UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

PAUL D. CEGLIA,

Plaintiff,

v.

MARK ELLIOT ZUCKERBERG, Individually, and FACEBOOK, INC.

Defendants.

Civil Action No. : 1:10-cv-00569-RJA

**DECLARATION OF JERRY GRANT IN SUPPORT OF REPLY TO DEFENDANT'S MOTION TO DISMISS**

JERRY GRANT, submits this declaration and hereby declares under penalty of perjury and pursuant to 28 U.S.C. 1746 and under the laws of the United States that the following is true and correct:

1. I make this declaration upon personal knowledge.
2. I am a Certified AccessData Forensic Examiner
3. I have more than 25 years of professional computer forensic expert and systems analysis experience.
4. I am currently a Computer Forensic Investigator for the Western District of New York Federal Public Defender's Office.
5. I perform forensic investigations on electronic evidence involved in Federal Criminal Cases.
6. I have lectured and conducting training programs for many large groups at various companies and have received many certificates in forensics, specialized computer training and programming. I have lectured at a number of local and

national computer forensics conferences.

7. Lectured on numerous technical subjects including DOS and Windows file systems, architecture and the boot process, DOS and Windows examination techniques and procedures, recovery of deleted files, date and time stamp definitions / alterations, recovering formatted disks, the process and problems in making duplicate copies of media, file type identification and the use of file viewing applications during examinations, archived files and compressed disks, data format conversion, and the examination of Windows swap and related files.

8. Metadata, often described as "data about data", can consist of many different things. It can be the dates of a file, the author of a document, the number of times a document was edited, or the amount of time a document was worked on. This is just a small portion of metadata items available. Between file system metadata and application (internal) metadata, the list of items is quite large and diverse. The one common thing about metadata when reviewed by a forensic examiner is that it needs to be looked at carefully and validated. That means examining not only the metadata itself, but all other factors associated with it or. A date on a file is only a factual piece of information without confirmation from another source how that date came to be. The conclusions of the Defendant's expert, Stroz Friedberg, relating to the e-mails on the floppy diskettes are based heavily on solely the metadata from those items. In other words, the conclusions are not validated by a source other than the floppy

diskettes themselves. Microsoft generally discredits the reliability of the "last accessed" timestamp, since it is easily altered by system operations that are not directly user-initiated. Stroz Friedberg themselves have published opinions with the very same conclusion of unreliability stating that "metadata are generally only as accurate as the underlying computer clock time."

9. On Thursday, March 31, 2011, I received 41 floppy disks for review. On Friday, April 1, 2011, I created forensically sound, bit by bit, images of each for analysis.

10. Following the creation of the forensic copies, I performed an initial review of the diskettes and determined that the first 2 were relevant to this matter. I further analyzed the 2 relevant disks to determine the dates and times that various documents on those disks were created.

11. In addition, I analyzed those disks specifically examining them for the following forensically relevant items:

    a. File Allocation Tables (FAT 12)

        i. The File allocation Table is the area of the drive that contains the name, date and location of files on the floppy disk (similar to the table of contents of a book). This is reviewed to compare the contents of the actual files that exist to the names in the FAT for discrepancies. It is also reviewed to determine if any residual information exists indicating duplicate files and or the names of previously deleted files that might be of interest. In this case nothing was located that would indicate fraud.

b. File Dates/Times (Created, Modified Accessed)

   i. The File dates/times are the actual dates/times on the physical files that reside on the floppy disk. These are compared to any internal dates found within the document content themselves to determine if there are any discrepancies. This is used to determine if the content matches the timeframe that the files were created and/or edited. In this case, no discrepancies existed that would indicate fraud.

c. Metadata Dates/Times (Created, Modified, Accessed, Printed)

   i. Like the file dates/time, Metadata dates/times are internal to the document and do not change if a document is copied from one device to another. They are reviewed and compared to the File Dates/Times as well to determine the sequence of events. In this case nothing was located that would indicate fraud.

