Clampet.E01

Digital Forensics Report

Prepared By:

**Brennen Yingling**

Professor:

**Mr. Michael Zambotti**

Class:

**CSA 201: Digital Forensics**

Date:

**December 12, 2025**

**Table of Contents**

1. Introduction ………………………………………………………..………………………… 2
   1. Executive Summary ………………………………………..………………………….... 2
   2. Tools Used …………………………………………………….………………………... 2
   3. Process ……………………………………………………….…………………….…… 3
2. Findings ……………………………………………………………………………………... 4
   1. Findings and Evidence – Initial Investigation ………………………………………….. 4
   2. Findings and Evidence – Moonshine …………………………………………………… 8
   3. Findings and Evidence – Money Laundering ………………………………………… 10
   4. Findings and Evidence – Password-Protected Files …………………………………... 14
3. Conclusion ………………………………………………………….,.…………………….. 16
   1. Story ………………………………………………………………………………….... 16
   2. Timeline ……………………………………………………………………………….. 17
   3. Concluding Statement ……………………………………………………...………….. 17
4. **Introduction**

The purpose of this assessment is to review the Clampet.E01 image and become familiar with using tools such as Autopsy, Kali, John the Ripper, and FTK Imager, as well as any other digital forensics tools that may be needed. In this report, I will provide pictures of any evidence of illegal activities I find on this image, along with a timeline of my findings, an overview of my process, and the various tools I used.

* 1. **Executive Summary**

On November 25, 2025, Professor Zambotti provided me with an image of the *Clampet* computer hard drive. Professor Zambotti is requesting a forensic examination to see what information may have been deleted, and is requesting a full forensic examination and report for the image of this drive. From the information provided, the *Clampet* image was collected in relation to a criminal investigation. I have searched for this drive to find evidence that shows the user is involved in illegal activity. After my investigation, the evidence I found suggests that the user could be related to buying, making, or selling moonshine, as well as money laundering.

* 1. **Tools Used**

Throughout my investigation, I used several different tools to analyze the image, document my findings, and show evidence, including:

|  |  |
| --- | --- |
| **Tool Name** | **What the Tool was used for** |
| Autopsy 4.22.1 (Latest Version) | I used this tool to examine the Clampet.E01 image. |
| Exterro FTK Imager (Latest Version) | I used FTK Imager to verify the MD5 hash related to the Clampet.E01 image. |
| John The Ripper (Kali Linux) | I used the John the Ripper tool in Kali Linux to crack passwords for three password-protected files. |
| Notepad | I used this tool to document my process and keep a timeline of when I found each flag. |
| Snipping Tool | I used this tool to screenshot and edit my findings. |

* 1. **Process**

Throughout my investigation period, my process involved first opening Notepad and documenting my start time for the day. Next, I had four steps to my investigation. First, I conducted my initial investigation, which involved verifying the image and examining it closely to tag anything that could be incriminating. The second step involved looking through one of the tagged items folders, in this case, that is anything involving moonshine. Third, I reviewed my next folder of tagged items, which is related to money laundering. The last step is opening Kali Linux on a virtual machine and running the John the Ripper tool for any password-protected files I found in my initial investigation. Any evidence I found throughout my investigation I screenshotted and placed it in a secure folder on my laptop. Whenever I finished for the day, I would document the end time for that investigation.

1. **Findings**

In this section of my report, I will include screenshots of any evidence I was able to locate, as well as a detailed description of what the evidence is, how I found it, and when I found it.

* 1. **Findings and Evidence – Initial Investigation**

This section of my report contains information about my initial investigation, including verification of the hash values, information about the device and user, and my initial findings. I began my investigation at 4:50 P.M. UTC on November 25th, 2025, by loading the Clampet.E01 file into Exterro FTK Imager. I clicked on the “Verify Image” button, and a text box appeared with the MD5 and SHA1 hash of the file. I then matched those hash values with the hash values provided by Professor Zambotti, as shown in Figure 1; they match up.

**A screenshot of a computer

AI-generated content may be incorrect.**

Figure : File Hash Values

At 5:03 P.M. UTC, I found the main user and the device operating system. After loading the image into Autopsy, I clicked on the Operating System Information tab in the left-hand pane of Autopsy. As shown in Figure 2, the main account user is Jethro Clampet, and the operating system is Microsoft Windows XP Service Pack 2.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : OS and main account user.

Then, at 5:20 P.M. UTC, I began my search for any suspicious evidence items that are in this image file. In my search, I found three different password-protected files that are shown in Figure 3. I will further examine these files later in my investigation. Also, any evidence I found I tagged with a custom tag. In Figure 4, you can see I tagged 32 items related to “Moonshine” and 17 items related to “Money Laundering.” At 6:32 P.M. UTC, on November 25th, 2025, I wrapped up my investigation for the day.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Password-protected file.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Custom tagged items.

