12/12/2025

Clampet Report

Report by Anthony Smithmyer

Executive Summary

There are several users on this Windows XP computer, but it is mainly used by Granny and Jethro despite being owned by Jed. These two users are involved in illicit activities like moonshine distilling and money laundering (the process of making a large amount of “dirty” funds appear legitimate), as shown through the pictures, files, emails, and web searches on the computer. Other people involved in the money laundering scheme with Jethro are known as Dang MeDang Me, Johnny Rottencore, Sluggy, and Milburn Drysdale. There are encrypted files on the computer, meaning only people who know the password can open and view the files. These files contained customer information, laundered money, and a plan to deliver potentially laundered money to a bank. The computer is set to Pacific Time, most likely in California since some files contained directions to and from places in California. Additionally, there were some deleted files useful to the investigation that were recovered. One of the deleted files shows that Jethro might be working with law enforcement, rather than actually conducting illegal activities.

Methods

Tools used:

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

The process:

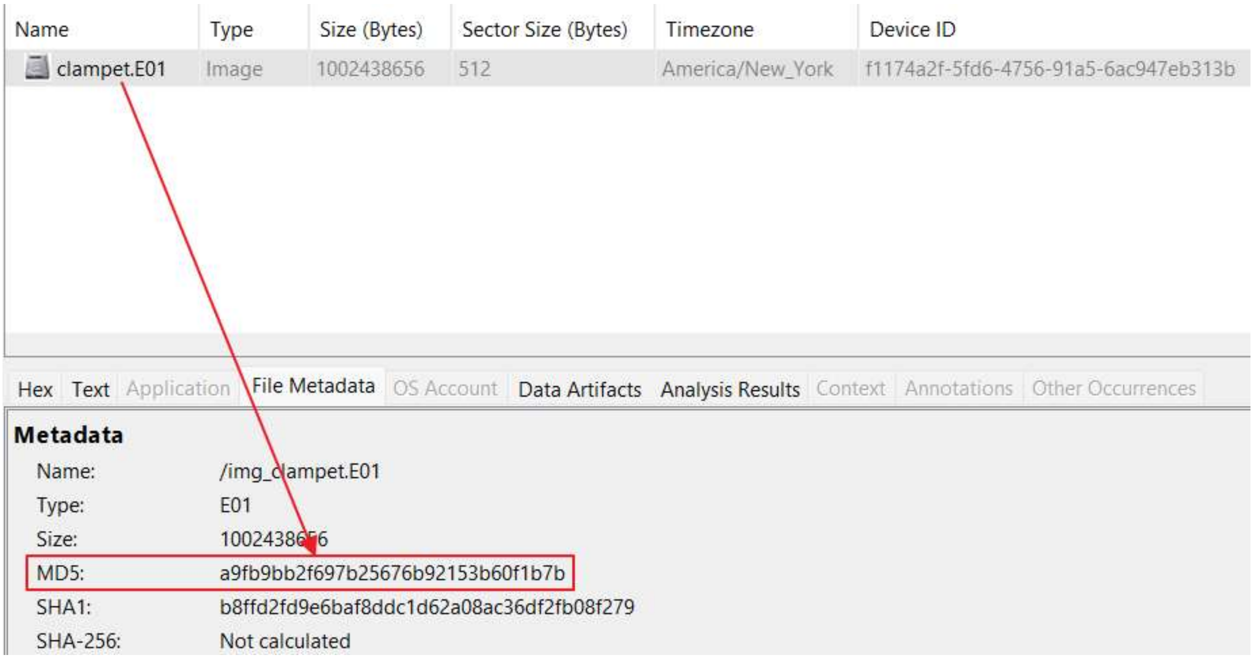
I downloaded the disk image of Clampet’s computer and started a new case in Autopsy 4.22.1. I selected the disk image as a data source. I began to look through the files on the image to tell the story about the people using the computer.

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, I verified the MD5 hash of the image to ensure that it wasn’t tampered with. A different file hash means that something in the image was changed. The file hash listed in the Clampet.E01.txt file is a9fb9bb2f697b25676b92153b60f1b7b. Using Autopsy, I went to Data Sources > Clampet.E01_1 Host and single-clicked on Clampet.E01 in the right pane. The hash of the disk image is listed in the “File Metadata” tab below. As shown in Figures 1 and 2, the file hashes are the same, which proves that the disk image was not tampered with.

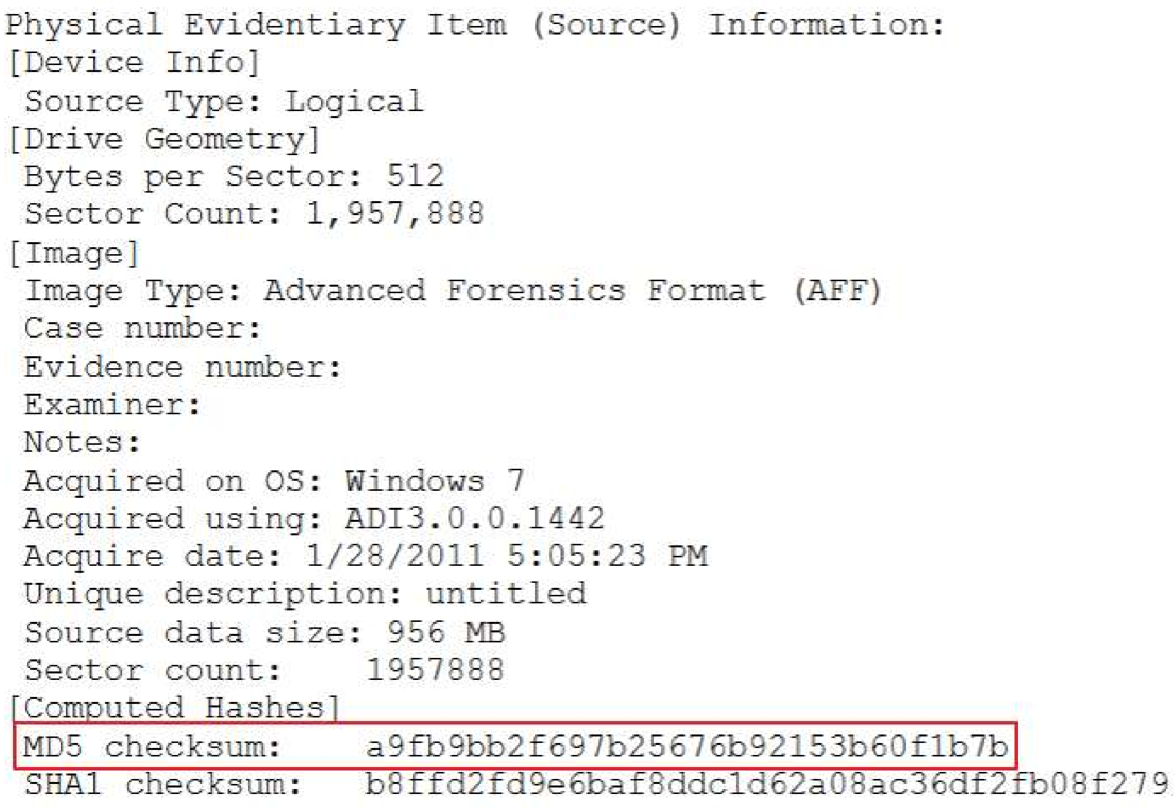


Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
clampet.E01	Image	1002438656	512	America/New_York	f1174a2f-5fd6-4756-91a5-6ac947eb313b

Metadata

Name:	/img_clampet.E01
Type:	E01
Size:	1002438656
MD5:	a9fb9bb2f697b25676b92153b60f1b7b
SHA1:	b8ffd2fd9e6baf8ddc1d62a08ac36df2fb08f279
SHA-256:	Not calculated

