Volume Serial Numbers and Format Date/Time Verification

Written by Craig Wilson, MSc MBCS CITP
Digital Detective Group
October 2003 (updated June 2005)

Table of Contents

Introduction

Format Date/Time

From time to time, it may be necessary to verify, or attempt to identify when a floppy diskette or hard drive was formatted. This may be possible by examining some of the data added to the disk at the time it was formatted. This whitepaper looks at some of the techniques for identifying when a volume or floppy diskette may have been formatted.

Naming Conventions

In this document I will use the C language syntax to represent hexadecimal numbers. Numbers that have been prefixed with "0x" are hexadecimal (base 16) numbers. Any numbers that have not been prefixed with "0x" are decimal (base 10) numbers.

Volume Serial Number

The volume serial number[1] was added to the standard format for IBM PC-compatible disks in 1987, when Microsoft and IBM were co-developing OS/2. They wanted the system to operate like the Macintosh, which automatically recognised which diskette (or removable disk cartridge) had been inserted in a drive. Up to that point, the only identifying information on an IBM-compatible disk was its volume label[2]. If the user declined to assign a name to the disk, or gave more than one disk the same name, there was no way to tell them apart.

With this in mind, the two companies decided to change the disk formats for both MS-DOS and OS/2 to include a four byte volume serial. When a disk was formatted, it would be stamped with this number, which in certain operating systems (see note below), was constructed from the exact date and time the format operation was performed. These values allowed FAT file system drivers to detect that the wrong disk had been inserted in a removable drive. The odds of two disks getting the same number were virtually nil on the same machine, and were still small even if users exchanged disks with one another.

When a diskette was reproduced by the operating system's disk copying program (DISKCOPY), the program would make a faithful copy of every byte on the entire disk except for the volume serial number, which would be changed to something different than the one on the original diskette.

Note: Some operating systems assign the volume serial number by calculating it from the format date/time. The calculation method seems to have changed for disks and volumes formatted with Microsoft Windows 2000 and XP. [2][1]

[1] Volume Serial Number – a 32-bit value assigned to a floppy diskette or FAT volume for identification purposes.
[2] Volume Label – a user assigned label to assist with the identification of a particular disk or volume.

Date/Time Calculation – Method One

Unfortunately for forensic examiners, it is not possible to decode the volume serial number and verify the format date/time unless you have some of the information already.

The Lo order word[3] is calculated by taking the month and day value and converting them to hexadecimal. The number of seconds and 100ths of seconds are also converted to hexadecimal and added to month & day value. The Hi order word is calculated by taking the hours & minutes value and converting them to hexadecimal. This is then added to the hexadecimal value of the year. If you know the year the disk was formatted, it is then possible to calculate the time. Calculating the date is a little more difficult as you need the exact seconds and 100ths of a second and vice versa. If you know the date, then it is possible to calculate the format time.

Here is an example from a formatted FAT12 floppy diskette. With reference to Figure 1 below, at offset 39 (0x27), you can see the hex values 25 14 1D F4 which is the Volume Serial Number.

With FAT32 volumes, the Volume Serial Number is stored in the Boot Sector at offset 67 (0x43).

