Evan Obal

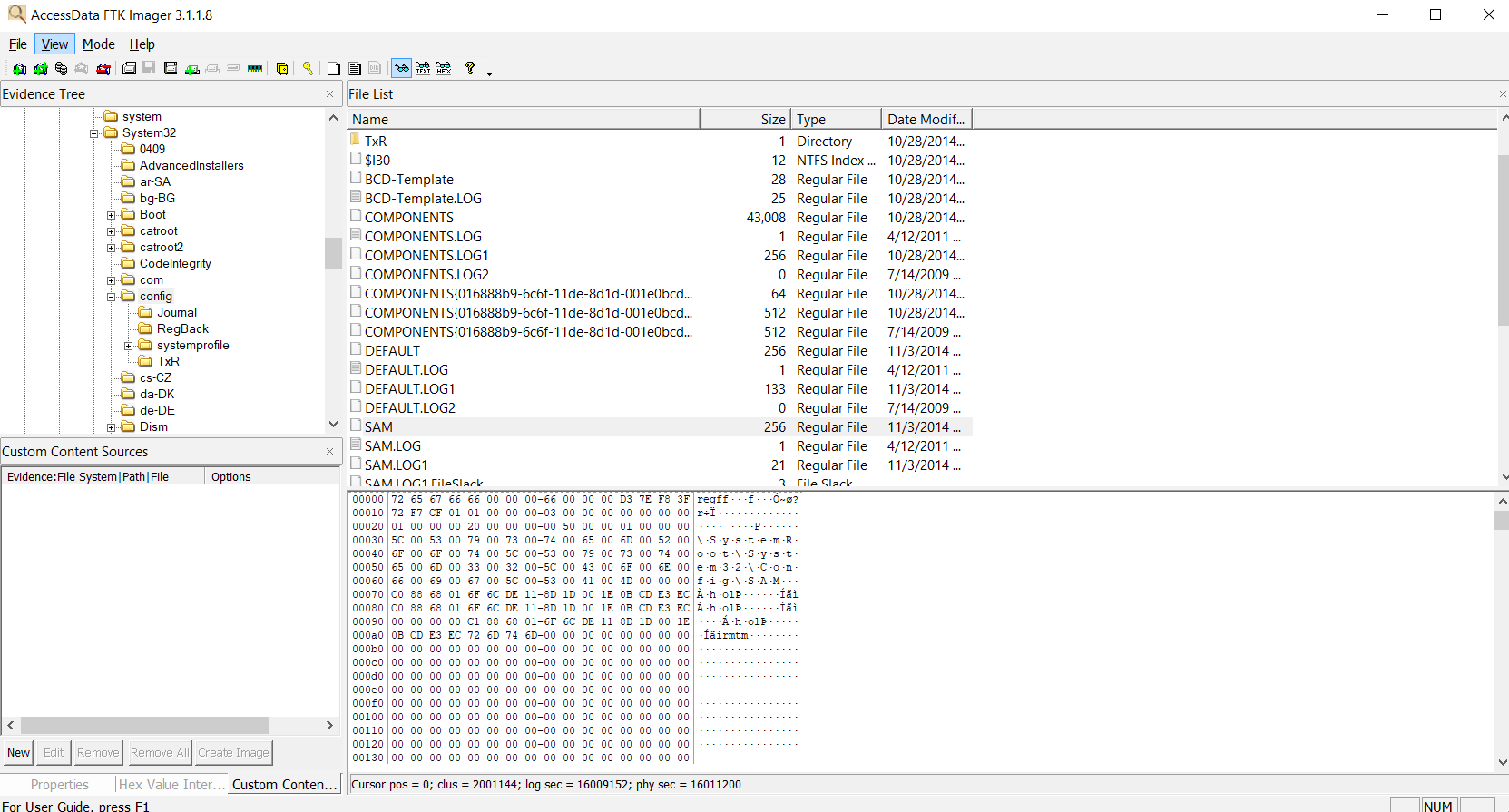
6/4/2019

CNS 320

DB Cooper Report

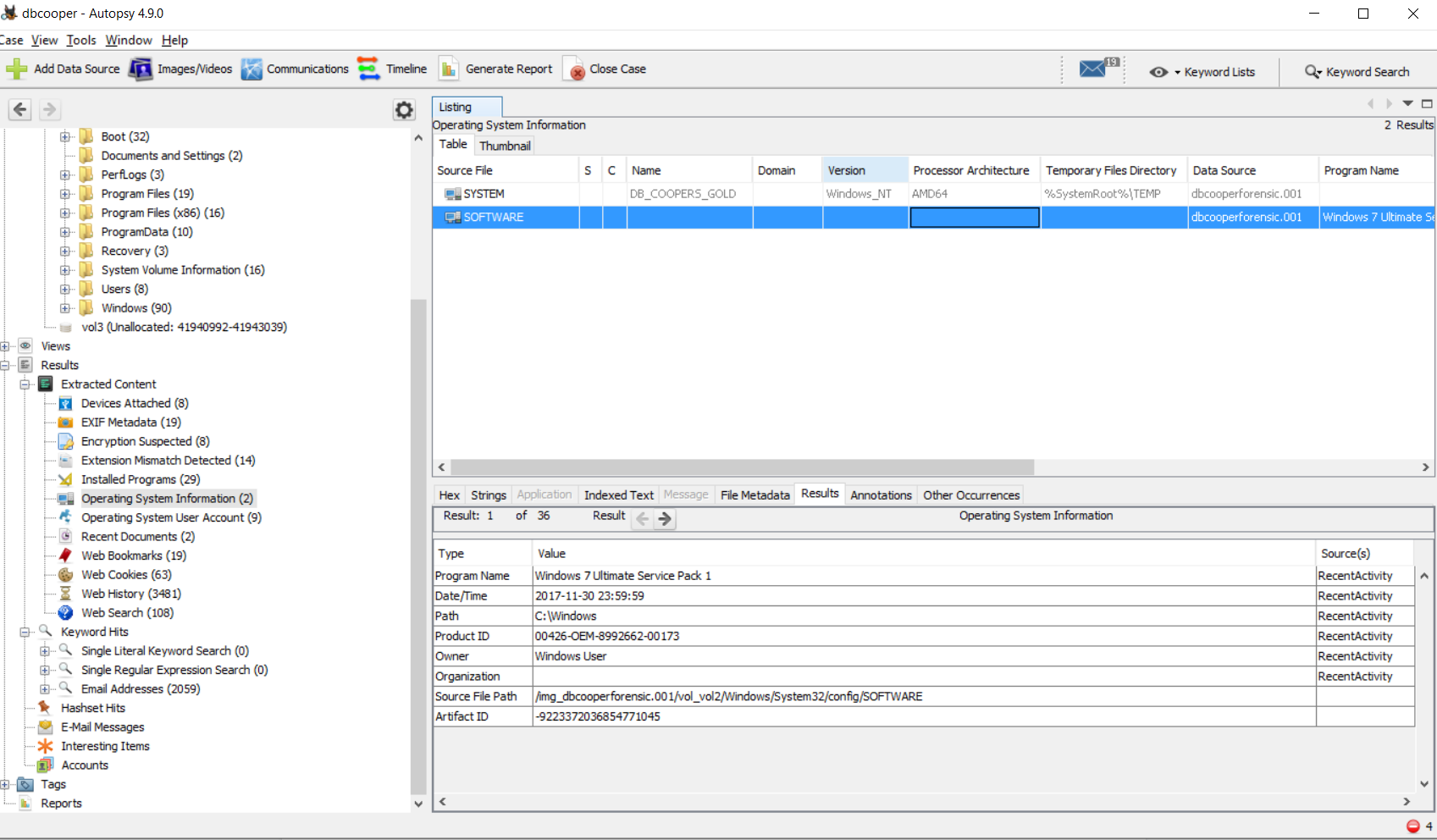
1.) The MD5 hash of the forensic image is: f175912b7e0ecb64ac0817d8d3cfe681 . I used winMD5Sum on the forensic image to retrieve the MD5 Hash.

2.) Using AccessData FTK Imager, we can extract files from the drive. Some of the files I extracted were the SAM and SYSTEM file from C:/windows/System32/config. Using the program SAMInside we are able to view the users and password