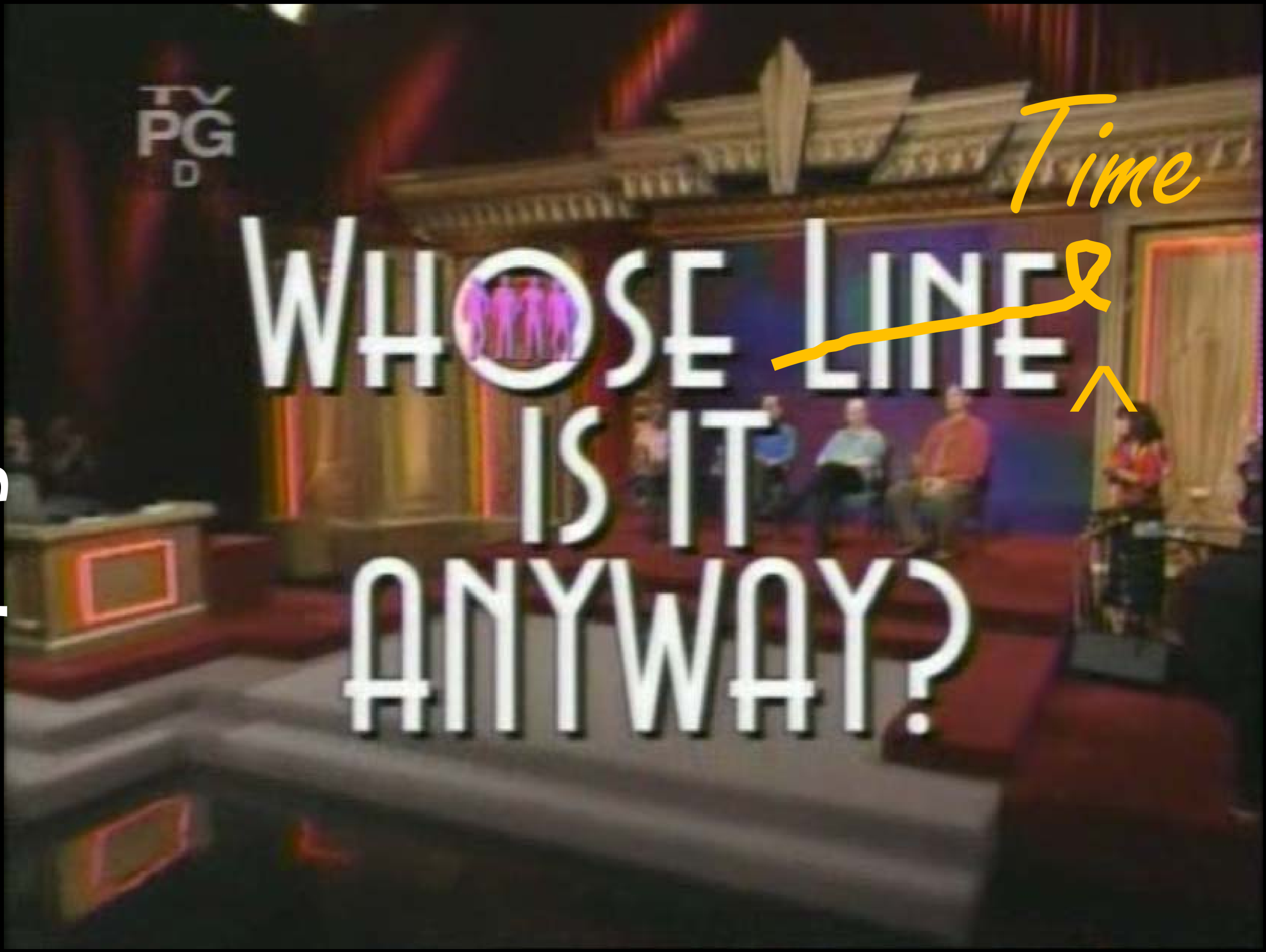
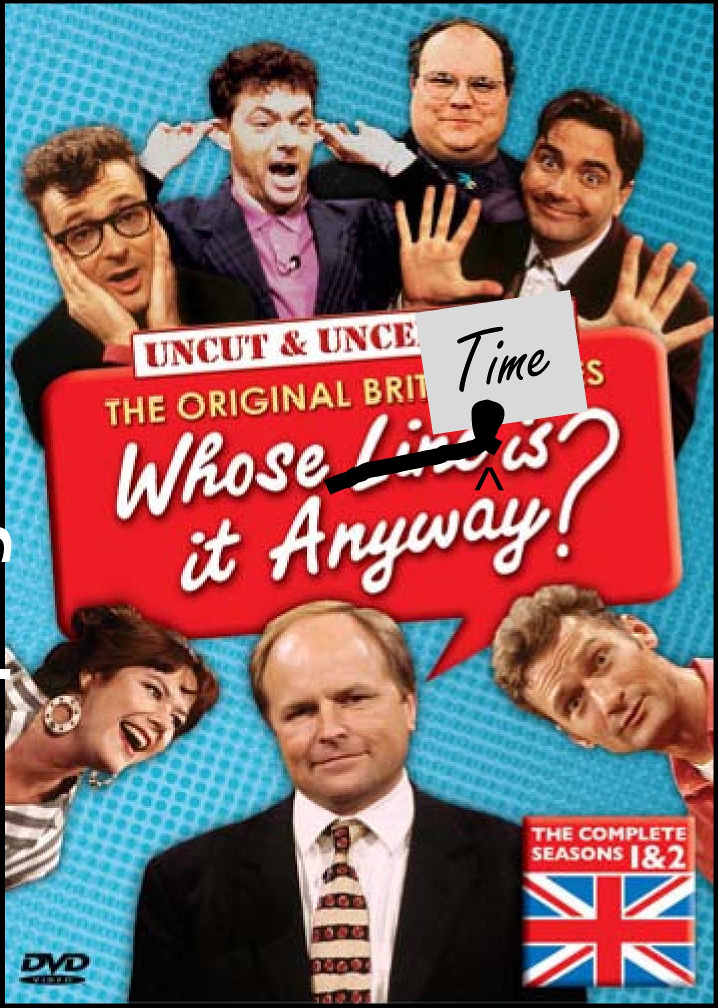
timestomping



For our guests from England, please allow me to translate.

timestomping



Quick background

Timestamps are important
in forensic analysis.

Timeline analysis is part
of event reconstruction.

Note: Timestamps and events are
analyzed in context, not isolation.

