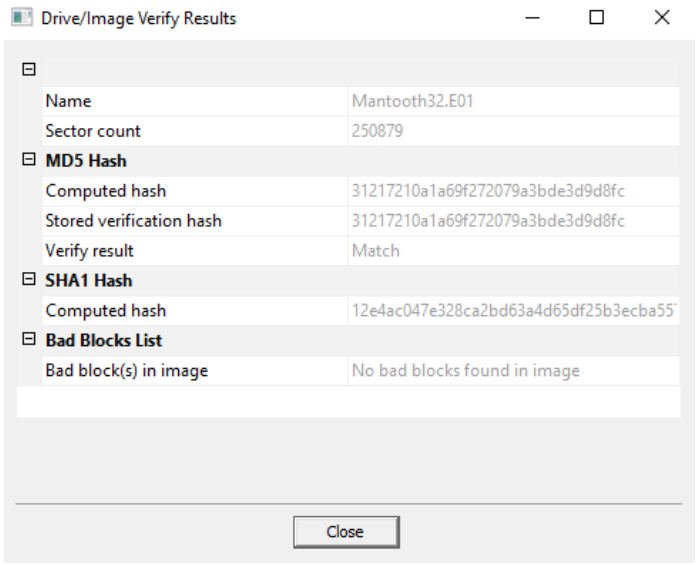
ITIS 5250
Parag Mhatre
Semester Project
Dec 4th 2018

Overview:

In this project, Detective Ketchum, has given me an image of a desktop computer, belonging to a gang member "Wes Mantooth". The image is in EnCase E01 format. I will examine this image and try to find evidence of the accused being involved in crimes. I will use different methods like File carving, Password Recovery, searching emails, etc. to find the evidence.

Forensic Acquisition & Exam Preparation:

I accessed the shared drive from the Forensics Lab in Cone to access "Mantooth32.E01" image and transferred it to my machine. I used FTK Imager to Hash and Verify Integrity of the Image which came as a "Match". I am using FTK, FTK Imager and PRTK for processing the file.

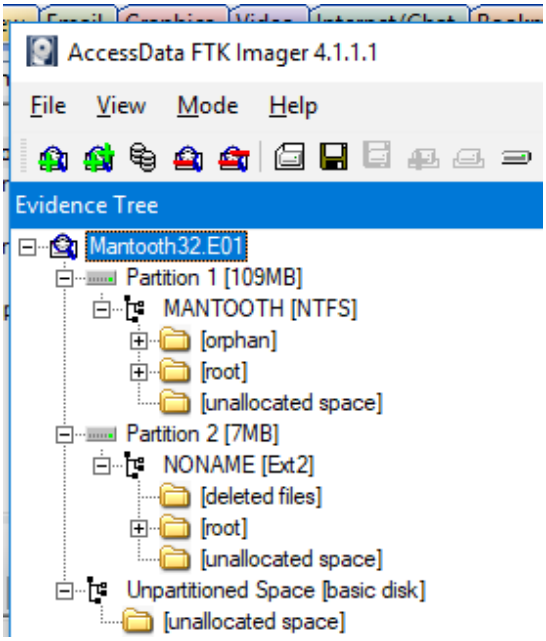


Then, I loaded up the file in FTK 6.3 with relevant Refinement options like Data and Meta Carving, Process Internet history for visualization, Performance Automatic Decryption, Document content Analysis, etc.

Findings and Report (Forensic Analysis):

1. Account for how all the space on the computer hard drive was used (partitions, used/free).

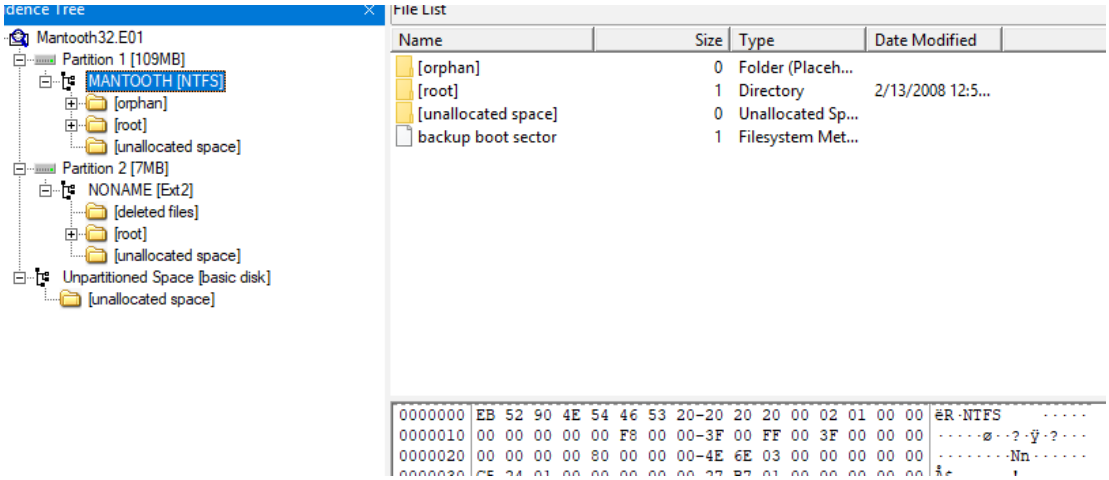
   I loaded the image on FTK Imager to see that the "Partition 1" has a total size of 109 Mb and "Partition 2" has a size of 7 Mb. Thus the total used space is 109+7 = 116Mb out of 128Mb.



2. Identify the type of file systems in use.

The file systems in use are as follows:

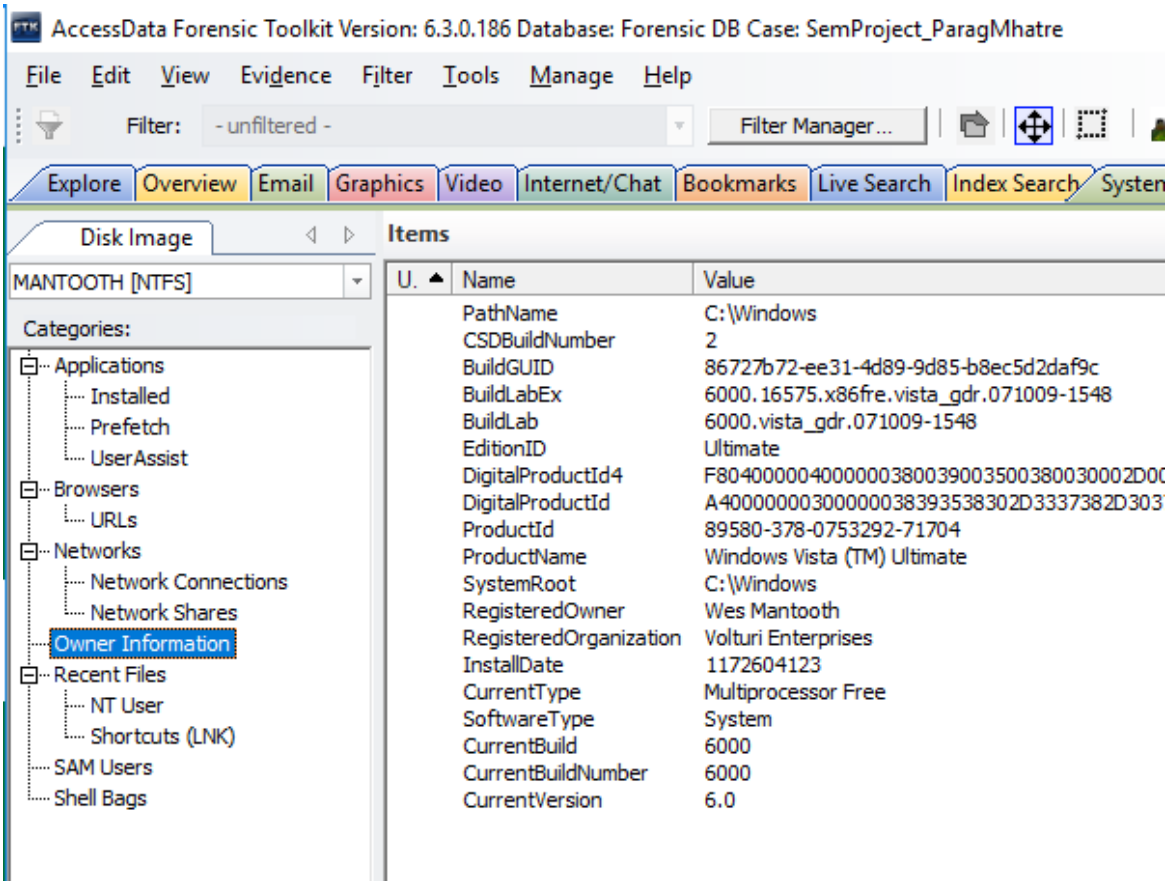
a. Partition 1 – NTFS
b. Partition 2 – Ext2



3. Identify the version and service pack of the Operating System.

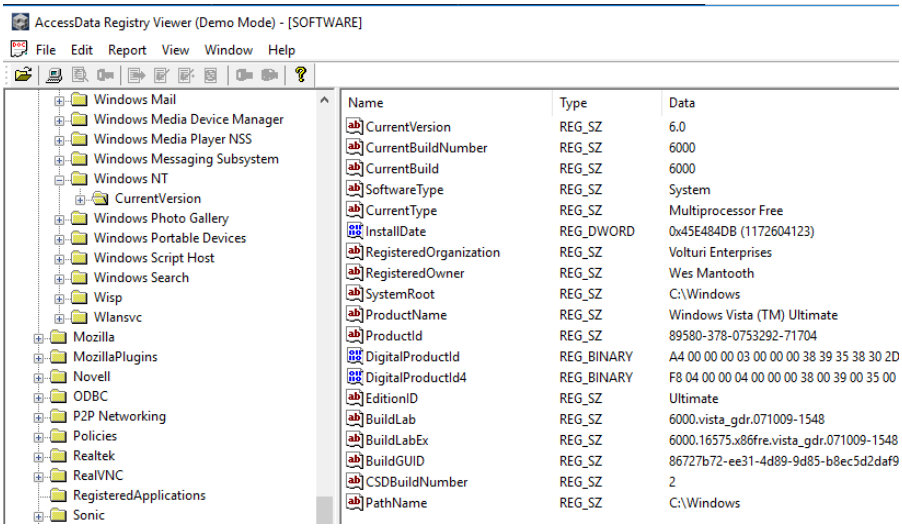
The System Information tab of the FTK shows that the OS is:

Windows Vista Ultimate 6.0 where 6.0 is the current version.

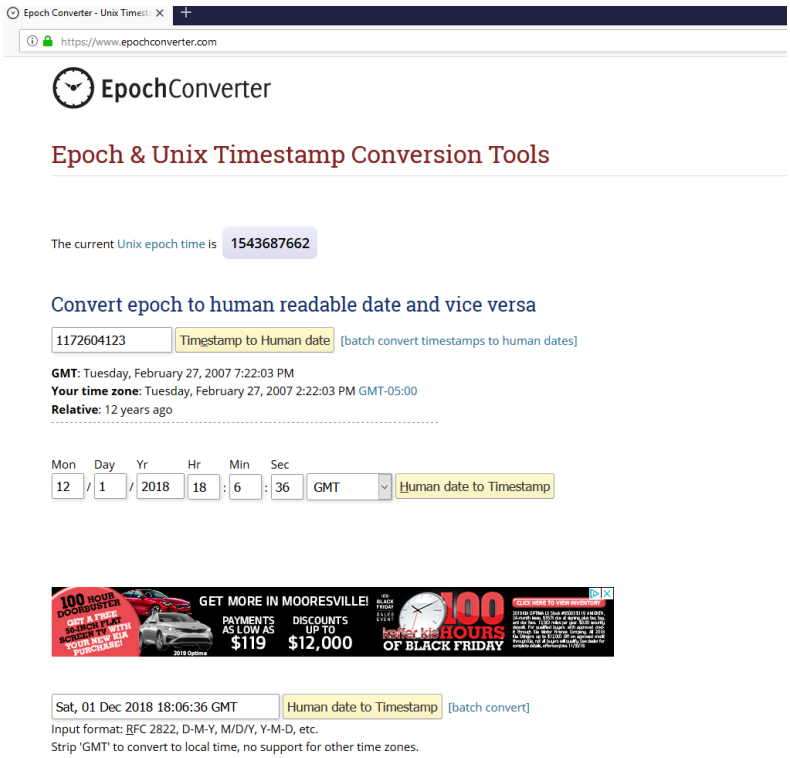


4. Find the date the OS was installed.

I opened the Software file in the Registry viewer, and found out the “InstallDate” value as “1172604123”.

