

 (<http://twitter.com/chadtilbury>)  (<http://plus.google.com/+ChadTilbury>)

 (<http://www.linkedin.com/in/chadtilbury>)  (<http://www.amazon.com/gp/pdp/profile/AKYG9NCGR570Y>)
 (<http://feeds.feedburner.com/ForensicMethods>)
<http://forensimethods.com>

FORENSICMETHODS

Home (<http://forensimethods.com>) /

Computer Forensics (<http://forensimethods.com/category/computer-forensics>) / NTFS \$I30 Index

Attributes: Evidence of Deleted and Overwritten Files



NTFS \$I30 Index Attributes: Evidence of Deleted

and Overwritten Files

By Chad Tilbury (<http://forensimethods.com/author/chadtilbury>) on September 26, 2011 in Computer Forensics (<http://forensimethods.com/category/computer-forensics>) — 7 Comments (<http://forensimethods.com/ntfs-index-attribute#comments>)

Note: This post originally appeared on the SANS Forensics blog

Daunting as it may seem, one of the most wonderful aspects of Windows forensics is its complexity. One of the fascinating aspects of digital forensics is how we often leverage conventional operating system features to provide information peripheral to their original design. One such feature is the Windows NTFS Index Attribute, also known as the \$I30 file. Knowing how to parse \$I30 attributes provides a fantastic means to identify deleted files, including those that have been wiped or overwritten.

A Simple Description of Index Attributes

Many popular file systems such as FAT and Unix store directory information as a simple flat file. Recognizing efficiency issues with lookups within large flat files, NTFS employed B-tree indexing for several of its building blocks, providing efficient storage of large data sets and very

fast lookups. As forensic examiners, we can take advantage of the NTFS B-tree implementation as another source to identify files that once existed in a given directory.

Similar to Master File Table (MFT) entries in NTFS, index entries within the B-tree are not completely removed when file deletion occurs. Instead, they are marked as deleted using a corresponding \$BITMAP attribute. Additionally, the size of index nodes can vary, particularly for large filenames, providing a type of slack that can hold previously existing filenames. Since B-tree nodes are regularly shuffled to keep the tree balanced, file name remnants are scattered and it is a common occurrence to find duplicate nodes referencing the same file. Of course, the flip side of re-balancing a B-tree is that it often results in data within unallocated nodes being overwritten. Thus while we commonly find evidence of long lost files within \$I30 attributes, there is no guarantee they will be present.

Interestingly, NTFS directory index entries utilize a \$FILE_NAME attribute type to store file information within the index. You may recall that this is the same attribute employed by the MFT and hence it provides a treasure trove of information about the file:

- Full filename
- Parent directory (useful if you recover a \$I30 file in free space and do not know its origin)
- File size
- Creation Time
- Modification Time
- MFT Change Time
- Access Time

Timestamps Found Within Index Attributes

A key distinction when reviewing timestamps stored within \$I30 files is that these timestamps are \$FILE_NAME attribute timestamps and not \$STANDARD_INFORMATION timestamps that we regularly view in Windows Explorer, your favorite GUI forensics tool, and within timelines. This distinction deserves a blog post of its own, but suffice to say \$FILE_NAME times are often updated in a much different (and even more arbitrary) set of circumstances.

Fortunately, for \$I30 files, I have observed that this set of timestamps tends to mirror those that are in \$STANDARD_INFORMATION. Thus even if the original file no longer exists, we may still be able to identify its name, file size, and original timestamps!

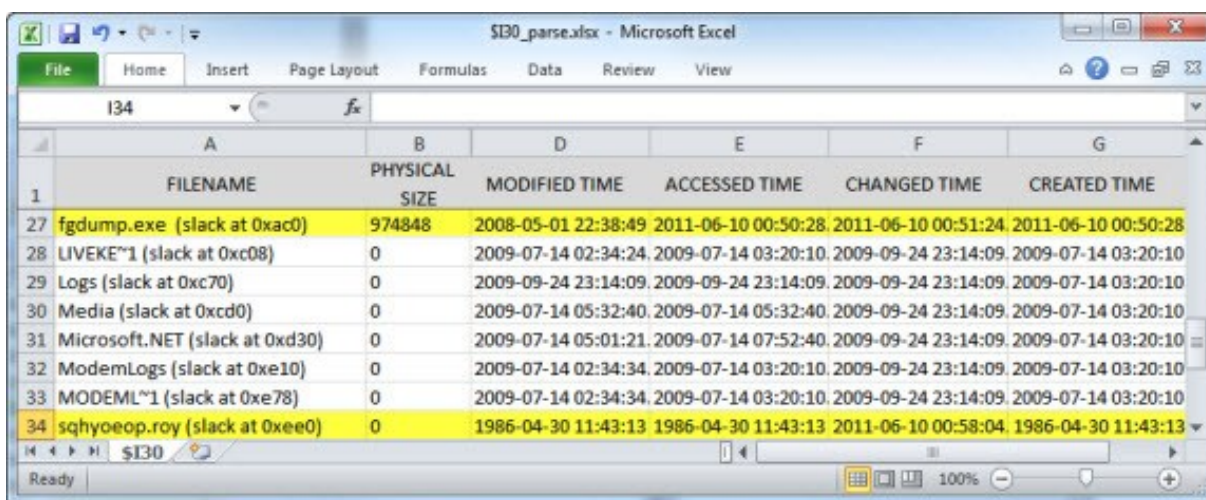
\$I30 Files in Practice

A few examples can better illustrate how useful these entries can be. I recently had a case where it appeared a large number of files were moved to the Recycle Bin, which was subsequently emptied and most of the corresponding INFO2 file was reallocated. The \$I30 file

still contained information on many of those files (albeit renamed according to the Recycle Bin schema). By analyzing the MFT Change Times of the \$I30 index entries, I was able to determine when the user placed each file within the Recycle Bin, and collect a list of what types of files were “recycled” using their file extensions.

In a malware or intrusion case, \$I30 entries provide knowledge of a file’s existence *and a separate and distinct set of timestamps* to compare against for signs of tampering. This is a great example of why it is extremely difficult for malware or an anti-forensics tool to reliably change all of the corresponding timestamps within a file system.

Evidence may still be found in Index Attributes even if wiping or anti-forensics software has been employed. Figure 1 shows the parsed output for a \$I30 file from the Windows directory. Two deleted index entries have been highlighted. In this example, a file named fgdump.exe was overwritten using a software tool named BCWipe. The original filename was overwritten with random characters (sqhyoeop.roy) and the Modified, Accessed, and Created time stamps were set to fictitious values. Since MFT Change Times cannot be directly modified via the Windows API, that timestamp still accurately reflects when the wipe occurred. Of course the interesting part of this example is that evidence of both the original file and the wiping artifacts are contained in the slack of the \$I30 file.



	A	B	D	E	F	G
1	FILENAME	PHYSICAL SIZE	MODIFIED TIME	ACCESSED TIME	CHANGED TIME	CREATED TIME
27	fgdump.exe (slack at 0xac0)	974848	2008-05-01 22:38:49	2011-06-10 00:50:28	2011-06-10 00:51:24	2011-06-10 00:50:28
28	LIVEKE~1 (slack at 0xc08)	0	2009-07-14 02:34:24	2009-07-14 03:20:10	2009-09-24 23:14:09	2009-07-14 03:20:10
29	Logs (slack at 0xc70)	0	2009-09-24 23:14:09	2009-09-24 23:14:09	2009-09-24 23:14:09	2009-07-14 03:20:10
30	Media (slack at 0xcd0)	0	2009-07-14 05:32:40	2009-07-14 05:32:40	2009-09-24 23:14:09	2009-07-14 03:20:10
31	Microsoft.NET (slack at 0xd30)	0	2009-07-14 05:01:21	2009-07-14 07:52:40	2009-09-24 23:14:09	2009-07-14 03:20:10
32	ModemLogs (slack at 0xe10)	0	2009-07-14 02:34:34	2009-07-14 03:20:10	2009-09-24 23:14:09	2009-07-14 03:20:10
33	MODEM~1 (slack at 0xe78)	0	2009-07-14 02:34:34	2009-07-14 03:20:10	2009-09-24 23:14:09	2009-07-14 03:20:10
34	sqhyoeop.roy (slack at 0xee0)	0	1986-04-30 11:43:13	1986-04-30 11:43:13	2011-06-10 00:58:04	1986-04-30 11:43:13

Figure 1: Evidence Found in \$I30 of Use of File Wiping Software

Exporting NTFS Index Attributes

One of the primary reasons many examiners don’t utilize index attribute files is because getting access to them is not always intuitive. I congratulate Access Data and their Forensic Toolkit (FTK) for clearly identifying \$I30 indexes for as long as I can remember. Figure 2 shows what they look like in FTK. Simply right-click on the \$I30 file to export from the image.

