# A Fistful of Dongles

Eric Huber's Information Security, Cyber Investigations, and Digital Forensics Blog

**SATURDAY, JUNE 19, 2010**

## Give Me $FILE_NAME or Give Me Death

I think we're long past the point as a community where we should be pushing the vendors of our GUI forensic tools to provide us with the $FILE_NAME time values inside of an NTFS $MFT record. Every tool parses the $STANDARD_INFORMATION time values, but that should no longer be considered the bare minimum for a GUI forensic tool. Most tools do not provide the $FILE_NAME time values as part of their standard file system navigation experience. The concern that has been expressed in the past was that adding this information would be confusing to the user. While I can certainly understand that it might be confusing to an inexperienced or poorly trained examiner, that's not a good reason for not presenting the information. If an examiner doesn't understand how an $MFT record works, then this confusion is a teachable moment that will hopefully prompt the examiner to learn more about the inner workings of an $MFT record. The information is out there and it's easily accessible on the Web, through training courses and books.

Yes, I can parse the data manually or by scripting with the various vendor tools. However, it's much more useful to me if I can have these data stamps parsed automatically and presented to me as part of the main user interface experience.

I'm not familiar with all of the forensic tools that are available so I'll have to rely on other people to let me know what tools might be doing this already. I've been using Sleuth Kit more and more these days and it parses everything (istat) because it's Brian Carrier's awesome tool. I heard a long time ago that Pro Discover might present some of this information to the user also, but I'd be curious if someone could verify that for me. Any other tools that are doing this?

What do you think? Am I missing something? Why wouldn't we want this information presented to us up front in our GUI tools?

**Forensic 4cast Awards Voting Has Opened**

The nominations have closed for the upcoming Forensic 4cast awards and the voting has started. SANS announce this week that the awards will be open to everyone so if you are in the DC area and aren't attending the SANS Forensic and Incident Response Summit, you can still attend the awards.

**New Tools**

I've been made aware of a couple new forensic tools that I'd like to share with everyone.

The first one is Defraser which is a tool by the Netherlands Forensic Institute. I learned about this tool when I was taking SEC563 at SANSFIRE recently. This is a carving tool that will recover full and partial video data. I have just started it so I can't yet speak to how well it works yet, but I'm excited about the possibilities.

The second tool is called raw2vdmk. It looks like it's an alternative to

**ABOUT ME**

Eric Huber is an internationally recognized leader and public speaker in the field of high technology investigations. His area of expertise covers a broad area of high technology investigations with a special emphasis on the investigation of fraud, intellectual property theft, and misuse of corporate resources. He has led and conducted many high-profile and complex cross-border investigations and is an authority in the field of digital forensics and high technology investigations.

Eric is a IEEE Senior Member who belongs to numerous professional organizations such as AAFS, HTCIA, FBI Infragard, and IACIS. He is a former member of the Board of Directors for the Consortium of Digital Forensics Specialists (CDFS). The HTCIA Northeast Chapter named him their 2010 Person of the Year.

Eric holds numerous professional certifications including GIAC Certified Forensic Analyst (GCFA), EnCase Certified Examiner (EnCE), and GIAC Certified Incident Handler (GCIH Gold). He is a graduate of the FBI Newark Division's 2010 Citizens Academy and has completed an executive education program through Dartmouth College's Tuck School of Business. He holds a Bachelor of Science in Law Enforcement with magna cum laude honors from Minnesota State University at Mankato and a Master of Public Administration from Drake University.

The content of this blog does not represent the views any organizations that I am affiliated with or my employer.

You can reach me at ericjhuber a/t/ computer d0t 0rg

FOLLOW ME ON twitter



**FAQ**

**Q: Why did you name your blog "A Fistful of Dongles"?**

**A:** I started in the crime fighting and security world in traditional physical law enforcement. However, my first job in the information security and digital forensics world was as an individual contributor doing tactical level digital

LiveView. I use LiveView quite a bit and I'm quite fond of it. I haven't tried raw2vdmk, but I would potentially give it a spin if it could do something that LiveView couldn't do for me.

0

Posted by Eric Huber

## 6 comments:

**Keydet89** June 19, 2010 at 4:40 PM

*Any other tools that are doing this?*

MFTRipper from Mark Menz, although there is an issue with the order of the times that hasn't been worked out in a new/updated version. I use David Kovar's analyzemft.py script to provide some verification for my own Perl code.

harlan.pl

Reply

**Eric Huber** June 19, 2010 at 4:46 PM

Thanks, Harlan! What I'll do is collect the information that people send me and then make a list (with links to the tools people mention) that I'll put in one of my next blog posts.

Congratulations on your Forensic 4cast nominations, btw. :)

Reply

**macaroni** June 19, 2010 at 6:05 PM

Looks like Harlan beat me to the two tools I was thinking of! I know a number of other people have built enscripts to be used within encase that will parse the MFT as well.

Dave

Reply

**Phillip Hellewell** June 24, 2010 at 3:21 PM

I work at AccessData and we added this feature in the Forensic Toolkit 3.1 release.

If the filename timestamps differ from the STANDARD_INFORMATION timestamps then they are parsed and can be seen in the properties window when viewing a file.

