JOURNAL OF FORENSIC SCIENCES

J Forensic Sci, January 2012, Vol. 57, No. 1
doi: 10.1111/j.1556-4029.2011.01919.x
Available online at: onlinelibrary.wiley.com

PAPER

DIGITAL & MULTIMEDIA SCIENCES

Douglas Elrick,[1] *B.A.*

Artifacts of CD Burning in the Microsoft Windows Master File Table

ABSTRACT: When theft of a physical item occurs it is detectable by the fact that the object is missing, however, when the theft of a digital item occurs it can go unnoticed as exact replicas can be created. The original file is left intact but valuable information has been absconded. One of the challenges facing digital forensic examiners is detecting when files have been copied off of a computer system in some fashion. While certain methods do leave residual evidence behind, CD Burning has long been held as a copying method that cannot be identified. Through testing of the burning process and close examination of the New Technology File System (NTFS), artifacts from the master file table in the various versions of Microsoft Windows, markers have been found that are associated with copying or "burning" files to CD or DVD. Potential evidence that was once overlooked may now be detectable.

KEYWORDS: forensic science, Microsoft Windows, CD Burning, master file table, NTFS, artifacts, Vista, XP, Windows 7, attributes

At 8 AM Monday morning, the president of a small local company entered her office and found, from the head of the sales department, a resignation letter that was effective immediately. Owing to the abrupt circumstances, the president contacted her IT manager to discuss what to do with the sales manager's computer. The IT manager reviewed the computer and network logs, and found indications that the sales manager was active on the network over the weekend and in the early hours of Monday morning. The resignation letter was apparently written at 2:30 AM on Monday. Being concerned with the suspicious nature of the activity and the unexpected resignation, the president and her attorney engaged a computer forensic examiner to determine if any proprietary company documents had been copied prior to the departure.

The examiner was requested to identify any items that were accessed over the weekend and to determine what, if anything, was copied from the network or local computer. Subsequent examinations revealed that numerous business documents had been last accessed late on Sunday evening, but review of the registry and link files did not indicate that a USB device had been connected at this time. The system was equipped with a CD/DVD burner but no third party burning software such as Nero™ EZ CD Creator™ was installed. The operating system was Microsoft Windows XP SP2™. The question which has confronted many examiners is, "Can it be determined if files were burned to CD or DVD?"

This above scenario is becoming more and more common in civil and even some criminal investigations. As individuals move from job to job, there is a realistic fear that people are taking proprietary or trade secret data to competitors. Microsoft Windows™ maintains no log when files are burned through the operating system. The registry has a CD Burning key under Software\Microsoft\Windows\CurrentVersion \Explorer\CDBurning, but the last written date appears to be updated every time any optical disk is loaded. Information about the burn session is temporarily available in the registry, but it is cleared on reset.

In a recent case similar to the one above, several hundred documents were last accessed just prior to the employee leaving. Many but not all the files in a particular subfolder were accessed, suggesting a selective process and not an automated routine, such as an antivirus scan, was initiated. Further examination revealed that the New Technology File System (NTFS) entry modified date/time was also updated seconds after the last accessed time. This raised the question as to what would access a file and update the $MFT record.

Methods

Test burning of files through Windows XP SP2™ revealed similar date/time results with the last accessed date/time and the entry modified date/time. An explanation of why the NTFS entry modified date changes requires a little background of the NTFS record. The version of NTFS utilized by Windows XP™, Vista™, and Windows 7™ is 3.1. Microsoft has released little data on exactly how the NTFS works. Most of the information that has been obtained has been through the work of a few select examiners and engineers. NTFS maintains information about all files in the master file table (MFT) (1). Each file has one or more records in the table and each record is 1024 bytes in length. Each record on an NTFS 3.1 system begins with FILE0 as shown in Fig. 1. The first 56 bytes make up the record header (Fig. 2). The table listing the description of record header is shown in Table 1.

The remainder of the record is made up of a series of NTFS attributes. The first attribute will be a standard information attribute (SIA). This attribute begins with a hexadecimal string 10 00 00 00 followed by the number of bytes in the attribute (Figs 3 and 4). Note that in Fig. 3, the first byte after the attribute header (10 00 00 00) is hexadecimal 60 or 96 decimal and this is the number of bytes in this attribute and is highlighted in Fig. 4. The SIA contains the file dates and times as well as legacy DOS attributes, quota tracking information, and a Security ID (1–3).