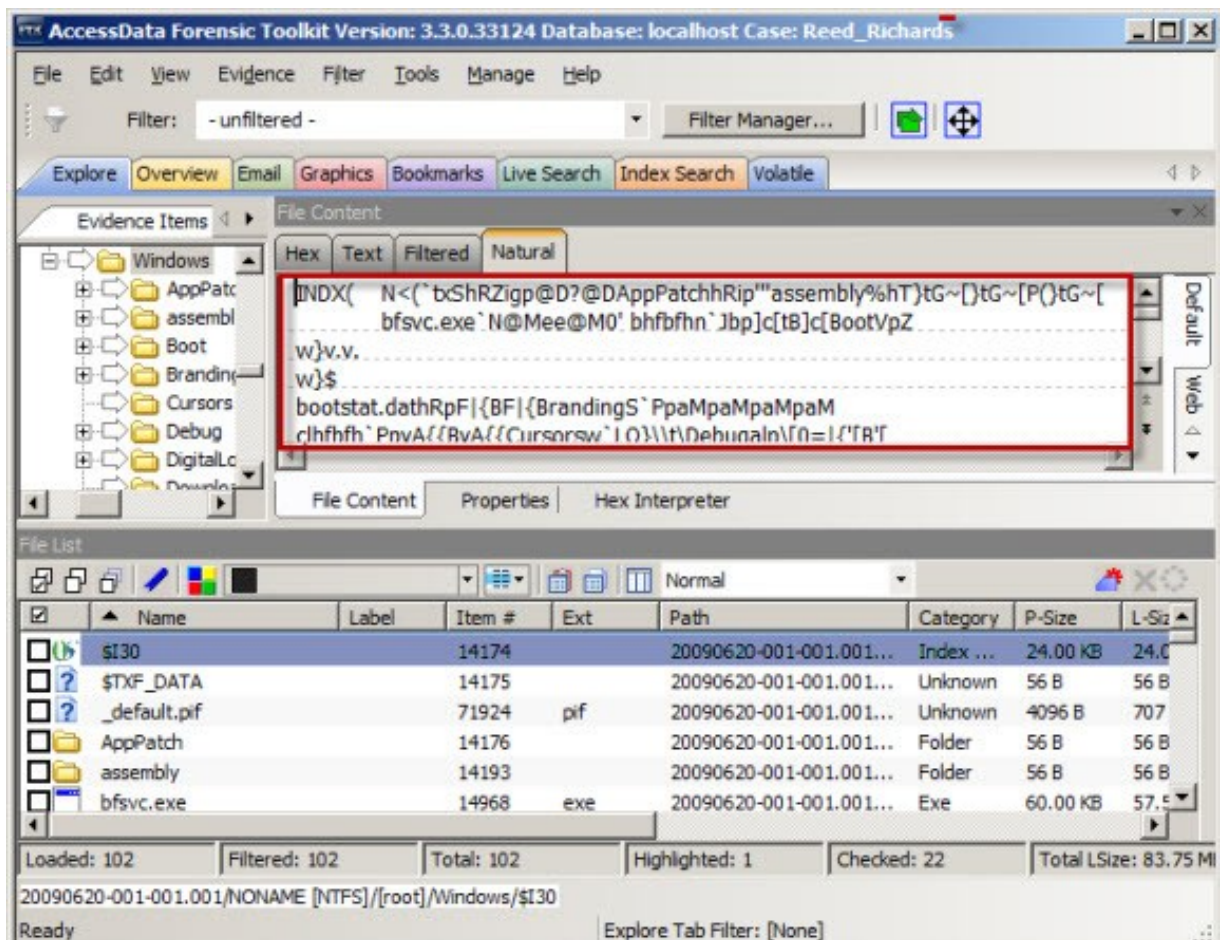


Figure 2: \$I30 File as Shown in AccessData Forensic Toolkit

The Sleuth Kit (TSK) also does an excellent job with Index Attributes, although the interface takes a little practice. Figure 3 shows output from the TSK **istat** tool for a RECYCLER child directory. Near the bottom of the output we see the NTFS attribute list.


```
root@SIFT-Workstation: /
File Edit View Terminal Help
root@SIFT-Workstation:/# istat image_2011_09_07.dd 8675
MFT Entry Header Values:
Entry: 8675          Sequence: 1
$LogFile Sequence Number: 183016620
Allocated Directory
Links: 2

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 361  ()
Created:             Sat Jun 30 22:54:25 2007
File Modified:       Fri Jan 16 23:27:24 2009
MFT Modified:        Fri Jan 16 23:27:24 2009
Accessed:            Fri Jan 16 23:27:24 2009

$FILE_NAME Attribute Values:
Flags: Directory
Name: S-1-5-21-1004336348-492894223-854245398-1003
Parent MFT Entry: 8674  Sequence: 1
Allocated Size: 0      Actual Size: 0
Created:             Sat Jun 30 22:54:25 2007
File Modified:       Sat Jun 30 22:54:25 2007
MFT Modified:        Sat Jun 30 22:54:25 2007
Accessed:            Sat Jun 30 22:54:25 2007

Attributes:
Type: $STANDARD_INFORMATION (16-0)  Name: N/A  Resident
Type: $FILE_NAME (48-3)             Name: N/A  Resident  size: 82
Type: $FILE_NAME (48-2)             Name: N/A  Resident  size: 154
Type: $INDEX_ROOT (144-6)           Name: $I30  Resident  size: 56
Type: $INDEX_ALLOCATION (160-4)      Name: $I30  Non-Resident
125129 125130
Type: $BITMAP (176-5)               Name: $I30  Resident  size: 8
```

Figure 3: TSK istat Output Showing NTFS Attributes

You may notice multiple attributes using the \$I30 name in Figure 3. Brian Carrier's File System Forensic Analysis book dissects each of these attributes, and the simple explanation is they are all components of the overall Index Attribute [1]. To export the \$I30 attribute from this directory, we use the icat tool from TSK and give it the MFT entry number of the directory along with the identifier for the \$INDEX_ALLOCATION attribute, which in this case is "160-4" (Figure 4). This output is redirected into a file named, \$I30.

```
root@SIFT-Workstation: /
File Edit View Terminal Help
root@SIFT-Workstation:/# icat image_2011_09_07.dd 8675-160-4 > $I30
```

Figure 4: Exporting a \$I30 attribute using The Sleuth Kit

To identify index attributes in EnCase, an EnScript is required. An Enscript ships within the stock Examples folder and is named, “Index buffer reader”. This script can be pointed at a specific directory, a collection of tagged directories, or the entire file system. The results are nicely bookmarked and the entries are parsed within each bookmark’s comments field. To export the \$I30 file in EnCase, you first select the “Index Buffer” that you are interested in within the Tree Pane, select all within the View Pane, and right-click and select Export (Figure 5).