d. Total Edited Time Metadata Field

   i. This field is part of the internal Metadata of the document and is updated by the Word Processing program that is used to create/edit the document. The field was reviewed to determine the actual time spent editing the content. In this case, the content of the documents was large compared to the logged editing time which is consistent with the pasting of data from the clipboard instead of typing or manually editing the content.

e. All Other Metadata fields

i. Any additional fields that contain data are reviewed for additional information related to the origin of document and/or the machine created on. In this case additional information on other computers, users and companies was located, but nothing was found indicating fraud.

f. Fonts Used

i. The font types are reviewed and compared to the fonts available at the time of the create/modify date of the document. This is done to determine if the document was created at a later date and the actual file and metadata dates were false. In this case all fonts were correct and nothing indicated any signs of fraud.

g. Allocated Space

i. The allocated space is the space that is taken up on the floppy disk from existing files. This is reviewed to determine what parts of the actual floppy disk the data resides on as well as to determine if any hidden or encrypted data exists. In this case nothing was located to indicate any fraud.

h. Unallocated Space

i. The unallocated space is the space that may contain data from previously deleted files. It is examined to review deleted data and to perform keyword searches for the content of deleted files. This is also done to look for any forensic artifacts of a file wiping process or to locate relevant data for comparison. In this case nothing was found that would indicate any fraud.

i. Slack Space

  i. The Slack Space is similar to the unallocated space but is the leftover data from another file that is at the end of an existing file. This is similar to a 2 hour movie on a VCR tape that was overwritten by a 1 hour movie. The first hour of the tape is the new movie but the last hour is the leftover last half of the old movie. This is examined to look for pieces of deleted data to compare to the actual files on the floppy disk to uncover evidence of file versions/editing. In this case, nothing was found to indicate that.

j. Temporary Files

  i. The temporary files are those that are created during the editing/printing of a document. These are then normally deleted after the document is saved or printed. These were reviewed, similar to the remnants of the slack space, to look for evidence of versions and/or editing. In this case, nothing was found to indicate other edited versions of any document relevant to fraud.

k. Carved Files

  i. The carved files are the files/remnants that were deleted on the floppy disk but could be recovered. These were reviewed like the Slack Space and Temporary Files for evidence of file versions and editing. In this case, nothing was found to indicate fraud.

l. Carved Folders

  i. Carved folders are folders that were once deleted but could be recovered similar to the carved files. Recovering a folder could uncover evidence of the actual files that once existed in them for comparison like the other processes. In this case, nothing was found to indicate fraud.

m. File Header Information

  i. The file header information is the beginning of a file that is unique and determines the type of document (Word 97, Rich Text, etc). These were compared to the versions of software that existed on the date/time the document was created. This is done to determine if the file was created with a program that did not exist at that time indicating fraud. In this case, all file headers matched the available versions of the programs at that time so nothing was found to indicate fraud.

n. File Comparisons for changes

  i. I compared files with the same and/or similar names to determine if they were exact. This was done to determine if there were multiple versions of the files or slightly modified versions that would indicate manipulation. In this case nothing was found to indicate fraud.

o. Versions of Programs/Documents (Word 97, Word 2002, Word 6.0, Microsoft RTF, Works 5.0)

  i. Similar to comparing the File Header Information, the versions of the programs indicated by the headers were compared to make sure they did indeed exist at the date/time of the file creation. The programs matched the header information, so in this case nothing was found to indicate fraud.

p. OLE Streams (Individual Components of Documents)

i. The OLE Streams are individual parts of a file/document within the file itself. These were reviewed to compare the types of OLE that existed at the time and to match them to the programs used. In this case, nothing was found to indicate fraud.

q. 0 Length Files (Remnants of deleted files)

i. The 0 Length Files are names of deleted files that were leftover in the File Allocation Table. These items are individually carved to recover any dates and/or information for comparison. In this case, nothing was found to indicate fraud.