[1]Director of Forensic Services, Digital Intelligence, 17165 W Glendale Drive, New Berlin, WI 53151.

Received 30 June 2010; and in revised form 3 Nov. 2010; accepted 27 Nov. 2010.

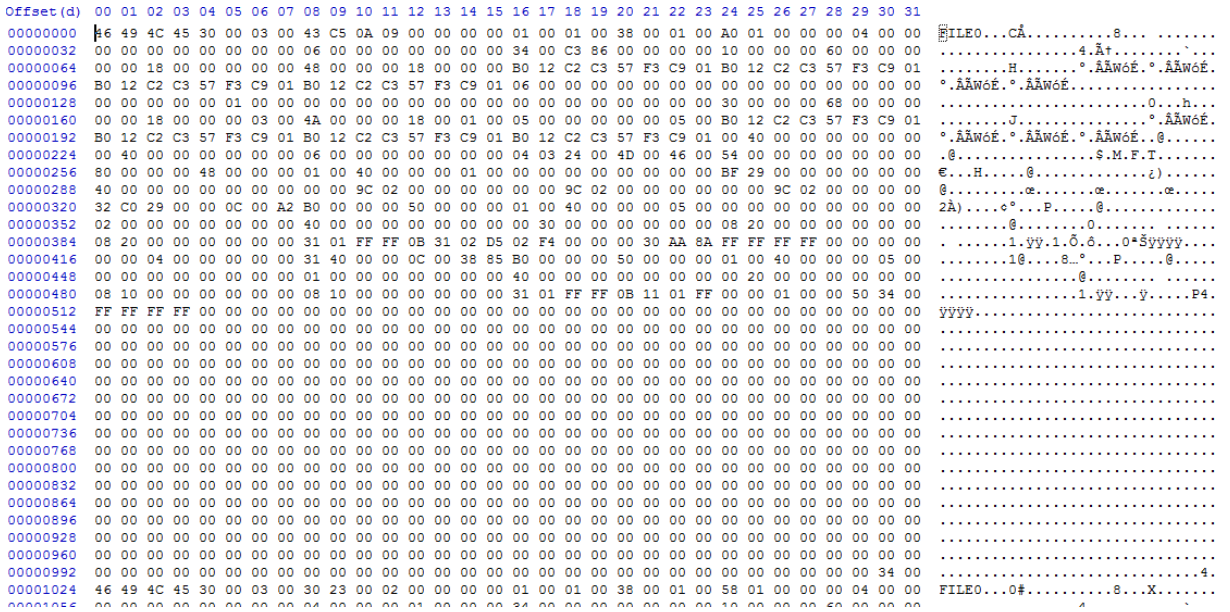

FIG. 1—*$MFT record consisting of 1024 bytes beginning with FILE0.*

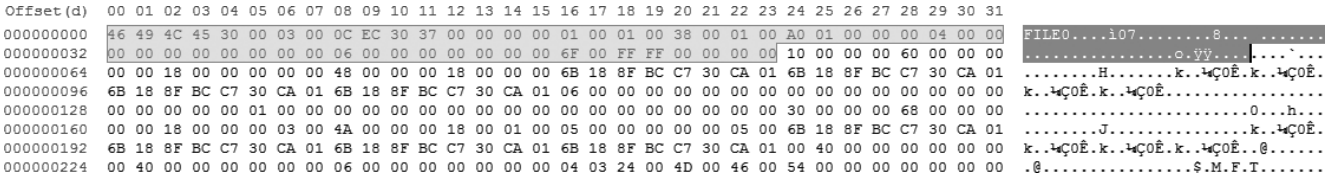

FIG. 2—*Fifty-six bytes $MFT record header.*

TABLE 1—*Header offset descriptions (1).*

$MFT Record Header		
Hex Offset	Size (Bytes)	Description of Bytes in Header
00	4	"FILE" SIGNATURE
04	2	Offset to update sequence
06	2	Size of update sequence
08	8	Log File Sequence Number
16	2	Sequence Number
18	2	Hard Link Count
20	2	Offset to Start of Attributes
22	2	Flags (Deleted Files, Allocated Files, Deleted Directory, Allocated Directory)
24	4	Amount of space used by $MFT records (bytes)
28	4	Amount of space allocated for $MFT records (bytes)
32	8	Base File Reference
40	2	Next Attribute ID
42	2	Update Sequence Number (WinNT/2000)
44	4	$MFT Record Number
48	8	Update Sequence Number (WinXP/Vista/Win7)