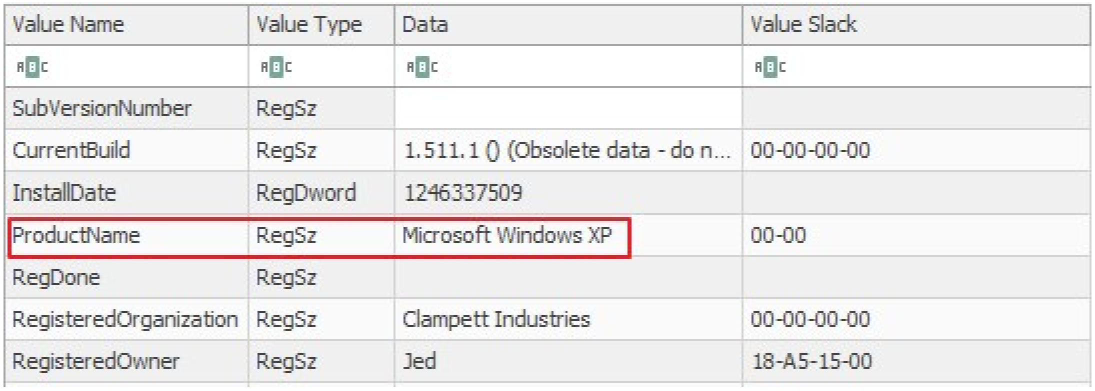
Figure 1: File hash of Clampet.E01 shown in Autopsy



```
Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 1,957,888
[Image]
 Image Type: Advanced Forensics Format (AFF)
 Case number:
 Evidence number:
 Examiner:
 Notes:
 Acquired on OS: Windows 7
 Acquired using: ADI3.0.0.1442
 Acquire date: 1/28/2011 5:05:23 PM
 Unique description: untitled
 Source data size: 956 MB
 Sector count:    1957888
[Computed Hashes]
 MD5 checksum:    a9fb9bb2f697b25676b92153b60f1b7b
 SHA1 checksum:   b8ffd2fd9e6baf8ddc1d62a08ac36df2fb08f279
```

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

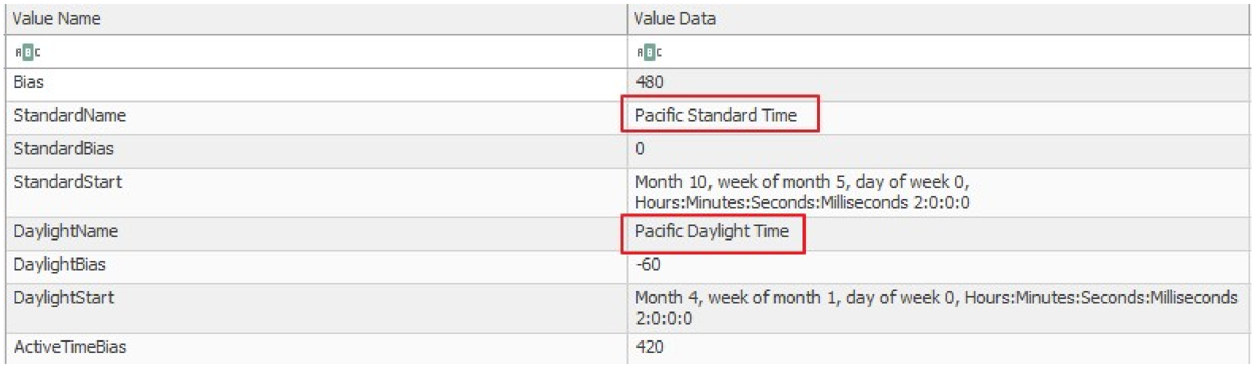
Once I verified the hashes, I began my investigation and looked through the file system. Using Registry Explorer, I went to SOFTWARE\Microsoft\Windows NT\CurrentVersion and determined that this computer was running Windows XP, and the owner of the computer is Jed. This is shown below in Figure 3.



Value Name	Value Type	Data	Value Slack
ABC	ABC	ABC	ABC
SubVersionNumber	RegSz		
CurrentBuild	RegSz	1.511.1 () (Obsolete data - do n...	00-00-00-00
InstallDate	RegDword	1246337509	
ProductName	RegSz	Microsoft Windows XP	00-00
RegDone	RegSz		
RegisteredOrganization	RegSz	Clampett Industries	00-00-00-00
RegisteredOwner	RegSz	Jed	18-A5-15-00

Figure 3: Operating System version shown in Registry Explorer

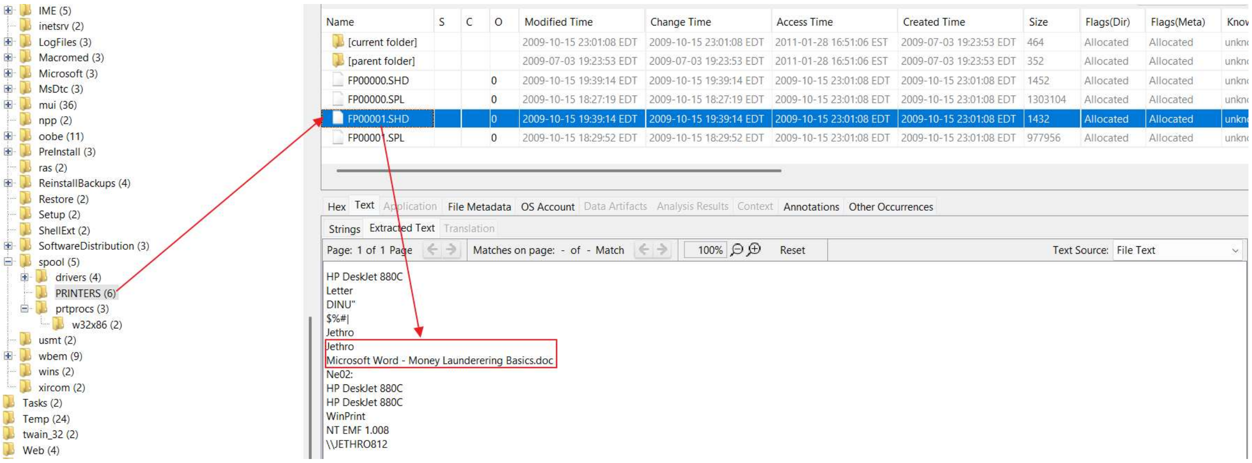
While looking through the registry, I determined that the computer's time zone was set to Pacific Time. I found this information by going to SYSTEM\CurrentControlSet\Control \TimeZoneInformation. This is shown in Figure 4.



Value Name	Value Data
RBC	RBC
Bias	480
StandardName	Pacific Standard Time
StandardBias	0
StandardStart	Month 10, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
DaylightName	Pacific Daylight Time
DaylightBias	-60
DaylightStart	Month 4, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
ActiveTimeBias	420

Figure 4: Time zone information in Registry Explorer

While looking through System32 in Autopsy, which is where I found the registry hives, I noticed printer spools saved to the computer, meaning that someone recently printed a document, website, etc. Clicking on the .SHD file shows which printer was used, what was printed, and the user that printed it. It shows that the user Jethro printed a Word document called “Money Laundering Basics.doc”. This could indicate evidence of criminal activity. See Figure 5 for more information.