File	Creation Date	Last Accessed
File 127	08/04/11 10:22:36	08/04/11 10:22:3
File 128	08/04/11 10:22:37	08/04/11 10:22:3
File 129	08/04/11 10:22:37	08/04/11 10:22:3
File 130	08/04/11 10:22:37	08/04/11 10:22:3
File 131	08/04/11 10:22:38	08/04/11 10:44:1
File 132	08/04/11 10:22:41	08/04/11 10:22:4
File 133	08/04/11 10:22:42	08/04/11 10:22:4
File 134	08/04/11 10:22:43	08/04/11 10:22:4
File 135	08/04/11 10:22:43	08/04/11 10:54:0
File 136	08/04/11 10:22:43	08/04/11 10:22:4
File 137	08/04/11 10:22:45	08/04/11 10:22:4
File 138	08/04/11 10:22:46	09/06/06 08:00:0
File 139	08/04/11 10:22:47	08/04/11 10:22:4
File 140	08/04/11 10:22:47	08/04/11 10:22:4
File 141	08/04/11 10:22:47	08/04/11 10:39:5
File 142	08/04/11 10:22:48	08/04/11 10:22:4
File 143	08/04/11 10:22:54	08/04/11 10:22:5
File 144	08/04/11 10:22:58	08/04/11 10:22:5

To hide activities, the computer’s clock could be changed.

That poses a separate set of problems
and leaves its own trail of evidence.

Anti-forensic demonstration of timestomp.exe at BlackHat 2005

AttributeMagic has since joined the scene.

The tools modify timestamps
(Created, Accessed, Modified, MFT Entry)
to fool an unsuspecting user.

But here’s the rub:

The tools don’t modify all timestamps
and they don’t look for all artifacts.

There are eight timestamps, not four,
associated with a file on NTFS file systems.

All eight timestamps are in $MFT.

$STANDARD_INFORMATION
Type: 0x10
Min Size: 0x30
Max Size: 0x48

Read offset to attribute content and add:

- Created (0x00)
- Last Modified (0x08)
- MFT Entry Modified (0x10)
- Last Accessed (0x18)

$FILE_NAME
Type: 0x30
Min Size: 0x44
Max Size: 0x242

Read offset to attribute content and add:

- Created (0x08)
- Last Modified (0x10)
- MFT Entry Modified (0x18)
- Last Accessed (0x20)

All eight timestamps are in $MFT.

$STANDARD_INFORMATION
Type: 0x10
Min Size: 0x30
Max Size: 0x48

Read offset to attribute content and add:

- Created (0x00)
- Last Modified (0x08)
- MFT Entry Modified (0x10)
- Last Accessed (0x18)

$FILE_NAME
Type: 0x30
Min Size: 0x44
Max Size: 0x242

Read offset to attribute content and add:

- Created (0x08)
- Last Modified (0x10)
- MFT Entry Modified (0x18)
- Last Accessed (0x20)

These are modified by the timestomp and AttributeMagic.
These are read by tools such as EnCase and FTK.

All eight timestamps are in $MFT.

$STANDARD_INFORMATION
Type: 0x10
Min Size: 0x30
Max Size: 0x48

Read offset to attribute content and add:

- Created (0x00)
- Last Modified (0x08)
- MFT Entry Modified (0x10)
- Last Accessed (0x18)

$FILE_NAME
Type: 0x30
Min Size: 0x44
Max Size: 0x242

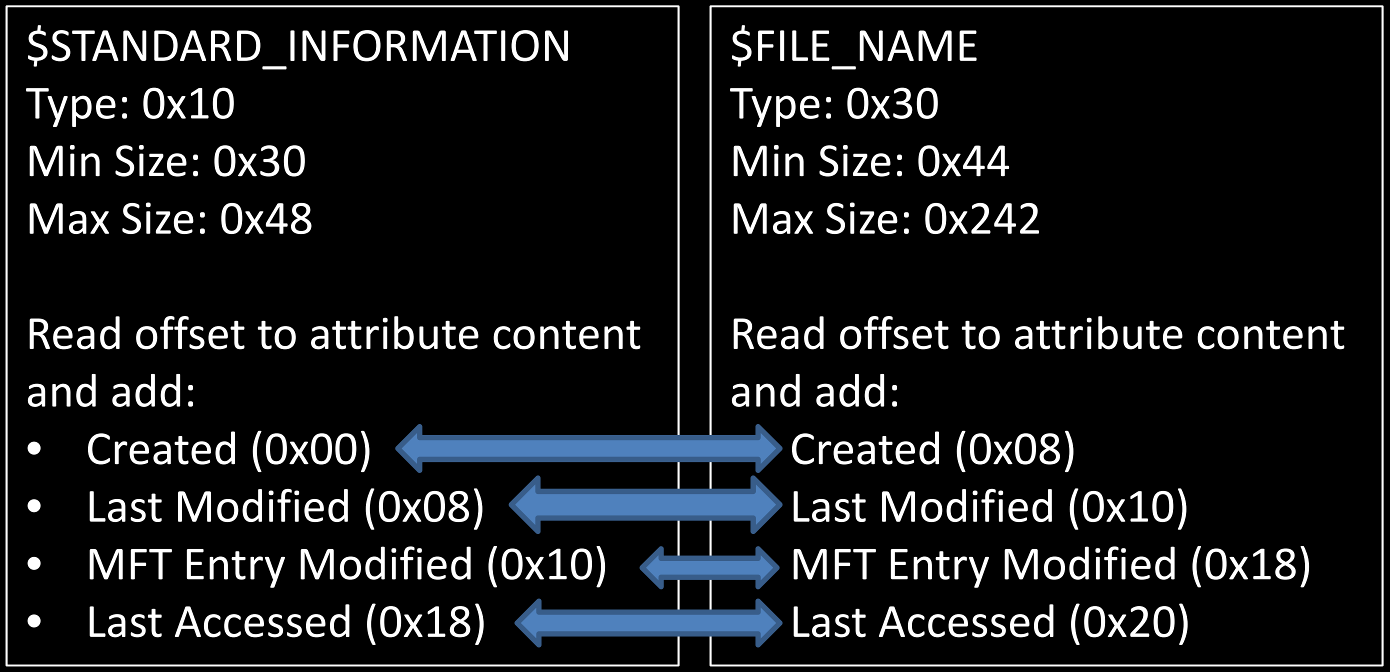
Read offset to attribute content and add:

- Created (0x08)
- Last Modified (0x10)
- MFT Entry Modified (0x18)
- Last Accessed (0x20)

These can be analyzed,
but it takes more work.

Many analysts would need a reason
to start doing this extra work.

All eight timestamps are in $MFT.