r. Pasted E-Mail header contents

i. I compared the portions of the pasted e-mails that contained actual e-mail header information. This would be the underlying information that the e-mail servers would use to actually deliver the e-mail. This was compared to determine if the format and information pasted, matched a true e-mail header format. In this case, they appear to be formatted properly and nothing was found to indicate fraud.

s. RTF Specification Versions and Dates

i. The RTF Specification is the blueprint of the Rich Text Format files that were located on the floppy disks. I reviewed the actual versions of the file format that existed at the time the files were created. This was done similar to comparison to the versions of the software used to determine if the physical structure of the file matched the specification out at the time. In this case, nothing was found to indicate fraud.

t. DOC Binary File Format Specification Versions and Dates

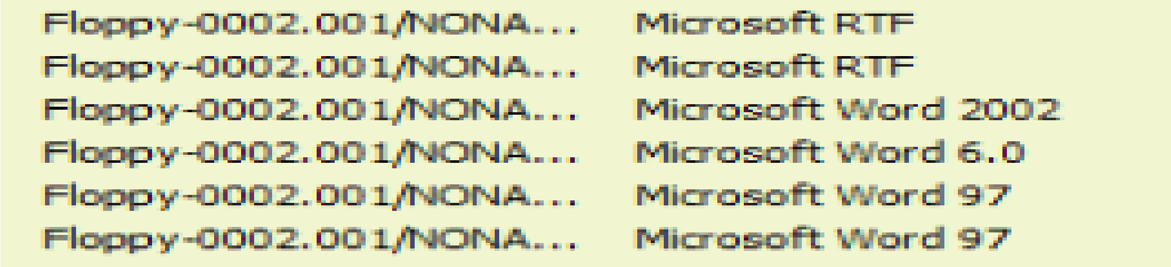
i. Similar to the RTF Specification, one exists for the DOC files (Microsoft Word). This was reviewed and compared to the existing files on the floppy disks and in this case, nothing was found to indicate fraud.

12. The documents containing the e-mail messages are on removable media (floppy diskettes). They are not uniquely tied to any particular machine or environment. These removable devices can be put into any computer that has the proper drive and operating system to read them. The media does not contain an internal clock, nor does it have an operating system installed that is controlling/identifying any date or time attributes. Stating conclusions based solely on the floppy media, without ruling out all other possibilities, simply can't be done. Unless the actual machine / software related to the individual documents can be examined, the fact that anomalies exist do not indicate fraud or backdating.

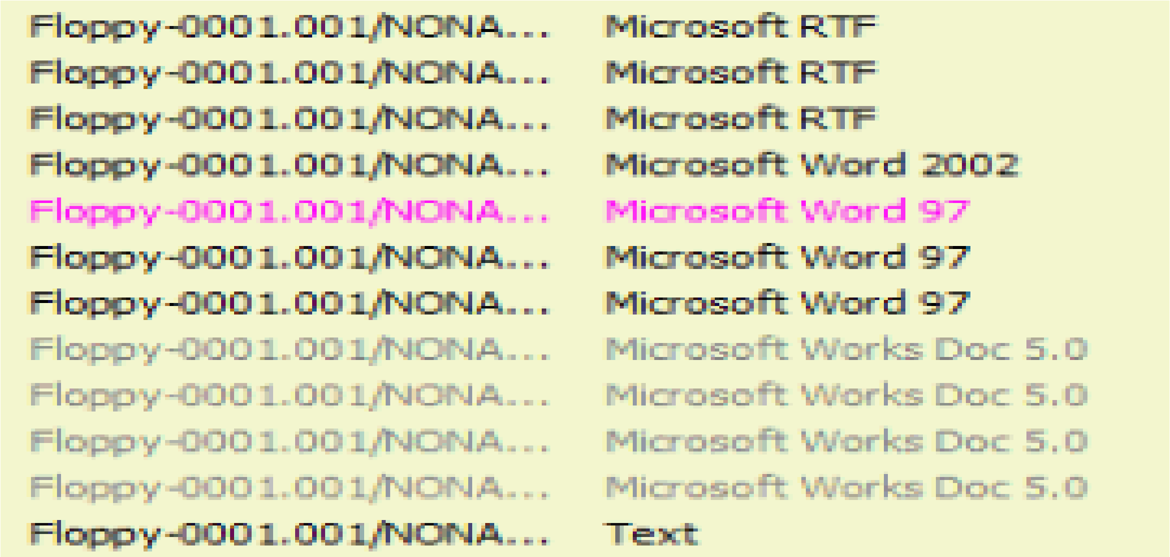
13. The individual contents of the documents are simply text. The items do contain formatting and/or inconsistencies. The fact that an inconsistency

