

**STATE OF ARIZONA  
OFFICE OF THE ATTORNEY GENERAL  
SPECIAL INVESTIGATIONS SECTION  
REPORT**

**DATE WRITTEN BY AGENT:** 04/07/2015

**LF NUMBER:** P-2010-0800  
PHX-#4401180

**CASE NAME:** Sorensen, Charles

**REPORT TYPE:** Supplemental RPT-Digital Evidence Examination

**AGENT:** F. Griffiths

**SUPERVISOR:** M. Edwards

**PAGE 1 OF 14 PAGE(S)**

---

**CHAIN OF CUSTODY**

Item Number(s): P-2010-0800-010  
Description: Copy of Digital Image "redacbackup.e01"  
Location Secured: Government Computer SA405-PC D:\P002-2010-0800\Case\Sorensen  
  
Date Received: 03/12/2015  
Received From: Kevin Heade ext. 3-0920  
Address: 602 W. Jackson Street 5th Floor  
Phone: (602) 506-7711  
Email: HeadeK@mail.maricopa.gov  
Examiner: F. Griffiths #405  
Examine Phone: (602) 542-7920  
Examiner Email: Frank.Griffitts@azag.gov

**AUTHORITY TO SEARCH**

At the request of Assistant Attorney General T. Campagnolo, I retrieved a copy of the image file in the custody of the Maricopa County Public Defender's Office in the possession of Kevin Heade. Authority to search was consented between counsel for the defense and counsel for the prosecution.

**ITEM DESCRIPTIONS**

Removable Media Make: Seagate  
Removable Media Model: Expansion SN:NA494RFT  
Removable Media Capacity: 500 GB

## PHOTOS OF CONSOLE/DEVICE

The following photographs were taken during the initial examination.



## ACQUISITION

Utility/Application: FTK Imager  
Version: 3.1.1  
Type of Acquisition: Other Media Image  
Acquisition Time: 03/12/2015 18:24 hours  
Hash Verification: Included Below

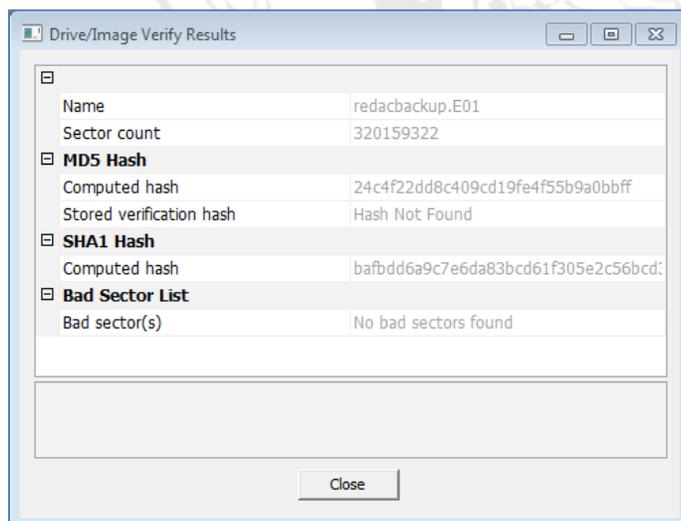
For most data acquisitions, a log of the process is generated by the forensic utility. This log typically displays the time and date of the extraction process, e.g., a summary of data extracted, device information, and, it also may include a hash verification report. Hash verification is a unique digital fingerprint of a set of data and is used to certify that the copy is exactly the same as the original evidence. A copy of the log or a screen shot of the summary is included below.

Image source: F:  
Image file name: redacbackup.e01  
Image file size: 163921572864  
Image created on Sunday, August 10, 2014, 4:15:11 PM

Copy method: Direct Sector Copy  
Checksum method: md5  
Checksum source( F: ): 24c4f22dd8c409cd19fe4f55b9a0bbff  
Checksum image ( redacbackup.e01 ): 24c4f22dd8c409cd19fe4f55b9a0bbff

Case: N/A  
Examiner Name: N/A  
Description:  
Location/Place:

This log was provided by the examiner who originally acquired the image from the original storage media. Since I was not provided a copy of the original storage media, I was unable to verify if the image file hash value was consistent with the original storage media.