Following the SIA, there will be at least one Filename Attribute for each file in the MFT record. If there is a long filename, then there may be two Filename Attributes, one for the 8.3 compliant short filename and one for the long filename. Each Filename Attribute will begin with the hexadecimal string 30 00 00 00 followed by the number of bytes in the attribute (Fig. 5). Included in this attribute will be a reference to the file's parent MFT record number (1–3). This is used to track a specific file's location.

There are numerous other attributes that may be associated with a file. See Table 2 for a listing of common attributes that may be associated with different types of files (1–3). As a reminder of how NTFS is designed, everything in NTFS is a file including traditional system areas, folders, and documents. Different file types will have various attributes, and some attributes are only used for specific file types.

Files such as programs and user created documents will have a Data Attribute (80 00 00 00) that is used to describe the contents of the file. If the amount of data is relatively small (<500 bytes), the data will be stored directly in the $MFT record in the Data Attribute and is referred to as resident data because it is resident in

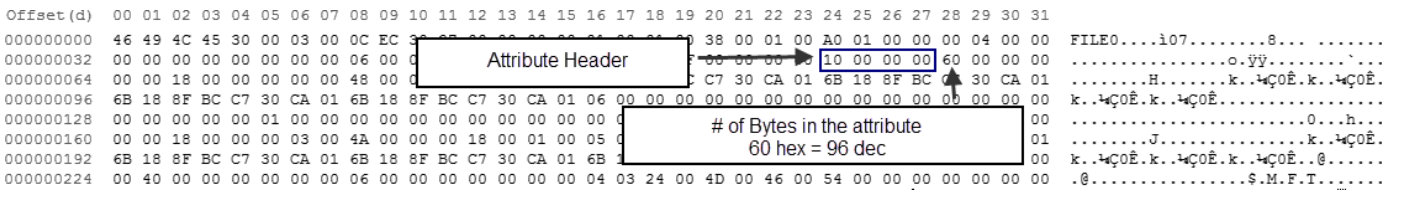

FIG. 3—*Standard information attribute.*

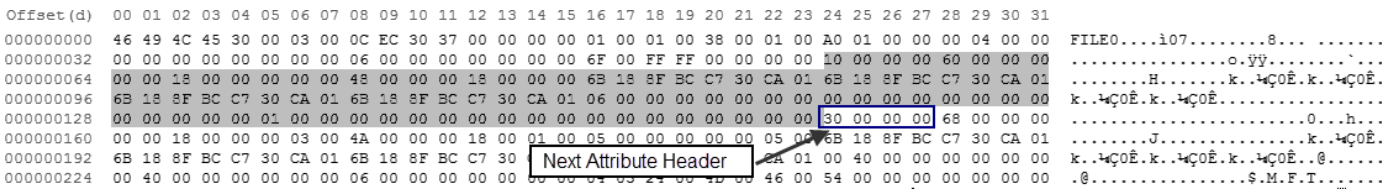

FIG. 4—*Ninety-six bytes of standard information attribute followed by Next Attribute and size.*