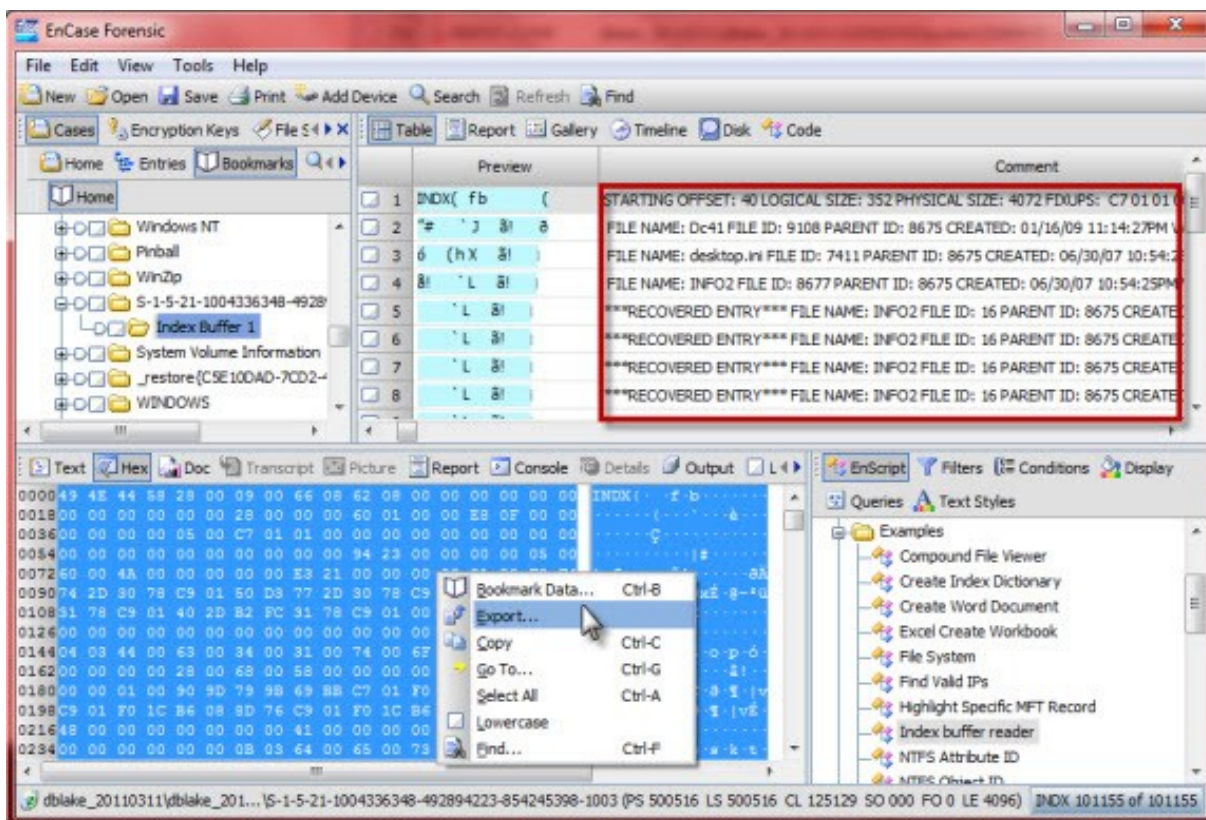


Figure 5: \$I30 Parsing in EnCase

Parsing Index Attributes

The format of \$I30 entries is well known and extensively documented. However, indexes commonly reach sizes in the hundreds of kilobytes and hold thousands of entries (theoretically they could have billions of entries). It is tiresome work to do the parsing by hand. Of the previously covered forensic suites, only EnCase has a native ability to parse the files, though the output is very difficult to use and analyze. Luckily, Willi Ballenthin recently released an open source tool (<http://www.williballenthin.com/forensics/indx/index.html>) that does an excellent job of parsing \$I30 files [2]. It formats output as CSV, XML, or bodyfile (for inclusion into a timeline) and has a feature to search remnant space for slack entries. The tool is written in Python and sample command line follows:

```
python INDXParse.py -d $I30 > $I30_Parse.csv
```


The resulting file can be opened and filtered in Excel (CSV output is the default). Notice the file names, file size, and four timestamps displayed in the output shown in Figure 6. Several deleted index node entries (slack) are also displayed within the output.

	FILENAME	LOGICAL SIZE	MODIFIED TIME	ACCESSED TIME	CHANGED TIME	CREATED TIME
2	Dc108.html	6106	2010-12-10 00:05:03	2011-06-21 20:06:15	2011-06-28 21:19:57	2010-12-10 00:05:03
3	DC108~1.HTM (slack at 0x7f0)	6106	2010-12-10 00:05:03	2011-06-21 20:06:15	2011-06-28 21:19:57	2010-12-10 00:05:03
4	Dc109.html (slack at 0x858)	7445	2010-12-10 00:05:03	2011-06-21 20:06:15	2011-06-28 21:19:57	2010-12-10 00:05:03
5	DC109~1.HTM (slack at 0x8c0)	7445	2010-12-10 00:05:03	2011-06-21 20:06:15	2011-06-28 21:19:57	2010-12-10 00:05:03
6	Dc11.txt (slack at 0x928)	42	2011-03-05 20:52:31	2011-03-05 20:53:07	2011-03-05 20:53:09	2011-03-05 20:52:31
7	Dc12.log (slack at 0x990)	551	2011-03-05 20:52:31	2011-03-05 20:53:01	2011-03-05 20:53:09	2011-03-05 20:52:31
8	Dc13.DAT (slack at 0x9f8)	3145728	2011-04-23 02:17:24	2011-06-21 01:36:52	2011-06-21 01:36:55	2009-04-09 22:39:59
9	Dc14 (slack at 0xa60)	0	2011-03-05 21:02:24	2011-06-28 21:19:56	2011-06-28 21:19:56	2011-03-05 20:51:42

Figure 6: INDXPaser.py Output for an Exported \$I30 Attribute

References

- [1] *File System Forensic Analysis* (<http://www.digital-evidence.org/fsfa/>), Brian Carrier
- [2] INDXPaser.py (<http://www.williballenthin.com/forensics/indx/index.html>) by Willi Ballenthin
- [3] John McCash previously discussed Index Attributes in this blog post (<http://computer-forensics.sans.org/blog/2011/08/01/ultimate-windows-timelining>)

Chad Tilbury, GCFA, has spent over twelve years conducting computer crime investigations ranging from hacking to espionage to multi-million dollar fraud cases. He teaches FOR408 Windows Forensics (<http://www.sans.org/course/computer-forensic-investigations-windows-in-depth>) and FOR508 Advanced Computer Forensic Analysis and Incident Response (<http://www.sans.org/course/advanced-computer-forensic-analysis-incident-response>) for the SANS Institute. Find him on Twitter @chadtilbury (<http://twitter.com/chadtilbury>) or at <http://ForensicMethods.com> (./).

Share this:

Twitter 6
<http://forensicmethods.com/ntfs-index-attribute?share=twitter&nb=1>



Facebook 2
<http://forensicmethods.com/ntfs-index-attribute?share=facebook&nb=1>

Google
<http://forensicmethods.com/ntfs-index-attribute?share=google-plus-1&nb=1>

LinkedIn 2
(<http://forensicmethods.com/ntfs-index-attribute?share=linkedin&nb=1>)

More

Google+

 (<https://plus.google.com/116673592452414934388>) Chad Tilbury
(<https://plus.google.com/116673592452414934388>)  Follow 356

Related

Book Review: Digital
Forensics with Open Source
Tools (/ntfs-index-attribute?
relatedposts_to=416&relatedp
osts_order=0)
In "Computer Forensics"

Cloud Forensics with F-
Response (/ntfs-index-
attribute?
relatedposts_to=1930&related
posts_order=1)
In "Computer Forensics"

Book Review: Mastering
Windows Network Forensics &
Investigations (/ntfs-index-
attribute?
relatedposts_to=1601&related
posts_order=2)
In "Computer Forensics"

Infographic: A Zettabyte World (<http://forensicmethods.com/zettabyte>)

FTC Asked to Investigate... (<http://forensicmethods.com/supercookies>)

7 responses to *NTFS \$I30 Index Attributes: Evidence of Deleted and Overwritten Files*



H. Carvey (<http://windowsir.blogspot.com>) September 30, 2011 at 8:45 pm
(<http://forensicmethods.com/ntfs-index-attribute#comment-117>)

Excellent post, Chad! Thanks for sharing.

Reply (/ntfs-index-attribute?replyto=117#respond)



Stefan Fleischmann (<http://www.x-ways.net/forensics/>) October 6, 2011 at 5:22 am
(<http://forensicmethods.com/ntfs-index-attribute#comment-121>)

As I was asked by users who had read this article, here some comments:

* Where the article says that "NTFS directory index entries utilize a \$FILE_NAME attribute", that is not correct IMO. In the terminology that I use, INDX buffers consist of index records. There are no \$FILE_NAME attributes in INDX buffers.

* If the slack of INDX buffers contain index records of previously existing files that are not yet known from any FILE record and thus may contain useful information about previously existing files or previous names or previous locations of renamed/moved files, then all that information from those index records is taken over by X-Ways Forensics when it's running its "particularly thorough file system data structure search"

and integrated into the so-called volume snapshot. That means there is no unnecessary duplication of information (information that is already available from the \$MFT), only additional information is added to the volume snapshot.

Reply (/ntfs-index-attribute?replytocom=121#respond)



Chad Tilbury (<http://forensicmethods.com>) *October 18, 2011 at 10:35 pm*
(<http://forensicmethods.com/ntfs-index-attribute#comment-138>)

Stefan,

Thanks for your comments. I think our discrepancy is indeed one of terminology. It is nice to hear how X-Ways handles Index Attributes.

