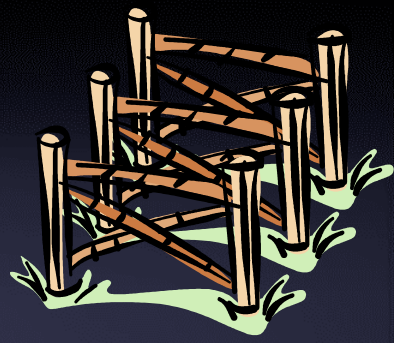
- Data carve for file path, time….

Where to find time stamps?

- Event logs
- Internet history
- Shortcuts
- Registry, and others?...

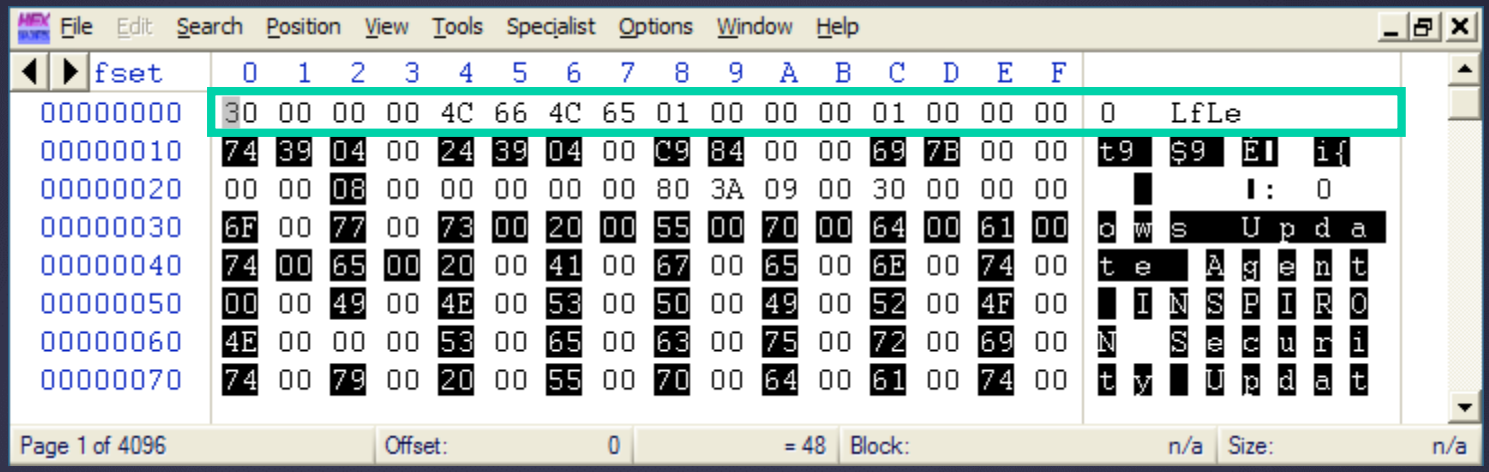


Log recovery process…



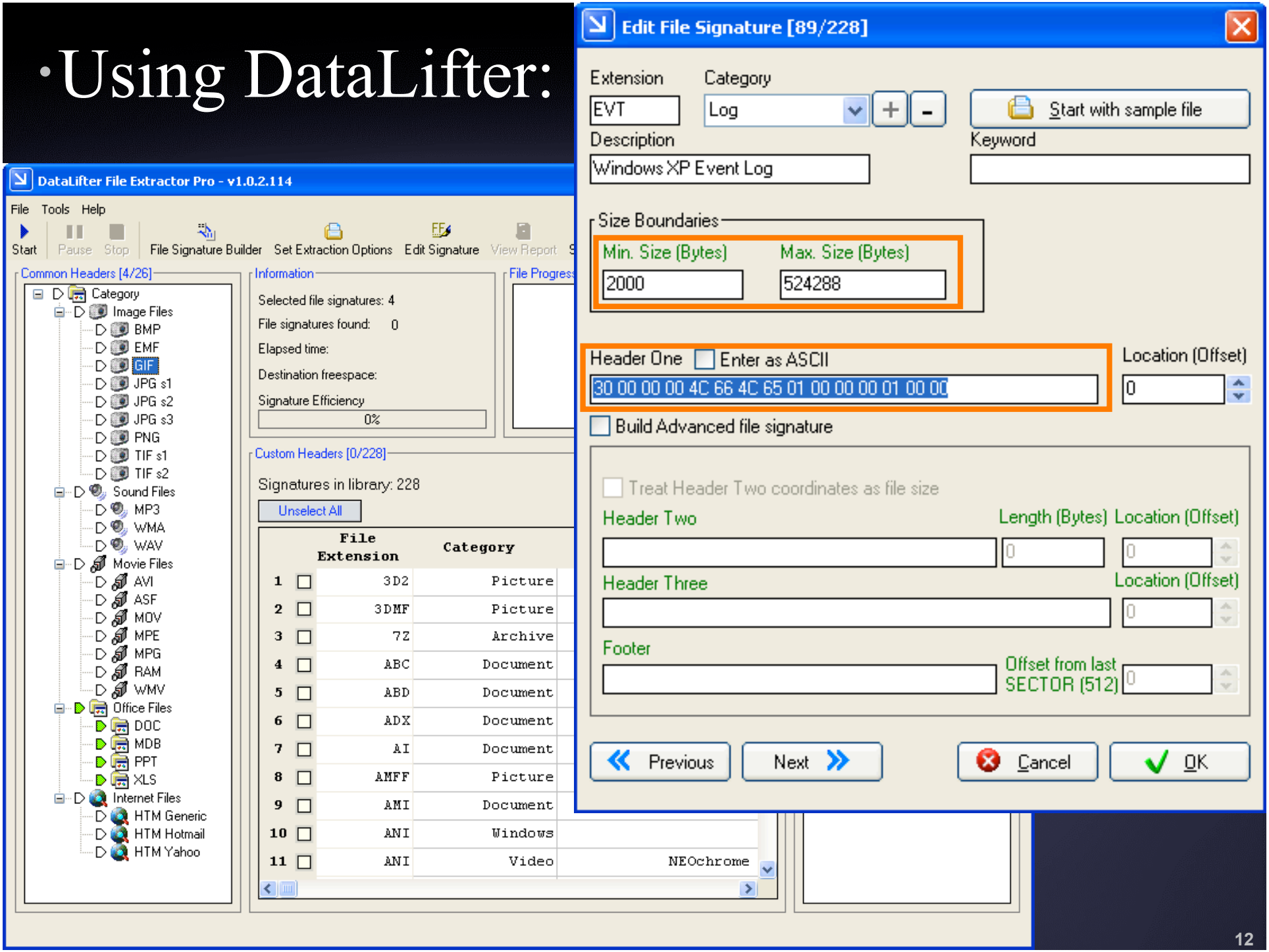
- Step 1 – Extract
  - Data Carve for Logs, etc.
- Step 2 – Repair
  - Fix corrupt log files.
- Step 3 – Correlate
  - Formulate queries for time, names,…

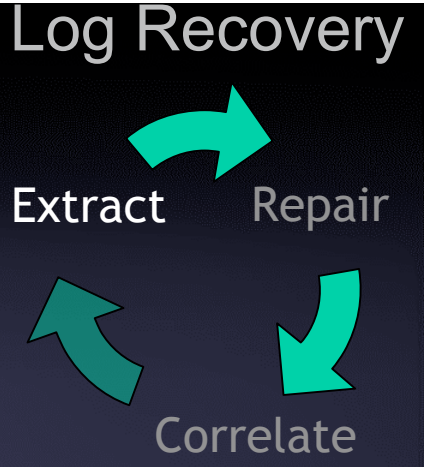
- XP log signature – 16 bytes
  - 30 00 00 00 4c 66 4c 65 01 00 00 00 01 00 00 00