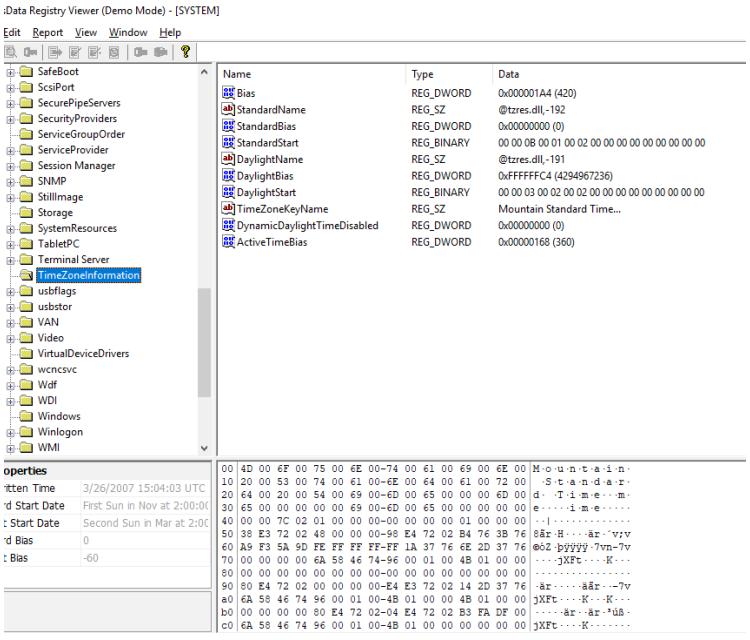


When I decoded the Epoch time to Human Readable time, the time was Tuesday 2/27/2007**.**



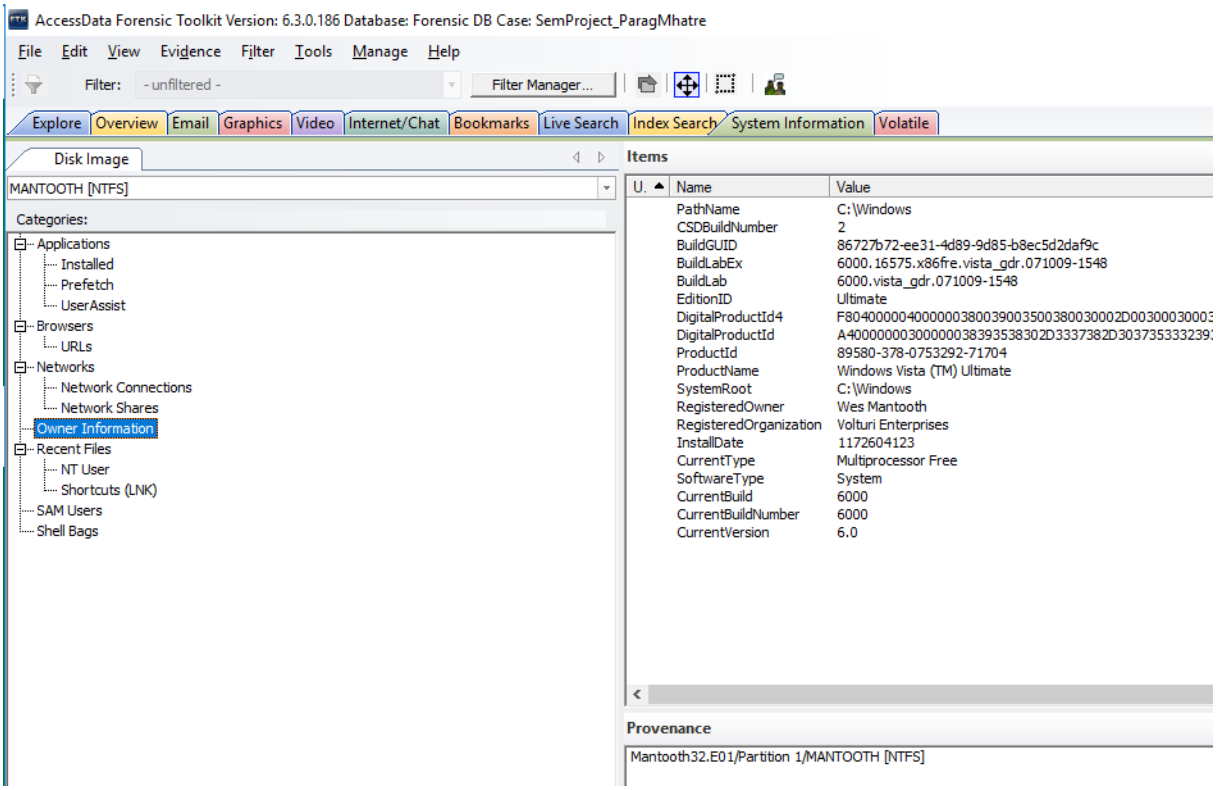
5. Identify the Time Zone information for the computer.

I opened the System file in Registry Viewer and found under “TimeZoneInformation”, that the key name for the set timezone is “Mountain Standard Time.



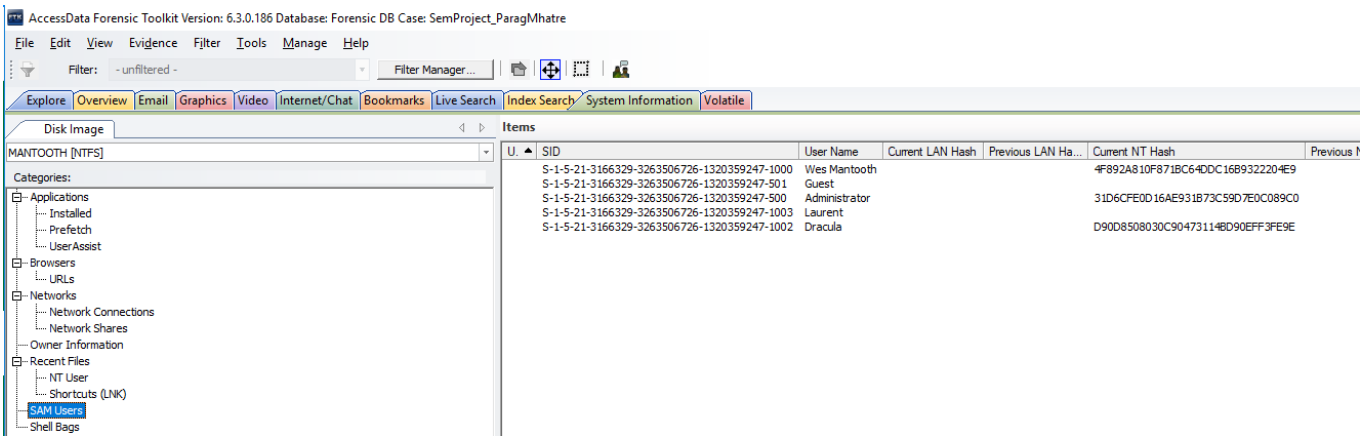
6. Show the owner of the computer.

In the “Owner Information” tab of “System Information”, the Registered Owner is given as “Wes Mantooth”.



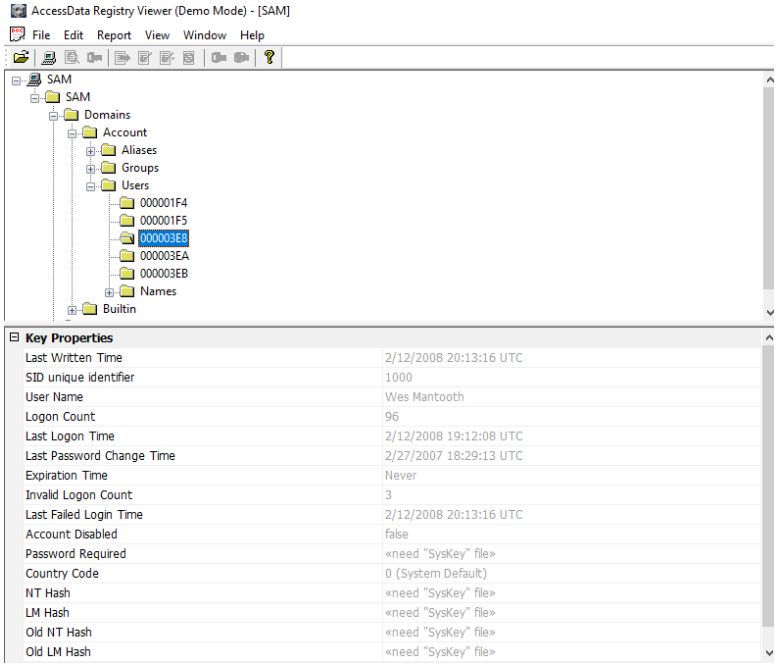
7. Show the most active user of the computer and list all users.

The list of all users is as given below as found from SAM Users category from “System Information” from FTK.



The user with the most logon count is “Wes Mantooth” with a logon count of 96. I found this out by opening the SAM file on Registry Viewer. Others have logon counts as follows:

Administrator – 1, Guest – 0, Laurent – 0 and Dracula – 3.

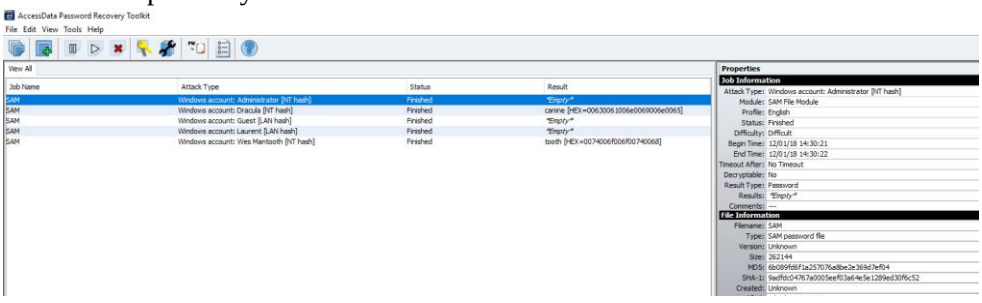


8. Identify user accounts and who uses the account.

   The user accounts are – Wes Mantooth, Dracula and Laurent.
   Wes Mantooth and Dracula use their accounts with a login count of 96 and 3 respectively.
   Laurent had not logged into his account even once.

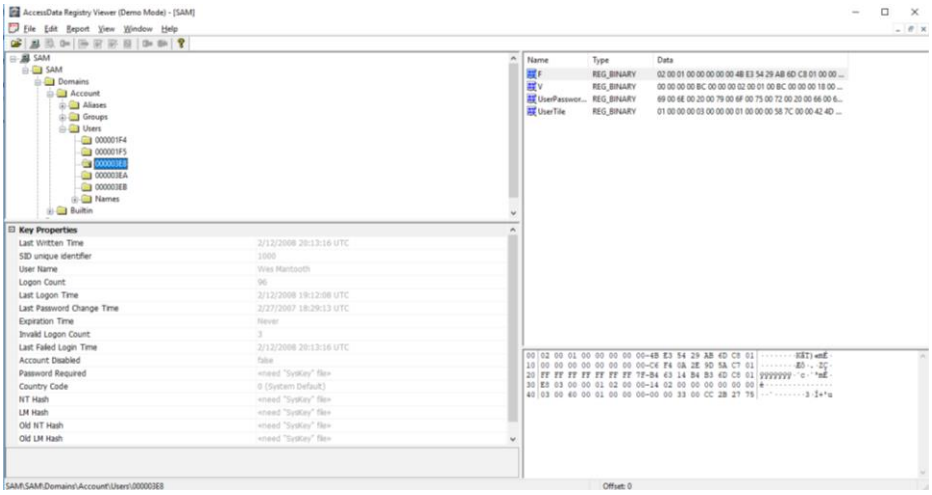
9. Acquire user passwords.

   I exported the SAM and SYSTEM files from FTK and loaded them into the Password Recovery Toolkit. The cracked passwords for the users Wes_Mantooth and Dracula are “tooth” and “canine” respectively.



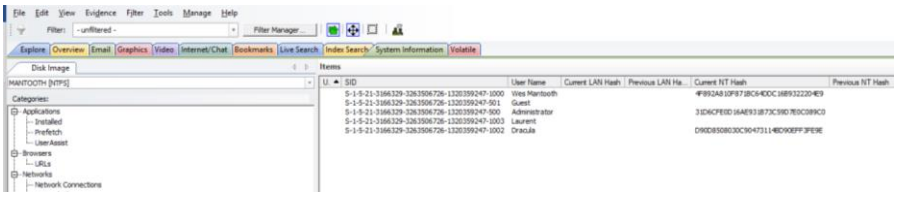
10. Identify the last date Wes Mantooth logged on.

