

Forensic Timeline Splunking

Nick Klein

Klein & Co.
experts in computer forensics.

A long time ago ...

Brian Carrier brought us Sleuthkit, based on the earlier work of **Dan Farmer** and **Wietse Venema**

date	size	type	meta	file
16 Nov 2011 15:39:44	46154	m ...	199175	/\$Recycle.Bin/S-I-5.../\$RH7KA4C.docx (deleted)
17 Nov 2011 11:24:45	46154	.a .b	199175	/\$Recycle.Bin/S-I-5.../\$RH7KA4C.docx (deleted)
17 Nov 2011 11:47:00	46154	..c .	199175	/\$Recycle.Bin/S-I-5.../\$RH7KA4C.docx (deleted)

M = Contents last modified **C** = Change to metadata (e.g. MFT, inode)

A = File last accessed **B** = “Birth” / creation of file on volume

A long time ago ...

In 2009, **Kristinn Gudjonsson** in consultation with **Rob Lee** developed log2timeline

date	size	type	meta	file
16 Nov 2011 15:39:44	46154	m ...	199175	/\$Recycle.Bin/S-I-5.../\$RH7KA4C.docx (deleted)
17 Nov 2011 11:24:45	46154	.a .b	199175	/\$Recycle.Bin/S-I-5.../\$RH7KA4C.docx (deleted)
17 Nov 2011 11:47:00	46154	..c .	199175	/\$Recycle.Bin/S-I-5.../\$RH7KA4C.docx (deleted)

M = Contents last modified **C** = Change to metadata (e.g. MFT, inode)

A = File last accessed

B = “Birth” / creation of file on volume

Now the “super timeline”

date	size	type	meta	file
13 Nov 2011 09:47:19	46154			[EXIF] Secret File.docx first created by user John
16 Nov 2011 15:39:44	46154	m ...	199175	/\$Recycle.Bin/S-I-5.../\$RH7KA4C.docx (deleted)
17 Nov 2011 11:14:50	46154			[index.dat] Secret File.docx accessed by user Bob from network drive P://Projects/Secret Project/
17 Nov 2011 11:24:45	46154	.a .b	199175	/\$Recycle.Bin/S-I-5.../\$RH7KA4C.docx (deleted)
17 Nov 2011 11:25:14	46154			[Registry] Microsoft Word executed by user Bob
17 Nov 2011 11:25:14	46154			[Recent] Secret File.docx accessed by user Bob from local path C:\...\Bob\Desktop
17 Nov 2011 11:47:00	46154	..c .	199175	/\$Recycle.Bin/S-I-5.../\$RH7KA4C.docx (deleted)

Current log2timeline modules

.sol (LSO) or Flash cookie file

Analog cache

Apache 2 access and error logs

Body file in TLN format

Chrome history

EnCase / FTK Imager file listing

Exif data

Firefox 2/3 browser history

Firefox bookmark file

Generic Linux logs

IE history index.dat files

IIS W3C log

ISA text export log

I2t CSV format

Linux syslog log

McAfee AV engine, HIPS event.log, HIPShield log

Microsoft Office 2007 OpenXML docs

MS SQL server error log

NTFS Change log

NTFS MFT

Opera global history file

Output from mactime

PCAP file

PDF document metadata

Safari History.plist

Skype SQL database

Squid access log

Symantec log

Volatility output

Windows event logs

Windows prefetch directories

Windows recycle bin directories

Windows Registry (sam, system, software, ntuser plus userassist)

Windows SetupAPI log

Windows shortcut (lnk)

Windows system restore points

wmiprov log

XeXAMInventory or AeXProcessList log

XP firewall log

However ...

Tue Nov 01 2011 00:01:25,504225,,a,,,r/rrwxrwxrwx,0,0,45879-128-3,/ProgramData/LogMeIn/LMI20111101.log

Tue Nov 01 2011 00:01:25,507174,,c,,,r/rrwxrwxrwx,0,0,60819-128-3,/ProgramData/LogMeIn/LMI201111031.log

Tue Nov 01 2011 00:35:29,40544,macb,r/rrwxrwxrwx,0,0,182643-128-3,/Users/Dr Evil/AppData/Roaming/Dropbox/4eae973b

Tue Nov 01 2011 01:06:18,930,,a,b,r/rrwxrwxrwx,0,0,100399-128-4,/Program Files/Splunk/var/lib/splunk/defaultdb/db/db_1320271900_1319756471_16/SourceTypes.data