- Typical log sizes:
  - 512K on desktops
  - 1MB on servers

Using DataLifter:





scalpel.conf entry:

- evt y 1048576 \x30\x00\x00\x00\x4c\x66\x4c\x65 \x01\x00\x00\x00\x01\x00\x00\x00

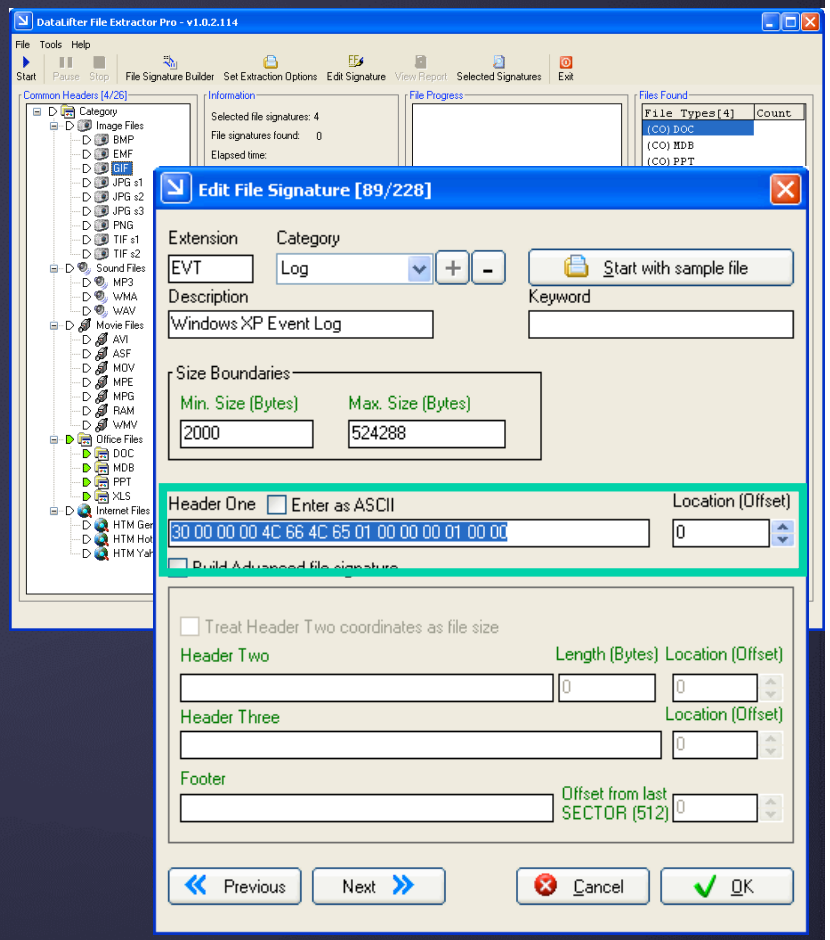
- Step 1 – Initial script to recover logs:

  scalpel /dev/sda1

The Results:

- Step 1 – Extract
  - Run DataLifter
  - 100 logs are extracted.
  - Only two are viewable.
  - 98 corrupt logs
- Step 2
  - Repair 98 corrupt logs?