Data acquisitions follow different processes depending on the type of device from which the data is being extracted. For example, persistent data stored on hard drives are typically acquired by removing power from the console, removing the storage media from the console, and creating an image or a clone of the storage media as a forensic copy. In this case, the storage media was an external hard drive having a forensic copy of the original media already on the media.

I did not make a forensic copy of the provided image, as it was already in a format widely accepted as a forensic copy. I copied the file from the evidence drive to a government hard drive and later transferred the file to a secure government computer. After I copied the file redacbackup.e01 to my government computer, I utilized FTK Imager (version 3.1.1.8) to verify the known hash value of the image. According to FTK Imager, the MD5 hash value for redacbackup.e01 was verified as 24c4f22dd8c409cd19fe4f55b9a0bbff (match).

The acquired image is stored in the following directory on a secure government computer:  
D:\P002-2010-0800 SORENSEN\Case\Sorensen\redacbackup.E01

## **PROCESSING EXTRACTED DATA**

After a forensic copy (an image or a clone) of the device or the data extraction has been made, the copy can be analyzed by an examiner using a forensic software application(s). More than one forensic software application may be used to index a single piece of evidence with various automated processes such as identifying the operating and/or file systems, indexing files on the system, analyzing metadata, and recovering deleted files, to name a just a few. All forensic applications used in this examination are widely accepted utilities within the digital forensic community. All of the processes utilized have been tested and verified for basic functionality.

On 03/13/2015 at 10:48 hours, I utilized FTK (version 3.0.4.2138) to index the acquired evidence stored as redacbackup.e01. I made a copy of the indexed case file available to the case agent along with a copy of the utility application required to view the case file. In this case, the viewer application is FTK. I saved the indexed case file of the evidence on a secure government computer in the following directory:

F:\P002-2010-0800\ on government media

## **SUMMARY OF RECOVERED ITEMS**

The following items represent an excerpt of data recovered during the initial indexing process, and is provided to the case agent for convenience. Additional data may exist on the examined evidence in the form of files, partial files, metadata, and operating system or file system artifacts, or application artifacts. These additional items may require more in-depth forensic analysis which can be performed at a later date at the request of the case agent.

- (1) \$MFT\_peoriaoverview (the entry for peoriaoverview.doc carved from the \$MFT)
- (2) \$MFT\_peoriaoverview(1) (the entry for peoriaoverview(1).doc carved from the \$MFT)
- (3) peoriaoverview.doc (a file in question found in the directory specified)
- (4) peoriaoverview(1).doc (a file in question found in the directory specified)
- (5) coffman1.jpg through coffman7.jpg (scans of a promissory note related to Magic Ranch)

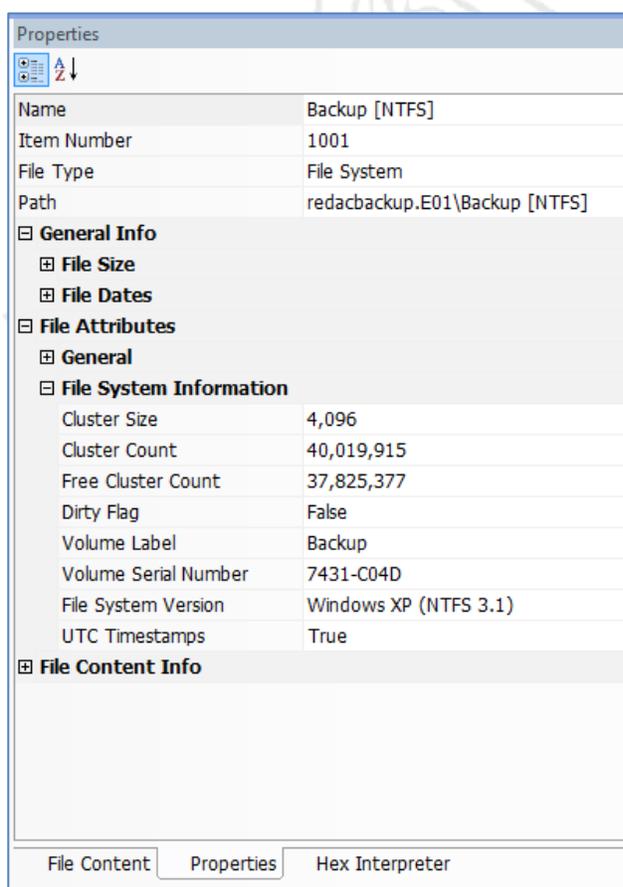
## **OPERATING SYSTEM**

This device did not appear to have an operating system. Rather, the original device appeared to be an unknown storage media device formatted with the NTFS file system. Possible scenarios include, but are not limited to, being just one of multiple partitions or volumes on a

suspect hard drive, being a secondary or tertiary hard drive in a suspect computer, or the drive being an external drive attached to an unknown suspect computer at some previous time.