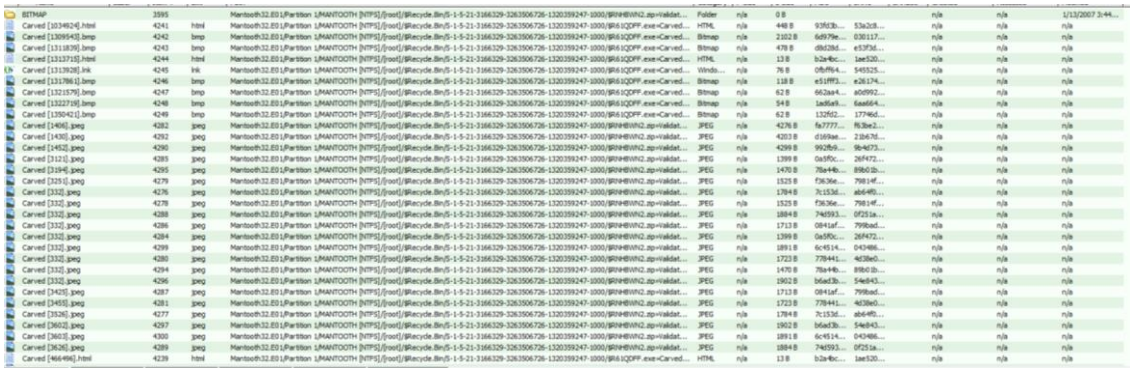
The last login date as shown from the screenshot of the SAM file opened in Registry viewer is 2/12/2008.



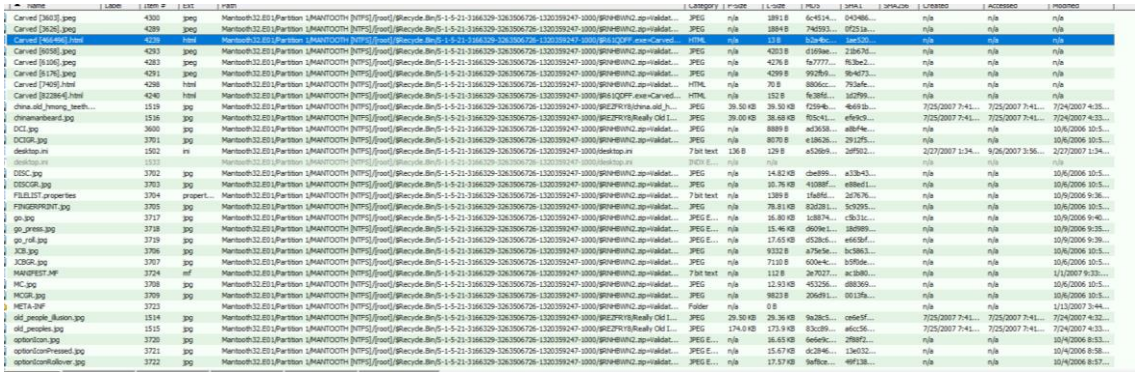
11. Identify files placed in the recycle bin by Wes Mantooth.

To find the files placed in the registry by Wes Mantooth, I followed a two-step process. Opening up the SAM file, I checked the SID for Wes Mantooth is "'S-1-5-21-31663293263506726-1320359247-1000". When I checked this specific SID folder from Recycle bin, I could see all the long list of files that were deleted by that particular user as shown in the screenshots below.





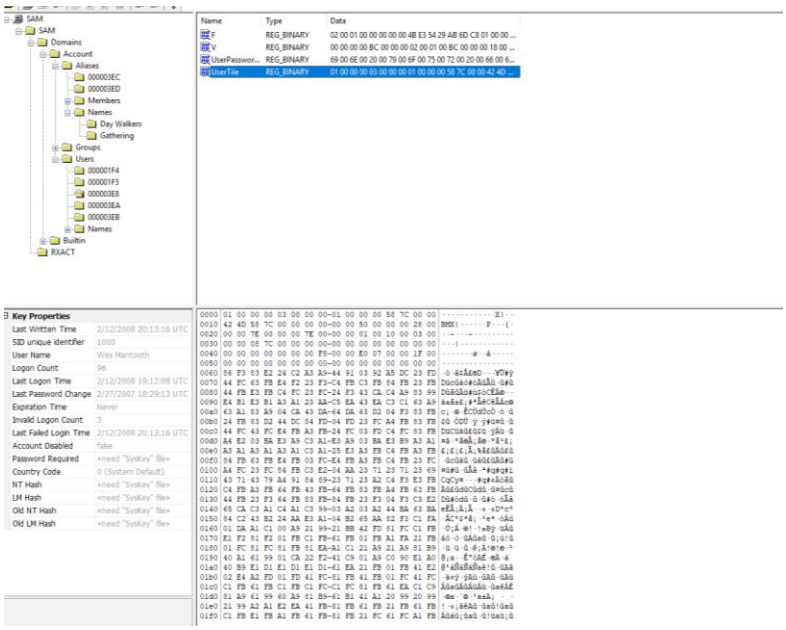
Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
DISC.jpg		3702	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	14.82 KB	cbe899...	a33b43...		n/a	n/a	10/6/2006 10:5...
DISCGR.jpg		3703	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	10.76 KB	41088f...	e88ed1...		n/a	n/a	10/6/2006 10:5...
FILELIST.properties		3704	propert...	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	7 txt text	n/a	1389 B	1fa8fd...	2d7676...		n/a	n/a	10/9/2006 9:36...
FINGERPRINT.jpg		3705	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	78.81 KB	82d281...	5c9295...		n/a	n/a	10/6/2006 10:5...
go.jpg		3717	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG E...	n/a	16.80 KB	1c8874...	c5b31c...		n/a	n/a	10/9/2006 9:40...
go_press.jpg		3718	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG E...	n/a	15.46 KB	d609e1...	18d989...		n/a	n/a	10/9/2006 9:35...
go_roll.jpg		3719	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG E...	n/a	17.65 KB	d528c6...	e665bf...		n/a	n/a	10/9/2006 9:39...
JCB.jpg		3706	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	9332 B	a75e5e...	bc5863...		n/a	n/a	10/6/2006 10:5...
JCBGR.jpg		3707	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	7110 B	600e4c...	b5f0de...		n/a	n/a	10/6/2006 10:5...
MANIFEST.MF		3724	mf	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	7 txt text	n/a	112 B	2e7027...	ac1b80...		n/a	n/a	1/1/2007 9:33:...
MC.jpg		3708	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	12.93 KB	453256...	d88369...		n/a	n/a	10/6/2006 10:5...
MCGR.jpg		3709	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	9823 B	206d91...	0013fa...		n/a	n/a	10/6/2006 10:5...
META-INF		3723		Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	Folder	n/a	0 B				n/a	n/a	1/13/2007 3:44...
old_people_illusion.jpg		1514	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RECYCLE.BIN\S-1-5-21-3166329-3263506726-1320359247-1000\$REZFRY8\Really Old I...	JPEG	29.50 KB	29.36 KB	9a28c5...	ce6e5f...		7/25/2007 7:41:...	7/25/2007 7:41:...	7/24/2007 4:32:...
old_peoples.jpg		1515	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RECYCLE.BIN\S-1-5-21-3166329-3263506726-1320359247-1000\$REZFRY8\Really Old I...	JPEG	174.0 KB	173.9 KB	83cd99...	e6cc56...		7/25/2007 7:41:...	7/25/2007 7:41:...	7/24/2007 4:33:...
optionIcon.jpg		3720	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG E...	n/a	16.65 KB	6e6e9c...	2f88f2...		n/a	n/a	10/4/2006 8:53:...
optionIconPressed.jpg		3721	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG E...	n/a	15.67 KB	dc2846...	13e032...		n/a	n/a	10/4/2006 8:58:...
optionIconRollover.jpg		3722	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG E...	n/a	17.57 KB	9affce...	49f138...		n/a	n/a	10/4/2006 8:57:...
Readme.txt		3582	txt	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>Readm...	7 txt text	n/a	354 B	627edb...	5ebf9d...		n/a	n/a	1/30/2007 5:48:...
Really Old Images		1511		Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RECYCLE.BIN\S-1-5-21-3166329-3263506726-1320359247-1000\$REZFRY8\Really Old I...	Folder	96 B	96 B				7/25/2007 7:41:...	9/26/2007 3:56:...	8/4/2007 12:04:...
Streetman.jpg		1510	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RECYCLE.BIN\S-1-5-21-3166329-3263506726-1320359247-1000\$REZFRY8\Streetman.jpg	JPEG	11.50 KB	11.44 KB	2c070e...	460af8...		7/25/2007 7:41:...	7/25/2007 7:41:...	7/24/2007 4:36:...
Super Old Images		1513		Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RECYCLE.BIN\S-1-5-21-3166329-3263506726-1320359247-1000\$REZFRY8\Really Old I...	Folder	512 B	512 B				7/25/2007 7:41:...	9/26/2007 3:56:...	8/4/2007 12:04:...
Thumbs.db		3710	db	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	Thumb...	n/a	76.50 KB	36870...	509efc...		n/a	n/a	1/13/2007 3:45...
validateCreditCard$1.cl...		3725	class	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	Java Cl...	n/a	436 B	f48ef4...	ee7c10...		n/a	n/a	1/1/2007 9:30:...
validateCreditCard$Car...		3726	class	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	Java Cl...	n/a	1479 B	76dee2...	8845a2...		n/a	n/a	1/1/2007 9:30:...
validateCreditCard$Car...		3727	class	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	Java Cl...	n/a	1124 B	0a440c...	f30318...		n/a	n/a	1/1/2007 9:30:...
validateCreditCard.class		3728	class	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	Java Cl...	n/a	17.87 KB	40f0b1...	20dc39...		n/a	n/a	1/1/2007 9:30:...
ValidateCreditCard.jar		3583	jar	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	Jar Exe	n/a	401.4 KB	fd0810...	ab6bfe...		n/a	n/a	1/13/2007 3:59:...
VCC_ABOUT.jpg		3711	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG E...	n/a	14.37 KB	1ecd40...	5d67ff...		n/a	n/a	1/13/2007 3:45:...
VISA.jpg		3712	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	9680 B	8de488...	8b49b2...		n/a	n/a	10/6/2006 10:5...
VISAGR.jpg		3713	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	7225 B	3758fb...	9de800...		n/a	n/a	10/6/2006 10:5...
woman.jpg		1509	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RECYCLE.BIN\S-1-5-21-3166329-3263506726-1320359247-1000\$REZFRY8\woman.jpg	JPEG	11.50 KB	11.35 KB	a2b9a0...	ed65a8...		7/25/2007 7:41:...	7/25/2007 7:41:...	7/24/2007 4:36:...

