

EXAM 3 Findings:

DON'T READ THIS UNTIL YOU HAVE COMPLETED EXAM 3! This is my favorite exam and if you don't download and attempt this examination you will break my heart. Download this or do not expect an invite to my birthday party. Last warning....don't read on!

For review, your financial wellbeing and the client need the created date of this document to be in 2009. Below is the important document information:

“Validate Word Dates.doc” File System Information:

Created: Wednesday, March 4, 2009, 2:53:46 PM

Modified: Tuesday, April 14, 2009, 8:32:58 PM

“Validate Word Dates.doc” Metadata Information:

Revision number: 10

Date created: 3/4/2009, 1:53 PM

Date modified: 4/14/2009, 8:32 PM

Last printed: 3/19/2009, 6:31 PM

Total editing time: 01:33:00

Findings:

- The file system creation date is 1 hour different from the Date created metadata field.
- The file system modification date and “Date modified” metadata field match perfectly.
- The document metadata appears to indicate normal use.
- Inside the document is the image of the company logo in the document header.
- This appears to have been saved on a server or NAS as the drive letter it was collected from is S.

- The file system creation date and the “Date created” metadata field date and time is 1 hour apart. This is most likely due to daylight saving time which begins on the second Sunday of March and ends on the first Sunday of November. In 2009 daylight saving time began on Sunday, March 8. With day light saving time the clock moves ahead one hour in March, whereas it moves back one hour in November. It appears that the workstation has day light saving enabled and the server or NAS does not.
- The EXIF data of the JPEG of the company logo save in the document header shows this image was saved using Adobe Photoshop CS5 using a Windows machine on 2/20/2015, 2:32 PM.
- Your work should NOT stop here! Look online and find that Adobe Photoshop CS5 was not released until May 2010!

Conclusion:

There is NO way this Microsoft Word document can be created on April 14th, 2009. The image’s EXIF data show it was created on February 20th, 2015 using Adobe Photoshop CS5. This document was created 5 years, 11 months, 16 days, 39 minutes and 51 seconds BEFORE the image was created. Additionally, Adobe Photoshop CS5 was not available for purchase for 421 days after this Microsoft Word document was created. This can only be accomplished by setting the clock back on the computer and falsifying the document.

Fun side facts:

- ALWAYS keep in mind that opposing council's forensic examiner is often hired to examine the data that supports opposing counsel's case ONLY. A forensic examiner is not typically asked to perform hours of examination on dates that the client and client are sure of. Remember that the opposing forensic examiner is your peer and is no better or worse than you. They are often placed in a bad situation because of the items they were asked to examine. Keep yourself in check!
- You can save an image as a JPG or TIF in Office 2010 and older and see the EXIF data natively if the image contains any. Right click on the image and select "Save as".
- If an image is large, the office application will often shrink it changing the image.