1. In the figure above it shows that you should have checked “Expand Compound Files.” What is a

compound file? [5 points]

ANSWER PROVIDED

A “compound file” is a file comprised of several files. For example, a ZIP file may contain several

other files within it. An email file may contain the original email and some attachments. A

Microsoft OLE file might consist of an Excel spread sheet file that has been cut and pasted into a

Word document.

If you select “Expand Compound Files” within FTK, FTK will extract the files that are within other

files and add them to the case. (p. 284)

2. One of the FTK settings is an “Entropy Test.” What file characteristic can an entropy test

identify? [5 points]

ANSWER PROVIDED

An entropy test can determine if a file is compressed or encrypted. (p. 284)

3. One of the FTK settings is “dtSearch Text Index.” What does this setting accomplish? [5 points]

ANSWER PROVIDED

This setting causes FTK to index every word within the case evidence items. Indexing every

word makes it possible to perform fast word searches. (p. 285-286)

4. One of the FTK settings is to “Create Thumbnails for Videos.” How frequently are thumbnails

created if this setting is used? [5 points]

ANSWER PROVIDED

A thumbnail can be created every “n” number of seconds or every fixed percent of the entire

video. (p. 286)

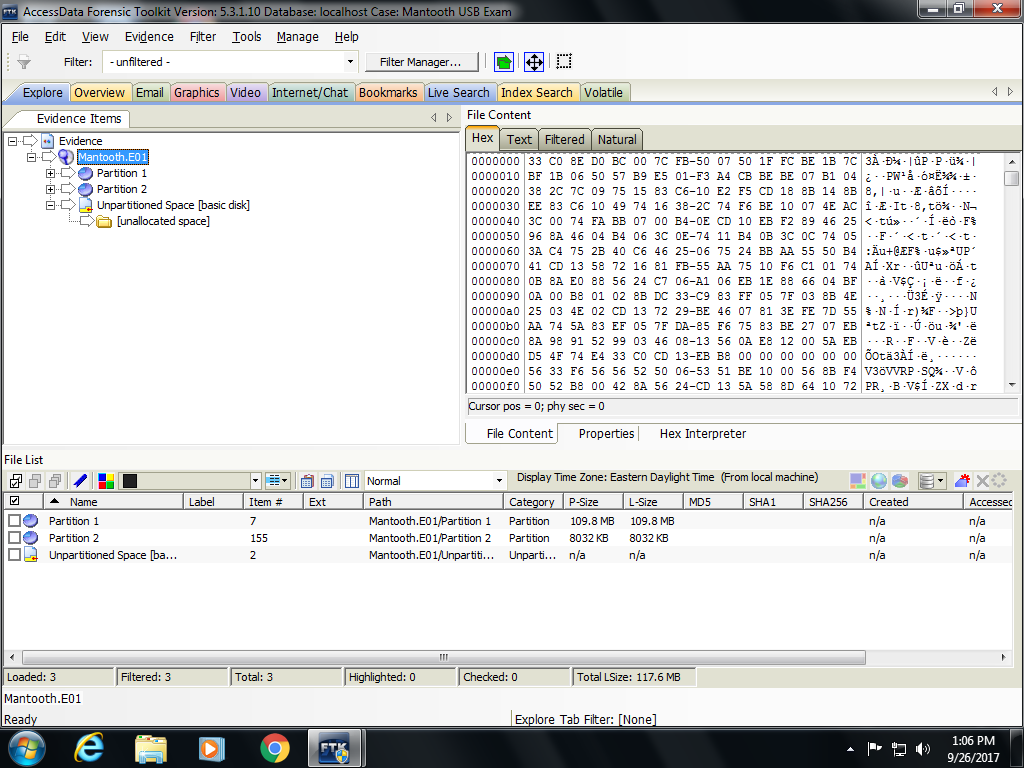
5. Add the Mantooth.E01 image to the case as an evidence item. Set the time-zone setting within

FTK to be “Eastern-Time with Daylight Savings (US – New York).” Process the case.

Looking at the evidence tree, within the “Evidence”\”Mantooth.E01”\”Unpartitioned Space”

there is a folder named “unallocated space.” What is unallocated space (also known as “free

space”)? [5 points]