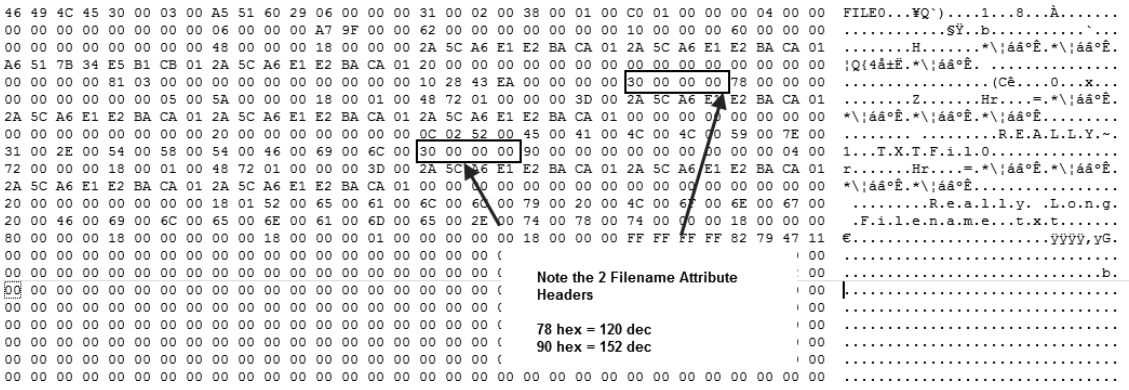

FIG. 5—*There are Filename Attributes for both the short and long filenames.*

TABLE 2—*Portion of attribute list.*

$MFT Attribute Headers	
Attribute Header (Hex)	Description
10 00 00 00	Standard Information
20 00 00 00	Attribute List
30 00 00 00	Filename
40 00 00 00	Object Identifier
50 00 00 00	Security Descriptor
60 00 00 00	Volume Name
70 00 00 00	Volume Information
80 00 00 00	Data

the record. Larger data will be stored in allocated clusters on the drive and the listing of the clusters used (runlist) will be stored in the Data Attribute of the MFT record (Fig. 6). This is referred to as nonresident, as the data is not resident in the MFT record.

While there is a great deal more information that could be reviewed on NTFS, the information above provides the primer for understanding why a $MFT record is updated when a file is burned to a disk through Microsoft Windows™. To determine what changes to the record take place when a file is burned to a CD through Microsoft Windows™, a comparison was done between a MFT file record before, during, and after the burn process. To begin, a sample file was selected that was located on the same volume as the operating system, which was identical to the actual case. The 1024 bytes from the MFT for the sample file were exported to a text file. The sample file was then dragged by use of Windows Explorer to the CD drive icon and the 1024 byte record from the MFT for the file was exported again. The burn process to the CD disk was then allowed to complete. The 1024 byte record from the MFT for the file was exported for a final time to another text file. The three text files generated were identified as PREBURN.TXT, MIDBURN.TXT, and POSTBURN.TXT. A comparison of the files revealed several bytes in the record that were changed. Most of the changes occur whenever a record is updated, regardless of what the changes were, and these were determined to be insignificant. One particular byte in the header that was updated, however, was the Next Attribute ID Number (see Table 1; [1–3]). Originally, there were four attributes present in the record of the sample file and the Next Attribute number recorded was five (Table 3 and Fig. 7).

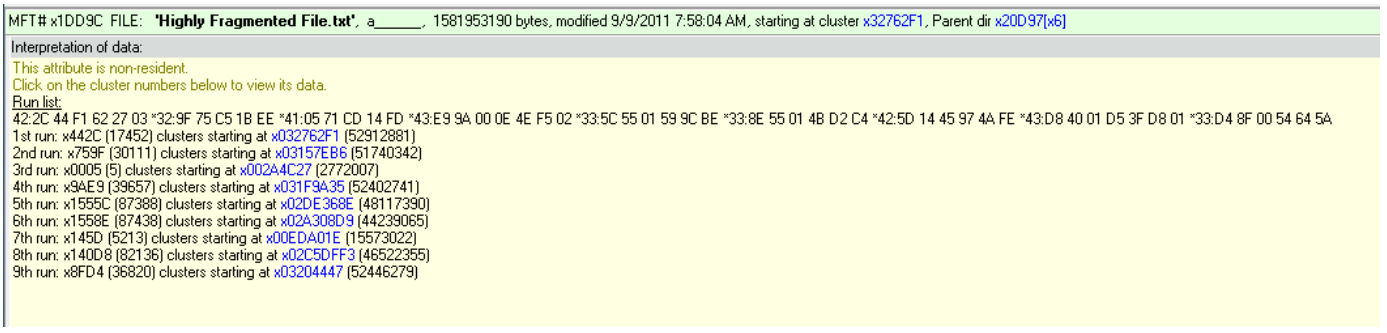

FIG. 6—*Runlist for a nonresident Data Attribute as displayed by DiskExplorer for NTFS (3).*

Documentation on the Next Attribute ID is very limited even from Microsoft (http://msdn.microsoft.com/en-us/library/bb470124%28VS.85%29.aspx; accessed November 3, 2010), but what is present reveals that this value should be the number of existing attributes plus one (1). As additional attributes are added, this value will increase.