When formatted, this floppy diskette returned the volume serial 2514-1DF4.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	EB	3C	90	4D	53	44	4F	53	35	2E	30	00	02	01	01	00	ë<□MSDOS5.0.....
00000016	02	E0	00	40	0B	F0	09	00	12	00	02	00	00	00	00	00	.à.@.ð..........
00000032	00	00	00	00	00	00	29	25	14	1D	F4	4E	4F	20	4E	41	......)%..ôNO NA
00000048	4D	45	20	20	20	20	46	41	54	31	32	20	20	20	33	C9	ME FAT12 3É
00000064	8E	D1	BC	F0	7B	8E	D9	B8	00	20	8E	C0	FC	BD	00	7C	ŽÑ¼ð{ŽÙ¸. ŽÀü½.|
00000080	38	4E	24	7D	24	8B	C1	99	E8	3C	01	72	1C	83	EB	3A	8N$}$‹Á™è<.r.ƒë:
00000096	66	A1	1C	7C	26	66	3B	07	26	8A	57	FC	75	06	80	CA	f¡.|&f;.&ŠWüu.€Ê
00000112	02	88	56	02	80	C3	10	73	EB	33	C9	8A	46	10	98	F7	.ˆV.€Ã.së3ÉŠF.˜÷
00000128	66	16	03	46	1C	13	56	1E	03	46	0E	13	D1	8B	76	11	f..F..V..F..Ñ‹v.
00000144	60	89	46	FC	89	56	FE	B8	20	00	F7	E6	8B	5E	0B	03	`‰Fü‰Vþ¸ .÷æ‹^..
00000160	C3	48	F7	F3	01	46	FC	11	4E	FE	61	BF	00	00	E8	E6	ÃH÷ó.Fü.Nþa¿..èæ
00000176	00	72	39	26	38	2D	74	17	60	B1	0B	BE	A1	7D	F3	A6	.r9&8-t.`±.¾¡}ó¦
00000192	61	74	32	4E	74	09	83	C7	20	3B	FB	72	E6	EB	DC	A0	at2Nt.ƒÇ ;ûræëÜ
00000208	FB	7D	B4	7D	8B	F0	AC	98	40	74	0C	48	74	13	B4	0E	û}´}‹ð¬˜@t.Ht.´.
00000224	BB	07	00	CD	10	EB	EF	A0	FD	7D	EB	E6	A0	FC	7D	EB	»..Í.ëï ý}ëæ ü}ë
00000240	E1	CD	16	CD	19	26	8B	55	1A	52	B0	01	BB	00	00	E8	áÍ.Í.&‹U.R°.»..è
00000256	3B	00	72	E8	5B	8A	56	24	BE	0B	7C	8B	FC	C7	46	F0	;.rè[ŠV$¾.|‹üÇFð
00000272	3D	7D	C7	46	F4	29	7D	8C	D9	89	4E	F2	89	4E	F6	C6	=}ÇFô)}ŒÙ‰Nò‰NöÆ

Figure 1

In the example above, the disk was formatted on Sunday, 19th October 2003 at 22:33:27.01, local time. Figure 2 shows how the Volume Serial Number would be calculated.

[3] Word – name used to describe two bytes or a 16-bit integer.

