Fast Food Forensics

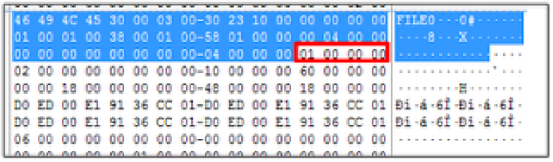
Thursday, March 22, 2012

Parsing MFT Entries

I can't share with you the specifics of the problems that make up the CFCE Mentor process, but I can tell you that knowing the ins and outs of basic File System structures is key. Doesn't give much away, does it? To understand all of the intricacies of NTFS, I relied heavily on Brian Carrier's book, File System Forensic Analysis. My first exposure to this book was when my co-worker and friend (and former cop) lent me his copy WAY back when I was studying for my EnCE (Guidance Software's EnCase Certified Examiner) certification. Let me describe the condition of his book – that thing was dog-eared, sticky-tabbed, highlighted and underlined and stunk of blood, sweat and tears. I don't think I had ever seen a book in such a "lovingly used" condition and at the time, I didn't understand it. Yet, now after putting the finishing touches on Problem 4 of my CFCE certification, I get it. I now own two copies (and my husband has one, too!) and I keep one in the back of my car at all times. I can't stress enough the many mysteries the book has revealed to me. Yet, there is one thing I ran into that was NOT in "the book" and I wish to share it here:

If you ever need to find the MFT entry number of a deleted entry, the old-school technique of figuring this out was to count the distance (in bytes) from the start of the MFT (Entry 0 - $MFT) to the start of the entry you needed to enumerate. Divide this value by the size of an MFT entry (1,024 bytes) and the resultant number will be the deleted entry number. So, what I didn't know, until just recently, is that there is an easier way.

At offset 44-47 of each MFT entry for Windows XP and later, the value is also that of the MFT entry number. (See image below)



```
46 49 4C 45 30 00 03 00-30 23 10 00 00 00 00 00  FILE0···0#······
01 00 01 00 38 00 01 00-58 01 00 00 00 04 00 00  ····8···X·······
00 00 00 00 00 00 00 00-04 00 00 00 01 00 00 00  ················
02 00 00 00 00 00 00 00-10 00 00 00 60 00 00 00  ·············`···
00 00 18 00 00 00 00 00-48 00 00 00 18 00 00 00  ········H·······
D0 ED 00 E1 91 36 CC 01-D0 ED 00 E1 91 36 CC 01  Ðí·á·6Ì·Ðí·á·6Ì·
D0 ED 00 E1 91 36 CC 01-D0 ED 00 E1 91 36 CC 01  Ðí·á·6Ì·Ðí·á·6Ì·
06 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

So, what does this mean?

1.) You need to write on p. 354 of your Carrier book a note in the top margin that offset 44-47 of the data structure of the basic MFT entry represents the Entry Record Number.

2.) You no longer need to do MATH to figure out the MFT entry number.

> This clearly is not easy-to-find information and that is why I was motivated to write this post. I spent DAYS searching for this information and found some very confusing documentation on the subject but no specifics!

Posted by Alissa Torres at 12:44 PM

+1 +2 Recommend this on Google

Newer Post Home Older Post

Other Forensics Blogs

Windows Incident Response
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 his WinFE blog. Not so much a ...
1 week ago

Journey Into Incident Response
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 about what it should look like....
2 weeks ago

A Fistful of Dongles
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 post. I’m still here, but my time ...
4 weeks ago

Girl, Unallocated
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 headers can contain. It all started ...
1 year ago

About Me

Alissa Torres

The views expressed here are my own and not those of my past or current employers.

View my complete profile

Blog Archive

- ► 2014 (3)
- ▼ 2012 (3)
  - ► July (1)
  - ▼ March (1)
    - Parsing MFT Entries
  - ► January (1)

Awesome Inc. template. Powered by Blogger.