* 1. **Findings and Evidence – Moonshine**

At 8:35 P.M. UTC on December 3rd, 2025, I reopened the Clampet image in Autopsy to continue my investigation. During my initial investigation, I located a total of 32 files relating to making, selling, or distributing moonshine. When I searched through these files in more depth, I realized that a lot of the files are the same or very similar. In this section, I will showcase three of the most incriminating pieces of evidence. At 8:38 P.M. UTC, I located a file named moonshiners[1].htm, which can be shown in Figure 5. This file appears to be an invitation to a moonshiners' reunion, indicating that there is some relation between the Clampets and moonshine.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Suspicious Invitation

The next piece of evidence was examined at 8:47 P.M. UTC and was a file called FREE MOONSHINE RECIPES.htm. This file, shown in Figure 6, appears to be a website containing different moonshine recipes. This website indicates that the user is possibly making their own moonshine.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Moonshine Recipes

Lastly, at 8:52 P.M. UTC, I found an image called still2[1].jpg, shown in Figure 7. This image appears to be an image of an old moonshine still, possibly used by the Clampets to make their own moonshine. Then, at 9:16 P.M. UTC, I closed Autopsy a finished my investigation for the time being.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Image of a still

* 1. **Findings and Evidence – Money Laundering**

At 12:24 A.M. UTC on December 4th, 2025, I started my investigation back up. In my initial investigation, I located 17 different pieces of evidence relating the Clampets to money laundering. At 12:30 A.M. UTC, I located three suspicious searches. The first is “smurf money,” where the first result is a money laundering panel, which can be shown in Figure 8. Next, shown in Figure 9, is a search for “money laundering,” and the last is a search for “money laundering techniques,” which can be seen in Figure 10.

A computer screen shot of a computer

AI-generated content may be incorrect.

Figure : Smurf Money

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Money Laundering

A computer screen with a computer screen

AI-generated content may be incorrect.

Figure : Money Laundering Techniques

At 12:42 A.M. UTC, I located two different files related to money laundering. The first document, called *simple concept.doc*, can be seen in Figure 11 and contains a lot of basic information about money laundering. The other document, called *Money Laundering Basics.doc*, is shown in Figure 12 and contains a lot of information about money laundering.

A computer screen shot of a computer screen

AI-generated content may be incorrect.

Figure : simple concept.doc

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Money Laundering Basics.doc

* 1. **Findings and Evidence – Password-Protected Files**

Now I will turn my attention towards the three password-protected files I found earlier, which can be seen in Figure 3. For this section, I will use a virtual machine to run some password-cracking tools like John the Ripper on a Kali machine. I began with the document named *Laundry List.doc*. At 4:57 P.M. UTC, I copied the file onto my virtual machine and ran the John the Ripper tool using the *rockyou.txt* wordlist, which is a list of commonly used passwords. The password *capone* worked for this file, the contents, shown in Figure 13, appear to be a list of names, contact information, amount in, and profit columns inside of a table.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Laundry List.doc

The next file is called *Customers.xls*. Since I already have a working password, I tested *capone*, but it did not give me access to the file. At 5:16 P.M. UTC, I copied the file onto my virtual machine and ran the John the Ripper tool using the *rockyou.txt* wordlist, it came back with the password *shine*. The contents of *Customers.xls,* can be seen in Figure 14, but appear to be a list of moonshine customers.