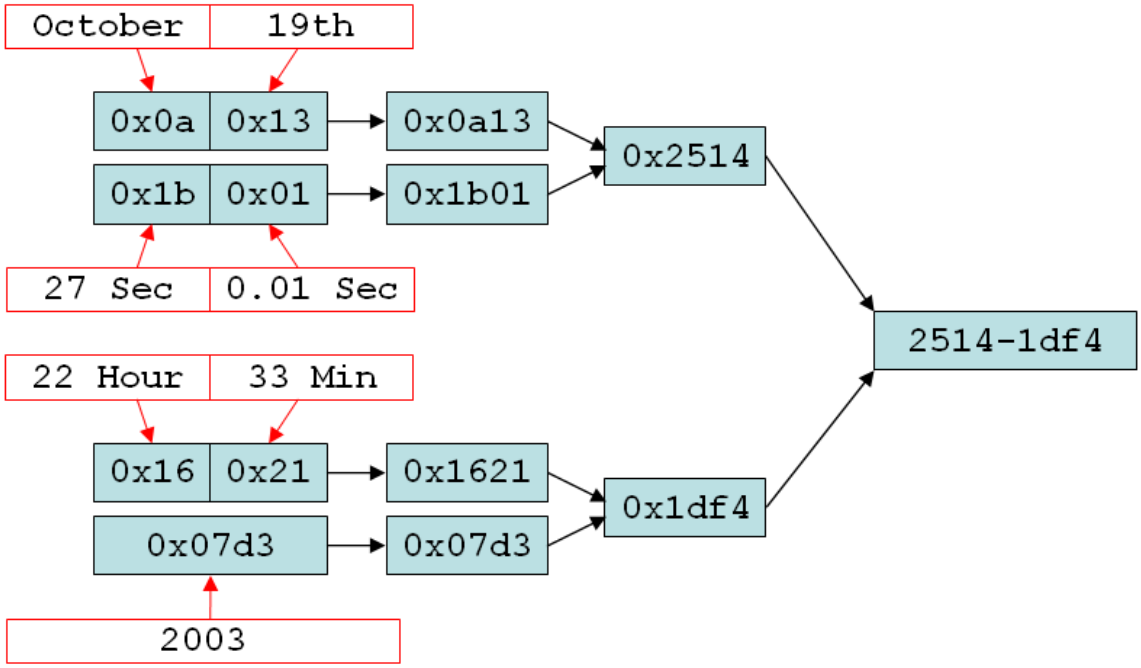

Figure 2

Alternative Verification – Method Two

We can now go one step further to see if we can verify this date/time value is correct. If the user set the volume label at the time of format, then this should be recorded in the boot sector and a root directory entry[4]. The field in the boot sector should match the 11-byte volume label recorded in the root directory [Microsoft 2000].

Note: FAT file system drivers should make sure that they update this field when the volume label file in the root directory has its name changed or created. However, Microsoft ignored their own recommendation as Windows XP does not update the boot sector field. It leaves the field set to the string "NO NAME ", which is the default for when the volume label has not been set.

Once again, differences in the formatting operating system will dictate whether this data area is set to reflect the volume label. If we query the disk by using the VOL command, Figure 3 clearly shows that in this case, the data is not being extracted from boot sector.

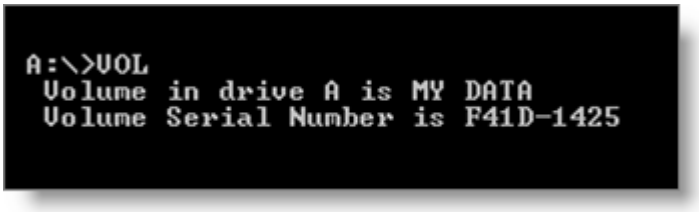

Figure 3

[4] Directory Entry – in a FAT file system, this is a 32 byte record which stores information about a particular file such as the name, size, date/times and starting cluster.

Examination of the root directory identifies a directory entry which contains a name identical to our volume label. The label is stored in the exact same way as a file or folder but has a special flag to indicate that this is a volume label.

FAT Directory Entry Structure

As mentioned previously, directory entries are made up from a 32 byte structure. This structure is outlined in Table 1. As we can see from the structure, there is an attribute for Volume_ID. We can also see that there are a number of date/time fields associated with this structure. When a disk is formatted and the volume serial number is added with a directory entry, the last written date/time fields are updated.

Offset	Size (Bytes)	Description
0 (0x00)	11	Short name
11 (0x0B)	1	File Attributes: ATTR_READ_ONLY 0x01 ATTR_HIDDEN 0x02 ATTR_SYSTEM 0x04 ATTR_VOLUME_ID 0x08 ATTR_DIRECTORY 0x10 ATTR_ARCHIVE 0x20 ATTR_LONG_NAME 0x0F
12 (0x0C)	1	Reserved for use by Windows NT
13 (0x0D)	1	Millisecond stamp of file creation time. This field actually contains a count of tenths of a second. The granularity of the seconds in created time field is 2 seconds so this field is a count of tenths of a second and its valid value range is 0-199 inclusive. ***NOTE: Some forensic applications do not take this field into account and therefore misrepresent the created time of a file or folder.***
14 (0x0E)	2	Time when file/folder created
16 (0x10)	2	Date when file/folder created
18 (0x12)	2	Last access date. Note that there is no last access time, only a date. This is the date of last read or write. In the case of a write, this should be set to the same date as last write date.
20 (0x14)	2	High word of this entry's first cluster number (always 0 for FAT12 or FAT16 volume).
22 (0x16)	2	Time of last write. Note that file creation is considered a write.
24 (0x18)	2	Date of last write. Note that file creation is considered a write.
26 (0x1A)	2	Low word of this entry's first cluster number – will be set to zero for a Volume_ID.
28 (0x1C)	4	32-bit DWORD[5] holding this file size in bytes – set to zero for folder

Table 1

If we examine the floppy diskette again, the directory entry is as shown in Figure 4.

