11/16/2025

Washer Report

Report by Anthony Smithmyer

Executive Summary

The main user on this Windows XP computer is the Administrator account. The owner of the computer is John Washer. This person is involved in various illegal activities such as check washing (which is the process of stealing checks and erasing details on the check with chemicals to be used by the criminal), drug dealing, and credit/debit card stealing, as shown through various emails, files, and web searches on the computer. Some of these activities are conducted with the help of Wes Mantooth, Rasco Badguy, and other possible suspects involved in a similar case. John has a more advanced understanding of computers because there are encrypted files on his computer. Encryption means a file is protected with a password and only people who know the password can view the file. The encrypted files contain stolen credit cards and directions to a possible hideout location. The computer is set to Eastern Time. Additionally, there are deleted files indicating illicit activities on the computer that were recovered.

Methods

Tools used:

- Autopsy 4.22.1 (The latest version)
- Windows Registry Explorer
- Windows Event Viewer
- PicPick Screenshot Tool
- Kali Linux

The process:

I downloaded the disk image of Washer's computer and started a new case in Autopsy 4.22.1. I selected the disk image as a data source. I began to look through the files on the image to find evidence of crimes and connections to Mantooth.

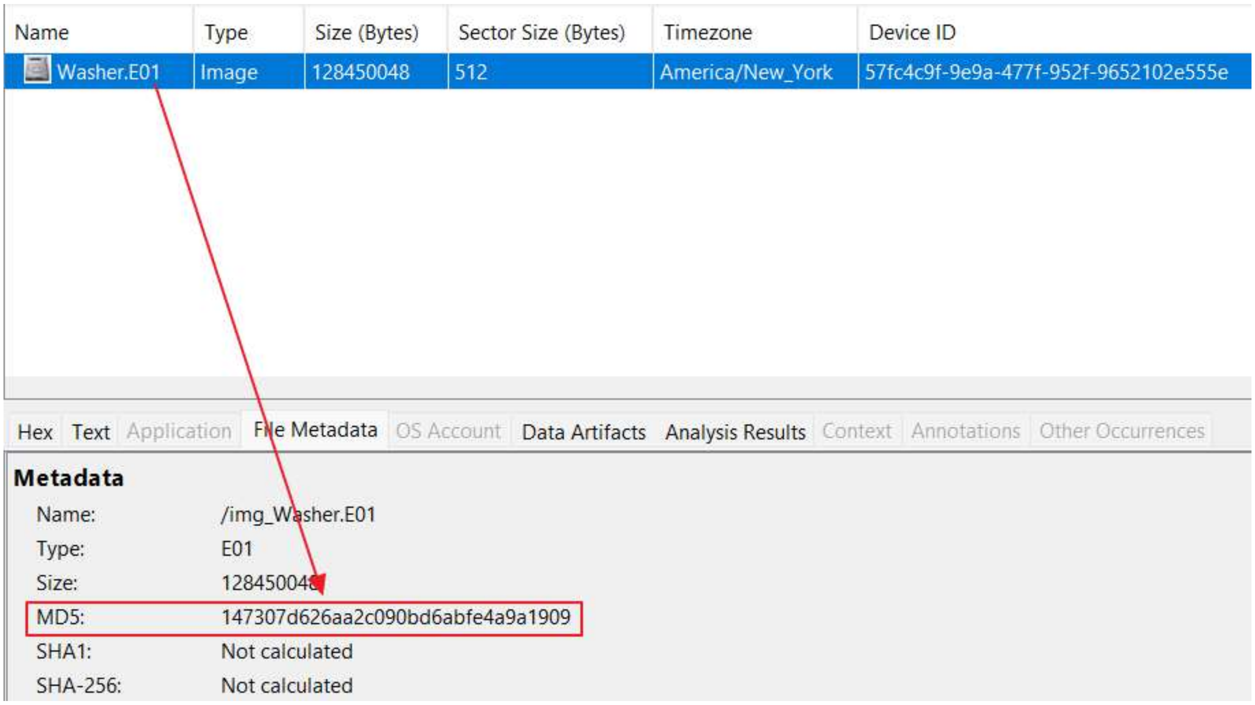
Verification:

I verified the evidence and artifacts by using the built-in data artifacts section in Autopsy, finding evidence within the files on the disk image, and exploring the registry hives in Registry Explorer.

Findings

Before investigating the disk image for evidence of illegal activities, I verified the MD5 hash of the image to ensure that the image wasn't tampered with. A different file hash indicates that something within the disk image was changed. The file hash listed in the Washer.E01.txt file is 147307d626aa2c090bd6abfe4a9a1909. Using Autopsy, I went to Data

Sources > Washer.E01_1 Host and single-clicked on Washer.E01 in the right pane. The hash of the disk image is listed in the "File Metadata" section below. As shown in Figures 1 and 2, the file hash is the same, meaning the disk image has not been tampered with.

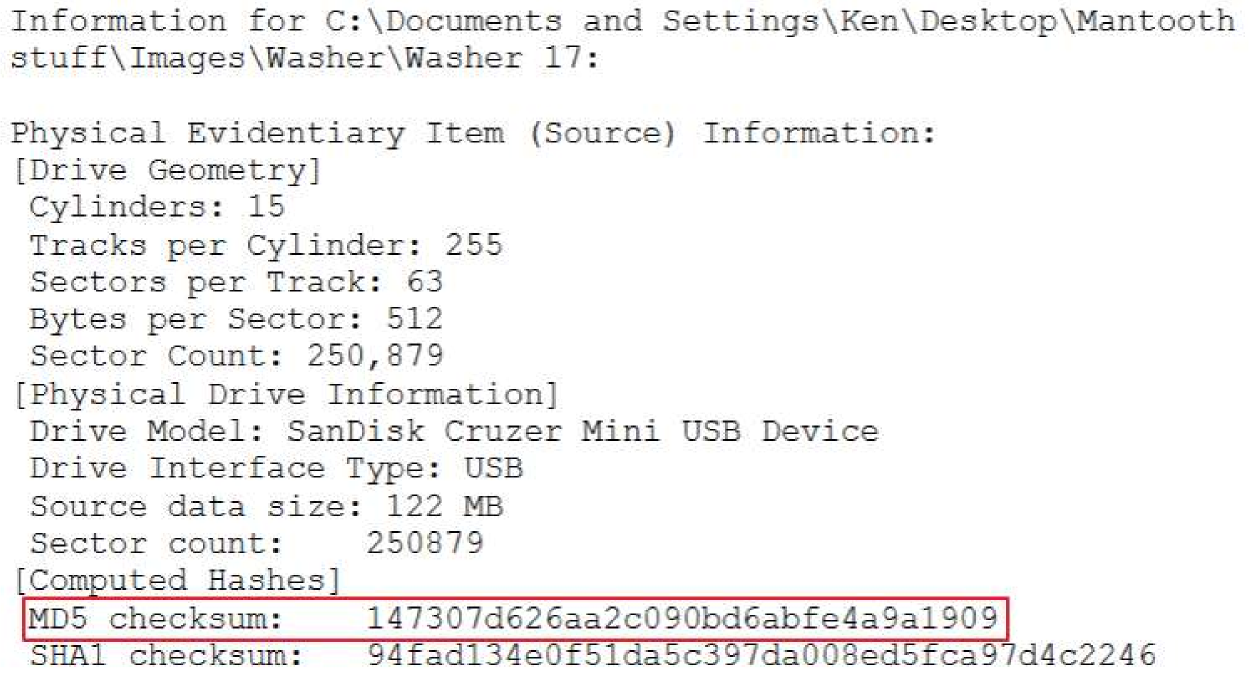


Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
Washer.E01	Image	128450048	512	America/New_York	57fc4c9f-9e9a-477f-952f-9652102e555e

Metadata

Name:	/img_Washer.E01
Type:	E01
Size:	128450048
MD5:	147307d626aa2c090bd6abfe4a9a1909
SHA1:	Not calculated
SHA-256:	Not calculated

Figure 1: File hash of Washer.E01 in Autopsy

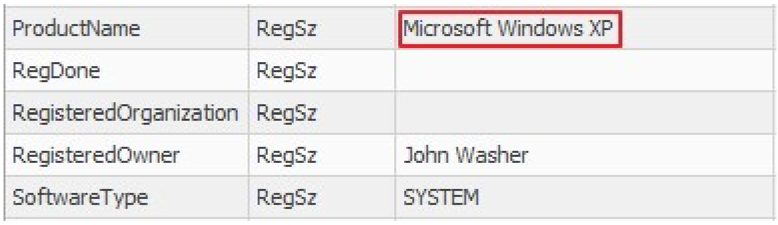


```
Information for C:\Documents and Settings\Ken\Desktop\Mantooth
stuff\Images\Washer\Washer 17:

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
 Cylinders: 15
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 250,879
[Physical Drive Information]
 Drive Model: SanDisk Cruzer Mini USB Device
 Drive Interface Type: USB
 Source data size: 122 MB
 Sector count:    250879
[Computed Hashes]
 MD5 checksum:    147307d626aa2c090bd6abfe4a9a1909
 SHA1 checksum:   94fad134e0f51da5c397da008ed5fca97d4c2246
```

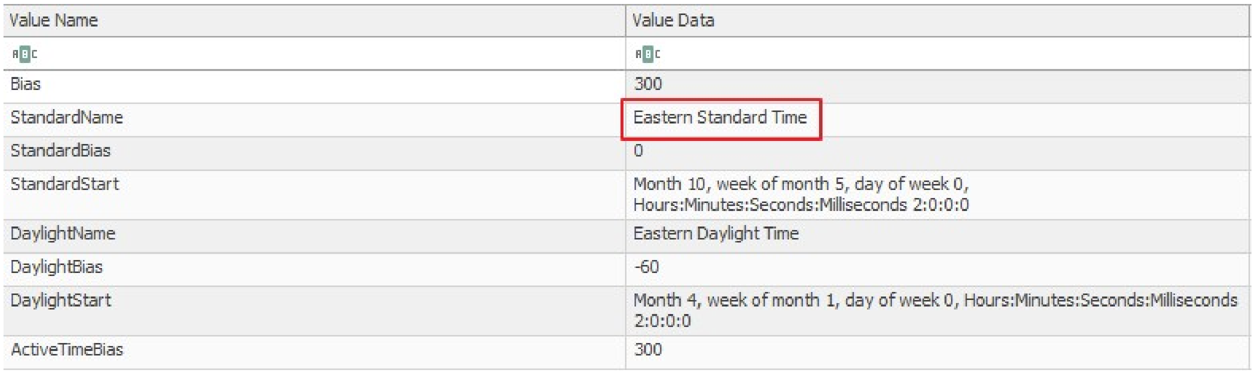
Figure 2: File hash of Washer.E01 in the associated text document

Once the file hashes were verified, I began to look through the file system. Using Registry Explorer, I discovered that Windows XP is the operating system on John Washer's computer. I also found that the computer is set to Eastern Time. This is shown in Figures 3 and 4.