hashes of the image. The username for the main profile is: DB Cooper



3.) Using the NT-hash from the SAM file, I used an online hash cracking website to find the password: hidemy$

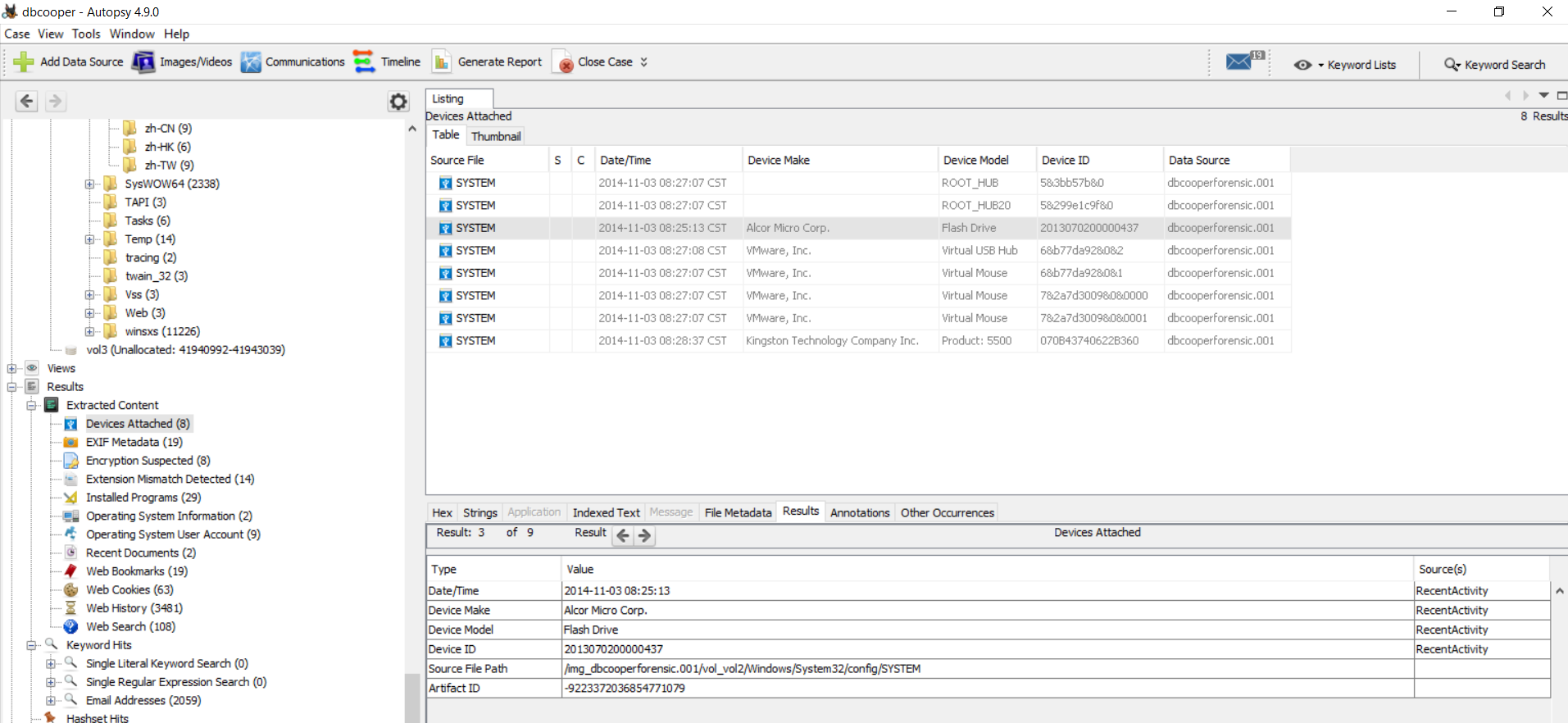
4.) I used the program Autopsy to generate a timeline of the data on the forensic image. In the Operating System Information section we can see that the operating system was registered under the name: DB\_COOPERS\_GOLD. The operating system is: Windows 7 Ultimate Pack 1.