$STANDARD_INFORMATION
Type: 0x10
Min Size: 0x30
Max Size: 0x48

Read offset to attribute content and add:

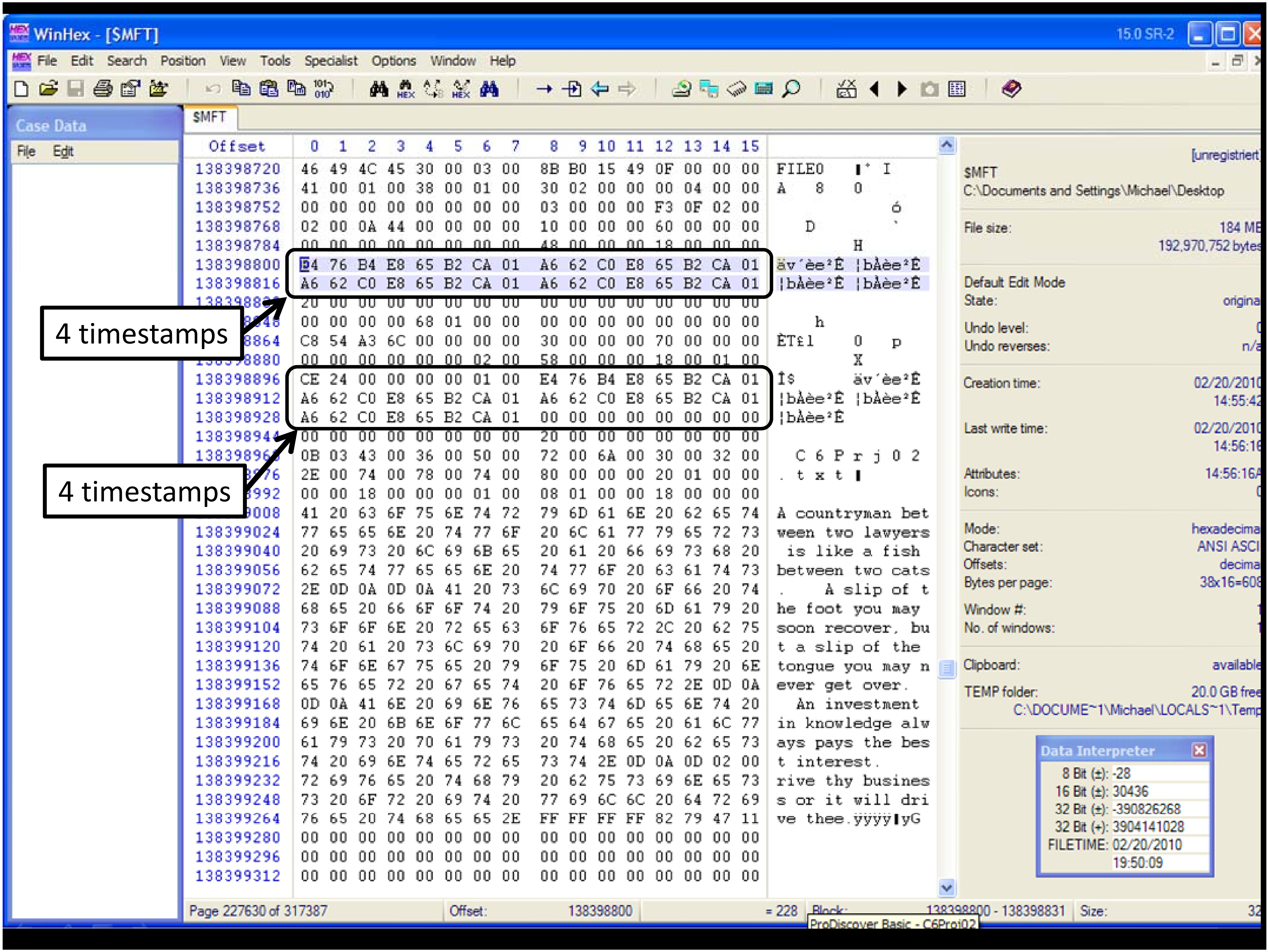
- Created (0x00)
- Last Modified (0x08)
- MFT Entry Modified (0x10)
- Last Accessed (0x18)

$FILE_NAME
Type: 0x30
Min Size: 0x44
Max Size: 0x242

Read offset to attribute content and add:

- Created (0x08)
- Last Modified (0x10)
- MFT Entry Modified (0x18)
- Last Accessed (0x20)