Tue Nov 01 2011 01:06:18,897,,a,b,r/rrwxrwxrwx,0,0,182191-128-4,/Program Files/Splunk/var/lib/splunk/defaultdb/db/db_1320271900_1319756471_16/Sources.data

Tue Nov 01 2011 01:31:30,40688,macb,r/rrwxrwxrwx,0,0,168127-128-3,/Users/Dr Evil/AppData/Roaming/Dropbox/4eaea421

Tue Nov 01 2011 01:39:32,2,,a,b,r/rrwxrwxrwx,0,0,182649-128-1,/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.129.Crwl

Tue Nov 01 2011 01:39:33,2,m,c,,,r/rrwxrwxrwx,0,0,182649-128-1,/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.129.Crwl

Tue Nov 01 2011 02:00:20,65536,,a,,,r/rrwxrwxrwx,0,0,186531-128-3,/Windows/System32/catroot2/edb004AF.log

Tue Nov 01 2011 02:27:31,40432,macb,r/rrwxrwxrwx,0,0,158207-128-3,/Users/Dr Evil/AppData/Roaming/Dropbox/4eae142

Tue Nov 01 2011 07:25:07,32921,macb,r/rrwxrwxrwx,0,0,182226-128-1,/ProgramData/Microsoft/Windows/Power Efficiency Diagnostics/energy-report-2011-11-01.xml

Tue Nov 01 2011 07:30:47,25000022,,a,,,r/rrwxrwxrwx,0,0,15904-128-7,/Program Files/Splunk/var/log/splunk/audit.log.1

Tue Nov 01 2011 07:30:47,25000537,m,,,r/rrwxrwxrwx,0,0,65850-128-9,/Program Files/Splunk/var/log/splunk/audit.log.2

Tue Nov 01 2011 19:58:37,256,mac,,d/drwxrwxrwx,0,0,183324-144-1,/Program Files/Splunk/var/lib/splunk/_internaldb/db/db_1320138038_1318220238_153/rawdata

Tue Nov 01 2011 20:00:42,56,,b,d/drwxrwxrwx,0,0,196668-144-7,/Program Files/Splunk/var/lib/splunk/_internaldb/db/db_1320271897_1320138041_155

Tue Nov 01 2011 20:00:42,256,,b,d/drwxrwxrwx,0,0,196669-144-1,/Program Files/Splunk/var/lib/splunk/_internaldb/db/db_1320271897_1320138041_155/rawdata

Tue Nov 01 2011 20:00:42,18034,,a,b,r/rrwxrwxrwx,0,0,196675-128-4,/Program Files/Splunk/var/lib/splunk/_internaldb/db/db_1320271897_1320138041_155/Strings.data

Tue Nov 01 2011 20:04:23,8487249,,a,b,r/rrwxrwxrwx,0,0,183125-128-3,/Program Files/Splunk/var/lib/splunk/_internaldb/db/db_1320271897_1320138041_155/rawdata/journal.gz

Tue Nov 01 2011 20:04:23,45888,,a,b,r/rrwxrwxrwx,0,0,183277-128-3,/Program Files/Splunk/var/lib/splunk/_internaldb/db/db_1320271897_1320138041_155/rawdata/slices.dat

Tue Nov 01 2011 20:08:27,102,,a,b,r/rrwxrwxrwx,0,0,167573-128-1,/Program Files/Splunk/var/lib/splunk/_internaldb/db/db_1320271897_1320138041_155/Hosts.data

Tue Nov 01 2011 23:59:49,504225,m,,,r/rrwxrwxrwx,0,0,45879-128-3,/ProgramData/LogMeIn/LMI20111101.log

Wed Nov 02 2011 00:01:11,464781,,a,,,r/rrwxrwxrwx,0,0,15760-128-3,/ProgramData/LogMeIn/LMI20111102.log

Wed Nov 02 2011 00:01:11,504225,,c,,,r/rrwxrwxrwx,0,0,45879-128-3,/ProgramData/LogMeIn/LMI20111101.log

Wed Nov 02 2011 00:45:26,2,,a,b,r/rrwxrwxrwx,0,0,183168-128-1,/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.130.Crwl

The time traveller's toolkit

- **fls** for extracting file system metadata
- **log2timeline** for extracting other temporal metadata
- **mactime** for converting the results into a consistent CSV