5.) Looking at the creation date of the operating system’s files we can see that the Operating System was installed on: 07/13/2009 at about 22:20:10 CDT

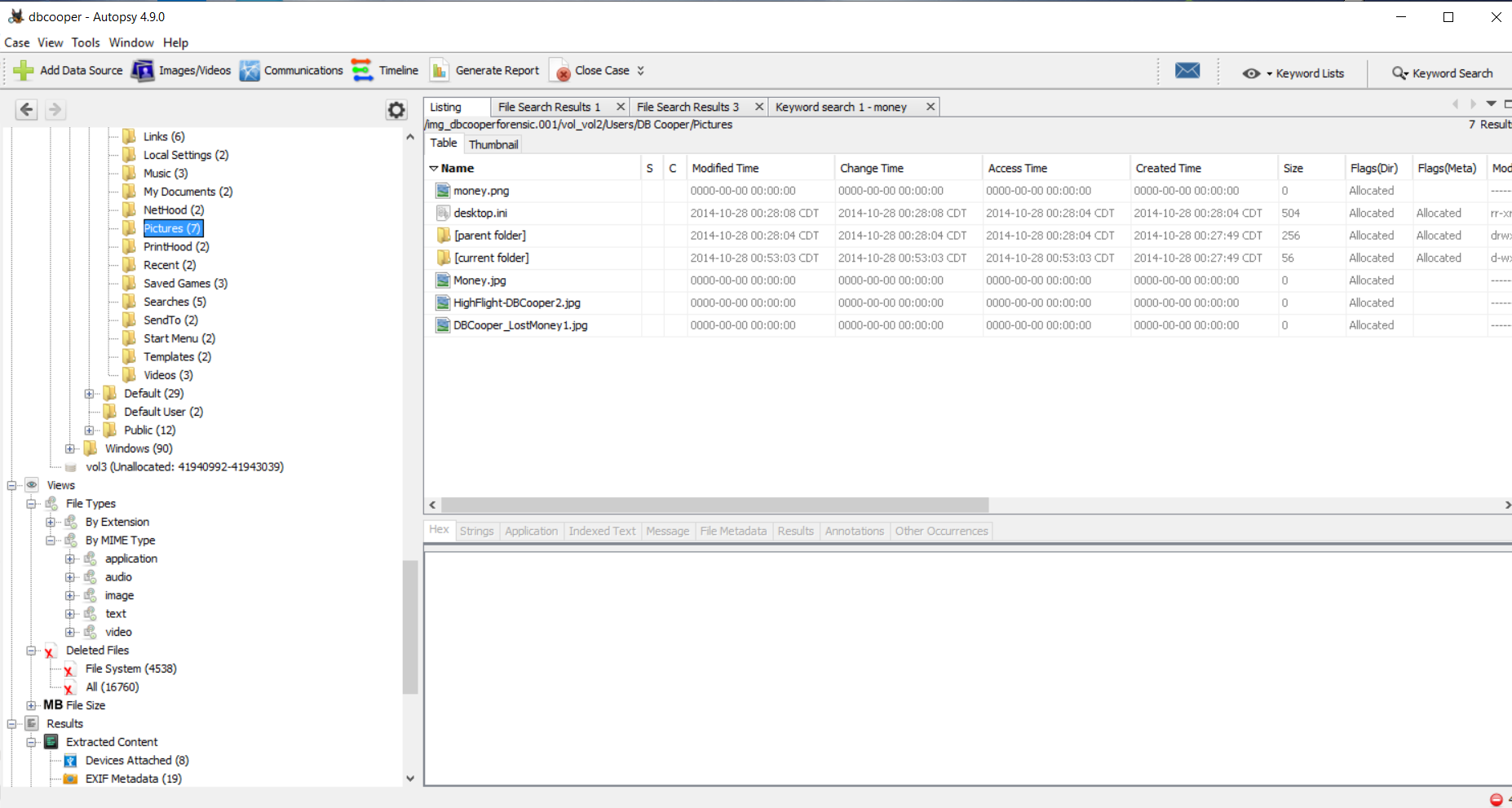
6.) Using Autopsy on the forensic image, we can see multiple USB devices used. One device is an Alcor Micro Corp. Flash Drive with serial number: 070B43740622B360&0. it was used on 11/03/2014. I used RegRipper on the image’s SOFTWARE file in

C:/windows/System32/config.