The values in each attribute can be compared, but it takes work.



```
Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
138398720  46 49 4C 45 30 00 03 00  8B B0 15 49 0F 00 00 00  FILE0    ▮˚ I
138398736  41 00 01 00 38 00 01 00  30 02 00 00 00 04 00 00  A   8   0
138398752  00 00 00 00 00 00 00 00  03 00 00 00 F3 0F 02 00              ó
138398768  02 00 0A 44 00 00 00 00  10 00 00 00 60 00 00 00     D        `
138398784  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
138398800  E4 76 B4 E8 65 B2 CA 01  A6 62 C0 E8 65 B2 CA 01  äv´èe²Ê ¦bÀèe²Ê
138398816  A6 62 C0 E8 65 B2 CA 01  A6 62 C0 E8 65 B2 CA 01  ¦bÀèe²Ê ¦bÀèe²Ê
1383988    20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
     8848  00 00 00 00 68 01 00 00  00 00 00 00 00 00 00 00       h
     8864  C8 54 A3 6C 00 00 00 00  30 00 00 00 70 00 00 00  ÈT£l     0   p
     8880  00 00 00 00 00 00 02 00  58 00 00 00 18 00 01 00           X
138398896  CE 24 00 00 00 00 01 00  E4 76 B4 E8 65 B2 CA 01  Î$       äv´èe²Ê
138398912  A6 62 C0 E8 65 B2 CA 01  A6 62 C0 E8 65 B2 CA 01  ¦bÀèe²Ê ¦bÀèe²Ê
138398928  A6 62 C0 E8 65 B2 CA 01  00 00 00 00 00 00 00 00  ¦bÀèe²Ê
13839894   00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
13839896   0B 03 43 00 36 00 50 00  72 00 6A 00 30 00 32 00    C 6 P r j 0 2
      976  2E 00 74 00 78 00 74 00  80 00 00 00 20 01 00 00  . t x t ▮
      992  00 00 18 00 00 00 01 00  08 01 00 00 18 00 00 00
     9008  41 20 63 6F 75 6E 74 72  79 6D 61 6E 20 62 65 74  A countryman bet
138399024  77 65 65 6E 20 74 77 6F  20 6C 61 77 79 65 72 73  ween two lawyers
138399040  20 69 73 20 6C 69 6B 65  20 61 20 66 69 73 68 20   is like a fish
138399056  62 65 74 77 65 65 6E 20  74 77 6F 20 63 61 74 73  between two cats
138399072  2E 0D 0A 0D 0A 41 20 73  6C 69 70 20 6F 66 20 74  .    A slip of t
138399088  68 65 20 66 6F 6F 74 20  79 6F 75 20 6D 61 79 20  he foot you may
138399104  73 6F 6F 6E 20 72 65 63  6F 76 65 72 2C 20 62 75  soon recover, bu
138399120  74 20 61 20 73 6C 69 70  20 6F 66 20 74 68 65 20  t a slip of the
138399136  74 6F 6E 67 75 65 20 79  6F 75 20 6D 61 79 20 6E  tongue you may n
138399152  65 76 65 72 20 67 65 74  20 6F 76 65 72 2E 0D 0A  ever get over.
138399168  0D 0A 41 6E 20 69 6E 76  65 73 74 6D 65 6E 74 20    An investment
138399184  69 6E 20 6B 6E 6F 77 6C  65 64 67 65 20 61 6C 77  in knowledge alw
138399200  61 79 73 20 70 61 79 73  20 74 68 65 20 62 65 73  ays pays the bes
138399216  74 20 69 6E 74 65 72 65  73 74 2E 0D 0A 0D 02 00  t interest.
138399232  72 69 76 65 20 74 68 79  20 62 75 73 69 6E 65 73  rive thy busines
138399248  73 20 6F 72 20 69 74 20  77 69 6C 6C 20 64 72 69  s or it will dri
138399264  76 65 20 74 68 65 65 2E  FF FF FF FF 82 79 47 11  ve thee.ÿÿÿÿ▮yG
138399280  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
138399296  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
138399312  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

4 timestamps

4 timestamps

[unregistriert]

$MFT
C:\Documents and Settings\Michael\Desktop

File size: 184 MB
192,970,752 bytes

Default Edit Mode
State: origina

Undo level: 0
Undo reverses: n/a

Creation time: 02/20/2010
14:55:42

Last write time: 02/20/2010
14:56:16

Attributes: 14:56:16A
Icons: 0

Mode: hexadecima
Character set: ANSI ASCI
Offsets: decima
Bytes per page: 38x16=608

Window #: 1
No. of windows: 1

Clipboard: available

TEMP folder: 20.0 GB free
C:\DOCUME~1\Michael\LOCALS~1\Temp

Data Interpreter

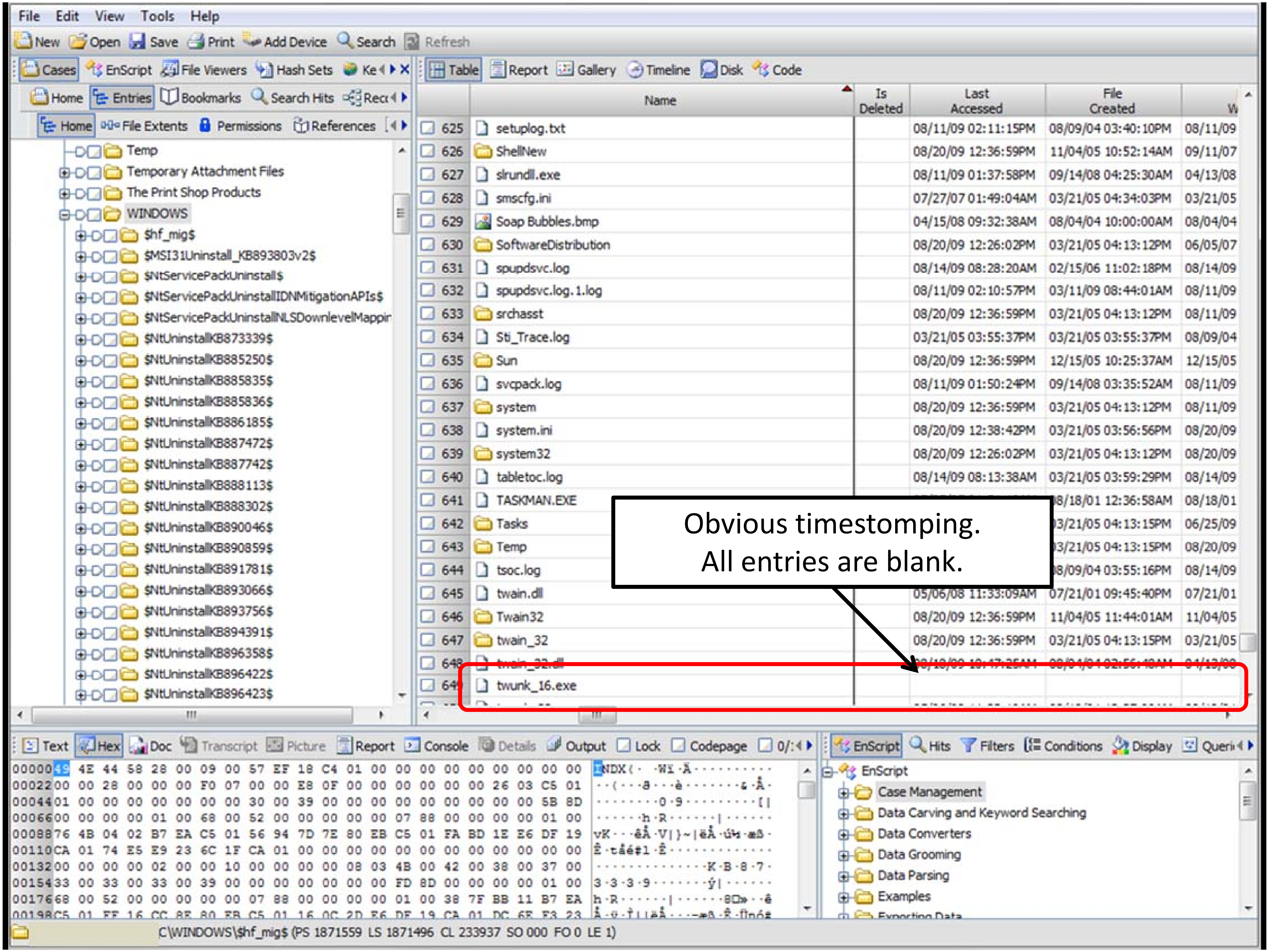
8 Bit (±): -28
16 Bit (±): 30436
32 Bit (±): -390826268
32 Bit (+): 3904141028
FILETIME: 02/20/2010
19:50:09

Page 227630 of 317387 | Offset: 138398800 | = 228 | Block: 138398800 - 138398831 | Size: 32

ProDiscover Basic - C6Proj02

So what would give an examiner a reason to start digging?

Obvious timestomping


File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases EnScript File Viewers Hash Sets Ke
Table Report Gallery Timeline Disk Code
Home Entries Bookmarks Search Hits Reco
Home File Extents Permissions References
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/:
EnScript Hits Filters Conditions Display Queri