6. What is “file slack”? [5 points]

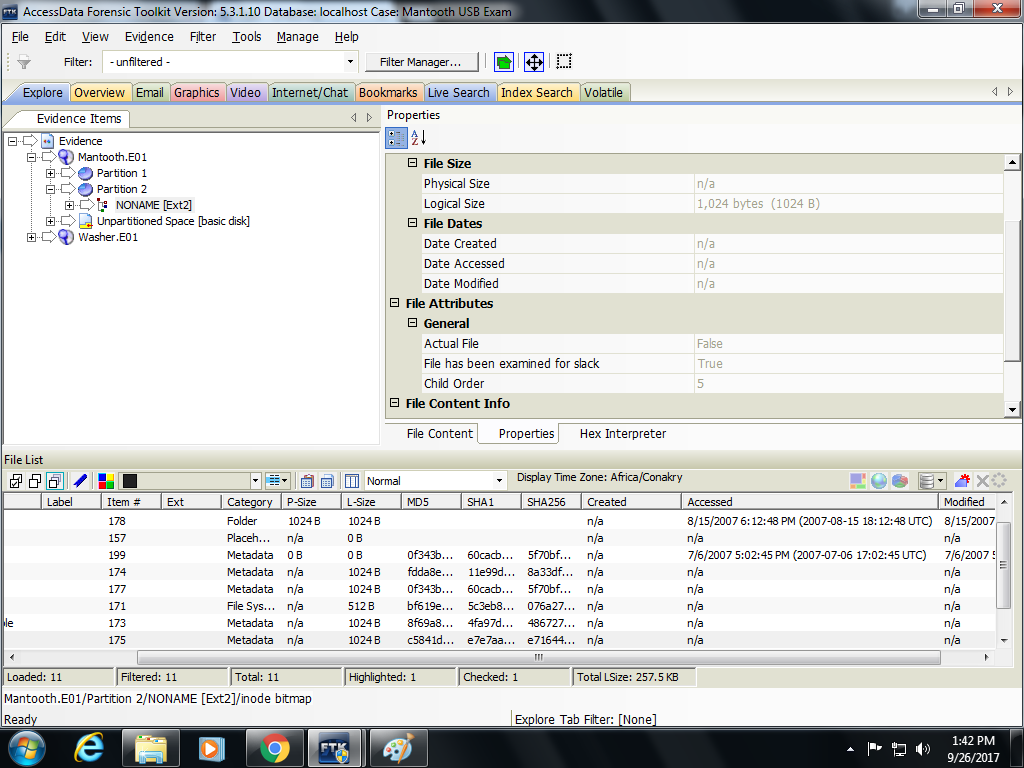
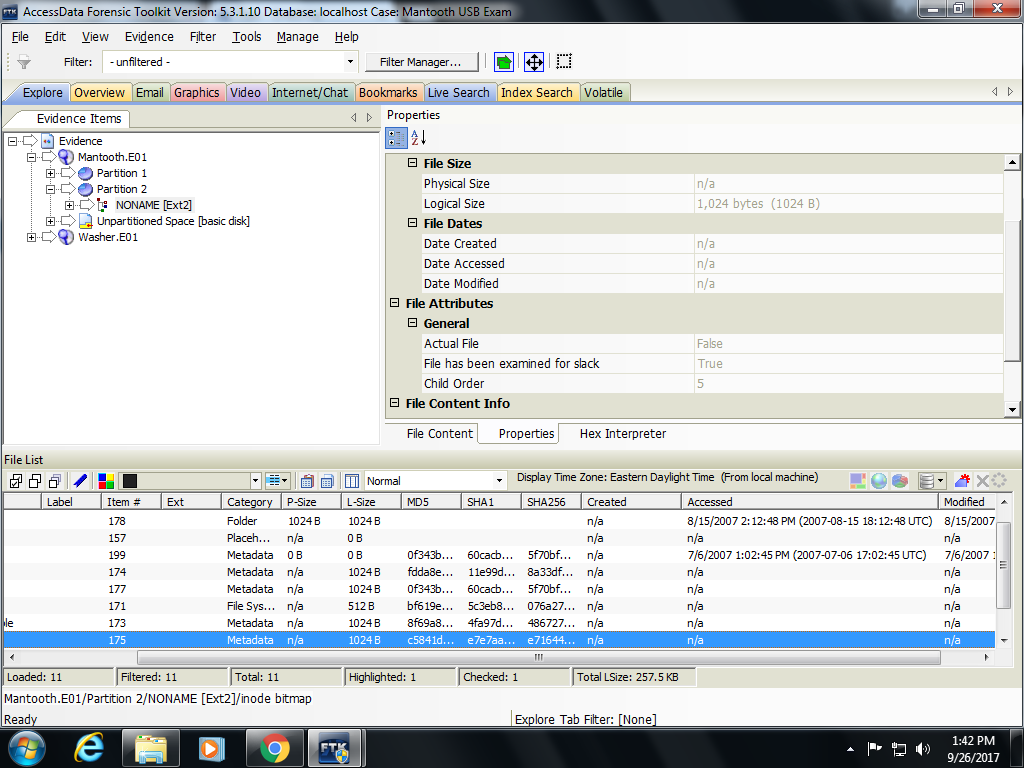
ANSWER PROVIDED

File slack is the memory location that is beyond the logical file but within the area allocated to

the file by the file system. (p. 294)

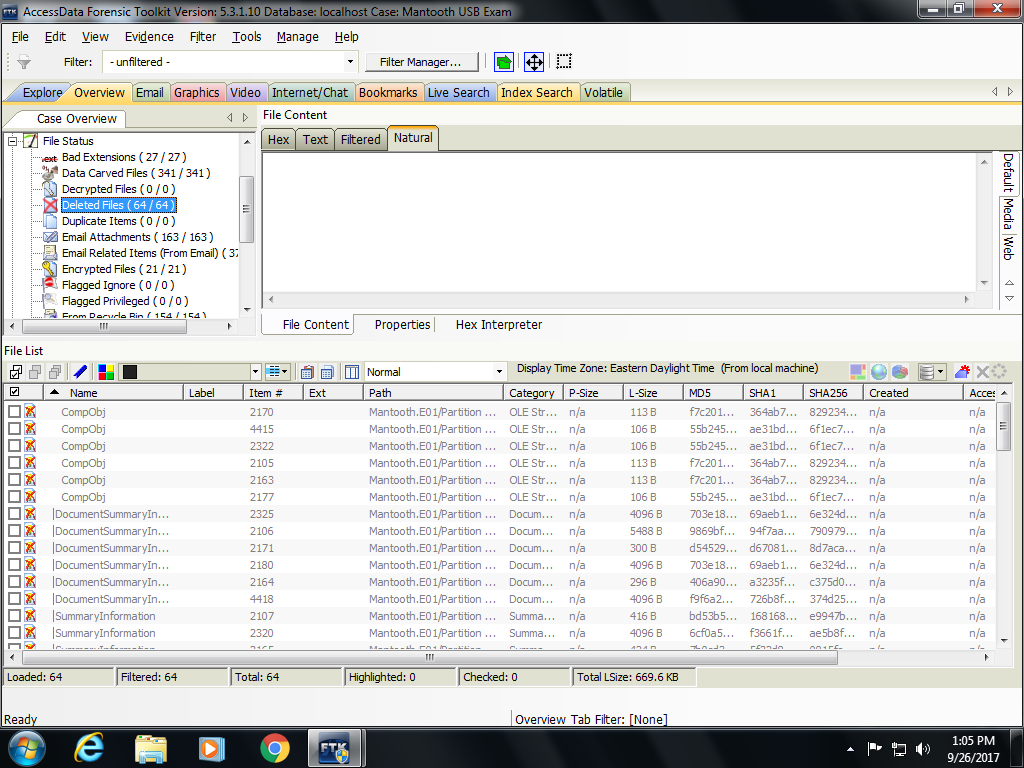
7. What effect does changing the time zone setting on FTK have on how the evidence is presented

to the user? (Provide an example to illustrate what you mean.) [5 points]