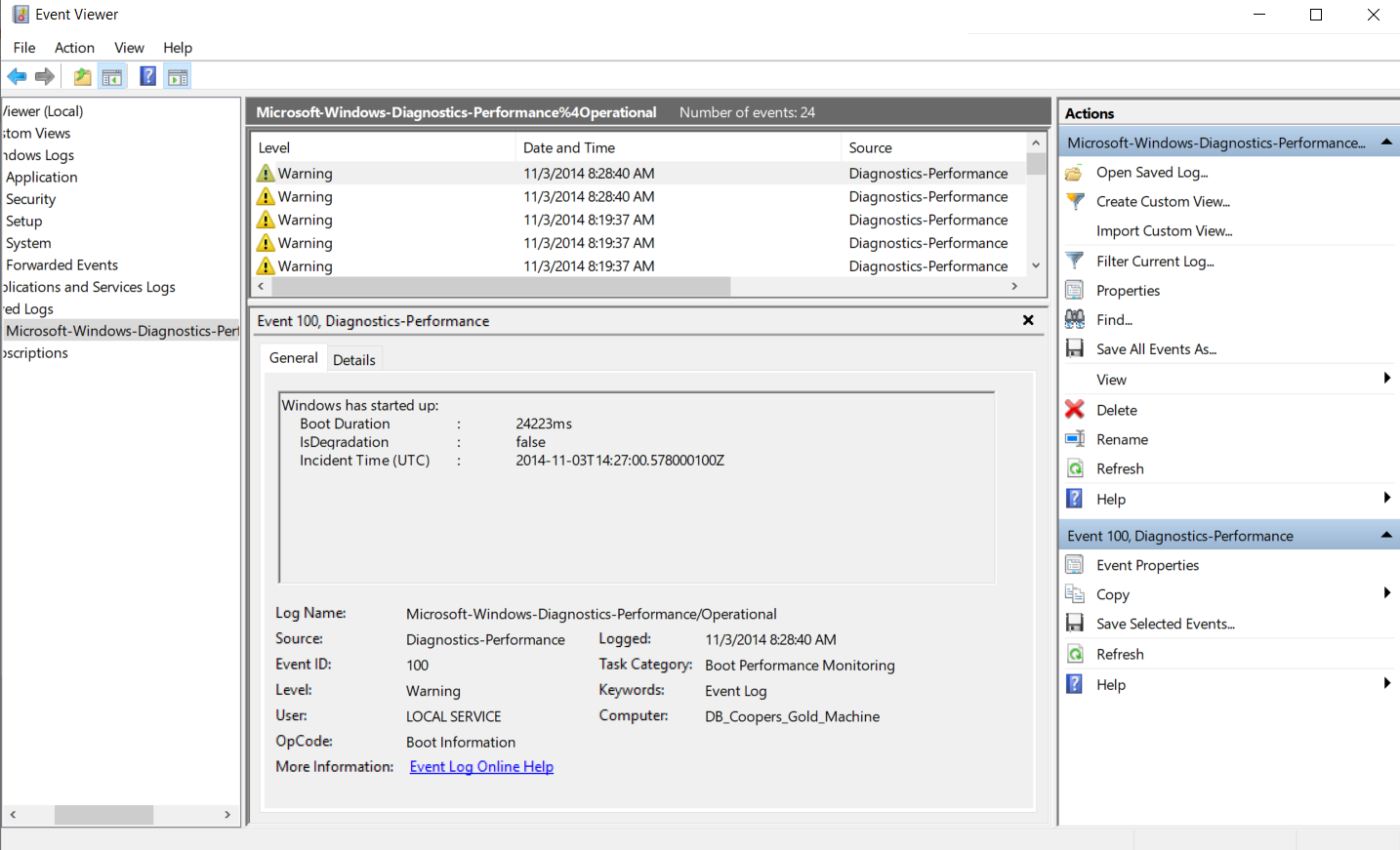


7.) Continuing to use Autopsy on the Forensic image, we can see that the USB flash drive contained a file secrets.zip. Inside a file was accessed called secrets.lnk

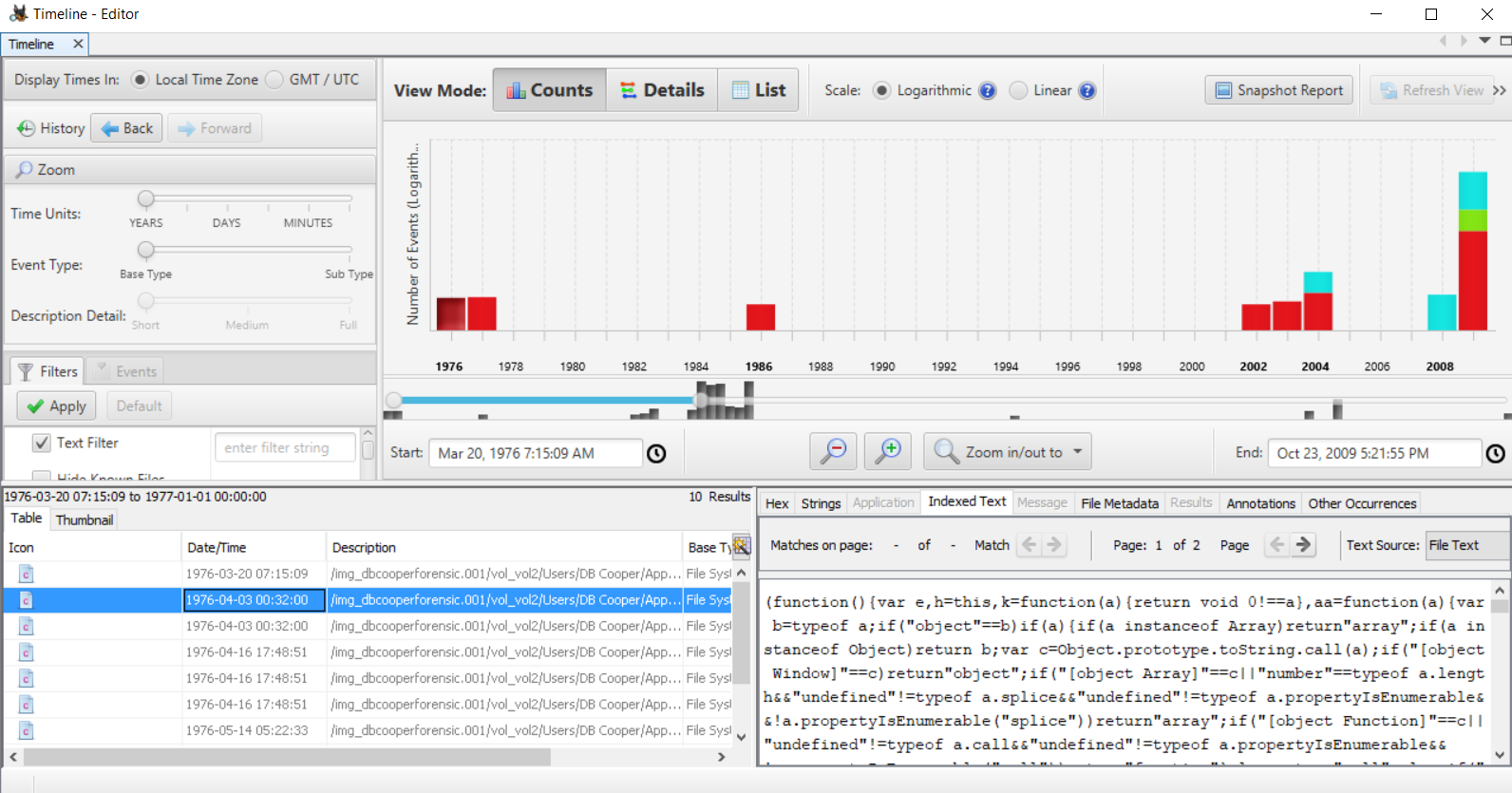
8.) Using Autopsy I was able to recover the images of the lost money: DBCooper\_LostMoney1.jpg, Money.jpg, and money.png