Reply (/ntfs-index-attribute?replytocom=138#respond)



John McCash *August 26, 2012 at 8:26 pm* (<http://forensicmethods.com/ntfs-index-attribute#comment-288>)

Stefan,

Actually, as I understand it, you're both correct. See Chapter 13 in File System Forensics by Brian Carrier for complete details. The index record is the primary subunit of an NTFS \$INDEX_ALLOCATION attribute. Each index record is composed of an index record header, node header, and one or more index entries. At offset 16 within each index entry for a regular file, is located a copy of the \$FILE_NAME attribute of the referenced file.

John

Reply (/ntfs-index-attribute?replytocom=288#respond)



Lakshmi *October 20, 2011 at 2:39 pm* (<http://forensicmethods.com/ntfs-index-attribute#comment-147>)

Very informative post Chad (you're my instructor for vLive SANS 508 class).

Thanks for posting.

Reply (/ntfs-index-attribute?replytocom=147#respond)



G.H. Stultz *December 18, 2011 at 11:39 am* (<http://forensicmethods.com/ntfs-index-attribute#comment-214>)

My apologies if my questions seem naive however I just finished Chad's 408 class in D.C. and I'm striving to become a member of the digital forensics team...BTW Chad – Great job in D.C.!

Figure One: I can't locate in the text how the tool indicates fgdump.exe was overwritten by sqhyoeo.roy unless the yellow highlighting is a feature of the tool and not the Chad's effort to highlight the referenced files.

Also in Figure Three I didn't make the connection regarding how Chad knew to use the value 8675 in the istat command line. Where did 8675 come from?

Reply (/ntfs-index-attribute?replytocom=214#respond)



Chad Tilbury (<http://forensicsmethods.com>) *December 27, 2011 at 12:03 am*
(<http://forensicsmethods.com/ntfs-index-attribute#comment-221>)

Hello Gary. Regarding what you see in Figure 1, I knew that fgdump.exe and sqhyoeo.roy were the same file because during my testing the latter appeared in the index after I successfully wiped the former. In a "real-life" situation you might be able to tie to two together based on the number of letters in the name (depending on the wiping tool) or the time stamp. Even if this were not possible, you could at least say that fgdump once existed and that a file may have been wiped in that folder.

Regarding the MFT entry 8675 in Figure 4, you found an error! That image should show 8674-160-4, which corresponds to the MFT entry information shown in Figure 3.

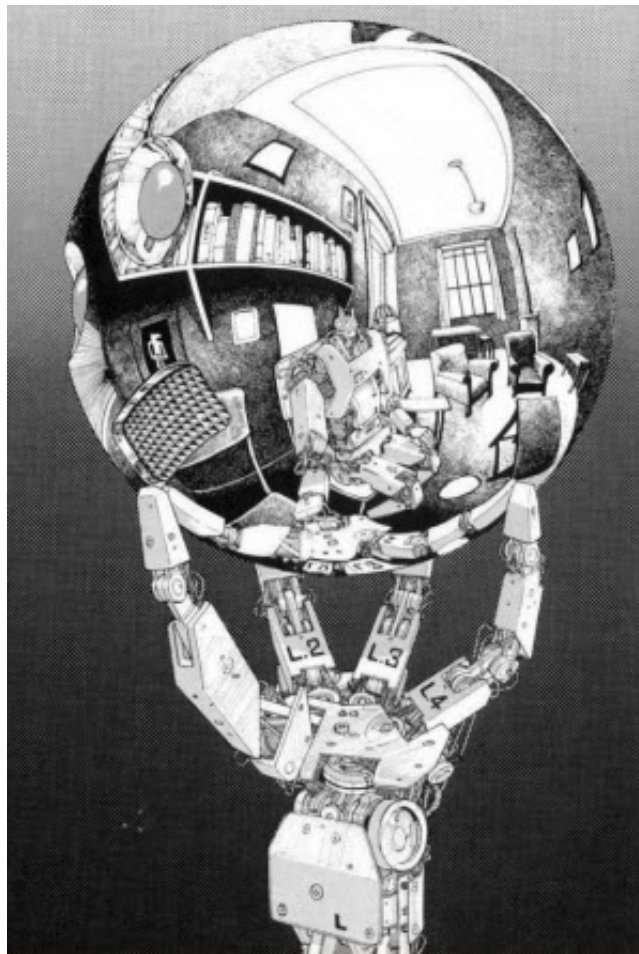
Thanks for taking the time to comment for future readers.

Reply (/ntfs-index-attribute?replytocom=221#respond)

Leave a Reply

Enter your comment here...

Search...



TEACHING SCHEDULE

FOR408: WINDOWS FORENSICS

05/10/14 - 05/15/14

San Diego, CA at SANS Security West 2014 (<http://www.sans.org/event/sans-security-west-2014/course/windows-forensic-analysis>)

09/08/14 - 09/13/14

Crystal City, VA at SANS Crystal City (<http://www.sans.org/event/crystal-city-2014/course/windows-forensic-analysis>)

10/20/14 - 10/25/14

Las Vegas, NV at SANS Network Security 2014 (<http://www.sans.org/event/network-security-2014/course/windows-forensic-analysis>)

FOR508: ADVANCED FORENSICS & INCIDENT RESPONSE

06/03/14 - 06/08/14

Austin, TX at SANS DFIR Summit 2014 (<https://www.sans.org/event/dfir-summit-2014/course/advanced->

computer-forensic-analysis-incident-response)

06/23/14 - 06/28/14

Baltimore, MD at SANSFIRE 2014 (<http://www.sans.org/event/sansfire-2014/course/advanced-computer-forensic-analysis-incident-response>)

07/21/14 - 08/27/14

Online at SANS vLive (<https://www.sans.org/vlive/details/for508-jul-2014-chad-tilbury>)

10/06/14 - 10/11/14

Prague, CZ at SANS Forensics Europe (<http://www.sans.org/event/dfir-prague-2014/course/advanced-computer-forensic-analysis-incident-response>)

MOST POPULAR POSTS

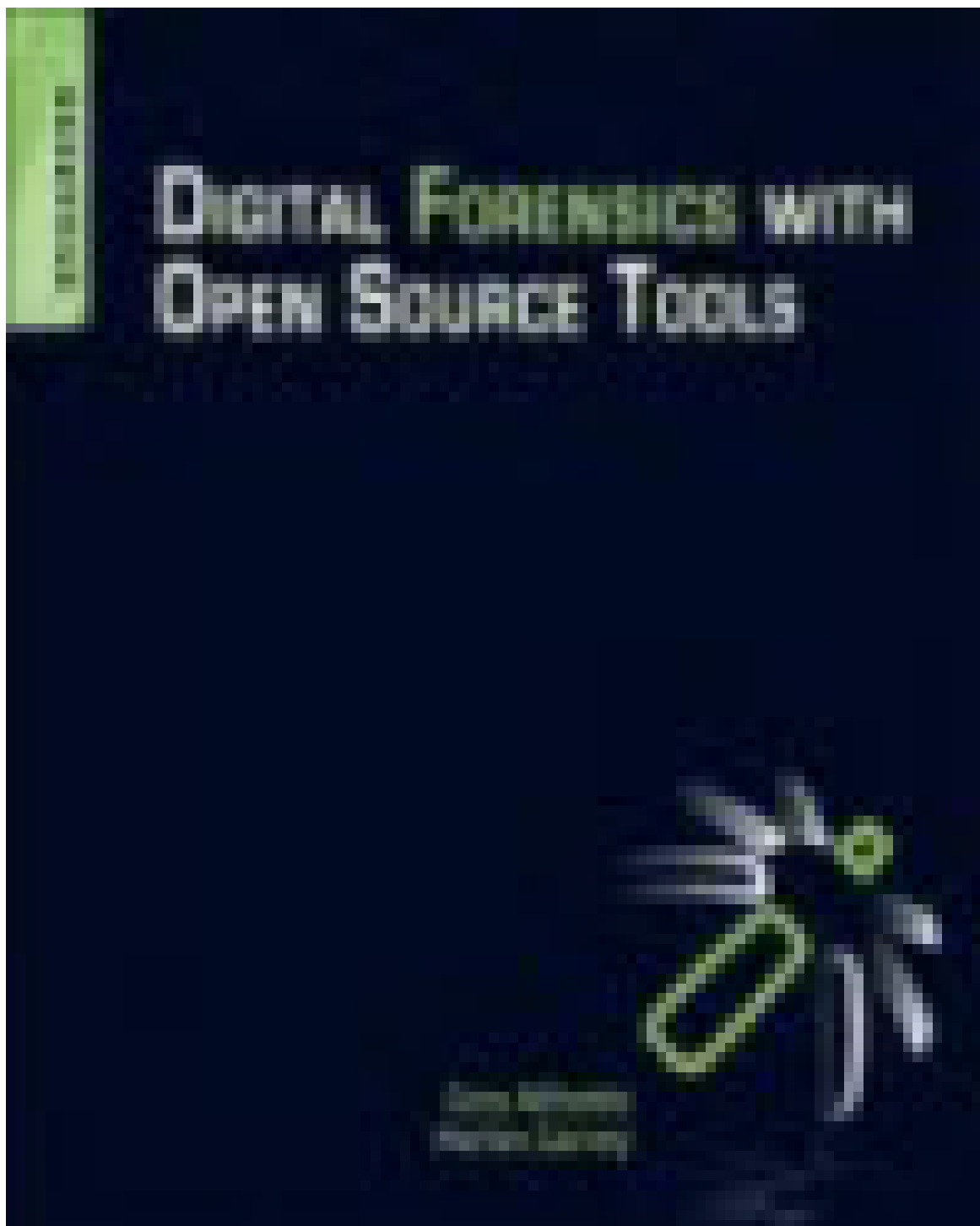
Signature Detection with CrowdResponse (<http://forensicmethods.com/crowdresponse>)