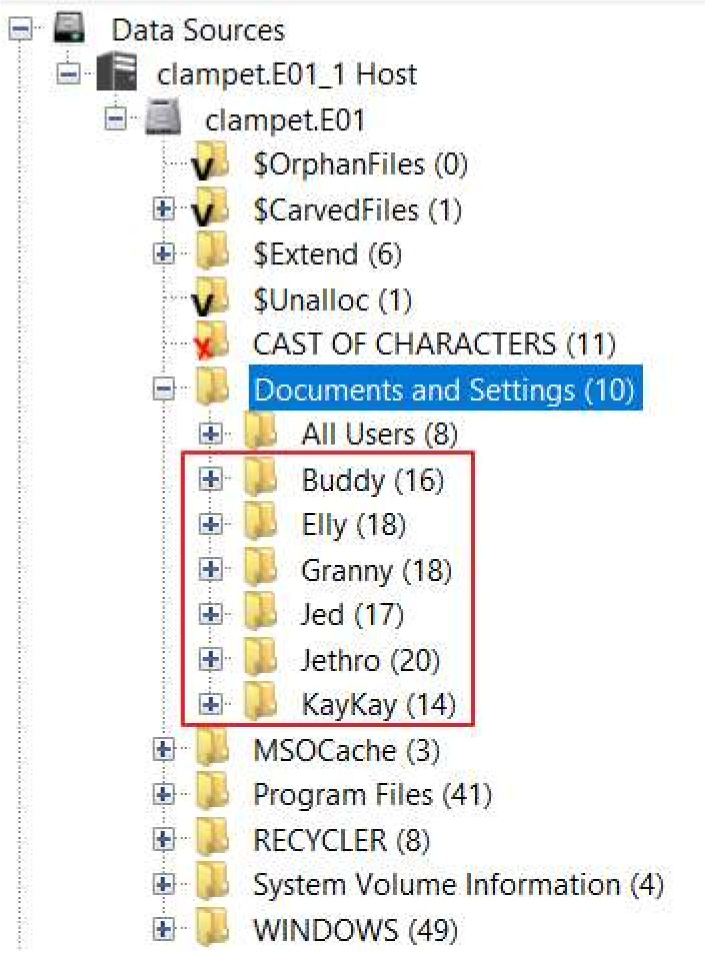


Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Know
[current folder]				2009-10-15 23:01:08 EDT	2009-10-15 23:01:08 EDT	2011-01-28 16:51:06 EST	2009-07-03 19:23:53 EDT	464	Allocated	Allocated	unkn
[parent folder]				2009-07-03 19:23:53 EDT	2009-07-03 19:23:53 EDT	2011-01-28 16:51:06 EST	2009-07-03 19:23:53 EDT	352	Allocated	Allocated	unkn
FP00000.SHD			0	2009-10-15 19:39:14 EDT	2009-10-15 19:39:14 EDT	2009-10-15 23:01:08 EDT	2009-10-15 23:01:08 EDT	1452	Allocated	Allocated	unkn
FP00000.SPL			0	2009-10-15 18:27:19 EDT	2009-10-15 18:27:19 EDT	2009-10-15 23:01:08 EDT	2009-10-15 23:01:08 EDT	1303104	Allocated	Allocated	unkn
FP00001.SHD			0	2009-10-15 19:39:14 EDT	2009-10-15 19:39:14 EDT	2009-10-15 23:01:08 EDT	2009-10-15 23:01:08 EDT	1432	Allocated	Allocated	unkn
FP00001.SPL			0	2009-10-15 18:29:52 EDT	2009-10-15 18:29:52 EDT	2009-10-15 23:01:08 EDT	2009-10-15 23:01:08 EDT	977956	Allocated	Allocated	unkn

```
HP DeskJet 880C
Letter
DINU"
$%#|
Jethro
Jethro
Microsoft Word - Money Laundering Basics.doc
Ne02:
HP DeskJet 880C
HP DeskJet 880C
WinPrint
NT EMF 1.008
\\JETHRO812
```

Figure 5: Printed document

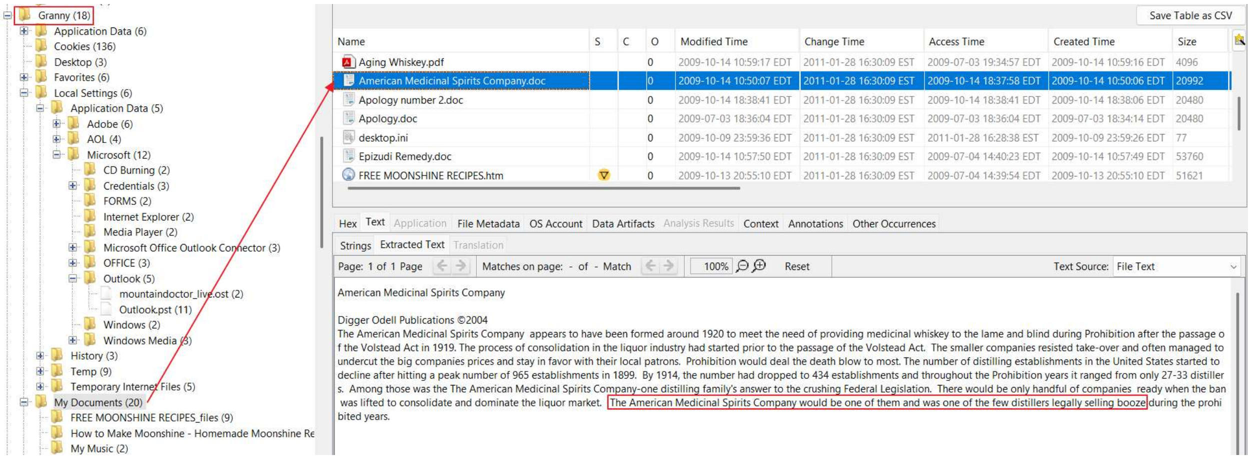
The users on this computer are Buddy, Elly, Granny, Jed, Jethro, and KayKay, as shown in Figure 6. Buddy has memes and funny pictures in his user folder. Elly has pictures and information about animals, as well as a Word document about proper dating etiquette. Granny has an encrypted file called “Customers.xls” and many files and pictures containing moonshine stills and recipes. Making moonshine without a permit/license is illegal. Jed has funny videos and banjo music sheets for “Oh Susana” and “Wabash Cannonball” in his user folder. Jethro has files related to money laundering, a plan (possibly for malicious intent), directions to an airport, registry searching, and informant debriefing questions. KayKay’s user folder contains regular expressions and .rsr files.



```
Data Sources
    clampet.E01_1 Host
        clampet.E01
            $OrphanFiles (0)
            $CarvedFiles (1)
            $Extend (6)
            $Unalloc (1)
            CAST OF CHARACTERS (11)
            Documents and Settings (10)
                All Users (8)
                Buddy (16)
                Elly (18)
                Granny (18)
                Jed (17)
                Jethro (20)
                KayKay (14)
            MSOCache (3)
            Program Files (41)
            RECYCLER (8)
            System Volume Information (4)
            WINDOWS (49)
```

Figure 6: Users shown in Autopsy

However, there is proof that Granny and Jethro are not actually committing crimes. Granny has a Word document that provides history about the American Medicinal Spirits Company, which was legally allowed to operate distilleries during the prohibition. Granny could be operating this company, meaning (if the licenses are up to date) she is legally allowed to make her own alcoholic beverages and sell them. This is shown below in Figure 7.



- Granny (18)
  - Application Data (6)
  - Cookies (136)
  - Desktop (3)
  - Favorites (6)
  - Local Settings (6)
    - Application Data (5)
      - Adobe (6)
      - AOL (4)
      - Microsoft (12)
        - CD Burning (2)
        - Credentials (3)
        - FORMS (2)
        - Internet Explorer (2)
        - Media Player (2)
        - Microsoft Office Outlook Connector (3)
        - OFFICE (3)
        - Outlook (5)
          - mountaindoctor_live.ost (2)
          - Outlook.pst (11)
        - Windows (2)
        - Windows Media (3)
    - History (3)
    - Temp (9)
    - Temporary Internet Files (5)
  - My Documents (20)
    - FREE MOONSHINE RECIPES_files (9)
    - How to Make Moonshine - Homemade Moonshine Re
    - My Music (2)