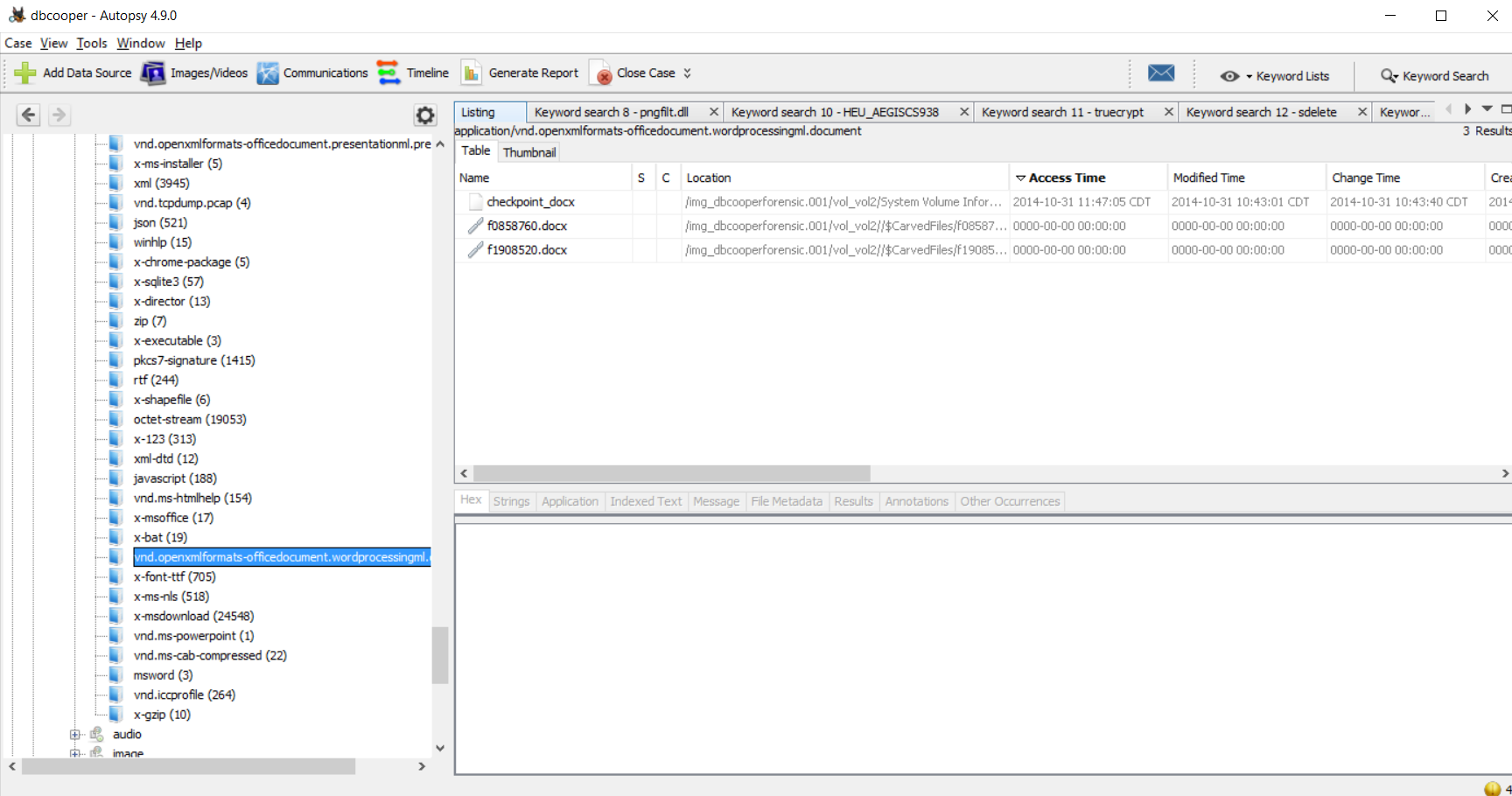
9.) By using Autopsy to extract system event log files, we are able to view the name of the suspect’s computer: DB\_Coopers\_Gold\_Machine. I used Windows’ event viewer to view the log files extracted from the image.



10.) There are signs of time/date manipulation on the suspect’s computer. Using Autopsy’s timeline functionality I revealed that there had been files created and changed that had absurd dates. Some of these files had creation dates of the year 1976.