TABLE 3—*Prior to burning, the Next Attribute ID count equals the number of attributes +1 as displayed by Disk Explorer for NTFS (http://www.runtime.org/diskexplorer.htm; accessed November 3, 2010).*

$MFT Record Header	
Description	Value (Decimal)
''FILE'' SIGNATURE	FILE
Offset to update sequence	48
Size of update sequence	3
Log File Sequence Number	124594657
Sequence Number	6
Hard Link Count	2
Offset to Start of Attributes	56
Flags (Deleted Files, Allocated Files, Deleted Directory, Allocated Directory)	1
Amount of space used by $MFT records (bytes)	520
Amount of space allocated for $MFT records (bytes)	1024
Base File Reference	0
Next Attribute ID	5
$MFT Record Number	11061

TABLE 4—*File that has been dragged to CD drive and Hard Link created as displayed by Disk Explorer for NTFS (http://www.runtime.org/diskexplorer.htm; accessed November 3, 2010).*

$MFT Record Header	
Description	Value (Decimal)
''FILE'' SIGNATURE	FILE
Offset to update sequence	48
Size of update sequence	3
Log File Sequence Number	124627367
Sequence Number	6
Hard Link Count	3
Offset to Start of Attributes	56
Flags (Deleted Files, Allocated Files, Deleted Directory, Allocated Directory)	1
Amount of space used by $MFT records (bytes)	688
Amount of space allocated for $MFT records (bytes)	1024
Base File Reference	0
Next Attribute ID	6
$MFT Record Number	11061

Results

The attributes present in the original record were the SIA, two Filename Attributes, and a Data Attribute (Fig. 7). After dragging the file to the CD Drive and examining the resultant record, it was noted that there was a Hard Link created for the file. This link was created in C:\Documents and Settings\User Profiles\Local Settings\Application Data\ Microsoft \CD Burning on a Microsoft Windows XP™ system or in C:\Users\User Profile\App Data\Local\Microsoft \Windows\Burn\Burn in Microsoft Windows Vista™ and Windows 7™. Unlike a Shortcut Link file, which creates a LNK file, the Hard Link is simply another Filename Attribute in the MFT record associated with the same data as the other Filename Attributes and may have with a different parent folder. Note that the two original Filename Attributes have the same parent folder (Fig. 7). Additionally, Hard Links can only be created on the same volume as the original file (1). The result of the creation of the Hard Link is that another Filename Attribute is inserted into the MFT record along with the original Filename Attributes. This pushes the Data Attribute further toward the end of the record. The Next Attribute ID number is increased because of the additional Filename Attribute. In the example from above, the Next Attribute ID number is increased to six. The Hard Link count number is also increased from two (short filename and long filename) to three (Table 4 and Fig. 8). Note that the parent of the additional Filename Attribute is different than the first two (Fig. 8) and resolves back to C:\Documents and Settings\User Profiles\Local Settings\Application Data\ Microsoft \CD Burning.

Once the file is successfully burned, then the Hard Link is deleted from the record. This leaves the original four attributes. What was noted of apparent significance was that the Next Attribute ID remains at six (Table 5).

Further examination of the postburn record also revealed data in the record slack (the area from the end of the Data Attribute to the end of the record). The data in the slack contains a portion of the information from the Hard Link Filename Attribute (Figs 9 and 10). It is apparent that once the burn is completed, the Data Attribute is then shifted back to its original record location. If the Hard Link Filename Attribute is sufficiently large and the Data Attribute relatively small (nonresident runlist), then only the beginning portion of the added Hard Link is overwritten by the shifted Data Attribute. The remaining portion of the attribute contains the attribute date and time information. The Hard Link count in the record header is decreased after the burn, but it is apparent that the Next Attribute ID counter that was increased when the record was added is not decreased when the attribute is deleted. This result was consistent with the Next Attribute ID testing conducted by Sammes and Jenkinson (3).