exists in standard text inside of a word processing document is not an indication of fraud. The floppy diskettes contained a number of files that were created/modified using different versions/types of word processors, computers and users based on the metadata. Word Processing programs contain auto-formatting and auto-correct options. These options can change words, add spaces, etc. Without associating the individual documents to a specific computer, word processing program and the settings at that particular time, it cannot be stated as an indication of backdating and/or fraud.

14. As stated previously, all of the different word processing software products and versions were identified based on the signature analysis of data files via the forensic software (see below). This process is common in an attempt to determine fraudulent activity. If a document was created or edited with a product or version of software that was not commercially available at the time, it creates an impossible situation and is a clear indication of fraud. In examining all of the data on the floppy diskettes in question, all products and versions were identified as commercially available during the 2003/2004 time period.



| | |
|---|---|
| Floppy-0002.001/NONA... | Microsoft RTF |
| Floppy-0002.001/NONA... | Microsoft RTF |
| Floppy-0002.001/NONA... | Microsoft Word 2002 |
| Floppy-0002.001/NONA... | Microsoft Word 6.0 |
| Floppy-0002.001/NONA... | Microsoft Word 97 |
| Floppy-0002.001/NONA... | Microsoft Word 97 |



| | |
|---|---|
| Floppy-0001.001/NONA... | Microsoft RTF |
| Floppy-0001.001/NONA... | Microsoft RTF |
| Floppy-0001.001/NONA... | Microsoft RTF |
| Floppy-0001.001/NONA... | Microsoft Word 2002 |
| Floppy-0001.001/NONA... | Microsoft Word 97 |
| Floppy-0001.001/NONA... | Microsoft Word 97 |
| Floppy-0001.001/NONA... | Microsoft Word 97 |
| Floppy-0001.001/NONA... | Microsoft Works Doc 5.0 |
| Floppy-0001.001/NONA... | Microsoft Works Doc 5.0 |
| Floppy-0001.001/NONA... | Microsoft Works Doc 5.0 |
| Floppy-0001.001/NONA... | Microsoft Works Doc 5.0 |
| Floppy-0001.001/NONA... | Text |

15. Different machines contain different versions of Windows, different versions/types of Web Browsers, different word processing programs and different settings. The floppy disks do not contain an operating system and thus the lack of forensic artifacts that can identify most of these factors. This is similar to a DNA test where they can neither confirm nor deny. The word processing program and version can be identified based on the signature of the actual file, but the settings for that particular installation will not be found on the floppy disk due to it being removable media.

16. Page 24 of the Stroz report discusses a particular file named Mark emails July 04.doc. It is clear that there are five forensic artifacts (entries) relating to this file. The report shows an active file and 2 deleted files. The deleted files show a date earlier than the active one with the same name. This was immediately identified as backdating but it was never taken into consideration that the files with a create date of 10/21/2003 could have been another file with a different name and that was just used and renamed. If an original file was created on

10/21/2003 and called e-mail.doc and was then later renamed as Mark emails July 04.doc, it would still have the same create date. The fact still remains that these floppies were in multiple machines and the machines are unavailable to perform a forensic analysis to determine if the clock was in fact working properly. A clock being inaccurate does not mean it was set that way intentionally by a user. Without having possession of those machines to examine, backdating cannot be argued as an absolute reason for an anomaly

17. Page 25 of the Stroz report states that the file “Mark harvard emails up to Dec.doc” has been backdated. This is similar to the argument made for the “Mark harvard emails up to Dec.doc” file. The deleted file forensic artifacts do not contain any text, therefore it can’t be stated that any of the ones last written on 10/21/2003 actually contained any e-mail that was past that date. For example, a user who creates a file on January 1st, 2003 can name the file “All work through December 2003". Even though the actual file at that time does not contain any information for dates/times in the future, it does not indicate backdating or fraud. This is simply work in progress.