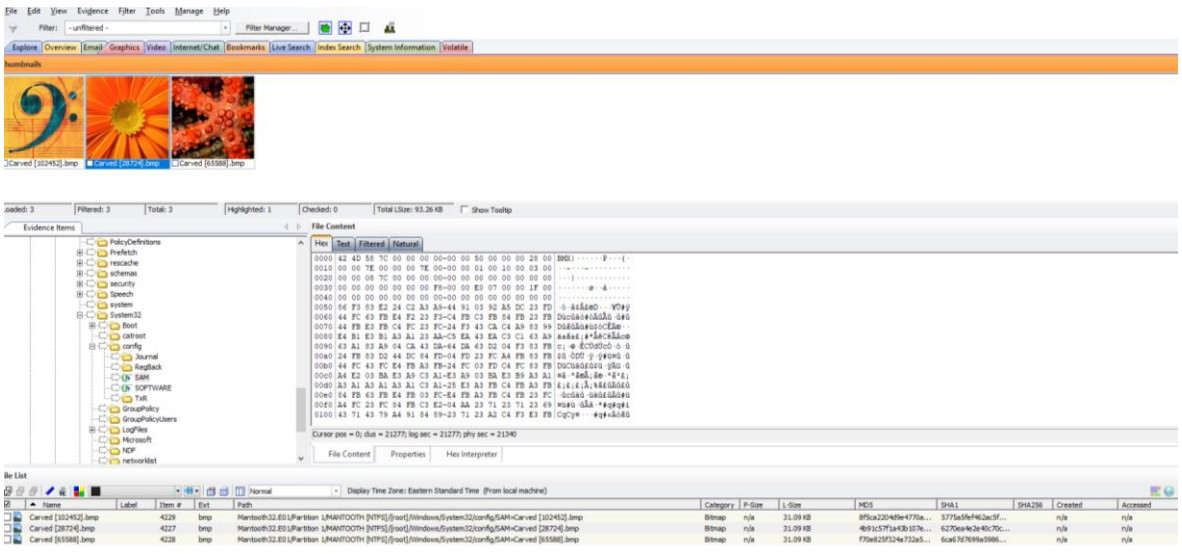


Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Carved [3603].jpeg		4300	jpeg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	1891 B	6c4514...	043486...		n/a	n/a	n/a
Carved [3626].jpeg		4289	jpeg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	1884 B	74d593...	0f251a...		n/a	n/a	n/a
Carved [466496].html		4239	html	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RECYCLE.BIN\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	HTML	n/a	13 B	b2a4bc...	1ae520...		n/a	n/a	n/a
Carved [8058].jpeg		4293	jpeg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	4203 B	d169ae...	21b67d...		n/a	n/a	n/a
Carved [8105].jpeg		4283	jpeg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	4276 B	fa7777...	ffc3be2...		n/a	n/a	n/a
Carved [8176].jpeg		4291	jpeg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	4299 B	992fb9...	9b4d73...		n/a	n/a	n/a
Carved [7409].html		4298	html	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	HTML	n/a	70 B	8806cc...	753efe...		n/a	n/a	n/a
Carved [822864].html		4240	html	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RECYCLE.BIN\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	HTML	n/a	152 B	fe3bfd...	1d2f99...		n/a	n/a	n/a
china.old_hmong_teeth....		1519	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RECYCLE.BIN\S-1-5-21-3166329-3263506726-1320359247-1000\$REZFRY8\china.old_h...	JPEG	39.50 KB	39.50 KB	f259eb...	4b69cb...		7/25/2007 7:41:...	7/25/2007 7:41:...	7/24/2007 4:35:...
chinamanbeard.jpg		1516	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RECYCLE.BIN\S-1-5-21-3166329-3263506726-1320359247-1000\$REZFRY8\Really Old I...	JPEG	39.00 KB	38.68 KB	f05c41...	efe9c9...		7/25/2007 7:41:...	7/25/2007 7:41:...	7/24/2007 4:33:...
DCI.jpg		3600	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	8889 B	ad3658...	a8bf4e...		n/a	n/a	10/6/2006 10:5...
DCIGR.jpg		3701	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	8070 B	e18626...	2912f5...		n/a	n/a	10/6/2006 10:5...
desktop.ini		1502	ini	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\desktop.ini	7 txt text	136 B	129 B	a526b9...	2df502...		2/27/2007 1:34:...	9/26/2007 3:56:...	2/27/2007 1:34:...
desktop.ini		1510	ini	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\desktop.ini	INDX E...	n/a	n/a				n/a	n/a	n/a
DISC.jpg		3702	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	14.82 KB	cbe899...	a33b43...		n/a	n/a	10/6/2006 10:5...
DISCGR.jpg		3703	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	10.76 KB	41088f...	e88ed1...		n/a	n/a	10/6/2006 10:5...
FILELIST.properties		3704	propert...	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	7 txt text	n/a	1389 B	1fa8fd...	2d7676...		n/a	n/a	10/9/2006 9:36...
FINGERPRINT.jpg		3705	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	78.81 KB	82d281...	5c9295...		n/a	n/a	10/6/2006 10:5...
go.jpg		3717	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG E...	n/a	16.80 KB	1c8874...	c5b31c...		n/a	n/a	10/9/2006 9:40...
go_press.jpg		3718	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG E...	n/a	15.46 KB	d609e1...	18d989...		n/a	n/a	10/9/2006 9:35...
go_roll.jpg		3719	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG E...	n/a	17.65 KB	d528c6...	e665bf...		n/a	n/a	10/9/2006 9:39...
JCB.jpg		3706	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	9332 B	a75e5e...	bc5863...		n/a	n/a	10/6/2006 10:5...
JCBGR.jpg		3707	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	7110 B	600e4c...	b5f0de...		n/a	n/a	10/6/2006 10:5...
MANIFEST.MF		3724	mf	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	7 txt text	n/a	112 B	2e7027...	ac1b80...		n/a	n/a	1/1/2007 9:33:...
MC.jpg		3708	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	12.93 KB	453256...	d88369...		n/a	n/a	10/6/2006 10:5...
MCGR.jpg		3709	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG	n/a	9823 B	206d91...	0013fa...		n/a	n/a	10/6/2006 10:5...
META-INF		3723		Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	Folder	n/a	0 B				n/a	n/a	1/13/2007 3:44...
old_people_illusion.jpg		1514	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RECYCLE.BIN\S-1-5-21-3166329-3263506726-1320359247-1000\$REZFRY8\Really Old I...	JPEG	29.50 KB	29.36 KB	9a28c5...	ce6e5f...		7/25/2007 7:41:...	7/25/2007 7:41:...	7/24/2007 4:32:...
old_peoples.jpg		1515	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RECYCLE.BIN\S-1-5-21-3166329-3263506726-1320359247-1000\$REZFRY8\Really Old I...	JPEG	174.0 KB	173.9 KB	83cd99...	e6cc56...		7/25/2007 7:41:...	7/25/2007 7:41:...	7/24/2007 4:33:...
optionIcon.jpg		3720	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG E...	n/a	16.65 KB	6e6e9c...	2f88f2...		n/a	n/a	10/4/2006 8:53:...
optionIconPressed.jpg		3721	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG E...	n/a	15.67 KB	dc2846...	13e032...		n/a	n/a	10/4/2006 8:58:...
optionIconRollover.jpg		3722	jpg	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3166329-3263506726-1320359247-1000\$RNHBWN2.zp>validat...	JPEG E...	n/a	17.57 KB	9affce...	49f138...		n/a	n/a	10/4/2006 8:57:...

12. Recover the user picture tile for Wes Mantooth's account. (Or tell me where it should be and that it isn't there – no credit for finding it, but I promise it is there)

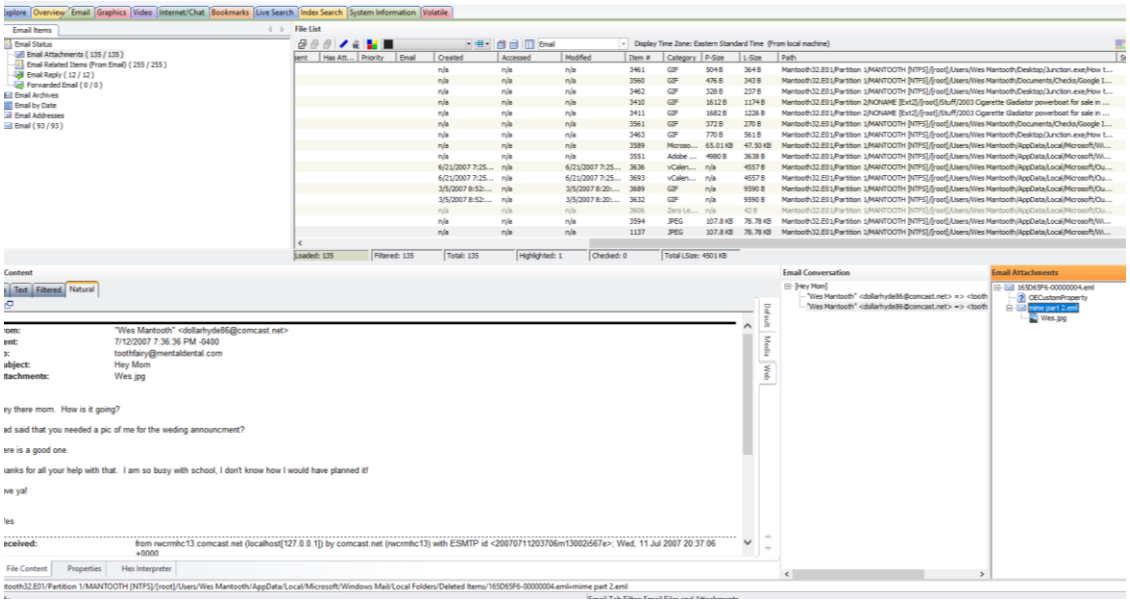
Opening up the SAM file in the registry viewer and checking out the UserTile value, gives me the hex of the user image tile that's supposed to be there. I also checked the SAM file in the graphics tab in FTK and I could see 3 carved files, and Hex value matching identified the User picture tile for Wes Mantooth's account. It is a picture of a sunflower.

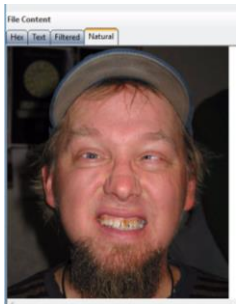




13. Identify any pictures of Wes Mantooth.

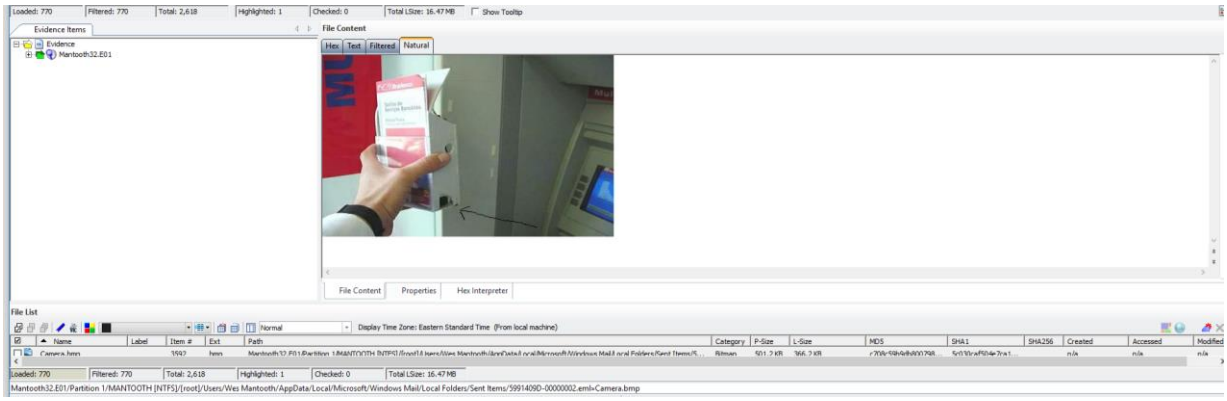
While surfing through emails, I found one email from the defendant which was sent to his mother. Also, a picture file, attachment was found with the mail which is named “wes.jpg”. This is as said by Wes Mantooth, his own photo for printing on wedding announcement.

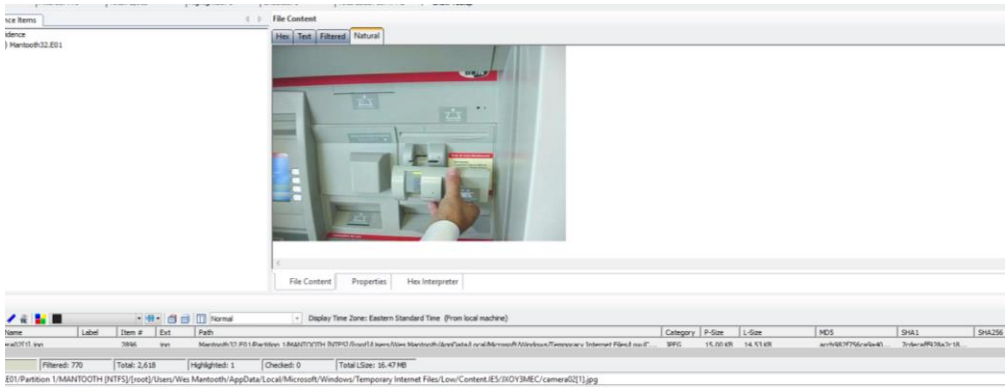




14. Identify any pictures related to the fraud or financial crimes mentioned above.

While examining the image on various tabs, I found the following pictures which were related to financial crimes.