ProductName	RegSz	Microsoft Windows XP
RegDone	RegSz	
RegisteredOrganization	RegSz	
RegisteredOwner	RegSz	John Washer
SoftwareType	RegSz	SYSTEM

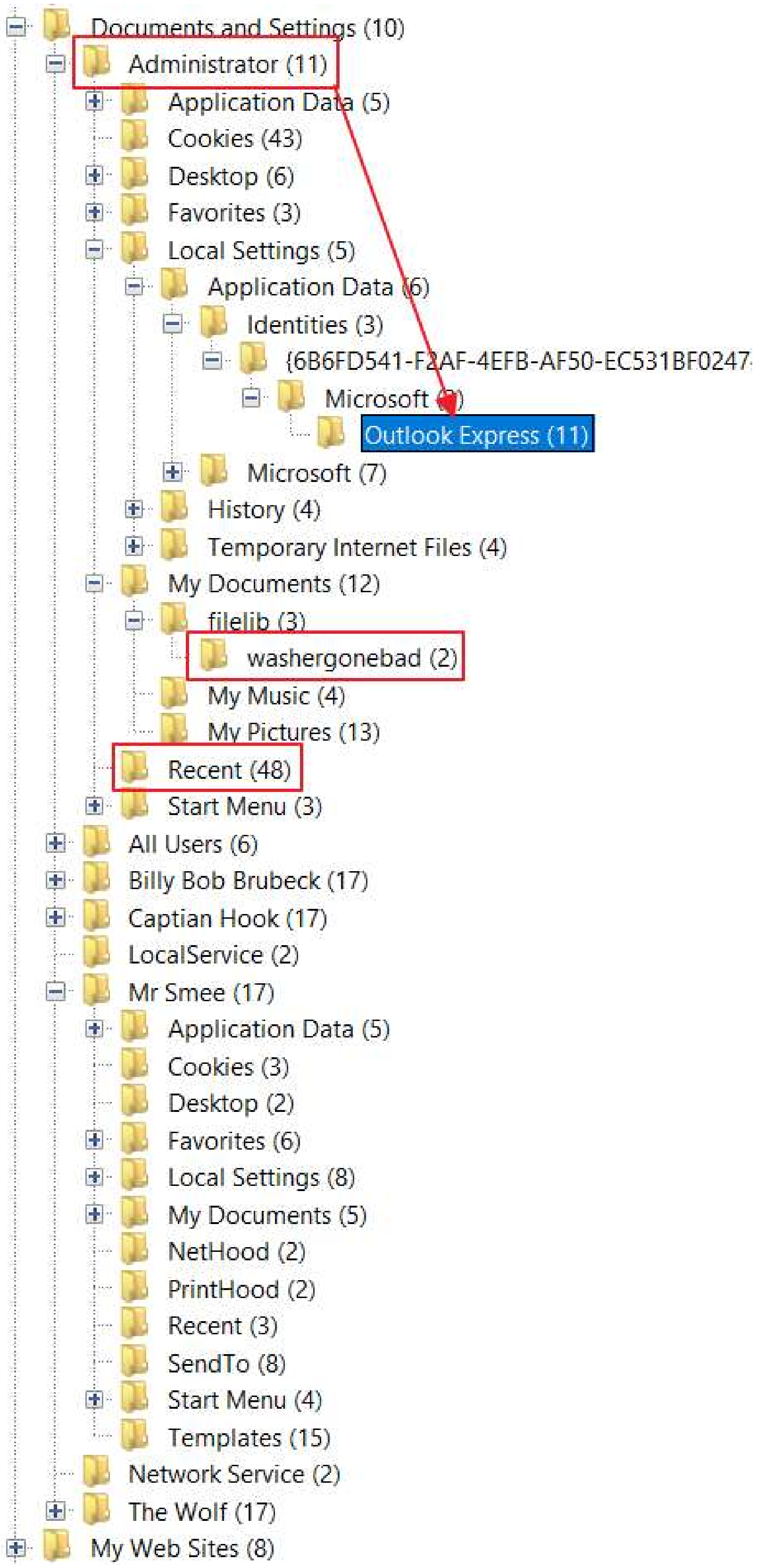
Figure 3: Operating System Information



Value Name	Value Data
ABC	ABC
Bias	300
StandardName	Eastern Standard Time
StandardBias	0
StandardStart	Month 10, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
DaylightName	Eastern Daylight Time
DaylightBias	-60
DaylightStart	Month 4, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
ActiveTimeBias	300

Figure 4: Time Zone Information

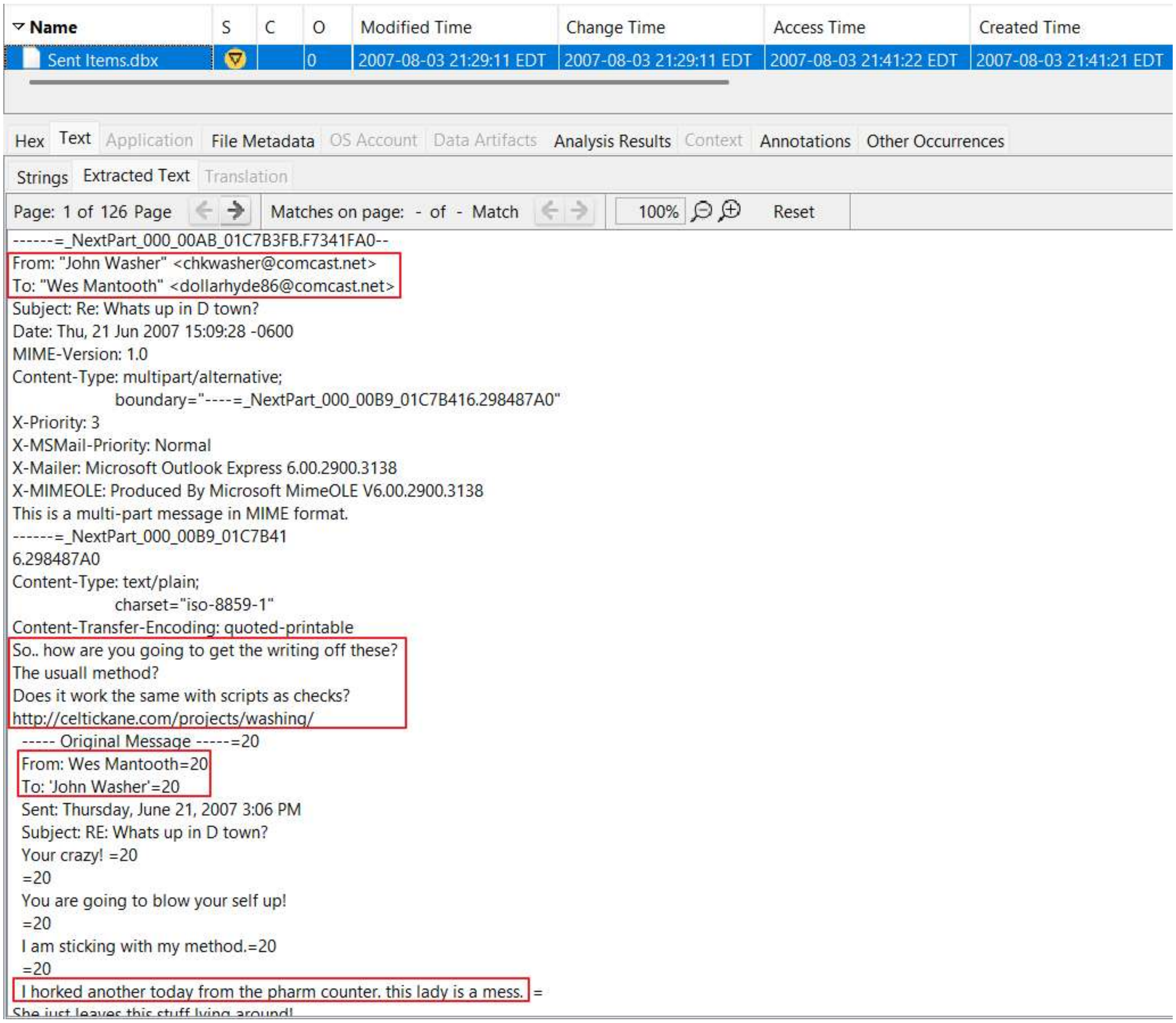
I found that the main user on this computer is the Administrator account. I determined this because it contains Washer's Outlook files, a folder titled "washergonebad", and recent files. The other user folders did not have any noticeable evidence relevant to the case.



```
Documents and Settings (10)
    Administrator (11)
        Application Data (5)
        Cookies (43)
        Desktop (6)
        Favorites (3)
        Local Settings (5)
            Application Data (6)
                Identities (3)
                    {6B6FD541-F2AF-4EFB-AF50-EC531BF0247
                        Microsoft ([illegible])
                            Outlook Express (11)
                Microsoft (7)
            History (4)
            Temporary Internet Files (4)
        My Documents (12)
            filelib (3)
                washergonebad (2)
            My Music (4)
            My Pictures (13)
        Recent (48)
        Start Menu (3)
    All Users (6)
    Billy Bob Brubeck (17)
    Captian Hook (17)
    LocalService (2)
    Mr Smee (17)
        Application Data (5)
        Cookies (3)
        Desktop (2)
        Favorites (6)
        Local Settings (8)
        My Documents (5)
        NetHood (2)
        PrintHood (2)
        Recent (3)
        SendTo (8)
        Start Menu (4)
        Templates (15)
    Network Service (2)
    The Wolf (17)
My Web Sites (8)
```