--
Phillip Hellewell
Software Engineer, AccessData

Reply

**Nathan Swenson** June 24, 2010 at 3:21 PM

FTK 3.1 exposes these values. In the properties pane for a file it lists the $FILE_NAME values for the name values like: "Date Modified (8.3 filename)" - for each of the filenames. It only lists them if they are set and if they differ from the $STANDARD_INFORMATION values, so if you don't see them they are the same. I think this was done because these are 16 extra values to complicate things that are usually the same.

Reply

forensics work. This involved working with software that required using USB dongles (essentially a special USB thumb drive) to authorize the utilization of the software. After almost a decade of doing this work, I've seen the use of these USB dongles expand to the point where my team has an seemingly never ending supply of them for many different programs.

I once joked that if I wrote a book about digital forensics that I'd call it "A Fistful of Dongles" as a joke based on the classic Clint Eastwood western that was titled "A Fistul of Dollars". When I created this blog, I didn't have a good name for it, but eventually decided on the present title.

The blog originally started out as a digital forensics blog, but has since expanded to cover broad topics such as cybercrime, fraud, and information security. Even though this isn't purely a digital forensics blog these days, I still like the name.

**Eric Huber** June 24, 2010 at 7:39 PM

Thanks for the information, Nathan and Phillip. I appreciate you guys taking the time to stop by and let us know how Access Data is innovating in this area.

I upgraded my FTK to the most recent version after reading your posts and I didn't find any files that showed the $FILE_NAME data, but it was just a very quick test.

While I can understand that adding this information might add more clutter to the UI, the solution that Access Data is offering, as you guys describe it, is still the tool deciding what the examiner should see.

I don't want or need that level of hand holding from the tool and I want to be able to see the $FILE_NAME information regardless of whether the tool maker thinks those time stamps are interesting or not.

I also want to be able to see it in the column view along with the $STANDARD_INFORMATION time stamps so that I can sort by that data.

How about allowing us to see this $FILE_NAME data no matter what in the properties window and have it be an optional display option for the column view?

You guys are doing great work with FTK 3. For example, I don't know when you introduced it, but I like the option to have the informational bubble (I forgot what it's called in the UI) appear if I put my cursor over a picture in Gallery view. It's nice to have the name, sizes and created time data at a glance like that.

Reply

Enter your comment...

Comment as: Google Accou

Publish Preview

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

CrowdResponse
*2 weeks ago*

**Lenny Zeltser on Information Security**
Scammers in Action: Domain Names and Family Resettlement to Australia
*3 weeks ago*

**Lance Mueller's ForensicKB**
EnCase v7 EnScript to quickly provide MD5/SHA1 hash values and entropy of selected files
*3 weeks ago*

**Volatility Labs**
Volatility Memory Forensics and Malware Analysis Training in Australia!
*3 weeks ago*

**Andrew Case's Memory Forensics**
Building a Decoder for the CVE-2014-0502 Shellcode
*3 weeks ago*

**Ryan Kubasiak's Apple Examiner**
Boot Camp, Windows and Thunderbolt
*4 weeks ago*

**Jonathan Rajewski's CyberBlog**
Have you seen IDrive in your computer forensic cases? This blog post discusses artifacts
*1 month ago*

**David Nides' nibble on dav nads**
4n6time v.05 - anyone know how I get a tax write off on this???
*2 months ago*

**Jesse Kornblum's A Geek Raised by Wolves**
Hashdeep version 4.4 released
*3 months ago*

**Cheeky4n6Monkey - Learning About Digital Forensics**
Android SMS script update and a bit of light housekeeping
*3 months ago*

**Jimmy Weg's JustAskWeg**
VMware VMs for Free (At Least for Some)
*3 months ago*

**Shelly Giesbrecht's Nerdiosity**
The Road to Lethality
*1 year ago*

**BLOG ARCHIVE**

► 2014 (1)
► 2013 (4)
► 2012 (12)
► 2011 (30)
▼ 2010 (34)
► 12/19 - 12/26 (1)
► 12/05 - 12/12 (1)
► 11/28 - 12/05 (1)
► 11/07 - 11/14 (1)
► 10/17 - 10/24 (1)
► 10/03 - 10/10 (2)
► 09/26 - 10/03 (1)

► 09/12 - 09/19 (2)
► 09/05 - 09/12 (1)
► 08/29 - 09/05 (1)
► 08/22 - 08/29 (2)
► 08/08 - 08/15 (1)
► 08/01 - 08/08 (2)
► 07/25 - 08/01 (1)
► 07/18 - 07/25 (1)
► 07/11 - 07/18 (1)
► 07/04 - 07/11 (1)
► 06/27 - 07/04 (1)
▼ 06/13 - 06/20 (2)
Give Me $FILE_NAME or Give Me Death
Bacon
► 05/30 - 06/06 (1)
► 05/23 - 05/30 (1)
► 05/16 - 05/23 (1)
► 05/09 - 05/16 (1)
► 05/02 - 05/09 (1)
► 04/25 - 05/02 (2)
► 04/18 - 04/25 (1)
► 04/11 - 04/18 (2)