```
Temp
Temporary Attachment Files
The Print Shop Products
WINDOWS
  $hf_mig$
  $MSI31Uninstall_KB893803v2$
  $NtServicePackUninstall$
  $NtServicePackUninstallIDNMitigationAPIs$
  $NtServicePackUninstallNLSDownlevelMappir
  $NtUninstallKB873339$
  $NtUninstallKB885250$
  $NtUninstallKB885835$
  $NtUninstallKB885836$
  $NtUninstallKB886185$
  $NtUninstallKB887472$
  $NtUninstallKB887742$
  $NtUninstallKB888113$
  $NtUninstallKB888302$
  $NtUninstallKB890046$
  $NtUninstallKB890859$
  $NtUninstallKB891781$
  $NtUninstallKB893066$
  $NtUninstallKB893756$
  $NtUninstallKB894391$
  $NtUninstallKB896358$
  $NtUninstallKB896422$
  $NtUninstallKB896423$
```

	Name	Is Deleted	Last Accessed	File Created	W
625	setuplog.txt		08/11/09 02:11:15PM	08/09/04 03:40:10PM	08/11/09
626	ShellNew		08/20/09 12:36:59PM	11/04/05 10:52:14AM	09/11/07
627	slrundll.exe		08/11/09 01:37:58PM	09/14/08 04:25:30AM	04/13/08
628	smscfg.ini		07/27/07 01:49:04AM	03/21/05 04:34:03PM	03/21/05
629	Soap Bubbles.bmp		04/15/08 09:32:38AM	08/04/04 10:00:00AM	08/04/04
630	SoftwareDistribution		08/20/09 12:26:02PM	03/21/05 04:13:12PM	06/05/07
631	spupdsvc.log		08/14/09 08:28:20AM	02/15/06 11:02:18PM	08/14/09
632	spupdsvc.log.1.log		08/11/09 02:10:57PM	03/11/09 08:44:01AM	08/11/09
633	srchasst		08/20/09 12:36:59PM	03/21/05 04:13:12PM	08/11/09
634	Sti_Trace.log		03/21/05 03:55:37PM	03/21/05 03:55:37PM	08/09/04
635	Sun		08/20/09 12:36:59PM	12/15/05 10:25:37AM	12/15/05
636	svcpack.log		08/11/09 01:50:24PM	09/14/08 03:35:52AM	08/11/09
637	system		08/20/09 12:36:59PM	03/21/05 04:13:12PM	08/11/09
638	system.ini		08/20/09 12:38:42PM	03/21/05 03:56:56PM	08/20/09
639	system32		08/20/09 12:26:02PM	03/21/05 04:13:12PM	08/20/09
640	tabletoc.log		08/14/09 08:13:38AM	03/21/05 03:59:29PM	08/14/09
641	TASKMAN.EXE			8/18/01 12:36:58AM	08/18/01
642	Tasks			3/21/05 04:13:15PM	06/25/09
643	Temp			3/21/05 04:13:15PM	08/20/09
644	tsoc.log			8/09/04 03:55:16PM	08/14/09
645	twain.dll		05/06/08 11:33:09AM	07/21/01 09:45:40PM	07/21/01
646	Twain32		08/20/09 12:36:59PM	11/04/05 11:44:01AM	11/04/05
647	twain_32		08/20/09 12:36:59PM	03/21/05 04:13:15PM	03/21/05
648	twain_32.dll		08/18/09 10:47:25AM	08/04/04 02:56:48AM	04/13/08
649	twunk_16.exe				

Obvious timestomping.
All entries are blank.