Figure 5: User folders in Autopsy

I looked through the inbox, sent items, and deleted items on Outlook and found several interactions between John Washer (chkwasher@comcast.net) and Wes Mantooth (dollarhyde86@comcast.net). The email in Figure 6 shows Mantooth and Washer conspiring to steal and wash checks, which is the process of removing the ink from a check to use for your own benefit.

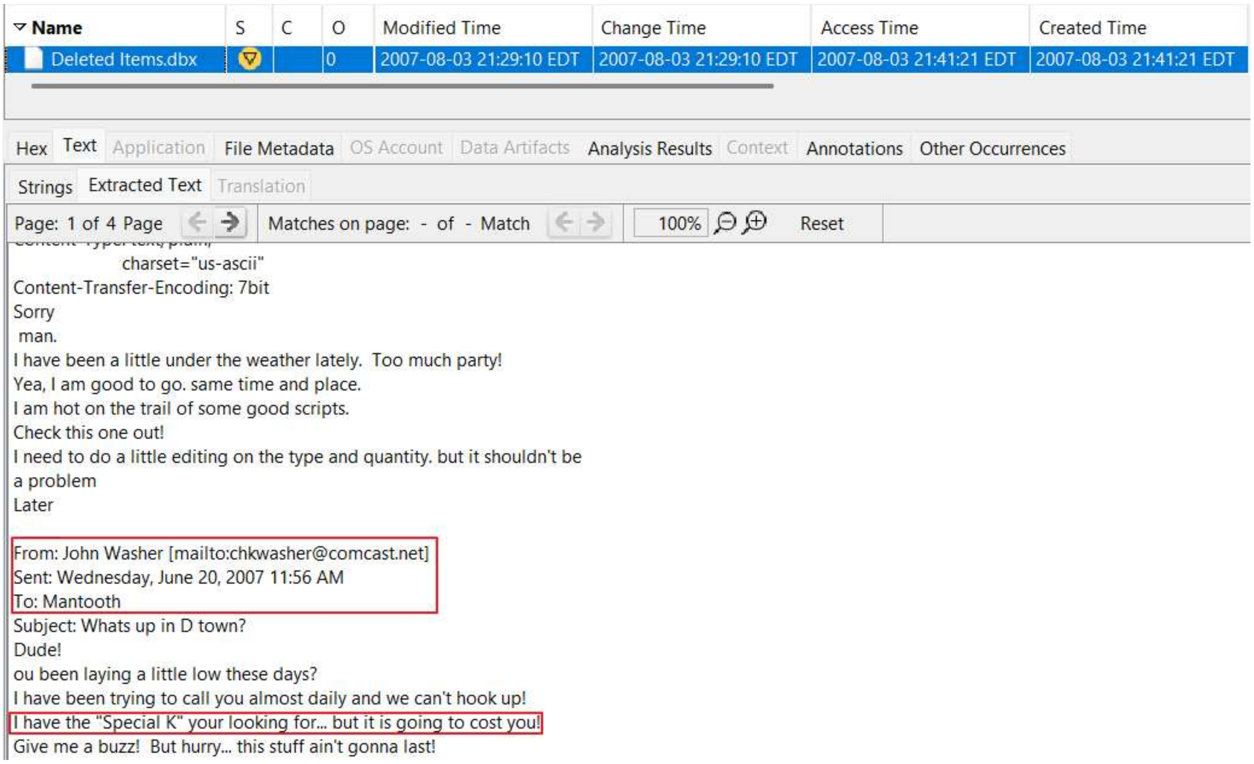


Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Sent Items.dbx			0	2007-08-03 21:29:11 EDT	2007-08-03 21:29:11 EDT	2007-08-03 21:41:22 EDT	2007-08-03 21:41:21 EDT

```
------=_NextPart_000_00AB_01C7B3FB.F7341FA0--
From: "John Washer" <chkwasher@comcast.net>
To: "Wes Mantooth" <dollarhyde86@comcast.net>
Subject: Re: Whats up in D town?
Date: Thu, 21 Jun 2007 15:09:28 -0600
MIME-Version: 1.0
Content-Type: multipart/alternative;
              boundary="----=_NextPart_000_00B9_01C7B416.298487A0"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.3138
X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2900.3138
This is a multi-part message in MIME format.
------=_NextPart_000_00B9_01C7B41
6.298487A0
Content-Type: text/plain;
              charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
So.. how are you going to get the writing off these?
The usuall method?
Does it work the same with scripts as checks?
http://celtickane.com/projects/washing/
 ----- Original Message -----=20
 From: Wes Mantooth=20
 To: 'John Washer'=20
 Sent: Thursday, June 21, 2007 3:06 PM
 Subject: RE: Whats up in D town?
 Your crazy! =20
 =20
 You are going to blow your self up!
 =20
 I am sticking with my method.=20
 =20
 I horked another today from the pharm counter. this lady is a mess. =
She just leaves this stuff lying around!
```

Figure 6: Check washing email

I also discovered a deleted email between Washer and Mantooth depicting drug dealing. This is shown below in Figure 7.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Deleted Items.dbx	▽		0	2007-08-03 21:29:10 EDT	2007-08-03 21:29:10 EDT	2007-08-03 21:41:21 EDT	2007-08-03 21:41:21 EDT

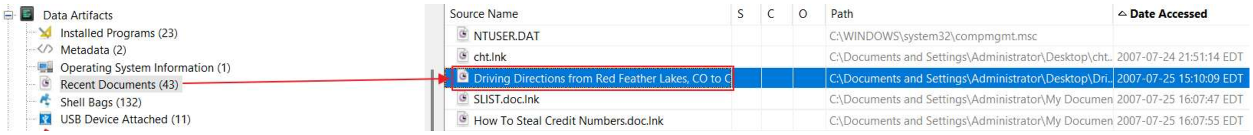
```
            charset="us-ascii"
Content-Transfer-Encoding: 7bit
Sorry
 man.
I have been a little under the weather lately.  Too much party!
Yea, I am good to go. same time and place.
I am hot on the trail of some good scripts.
Check this one out!
I need to do a little editing on the type and quantity. but it shouldn't be
a problem
Later

From: John Washer [mailto:chkwasher@comcast.net]
Sent: Wednesday, June 20, 2007 11:56 AM
To: Mantooth
Subject: Whats up in D town?
Dude!
ou been laying a little low these days?
I have been trying to call you almost daily and we can't hook up!
I have the "Special K" your looking for... but it is going to cost you!
Give me a buzz!  But hurry... this stuff ain't gonna last!
```

Figure 7: Drug dealing email

There were also emails between Washer and other possible suspects related to Mantooth, such as Rasco Badguy (txkidd@swbell.net), David Thomas (skimmerman27@hotmail.com), and Mr. Smee (smee.rox@gmail.com).

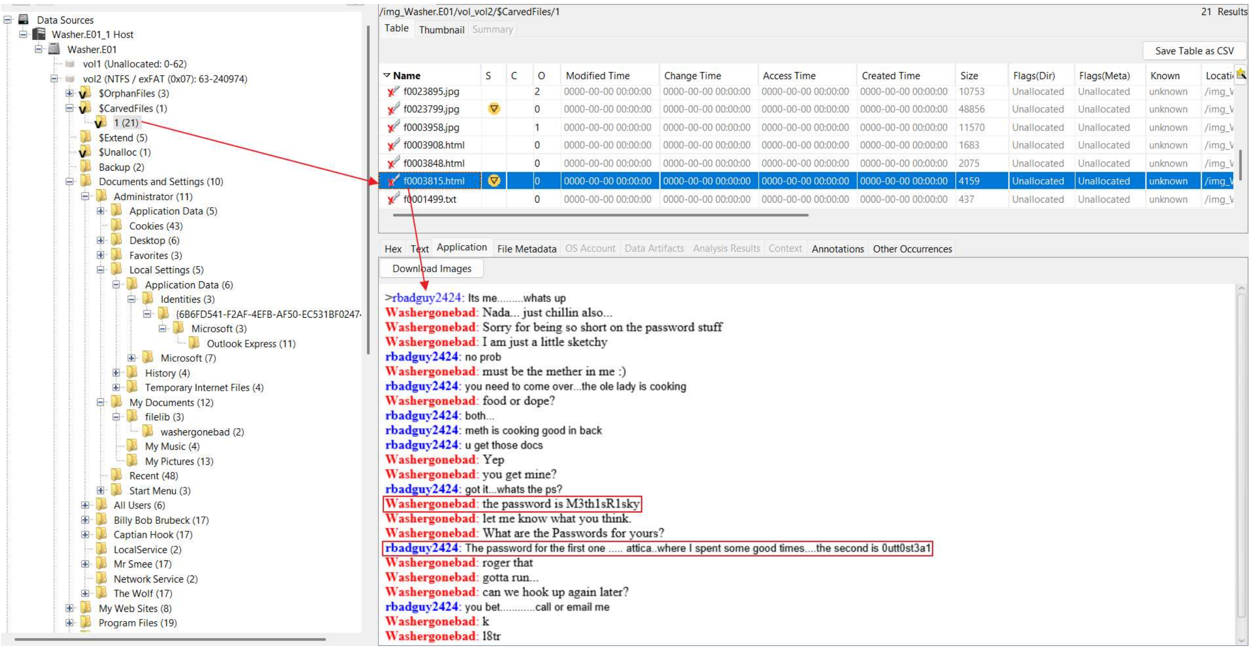
One of the recent documents opened by John Washer was Driving Directions from Red Feather Lakes, CO to Cut and Shoot, TX.mht. This file could depict a possible escape route for Wes Mantooth since his computer was set to Mountain Time. This also shows that John Washer is connected to Wes Mantooth.