MO' SHELLS MO' PROBLEMS: WEB SERVER LOG ANALYSIS (<http://forensicmethods.com/webshell-log-analysis>)

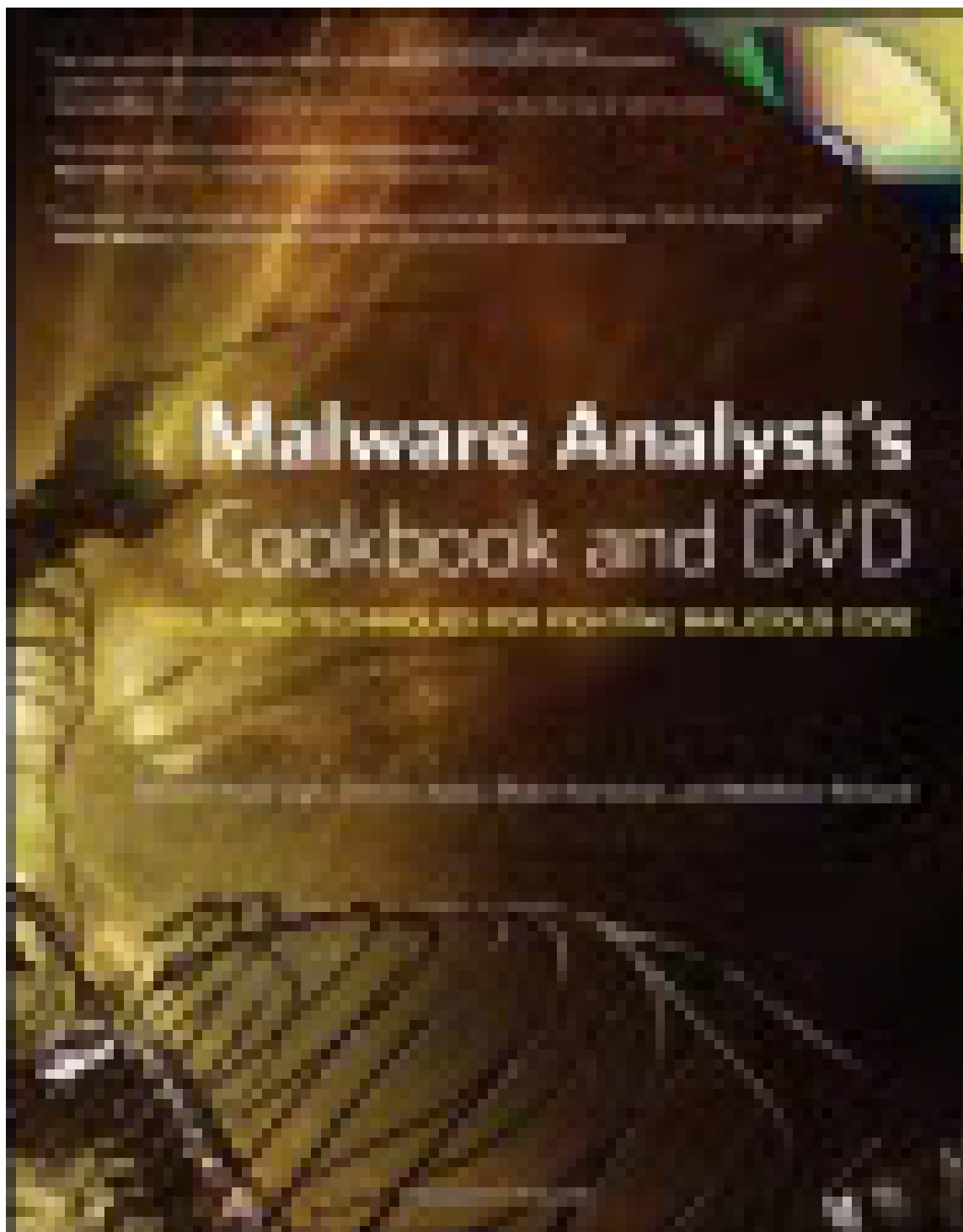
Linux File Recovery using the EXT3 Journal (<http://forensicmethods.com/linux-recovery>)

Book Review: Malware Analyst's Cookbook (<http://forensicmethods.com/malware-analyst>)

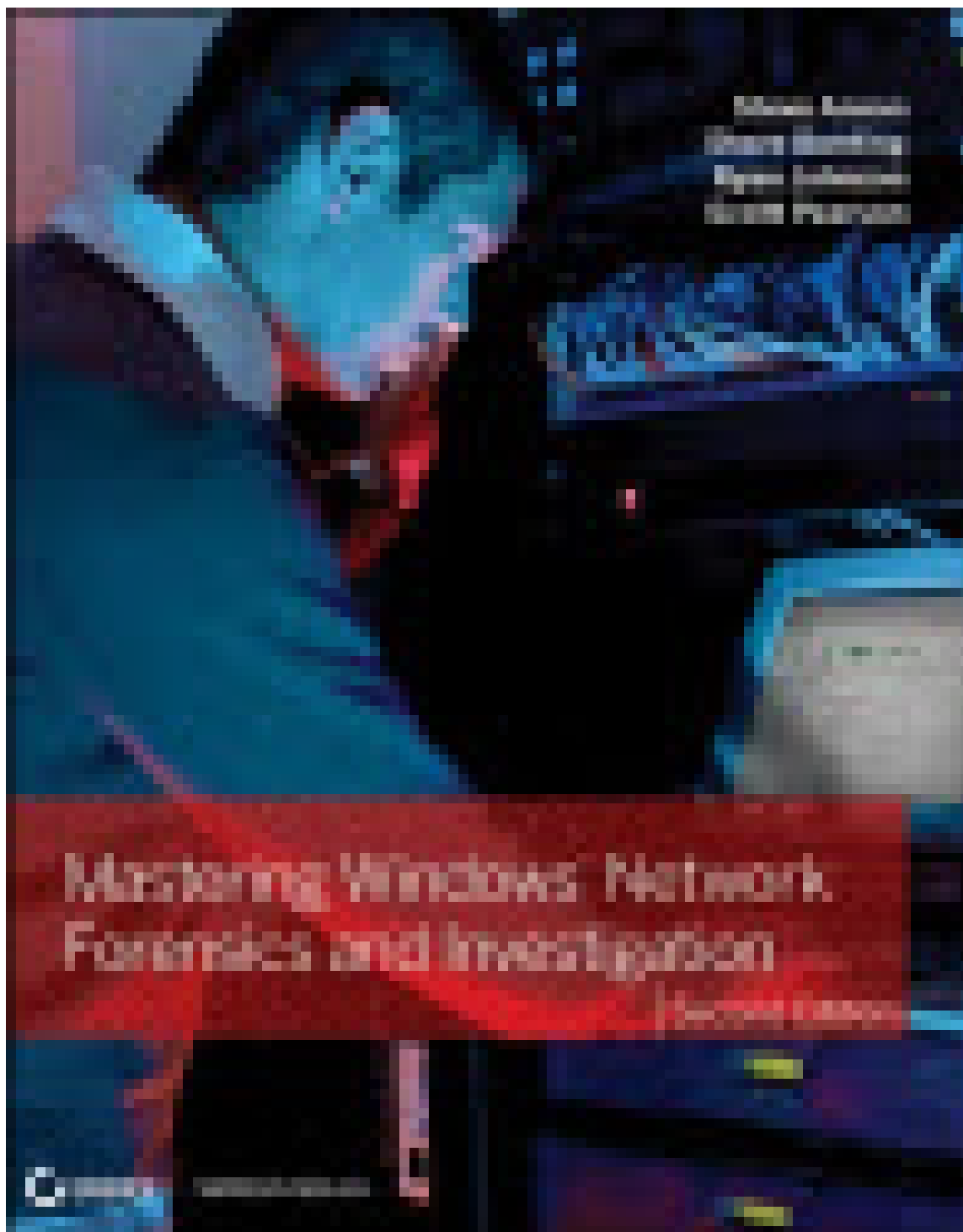
SANS FOR408 vs. FOR508 (<http://forensicmethods.com/sans-for408-vs-for508>)