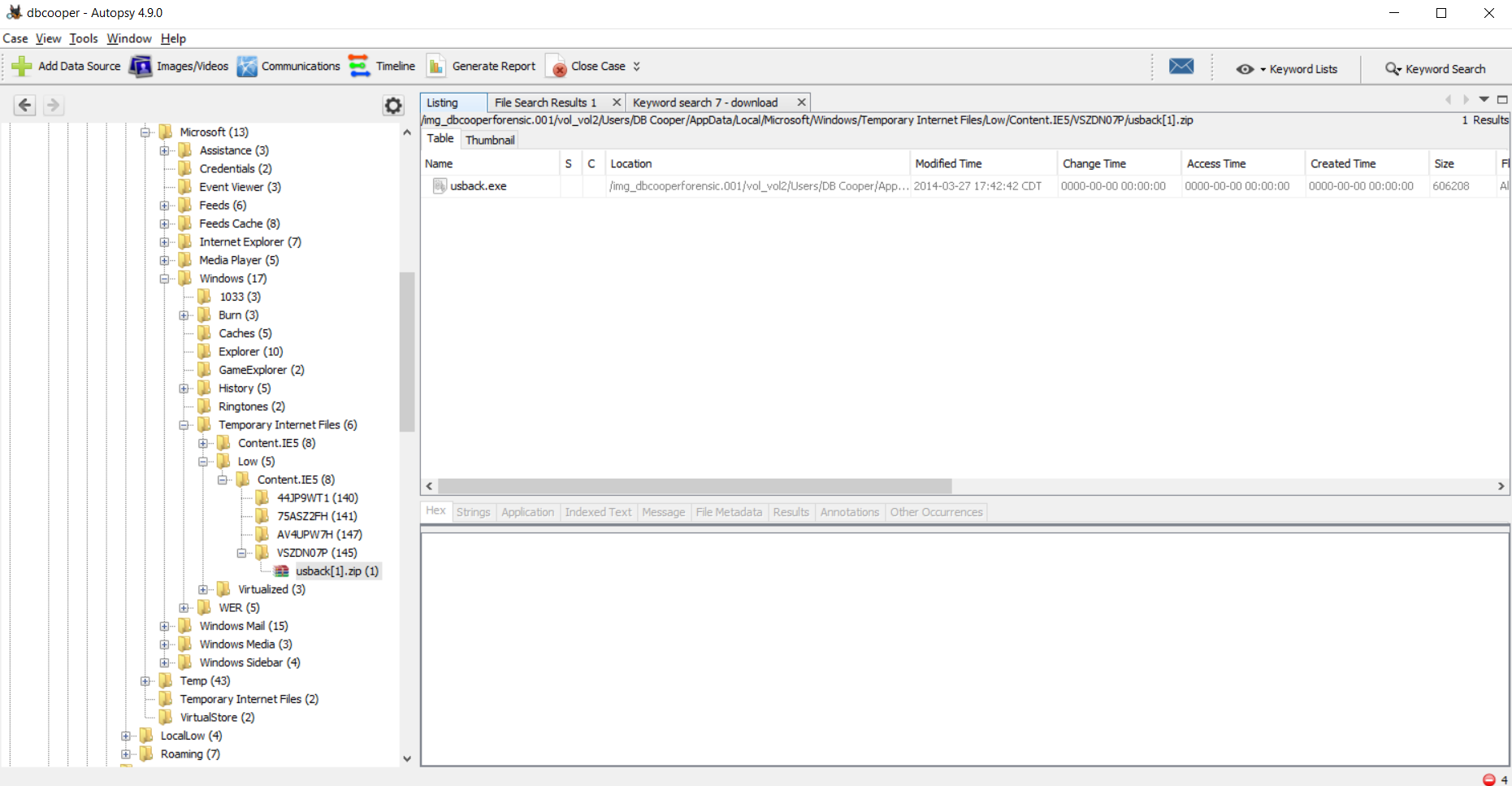


11.) By using Autopsy to look at the MIME Type of all files, I have deduced that the suspect accessed the document: checkpoint.docx.

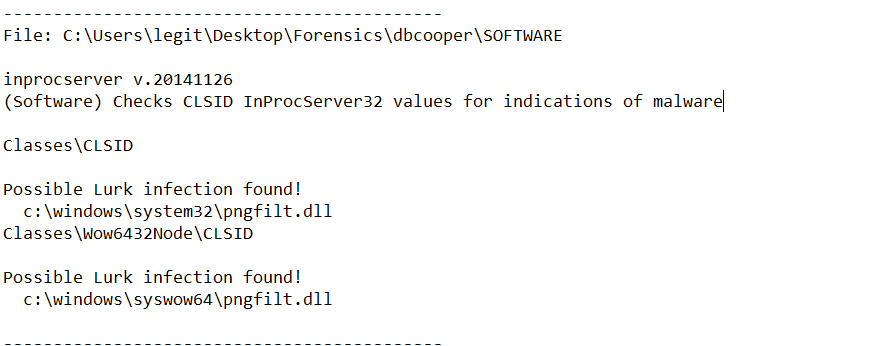


12.) Using Autopsy I was able to see the many searches the suspect made. Some of these searches are: “downloading a virus via dropbox”, “how to shred documents with sdelete”, “how to use truecrypt”, “where is db cooper now?”, “Where to hide in belize”. These searches are contained in index.dat files on the forensic image.

13.) Using Autopsy, I can see what the suspect has downloaded in the temporary internet files directory. I can see a zip file that was downloaded called “usback[1].zip” inside is an executable. The access and modified times shows that it was used on 11/03/2014.