Source Name	S	C	O	Path	Date Accessed
NTUSER.DAT				C:\WINDOWS\system32\compmgmt.msc	
cht.lnk				C:\Documents and Settings\Administrator\Desktop\cht..	2007-07-24 21:51:14 EDT
Driving Directions from Red Feather Lakes, CO to C				C:\Documents and Settings\Administrator\Desktop\Dri..	2007-07-25 15:10:09 EDT
SLIST.doc.lnk				C:\Documents and Settings\Administrator\My Documen	2007-07-25 16:07:47 EDT
How To Steal Credit Numbers.doc.lnk				C:\Documents and Settings\Administrator\My Documen	2007-07-25 16:07:55 EDT

Figure 8: Driving directions file recently accessed

I discovered a deleted chatlog between Washer and Rasco in which passwords for encrypted documents were transferred. This is shown below in Figure 9.



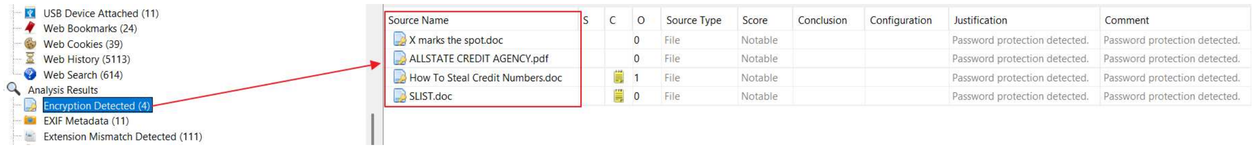
/img_Washer.E01/vol_vol2/$CarvedFiles/1 21 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Locati
f0023895.jpg			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	10753	Unallocated	Unallocated	unknown	/img_V
f0023799.jpg	▽		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	48856	Unallocated	Unallocated	unknown	/img_V
f0003958.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11570	Unallocated	Unallocated	unknown	/img_V
f0003908.html			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1683	Unallocated	Unallocated	unknown	/img_V
f0003848.html			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2075	Unallocated	Unallocated	unknown	/img_V
f0003815.html	▽		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4159	Unallocated	Unallocated	unknown	/img_V
f0001499.txt			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	437	Unallocated	Unallocated	unknown	/img_V

```
>rbadguy2424: Its me.........whats up
Washergonebad: Nada... just chillin also...
Washergonebad: Sorry for being so short on the password stuff
Washergonebad: I am just a little sketchy
rbadguy2424: no prob
Washergonebad: must be the mether in me :)
rbadguy2424: you need to come over...the ole lady is cooking
Washergonebad: food or dope?
rbadguy2424: both...
rbadguy2424: meth is cooking good in back
rbadguy2424: u get those docs
Washergonebad: Yep
Washergonebad: you get mine?
rbadguy2424: got it...whats the ps?
Washergonebad: the password is M3th1sR1sky
Washergonebad: let me know what you think.
Washergonebad: What are the Passwords for yours?
rbadguy2424: The password for the first one ..... attica..where I spent some good times....the second is 0utt0st3a1
Washergonebad: roger that
Washergonebad: gotta run...
Washergonebad: can we hook up again later?
rbadguy2424: you bet............call or email me
Washergonebad: k
Washergonebad: l8tr
```

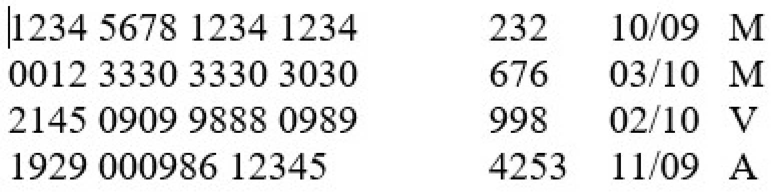
Figure 9: Chatlog with file passwords

With this information, I found and extracted the encrypted files on Washer's computer and tried the passwords on each. Figure 10 shows the encrypted files. The password "M3th1sR1sky" did not work on any of them. However, "attica" worked for SLIST.doc and "0utt0st3a1" worked for How To Steal Credit Numbers.doc. The unencrypted documents are shown in Figures 11 and 12. Fortunately, the credit card numbers in SLIST.doc are not valid credit card numbers.



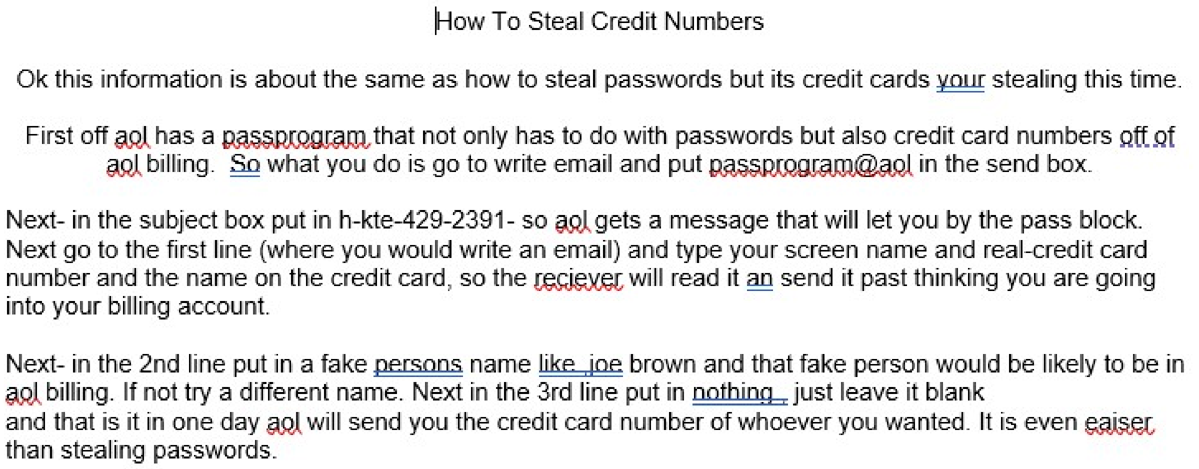
Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Comment
X marks the spot.doc			0	File	Notable			Password protection detected.	Password protection detected.
ALLSTATE CREDIT AGENCY.pdf			0	File	Notable			Password protection detected.	Password protection detected.
How To Steal Credit Numbers.doc		▤	1	File	Notable			Password protection detected.	Password protection detected.
SLIST.doc		▤	0	File	Notable			Password protection detected.	Password protection detected.

Figure 10: Encrypted Files



1234 5678 1234 1234	232	10/09	M
0012 3330 3330 3030	676	03/10	M
2145 0909 9888 0989	998	02/10	V
1929 000986 12345	4253	11/09	A

Figure 11: SLIST.doc unencrypted



How To Steal Credit Numbers

Ok this information is about the same as how to steal passwords but its credit cards your stealing this time.

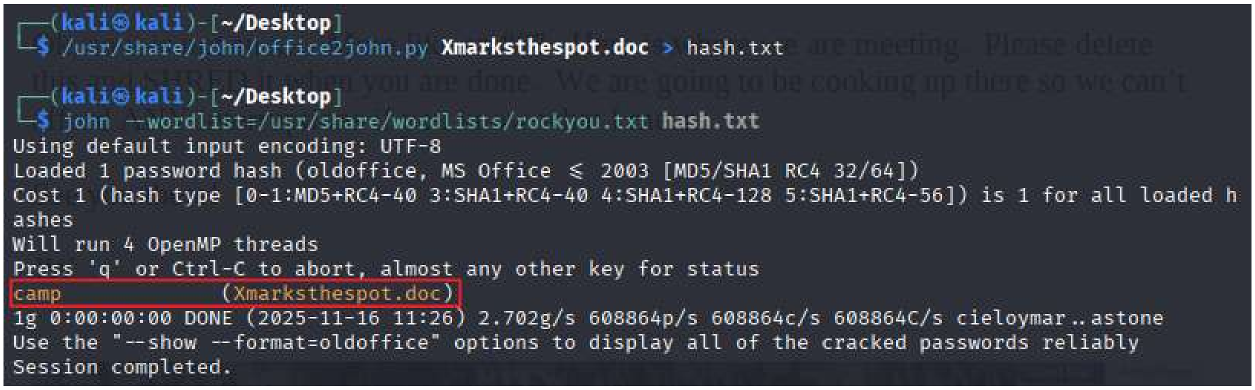
First off aol has a passprogram that not only has to do with passwords but also credit card numbers off of aol billing. So what you do is go to write email and put passprogram@aol in the send box.

