Clampet Image Analysis

Report

Prepared By:

Jimmie Neese

Professor Zambotti

CSA 201: Digital Forensics I

9 Dec 2025

*Executive Summary*

Throughout this report, there will be information and evidence that was obtained from an exact copy of a hard drive from a computer named “Clampet.eo1.” The user of the computer being investigated was determined to have the name “Jethro”. There were multiple different tools that were used to investigate the hard drive. These tools were all open-source tools. The hard drive was searched for multiple different forms of criminal evidence and also the criminal evidence that was found was determined to all be correlated with other members. Throughout the rest of this report, evidence on the crimes committed will be shown and explained thoroughly. The crimes that the user was determined to commit involved multiple forms and occasions of money laundering, and also the user was determined to be running a moonshining business. All the evidence included is in the form of screenshots. Also, the screenshots all have a figure assigned to them with an explanation of how the evidence is correlated. Included in the rest of the following report are the Methods/Tools Used, the Findings and Evidence, the Timeline of the investigation, and the Conclusion of the evidence.

*Methods/Tools Used*

Below is a list of Open-Source tools used during the investigation and what they were used for:

|  |  |
| --- | --- |
| Tool | Used For: |
| Forensic Toolkit (FTK) Imager | Used to make a bit-by-bit copy of the hard drive being examined |
| Autopsy | Used to search through the bit-by-bit copy of the hard drive in order to find evidence within the drive |
| Windows Registry Explorer | Used to look through multiple different hives found within the image |
| PrefetchWindows Event Viewer | Used to look through the event log found in the image. Used to search for the last use of the drive |
| PicPick (Screenshot Tool) | Used to document the evidence found within the screenshots taken |

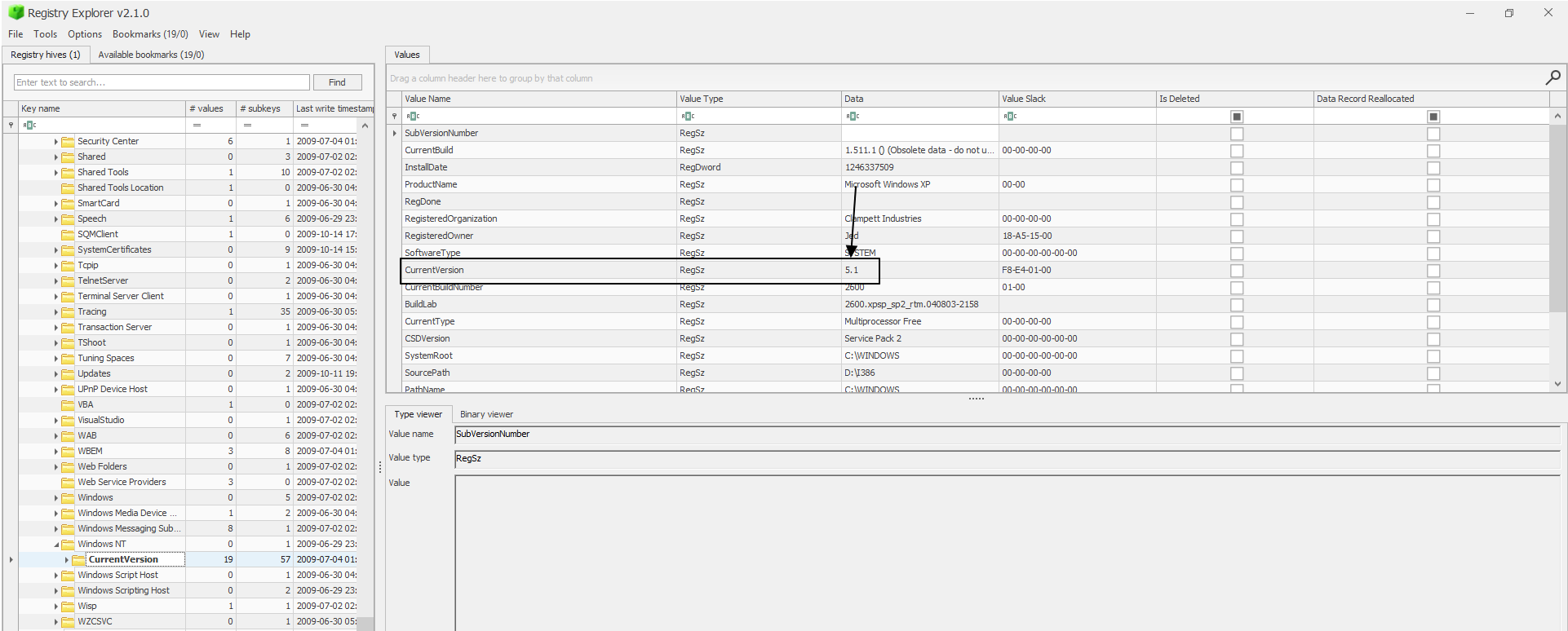
*Findings*

While investigating the “Clampet.e01” image, multiple forms of evidence brought up questions. (See below)

A screenshot of a computer

AI-generated content may be incorrect.