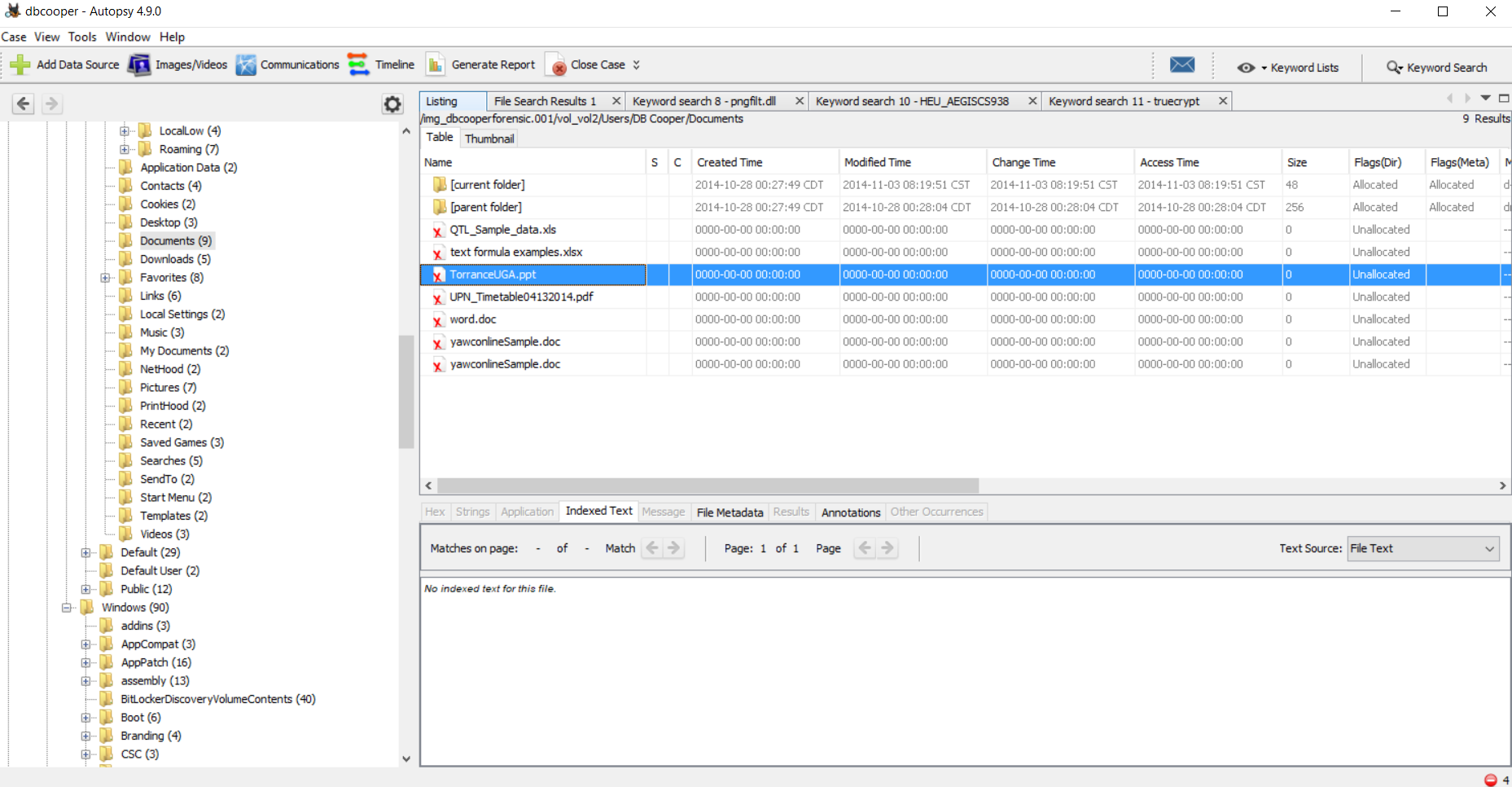
14.) Using RegRipper on the suspect’s SOFTWARE file, we can see several malware files. The files: c:\windows\system32\pngfilt.dll and c:\windows\syswow64\pngfilt.dll shows signs of malware infection. With the change time we can tell that the file was infected on 10/28/2014 by usback.exe



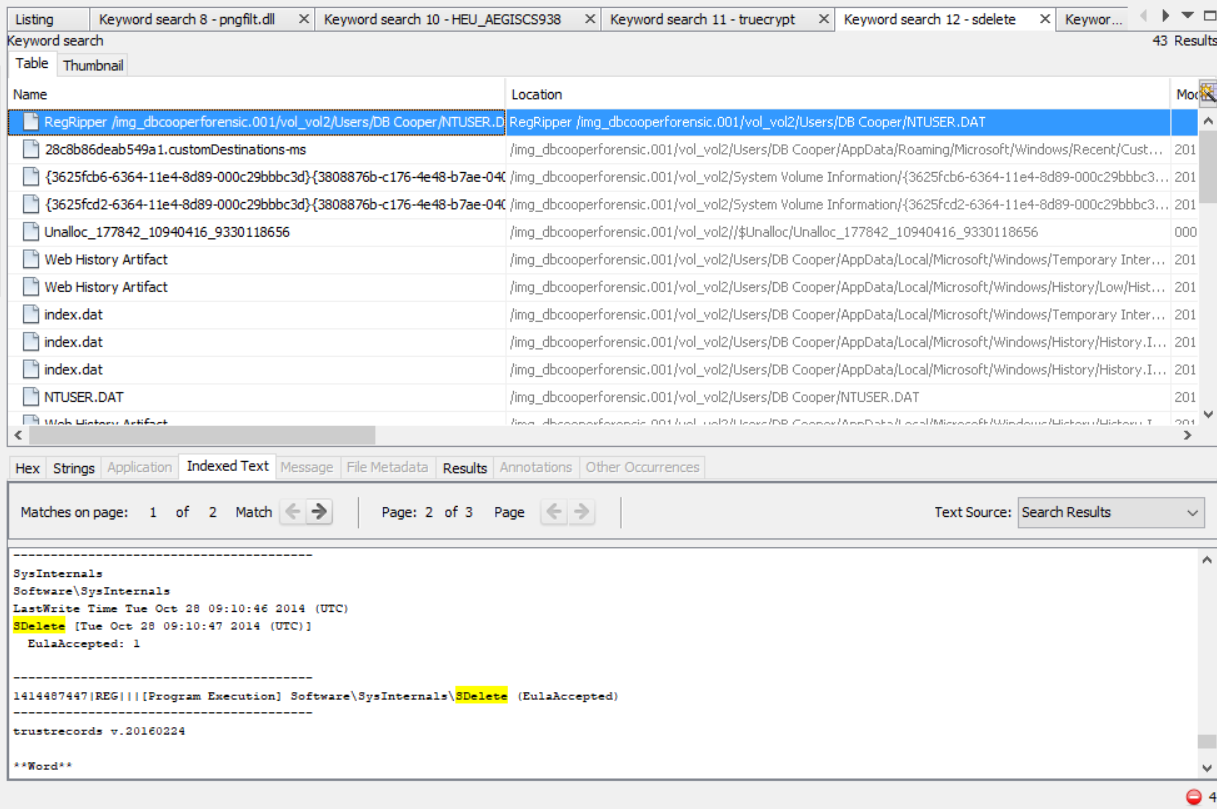
15.) I can see that the suspect had encrypted a few files on their computer. I used autopsy to show files that are encrypted on the forensic image. Some of the files include a file called “data” in the system32 directory that is suspicious.