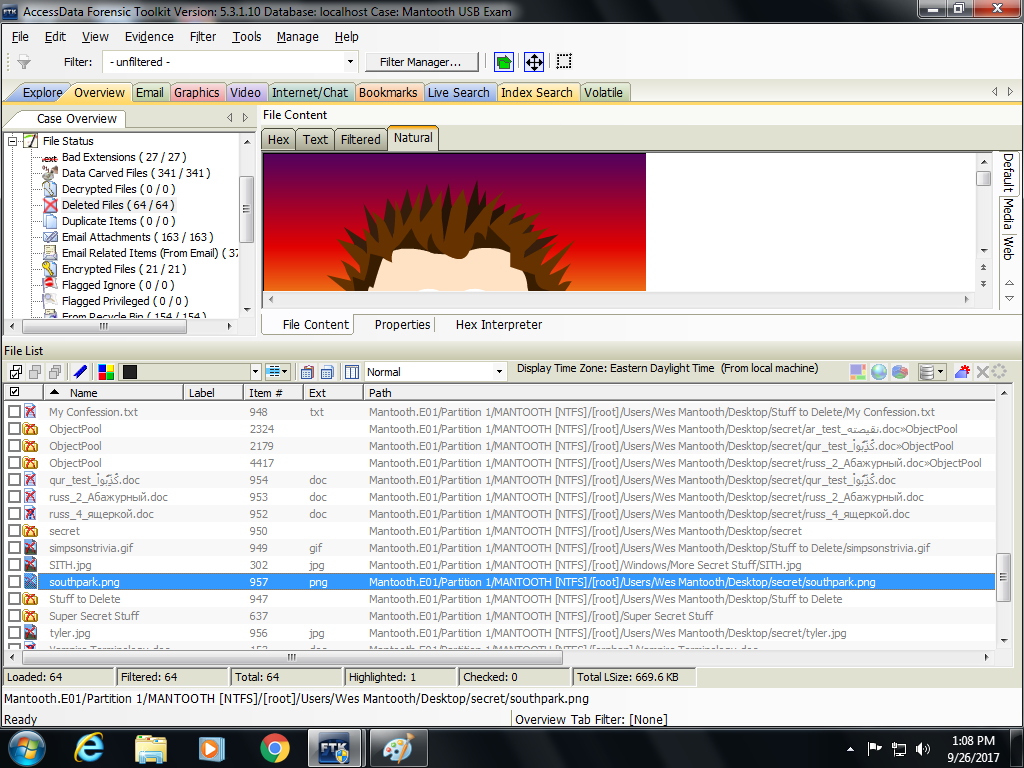
8. Within the “Overview” tab, navigate within the file tree to the “File Status”\”Deleted Files”

container. How many deleted files are there in this container? [5 points]



9. Within the deleted files container there is a fine named “southpark.png”. Where was this file

located within the suspect’s computer before it was deleted? [5 points]



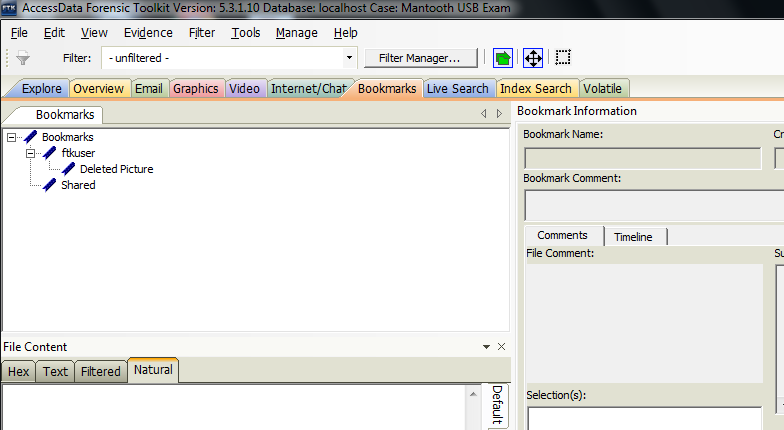
10. Add the “southpark.png” picture to a bookmark named “Deleted Picture.” Navigate to the

“Bookmarks” tab and expand the tree of bookmarks so the “Deleted Picture” bookmark is

visible. Take a ‘print-screen’ of tree of bookmarks and past it into this assignment to show that

you created the bookmark. (Please crop the print-screen so the bookmark tree is clearly visible.)