## PARTITION INFORMATION

During the course of this examination, I noted the following allocated partitions and unallocated areas on the image of this volume:



The name of the partition was identified as "Backup". The file system version was NTFS 3.1.

A cluster is made up of sectors of 512 bytes. The cluster size on this partition was 4,096 bytes or 8 sectors.

The partition "Backup" contained over 40 million clusters or 40 million times 4,096 bytes, which is equal to 163.9 GB.

The Volume Serial Number was identified as 7431-C04D.

This device did not have an operating system, and as such, no time zone is intrinsically associated with this file system. Additionally, one would not expect to find any Windows registry artifacts typically associated with an examination of a volume that did not have a Windows operating system installed. That is true for this examination.

## USER ACCOUNTS

User accounts are typically associated with operating systems rather than file systems. As such, no user accounts were identified as being intrinsically associated with this file system. However, there were a number of user created directories in the root of the file system, and one of the directories (file folders) was named "Chuck."

## PROGRAMS AND APPLICATIONS

During the course of this examination, I recovered no notable program files or applications.

## NOTABLE DOCUMENT FILES

During the course of the examination, I recovered the following notable document files: (1) peoriaoverview.doc and (2) peoriaoverview(1).doc.

As a side note, when a file is copied and pasted into the same directory as the original file, the default naming convention for Windows operating system is to change the filename from filename.ext to filename(1).ext where the number within the parenthesis designates the copied file and the order in which it was copied. Another possibility is that the user created a different file but attempted to save the new file into the same directory with the same name as a file already existing in that directory. Since the data and hash values of both files are identical, one may draw the reasonable inference that peoriaoverview(1).doc is a file that was copied from peoriaoverview.doc and pasted into the same directory.

As such, the file peoriaoverview.doc is referred to as the ORIGINAL FILE, and the file peoriaoverview(1).doc is referred to as the COPIED FILE.

## NOTABLE GRAPHIC IMAGE FILES AND MULTIMEDIA FILES

During the course of the examination, FTK reported that there were over 20,000 graphic image files. I recovered a number of scanned items from the directory identified by the defense, some of which were named "coffman1.jpg" through "coffman7.jpg." These files appeared to be scans or electronic copies of promissory note pages between the suspect and a subject identified as Coffman.

During the course of the examination, FTK reported that there were at least 118 multimedia files on storage media. I did not recover any notable video and/or multimedia files during this examination.

## NOTABLE EMAIL FILES AND ARTIFACTS

During the course of the examination, FTK recovered and I bookmarked over 2,900 calendar appointments. FTK recovered and I bookmarked over 5,900 address book contacts. FTK recovered and I bookmarked over 8,400 email messages and related artifacts. FTK also recovered and I bookmarked 10 Outlook PST files. I did not review the content of any of the bookmarked items. Rather, those items have been exported in a report format to allow the case agent/investigator to review them at a later date.

During the course of the examination, FTK recovered and I bookmarked 29 items identified as "Text Internet Email." I did not review the bookmarked items. Like the email files listed above, those items have been bookmarked and exported in a report format for later review.

### **TIME AND DATE STAMP METADATA ANALYSIS**

Time and date stamps are created in various ways, including (1) within entries in the file system index (a file called \$MFT in the NTFS file system) and (2) within the metadata of the file itself (contained in a data stream of a Microsoft Word document, for example).