... and one tool to analyse them all: **Splunk**

The time traveller's toolkit

- fls and mactime = www.sleuthkit.org
- log2timeline = log2timeline.net
- Splunk = www.splunk.com *“Take the sh out of IT”*

First two (and much more) is also provided pre-built on the **SIFT Workstation** Linux distro provided by Rob Lee of SANS at computer-forensics.sans.org

Extract file system timestamps

First we extract file system timestamps by pointing **fls** at a block device or raw forensic (dd) image:

```
fls -m "" -o offset -r image.dd > fls.body
```

- | | |
|------------------|---|
| -m "" | Output in mactime format and add a string |
| -o offset | Sector offset to the start of the file system |
| -r | Recurse through directories |
| image.dd | Raw forensic image (or device) to parse |
| fls.body | Output file |

Extract file system timestamps

Output looks something like this:

```
0 | /Users/Scott/Desktop/desktop.ini | 190064-128-1 | r/  
rr-xr-xr-x | 0 | 0 | 282 | 1321489198 | 1321489199 |  
1321489199 | 1321489198
```

Convert to mactime format

Convert our fls output into CSV using **mactime**:

```
mactime -b fls.body -d > fls.csv
```

-b fls.body Input file to parse

-d Output in CSV format

fls.csv Name of output file

```
Thu Nov 17 2011 11:19:59,282,m.c.,r/rr-xr-xr-x,  
0,0,190064-128-1,"/Users/Scott/Desktop/desktop.ini"
```

Extract other temporal data

Extract other temporal data by pointing **log2timeline** at the mounted file system:

```
log2timeline -f exif,pdf -o mactime -r -w  
log2timeline.body /mnt/volume
```

-f exif,pdf

Input modules to use

-o mactime

Output in mactime format

-r

Recurse through directories

-w log2timeline.body

Output file to write

/mnt/volume

Path to mounted volume

Beware when crossing timezones

- Each tool allows you to specify the source data timezone
- Each use a common switch: **-z *timezone* | local**
- I've found issues with specifying timezone on certain builds
- Recommend to test your build on known evidence first

Almost there ...

So now we have two files to import into Splunk:

- **fls.csv**
- **log2timeline.csv**

Just one small tweak; let's change the header from this:

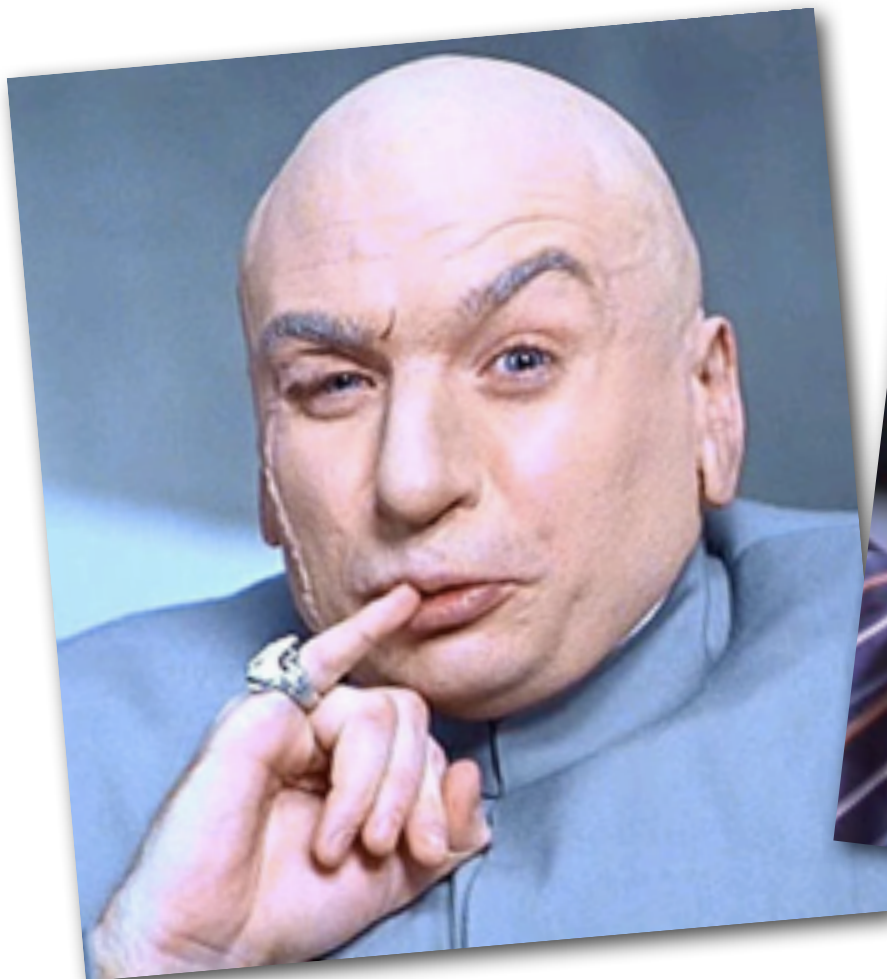
`Date,Size,Type,Mode,UID,GID,Meta,File Name`

