Digital Forensics

Contents

Abstract

This digital forensics investigation examines the case of Craig Tucker, a suspect apprehended for allegedly using counterfeit coupons at a Walmart store in Santa Monica. Following Tucker's arrest, a forensic analysis of his computer was conducted under a search warrant to uncover evidence linking him to the creation, distribution, or possession of fraudulent coupons . Using tools such as Autopsy , FTK Imager , and Registry Explorer , the investigation analyzed artifacts including browser history, deleted files, email communications, and USB device logs. The objectives were to determine the origin of the counterfeit coupons, validate Tucker's claim of obtaining them via an online survey, and identify potential collaboration with external parties. The analysis adhered to forensic best practices, ensuring evidentiary integrity for legal proceedings. This case highlights the critical role of digital forensics in correlating physical evidence with digital footprints while addressing challenges such as recovering deleted data and verifying intent.

Introduction

This investigation centers on the Craig Tucker case , where Walmart security identified a surge in fraudulent coupon redemptions for Monster Energy drinks and Arizona Ice Tea beverages at their Santa Monica store. Surveillance footage led to the detention of Craig Tucker, a suspect who matched the description of an individual passing counterfeit coupons. Despite Tucker's claim that the coupons were obtained innocently through an online survey for Santa Monica Community College students, Walmart security escalated the case to the Santa Monica Police Department, resulting in his arrest. A search warrant authorized a forensic analysis of Tucker's computer to uncover evidence related to the creation, distribution, or possession of fraudulent coupons . The investigation aims to determine whether digital artifacts—such as files, emails, browser history, or USB device logs—support Tucker's claims or reveal intent to commit fraud. By analyzing the forensic image of his hard drive using tools like Autopsy and Registry Explorer, the goal is to reconstruct his digital activities, validate the origin of the coupons, and produce findings admissible for prosecution. This case underscores the critical role of digital forensics in bridging physical evidence with digital footprints while navigating challenges like deleted data recovery and ensuring legal compliance.

Literature Review

Hayes, D. (2020). Practical Guide to Digital Forensics Investigations .

This text emphasizes hands-on techniques for evidence collection, analysis, and reporting, aligning with the phased approach used in this project. It highlights tools like Autopsy and Registry Explorer, which were critical for analyzing the Craig Tucker case.

Le-Khac, N.-A., & Choo, K.-K. R. (2020). Cyber and Digital Forensic Investigations: A Law Enforcement Practitioner's Perspective .

This work bridges technical analysis with legal compliance, ensuring evidence preservation and admissibility. It guided the interpretation of USB device logs and network timestamps in compliance with forensic standards.

Scott, P. (2020). Digital Forensic Analysis of Smart Watches .

While focused on IoT devices, this study underscores the importance of recovering data from unconventional sources. Its principles informed the analysis of USB artifacts and unallocated space in this project.

Kavrestad, J. (2020). Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications .

A comprehensive resource for timeline reconstruction and evidence correlation. It provided frameworks for linking file deletions, USB connections, and network activity in the Tucker case.

Methodology

Requirement Analysis

Hardware Requirements

1. **Processor**: Intel i5 or equivalent.
2. **RAM**: Minimum 8 GB (to ensure smooth operation of forensic tools).
3. **Storage**: 500 GB HDD (to store forensic images, tools, and analysis outputs).
4. **Operating System**: Windows/Linux (for compatibility with tools like Autopsy and Ophcrack).

Software Requirements

Open-Source Forensic Tools:

1. **Autopsy**: For disk imaging, file recovery, and timeline analysis.
2. **Registry Explorer**: To analyze Windows Registry for user activity.
3. **Ophcrack v3.7**: For password recovery and cracking.
4. **USB Historian v1.3**: To track USB device connection history.
5. **JumpLister v1.1.0**: To analyze user application usage via jump lists.
6. **DCode v4.2**: For timestamp decoding (e.g., UTC to local time).
7. **7Zip v16.04**: To extract compressed forensic artifacts.
8. **USBDeview**: To identify connected USB devices and their metadata.

Other Tools:

- **Virtual Machine**: For sandboxed analysis of suspicious files.
- **Screenshot Tool**: To capture timestamped evidence (as per submission rules).

Data Requirements

1. **Forensic Image**:
    - A bit-by-bit copy of Craig Tucker's hard drive (provided as part of the case).
    - **Verification**: SHA-256 hash validation to ensure integrity.

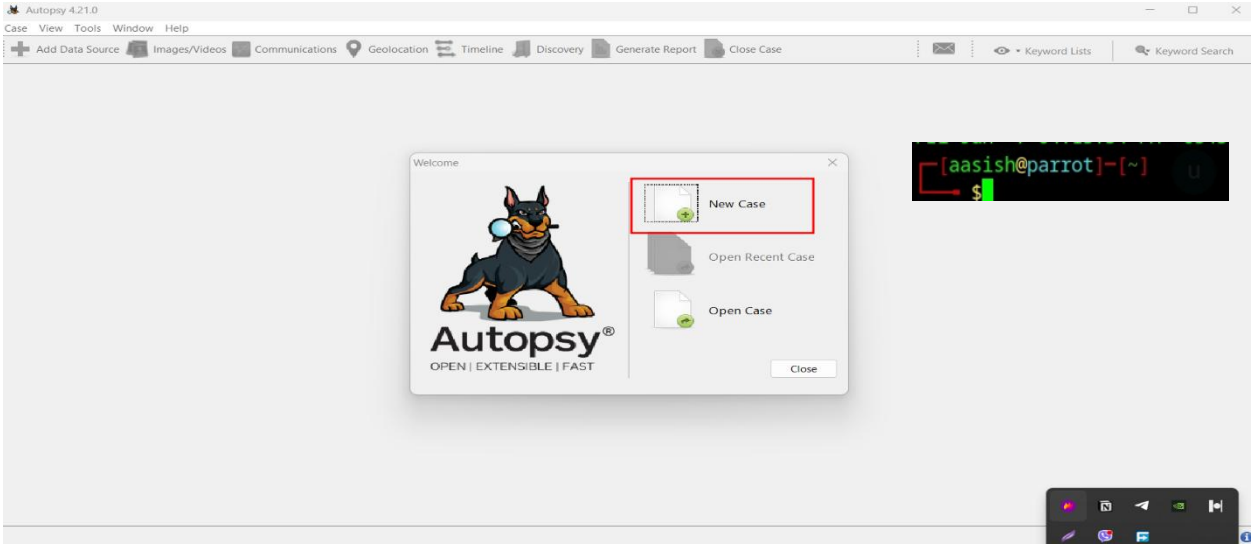
Tucker Case Summary

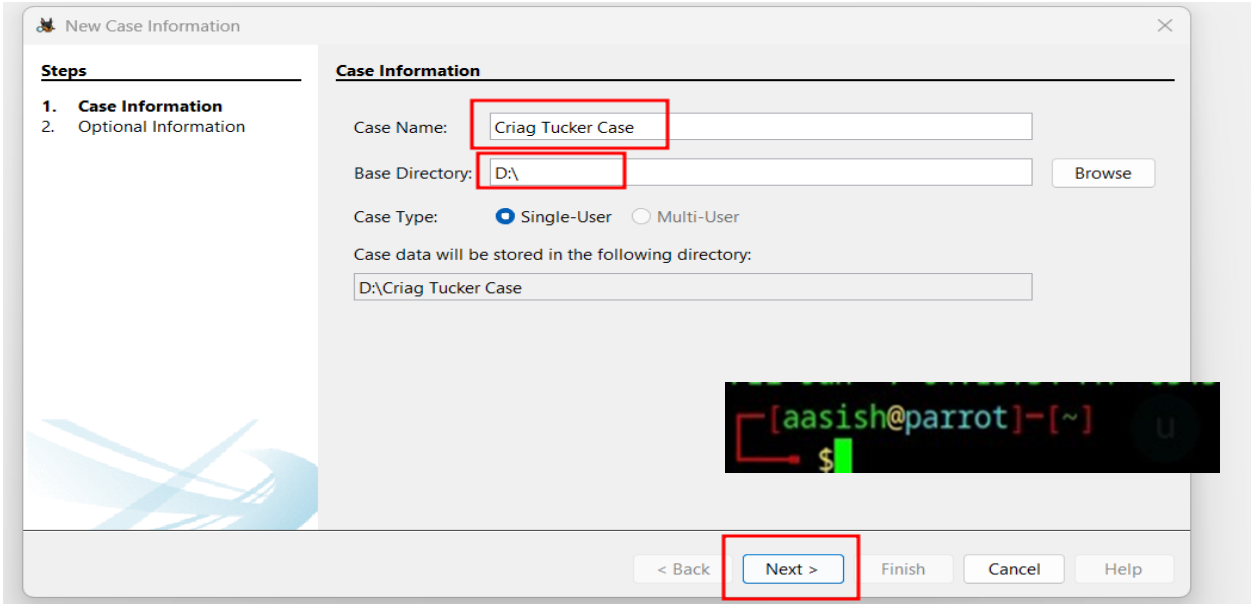
Walmart's Santa Monica store experienced a surge in fraudulent coupon redemptions for Monster Energy drinks and Arizona Ice Tea beverages. Surveillance footage identified a suspect, Craig Tucker, who was detained on **December 22, 2013** , after using counterfeit coupons during a transaction. Tucker claimed the coupons were obtained innocently through an online survey for Santa Monica Community College students.

Now this investigation begins in phases.