[5] DWORD – 32-bit integer or double word

```
offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00002600   4D 59 20 44 41 54 41 20  20 20 20 08 00 00 00 00   MY DATA     .....
00002610   00 00 00 00 00 00 35 B4  53 2F 00 00 00 00 00 00   ......5´S/......
```

Figure 4

Record offset 11 (0x0B) is set to 0x08 which indicates the attribute is for a Volume_ID. We can also see that from record offset 22 (0x16) there are last written date/time values. If the volume label has not been updated since this disk was first formatted, then this date/time value should be very close to the data used to create the volume serial number.

To decode this date/time value, I have used a free tool called DCode [3] which was written to extract different types of date/time values found during forensic investigations. This tool is available from http://www.digital-detective.co.uk.

To decode the date/time value, take the raw hex values (35 B4 53 2F) and enter them as shown in Figure 5. Time zone settings make no difference to the final outcome in this case as MS-DOS date/time values are stored as a local time.

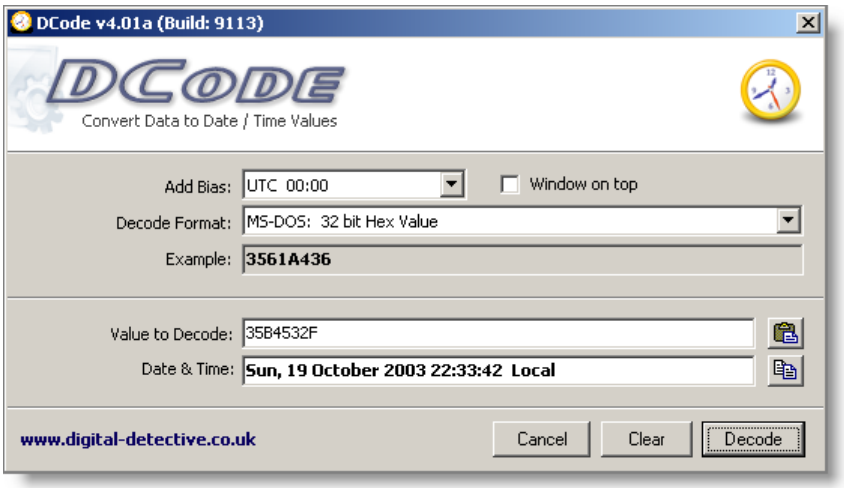

Figure 5

This value decodes to Sunday, 19th October 2003 22:23:42 hours. If we refer to the data extracted from the volume serial calculation as outlined on page 4 (Sunday, 19th October 2003 at 22:33:27.01), we can see that the date/time value recorded in the directory entry is approximately 10 seconds earlier.

Summary

As we have seen in this paper, it may be possible to identify the format date/time of a FAT volume depending on which operating system created it. However, because of the method used to create the serial number, some of the date/time information will need to be known if there is an attempt to extract this date/time.

If the user assigned a volume label at the time of format, then the Volume_ID directory entry should reflect the last time this was updated, as long as this label has not been changed since format. If the label has been updated, then the entry will be modified to reflect the time of change.

List of References

[1] Microsoft, (2000). *"Microsoft Extensible Firmware Initiative FAT32 File System Specification - FAT: General Overview of On-Disk Format" Hardware white paper*. Retrieved January 19, 2003, from http://www.microsoft.com/whdc/system/platform/firmware/fatgen.mspx.

[2] Carrier, B. (2005). *File System Forensic Analysis*. United States: Addison-Wesley.

[3] Wilson, C. (2002). *DCode Software*. Retrieved January 19, 2003, from Digital Detective: http://www.digital-detective.co.uk.