Next- in the subject box put in h-kte-429-2391- so aol gets a message that will let you by the pass block. Next go to the first line (where you would write an email) and type your screen name and real-credit card number and the name on the credit card, so the reciever will read it an send it past thinking you are going into your billing account.

Next- in the 2nd line put in a fake persons name like joe brown and that fake person would be likely to be in aol billing. If not try a different name. Next in the 3rd line put in nothing , just leave it blank
and that is it in one day aol will send you the credit card number of whoever you wanted. It is even eaiser than stealing passwords.

Figure 12: How To Steal Credit Numbers.doc unencrypted

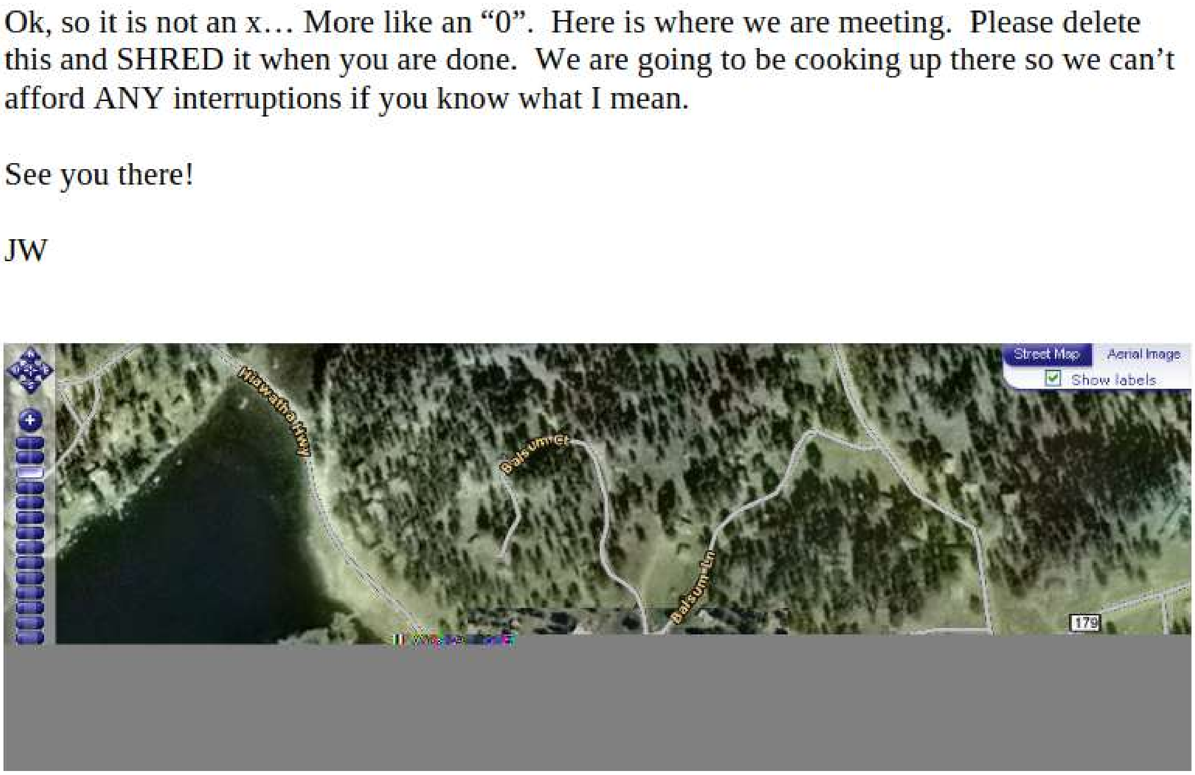
The other two files will have to be cracked using John the Ripper in Kali Linux. I used the rockyou.txt wordlist and a custom wordlist created by using bulk-extractor on the disk image to crack the passwords. Once I successfully cracked the passwords, I was able to open the encrypted files and discovered that X marks the spot.doc contains a partially corrupted image from MapQuest depicting a meeting location. ALLSTATE CREDIT AGENCY.pdf contains credit history for a person named Michael McNeil, which could have been stolen. These are shown below in Figures 13-17.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ /usr/share/john/office2john.py Xmarksthespot.doc > hash.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (oldoffice, MS Office ≤ 2003 [MD5/SHA1 RC4 32/64])
Cost 1 (hash type [0-1:MD5+RC4-40 3:SHA1+RC4-40 4:SHA1+RC4-128 5:SHA1+RC4-56]) is 1 for all loaded h
ashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
camp             (Xmarksthespot.doc)
1g 0:00:00:00 DONE (2025-11-16 11:26) 2.702g/s 608864p/s 608864c/s 608864C/s cieloymar..astone
Use the "--show --format=oldoffice" options to display all of the cracked passwords reliably
Session completed.
```

Figure 13: Cracked password for X marks the spot.doc

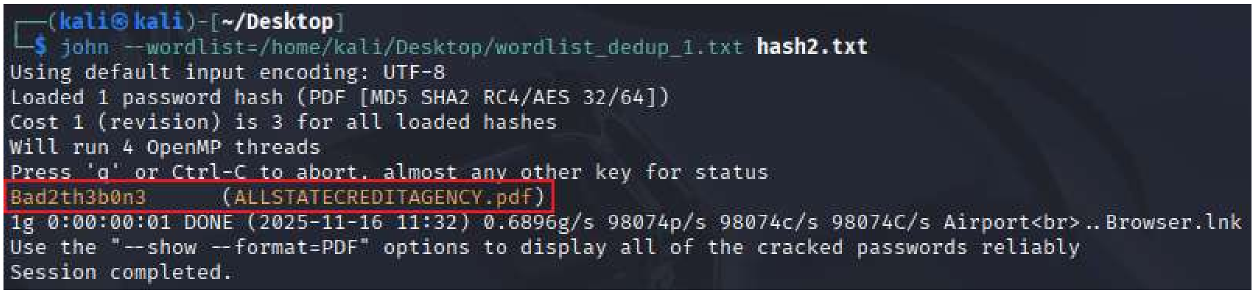


Ok, so it is not an x… More like an "0". Here is where we are meeting. Please delete this and SHRED it when you are done. We are going to be cooking up there so we can't afford ANY interruptions if you know what I mean.

See you there!

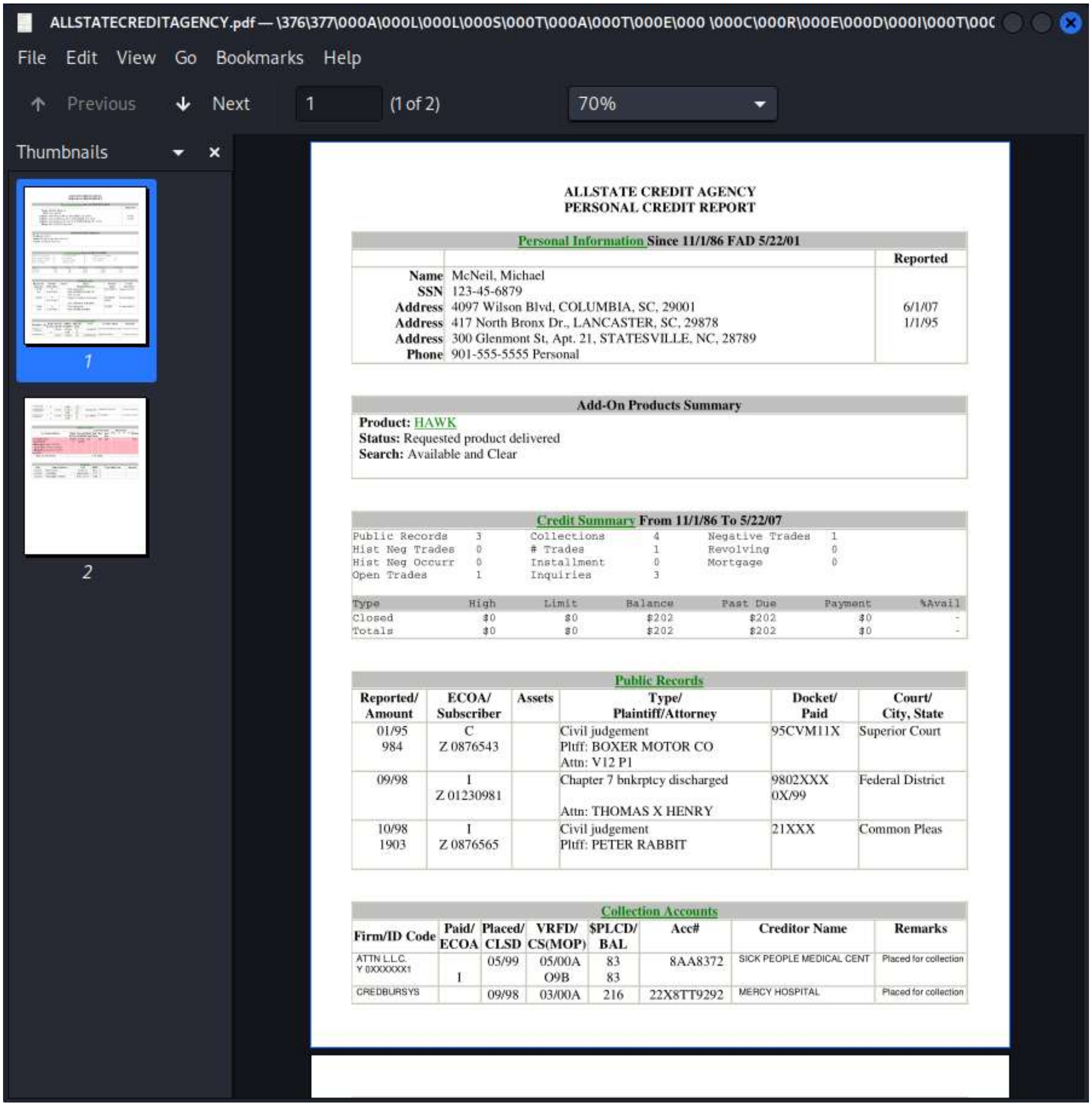
JW

Figure 14: X marks the spot.doc unencrypted



