

FILETIME Timestamp and Structure

A FILETIME is a 64-bit value that represents the number of 100-nanosecond intervals that have elapsed since 1st January 1601 at 00:00 Hours Coordinated Universal Time (UTC). The system records file times when applications create, access, and write to (modify) files. The NTFS file system stores time values in UTC format, so they are not affected by changes in time zone or daylight saving time. The FAT file system stores time values based on the local time of the computer. For example, a file that is saved at 3:00pm PST in Washington is seen as 6:00pm EST in New York on an NTFS volume, but it is seen as 3:00pm EST in New York on a FAT volume. Timestamps are updated at various times and for various reasons.

Not all file systems can record creation and last access times, and not all file systems record them in the same manner. For example, the resolution of the created timestamp on FAT is 10 milliseconds, whilst the write (modification) timestamp has a resolution of 2 seconds; the access timestamp has a resolution of 1 day, so it is really the access date. The NTFS file system delays updates to the last access time for a file by up to 1 hour after the last access.

FILETIME Structure

The FILETIME structure contains a 64-bit value representing the number of 100-nanosecond intervals since January 1, 1601 (UTC).

```
typedef struct _FILETIME {
    DWORD dwLowDateTime;
    DWORD dwHighDateTime;
} FILETIME, *PFILETIME;
```

Members

The structure contains two members as follows.

dwLowDateTime

The low-order part of the file time

dwHighDateTime

The high-order part of the file time



This structure can be seen in Microsoft Internet Explorer Cookie files where the timestamp is stored as two 32bit integer values.