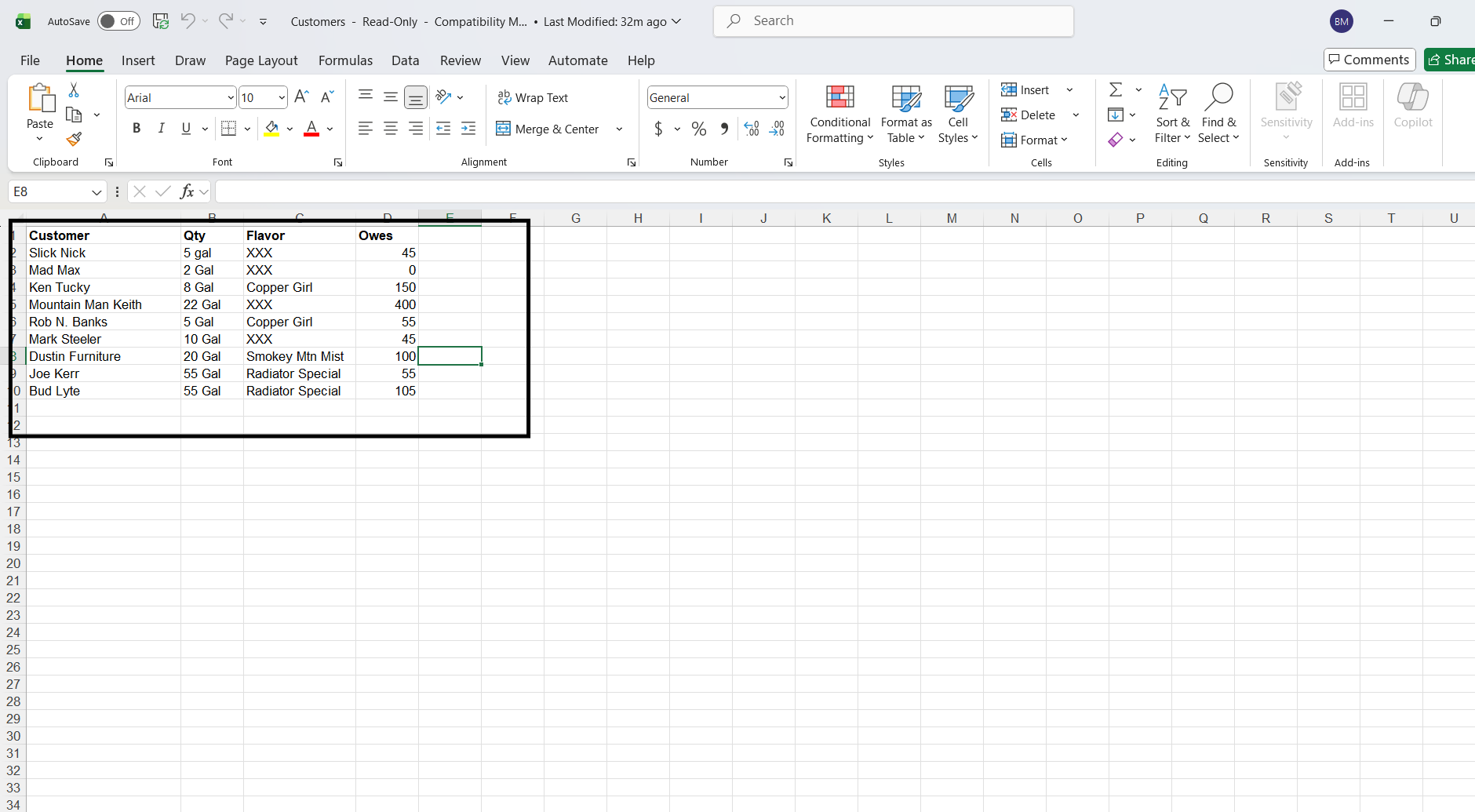


Figure : Customers.xls

The last file, named *TheBigOne.zip*, was created because I already had two previous passwords that worked. I tested them, and at 5:23 P.M. UTC, when I tested the password *Capone*, I was granted access to an MP3 file, which can be seen below. This message is a recording explaining directions; it also talks about how the iPod is password-protected. At 5:25 P.M. UTC on December 4th, 2025, I concluded my investigation of the Clampet.E01 image.



Figure : TheBigOne.zip

1. **Conclusion**
   1. **Story**

As a result of a detailed digital investigation of the Clampet.E01 drive, a much greater story emerged. Jethro Clampet, the individual who used the computer, appeared to be engaged in a secret moonshine business with a money laundering operation as well, to cover up the profits from his moonshining. The disarray of evidence, moonshine recipes, invites to family reunions, pictures of the equipment used for distilling moonshine, as well as papers that detail the methods of laundering money and suspicious online searches, indicates that this individual was directly involved with producing and distributing illegal alcohol, as well as financially manipulating the money earned from this industry. Upon further inspection of the password-protected folders found using John the Ripper, many files contained lists of customers, financial logs, and secret, coded communications that connected the moonshine business with smuggled money. The numerous digital artifacts that were retrieved and later confirmed with forensic programs such as FTK Imager and Autopsy tell the tale of a small but deliberate criminal organization that hides behind the appearance of an average Windows XP user.

* 1. **Timeline**

|  |  |  |
| --- | --- | --- |
| **Object** | **Open or Installed (UTC)** | **Significance** |
| Moonshiners[1].htm | 2009-10-13 21:09.33 | This file is an invitation to a moonshiners' reunion. The significance is that moonshining is illegal. |
| FREE MOONSHINE RECIPES.htm | 2009-10-13 20:55.10 | This file is a website containing free moonshine recipes. The significance is that moonshining is illegal. |
| Still2[1].jpg | 2009-10-13 20:31.50 | This file is a picture of a moonshine still. The significance is that moonshining is illegal. |
| Search[2].htm | 2009-07-31 13:42.54 | This file is a search for money laundering. The significance is that money laundering is illegal. |

* 1. **Concluding Statement**

In summary, the forensic examination of the Clampet.E01 image yielded a consistent and convincing pattern of unlawful activity relative to moonshine production and money laundering. The combination of tagged evidence of suspicious documents, incriminating web searches, and decrypted password-protected files together demonstrates that the user was involved in a coordinated effort to manufacture illegal alcohol and hide the proceeds. Using industry-standard tools like Autopsy, FTK Imager, and John the Ripper, each finding was verified, documented, and correlated to the greater narrative of criminal behavior. By the totality of evidence recovered, it would be reasonable to conclude that the Clampet system played a central role in facilitating and storing information related to these unlawful operations.