To this:

`date,size,type,mode,uid,gid,meta,file`

Also need to apply Splunk customisations - see www.kleinco.com.au

Show me the money !!



Hotmail – scottydont2000@hotmail.com – Windows Live

http://co107w.col107.mail.live.com/default.aspx#!/mail/InboxLight.aspx?n Google

Splunk Nessus Google Maps Jupiter YouTube Wikipedia News (263) Popular LinkedIn MobileMe Easynews

Windows Live™ Hotmail (1) Messenger SkyDrive | ninemsn Scott Evil profile | sign out

Hotmail

New | Reply | Reply all | Forward | Delete | Junk | Sweep | Mark as | Move to | Options

Inbox (1)

Keep this for me Back to messages

Scott Evil 17/11/2011
To Scott Evil Reply

1 attachment (45.1 KB) Hotmail Active View

Secret pl...docx
View online
Download (45.1 KB)

Download as zip

File from the office.

New | Reply | Reply all | Forward | Delete | Junk | Sweep | Mark as | Move to

You're signed in to Messenger. To change your status, click your name in the upper right corner.
Keep me signed in | Sign out of Messenger

Search contacts


Your friends are offline right now.
Sign out of Messenger

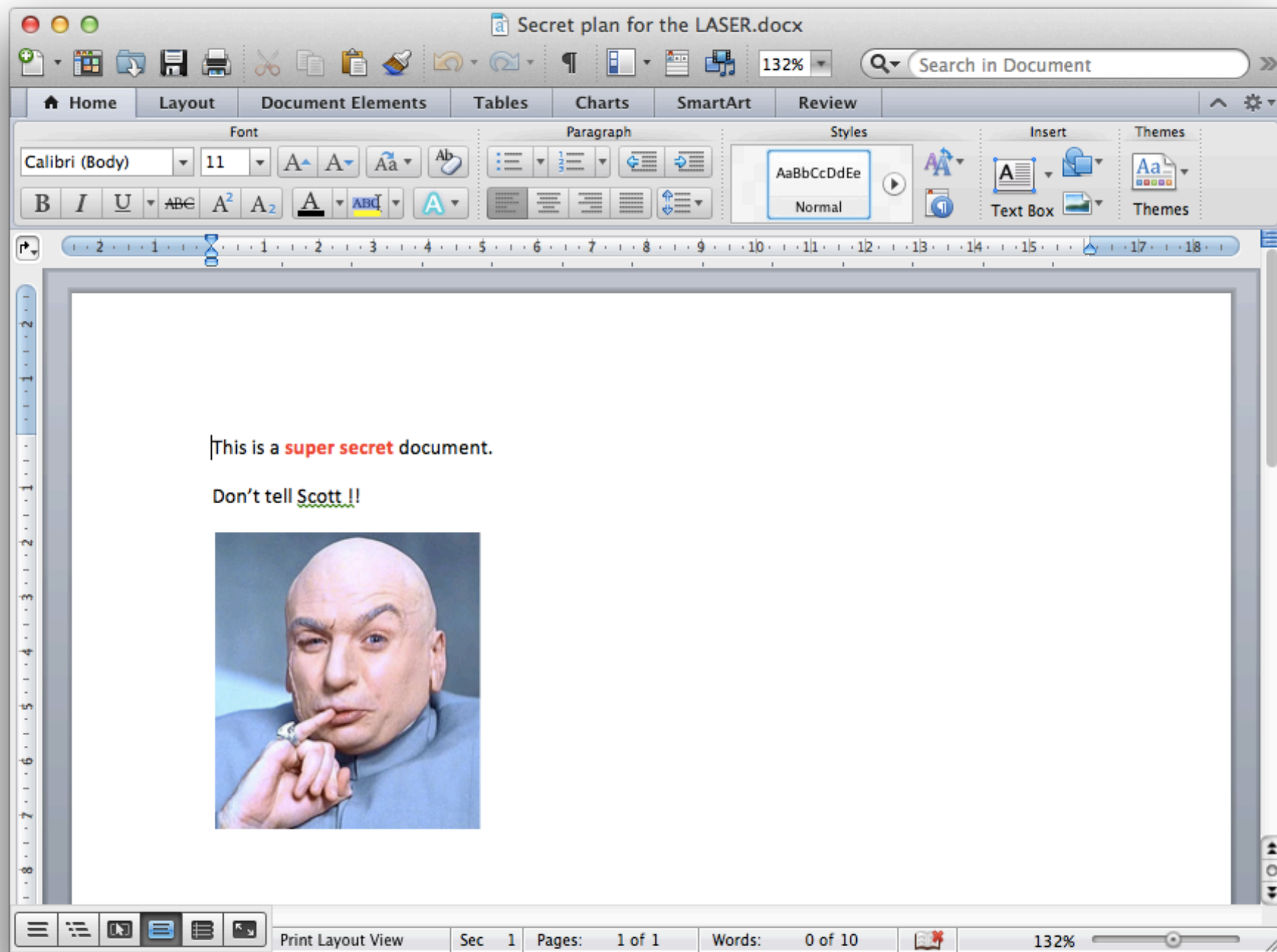
SENIOR DATING AUSTRALIA

Meet 50+ Singles In Your Area TODAY!

Register Here

www.be2.com.au





MAC Meaning by File System

- The MACB column changes depending on the file system that is being examined
- NTFS and EXT2/3 Systems identify "C" as the metadata change time
- File creation time is listed as a 'B' for file "Birth"

File System	Time Stored	Time Resolution	M	A	C	B
Ext2/3	Epoch	1 sec since Jan 1, 1970	Modified	Accessed	Inode Changed	
FAT	Local	Jan 1, 1980	Modified (2 sec)	Accessed Date (1 day)		Created (10 ms)
NTFS	UTC	100 ns since Jan 1, 1601	Modified	Accessed	MFT Modified	Created

Linux Time Rules

File Move	File Copy	File Access	File Modify	File Creation
Modified – No Change	Modified – Change	Modified – No Change	Modified – Change	Modified – Change
Access – No Change	Access - Change	Access – Change (unless noatime)	Access – No Change	Access – Change
Changed - Change	Changed – Change	Changed – No Change	Changed – Change	Changed – Change

Windows Time Rules \$STDINFO