Figure 1 (Above): This screenshot was found in Autopsy. The evidence shows that the main user of the computer is “Jethro”. This was determined by the login count of the user. The user had the highest number of logins at 52 logins.

  
Figure 2 (Above): The figure above shows the current version of the software that is on the computer. The software was found to be Windows 5.1. This was found by inputting the software hive into the Windows Registry Explorer.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 3 (Above): The figure above shows the time zone that the computer was used in. The time zone was determined to be Pacific Standard Time. This was found by inputting the system hive into the Windows Registry Explorer.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4 (Above): The figure above was found in Autopsy. It shows that a document on the computer is named “FREE\_MOONSHINE\_RECIPES”. This brings up the question to whether or not the user was involved in illegal alcohol activities.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5 (Above): A document found while searching through the Clampet image is pictured above. The document describes what moonshine is and gives the ingredients needed to make it. This reinforces the idea that the user could have been involved with making moonshine.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 6 (Above): The figure above shows an email sent to “Jed” by an interesting email. The email asks for Jed to pick up a certain list of ingredients and asks when the “moon will be waxing next”. The email was determined to be very suspicious.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 7 (Above): The email found above is a response to the email found in Figure 6. “Jed” refers to the sender as “Granny”. Jed also refers to “Duke” in the email. This email was determined to be suspicious, and also brings up the question to whether or not the moonshining could be a family business.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 8 (Above): The figure above was found in Autopsy and seems to be an advertisement focused on buying moonshine and also items to make moonshine. This also reinforces the idea that the family could have been attempting to sell the moonshine that they made.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 9 (Above): The figure above shows the Wikipedia page for Moonshine. The Wikipedia page says that the practice is illegal. This was found using Autopsy and could also be very good for reinforcing the previous evidence.

A person standing next to a copper still

AI-generated content may be incorrect.

Figure 10 (Above): The image above is titled “moonshine-still.jpg”. This is an image of someone making moonshine, and brings up question to whether or not the individual in the photo is one of the people involved in the crime being investigated.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 11 (Above): The figure above is another photo of what moonshine can be made in. The picture is also titled “moonshine\_still3.jpg”. This helps to reinforce the evidence above.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 12 (Above): The figure above is another photo of moonshine. The picture is also titled “moonshine\_still4.jpg”. This helps to reinforce the evidence above.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 13 (Above): The figure above shows a document to a “Moonshiners Reunion”. This was determined to be suspicious because there seems to possibly be an event where groups of moonshiners show up. This could be important for further investigation.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 14 (Above): The conversation found above refers to a jug marked “Special Tea”. This could be a keyword or phrase that the suspects call the moonshine they make in order to keep it secretive.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 15 (Above): The figure above shows a conversation that includes information about the user possibly burying money. This email was determined to be very suspicious and was looked into further.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 16 (Above): This document was found in Autopsy while examining the Clampet image. The document gives information on “Money Laundering Basics”. This helps to reinforce the idea that the user could have been involved in money laundering

A screenshot of a computer

AI-generated content may be incorrect.

Figure 17 (Above): The figure above is a web search that was made by the user. The search was for “money laundering techniques”. This is a very important piece of evidence that also reinforces that the user could have been money laundering.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 18 (Above): Above is another piece of evidence found. This evidence is a document that was found on the computer titled “Money Laundering Basics.doc”

A screenshot of a computer

AI-generated content may be incorrect.

Figure 19 (Above): In the screenshot above, a web search for “money laundering images” was found in Autopsy. This provides more concrete evidence concerning the user’s involvement in money laundering.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 20 (Above): The screenshot above shows a search made by the user for “Money laundering”. This also reinforces the idea that the user had an interest in money laundering and could have been doing so.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 21 (Above): The image above shows a search made by the user for “smurf money”. After looking into the topic, it was concluded that smurf money is basically just laundered money. This is more concrete evidence that the user was money laundering.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 22 (Above): Above is a document found on the computer that is a “Debriefing Report Questionnaire”. This brings up question to whether or not the user has been arrested before, or if the user had to debrief someone before.