18. Page 26 of the Stroz report states an inconsistency with the amount of space available on the floppy disk in relation with the activity. Once again the fact remains that this is a removable device. The dates/times of file activity are directly related to the machine that the file was created/edited/modified on. Without that forensic connection we cannot state a true time line of events.

19. Page 27 of the Stroz report mentions the fact that the e-mails contain wrong

time zone stamps. This again is simply text inside a word processing document. The text does not have any direct connection with an actual clock or setting. Due to the fact that these e-mail messages are not in their native file format, the e-mail header can't be examined to find the actual Coordinated Universal Time (UTC) stamp of the e-mail and determine the proper offset.

20. Page 29 of the Stroz report mentions the inconsistency in spaces within the header. Similar to the time zone issue mentioned in the previous paragraph, we are dealing with text inside a word processing document. Without having the actual environment that the documents were created in, other possibilities for these anomalies cannot be ruled out

21. Page 31 of the Stroz report mentions both an inconsistency in the abbreviations of the day and also an additional space in the e-mail address. These again fall into the same argument of the time zone and spaces. Without having the actual computer, word processor, clock and program settings, authenticity cannot be discredited.

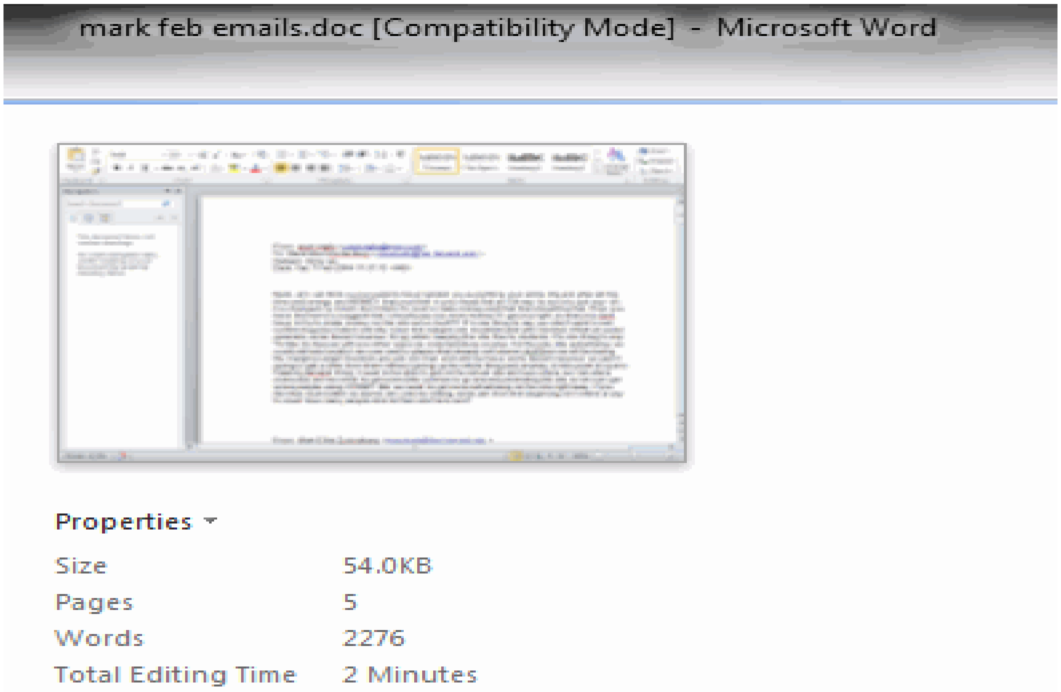
22. Page 33 of the Stroz report mentions that the fact that a document has a created date that is later than the last written or last accessed date is not an indication that backdating occurred. The file could have been copied from one form of media to another. If a file is on a computer and was created, modified and accessed on a particular date (1/1/2001) and then on a later date the file is copied to another source (floppy disk) the create date on the file will change to the date of the copy. Once this file is on the floppy disk, it is now once again