PHASE-1

Creating the case:

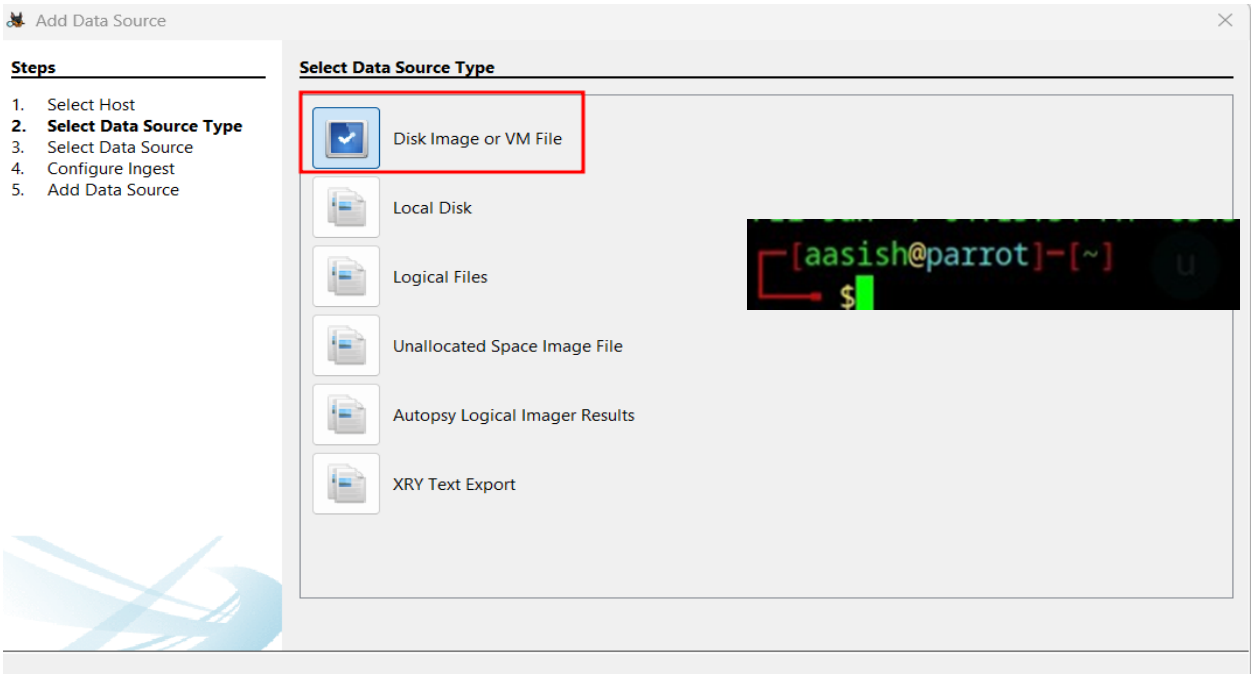




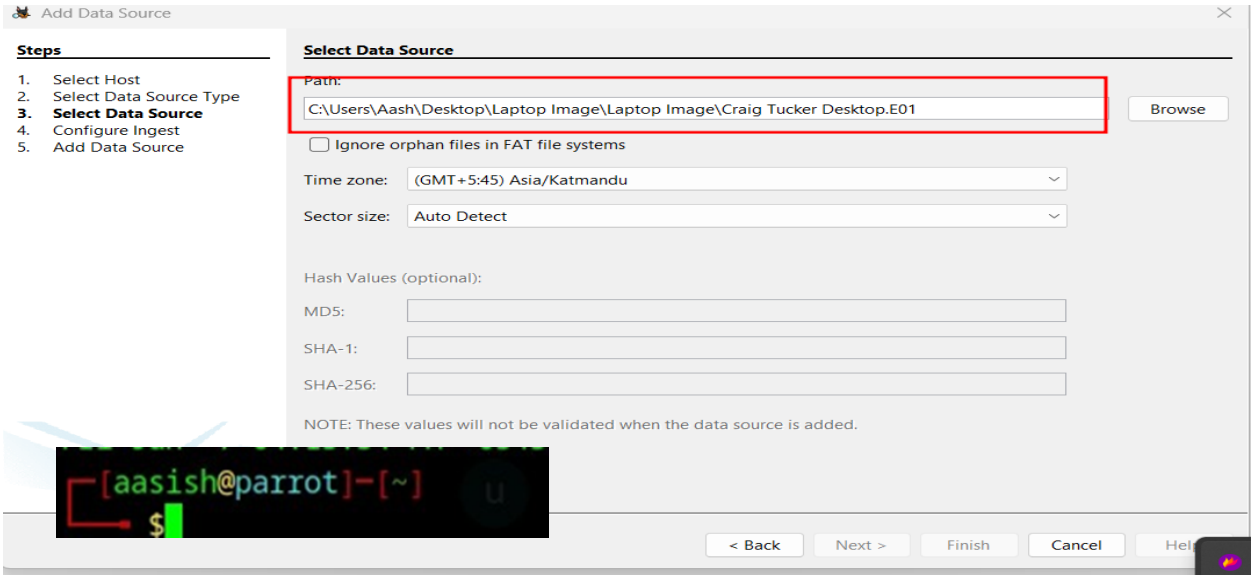
Case name: Criag Tucker Case

Base Directory: D:\

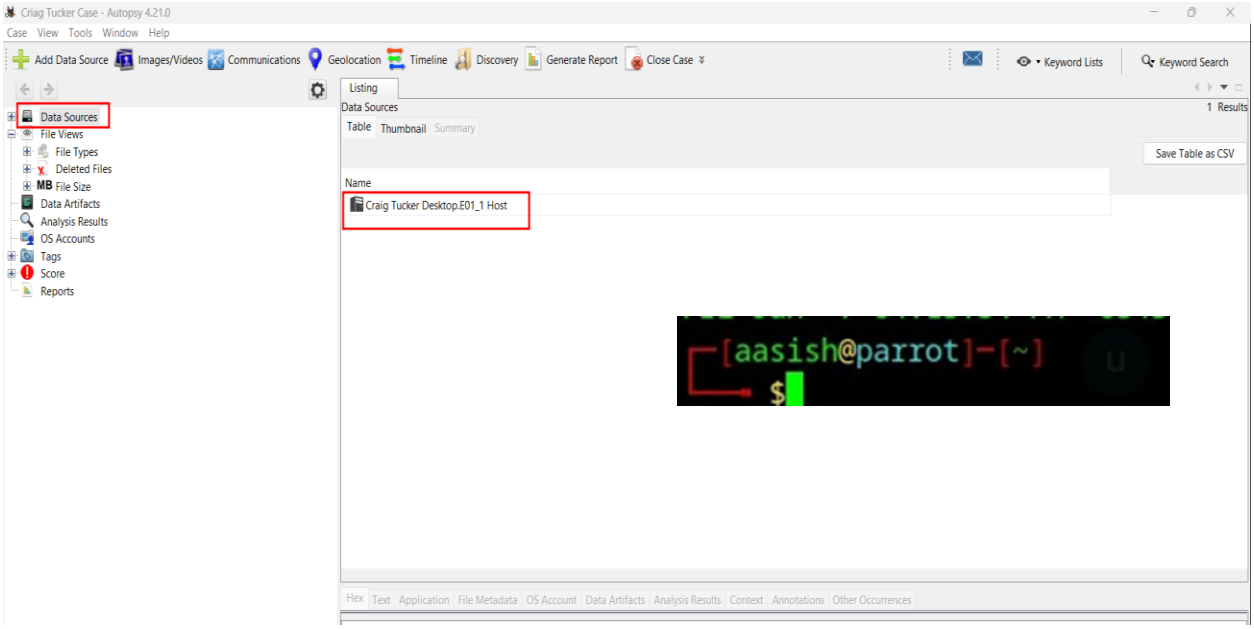
Selecting Disk Image because it’s E01 file that is given to us



Specifying the disk path “Criag Tucker Desktop.E01”

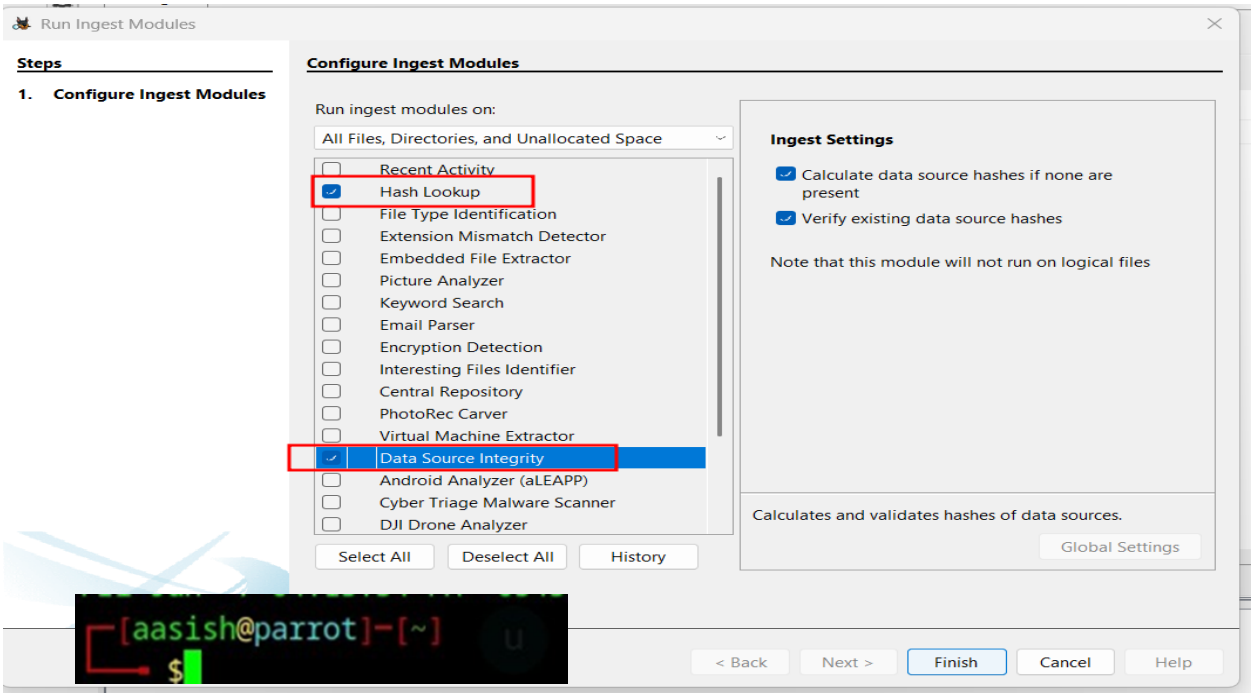


Finally after completing the ingest module here comes the extracted file from the E01 file