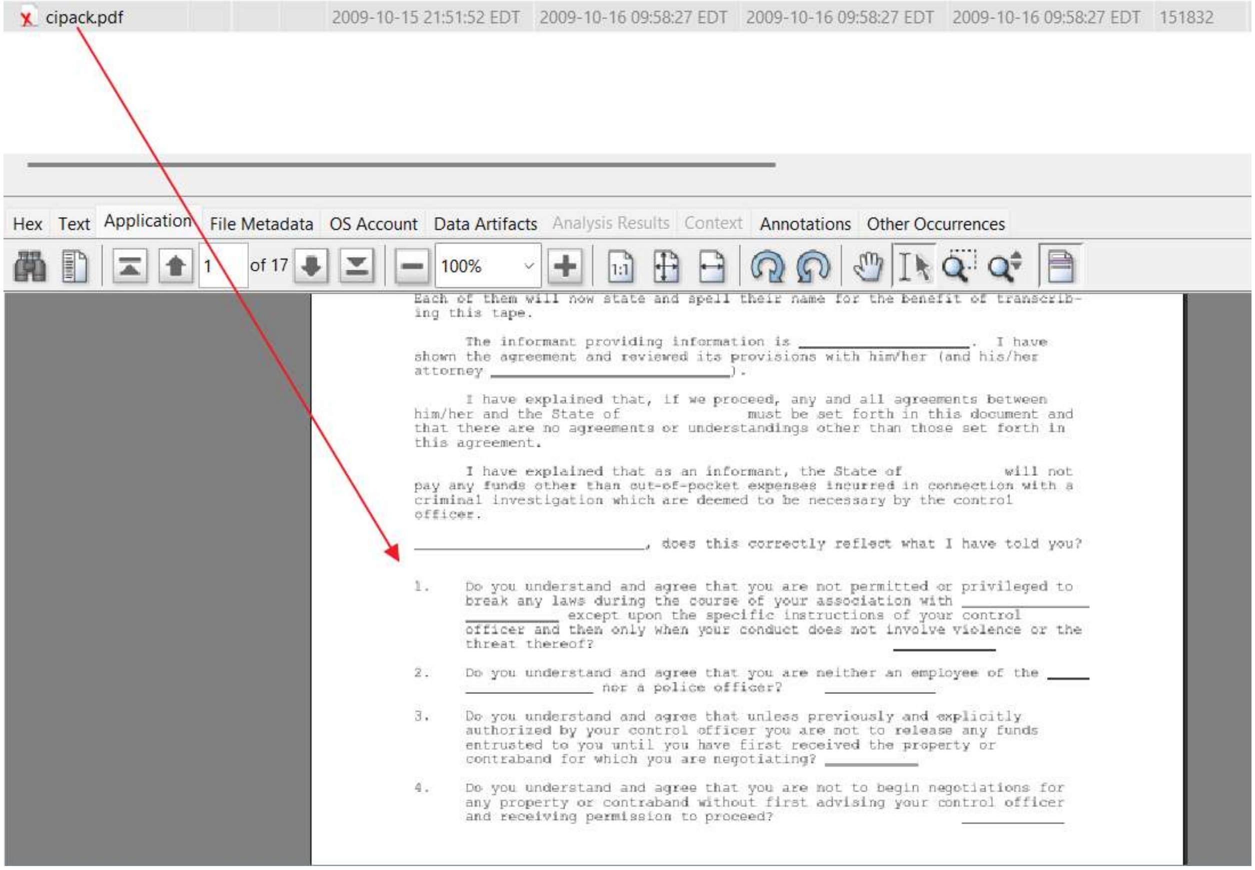
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Aging Whiskey.pdf			0	2009-10-14 10:59:17 EDT	2011-01-28 16:30:09 EST	2009-07-03 19:34:57 EDT	2009-10-14 10:59:16 EDT	4096
American Medicinal Spirits Company.doc			0	2009-10-14 10:50:07 EDT	2011-01-28 16:30:09 EST	2009-10-14 18:37:58 EDT	2009-10-14 10:50:06 EDT	20992
Apology number 2.doc			0	2009-10-14 18:38:41 EDT	2011-01-28 16:30:09 EST	2009-10-14 18:38:41 EDT	2009-10-14 18:38:06 EDT	20480
Apology.doc			0	2009-07-03 18:36:04 EDT	2011-01-28 16:30:09 EST	2009-07-03 18:36:04 EDT	2009-07-03 18:34:14 EDT	20480
desktop.ini			0	2009-10-09 23:59:36 EDT	2011-01-28 16:30:09 EST	2011-01-28 16:28:38 EST	2009-10-09 23:59:26 EDT	77
Epizudi Remedy.doc			0	2009-10-14 10:57:50 EDT	2011-01-28 16:30:09 EST	2009-07-04 14:40:23 EDT	2009-10-14 10:57:49 EDT	53760
FREE MOONSHINE RECIPES.htm	▽		0	2009-10-13 20:55:10 EDT	2011-01-28 16:30:09 EST	2009-07-04 14:39:54 EDT	2009-10-13 20:55:10 EDT	51621

American Medicinal Spirits Company

Digger Odell Publications ©2004
The American Medicinal Spirits Company appears to have been formed around 1920 to meet the need of providing medicinal whiskey to the lame and blind during Prohibition after the passage of the Volstead Act in 1919. The process of consolidation in the liquor industry had started prior to the passage of the Volstead Act. The smaller companies resisted take-over and often managed to undercut the big companies prices and stay in favor with their local patrons. Prohibition would deal the death blow to most. The number of distilling establishments in the United States started to decline after hitting a peak number of 965 establishments in 1899. By 1914, the number had dropped to 434 establishments and throughout the Prohibition years it ranged from only 27-33 distillers. Among those was the The American Medicinal Spirits Company-one distilling family's answer to the crushing Federal Legislation. There would be only handful of companies ready when the ban was lifted to consolidate and dominate the liquor market. The American Medicinal Spirits Company would be one of them and was one of the few distillers legally selling booze during the prohibited years.

Figure 7: Proof that Granny can legally make and distribute alcohol

As for Jethro, he has a deleted file that contains legal questions for an informant and police officer to fill out so law enforcement can gain intelligence about a crime group and break it up. The file is shown below in Figure 8. This indicates that although Jethro may be committing crimes, he is also working with law enforcement to break up the crime group. An explanation for why he deleted this file could be that he didn't want anyone to figure out that he was working undercover with law enforcement.



cipack.pdf	2009-10-15 21:51:52 EDT	2009-10-16 09:58:27 EDT	2009-10-16 09:58:27 EDT	2009-10-16 09:58:27 EDT	151832

Each of them will now state and spell their name for the benefit of transcribing this tape.

The informant providing information is ________________. I have shown the agreement and reviewed its provisions with him/her (and his/her attorney ________________________).

I have explained that, if we proceed, any and all agreements between him/her and the State of must be set forth in this document and that there are no agreements or understandings other than those set forth in this agreement.

I have explained that as an informant, the State of will not pay any funds other than out-of-pocket expenses incurred in connection with a criminal investigation which are deemed to be necessary by the control officer.

______________________, does this correctly reflect what I have told you?

1. Do you understand and agree that you are not permitted or privileged to break any laws during the course of your association with ____________ ________ except upon the specific instructions of your control officer and then only when your conduct does not involve violence or the threat thereof? __________

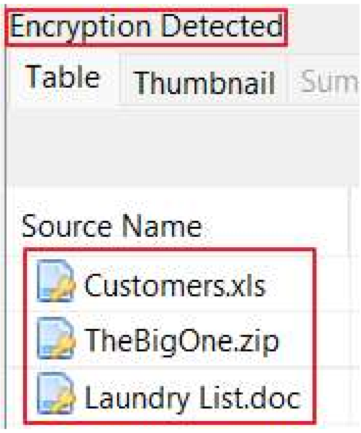
2. Do you understand and agree that you are neither an employee of the ____ ____________ nor a police officer? ___________

3. Do you understand and agree that unless previously and explicitly authorized by your control officer you are not to release any funds entrusted to you until you have first received the property or contraband for which you are negotiating? _________

4. Do you understand and agree that you are not to begin negotiations for any property or contraband without first advising your control officer and receiving permission to proceed? __________