```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=/home/kali/Desktop/wordlist_dedup_1.txt hash2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
Cost 1 (revision) is 3 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Bad2th3b0n3      (ALLSTATECREDITAGENCY.pdf)
1g 0:00:00:01 DONE (2025-11-16 11:32) 0.6896g/s 98074p/s 98074c/s 98074C/s Airport<br>..Browser.lnk
Use the "--show --format=PDF" options to display all of the cracked passwords reliably
Session completed.
```

Figure 15: Cracked password for ALLSTATE CREDIT AGENCY.pdf


ALLSTATECREDITAGENCY.pdf — \376\377\000A\000L\000L\000S\000T\000A\000T\000E\000 \000C\000R\000E\000D\000I\000T\000C
File
Edit
View
Go
Bookmarks
Help
Previous
Next
1
(1 of 2)
70%
Thumbnails
1
2

ALLSTATE CREDIT AGENCY
PERSONAL CREDIT REPORT

Personal Information Since 11/1/86 FAD 5/22/01

		Reported
Name	McNeil, Michael	
SSN	123-45-6879	
Address	4097 Wilson Blvd, COLUMBIA, SC, 29001	6/1/07
Address	417 North Bronx Dr., LANCASTER, SC, 29878	1/1/95
Address	300 Glenmont St, Apt. 21, STATESVILLE, NC, 28789	
Phone	901-555-5555 Personal	

Add-On Products Summary

Product: HAWK
Status: Requested product delivered
Search: Available and Clear

Credit Summary From 11/1/86 To 5/22/07

```
Public Records     3        Collections       4        Negative Trades    1
Hist Neg Trades    0        # Trades          1        Revolving          0
Hist Neg Occurr    0        Installment       0        Mortgage           0
Open Trades        1        Inquiries         3