not tied to any particular computer, operating system and internal clock. If this file was then opened on another computer and that clock was not accurate, it would simply modify the access date

23. What is not taken into consideration is the edited time of each of these documents. The total editing time is 2 minutes on each document that contains the relevant e-mail messages. This minimum editing time is more consistent with a copy/paste function than individual typing/editing of a document due to the amount of text.

The following is a comparison of the number of words vs. the total editing time based on the internal metadata:

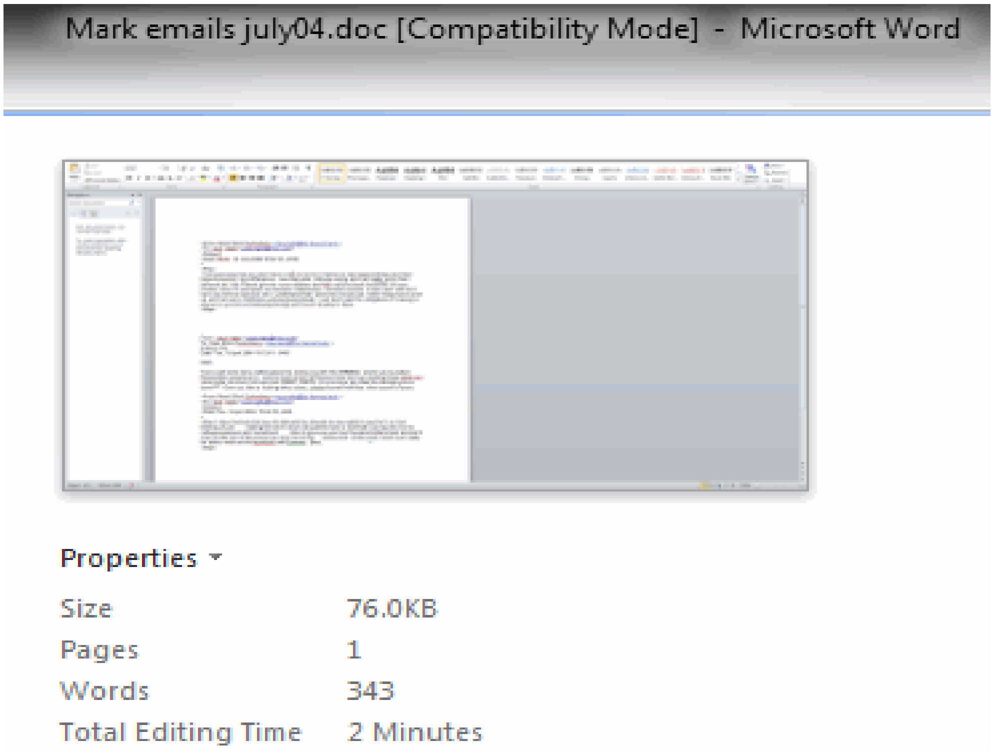
| File Name | Words | Total Editing Time | Words per Minute |
|---|---|---|---|
| mark feb emails.doc | 2276 | 2 minutes | 1,138 |
| Mark emails july04.doc | 343 | 2 minutes | 171.5 |
| Mark harvard emails up to Dec.doc | 1528 | 3 minutes | 764 |