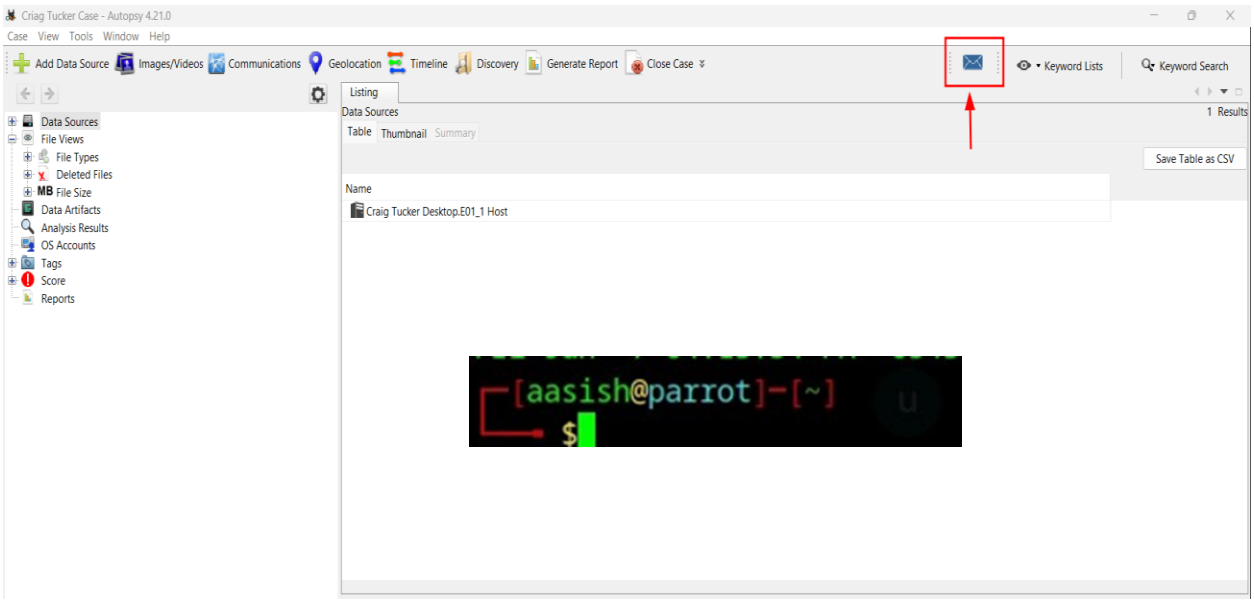


Verifying the Forensic Image

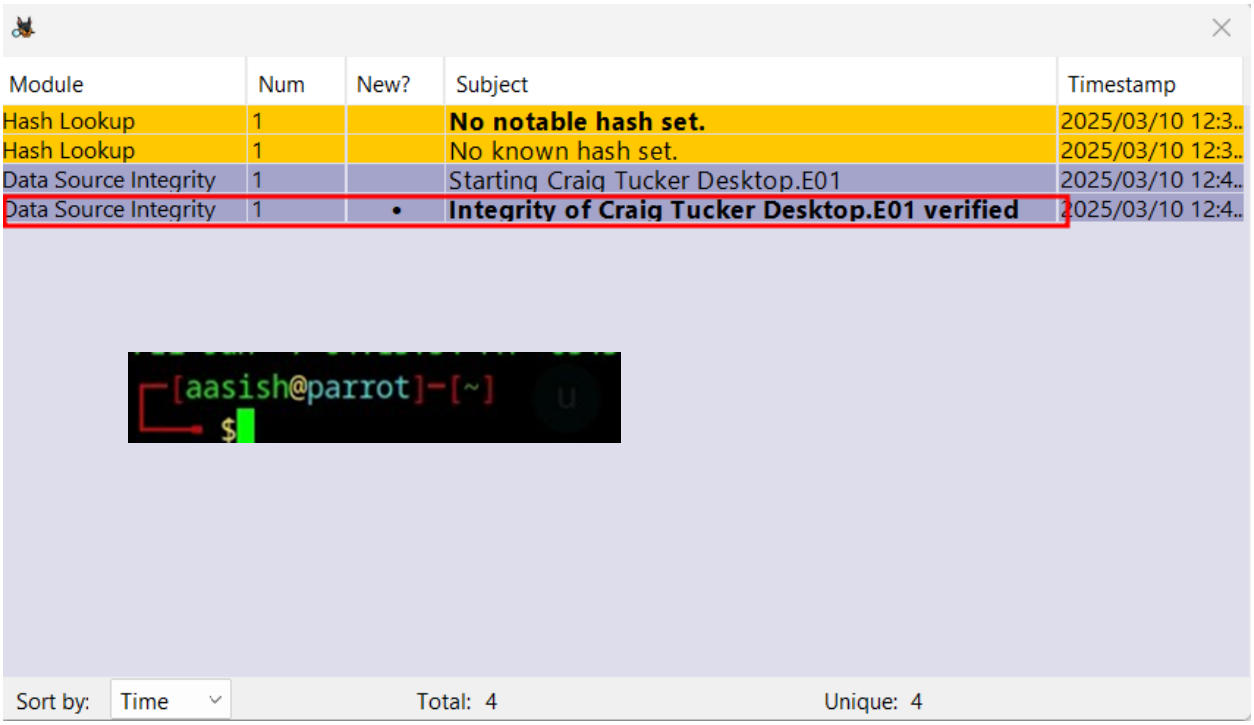
Next step is to verify the integrity of the file that the given file is integrity safe or not



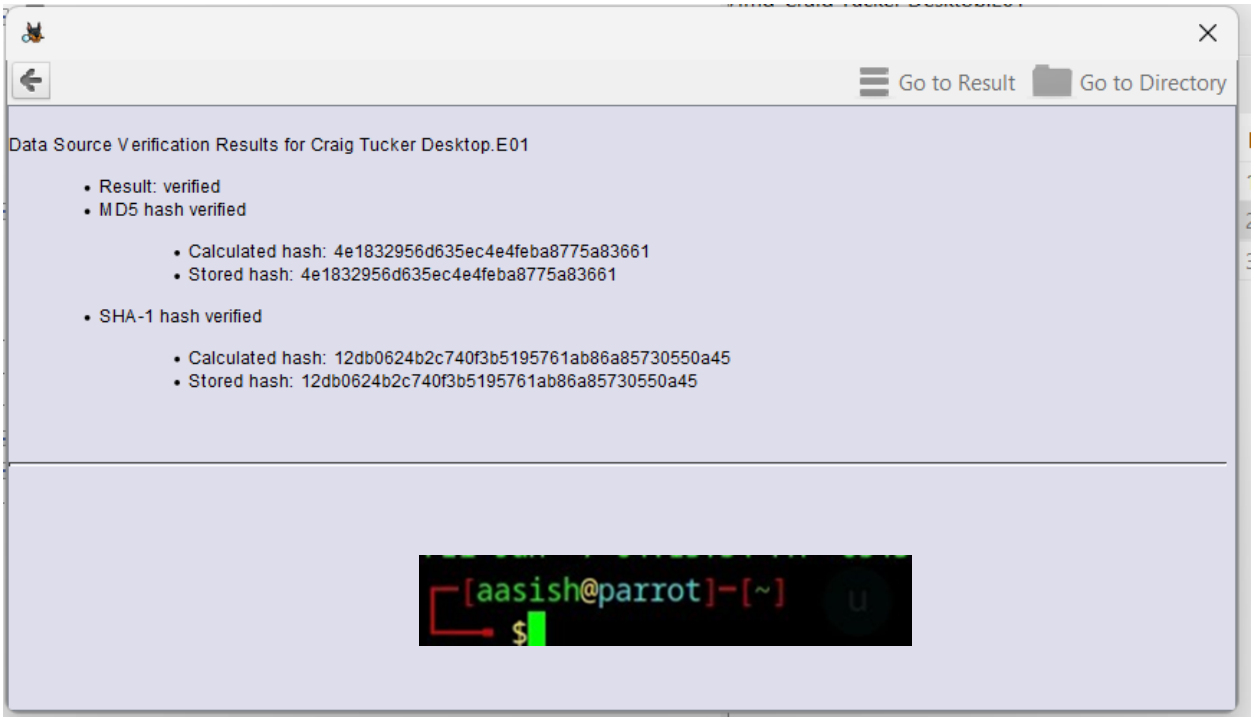
Running the ingest module and after the message box gives the reuslt