Type              High        Limit       Balance       Past Due       Payment        %Avail
Closed              $0           $0          $202           $202            $0             -
Totals              $0           $0          $202           $202            $0             -
```

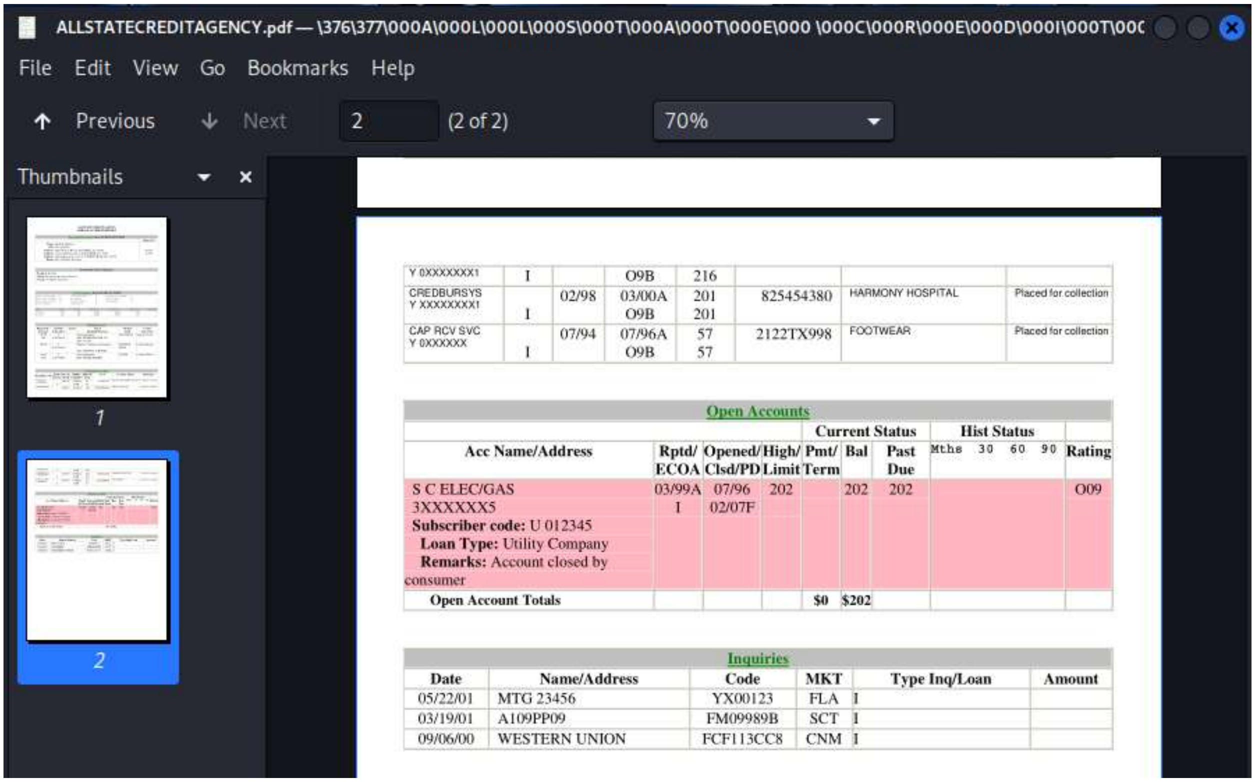
Public Records

Reported/ Amount	ECOA/ Subscriber	Assets	Type/ Plaintiff/Attorney	Docket/ Paid	Court/ City, State
01/95 984	C Z 0876543		Civil judgement Pltff: BOXER MOTOR CO Attn: V12 P1	95CVM11X	Superior Court
09/98	I Z 01230981		Chapter 7 bnkrptcy discharged Attn: THOMAS X HENRY	9802XXX 0X/99	Federal District
10/98 1903	I Z 0876565		Civil judgement Pltff: PETER RABBIT	21XXX	Common Pleas

Collection Accounts

Firm/ID Code	Paid/ ECOA	Placed/ CLSD	VRFD/ CS(MOP)	$PLCD/ BAL	Acc#	Creditor Name	Remarks
ATTN L.L.C. Y 0XXXXXX1	I	05/99	05/00A O9B	83 83	8AA8372	SICK PEOPLE MEDICAL CENT	Placed for collection
CREDBURSYS		09/98	03/00A	216	22X8TT9292	MERCY HOSPITAL	Placed for collection

Figure 16: ALLSTATE CREDIT AGENCY.pdf unencrypted (1)


ALLSTATECREDITAGENCY.pdf — \376\377\000A\000L\000L\000S\000T\000A\000T\000E\000 \000C\000R\000E\000D\000I\000T\000C
File Edit View Go Bookmarks Help
Previous
Next
2
(2 of 2)
70%
Thumbnails
1
2

Y 0XXXXXXX1	I		O9B	216			
CREDBURSYS Y XXXXXXXX1	I	02/98	03/00A O9B	201 201	825454380	HARMONY HOSPITAL	Placed for collection
CAP RCV SVC Y 0XXXXXX	I	07/94	07/96A O9B	57 57	2122TX998	FOOTWEAR	Placed for collection

Open Accounts

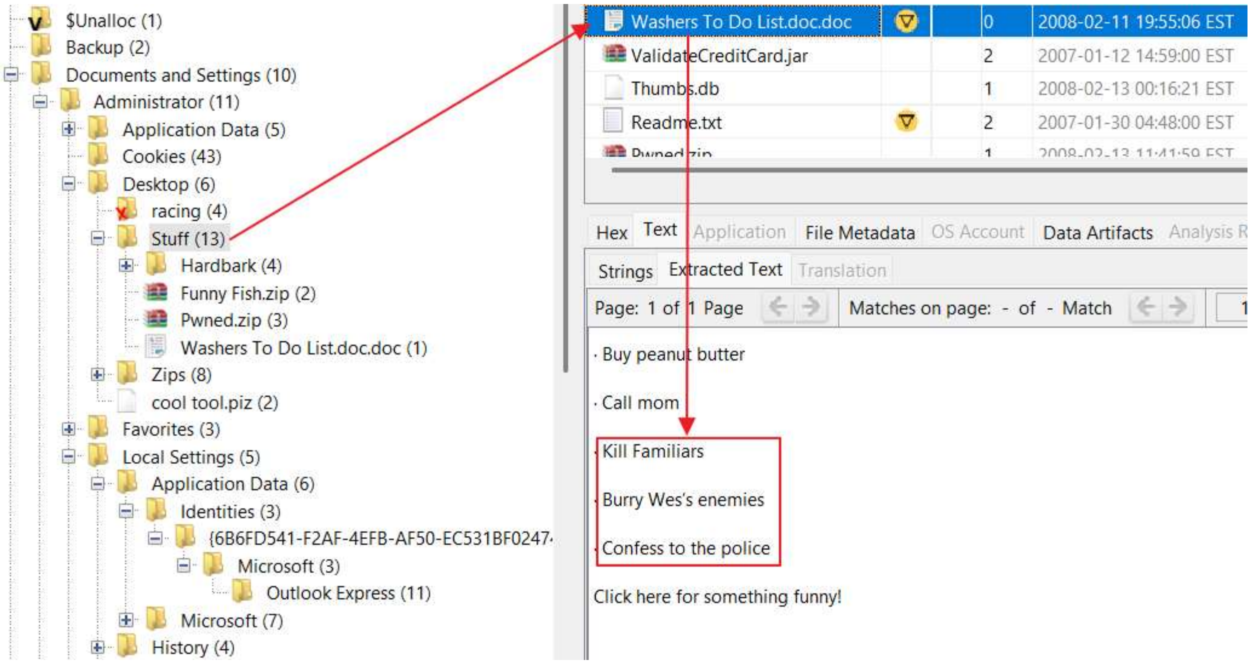
				Current Status			Hist Status	
Acc Name/Address	Rptd/ ECOA	Opened/ Clsd/PD	High/ Limit	Pmt/ Term	Bal	Past Due	Mths 30 60 90	Rating
S C ELEC/GAS 3XXXXXX5 **Subscriber code:** U 012345 **Loan Type:** Utility Company **Remarks:** Account closed by consumer	03/99A I	07/96 02/07F	202		202	202		O09
Open Account Totals				**$0**	**$202**			

Inquiries

Date	Name/Address	Code	MKT	Type Inq/Loan	Amount
05/22/01	MTG 23456	YX00123	FLA	I	
03/19/01	A109PP09	FM09989B	SCT	I	
09/06/00	WESTERN UNION	FCF113CC8	CNM	I	

Figure 17: ALLSTATE CREDIT AGENCY.pdf unencrypted (2)

Additionally, I discovered a word document on the desktop of the Administrator account, which contains a to do list. The phrases “Kill Familiars”, “Burry Wes’s enemies”, and “Confess to the police” depict that John Washer is planning to commit murder and turn himself into the police. The document also contains a link, which redirects to a cat image. These are shown in Figures 18 and 19.



Washers To Do List.doc.doc	▽	0	2008-02-11 19:55:06 EST
ValidateCreditCard.jar		2	2007-01-12 14:59:00 EST
Thumbs.db		1	2008-02-13 00:16:21 EST
Readme.txt	▽	2	2007-01-30 04:48:00 EST
Pwned.zip		1	2008-02-13 11:41:59 EST

· Buy peanut butter

· Call mom

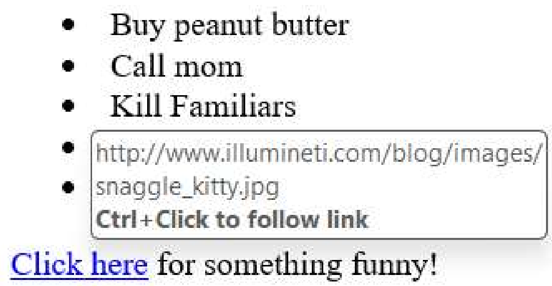
· Kill Familiars

· Burry Wes's enemies

· Confess to the police

Click here for something funny!

Figure 18: To do list



- Buy peanut butter
- Call mom
- Kill Familiars
-
-

http://www.illumineti.com/blog/images/snaggle_kitty.jpg
Ctrl+Click to follow link

Click here for something funny!

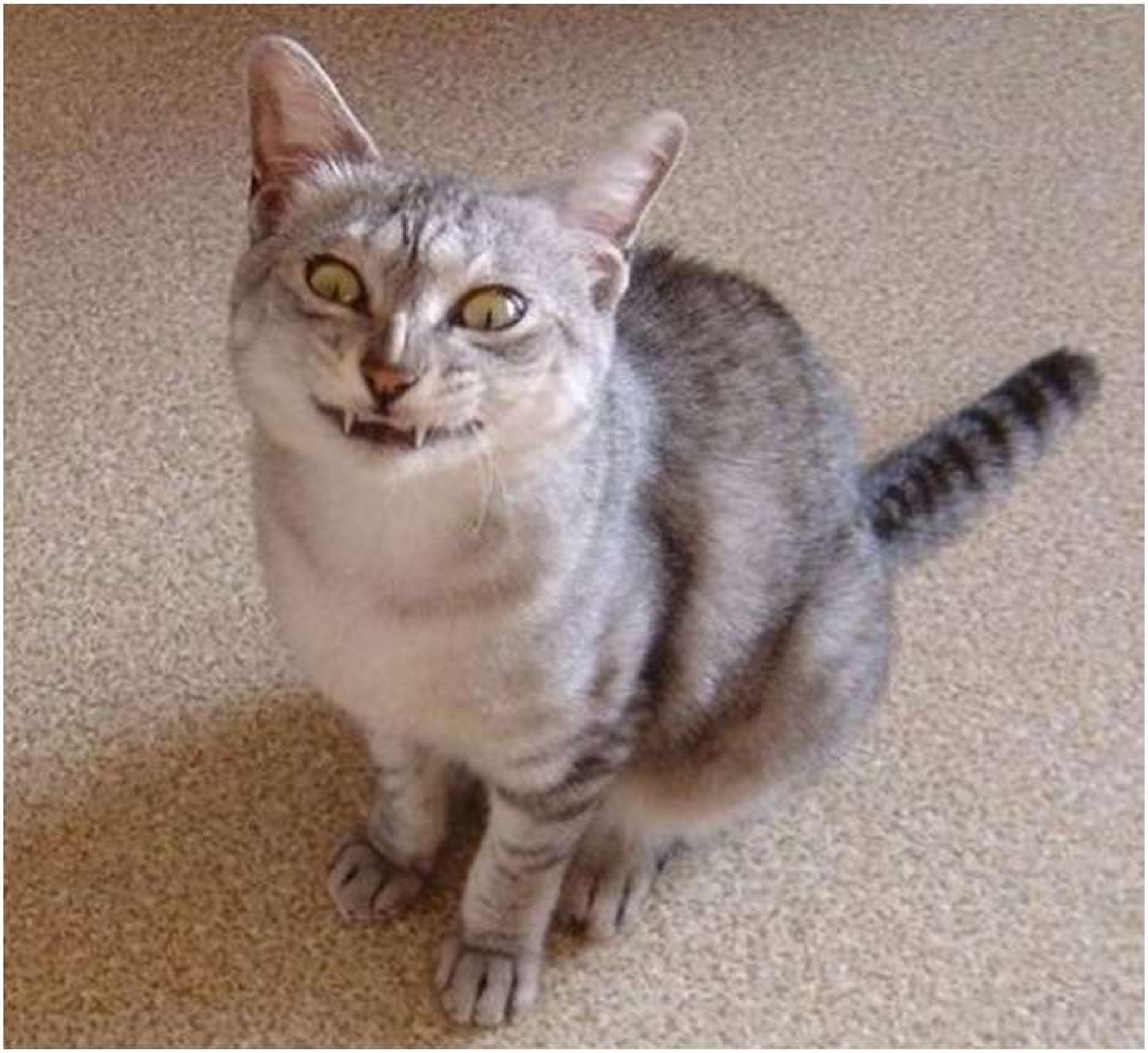
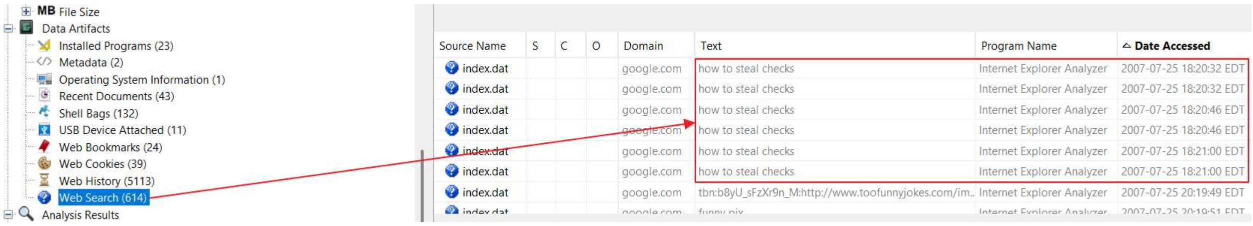


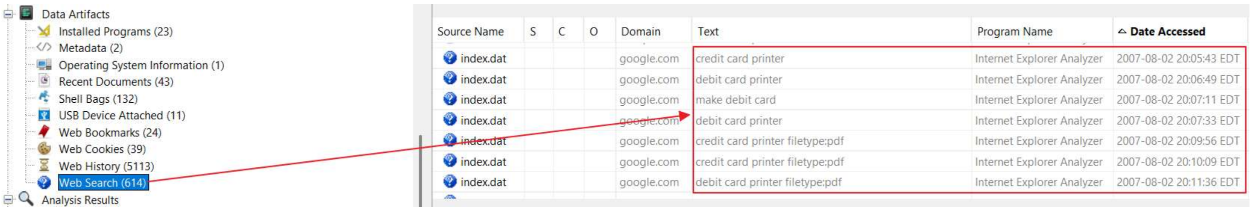
Figure 19: Link in the to do list

Next, I looked at the search queries and websites that Washer used. I discovered that he searched "how to steal checks", "credit card printer", "debit card printer", "changing your identity", and "disappearing". He also visited a website called http://www.plasticprinters.com/creditdebit/, which is a site that allows people to buy credit card printers, possibly for malicious intent. The searches show interest in illicit activities and an attempt to hide evidence. These are shown in Figures 20-24.



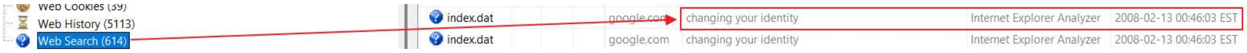
Source Name	S	C	O	Domain	Text	Program Name	Date Accessed
index.dat				google.com	how to steal checks	Internet Explorer Analyzer	2007-07-25 18:20:32 EDT
index.dat				google.com	how to steal checks	Internet Explorer Analyzer	2007-07-25 18:20:32 EDT
index.dat				google.com	how to steal checks	Internet Explorer Analyzer	2007-07-25 18:20:46 EDT
index.dat				google.com	how to steal checks	Internet Explorer Analyzer	2007-07-25 18:20:46 EDT
index.dat				google.com	how to steal checks	Internet Explorer Analyzer	2007-07-25 18:21:00 EDT
index.dat				google.com	how to steal checks	Internet Explorer Analyzer	2007-07-25 18:21:00 EDT
index.dat				google.com	tbn:b8yU_sFzXr9n_M:http://www.toofunnyjokes.com/im..	Internet Explorer Analyzer	2007-07-25 20:19:49 EDT
index.dat				google.com	funny pix	Internet Explorer Analyzer	2007-07-25 20:19:51 EDT

Figure 20: Search query for "how to steal checks"



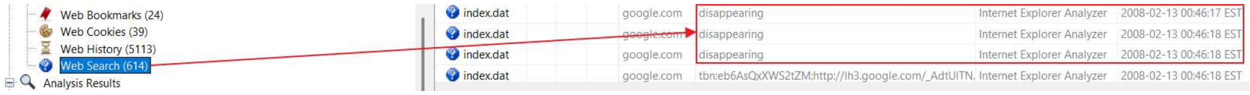
Source Name	S	C	O	Domain	Text	Program Name	Date Accessed
index.dat				google.com	credit card printer	Internet Explorer Analyzer	2007-08-02 20:05:43 EDT
index.dat				google.com	debit card printer	Internet Explorer Analyzer	2007-08-02 20:06:49 EDT
index.dat				google.com	make debit card	Internet Explorer Analyzer	2007-08-02 20:07:11 EDT
index.dat				google.com	debit card printer	Internet Explorer Analyzer	2007-08-02 20:07:33 EDT
index.dat				google.com	credit card printer filetype:pdf	Internet Explorer Analyzer	2007-08-02 20:09:56 EDT
index.dat				google.com	credit card printer filetype:pdf	Internet Explorer Analyzer	2007-08-02 20:10:09 EDT
index.dat				google.com	debit card printer filetype:pdf	Internet Explorer Analyzer	2007-08-02 20:11:36 EDT

Figure 21: Search query for "credit card printer" and "debit card printer"



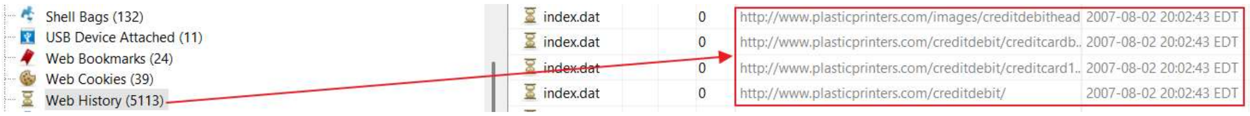
index.dat				google.com	changing your identity	Internet Explorer Analyzer	2008-02-13 00:46:03 EST
index.dat				google.com	changing your identity	Internet Explorer Analyzer	2008-02-13 00:46:03 EST

Figure 22: Search query for "changing your identity"



index.dat				google.com	disappearing	Internet Explorer Analyzer	2008-02-13 00:46:17 EST
index.dat				google.com	disappearing	Internet Explorer Analyzer	2008-02-13 00:46:18 EST
index.dat				google.com	disappearing	Internet Explorer Analyzer	2008-02-13 00:46:18 EST
index.dat				google.com	tbn:eb6AsQxXWS2tZM:http://lh3.google.com/_AdtUITN.	Internet Explorer Analyzer	2008-02-13 00:46:18 EST

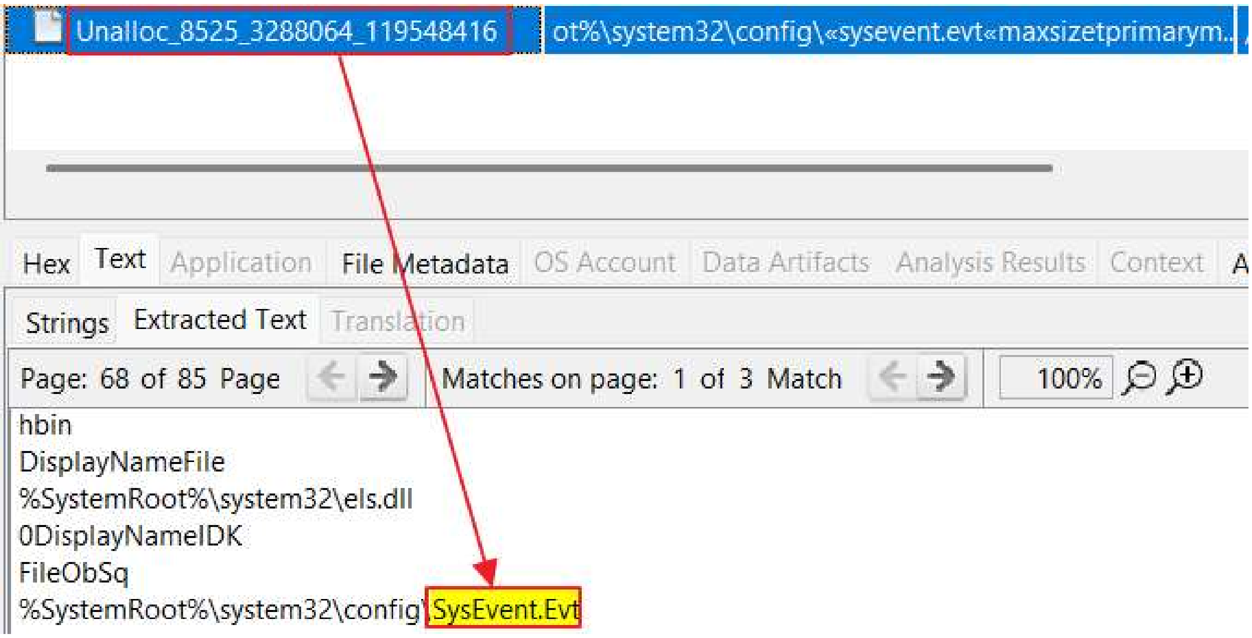
Figure 23: Search query for "disappearing"



index.dat	0	http://www.plasticprinters.com/images/creditdebithead	2007-08-02 20:02:43 EDT
index.dat	0	http://www.plasticprinters.com/creditdebit/creditcardb..	2007-08-02 20:02:43 EDT
index.dat	0	http://www.plasticprinters.com/creditdebit/creditcard1..	2007-08-02 20:02:43 EDT
index.dat	0	http://www.plasticprinters.com/creditdebit/	2007-08-02 20:02:43 EDT

Figure 24: Website visited showing illicit activity

As shown in Figure 25, I also discovered that the event logs were deleted from John's computer, indicating that he tried to hide key evidence like login timestamps.