```
0000049 4E 44 58 28 00 09 00 57 EF 18 C4 01 00 00 00 00 00 00 00 00 INDX(··WïÄ··········
0002200 00 28 00 00 00 F0 07 00 00 E8 0F 00 00 00 00 00 00 26 03 C5 01 ··(···ð···è·······&·Å·
0004401 00 00 00 00 00 00 00 30 00 39 00 00 00 00 00 00 00 00 00 5B 8D ········0·9·········[|
0006600 00 00 00 01 00 68 00 52 00 00 00 00 00 07 88 00 00 00 00 01 00 ······h·R······|······
0008876 4B 04 02 B7 EA C5 01 56 94 7D 7E 80 EB C5 01 FA BD 1E E6 DF 19 vK··êÅ·V|}~|ëÅ·ú½·æß·
00110CA 01 74 E5 E9 23 6C 1F CA 01 00 00 00 00 00 00 00 00 00 00 00 Ê·tåé#l·Ê············
0013200 00 00 00 02 00 00 10 00 00 00 00 08 03 4B 00 42 00 38 00 37 00 ·············K·B·8·7·
0015433 00 33 00 33 00 39 00 00 00 00 00 00 00 FD 8D 00 00 00 00 01 00 3·3·3·9·······ý|······
0017668 00 52 00 00 00 00 00 07 88 00 00 00 00 01 00 38 7F BB 11 B7 EA h·R······|······8□»··ê
00198C5 01 FF 16 CC 8E 80 EB C5 01 16 0C 2D E6 DF 19 CA 01 DC 6E F3 23 Å·ÿ·Ì|||ëÅ···-æß·Ê·Ünó#
```

C\WINDOWS\hf_mig (PS 1871559 LS 1871496 CL 233937 SO 000 FO 0 LE 1)

Example

Inconsistent timestamps with respect to MFT.

Example

Timestamps matching the OS release date.

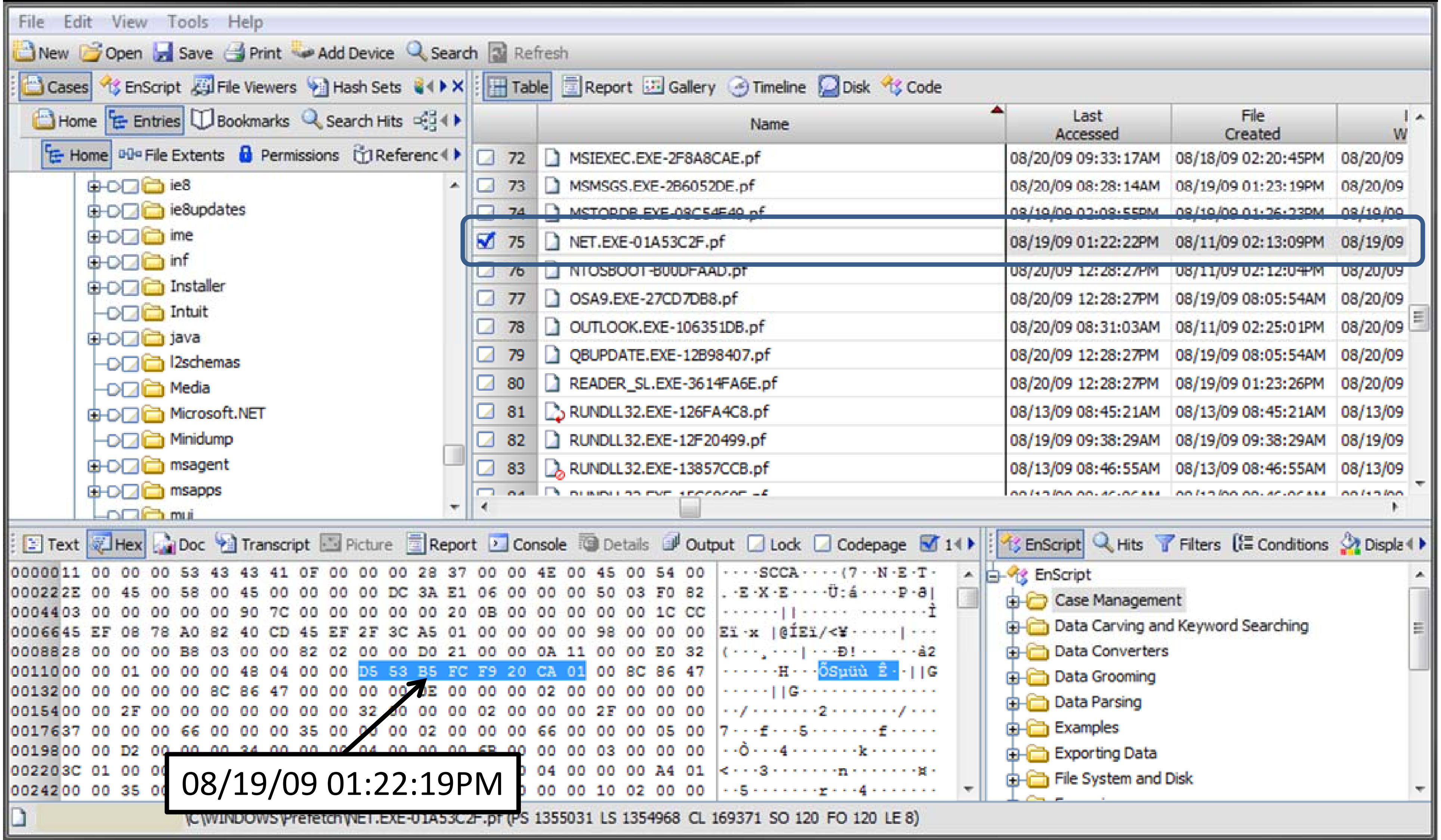
Remember: forensic timelines are built on context.

Running executables can leave a trail in
the Windows Prefetch and the Registry (MRU)

The problem with the Windows Prefetch…

A Windows Prefetch file (.pf) has eight time stamps ($STANDARD_INFORMATION, $FILE_NAME).

There is also an embedded timestamp of the last time the executable was run.



File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases EnScript File Viewers Hash Sets
Home Entries Bookmarks Search Hits
Home File Extents Permissions Referenc
ie8
ie8updates
ime
inf
Installer
Intuit
java
l2schemas
Media
Microsoft.NET
Minidump
msagent
msapps
mui
Table Report Gallery Timeline Disk Code
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage
EnScript Hits Filters Conditions Displa
EnScript
Case Management
Data Carving and Keyword Searching
Data Converters
Data Grooming
Data Parsing
Examples
Exporting Data
File System and Disk

		Name	Last Accessed	File Created	W
□	72	MSIEXEC.EXE-2F8A8CAE.pf	08/20/09 09:33:17AM	08/18/09 02:20:45PM	08/20/09
□	73	MSMSGS.EXE-2B6052DE.pf	08/20/09 08:28:14AM	08/19/09 01:23:19PM	08/20/09
□	74	MSTORDB.EXE-08C54E49.pf	08/19/09 02:08:55PM	08/19/09 01:26:23PM	08/19/09
☑	75	NET.EXE-01A53C2F.pf	08/19/09 01:22:22PM	08/11/09 02:13:09PM	08/19/09
□	76	NTOSBOOT-B00DFAAD.pf	08/20/09 12:28:27PM	08/11/09 02:12:04PM	08/20/09
□	77	OSA9.EXE-27CD7DB8.pf	08/20/09 12:28:27PM	08/19/09 08:05:54AM	08/20/09
□	78	OUTLOOK.EXE-106351DB.pf	08/20/09 08:31:03AM	08/11/09 02:25:01PM	08/20/09
□	79	QBUPDATE.EXE-12B98407.pf	08/20/09 12:28:27PM	08/19/09 08:05:54AM	08/20/09
□	80	READER_SL.EXE-3614FA6E.pf	08/20/09 12:28:27PM	08/19/09 01:23:26PM	08/20/09
□	81	RUNDLL32.EXE-126FA4C8.pf	08/13/09 08:45:21AM	08/13/09 08:45:21AM	08/13/09
□	82	RUNDLL32.EXE-12F20499.pf	08/19/09 09:38:29AM	08/19/09 09:38:29AM	08/19/09
□	83	RUNDLL32.EXE-13857CCB.pf	08/13/09 08:46:55AM	08/13/09 08:46:55AM	08/13/09