mark feb emails.doc [Compatibility Mode] - Microsoft Word

Properties ▾

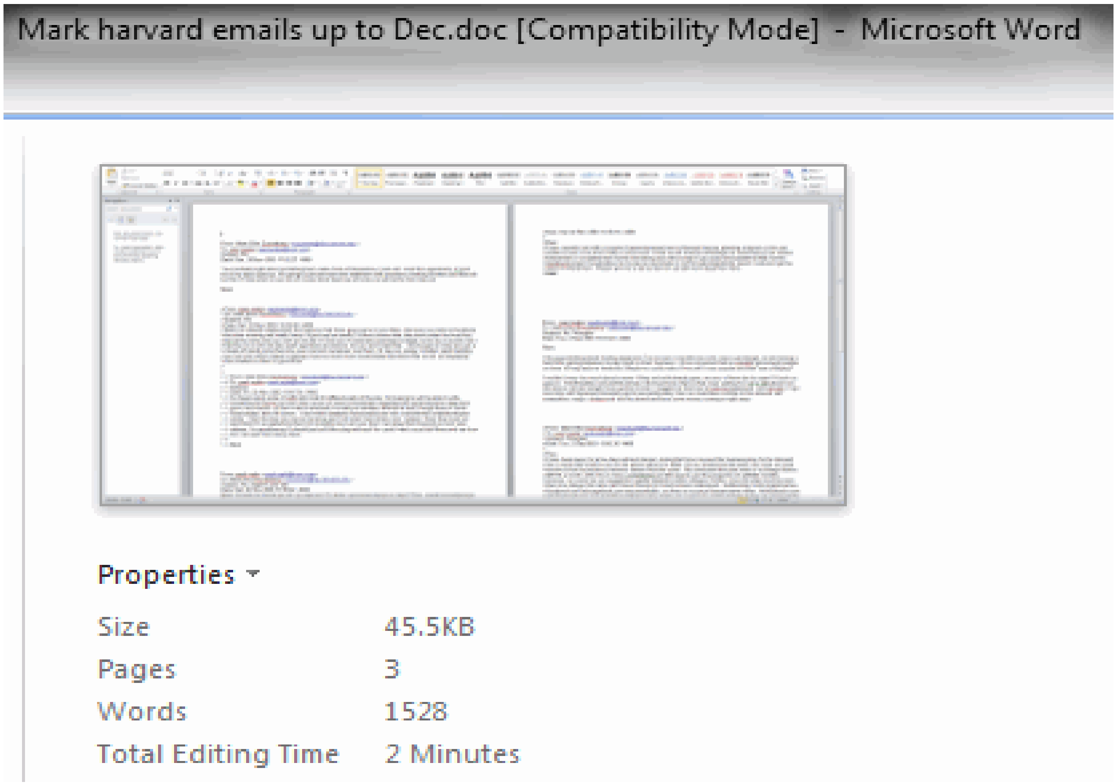
Size 54.0KB
Pages 5
Words 2276
Total Editing Time 2 Minutes



Mark emails july04.doc [Compatibility Mode] - Microsoft Word

Properties

| | |
|---|---|
| Size | 76.0KB |
| Pages | 1 |
| Words | 343 |
| Total Editing Time | 2 Minutes |



Mark harvard emails up to Dec.doc [Compatibility Mode] - Microsoft Word

Properties

| | |
|---|---|
| Size | 45.5KB |
| Pages | 3 |
| Words | 1528 |
| Total Editing Time | 2 Minutes |

Even the smallest file would require a high level typing skill if the contents of were typed manually. The others would be humanly impossible.

24. The floppy disk dates, times, computers, users, time zones, metadata, etc. only show a limited scope based solely on what forensic artifacts are retrieved from them alone. The anomalies found are not conclusive of fraud/back dating on their own. When the results do not include many unknown factors (the computers used, the settings, the versions, etc.) it is simply just an opinion and can neither be confirmed nor denied.

I hereby declare under penalty of perjury and pursuant to 28 U.S.C. 1746 and under the laws of the United States that the following is true and correct:

DATED: June 4, 2012.

Jerry R Grant

Declarant – Jerry Grant