Here it is, says verified

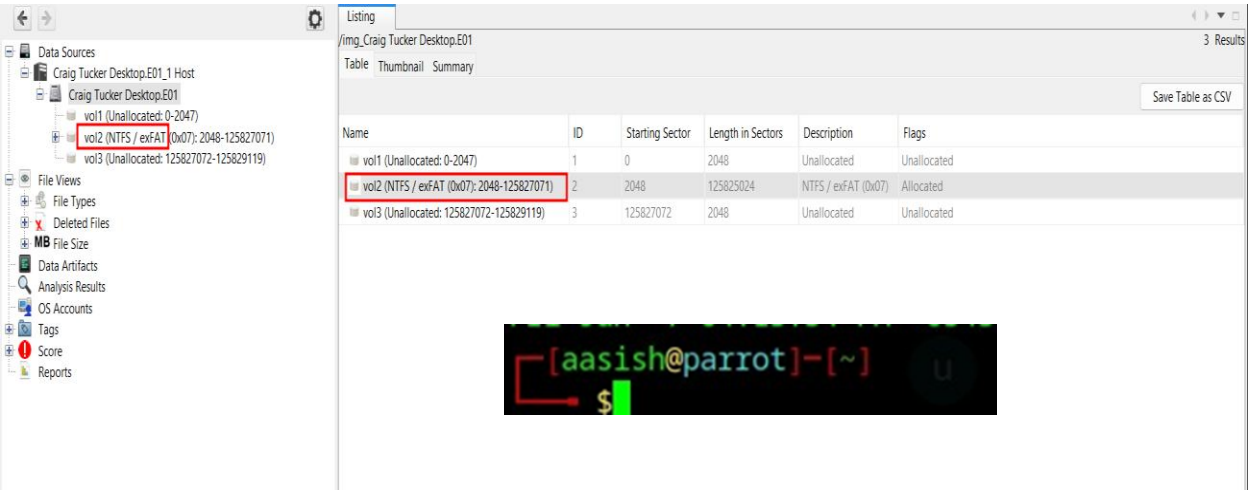


Let’s check and now it’s verified!



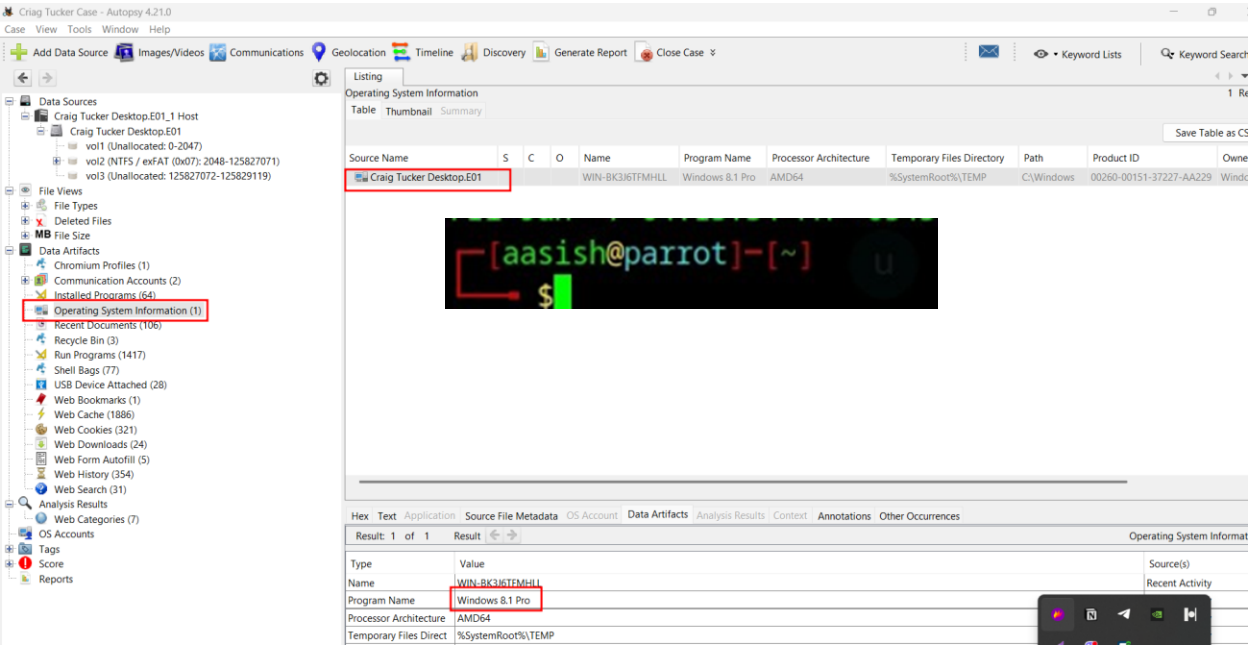
Drive Geometry

Next up, Drive Geometry, after pulling down the drop down list it says NTFS/exFAT geometry



Operating System

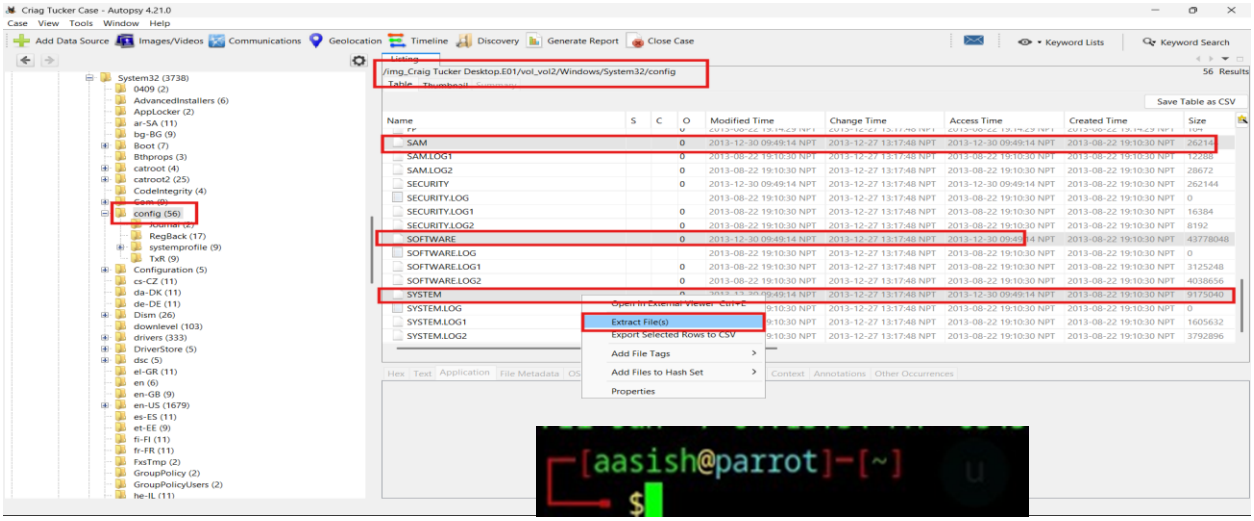
The extracted section contains operatin system information using it's artifacts it gives us the operating system information: windows 8.1 pro