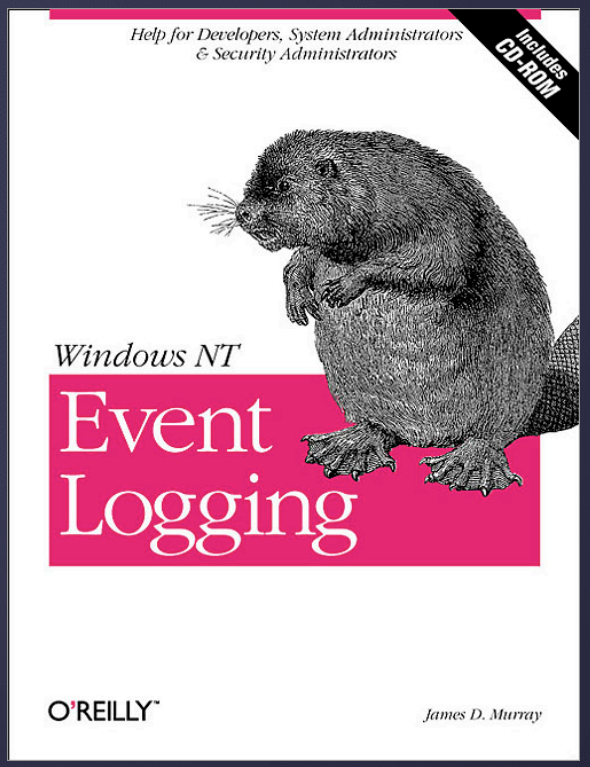
```
evt y 1048576
  \x30\x00\x00\x00\x4c\x66\x4c\x65
  \x01\x00\x00\x00\x01\x00\x00\x00
% scalpel /dev/sda1
```

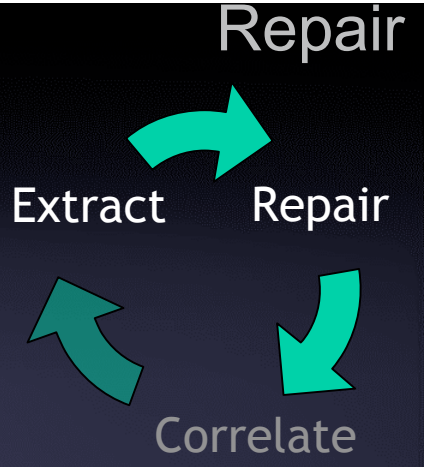


- Windows 2000, XP, 2003
  - Time, SID, Source, Severity, Message

windows/system32/config:

- AppEvent.evt
- SecEvent.evt
- SysEvent.evt
- Internet.evt





- FixEvt – an XP log repair tool
  - Automatically repairs corrupt logs
- Repairs or identifies known forms of corruption.
  - In seconds.

http://murphey.org

FixEvt - Repairs Corrupted Windows Event Logs

FixEvt is a native Windows console (command line) application that repairs a common form of corruption of Windows event logs that occurs when the event logging service stops without properly closing the log file.

Download Now:

- **fixevt.exe** (Executable for Widows 98, NT, 2K, XP, 2003, and Vista)
- **fixevt.exe.md5.txt** (md5 checksum of the above executable)

Fixevt.exe is a native, standalone, console (command line) appication for Windows 98, NT, 2K, XP, 2003, and Vista. It requires no other files, and no installation. Simply download the executable and run it from the command line as shown below. To see this documentation, invoke it with no command line arguments.

Stephen Bunting first described the signs of log corruption and a manual method to repair it on his web site.

http://linuxbox.cms.udel.edu/forensics/repaireventlogfile.htm

Steve Bunting's Manual Method

- http://128.175.24.251/forensics

XP event log repair

- Invalid Header:

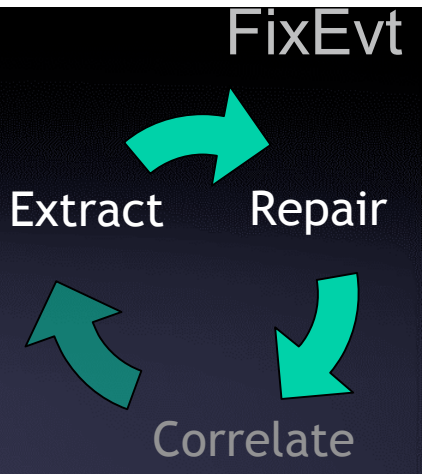
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	30	00	00	00	4C	66	4C	65	01	00	00	00	01	00	00	00
00000010	6C	18	00	00	BC	17	00	00	FC	4F	00	00	6E	45	00	00
00000020	00	00	08	00	0B	00	00	00	80	3A	09	00	30	00	00	00