Figure 8: Proof that Jethro is working with law enforcement

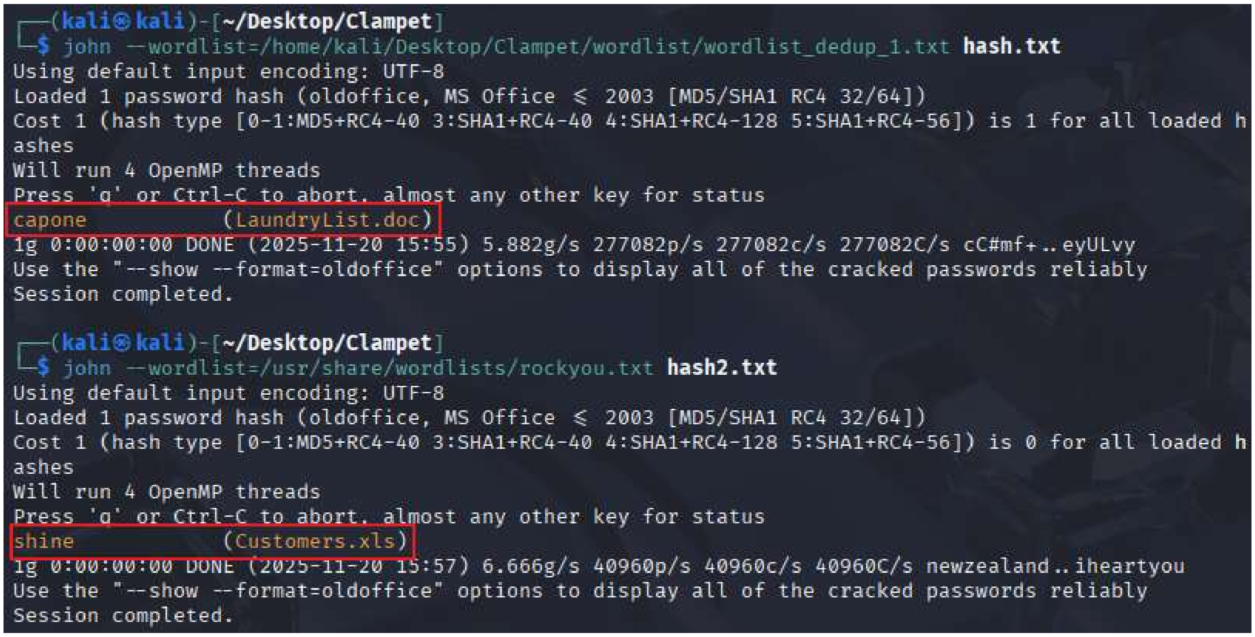
There were encrypted files on the computer that required the use of John the Ripper in Kali Linux to crack the password. These three files are shown below in Figure 9.



Source Name
Customers.xls
TheBigOne.zip
Laundry List.doc

Figure 9: Encrypted files in Autopsy

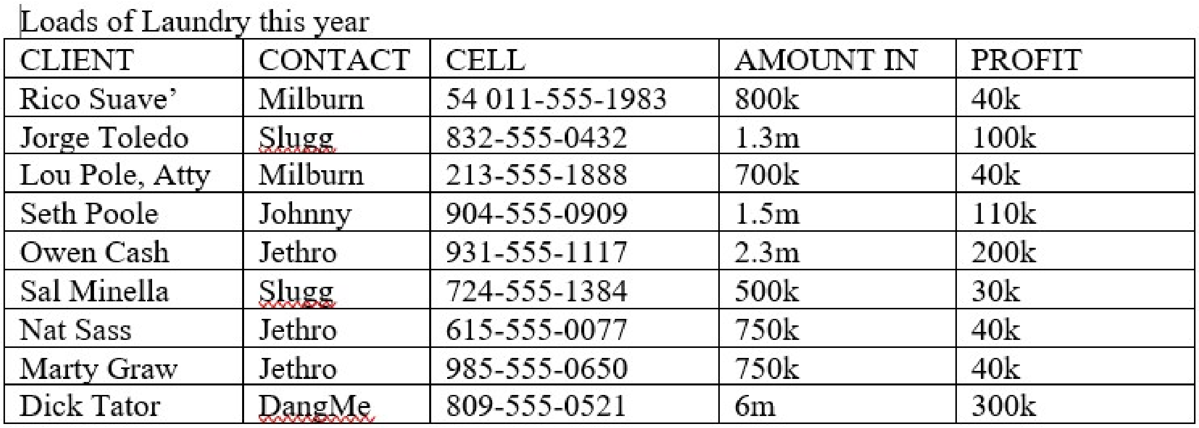
I used Bulk Extractor to create a custom wordlist from the disk image, which would be used with John the Ripper to crack the password hashes of the encrypted files. If the custom wordlist didn't work, then I used the rockyou.txt wordlist that comes with Kali Linux. The successful password cracking process is shown in Figure 10. The .zip file “TheBigOne.zip” itself is not encrypted, but the .mp3 inside of it is encrypted. Like “Laundry List.doc”, the password was “capone”. The message in the .mp3 file was a plan for Jethro to go to an airport in California, get money from a plane, and take it to a local bank. The contents of the other two encrypted files are shown in Figures 11 and 12. “Laundry List.doc” shows who are involved in the crime group, as well as how much money was laundered. “Customers.xls” shows what types of alcoholic beverages Granny is making, who buys them, and how much they owe her.



```
┌──(kali㉿kali)-[~/Desktop/Clampet]
└─$ john --wordlist=/home/kali/Desktop/Clampet/wordlist/wordlist_dedup_1.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
capone           (LaundryList.doc)
1g 0:00:00:00 DONE (2025-11-20 15:55) 5.882g/s 277082p/s 277082c/s 277082C/s cC#mf+..eyULvy
Use the "--show --format=oldoffice" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop/Clampet]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash2.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 0 for all loaded h
ashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
shine            (Customers.xls)
1g 0:00:00:00 DONE (2025-11-20 15:57) 6.666g/s 40960p/s 40960c/s 40960C/s newzealand..iheartyou
Use the "--show --format=oldoffice" options to display all of the cracked passwords reliably
Session completed.
```

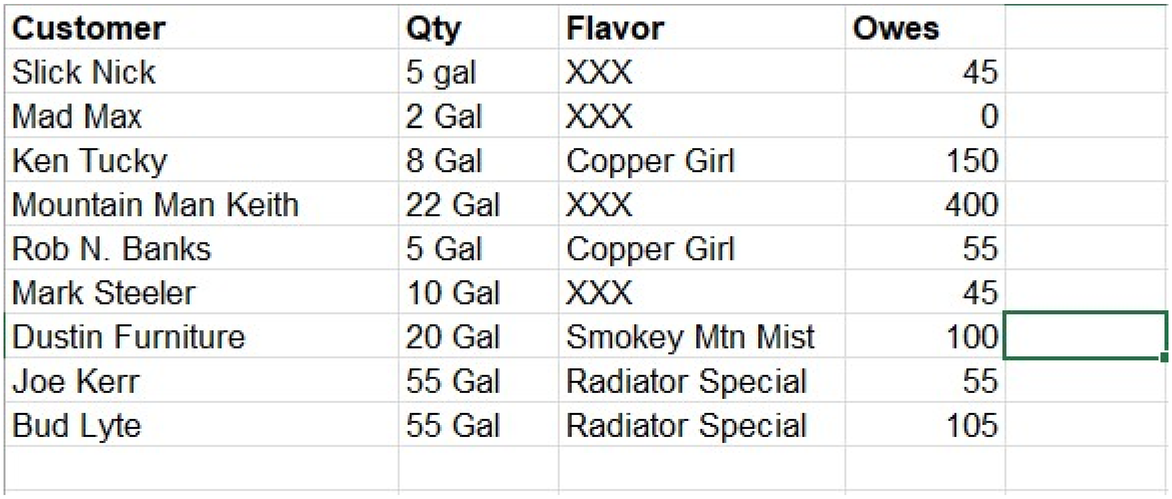
Figure 10: Cracked passwords for the encrypted files



