R3 Digital Forensics

1803 West Avenue
Austin, Texas 78701
(512) 895-9555
(512) 895-9555
www.r3forensics.com

How Microsoft Word Metadata Works

Digital forensic training and experience provides an understanding of how Microsoft Word metadata functions. However, in order to confirm opinions and conclusions derived from Microsoft Word metadata analysis, "in-house" experiments were conducted using Windows 7 Professional and Microsoft Word 2010. Experiment results were considered conclusive if the same process generated the same result three consecutive times.

Notable Observation: As soon as Microsoft Word opens a document, the edit time clock starts ticking and is updated within the metadata in real time for as long as the document is open. If it is a new blank document, the created time is the time Microsoft word opened the blank document.

1. Start MS Word, Open blank document:
    a. Create time: reflects the time the blank document initiated
    b. Last modified time: <none>
    c. Revision #: set to 1
    d. Author: current user
    e. modified by: <none>

2. Save new document for the first time:
    a. Create time: does not change
    b. Last modified time: updated to current time (time saved)
    c. Edit time: updated to reflect total time document has been open since creation
    d. Author: unchanged
    e. Modified by: current user (in this case, same as author)
    f. Revision #: does not change (stays set to 1)

3. Open an already existing document:
    a. Create time: does not change
    b. Last modified: date does not change
    c. Edit time: clock starts ticking
    d. Author: does not change
    e. Modified By: does not change
    f. Revision #: does not change

4. Save an already existing document that has been opened:
    a. Create time does not change
    b. Last modified: changes to current time
    c. Edit time: updated to reflect total time document has been open since creation
    d. Author: unchanged
    e. Modified By: changes to current user
    f. Revision #: increases by 1

5. Save as -- moving or renaming file:
    a. Create time: reset to current time
    b. Last modified: reset to current time
    c. Edit time:
        1. Resets to 0 if the "save as" process starts and completes in the same minute
        2. Resets to 1 if the process started before the end of a minute, and completes after the second hand crosses 12, into a new minute
    d. Modified By: changes to current user
    e. Revision #: Set to 2, regardless of the number of revision that have occurred