16.) One of the pictures found on the forensic image (IMG\_3573.JPG) contained EXIF data. The coordinates from the EXIF data leads to Belize City in Belize. This finding combined with the recent internet searches performed on the computer leads me to suspect that DB Cooper is hiding in Belize City in Belize.

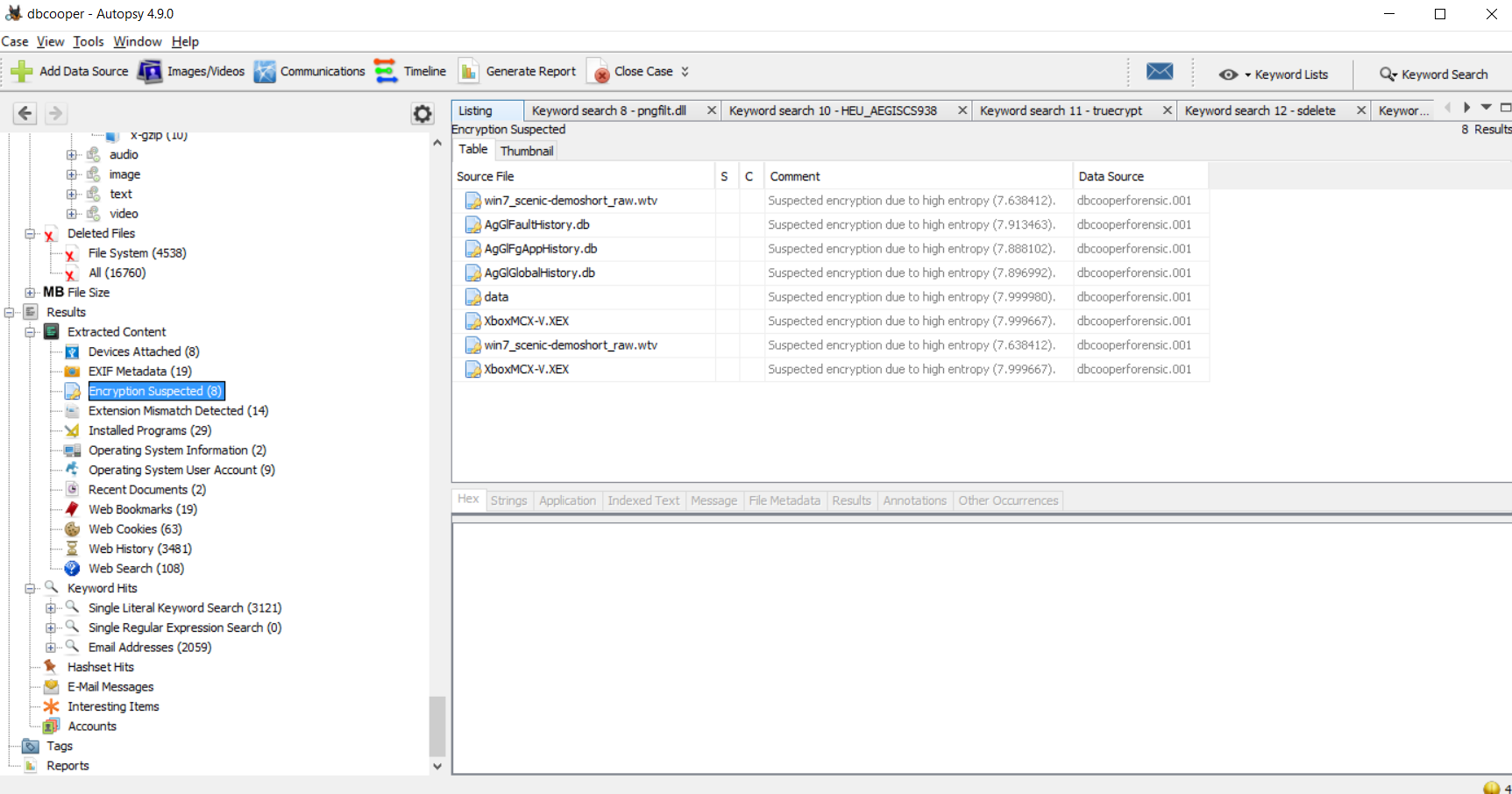
17.) The suspect’s computer image shows that there are many files that have been deleted, some interesting files I found were named “UPN\_Timetable04132014.pdf”, “word.doc”, “text formula examples.xslx” and “QTL\_Sample\_Data.xls” located in DB Cooper’s Documents folder.



18.) Using Autopsy I can see that DB Cooper used the program SDelete to remove files from his computer. It appears that the tip is correct and SDelete was ran and deleted files on 10/28/2014. It’s located in the Software\SysInternals\SDelete



19.) A docx file called checkpoint.docx contains the suspect’s TrueCrypt Password for the “data” fault: 85458xskdrirj. The password file indicates that the encrypted container is called “data”. A file named “data” was suspected of encryption due to high entropy.



20.) Using TrueCrypt 7.2, and the password found in checkpoint.docx, I was able to extract the image: gold-clipart-pot\_of\_gold\_coins.png