Loads of Laundry this year

CLIENT	CONTACT	CELL	AMOUNT IN	PROFIT
Rico Suave’	Milburn	54 011-555-1983	800k	40k
Jorge Toledo	Slugg	832-555-0432	1.3m	100k
Lou Pole, Atty	Milburn	213-555-1888	700k	40k
Seth Poole	Johnny	904-555-0909	1.5m	110k
Owen Cash	Jethro	931-555-1117	2.3m	200k
Sal Minella	Slugg	724-555-1384	500k	30k
Nat Sass	Jethro	615-555-0077	750k	40k
Marty Graw	Jethro	985-555-0650	750k	40k
Dick Tator	DangMe	809-555-0521	6m	300k

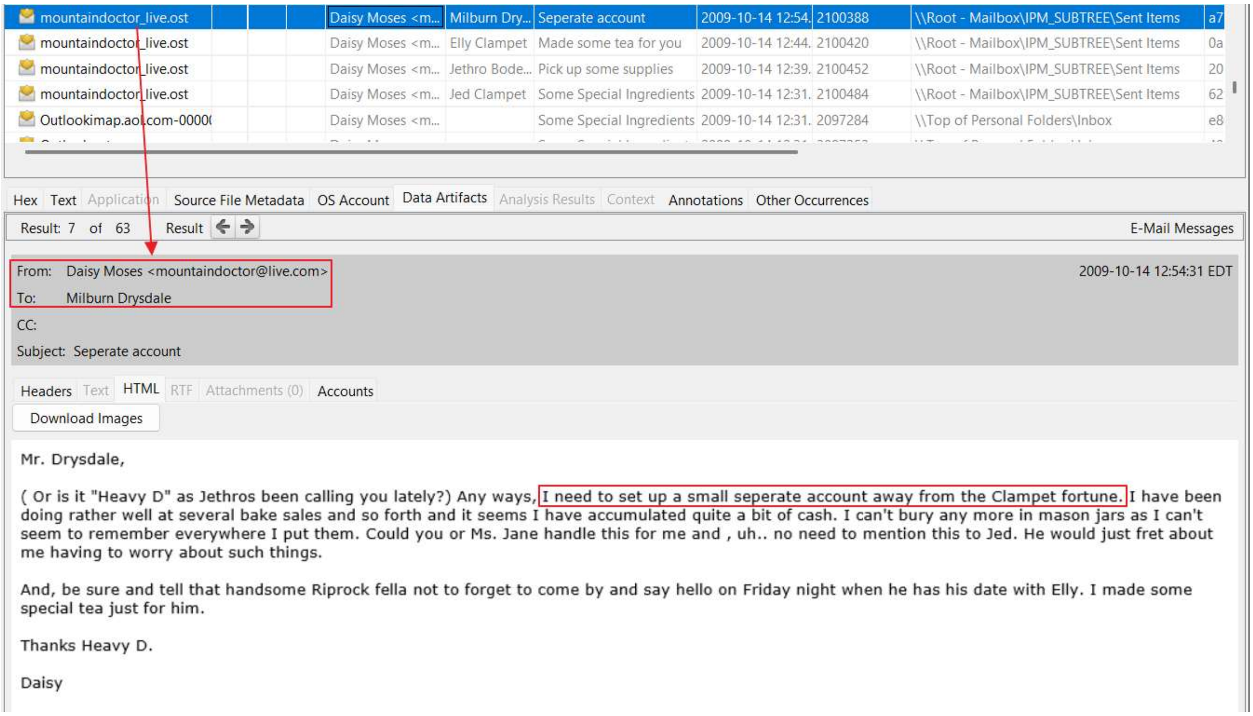
Figure 11: Laundry List.doc unencrypted



Customer	Qty	Flavor	Owes
Slick Nick	5 gal	XXX	45
Mad Max	2 Gal	XXX	0
Ken Tucky	8 Gal	Copper Girl	150
Mountain Man Keith	22 Gal	XXX	400
Rob N. Banks	5 Gal	Copper Girl	55
Mark Steeler	10 Gal	XXX	45
Dustin Furniture	20 Gal	Smokey Mtn Mist	100
Joe Kerr	55 Gal	Radiator Special	55
Bud Lyte	55 Gal	Radiator Special	105

Figure 12: Customers.xls unencrypted

There are several emails and contacts found on this computer, indicating connections between Jethro and the other people involved in the money laundering scheme. They are listed as Dang MeDang Me, Johnny Rottencore, Sluggy, and Milburn Drysdale. There was an email between Granny and Milburn in which Granny asked him to set up a new bank account for her to store money she earns, possibly to avoid getting questioned by the bank. This can be seen below in Figure 13. The other emails were about the some of the other users on this computer doing chores for one another.



mountaindoctor_live.ost				Daisy Moses <m...	Milburn Dry...	Seperate account	2009-10-14 12:54.	2100388	\\Root - Mailbox\IPM_SUBTREE\Sent Items	a7
mountaindoctor_live.ost				Daisy Moses <m...	Elly Clampet	Made some tea for you	2009-10-14 12:44.	2100420	\\Root - Mailbox\IPM_SUBTREE\Sent Items	0a
mountaindoctor_live.ost				Daisy Moses <m...	Jethro Bode...	Pick up some supplies	2009-10-14 12:39.	2100452	\\Root - Mailbox\IPM_SUBTREE\Sent Items	20
mountaindoctor_live.ost				Daisy Moses <m...	Jed Clampet	Some Special Ingredients	2009-10-14 12:31.	2100484	\\Root - Mailbox\IPM_SUBTREE\Sent Items	62
Outlookimap.aol.com-0000(				Daisy Moses <m...		Some Special Ingredients	2009-10-14 12:31.	2097284	\\Top of Personal Folders\Inbox	e8

From: Daisy Moses <mountaindoctor@live.com>
To: Milburn Drysdale
CC:
Subject: Seperate account

2009-10-14 12:54:31 EDT

Mr. Drysdale,

(Or is it "Heavy D" as Jethros been calling you lately?) Any ways, I need to set up a small seperate account away from the Clampet fortune. I have been doing rather well at several bake sales and so forth and it seems I have accumulated quite a bit of cash. I can't bury any more in mason jars as I can't seem to remember everywhere I put them. Could you or Ms. Jane handle this for me and , uh.. no need to mention this to Jed. He would just fret about me having to worry about such things.

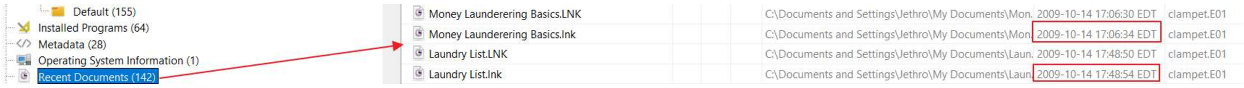
And, be sure and tell that handsome Riprock fella not to forget to come by and say hello on Friday night when he has his date with Elly. I made some special tea just for him.

Thanks Heavy D.