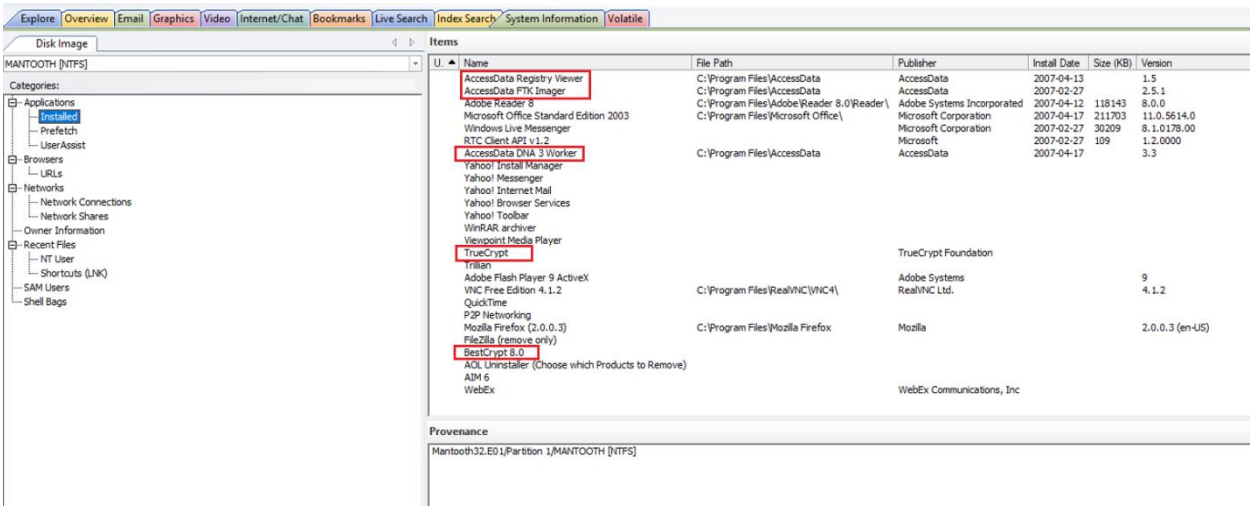


\

15. Identify any software that could be used to encrypt, obscure or forensically analyze data, or defeat forensics.

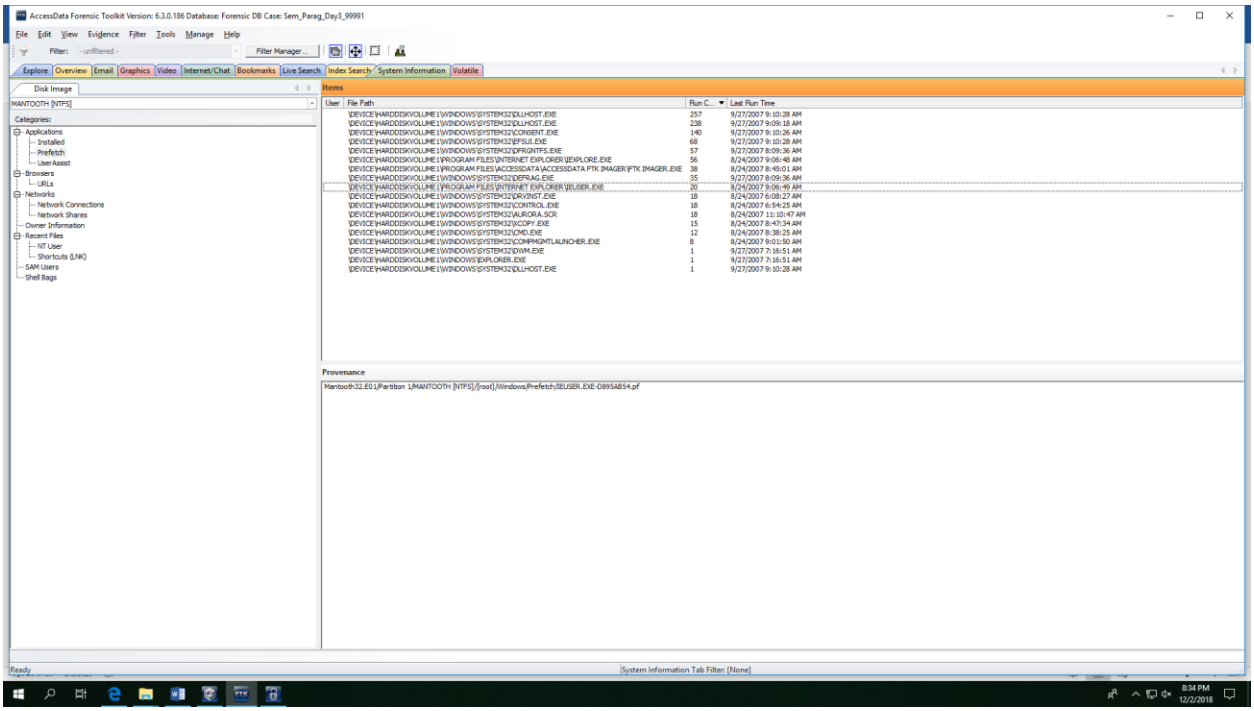
The following softwares can be used to encryt, obsure or forensically anazyze data or defeat forensics.

AccessData Registry Viewer, AccessData FTK Imager, AccessData DNA 3 Worker, Truecrypt, BestCrypt 8.0



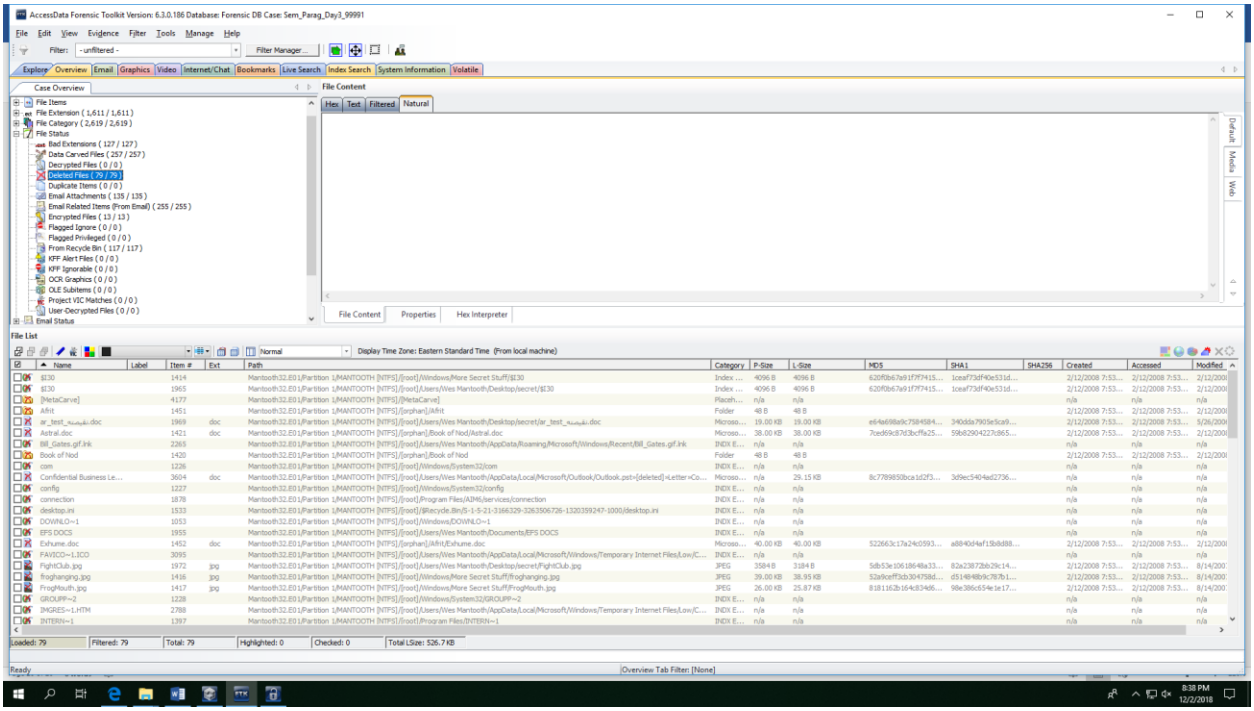
16. Identify the most commonly opened programs

The most commonly opened programs can be viewed in the prefetch. The FTK tool provides a direct access to the contents of the prefetch and as seen in the screen shot below, there is a list of programs in descending order of their frequency of being launched. From the list, user launch able programs, Internet Explorer is the most opened program with 56 launches.



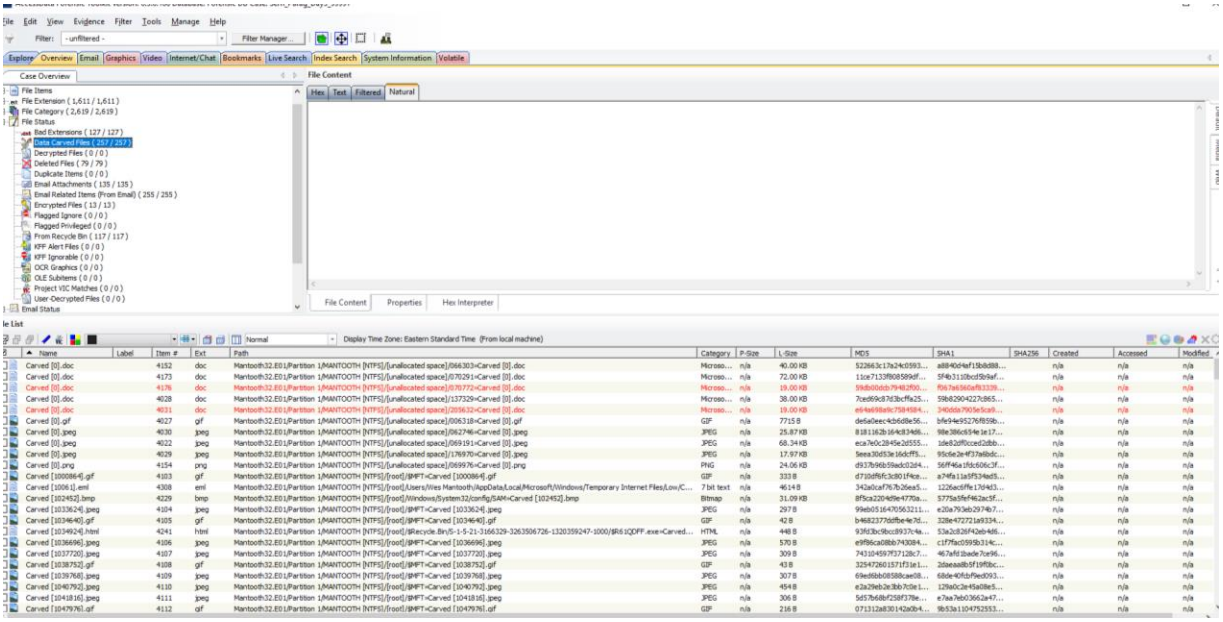
17. Provide total number of deleted files.

Using the FTK's Case Overview section, in the Deleted files, 79 files were found as listed in the screenshot below.



18. Perform a file carving and find total number of carved files found.

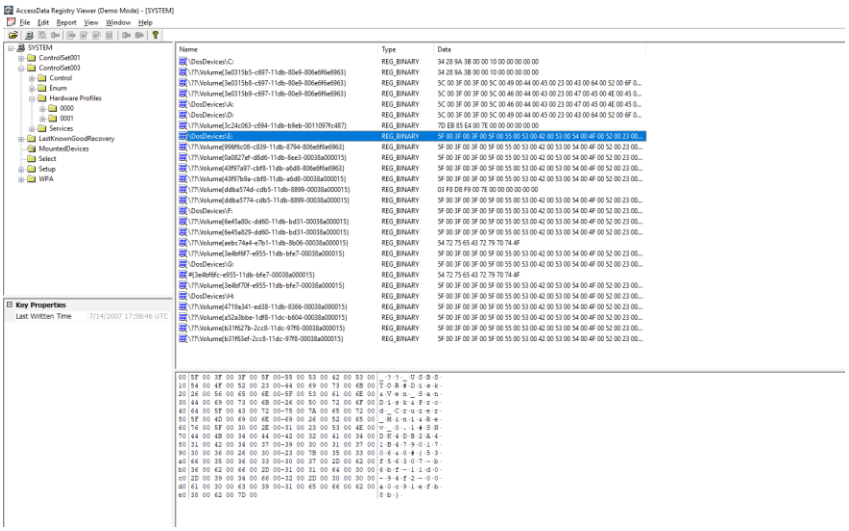
As seen in the screenshot below, FTK has carved 257 files, all of which are listed in the window.



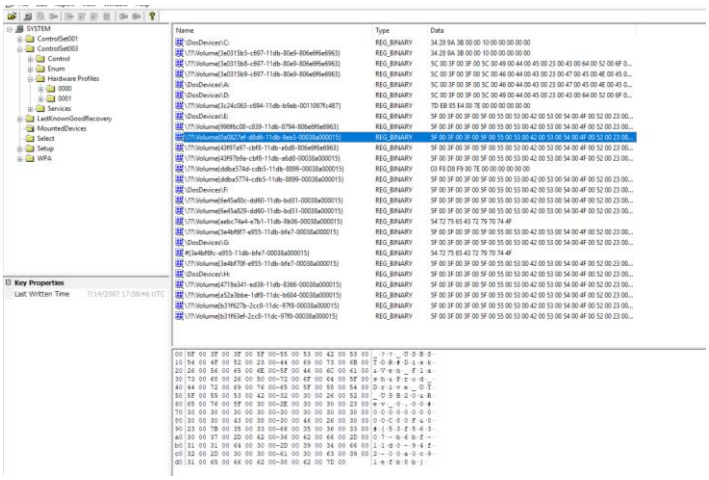
19. Identify any cameras, USB drives or other devices that have been attached to the computer.