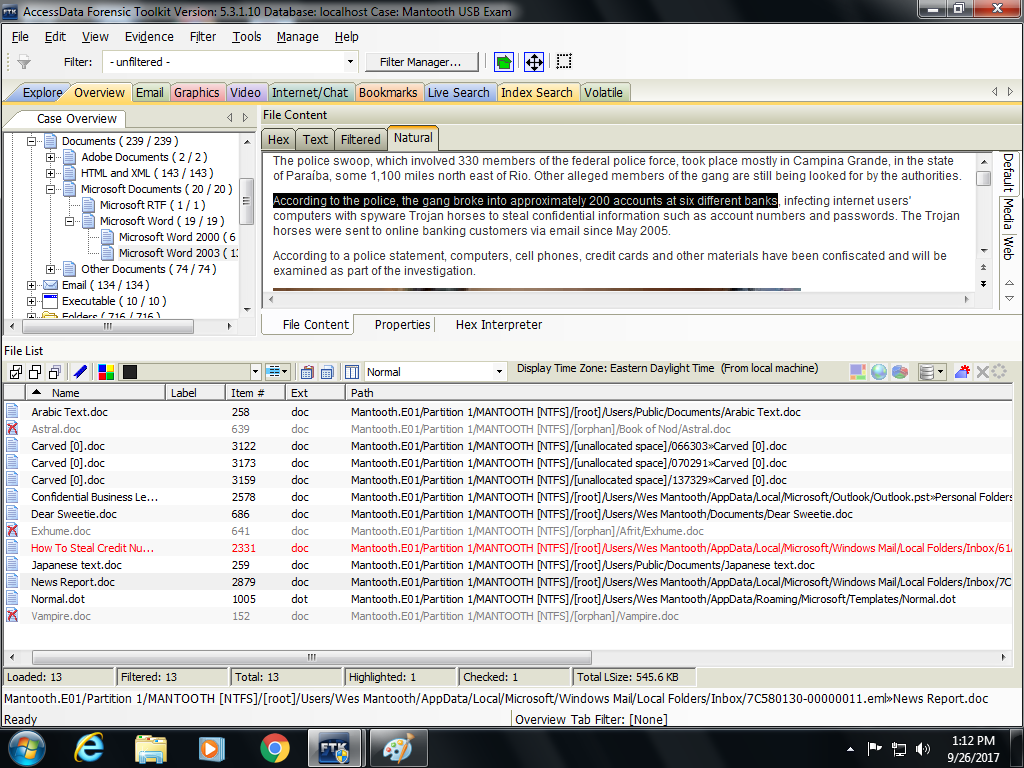
[5 points]



11. Somewhere within the evidence there is a file named “News Report.doc.” Find it. Inspect the

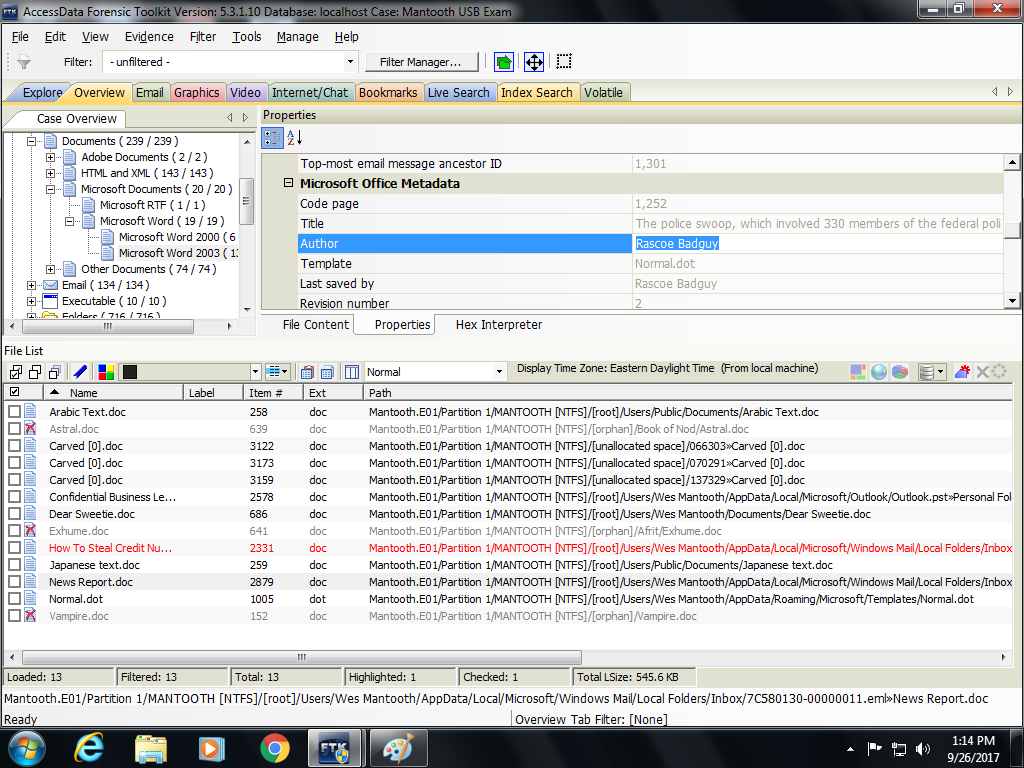
contents of this file and answer the following question.

According to the police, how many accounts did the gang break into? [5 points]



12. According to the metadata associated with the “New Report.doc” file, who is the author of this

document? [5 points]