Daisy

Figure 13: Email between Granny and Milburn

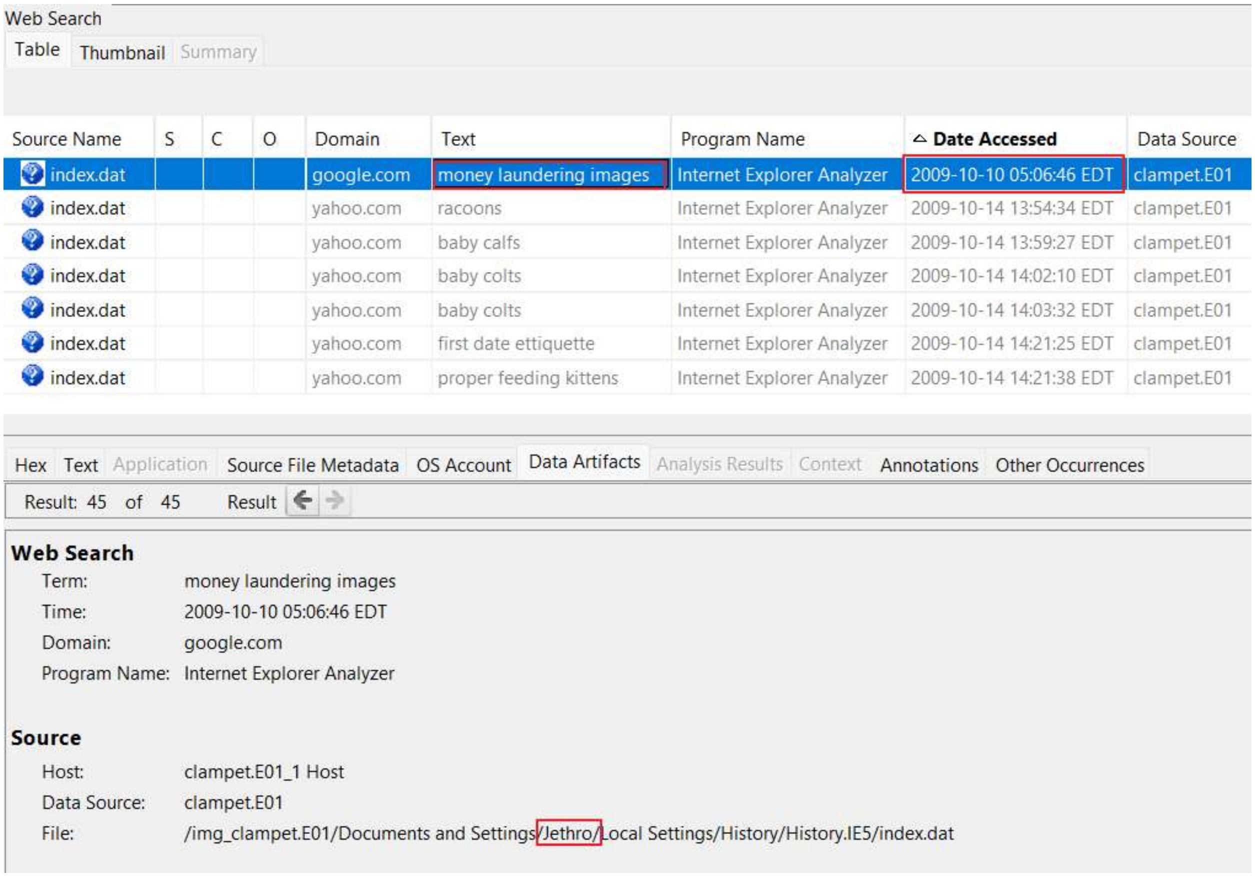
Next, I decided to look at the recent documents. I saw that Jethro opened "Money Launderering Basics.doc" on 10/14/2009 at 14:06:34 PDT and "Laundry List.doc" on 10/14/2009 at 14:48:54 PDT. This is shown in Figure 14.



Money Launderering Basics.LNK	C:\Documents and Settings\Jethro\My Documents\Mon.	2009-10-14 17:06:30 EDT	clampet.E01
Money Launderering Basics.lnk	C:\Documents and Settings\Jethro\My Documents\Mon	2009-10-14 17:06:34 EDT	clampet.E01
Laundry List.LNK	C:\Documents and Settings\Jethro\My Documents\Laun.	2009-10-14 17:48:50 EDT	clampet.E01
Laundry List.lnk	C:\Documents and Settings\Jethro\My Documents\Laun	2009-10-14 17:48:54 EDT	clampet.E01

Figure 14: Recent documents shown in Autopsy

I also noticed that Jethro searched for "money laundering images" on Google on 10/10/2009 at 2:06:46 PDT. He visited a website called moneylaundering.com on 7/31/2009 at 18:27:44 PDT. Granny visited jackdaniels.com on 10/14/2009 at 11:54:55 PDT, showing her interest in alcohol. This can be seen in Figures 15-17.



Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
index.dat				google.com	money laundering images	Internet Explorer Analyzer	2009-10-10 05:06:46 EDT	clampet.E01
index.dat				yahoo.com	racoons	Internet Explorer Analyzer	2009-10-14 13:54:34 EDT	clampet.E01
index.dat				yahoo.com	baby calfs	Internet Explorer Analyzer	2009-10-14 13:59:27 EDT	clampet.E01
index.dat				yahoo.com	baby colts	Internet Explorer Analyzer	2009-10-14 14:02:10 EDT	clampet.E01
index.dat				yahoo.com	baby colts	Internet Explorer Analyzer	2009-10-14 14:03:32 EDT	clampet.E01
index.dat				yahoo.com	first date ettiquette	Internet Explorer Analyzer	2009-10-14 14:21:25 EDT	clampet.E01
index.dat				yahoo.com	proper feeding kittens	Internet Explorer Analyzer	2009-10-14 14:21:38 EDT	clampet.E01

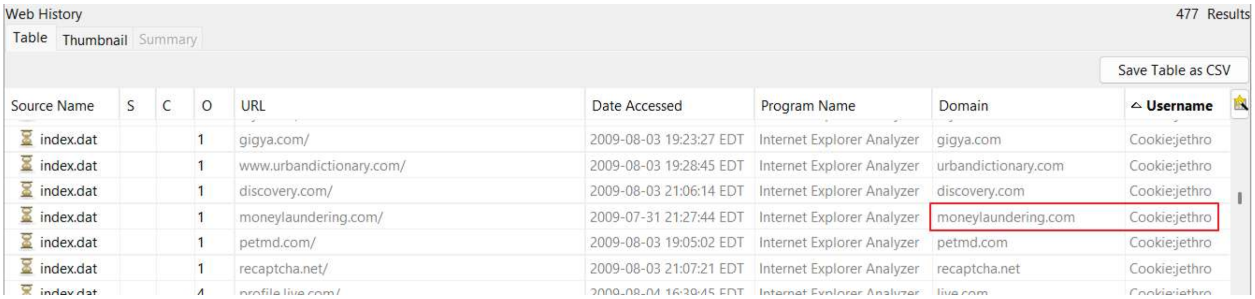
Web Search

Term:	money laundering images
Time:	2009-10-10 05:06:46 EDT
Domain:	google.com
Program Name:	Internet Explorer Analyzer

Source

Host:	clampet.E01_1 Host
Data Source:	clampet.E01
File:	/img_clampet.E01/Documents and Settings/Jethro/Local Settings/History/History.IE5/index.dat

Figure 15: Suspicious search term by Jethro

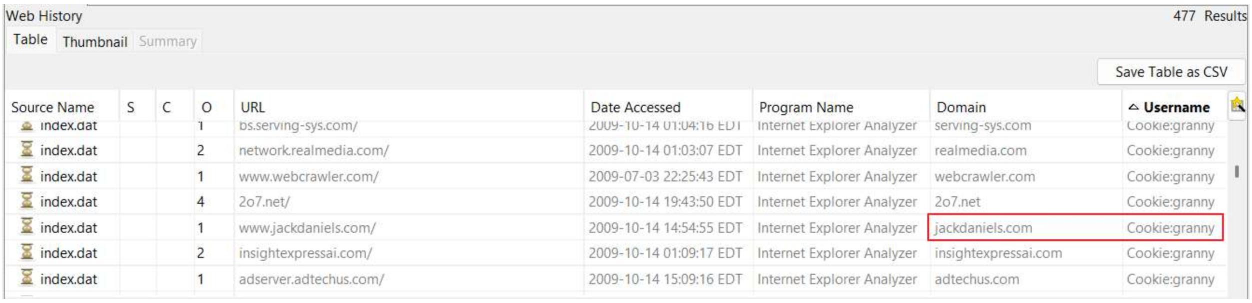


Web History

477 Results

Source Name	S	C	O	URL	Date Accessed	Program Name	Domain	Username
index.dat			1	gigya.com/	2009-08-03 19:23:27 EDT	Internet Explorer Analyzer	gigya.com	Cookie:jethro
index.dat			1	www.urbandictionary.com/	2009-08-03 19:28:45 EDT	Internet Explorer Analyzer	urbandictionary.com	Cookie:jethro
index.dat			1	discovery.com/	2009-08-03 21:06:14 EDT	Internet Explorer Analyzer	discovery.com	Cookie:jethro
index.dat			1	moneylaundering.com/	2009-07-31 21:27:44 EDT	Internet Explorer Analyzer	moneylaundering.com	Cookie:jethro
index.dat			1	petmd.com/	2009-08-03 19:05:02 EDT	Internet Explorer Analyzer	petmd.com	Cookie:jethro
index.dat			1	recaptcha.net/	2009-08-03 21:07:21 EDT	Internet Explorer Analyzer	recaptcha.net	Cookie:jethro
index.dat			4	profile.live.com/	2009-08-04 16:39:45 EDT	Internet Explorer Analyzer	live.com	Cookie:jethro