After exporting the SYSTEM file from FTK and launching it in Registry viewer, you can find the Mounted Devices section where all the connected/disconnected devices are listed. Some of them are listed below with screenshots:

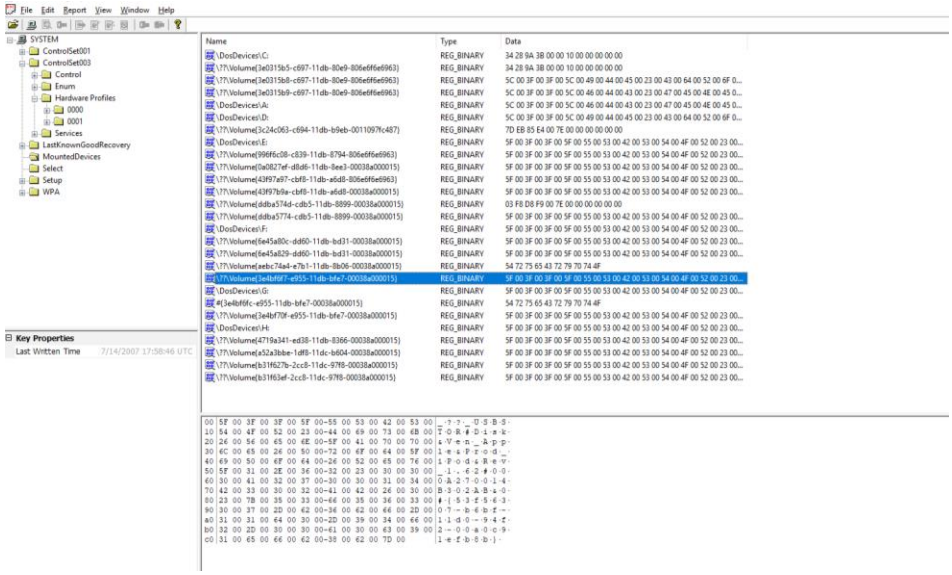
1. USBSTOR#Disk&Ven_SanDisk&Prod_Cruzer_Mini



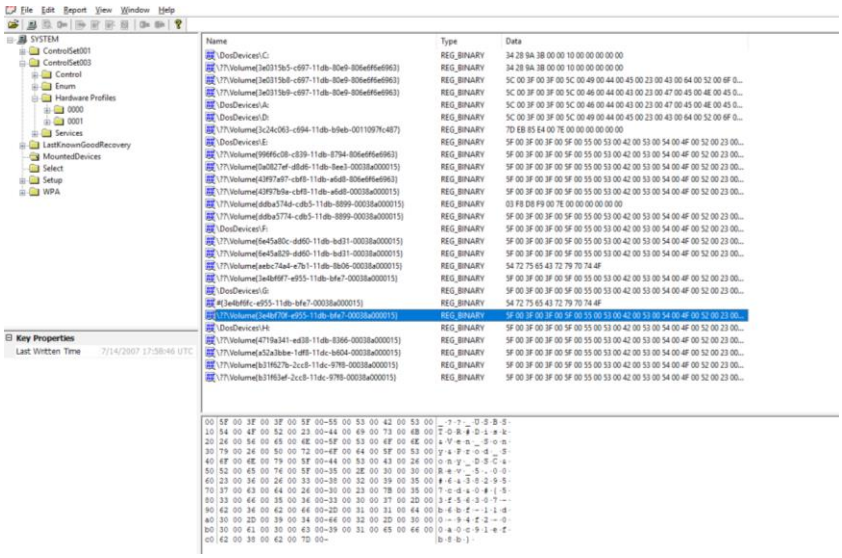
2. USBSTOR#Disk&Ven_Flash&ProdDrive_UT



3. Apple iPod

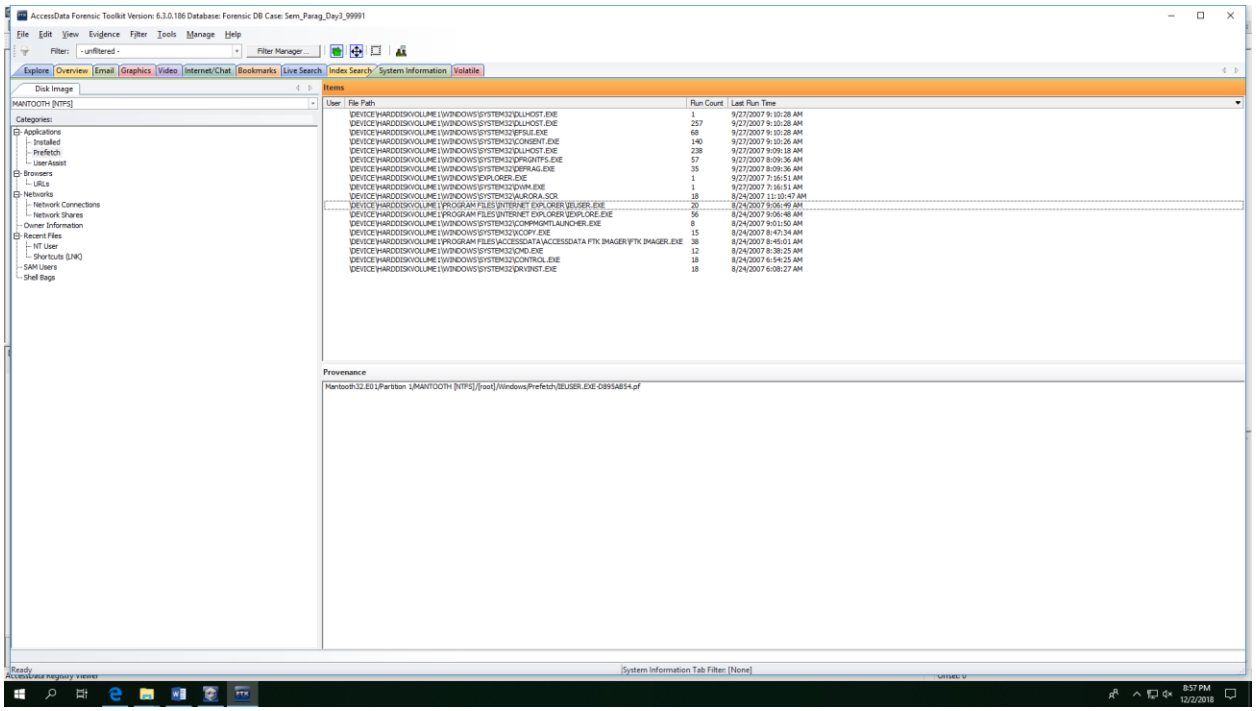


4. USBSTOR#Disk&Ven_Sony_DSC



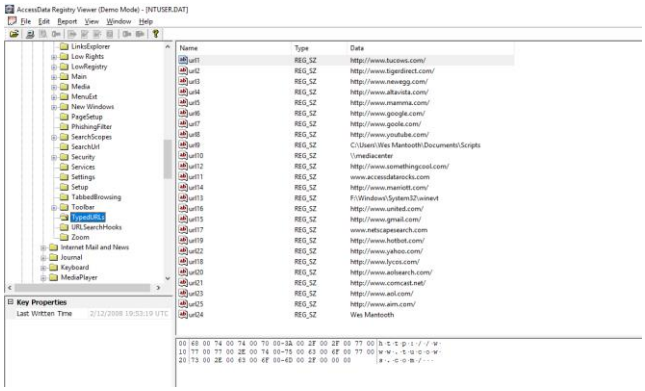
20. Identify the most recently run programs.

The prefetch can tell us the most recently run programs with their run count and when a particular executable was launched for the past 8 times. In the screenshot below, all the executables are in the descending order (most recently launched first in the list)



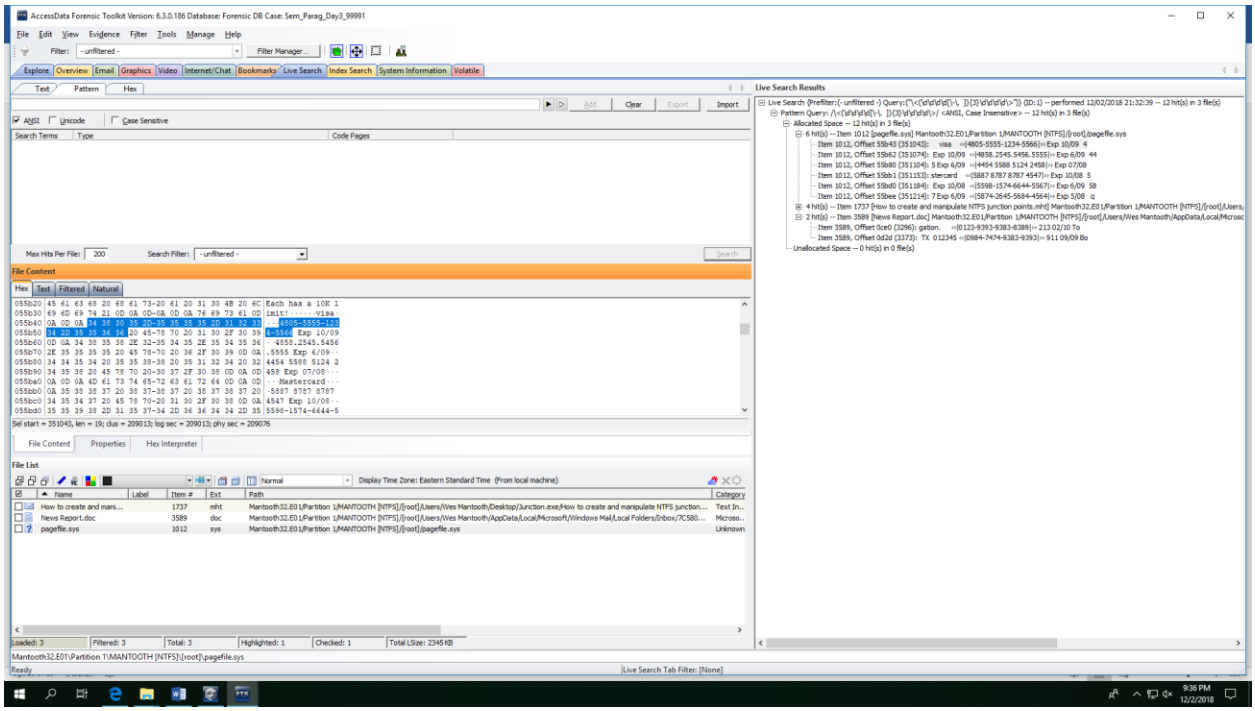
21. Identify any URLs that were visited by manually typing the address.

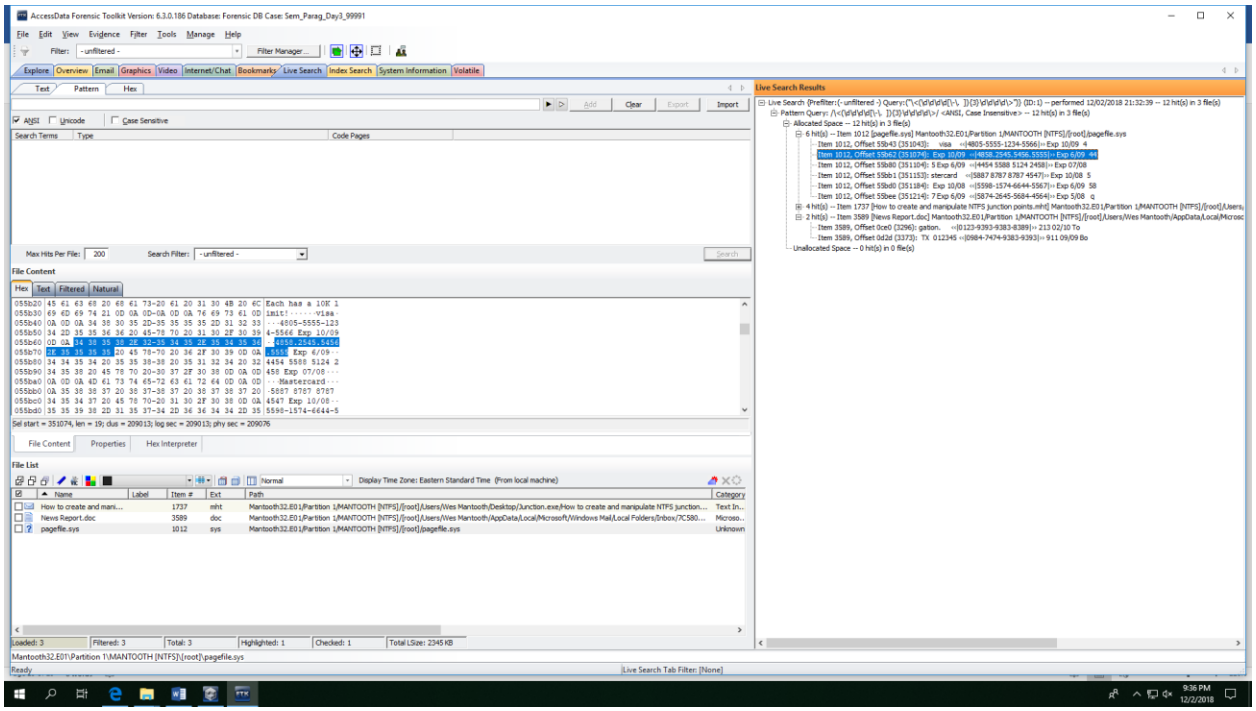
The NTUSER.dat has a section called “TypedURLs” where all the urls that were typed and entered into the browser are stored. Below is a screenshot of the same.