*Timeline*

Below is a timeline of the investigation taken place on the “Clampet.e01” image:

|  |  |  |
| --- | --- | --- |
| Date: | Time: | Event: |
| 4 Dec 2025 | 2:50 PM | The SECURITY hive was located and extracted from the image |
| 4 Dec 2025 | 2:55 PM | The SOFTWARE hive was located and extracted from the image |
| 4 Dec 2025 | 2:57 PM | The SYSTEM hive was located and extracted from the image |
| 4 Dec 2025 | 3:00 PM | The SysEvent.Evt hive was located and extracted from the image |
| 9 Dec 2025 | 2:59 PM | The main user of the computer was located and documented |
| 9 Dec 2025 | 3:03 PM | The current version of the software on the computer was located on the Windows Registry Viewer |
| 9 Dec 2025 | 3:13 PM | The TimeZoneInformation was found and documented from the Windows Registry Viewer |
| 9 Dec 2025 | 3:18 PM | A suspicious debriefing document was found and documented |
| 9 Dec 2025 | 3:42 PM | A search made by the user for “Money Laundering Images” was found and documented |
| 9 Dec 2025 | 3:55 PM | A suspicious document titled “Free Moonshine Recipes” was found and documented |
| 9 Dec 2025 | 4:08 PM | An email conversation including a list of ingredients was found and documented |
| 9 Dec 2025 | 4:15 PM | The reply to the ingredients email was found and documented |
| 9 Dec 2025 | 4:22 PM | An email with a conversation about the “Special Tea” was found and documented |
| 9 Dec 2025 | 4:33 PM | An email conversation about burying money with possible hints of money laundering was found and documented |
| 9 Dec 2025 | 4:37 PM | A search made by the user for “money laundering basics” was found and documented |
| 9 Dec 2025 | 4:42 PM | A “MoonShiners Reunion” invitation was found and documented |
| 9 Dec 2025 | 4:45 PM | An advertisement selling moonshine was found and documented |
| 9 Dec 2025 | 4:55 PM | A suspicious document called “HowToMakeHomemadeMoonshine” was found and documented |
| 9 Dec 2025 | 4:57 PM | Three images of people making moonshine were found and documented |
| 9 Dec 2025 | 5:11 PM | A search for “smurf money” made by the user was found and documented |
| 9 Dec 2025 | 5:15 PM | Another search regarding money laundering was found and documented |
| 9 Dec 2025 | 5:22 PM | A search made by the user for “Money Laundering Techniques” was found and documented |
| 9 Dec 2025 | 5:29 PM | A search made by the user for “Money Laundering Basics” was found and documented |

*Conclusion*

Following the examination of the “Clampet.eo1” image, many different things can be taken into consideration. The investigation of the hard drive was done using multiple different online tools. These tools include FTK Imager, Autopsy, Windows Registry Explorer, PrefetchWindows Event Viewer, and PicPick. The tools were used in different ways and occurrences to help to find all the evidence and connections made within the report. The main user of the computer was determined to be “Jethro”. Jethro was determined to be involved in two main types of crimes that could prove him to be a criminal. These crimes included money laundering in multiple different forms and making and selling moonshine. First, many different forms of evidence were found that could convict Jethro of buying and selling moonshine. The user seemed to be very interested in searching for recipes (Figure 4,5). This brought up suspicion as to whether the user was actually acting on these activities. The hard drive was further looked in to, and it was found that there were multiple email conversations that included information on the crime (Figure 6,7). These emails involved communication with multiple different people, one of them being named “Granny.” This brought up suspicion that the moonshining could have possibly been a family business. This was also further investigated, and it was determined that it was either a family business, or the business was run using codenames over email to ensure the confidentiality of who was actually behind the crimes. It was determined that the user was selling the moonshine because of evidence found of advertising and a “Moonshiners Reunion” (Figure 8,13). Secondly, there are many different pieces of evidence that lead the investigator to determine that the user was also money laundering. In multiple of the figures above, it is shown that the user has made many different searches about money laundering and the techniques of money laundering (Figure 16, 17, 20, 21). Furthermore, the user also has an email conversation that has information about money being buried and hidden (Figure 15). Overall, the user, Jethro, could be determined to be a criminal due to the multiple crimes he has been determined to commit. These crimes include making and selling moonshine, and multiple different occurrences of money laundering.