Figure 16: Website visited by Jethro



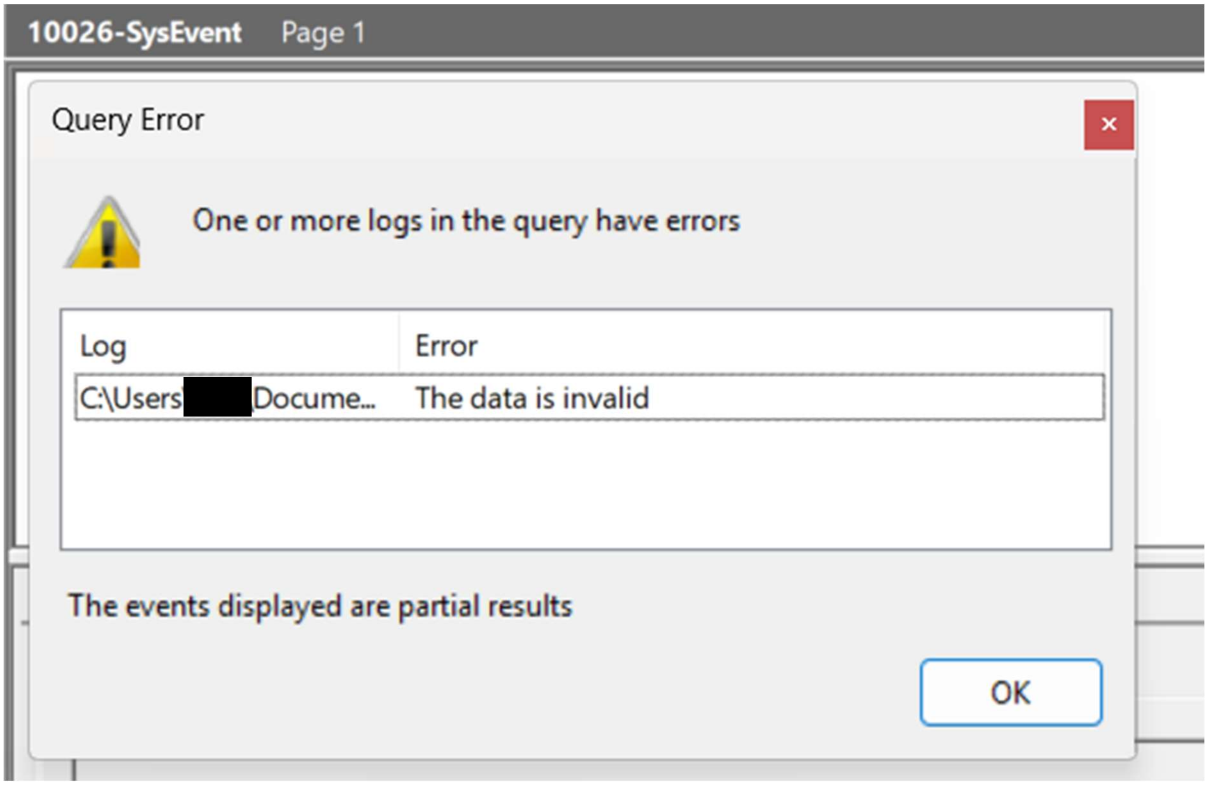
Web History

477 Results

Source Name	S	C	O	URL	Date Accessed	Program Name	Domain	Username
index.dat			1	bs.serving-sys.com/	2009-10-14 01:04:16 EDT	Internet Explorer Analyzer	serving-sys.com	Cookie:granny
index.dat			2	network.realmedia.com/	2009-10-14 01:03:07 EDT	Internet Explorer Analyzer	realmedia.com	Cookie:granny
index.dat			1	www.webcrawler.com/	2009-07-03 22:25:43 EDT	Internet Explorer Analyzer	webcrawler.com	Cookie:granny
index.dat			4	2o7.net/	2009-10-14 19:43:50 EDT	Internet Explorer Analyzer	2o7.net	Cookie:granny
index.dat			1	www.jackdaniels.com/	2009-10-14 14:54:55 EDT	Internet Explorer Analyzer	jackdaniels.com	Cookie:granny
index.dat			2	insightexpressai.com/	2009-10-14 01:09:17 EDT	Internet Explorer Analyzer	insightexpressai.com	Cookie:granny
index.dat			1	adserver.adtechus.com/	2009-10-14 15:09:16 EDT	Internet Explorer Analyzer	adtechus.com	Cookie:granny

Figure 17: Website visited by Granny

I tried to look through the event logs to determine when the computer was turned on and who logged in at specific times, but the logs are corrupted and won't open properly, as shown below in Figure 18.



Query Error

One or more logs in the query have errors

Log	Error
C:\Users[redacted]Docume...	The data is invalid

The events displayed are partial results

Figure 18: Corrupted event log

Timeline

Date/Time	Event	Relevance
7/03/2009 – 16:31:27 PDT	Granny opened a file containing customer information	Shows her interest in selling homemade alcohol.
7/31/2009 – 18:27:44 PDT	Jethro visits moneylaundering.com	Indicates possible involvement with crime
10/10/2009 – 2:06:46 PDT	Jethro searches for money laundering images	Shows his involvement with crime
10/14/2009 – 7:50:06 PDT	Granny creates a document containing the history of a distillery business	Indicates interest in making moonshine and other alcoholic beverages
10/14/2009 – 9:54:31 PDT	Granny sends an email to Milburn Drysdale	Shows possible involvement with the money laundering scheme
10/14/2009 – 11:54:55 PDT	Granny visits jackdaniels.com	Indicates interest in making alcoholic beverages

10/14/2009 – 14:06:34 PDT	Jethro opened a file about money laundering	Indicates involvement with money laundering
10/14/2009 – 14:48:54 PDT	Jethro opened a file containing a list of laundered money	Indicates involvement with money laundering
10/15/2009 – 15:02:03 PDT	Jethro receives a .zip folder containing a secret message with a plan to take money from a plane to a bank	Shows his involvement with other criminals
10/15/2009 – 18:51:52 PDT	Jethro obtains a file containing questions for an informant	Indicates possible interaction with law enforcement, either to come clean or help take down the crime group

Conclusions

There are several users on this Windows XP computer, but it is mainly used by Granny and Jethro despite being owned by Jed. These two users are involved in illicit activities like moonshine distilling and money laundering (the process of making a large amount of "dirty" funds appear legitimate), as shown through the pictures, files, emails, and web searches on the computer. Other people involved in the money laundering scheme with Jethro are known as Dang MeDang Me, Johnny Rottencore, Sluggy, and Milburn Drysdale. There are encrypted files on the computer, meaning only people who know the password can open and view the files. However, the passwords were easily cracked. These encrypted files contained customer information, laundered money, and a plan to deliver potentially laundered money to a bank. The computer is set to Pacific Time, most likely in California since some files contained directions to and from places in California. Additionally, there were some deleted files useful to the investigation that were recovered, such as an informant questionnaire. It shows that Jethro might be working with law enforcement instead of actually committing crime and laundering money. There is also reason to believe that Granny can legally make and distribute homemade alcohol because of a file on her computer explaining the history and legal status of a distillery company. She could be an owner of that company or trying to form a new branch/location.