The time and date stamp metadata analysis in this report is limited to two files which include (1) peoriaoverview.doc and (2) peoriaoverview(1).doc. For all practical intents and purposes, the data content of these two files is identical with identical MD5 and SHA1 hash values. The metadata suggests, however, that the original file was *moved to* the volume of which the image was made rather than *created on* that volume. The following metadata evidence explains how this conclusion was derived:

The \$MFT (Master File Table) is an index of all files on a given file system such as the partition identified above as Backup [NTFS]. Typically, four time and date stamp categories are created for every file within the \$MFT. These four date and time stamps are sometimes referred to as MACE times and are explained as follows:

1. Modified Last: the time the file was last changed, whether on the current volume or the time it was last modified on another volume on which it may have resided; this time stamp is created by the file system on which the file resided when modified and reflected in the metadata of the file. Thus, the time modified can actually show a time earlier than the time created if the file was placed on a new volume after it was modified.
2. Accessed Last: the time last accessed generally corresponds to a time the file was created, opened, copied, highlighted, viewed as a thumbnail, or scanned by an anti-virus program.
3. Created: the time the file first appeared on the current file system (the file may have existed previously on another volume with a different file system, but the Time Created metadata represents the time the file first appeared on the current volume).
4. Entry Updated: the time the file entry was last updated in the \$MFT; for example, if the file attributes were changed (read-only, hidden, etc.), if the file was renamed, if the file was copied to, moved to, or deleted from a volume, or opened by an application.

I utilized FTK to extract the \$MFT entry for the file peoriaoverview.doc and for the file peoriaoverview(1).doc. I then copied the four MACE time stamps (displayed as 8-byte hexadecimal values) from the \$MFT entry for each file and pasted that value into the utility

DCode (version 4.02a), which converts the hexadecimal value into a human readable time format. The following screen shots illustrate the time stamps defined above:

### MODIFIED LAST TIME FOR ORIGINAL FILE

The screenshot shows the DCode v4.02a (Build: 9306) application window. The 'Value to Decode' field contains the hexadecimal string /00/BF/D8/CF/24/F2/C5/01. The 'Date & Time' field displays the result: Fri, 25 November 2005 18:00:36 -0700. The 'Decode Format' is set to 'Windows: 64 bit Hex Value - Little Endian'. The background shows a hex dump of a file named 'peoriaoverview.doc' with the corresponding hex value highlighted in blue.

The file peoriaoverview.doc Modified Last Time is shown above as /00/BF/D8/CF/24/F2/C5/01 and has a human readable time of Fri, 25 November 2005 at 6:00pm. In other words, this file was last altered on 11/25/05 on the volume where it was previously stored prior to being placed on this volume on 4/27/06.

### CREATED TIME FOR ORIGINAL FILE

The screenshot shows the DCode v4.02a (Build: 9306) application window. The 'Value to Decode' field contains the hexadecimal string /D0/7D/79/24/6E/6A/C6/01. The 'Date & Time' field displays the result: Thu, 27 April 2006 19:47:51 -0700. The 'Decode Format' is set to 'Windows: 64 bit Hex Value - Little Endian'. The background shows a hex dump of a file named 'peoriaoverview.doc' with the corresponding hex value highlighted in blue.

The file peoriaoverview.doc Created Time is shown above as /D0/7D/79/24/6E/6A/C6/01 and has a human readable time of Thu, 27 April 2006 at 7:47pm, i.e., this file was placed on this volume on 4/27/06.

### ENTRY UPDATED TIME FOR ORIGINAL FILE

The screenshot displays a hex dump on the left and a DCode v4.02a (Build: 9306) window on the right. The hex dump shows the following entry highlighted in blue:

```
0096 C2 F7 8B 40 95 C3 CE 01
```

The DCode window shows the following decoded information:

- Add Bias: UTC -07:00
- Decode Format: Windows: 64 bit Hex Value - Little Endian
- Example: FF03D2315FE1C701
- Value to Decode: C2F78B4095C3CE01
- Date & Time: Mon, 07 October 2013 12:41:44 -0700

The file *peoriaoverview.doc* *Entry Updated Time* is shown above as */C2/F7/8B/40/95/C3/CE/01/* and has a human readable time of Mon, 07 October 2013 at 12:41pm, i.e., the NTFS file system updated the time stamp of this file due to some user activity on 10/07/13, approximately ten minutes before the copy of this file was last accessed.