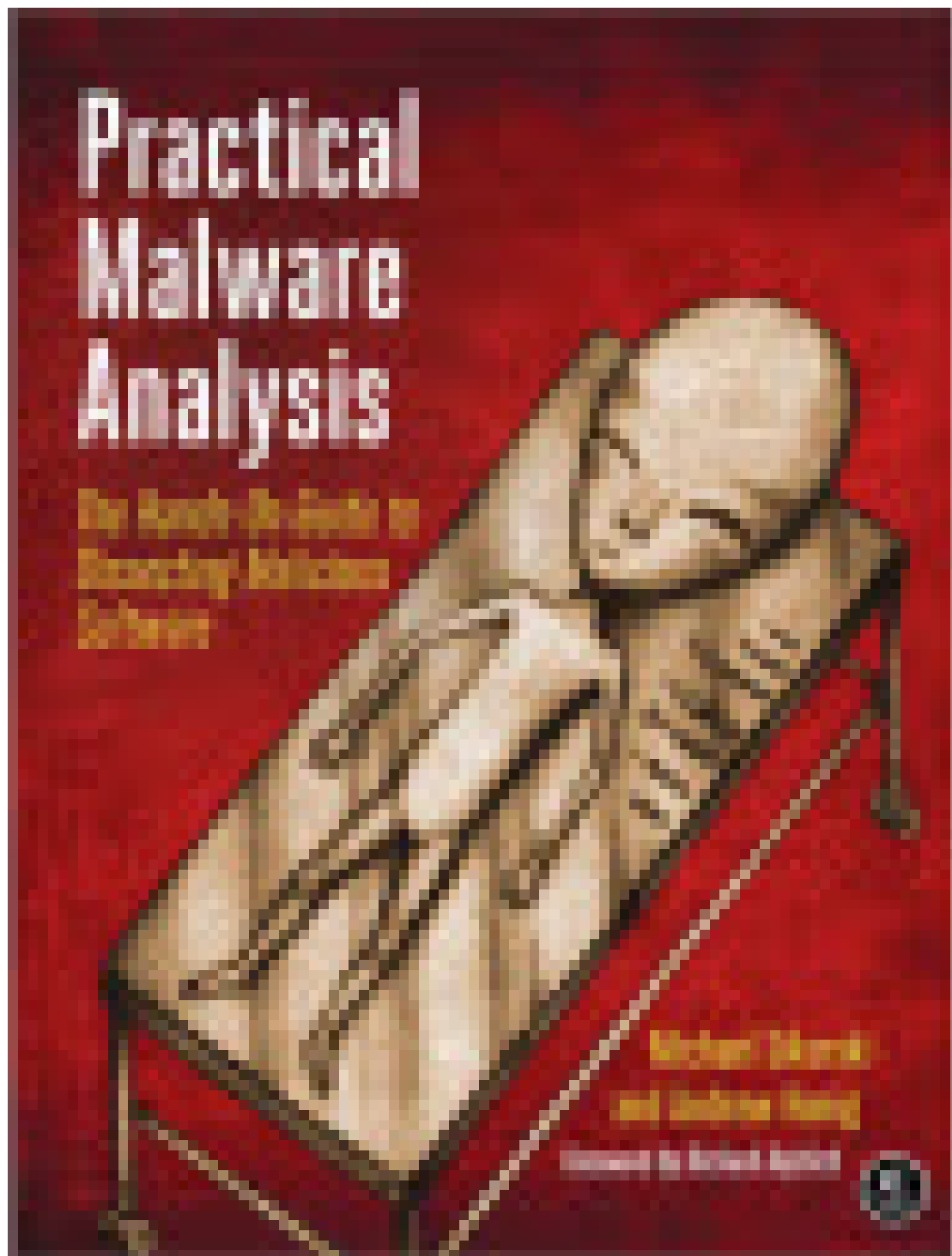
(<http://forensicmethods.com/book-review-digital-forensics-with-open-source-tools>)



(<http://forensicmethods.com/malware-analyst>)



(<http://forensicmethods.com/windows-network-forensics>)



(<http://www.amazon.com/Practical-Malware-Analysis-Dissecting-Malicious/dp/1593272901>)

THE H-BOOK DEVELOPER

Malware Forensics

Investigating and Analyzing Malicious Code

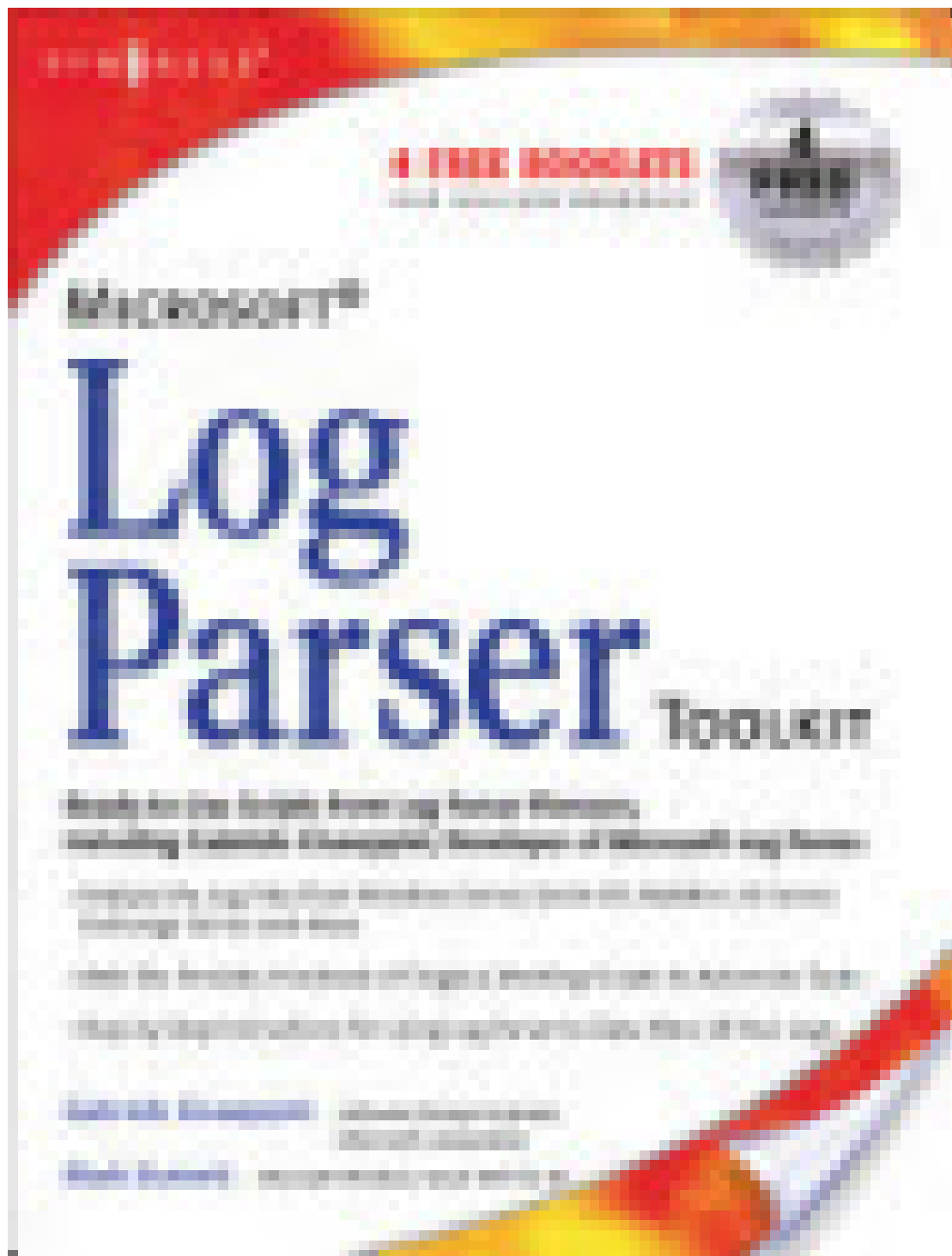
The Only Essential, Hands-On Guide to Malicious Code Investigation