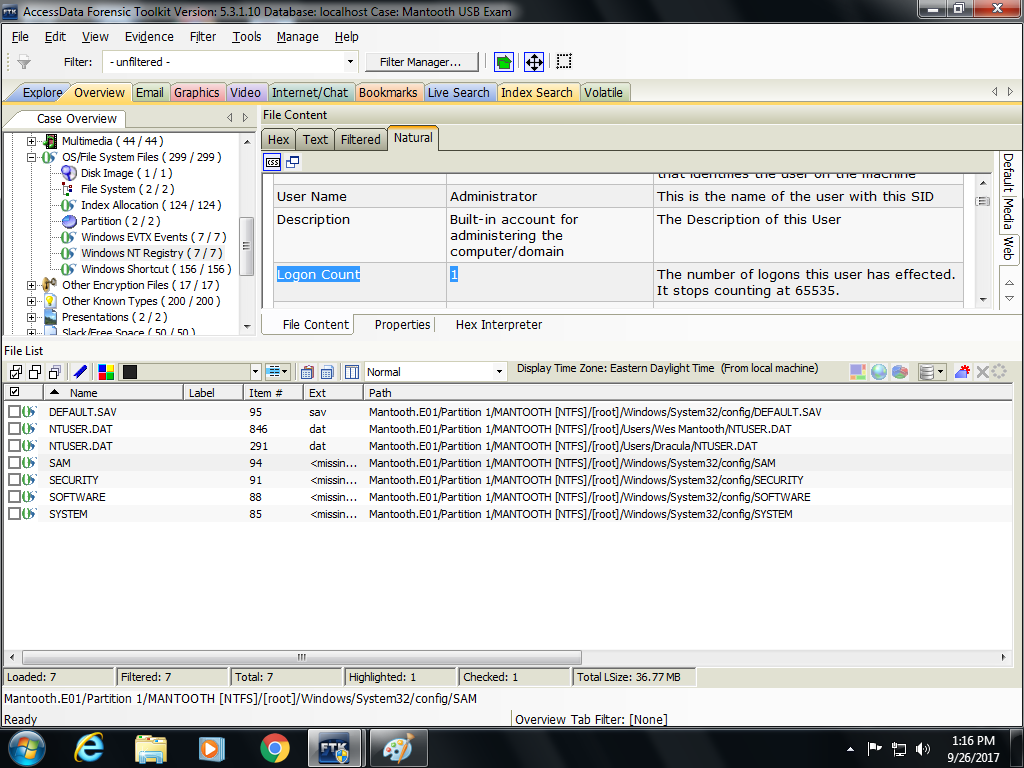


13. Navigate to the “File Category”/ “OS/File System Files”/”Windows NT Registry”. Notice that

some of the same registry information can be seen with FTK as with the Registry Viewer tool.

Select the SAM file for viewing and answer the following question.

How many times has someone logged on with the Administrator account? [5 points]



14. Navigate to the $Recycle.Bin directory and select the SID that ends in “1000”. Notice the files

with names that start with “$I” and “$R”. When Windows Vista (or Win 7) sends a file to the

$Recycle.Bin , the original file gets separated into two files with names that start with “$I” and

“$R”. The rest of the name will match. For example, the file named $R9HZOZ0.jpg should be

matched with the file named $I9HZOZ0.jpg. The file containing the original file always has a

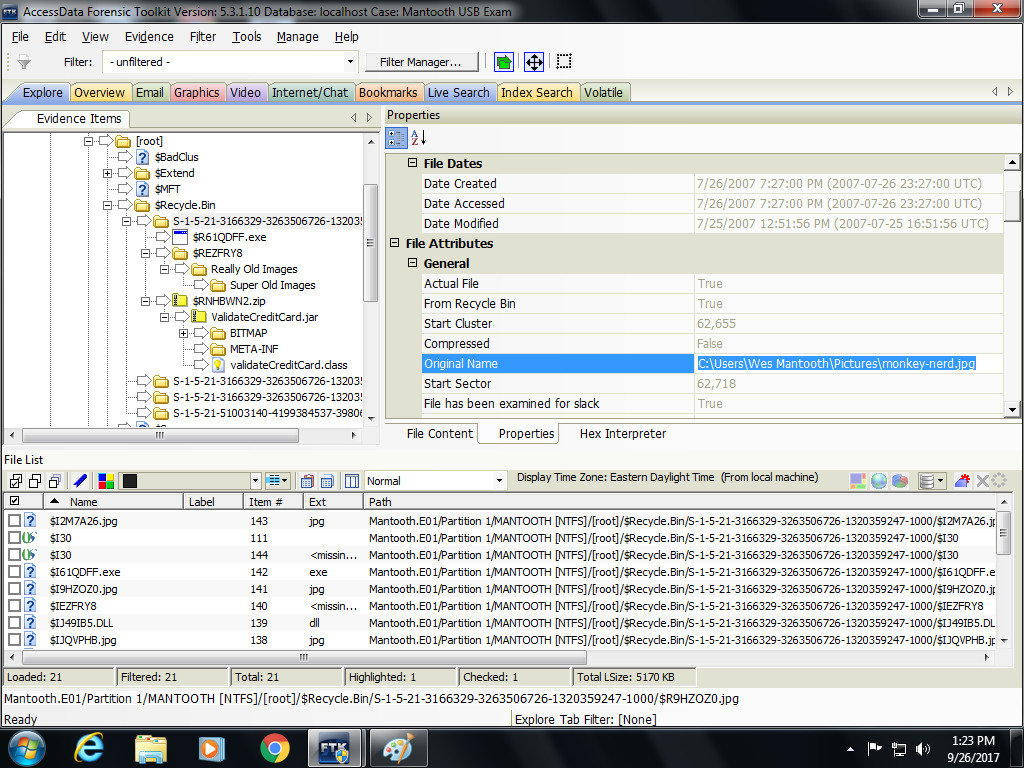
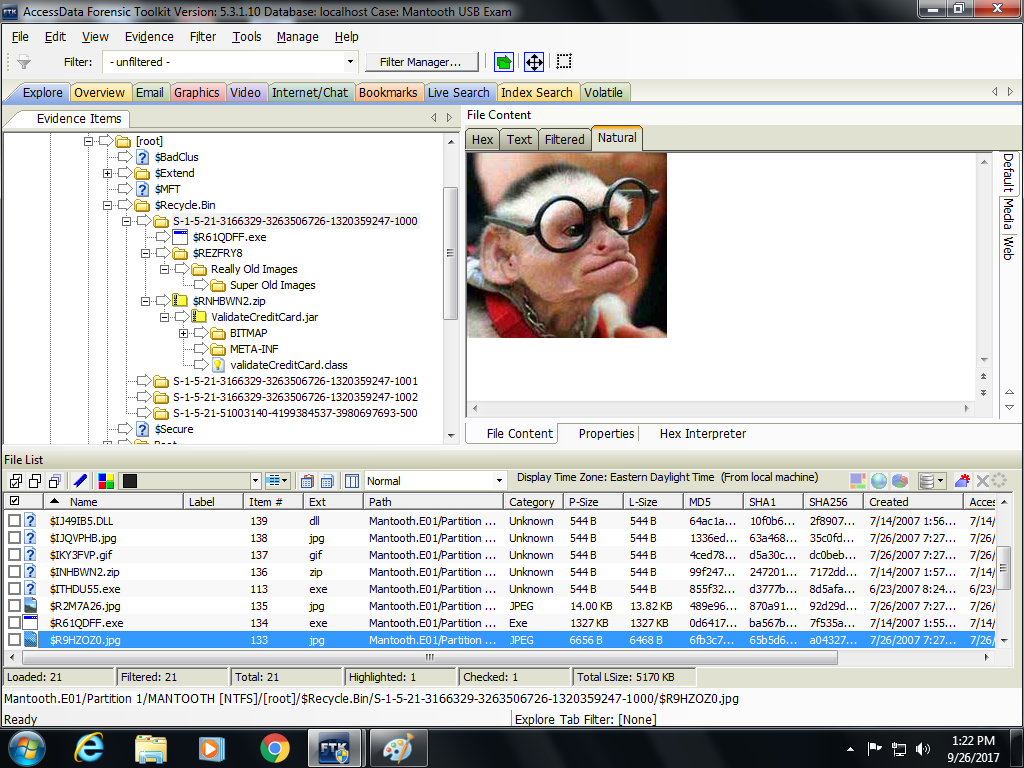
name that begins with “$R” and the metadata regarding the file is in the file with a name that