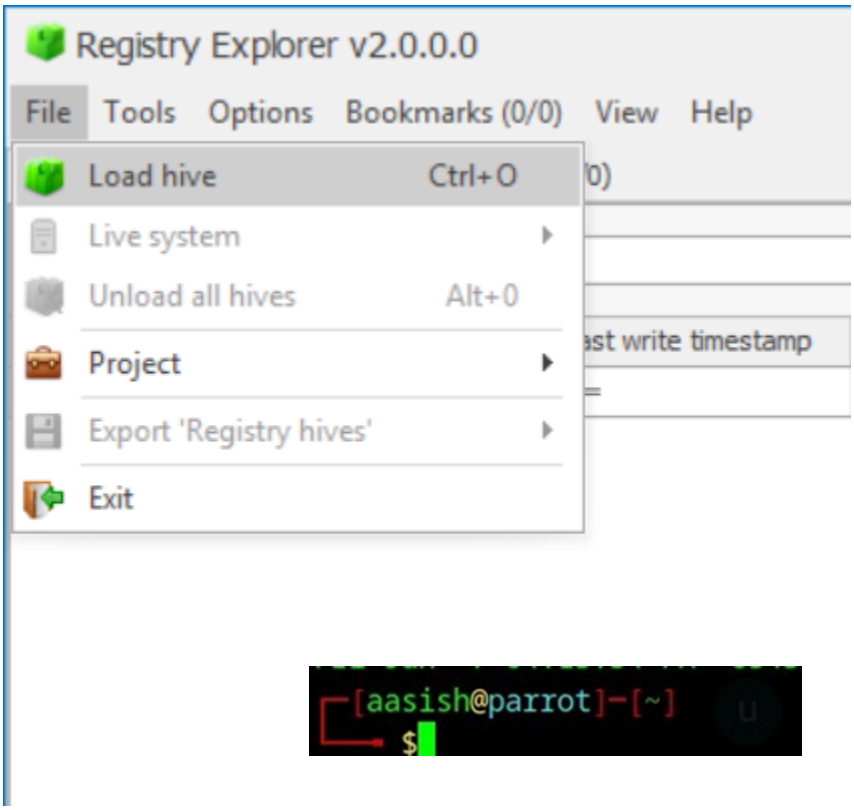
Establishing the Time Zone

Now the time zone specifiying the location

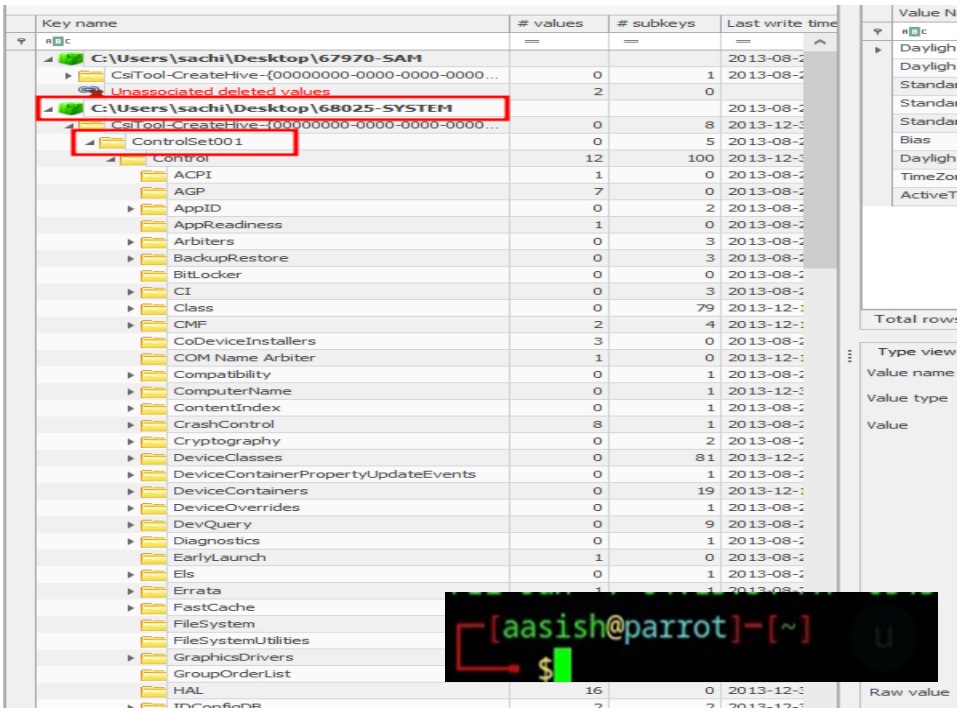
Exporting the hive files “SAM” “SOFTWARE” “SYSTEM”

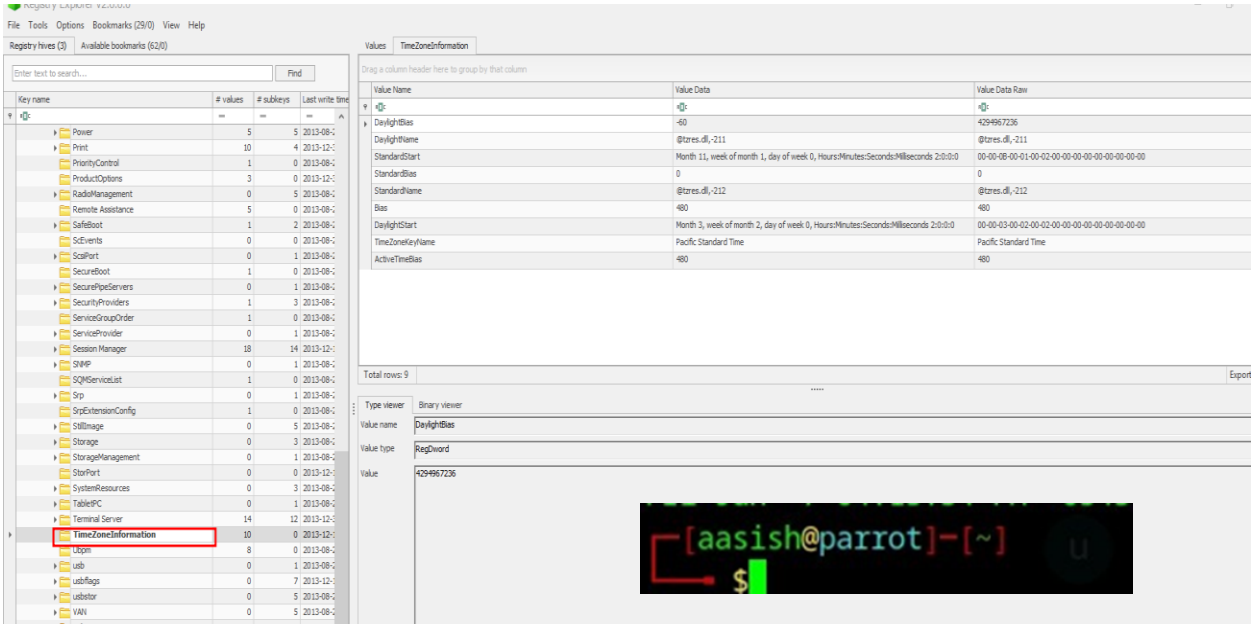


Now loading the file into the registry explorer



Here we go! Now as we need time zone information we travel through SYSTEM hive and further to controlset001 followed by TimeZoneInformation



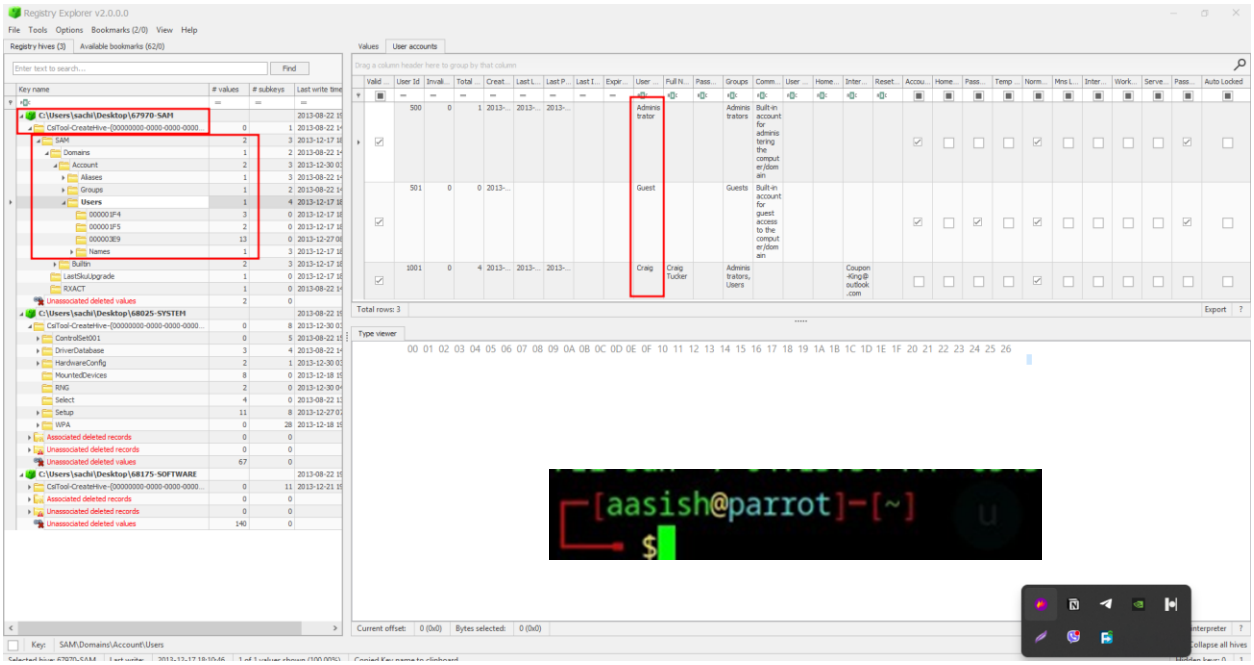


Value Name	Value Data	Value Data Raw
DaylightBias	-60	4294967236
DaylightName	@tzres.dll,-211	@tzres.dll,-211
StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-0B-00-01-00-02-00-00-00-00-00-00-00-00-00
StandardBias	0	0
StandardName	@tzres.dll,-212	@tzres.dll,-212
Bias	480	480
DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-03-00-02-00-02-00-00-00-00-00-00-00-00-00
TimeZoneKeyName	Pacific Standard Time	Pacific Standard Time
ActiveTimeBias	480	480