### ACCESSED LAST TIME FOR ORIGINAL FILE

The screenshot displays a hex dump on the left and a DCode v4.02a (Build: 9306) window on the right. The hex dump shows the following entry highlighted in blue:

```
0096 C2 22 8B 7A 19 F3 54 CF 01
```

The DCode window shows the following decoded information:

- Add Bias: UTC -07:00
- Decode Format: Windows: 64 bit Hex Value - Little Endian
- Example: FF03D2315FE1C701
- Value to Decode: C2228B7A19F354CF01
- Date & Time: Thu, 10 April 2014 12:28:49 -0700

The file *peoriaoverview.doc* *Accessed Last Time* is shown above as */22/8B/7A/19/F3/54/CF/01/* and has a human readable time of Thu, 10 April 2014 at 12:28pm, i.e., this file created, opened, copied, highlighted, viewed as a thumbnail, or scanned by an anti-virus program on 04/10/14 after it was placed here on 05/06/10.

### MODIFIED LAST TIME FOR COPIED FILE

The screenshot displays a hex dump on the left and the DCode v4.02a (Build: 9306) application window on the right. The hex dump highlights the path `/00/BF/D8/CF/24/F2/C5/01` in blue. The DCode window shows the 'Value to Decode' field containing `00BF08CF24F2C501` and the resulting 'Date & Time' as `Fri, 25 November 2005 18:00:36 -0700`. The application also shows 'Add Bias: UTC -07:00' and 'Decode Format: Windows: 64 bit Hex Value - Little Endian'.

The file `peoriaoverview(1).doc` *Modified Last Time* is shown above as `/00/BF/D8/CF/24/F2/C5/01` and has a human readable time of Fri, 25 November 2005 at 6:00pm, i.e., this file was last altered on 11/25/05 on the volume where it was previously stored on prior to being copied to this volume on 4/27/06.

### CREATED TIME FOR COPIED FILE

The screenshot displays a hex dump on the left and the DCode v4.02a (Build: 9306) application window on the right. The hex dump highlights the path `/D0/7D/79/24/6E/6A/C6/01` in blue. The DCode window shows the 'Value to Decode' field containing `D07D79246E6AC601` and the resulting 'Date & Time' as `Thu, 27 April 2006 19:47:51 -0700`. The application also shows 'Add Bias: UTC -07:00' and 'Decode Format: Windows: 64 bit Hex Value - Little Endian'.

The file `peoriaoverview(1).doc` *Created Time* is shown above as `/D0/7D/79/24/6E/6A/C6/01` and has a human readable time of Thu, 27 April 2006 at 7:47pm, i.e., this file first appeared on this volume on 4/27/06.

### ENTRY UPDATED TIME FOR COPIED FILE

The screenshot displays a hex dump on the left and the DCode v4.02a (Build: 9306) interface on the right. The hex dump shows a file entry with a highlighted path: /A816469867EDCA01DEE5EC9796C3CE01. The DCode interface shows the decoded date and time: Thu, 06 May 2010 15:00:52 -0700.

The file *peoriaoverview(1).doc* *Entry Update Time* is shown above as /A8/16/46/98/67/ED/CA/01 and has a human readable time of Thu, 06 May 2010 at 3:00pm. There are a number of explanations for this time stamp update, including the possibility that the file attributes were changed (read-only, hidden, etc.), or the file was renamed, or the file was copied to, moved to, or deleted from a volume, or opened by an application 5/06/2010.

### ACCESSED LAST TIME FOR COPIED FILE

The screenshot displays a hex dump on the left and the DCode v4.02a (Build: 9306) interface on the right. The hex dump shows a file entry with a highlighted path: /DEE5EC9796C3CE01. The DCode interface shows the decoded date and time: Mon, 07 October 2013 12:51:20 -0700.

The file *peoriaoverview(1).doc* *Accessed Last Time* is shown above as /DEE5EC9796C3CE01/ and has a human readable time of Mon, 07 October 2013 at 12:51pm, i.e., this file may have been created, opened, copied, highlighted, or scanned by an anti-virus program on this volume on 10/07/13 after it placed here on 05/06/10.

## **TIMELINE SUMMARY**

11/25/05: Original file and Copied file last modified (allegedly) on an unknown volume (MODIFIED).

4/27/06: Original file and Copied file both created on the imaged volume (CREATED).

05/06/10: Copied file attributes were changed (read-only, hidden, etc.), or the file was renamed, or the file was copied to, moved to, or deleted from a volume, or opened by an application MFT (ENTRY UPDATED).

10/07/13: Original file attributes were changed (read-only, hidden, etc.), or the file was renamed, or the file was copied to, moved to, or deleted from a volume, or opened by an application (ENTRY UPDATED).