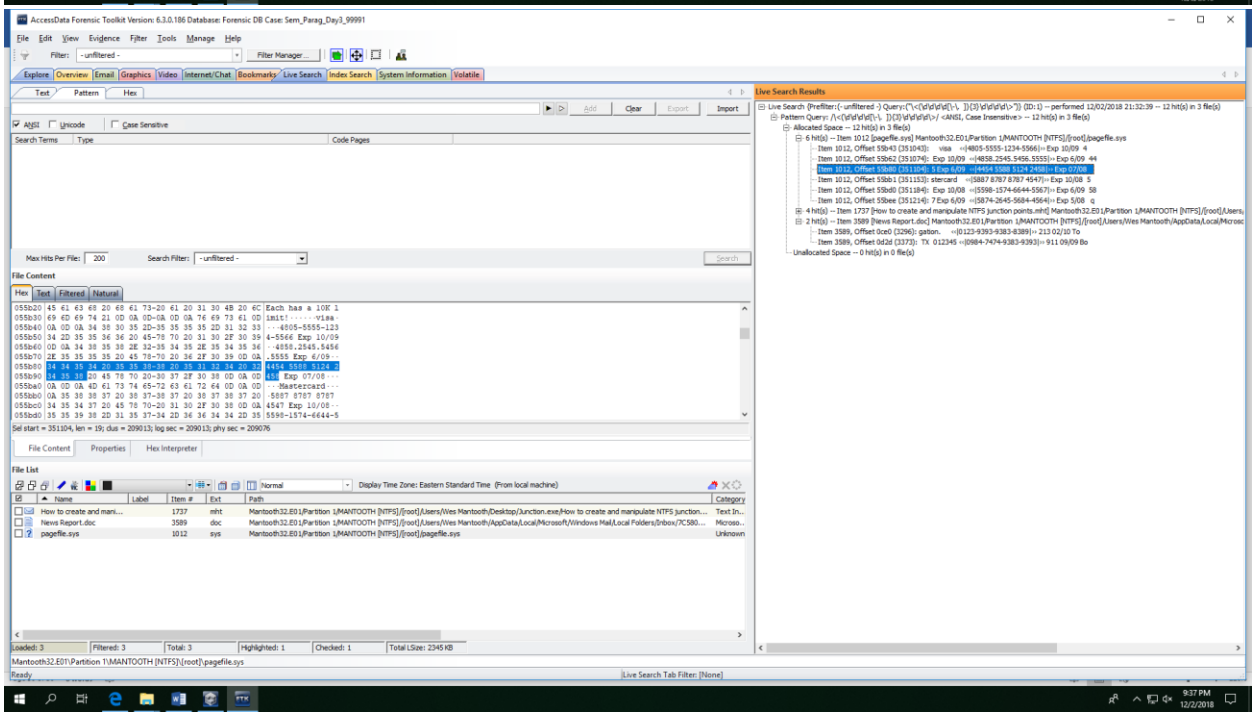


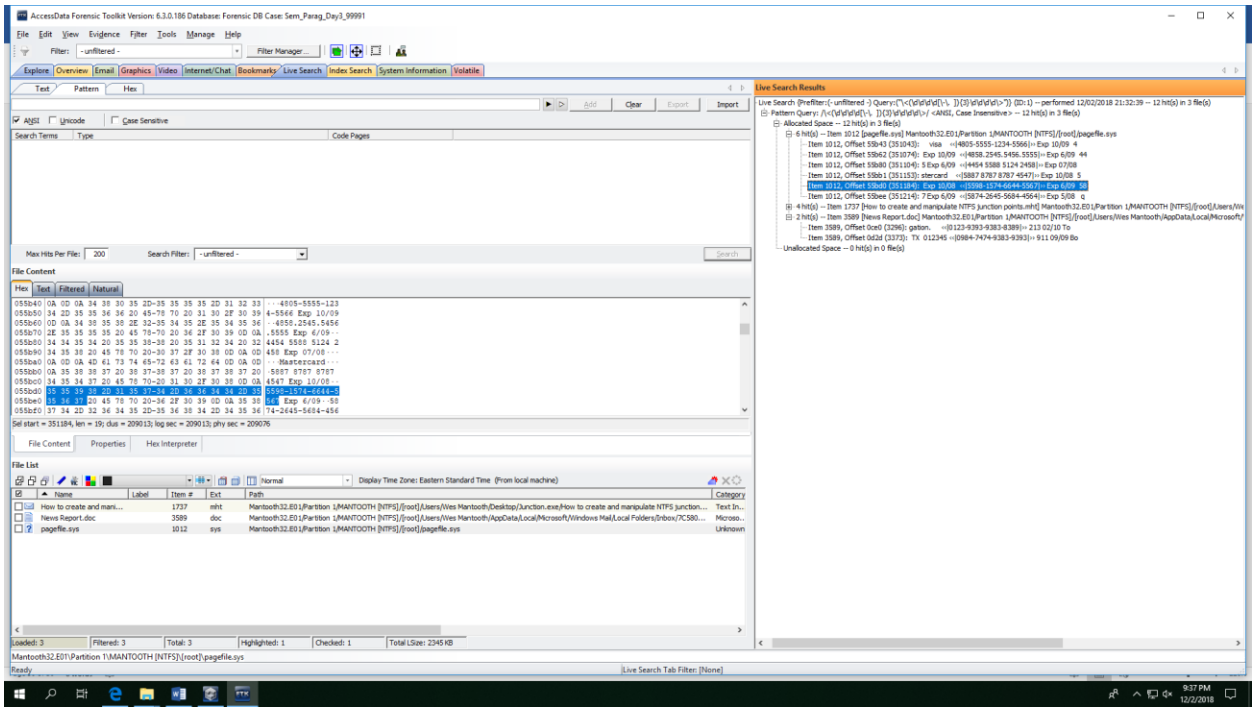
22. Identify any credit card numbers on the drive. (This will require live search with a regular expression)

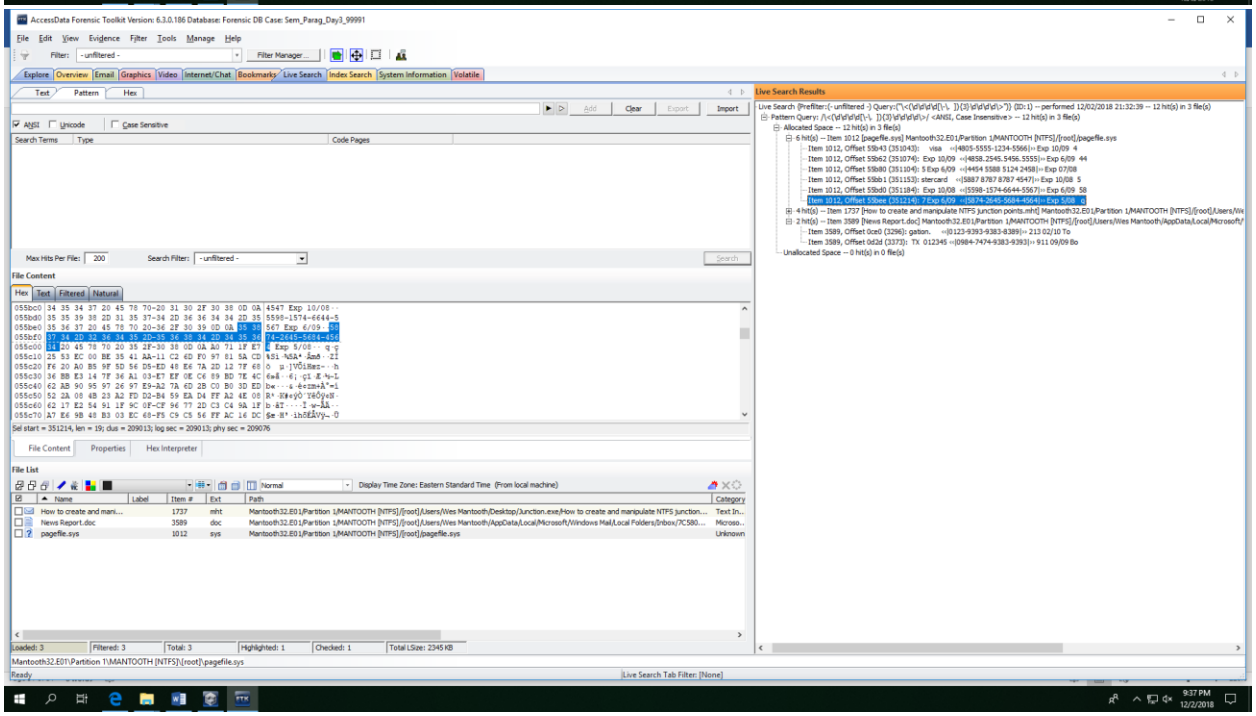
I made user of Live Search in FTK and used pattern search that is pre built with Credit Card query pattern to find Credit card information. Below are screenshots of the same.

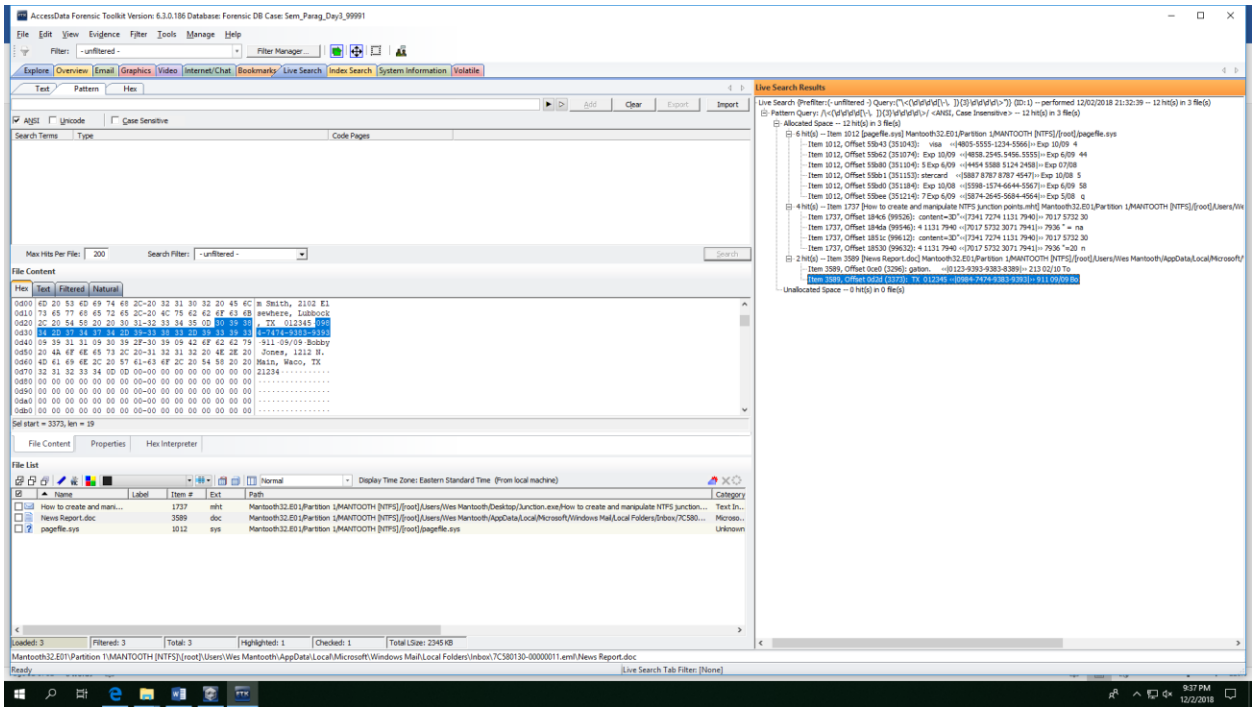

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Sem_Parag_Day3_99991
File Edit View Evidence Filter Tools Manage Help
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Live Search Results
File Content
File List
Ready