- Collect and analyze evidence from compromised Windows systems
- Investigating a new threat: Writing Scripts for Malware Analysis on Windows
- Malware analysis: Windows, Linux, and Mac OS X systems

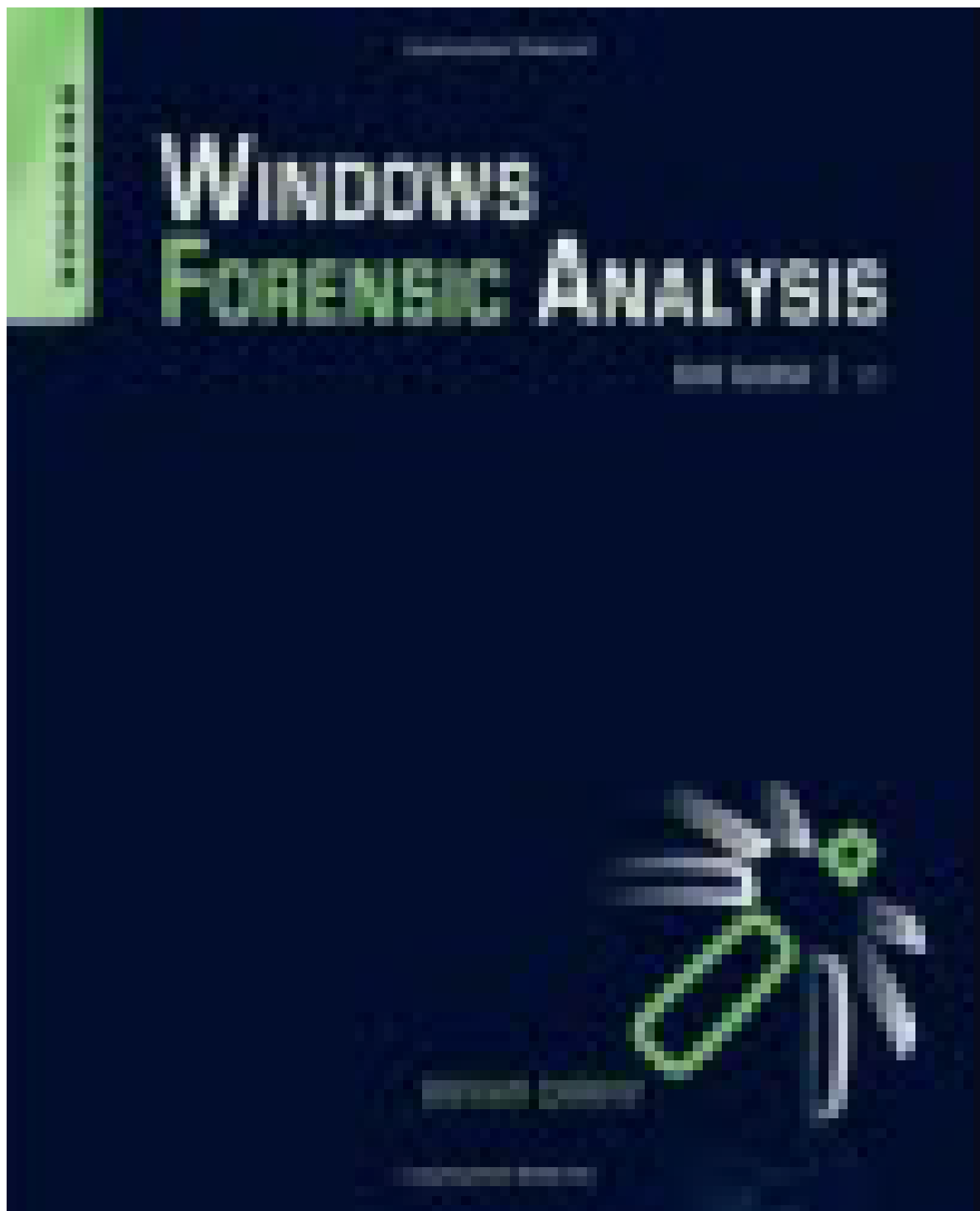
James R. Hughes
Sergey Koshkin
Colin McEneaney

NOVA 98 Series Publications

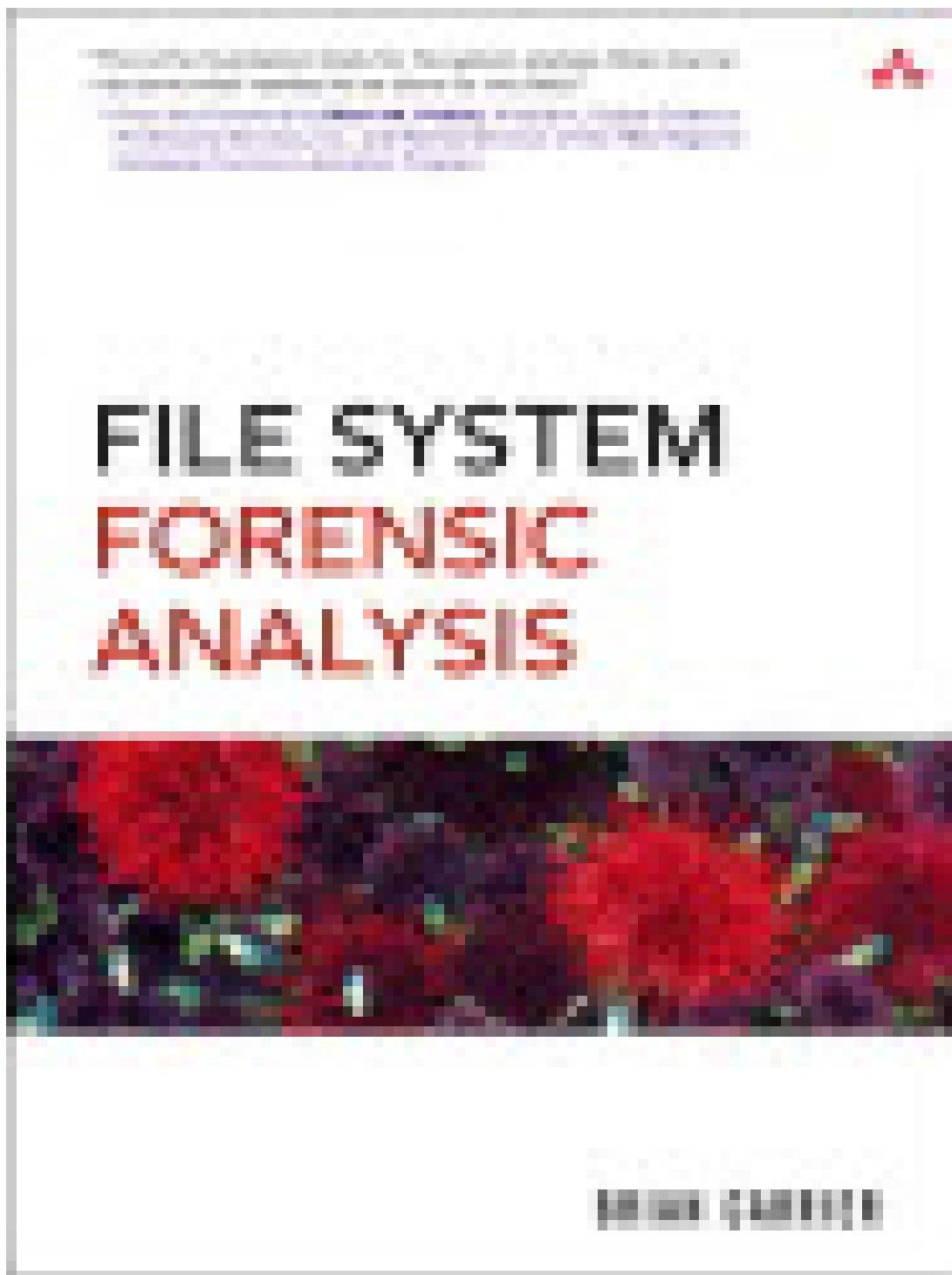
(<http://www.amazon.com/Malware-Forensics-Investigating-Analyzing-Malicious/dp/159749268X>)