10/07/13: Copied file opened, copied, moved, highlighted, or scanned by an anti-virus program (ACCESSED LAST).

4/10/14: Original file was copied, moved, highlighted, or scanned by an anti-virus program (ACCESSED LAST).

8/10/14: The acquisition log provided by the defense's examiner indicates that the hard drive on which the files peoriaoverview.doc and peoriaoverview(1).doc was imaged on 8/10/14.

## **TIME STAMP ANOMALY**

As stated above, the MACE time stamps were originally observed in a hexadecimal (base 16) format. I used DCode to convert the hexadecimal value to human readable format. The hexadecimal format (base 16) can be converted to other formats such as binary (base 2) or decimal (base 10). The decimal (base 10) format is the counting system universally used by humans when counting. Computers, on the other hand, often record and read numeric values in hexadecimal (base 16) or binary (base 2) formats.

A time stamp recorded as a 64 bit hexadecimal string such as /00/BF/D8/CF/24/F2/C5/01 has a human readable time of Fri, 25 November 2005 at 6:00 (36.976000 seconds) pm. If you convert this value from hexadecimal (base 16) to decimal (base 10) you get a value of 127774404369760000. This value represents 100 nanosecond intervals from January 1<sup>st</sup>, 1601, and this is how the NTFS file system records time and date stamps for all files saved on that file system. The program DCode calculates these 100 nanosecond intervals from January 1<sup>st</sup> 1601 in order to determine the current MACE time stamps of a given file (see calculator exhibits below).



This decimal value of 127774404369760000, however, is unique from all of the other MACE time stamps associated with the files peoriaoverview.doc and peoriaoverview(1).doc. The anomaly lies in the fact that the last four place values of the integer are represented by four zeros. It is extremely rare (1 in 10,000) that a file generated or modified by a user would record a time stamp with this value (imagine pumping gas into your car without looking at the dollar value on the pump, stopping the pump at a random moment in time, and having the dollar counter stop on exactly \$100.00).

All of the other MACE values are populated with integers other than zero all the way out to the 100 nanosecond place value, as expected. Only the value in question (MODIFIED LAST TIME) has this uniquely lower time stamp resolution.

One possible explanation for this anomaly is chance. It is possible, however rare (see above), that this time stamp naturally occurred with the last four place values ending in zero.

A second possible explanation for the anomaly is that the time stamp was altered with a program designed to alter time stamps. Most utilities designed to alter time stamps only allow the user to alter the hh:mm:ss and do not have an option to alter fractions of a second. Thus, one would expect the decimal value of this time stamp if altered by a time-stamp-altering program to be 1277744043600000000 (Fri, 25 November 2005 at 6:00 (36 seconds) pm). This resolution is two place values lower than the actual resolution for the time stamp of the examined file.

A third possible explanation for this anomaly is that the user utilized another program designed to read the hexadecimal values of a file (commonly known as a hex-editor) and manually changed the time stamp to /00/BF/D8/CF/24/F2/C5/01.

Without examining the original volume on which the file was created, I cannot make a conclusive statement about which, if any, of the three possibilities actually transpired.

## **CONCLUSION**

The file peoriaoverview.doc was created on an unknown volume. The last time the file was modified (content was changed by a user) prior to placing the file on the volume "Backup" was 11/25/05. However, without reviewing the operating system logs for the volume that created the file, there is no way to determine if the time/date stamp indicated is accurate, is in the correct time zone, or if it has been tampered.

The file peoriaoverview.doc was placed on the volume known as "Backup" on 4/27/06. This time/date stamp is also contingent up on the operating system clock of the system to which this volume was connected.

It is unknown if the original file peoriaoverview.doc (which was created on an unknown volume) was modified after 11/25/05 on the originating volume. The volume on which the file was created would have to be identified and examined forensically to make such a determination.

The file peoriaoverview.doc was altered on the volume known as "Backup" approximately four years later on 05/06/10, effectively updating the \$MFT on that volume.

The time stamp in question has an anomalous value which may be indicative of tampering with the time stamp by the end user.

Without examination of the volume with the operating system, it is inconclusive at this point as to whether or not metadata manipulation occurred on any of the files provided. The defense has not provided the State with that volume.

Upon completion of the initial examination, I copied this report and the FTK bookmarks to disk for review by the case agent. The forensic copy of the image has been retained on a secure government computer as listed above.

End of Supplement