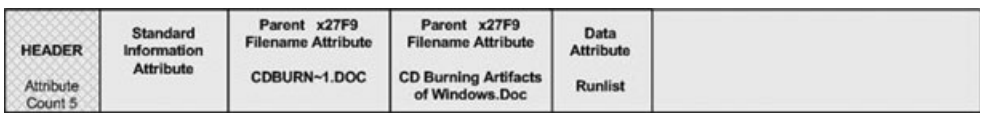

FIG. 7—*Graphical representation of the master file table record prior to selecting the file for burning.*

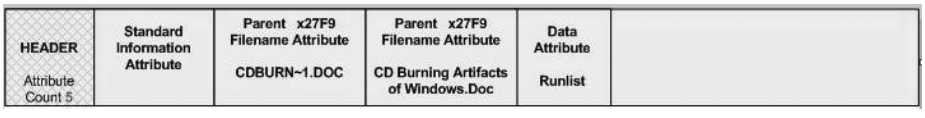

FIG. 8—*Graphical representation of the master file table record when file has been selected for burning and the additional attribute.*

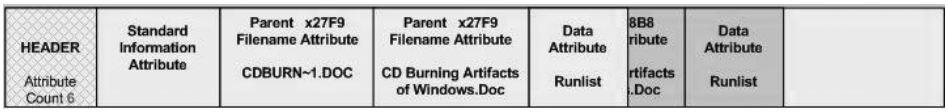

FIG. 9—*Graphical representation showing the Data Attribute shifted and overwriting part of the Filename Attribute.*

TABLE 5—*After the file is burned, the Hard Link is deleted but the Next Attribute ID count is not reduced.*

$MFT Record Header	
Description	Value (Decimal)
"FILE" SIGNATURE	FILE
Offset to update sequence	48
Size of update sequence	3
Log File Sequence Number	124654509
Sequence Number	6
Hard Link Count	2
Offset to Start of Attributes	56
Flags (Deleted Files, Allocated Files, Deleted Directory, Allocated Directory)	1
Amount of space used by $MFT records (bytes)	520
Amount of space allocated for $MFT records (bytes)	1024
Base File Reference	0
Next Attribute ID	6
$MFT Record Number	11061

```
00 00 00 00 00 00 00 00 30 00 00 00 78 00 00 00  ........0...x...
00 00 00 00 00 00 03 00 5A 00 00 00 18 00 01 00  ........Z.......
F9 27 00 00 00 00 01 00 42 9B 5F DD C5 A2 CA 01  ù'......B›_ÝÅ¢Ê.
42 9B 5F DD C5 A2 CA 01 42 9B 5F DD C5 A2 CA 01  B›_ÝÅ¢Ê.B›_ÝÅ¢Ê.
42 9B 5F DD C5 A2 CA 01 00 00 00 00 00 00 00 00  B›_ÝÅ¢Ê.........
00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00  ........ .......
0C 02 43 00 44 00 42 00 55 00 52 00 4E 00 7E 00  ..C.D.B.U.R.N.~.
31 00 2E 00 44 00 4F 00 43 00 72 00 74 00 69 00  1...D.O.C.r.t.i.
30 00 2E 00 A8 00 00 00 00 00 00 00 00 00 02 00  0...¨...........
8E 00 00 00 18 00 01 00 F9 27 00 00 00 00 01 00  Ž.......ù'......
42 9B 5F DD C5 A2 CA 01 42 9B 5F DD C5 A2 CA 01  B›_ÝÅ¢Ê.B›_ÝÅ¢Ê.
42 9B 5F DD C5 A2 CA 01 42 9B 5F DD C5 A2 CA 01  B›_ÝÅ¢Ê.B›_ÝÅ¢Ê.
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
20 00 00 00 00 00 00 00 26 01 43 00 44 00 20 00   .......&.C.D. .
42 00 75 00 72 00 6E 00 69 00 6E 00 67 00 20 00  B.u.r.n.i.n.g. .
41 00 72 00 74 00 69 00 66 00 61 00 63 00 74 00  A.r.t.i.f.a.c.t.
73 00 20 00 6F 00 66 00 20 00 4D 00 69 00 63 00  s. .o.f. .M.i.c.
72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 2E 00  r.o.s.o.f.t. ...
64 00 6F 00 63 00 00 00 80 00 00 00 48 00 00 00  d.o.c...€...H...
01 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00  ................
76 01 00 00 00 00 00 00 40 00 00 00 00 00 00 00  v.......@.......
00 70 17                 17 00 00 00 00 00 00 00  .p......h.......
00 68 17                 01 CF C2 26 05 00 00 00  .h.....2w.ÏÂ&...
FF FF FF                 00 00 00 00 00 00 00 00  ÿÿÿÿ.yG ........
26 01 43 00 44 00 20 00 42 00 75 00 72 00 6E 00  &.C.D. .B.u.r.n.
69 00 6E 00 67 00 20 00 41 00 72 00 74 00 69 00  i.n.g. .A.r.t.i.
66 00 61 00 63 00 74 00 73 00 20 00 6F 00 66 00  f.a.c.t.s. .o.f.
20 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00   .M.i.c.r.o.s.o.
66 00 74 00 20 00 2E 00 64 00 6F 00 63 00 00 00  f.t. ...d.o.c...
80 00 00 00 48 00 00 00 01 00 00 00 00 00 04 00  €...H...........
00 00 00 00 00 00 00 00 76 01 00 00 00 00 00 00  ........v.......
40 00 00 00 00 00 00 00 70 17 00 00 00 00 00 00  @.......p.......
00 68 17 00 00 00 00 00 00 68 17 00 00 00 00 00  .h.......h......
32 77 01 CF C2 26 00 00 FF FF FF FF 82 79 47 11  2w.ÏÂ&..ÿÿÿÿ,yG.
```