- Trailer with good data:

fset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00003B10	A4	00	00	00	28	00	00	00	11	11	11	11	22	22	22	22
00003B20	33	33	33	33	44	44	44	44	58	3B	00	00	14	3B	00	00
00003B30	2A	50	00	00	9B	45	00	00	28	00	00	00	00	00	00	00
00003B40	00	00	00	00	45	00	31	00	30	00	30	00	42	00	00	00

- Repaired Header:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	30	00	00	00	4C	66	4C	65	01	00	00	00	01	00	00	00
00000010	58	3B	00	00	14	3B	00	00	2A	50	00	00	9B	45	00	00
00000020	00	00	08	00	00	00	00	00	80	3A	09	00	30	00	00	00

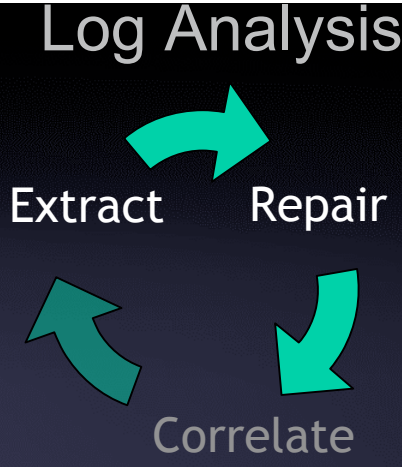


- Available on the web.
- A 4K command line executable.
- Very simple – no install.

```
% fixevt *.evt
```

- For each log, FixEvt reports either:
  - 1 - Did not need repair
  - 2 - Was repaired
  - 3 - Cannot be repaired
  - 4 - Might be repaired by another method

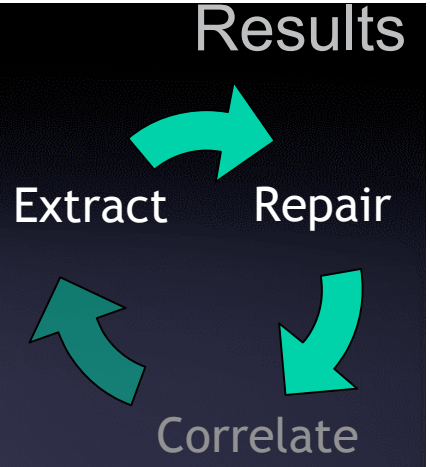
How the process works



- Step 1 – Extract
  - Run DataLifter
  - 100 logs are extracted.
  - 98 corrupt logs.

- Step 2 – Repair the Logs
  - Manual: 15 minutes/log * 98 Logs = 3 days
  - "FixEvt *.evt": 2 seconds.

The Results:

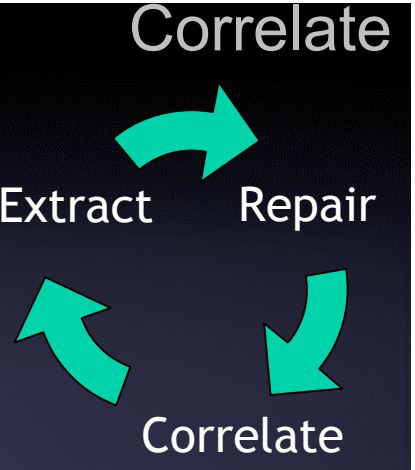


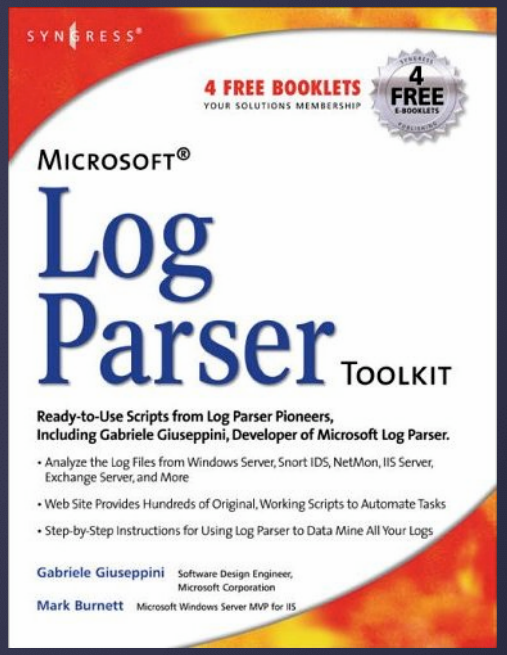
- Step 1 – Extract
  - 100 logs are extracted.
  - 98 corrupt logs.
  - 2 valid logs
- Step 2 – Repair
  - 50 logs repaired
  - 52 Total logs.
- Step 3 – Correlate events in 51 logs?

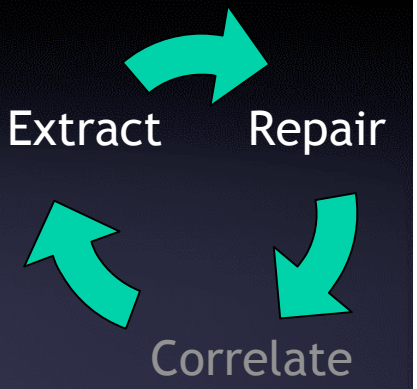
```
scalpel /dev/sda1
fixevt *.evt
```

LogParser

- Input:
  - evt, IIS, REG, FS, ADS
- Output:
  - csv, XML, SQL, HTML
- Run SQL queries on multiple log files







- 50 logs were repaired.
  - Some are still invalid due to corruption.
  - Tools will not parse a sets containing corrupt logs.
- Use LogParser to validate the logs.
  - LogParser "select count(*) from log.evt"
  - Returns an error status that indicates parsing errors.
- Script to extract, repair and validate logs:

```
scalpel /dev/sda1
fixevt *.evt
for i in *.evt;do LogParser "select count(*) from $i" \
    && cp $i goodlogs; done
```

- Result: 46 total valid logs
  - 23 empty, 23 non-empty
  - 87,413 events total
- 14 months of activity
  prior to reformatting of the hard drive.

Step 3 – Correlate

select <columns> from <table> into <output-file>

logparser “select * from system.evt into excel.csv”

- Reads the log file: system.evt
- Creates a spreadsheet of comma separated values
- “*” selects all columns of data

Write Queries – for correlating time, name…

… select TimeGenerated, Message from system.evt …

- Output timestamp and full message

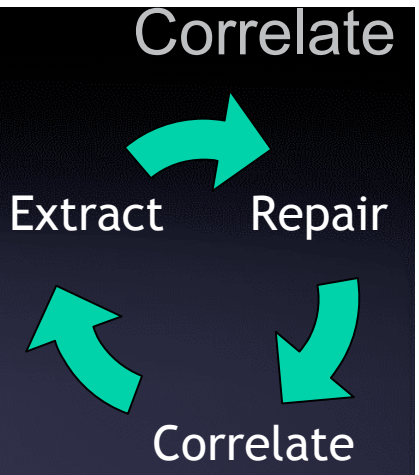
… where TimeGenerated > '2006-11-11 00:00:00'
and TimeGenerated < '2006-11-12 00:00:00'

- Filter a one day period.