File Rename	Local File Move	Volume File Move	File Copy	File Access	File Modify	File Creation	File Deletion
Modified – No Change	Modified – No Change	Modified – No Change	Modified – No Change	Modified – No Change	Modified – Change	Modified – Change	Modified – No Change
Access – No Change	Access – No Change	Access – Changed	Access – Changed	Access – Changed (No Change on Vista/Win7)	Access – No Change	Access – Change	Access – No Change
Creation – No Change	Creation – No Change	Creation – No Change	Creation – Changed	Creation – No Change	Creation – No Change	Creation – Change	Creation – No Change
Metadata – Changed	Metadata – Changed	Metadata – Changed	Metadata – Changed	Metadata – No Change	Metadata – No Change	Metadata – Change	Metadata – No Change

Windows Creation Time Rules

General Rules

- **Modification date** stays the same if a file is copied or moved. Always.
- **Creation date** and time depending on if file was copied or moved.

Creation date unchanged

- Move from C: \FAT to D: \NTFS
- Move from C: \FAT to C: \FAT\subdir
- Move from D: \NTFS to D: \NTFS\subdir

Creation date updated to current time

- Copy from C: \FAT to D: \NTFS
- Copy from C: \FAT to C: \FAT\subdir
- Copy from D: \NTFS to D: \NTFS\subdir

Traps for new time travellers

- Beware the CSI effect! Question all observations
- Know how programs and operating systems record time
- Consider the granularity of time; e.g. access times on FAT
- Know the common anomalies of timestamps
- These tools group events by second
- Consider “anti-forensic” situations
- This isn’t a complete history, since timestamps overwrite
- And it’s all based on the accuracy of computer clocks

Back to the future

If you set out to find something, you probably won't find it

But if you set out to find anything, you'll find something

- Reverses the traditional paradigm; let the evidence talk
- Provides context, therefore more detailed findings
- Can quickly identify relevant events and speed investigations
- Encourages further research, testing and learning

Thanks.

Klein & Co.
experts in computer forensics.