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Sem_Parag_Day3_99991
Live Search Results
Each has a 10K l
imit! · · · · visa ·
· · 4805-5555-123
4-5566 Exp 10/09
· · 4858.2545.5456
5555 Exp 6/09 · ·
4454 5588 5124 2
458 Exp 07/08 · · ·
· · Mastercard · · ·
· 5887 8787 8787
4547 Exp 10/08 · ·
5598-1574-6644-5
Sel start = 351074, len = 19; dus = 209013; log sec = 209013; phy sec = 209076
How to create and mani...
News Report.doc
pagefile.sys
9:36 PM
12/2/2018


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Sem_Parag_Day3_99991
Live Search Results
Each has a 10K l
imit! · · · · visa ·
· · 4805-5555-123
4-5566 Exp 10/09
· · 4858.2545.5456
5555 Exp 6/09 · ·
4454 5588 5124 2
458 Exp 07/08 · · ·
· · Mastercard · · ·
· 5887 8787 8787
4547 Exp 10/08 · ·
5598-1574-6644-5
Sel start = 351104, len = 19; dus = 209013; log sec = 209013; phy sec = 209076
How to create and mani...
News Report.doc
pagefile.sys
9:37 PM
12/2/2018

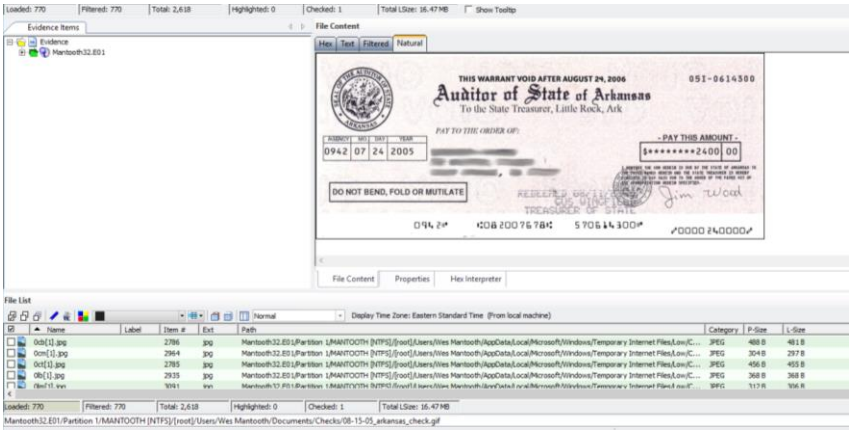

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Sem_Parag_Day3_99991
Live Search Results
File Content
File List
9:37 PM
12/2/2018

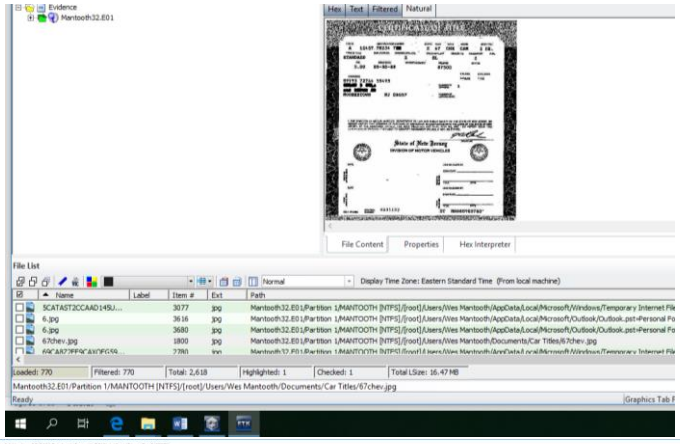

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Sem_Parag_Day3_99991
Live Search Results
File Content
File List
9:37 PM
12/2/2018

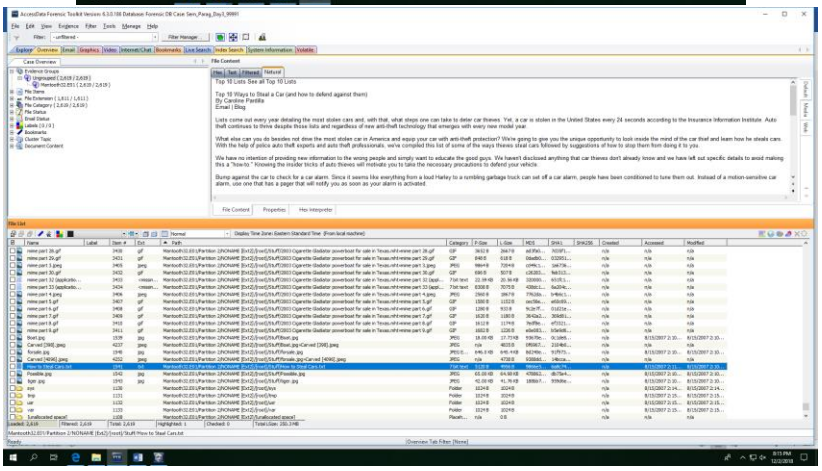


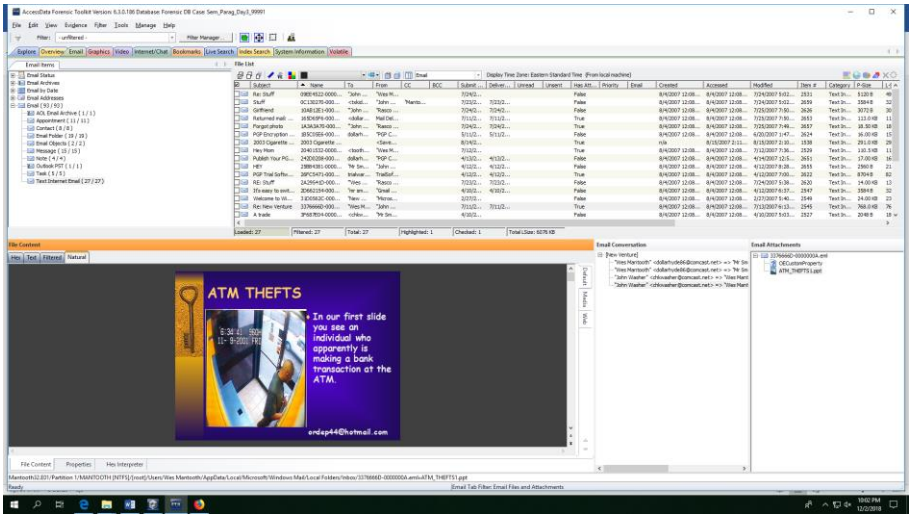
23. Detective Ketchum has provided a list of search terms: Theft, Title, Checks, Scam, and Forensics. Provide ONLY (a few examples of) results of these that you believe may be relevant.

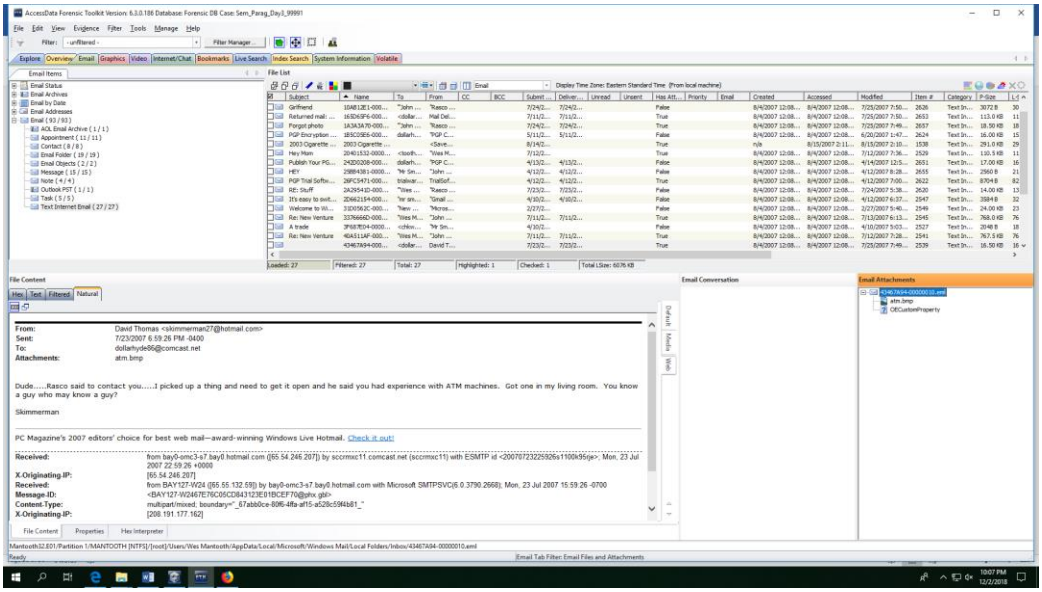
Some of the other evidence which I found relevant to the above terminologies are below:



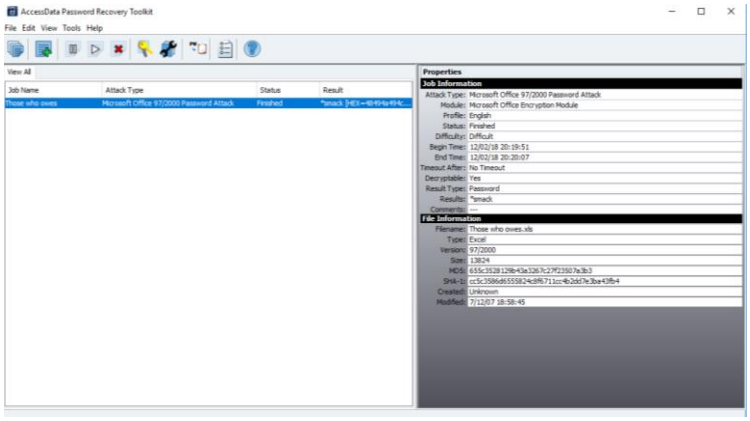


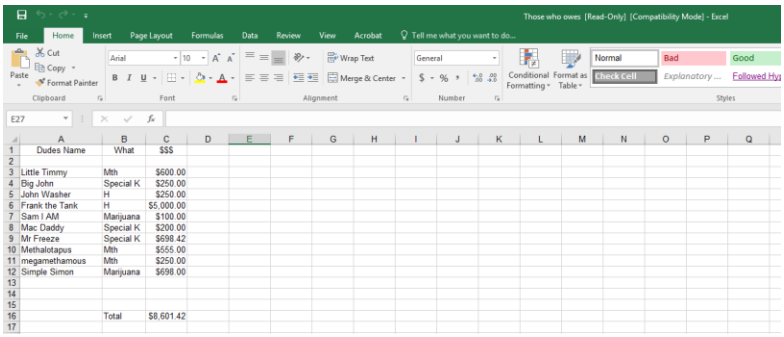



ATM THEFTS
In our first slide you see an individual who apparently is making a bank transaction at the ATM.
erdap44@hotmail.com



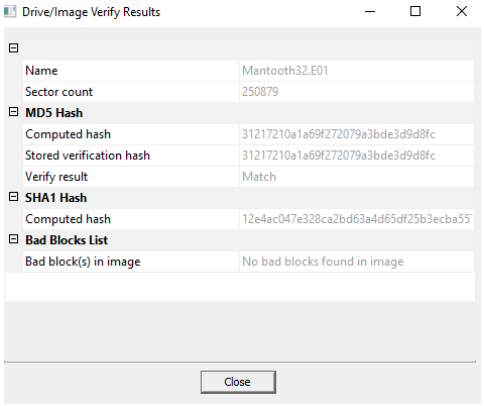
I also found one password protected .xml file which I cracked using PRTK as shown below:





	A	B	C
1	Dudes Name	What	$$$
2			
3	Little Timmy	Mth	$600.00
4	Big John	Special K	$250.00
5	John Washer	H	$250.00
6	Frank the Tank	H	$5,000.00
7	Sam I AM	Marijuana	$100.00
8	Mac Daddy	Special K	$200.00
9	Mr Freeze	Special K	$698.42
10	Methalotapus	Mth	$555.00
11	megamethamous	Mth	$250.00
12	Simple Simon	Marijuana	$698.00
13			
14			
15			
16		Total	$8,601.42
17			

Finally, I hashed the image file again to verify if there was any tampering after we acquired the image.



Conclusion:

In this case, I examined the forensic image given to me by Detective Ketchum and I performed various different tasks to find out the information for the report. I found the user passwords, understood which user logged on the most, also which OS and service pack is it running. I also, found evidence related to Mantooth's case. Moreover, I also identified recently run programs, recovered credit card info numbers, etc. I performed hash verification twice in this project to ensure the integrity during the acquisition and after performance.