Here we get Pacific Standard Time

Identify Computer User

Now identifying the users



Here we get three users,

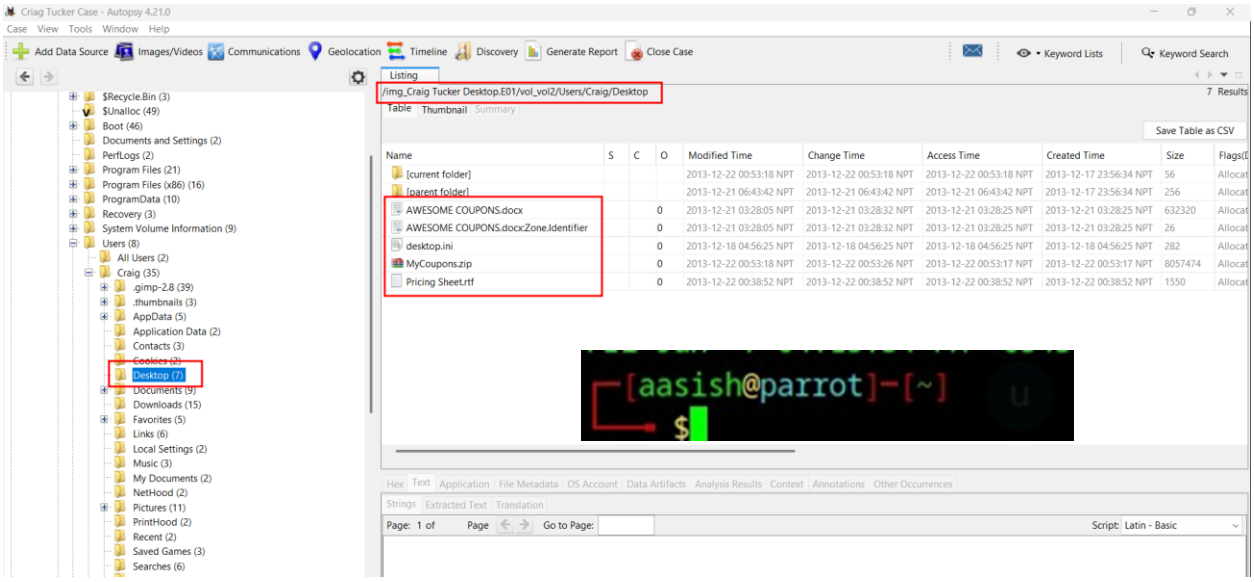
Administrator, Guest and Criag

Phase - 2

User's Personal Data

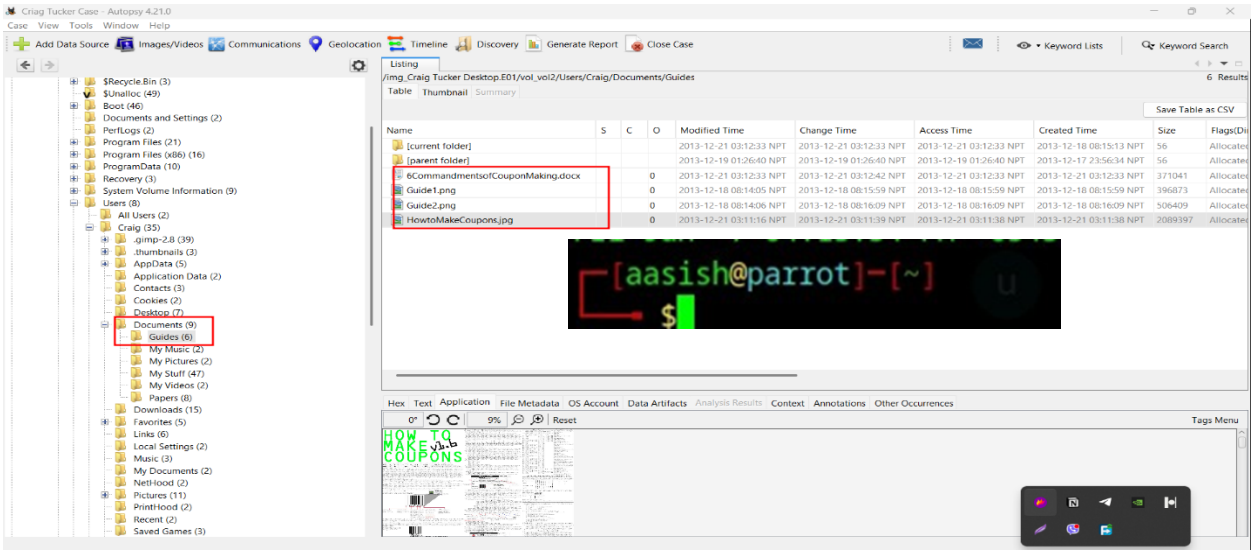
Now we explore more we find the personal information of users:

Desktop section



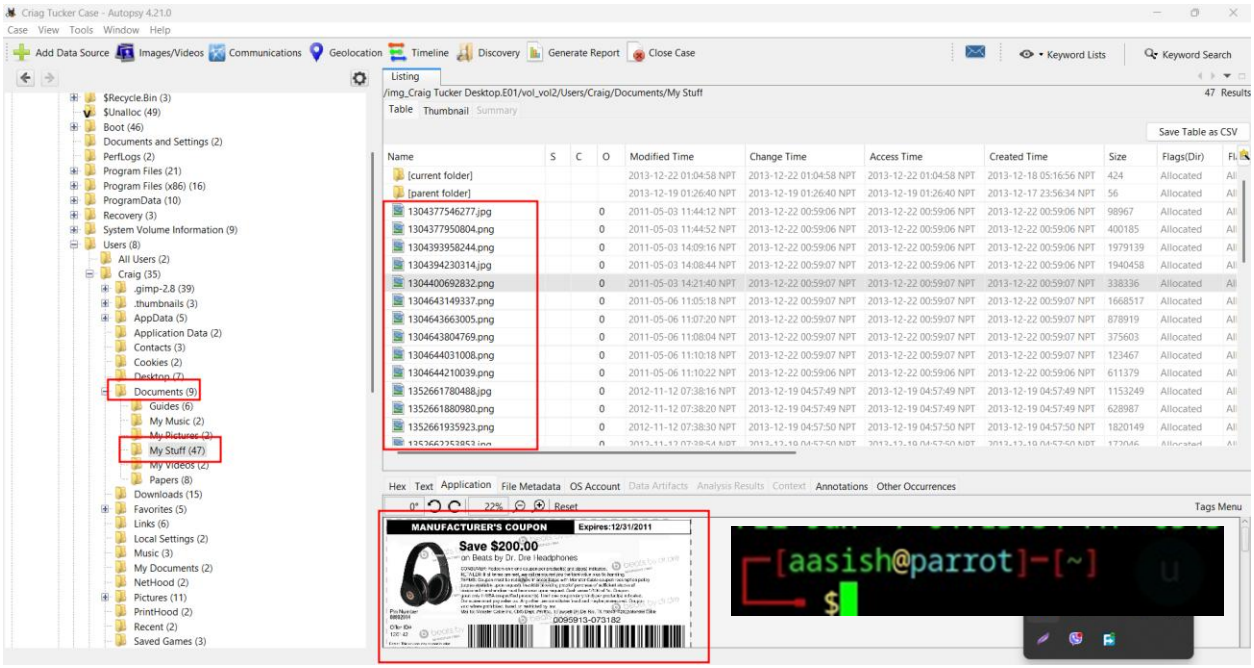
Here we found some files name coupons

Documents>Guides section



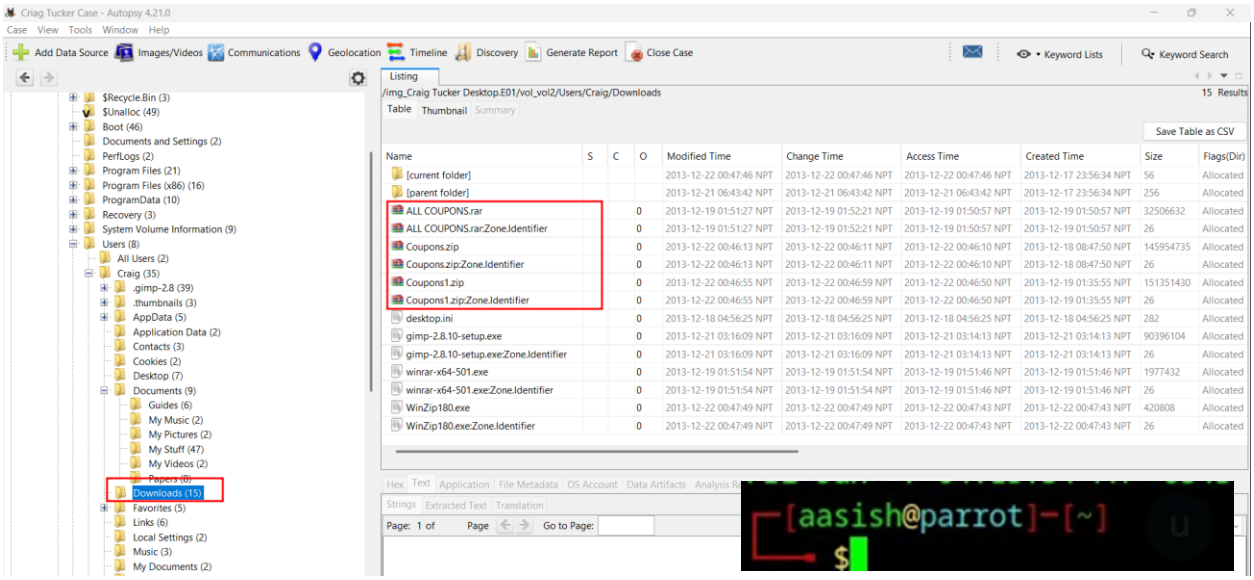
We found some tutorial that explains how to make coupons