begins with “$I”.

Review item named $R9HZOZ0.jpg as shown in the file list with the $Recycle.Bin directory for

the SID that ends with “1000”. What is the picture of? What is the original file path of this

picture? When was it created? [15 points]



15. Within the evidence tree, navigate to the “File Status” “Decrypted Files” container and notice

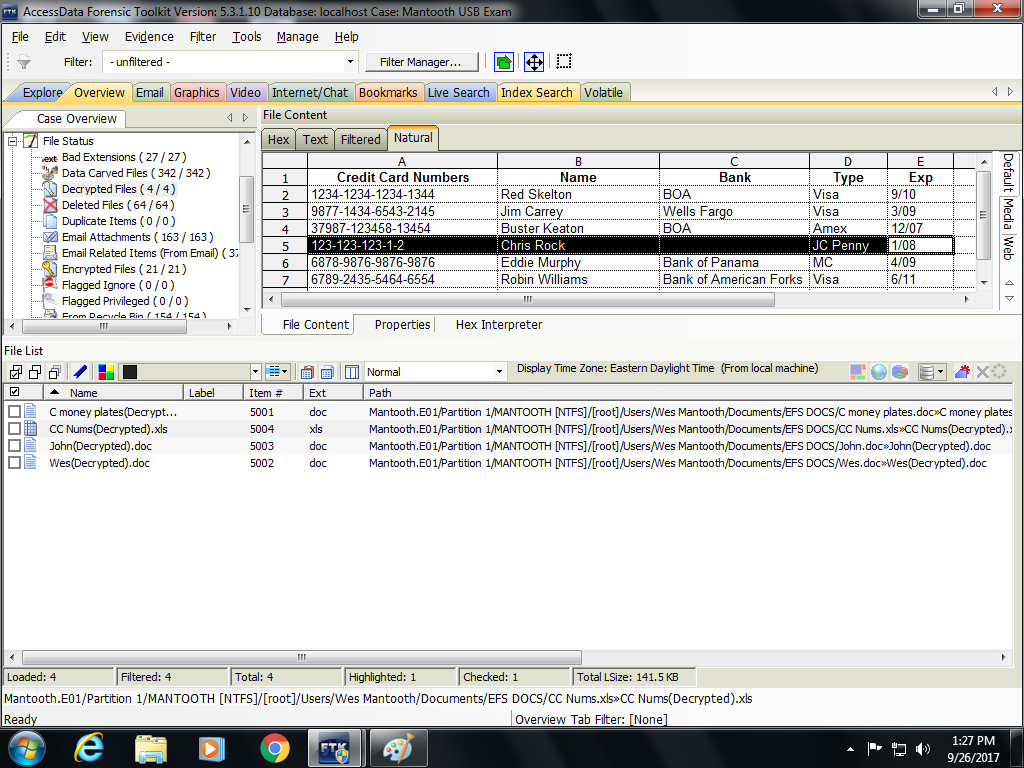
that there are no decrypted files.

On the FTK interface, select Tools > Decrypt Files. In the password box type “tooth”, select “OK”

and select “decrypt”. Notice that 4 files are reported to have been decrypted. Navigate back to

the File Status” “Decrypted Files” container again and inspect the decrypted files.