```
0000011 00 00 00 53 43 43 41 0F 00 00 00 28 37 00 00 4E 00 45 00 54 00   ····SCCA····(7··N·E·T·
000222E 00 45 00 58 00 45 00 00 00 00 DC 3A E1 06 00 00 00 50 03 F0 82   .·E·X·E····Ü:á····P·ð|
0004403 00 00 00 00 00 90 7C 00 00 00 00 00 20 0B 00 00 00 00 00 1C CC   ······||·····  ·······Ì
0006645 EF 08 78 A0 82 40 CD 45 EF 2F 3C A5 01 00 00 00 00 98 00 00 00   Eï·x |@ÍEï/<¥·····|···
0008828 00 00 00 B8 03 00 00 82 02 00 00 D0 21 00 00 0A 11 00 00 E0 32   (···¸···|···Ð!·····à2
0011000 00 01 00 00 00 48 04 00 00 D5 53 B5 FC F9 20 CA 01 00 8C 86 47   ······H···ÕSµüù Ê·||G
0013200 00 00 00 00 8C 86 47 00 00 00 00 E 00 00 00 02 00 00 00 00 00   ·····||G··············
0015400 00 2F 00 00 00 00 00 00 00 32 00 00 00 02 00 00 00 2F 00 00 00   ··/·······2·······/···
0017637 00 00 00 66 00 00 00 35 00 0 00 02 00 00 00 66 00 00 00 05 00   7···f···5·······f·····
0019800 00 D2 00 00 00 34 00 00 00 04 00 00 00 6B 00 00 00 03 00 00 00   ··Ò···4·······k·······
002203C 01 00 0                                 04 00 00 00 A4 01   <···3·······n·······¤·
0024200 00 35 0                                 00 00 10 02 00 00   ··5·······r···4·······
```

08/19/09 01:22:19PM

\C\WINDOWS\Prefetch\NET.EXE-01A53C2F.pf (PS 1355031 LS 1354968 CL 169371 SO 120 FO 120 LE 8)

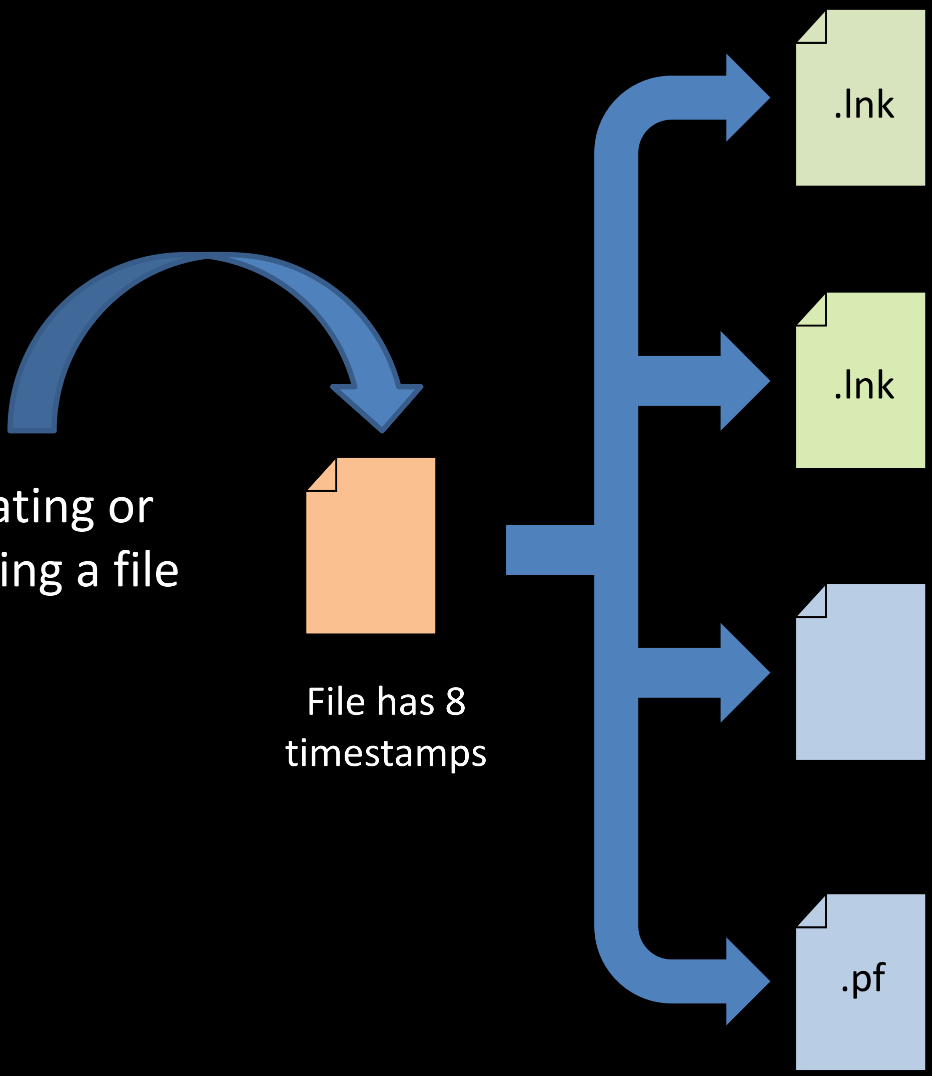
If the running of an executable needs to be done stealthily, the timestamps in the Prefetch file need to be modified, or the Prefetch file needs to be deleted entirely.

The MRU values in the Registry

Modified Registry entries
Stored in ROT-13

Data files can be a problem as well.

What happens when a file is created or opened?



Creating or opening a file

File has 8 timestamps

Created files will have a shortcut in the Windows Recent directory. (8 timestamps)

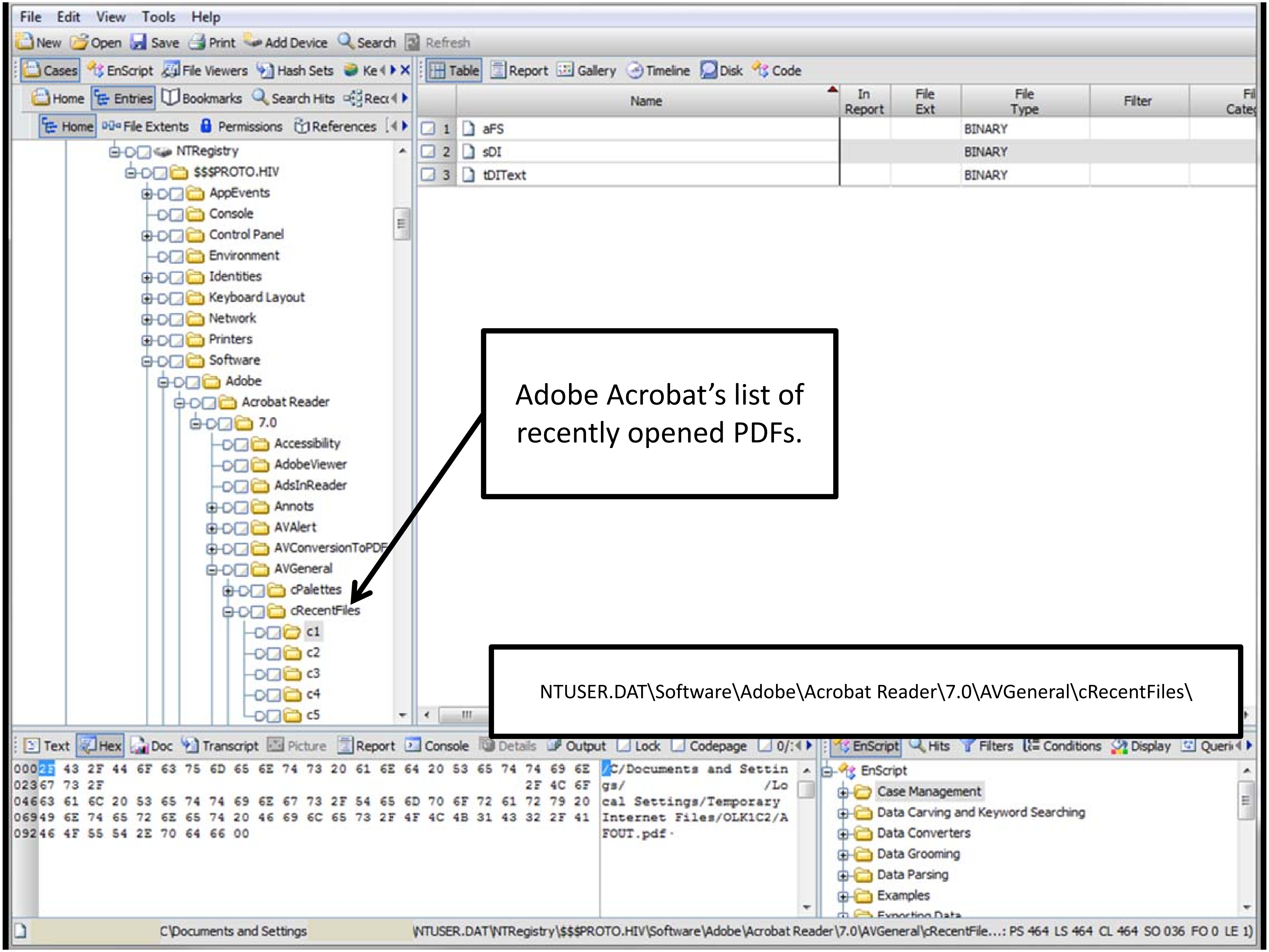
If it’s an Office file, there will be a shortcut in the Office’s Recent directory. (8 timestamps)

Many applications keep a list of recent files on a menu. Data can be stored in the Windows Registry (NTUSER.DAT). (Sometimes the keys have dates.)

The file’s name could appear in the Windows Prefetch file, which monitors the system for up to 10 seconds. (9 timestamps)

Example

Opening an accounting spreadsheet.


File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases EnScript File Viewers Hash Sets Ke
Table Report Gallery Timeline Disk Code
Home Entries Bookmarks Search Hits Reco
Home File Extents Permissions References
NTRegistry
$$$PROTO.HIV
AppEvents
Console
Control Panel
Environment
Identities
Keyboard Layout
Network
Printers
Software
Adobe
Acrobat Reader
7.0
Accessibility
AdobeViewer
AdsInReader
Annots
AVAlert
AVConversionToPDF
AVGeneral
cPalettes
cRecentFiles
c1
c2
c3
c4
c5
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/:
EnScript Hits Filters Conditions Display Queri
EnScript
Case Management
Data Carving and Keyword Searching
Data Converters
Data Grooming
Data Parsing
Examples
Exporting Data

		Name	In Report	File Ext	File Type	Filter	File Categ
□	1	aFS			BINARY		
□	2	sDI			BINARY		
□	3	tDIText			BINARY		