```
hbin
DisplayNameFile
%SystemRoot%\system32\els.dll
0DisplayNameIDK
FileObSq
%SystemRoot%\system32\config\SysEvent.Evt
```

Figure 25: System event log found in unallocated space

Timeline

Date/Time	Event	Relevance
6/20/2007 – 11:56:00 EDT	John Washer emails Wes Mantooth about ketamine	Indicates interaction with Mantooth regarding illegal activities
6/21/2007 – 15:06:00 EDT	Wes emails John about obtaining a stolen check	Shows another interaction between Wes Mantooth and John Washer regarding illicit activities
6/21/2007 – 15:09:28 EDT	John replies to Mantooth's email with steps to wash the check	Shows involvement with check washing
7/25/2007 – 15:10:09 EDT	Washer opens a file containing driving directions from Red Feather Lakes, Colorado to Cut and Shoot Texas	Shows relation between Washer and Mantooth
7/25/2007 – 18:20:32 EDT	Washer searches for "how to steal checks" on Google	Shows interest in check stealing and washing
8/2/2007 – 20:02:43 EDT	John visits http://www.plasticprinters.com/creditdebit/	Indicates involvement in illegal activities

8/2/2007 – 20:05:43 EDT	John Washer searches for “credit card printer”	Shows involvement in credit card stealing
8/2/2007 – 20:06:49 EDT	Washer searches for “debit card printer”	Shows John’s interest in debit card stealing
2/11/2008 – 19:55:06 EST	John accesses “Washers To Do List.doc.doc”, which contains evidence of murder plans and confessing to the police	Indicates involvement in illegal activities
2/13/2008 – 00:46:03 EST	John searches for “changing your identity” on Google	Shows an attempt to steal identities or hide evidence
2/13/2008 – 00:46:17 EST	John Washer searches for “disappearing”	Indicates an attempt to hide evidence

Conclusions

The main user on this Windows XP computer is the Administrator account. The owner of the computer is John Washer. This person is involved in various illegal activities such as check washing, drug dealing, and credit/debit card stealing, as shown through various emails, files, and search queries on the computer. Some of these activities are conducted with the help of Wes Mantooth, Rasco Badguy, and other possible suspects involved in a similar case. John Washer seems to mostly work with Rasco, as shown through the emails and chatlogs on his computer. John has a more advanced understanding of computers because there are encrypted files on his computer. Encryption means a file is protected with a password and only people who know the password can view the file. Some passwords were found in a chat between John and Rasco, while others had to be cracked in Kali Linux in order for an investigator to view the contents of the file. The encrypted files contain stolen credit cards, stolen identities, and directions to a possible hideout location. The computer is set to Eastern Time. Additionally, there are deleted files on the computer that were recovered, one of which indicates an interaction between John Washer and Rasco Badguy, who is another possible suspect in this case.