(<http://forensicmethods.com/log-parser-book>)



(<http://www.amazon.com/Windows-Forensic-Analysis-Toolkit-Edition/dp/1597497274/>)



(<http://www.digital-evidence.org/fsfa/>)

CATEGORIES

Apple Forensics (<http://forensicmethods.com/category/apple-forensics>)

Browser Forensics (<http://forensicmethods.com/category/browser-forensics>)

Computer Forensics (<http://forensicmethods.com/category/computer-forensics>)

Forensic Blogs (<http://forensicmethods.com/category/forensic-blogs>)

Forensics Jobs (<http://forensicmethods.com/category/forensics-jobs>)

Geolocation (<http://forensicmethods.com/category/geolocation>)

Incident Response (<http://forensicmethods.com/category/incident-response>)

Linux Forensics (<http://forensicmethods.com/category/linux-forensics>)

Malware (<http://forensicmethods.com/category/malware>)

Memory Forensics (<http://forensicmethods.com/category/memory-forensics>)

Mobile Devices (<http://forensicmethods.com/category/mobile-devices>)

Tool Review (<http://forensicmethods.com/category/tool-review>)

Windows Registry (<http://forensicmethods.com/category/windows-registry>)

Chad Tilbury



FORENSIC CHALLENGES

Computer Forensic Reference Data Sets (<http://www.cfreds.nist.gov/>)

Cyber Security Challenge UK (<https://cybersecuritychallenge.org.uk/index.php>)

DC3 Digital Forensic Challenges (<http://www.dc3.mil/challenge/>)

DFRWS Forensic Challenge 2011 (<http://www.dfrws.org/2011/challenge/index.shtml>)

Digital Corpora Scenarios (<http://digitalcorpora.org/archives/category/scenarios>)

Digital Forensics Treasure Hunt (<http://digitalforensics.securitytreasurehunt.com/>)

Enron Email Dataset (e-Discovery) (<http://www.edrm.net/resources/data-sets/edrm-enron-email-data-set-v2>)

Forensic Practical (<http://www.forensickb.com/2008/01/forensic-practical.html>)

Hacking Exposed Exercises (<http://hackingexposedcomputerforensicsblog.blogspot.be/2014/03/daily-blog-277-sample-forensic-images.html>)

HandlerDiaries DFIR Challenges (<http://blog.handlerdiaries.com/>)

Hogfly's Memory Images (<https://skydrive.live.com/?cid=5694a755c9c6a175&id=5694A755C9C6A175!106>)

Honeynet Project Challenges (<http://www.honeynet.org/challenges>)

ISFCE Sample Practical (<http://www.isfce.com/sample-pe.htm>)

Linux LEO Exercises (<http://linuxleo.com/>)

Linux Memory Images (<http://secondlookforensics.com/linux-memory-images/>)

Network Forensic Challenges (<http://forensicscontest.com/puzzles>)

RealityNet Cloud Forensics Challenge (http://www.realitynet.it/downloads/cloud_lab_files.zip)

Shortinfosec Computer Forensic Investigation (<http://www.shortinfosec.net/2008/07/competition-computer-forensic.html>)

Stuxnet Memory Forensics (<http://mnin.blogspot.com/2011/06/examining-stuxnets-footprint-in-memory.html>)

Tool Testing Images (<http://dfft.sourceforge.net/>)

DIGITAL FORENSICS BLOGS

 Linux Sleuthing (<http://linuxsleuthing.blogspot.com/>)

just recently: (last change) Searching for Searches (In a recent examination of smart phone content, it became necessary to know the personal interests of the device's owner. ...)

 Digfor (<http://digfor.blogspot.com/>)


yesterday : (last change) InfoSec To-Do list (Chief InfoSec Officer's (CISO) To-Do list as mentioned by E. Cole.)

 Hexacorn Tech Blog (<http://www.hexacorn.com/blog/>)


9 days ago: (last change) Beyond good ol' Run key, Part 11 (I must admit that finding new paths that could be exploited as a persistence mechanism is a silly hobby of mine. When I started ...)

 M-union (<http://blog.mandiant.com/>)

11 days ago: (last change) An Intel Analyst's Key Takeaways from M-Trends: Beyond the Breach (It's been a few weeks since we released the 2014 edition of M-Trends. This year we explored a number of diverse threat actors ...)

 Windows Incident Response (<http://windowsir.blogspot.com>)

11 days ago: (last change) WFA 4/e Reviews (Brett Shavers has posted the first (that I'm aware of) reviews of WFA 4/e...one on Amazon, and a longer one can be found on ...)

 Journey into IR (<http://journeyintoir.blogspot.com/>)

15 days ago: (last change) Triaging with the RecentFileCache.bcf File (When you look at papers outlining how to build an enterprise-scale incident response process it shows the text book picture ...)

 JL's Stuff (<http://gleeda.blogspot.com/>)

21 days ago: (last change) Volatility Talk at Upcoming NYC4SEC (The Volatility team will give a talk at the next NYC4SEC meetup on memory forensics on May 8th, 2014 at John Jay College. Make ...)

 SANS Computer Forensics (<http://computer-forensics.sans.org/blog>)

22 days ago: (last change) "#FOR526 #MemoryForensics Course - Special Deal for Online Training and

Capital City in July" (FOR526 - 10% Off for vLive (Online Live Training)orCapital City in July. Use code = m3mory[caption ...)

 Memory Forensics (<http://memoryforensics.blogspot.com/>)

27 days ago: (last change) Building a Decoder for the CVE-2014-0502 Shellcode (Yesterday on the Volatility Labs blog I published a post on analyzing some interesting shellcode from a recent attack campaign ...)

 A Fistful of Dongles (<http://www.ericjhuber.com/>)

33 days ago: (last change) The State Of The Blog (I get enough people asking me about the fate of the blog where I thought it would make more sense to just crank out a blog ...)

 Zena Forensics (<http://blog.digital-forensics.it>)

39 days ago: (last change) mimikatz offline addendum (I must admit I did not expect so many acknowledgments by writing the volatility mimikatz plugin. I want to say thanks to all ...)

 Forensicaliente (<http://forensicaliente.blogspot.com/>)

51 days ago: (last change) Presenting DFIR, Shakespeare Style - DFIR Summit 2014 (I have been given the opportunity to speak at the SANS DFIR Summit in Austin this year, on a topic that I think is very ...)

 The Digital Standard (<http://www.thedigitalstandard.blogspot.com/>)

57 days ago: (last change) 2014 SANS DFIR Summit (Can't wait to be back at the DFIR Summit!)

 Forensic Focus Blog (<http://forensicrofocus.blogspot.com/>)

70 days ago: (last change) Webinar: Accelerating Investigations Using Advanced eDiscovery Techniques (Join this free webinar from Nuix to find out how to deal with large volumes of electronic evidence while balancing business ...)

 System Forensics (<http://www.sysforensics.org/>)

103 days ago: (last change) Do not fumble the lateral movement (I posted a blog post about Windows Processes and how knowing what's "normal" can be used to spot malicious ...)

 Cheeky4n6Monkey (<http://cheeky4n6monkey.blogspot.com/>)

103 days ago: (last change) Android SMS script update and a bit of light housekeeping (Knock, Knock ...During recent research into Android SQLite databases (eg sms), Mari DeGrazia discovered a bug in the ...)

 Girl Unallocated Blog (<http://girlunallocated.blogspot.com/>)

564 days ago: (last change) Be Very Quiet... I'm Tracking Emails Through Headers (That's right... I'm on the e-mail header hunt. Or, more specifically, on the hunt for the juicy information e-mail ...)

 Forensic Gremlins (<http://www.geoffblack.com/>)

609 days ago: (last change) Sorting in EnScript – Sorting Arrays and NameListClass / NameValueCollection (Every language has its own quirks when it comes to sorting data. In this post, I'll take an introductory look at some of ...)

 Cyber Crime 101 (<http://www.cybercrime101.com/>)

668 days ago: (last change) 2012 SANS DFIR Summit Wrap Up (Last week I had the opportunity to attend the 2012 SANS Digital Forensics & Incident Response Summit. It was held in ...)

 Apple Examiner (<http://www.appleexaminer.com/>)
(last change)

[HOME \(http://forensicmethods.com/\)](http://forensicmethods.com/) [ABOUT \(http://forensicmethods.com/about\)](http://forensicmethods.com/about)

[ARCHIVES \(http://forensicmethods.com/archives\)](http://forensicmethods.com/archives)

© 2014 Forensic Methods (<http://forensicmethods.com>)

⌂