What is the JC Penney credit card number associated with Chris Rock? [5 points]



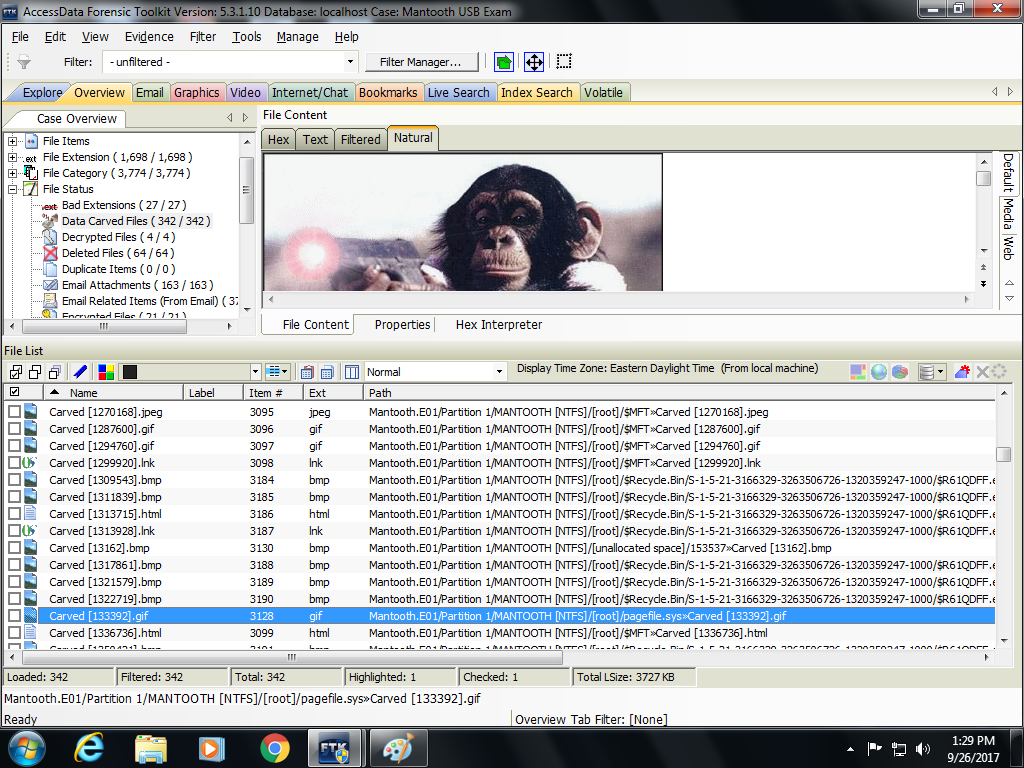
16. Navigate to the “File Status” > “Data Carved Files” container and notice the files within it.

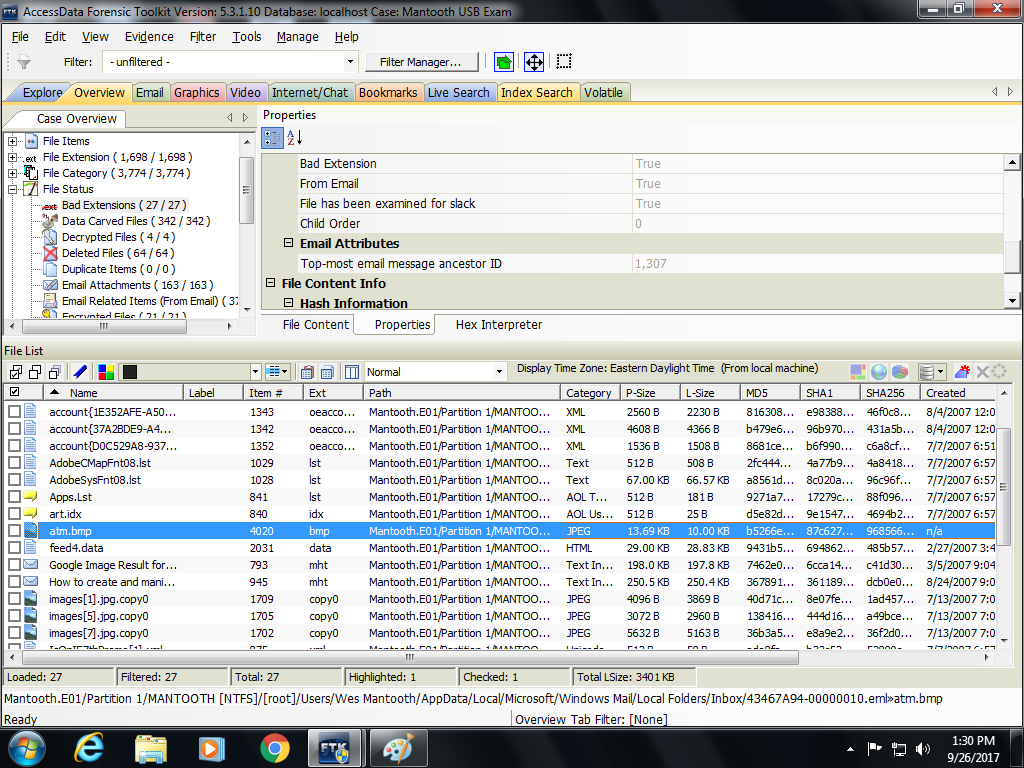
Notice that these files are assigned numbers rather than having names. The original names

have been lost. When a file is carved, (usually) only the contents of the file are recovered. The