… where Message like “%CD Burning%” …

- Filters for start, stop, running events

SQL queries to identify patterns



logparser

"select TimeGenerated, Message
from system.evt
where TimeGenerated > '2006-11-11 00:00:00'
and TimeGenerated < '2006-11-12 00:00:00'
and Message like "%CD Burning%"

Time (UTC)	Message
11/11/2006 15:21	The CD Burning service was successfully sent a start control.
11/11/2006 15:21	The CD Burning service entered the running state.
11/11/2006 15:22	The CD Burning service entered the running state.
11/11/2006 15:23	The CD Burning service entered the running state.
11/11/2006 15:24	The CD Burning service entered the running state.
11/11/2006 15:25	The CD Burning service entered the running state.
11/11/2006 15:26	The CD Burning service entered the running state.
11/11/2006 15:27	The CD Burning service entered the running state.
11/11/2006 15:27	The CD Burning service entered the stopped state.

Shortcuts may contain IDs, label, size

- A snapshot of file's attributes, media's attributes

Link target information	
Local Path	D:\OfInterest.doc
Volume Type	CD-ROM
Volume Label	Nov 11 2006
Volume Serial Number	E2C3-F184
File size	1643743
Creation time (UTC)	11/11/2006 3:21:14 PM
Last write time (UTC)	11/3/2006 10:12:34 AM
Last access time (UTC)	N/A
File attributes	
Read-only	

Timestamp Analysis

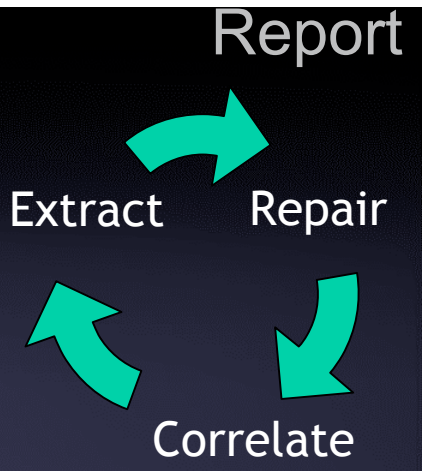
Link target information	
Local Path	D:\OfInterest.doc
Volume Type	CD-ROM
Volume Label	Nov 11 2006
Volume Serial Number	E2C3-F184
File size	1643743
Creation time (UTC)	11/11/2006 3:21:14 PM
Last write time (UTC)	11/3/2006 10:12:34 AM
Last access time (UTC)	N/A
File attributes	
Read-only	

- Last write time is earlier than created.

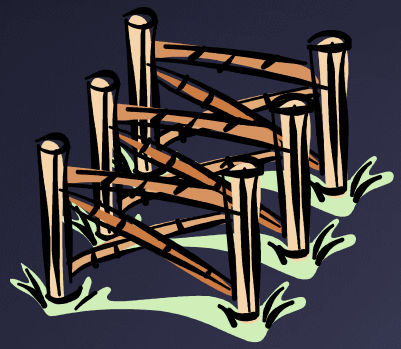
Created	**11/11/2006 3:21:14 PM**
Last write	**11/3/2006 10:12:34 AM**

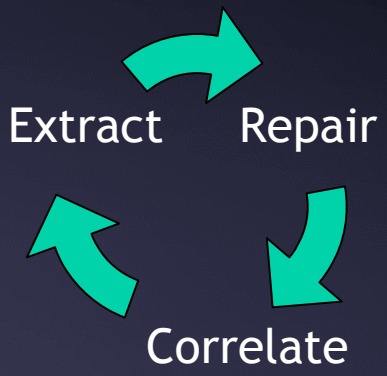
- Can indicate the time at which a file was transferred from source media.
- Can help identify the location of the source media.

Correlations indicate



- A CD-ROM was burned
  - On this system.
  - By account name: Bob
  - At: 11/11/2006 3:21 PM UTC
- The CD media may be identified:
  - Label: “Nov 11 2006”
  - Volume serial number: E2C3-F184
- The source media may be identified:
  - OfInterest.doc with size = 1643743 bytes, and
  - Last Modified = 11/3/2006 10:12:34 AM UTC





Questions?

Rich@Murphey.org
http://murphey.org
http://acsworldwide.com