Record Slack

FIG. 10—*Data Attribute is shifted and overwrites part of the Filename Attribute.*

It was noted that if another MFT attribute is present between the Filename Attribute and the Data Attribute, such as the Object ID Attribute (40 00 00 00) when the Hard Link is deleted, then both the Object ID Attribute and the Data Attribute shift and overwrite most if not all of the added Hard Link in the record slack. This can also occur if there is resident data in the Data Attribute. Repeated test were conducted using different files and folders with consistent results.

After making the determination as to the creation and deletion of the Hard Link, an analysis was conducted to see what other functions would produce the same results. Hard Links can be manually created and deleted for a file at a command prompt using "fsutil hardlink" in Microsoft Windows XP or "mklink" in Microsoft Vista and Windows 7. However, simply creating the Hard Link does not update the last accessed date and time. Also, the number of files and the time range in which the Hard Links were created and accessed must be considered. It is unlikely that numerous files could be accessed simultaneously and Hard Links created manually in the span of a few seconds. While the artifacts mentioned above are not conclusive evidence that a file was burned to disk, no other process has been found to produce the same effects.

The artifacts described above will also occur if a file is dragged to the CD and then deleted from the CD without burning. Deleting the file reference from the CD removes the Hard Link just as if the file had been burned.

Discussion

In summary, the method for determining potential files burned to disk starts with identifying groups of files with the same or very similar Last Accessed date/times. Then, examine the Entry Modified dates of these files to see if they are also in this same time range and shortly after the Last Accessed times. This will obviously give false positives; however, the MFT records can then be examined to see if the Next Attribute ID number is higher than expected for the number of attributes present. Finally, the record slack for each of these can be examined to see if it contains remnants of a Filename Attribute. This can provide a list of files that could have been burned to a disk.

As described above, Hard Links are only created on the same volume as the original file. For CD/DVD burning through Windows, if the original file is not located on the system volume (where the CD BURNING or BURNING folder is located) then a complete copy of the file is created and then deleted when the burn is completed. An examination for deleted files in this folder or for deleted MFT records can provide evidentiary information.

While no conclusive method has been established, the examination of the MFT records can help provide strong evidence of the file activity.

References

1. Carrier B. File system forensic analysis. Upper Saddle River, NJ: Addison-Wesley, 2005.
2. Guidance Software Inc. NT File System and Artifacts training manual. Pasadena, CA: Guidance Software, 2005.
3. Sammes T, Jenkinson B. Forensic computing: a practitioner's guide, 2nd edn. London, UK: Springer-Verlag, 2007.

Additional information and reprint requests:
Douglas Elrick, B.A.
Director of Forensic Services
Digital Intelligence
17165 W Glendale Drive
New Berlin, WI 53151
E-mail: delrick@digitalintelligence.com