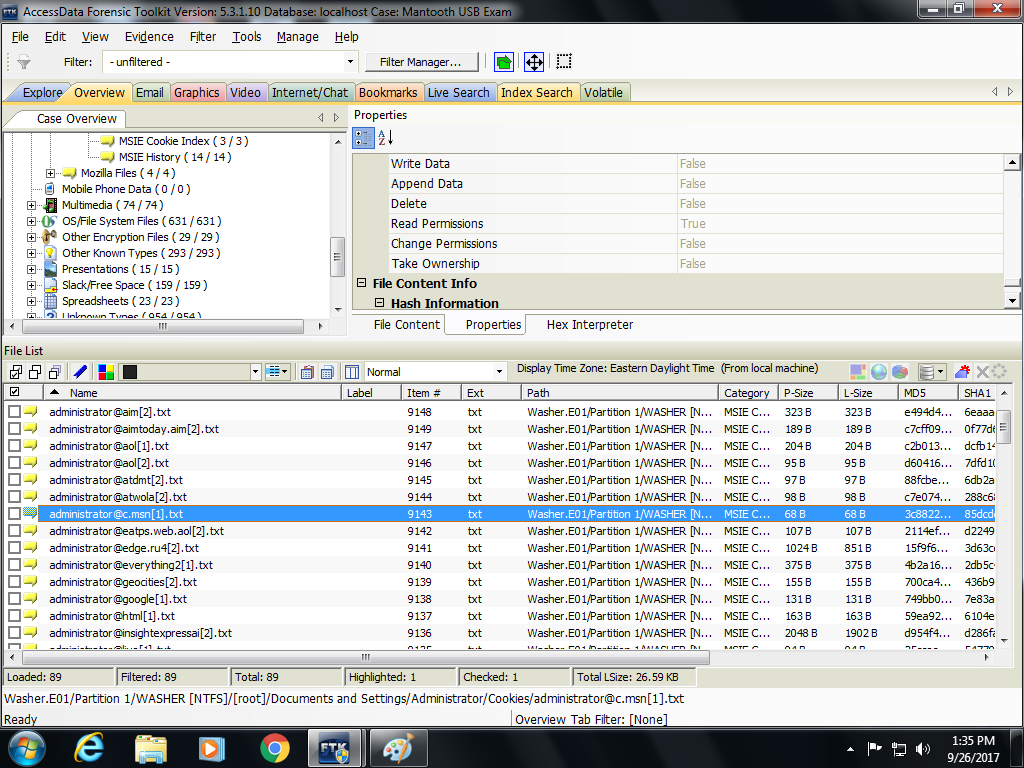
Metadata is often lost. Scroll through the carved files. What is the item number for the picture

of a monkey shooting a gun? See the picture below. [5 points]

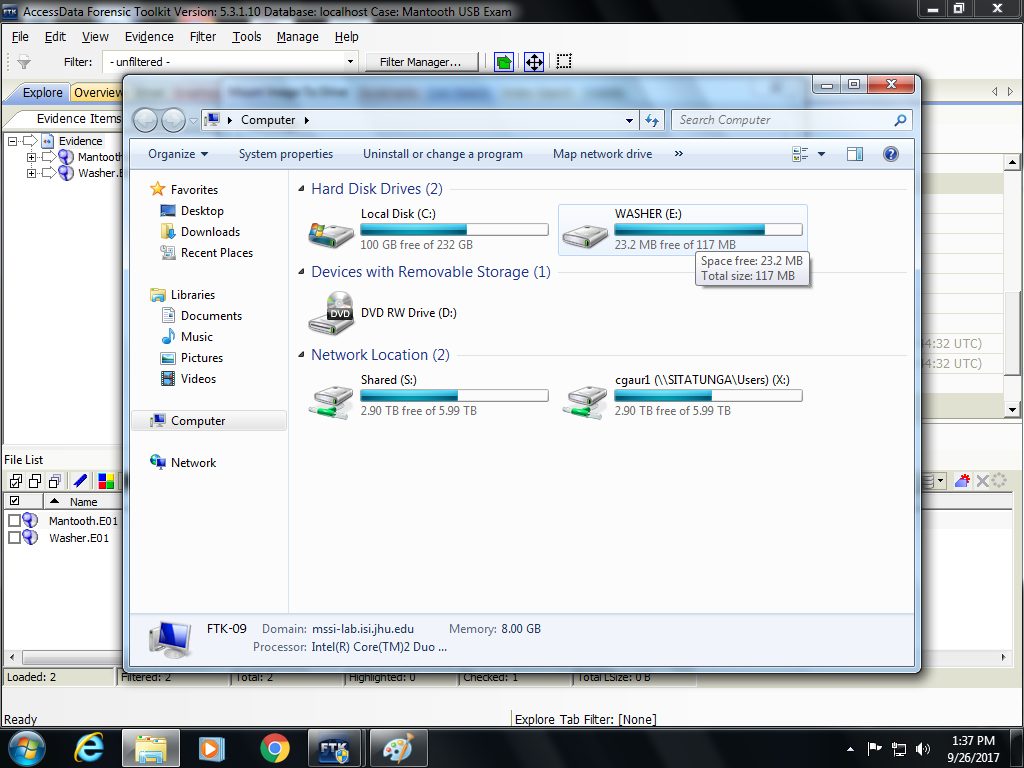


17. Navigate to the “File Status” > “Bad Extensions” container. Notice the file names “atm.bmp”. Why is this file identified as having a bad extension? [5 points] 

18. Add the “Washer.E01” file to this case. (Accept the default settings for processing.) Navigate to the “File Category” > “Internet Chat Files” > “Internet Explorer Browser” > “Internet Explorer Files” > “MSIE Cookie File”. Review the files in this container. These are Internet browsing cookies. These records imply that the user of the computer had an interest in these web sites. If these were web site that had illicit information associated with them, these records might be used to demonstrate an “intent” to commit a crime. [5 points] What is the item number associated with the administrator@c.msn[1].txt record?



19. Mounting a drive allows one to open a drive in a read-only mode and brows the contents within a Windows operating system and other applications. Mount the Washer.E01 file. On your Windows operating system start menu, navigate to the “Computer” tab. (See the picture below).



20. After every examination, it is important to re-calculate the hash value of the image file that you have been viewing/examining. This helps assure the court that the file was not altered during your examination. Use the FTK tool (not FTK Imager) to re-verify the hash values for the Mantooth.E01 image. What are these values and do they match the previous values? [5 points]