```
0002F 43 2F 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E  /C/Documents and Settin
02367 73 2F                                                      2F 4C 6F  gs/             /Lo
04663 61 6C 20 53 65 74 74 69 6E 67 73 2F 54 65 6D 70 6F 72 61 72 79 20  cal Settings/Temporary
06949 6E 74 65 72 6E 65 74 20 46 69 6C 65 73 2F 4F 4C 4B 31 43 32 2F 41  Internet Files/OLK1C2/A
09246 4F 55 54 2E 70 64 66 00                                              FOUT.pdf·
```

C\Documents and Settings   \NTUSER.DAT\NTRegistry\$$$PROTO.HIV\Software\Adobe\Acrobat Reader\7.0\AVGeneral\cRecentFile...: PS 464 LS 464 CL 464 SO 036 FO 0 LE 1)

Adobe Acrobat's list of recently opened PDFs.

NTUSER.DAT\Software\Adobe\Acrobat Reader\7.0\AVGeneral\cRecentFiles\

Granularity

NTFS stores time in 64 bit values, which gives an accuracy down to
100 nanoseconds since January 1, 1601.

Timestomp.exe and Magic Attribute only go down to the nearest second.

If the values in the attributes are examined,
timestomping will be obvious…

…unless an existing timestamp value is copied into the attribute.
(Don’t stomp it outright, copy it from another source.)

Example

Rounded timestamp values

Bottom Line:

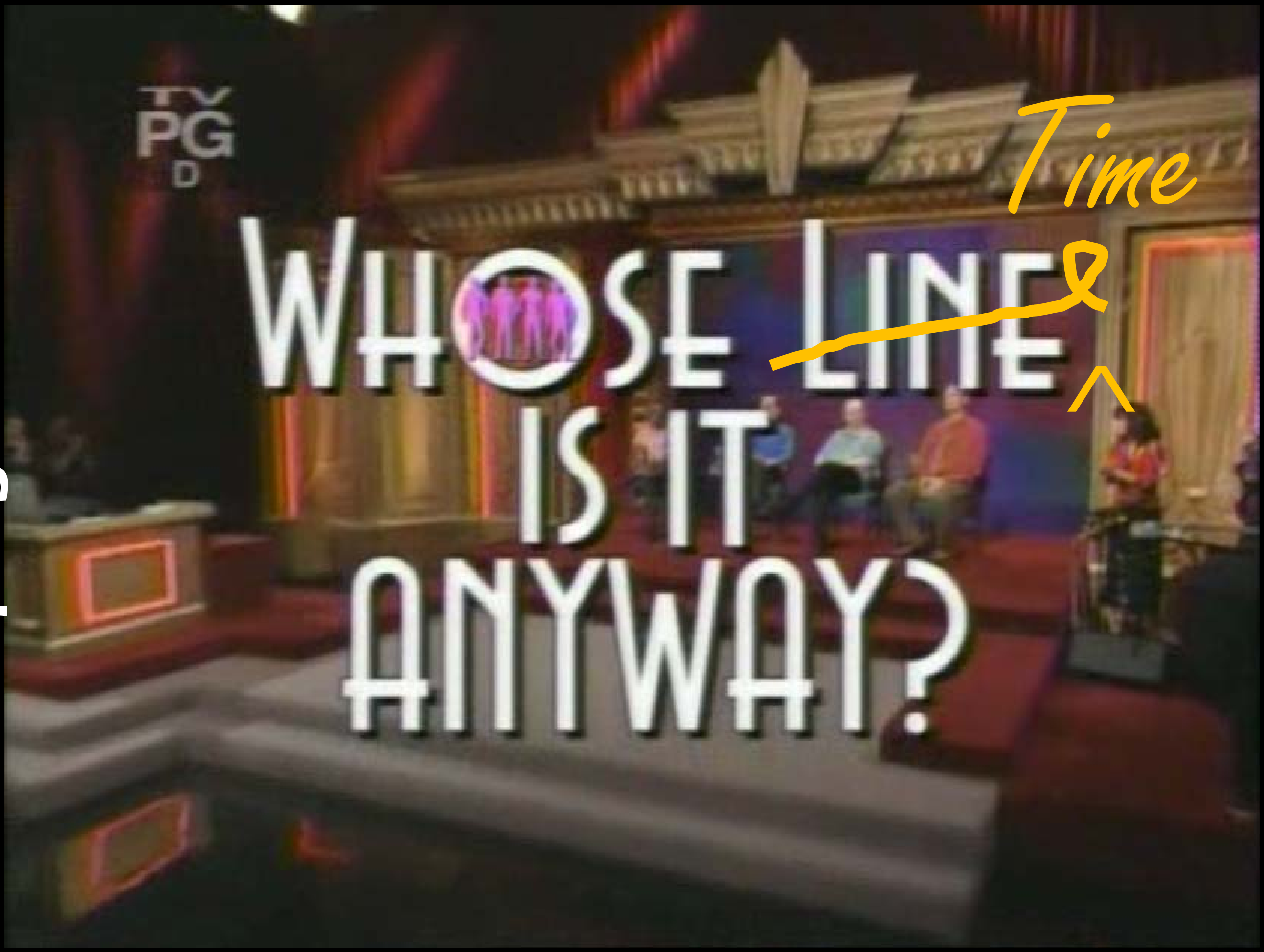
It’s damn near impossible to change all of the timestamps associated with running an executable.

Change (or delete) enough data to avoid detection.

Want a copy?

gimmethepresentation@gmail.com

timestomping


TV PG D
WHOSE ~~LINE~~ Time
IS IT
ANYWAY?