Documents> My Stuff section



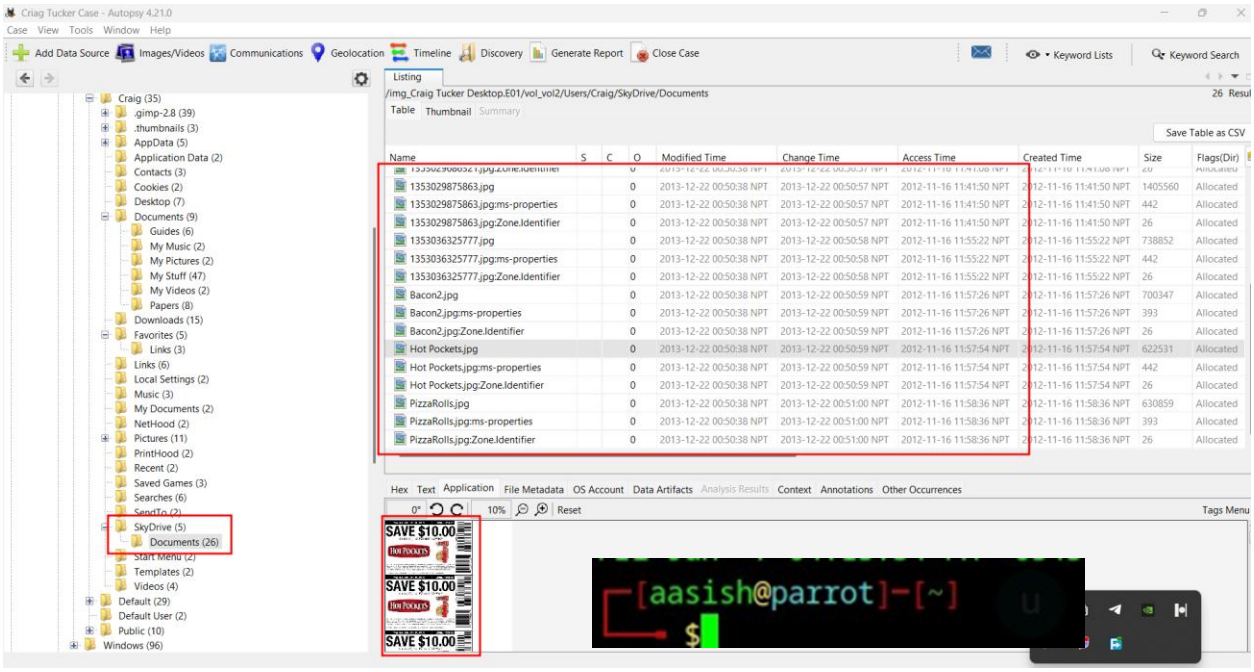
Here we found tons of coupons

Next Downloads section:



Here we found zip files all about coupons

Next SkyDrive>Documents section

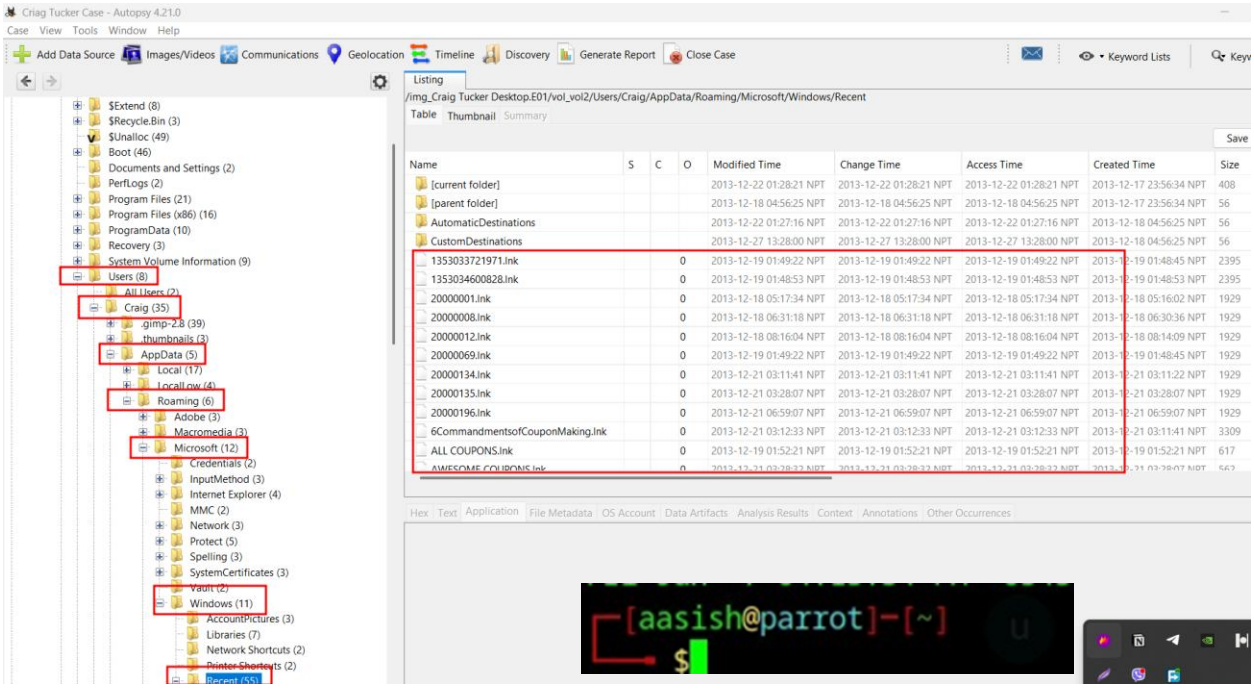


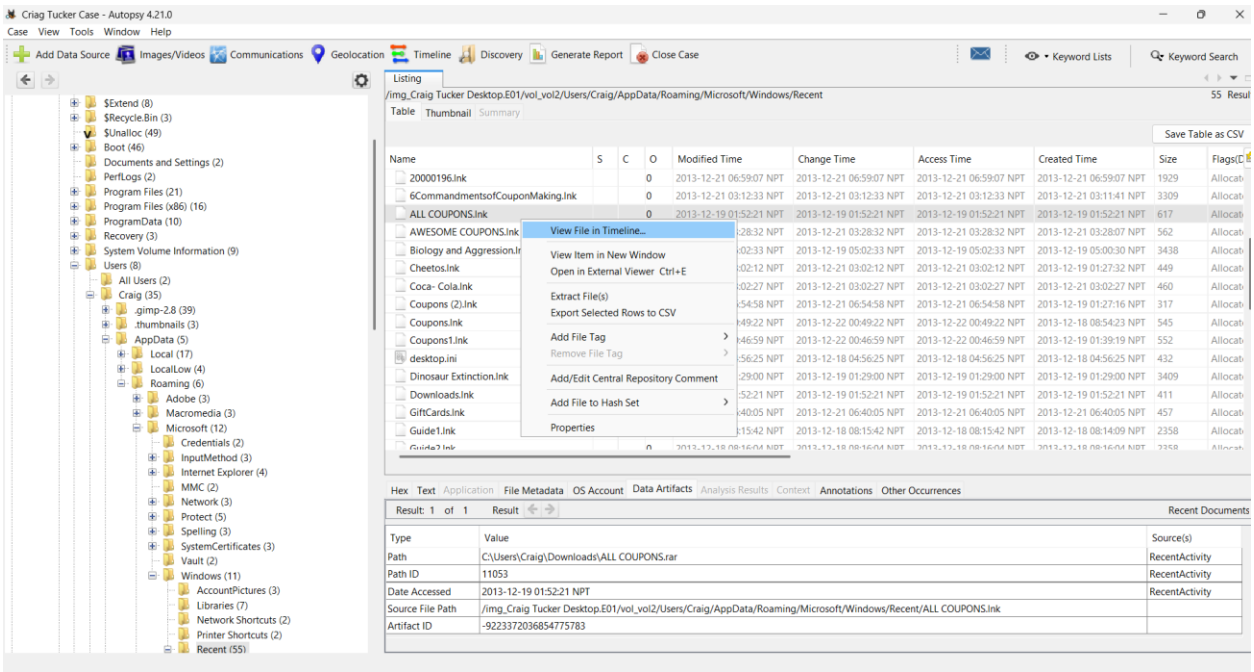
Again we found a lots of coupons all under User “Criag”

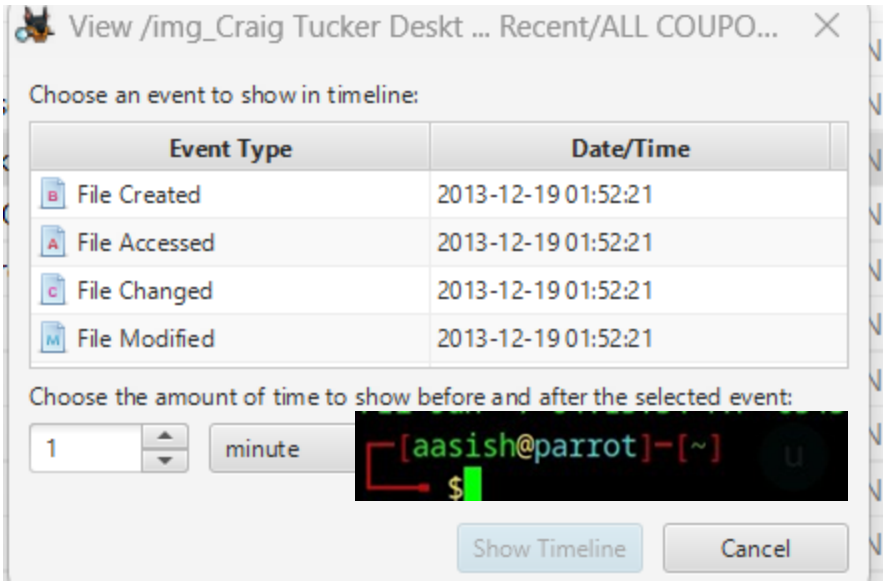
LNK Files and JumpLists

Link Files:

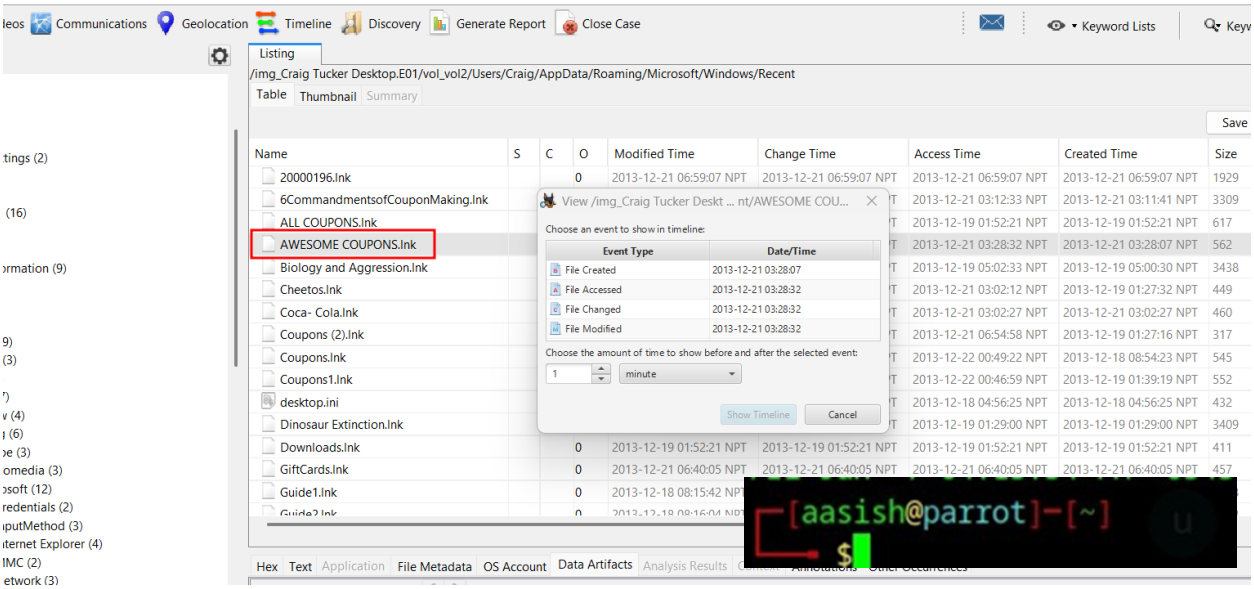
Next Link Files “LNK” that directs about the timestamp and the original file destination



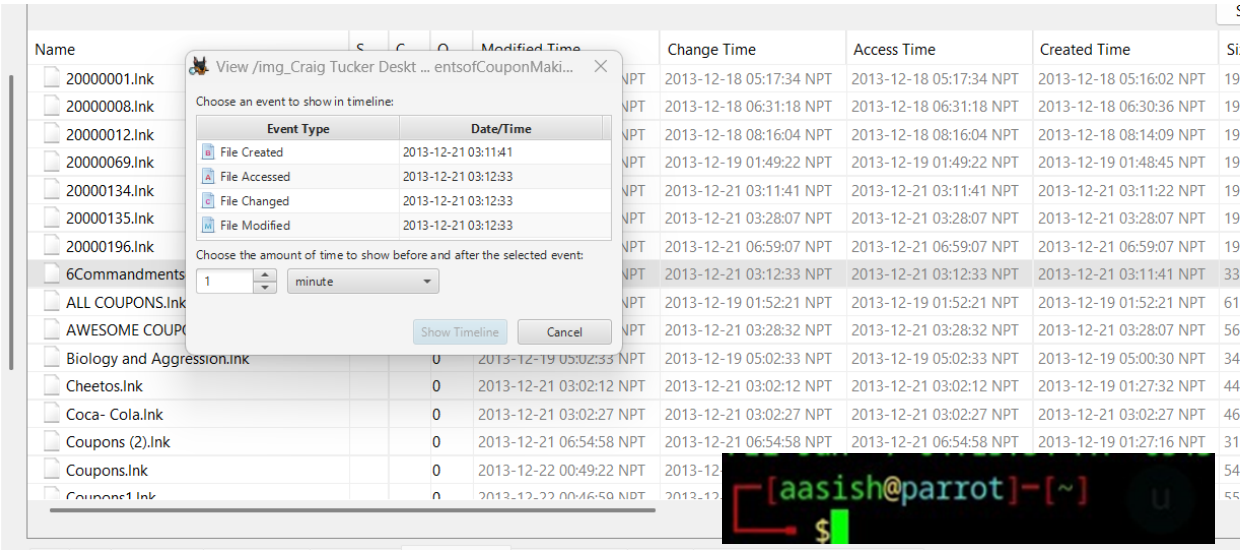




So All coupons.jar is accessed by user criag at this timestamp

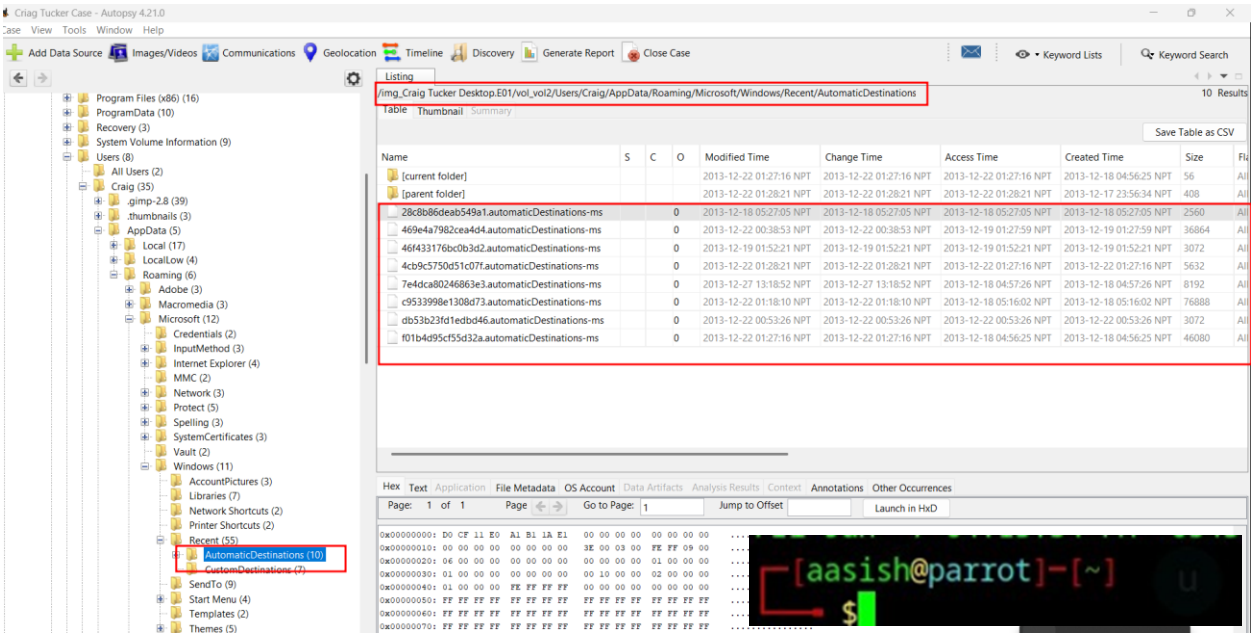


Criag Accessing the Awsome coupons.lnk files timestamp

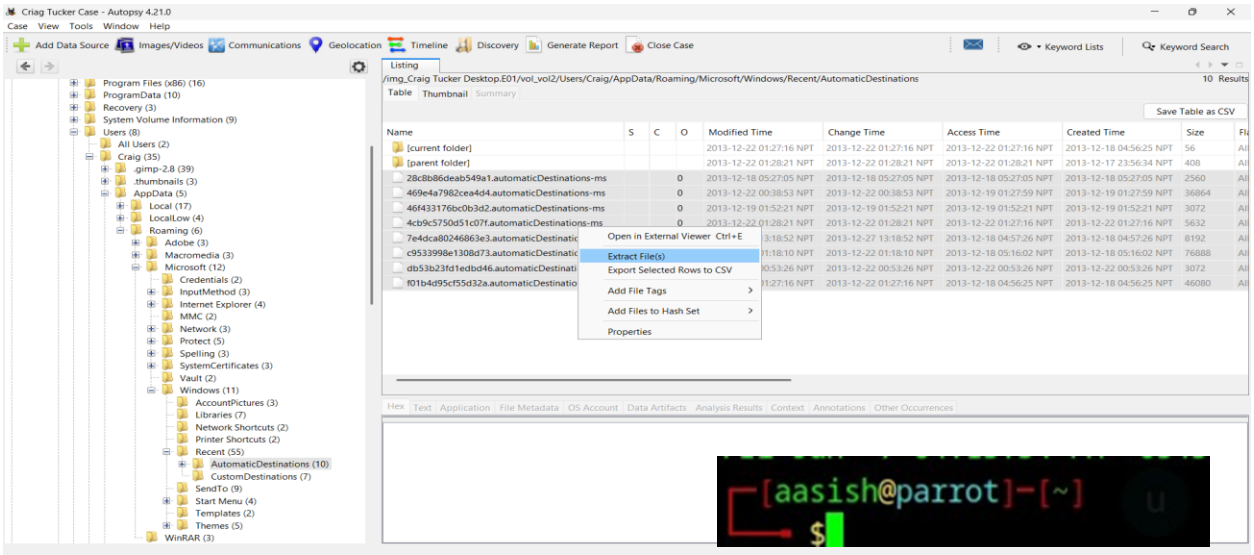


Jumplists

Now jumplists

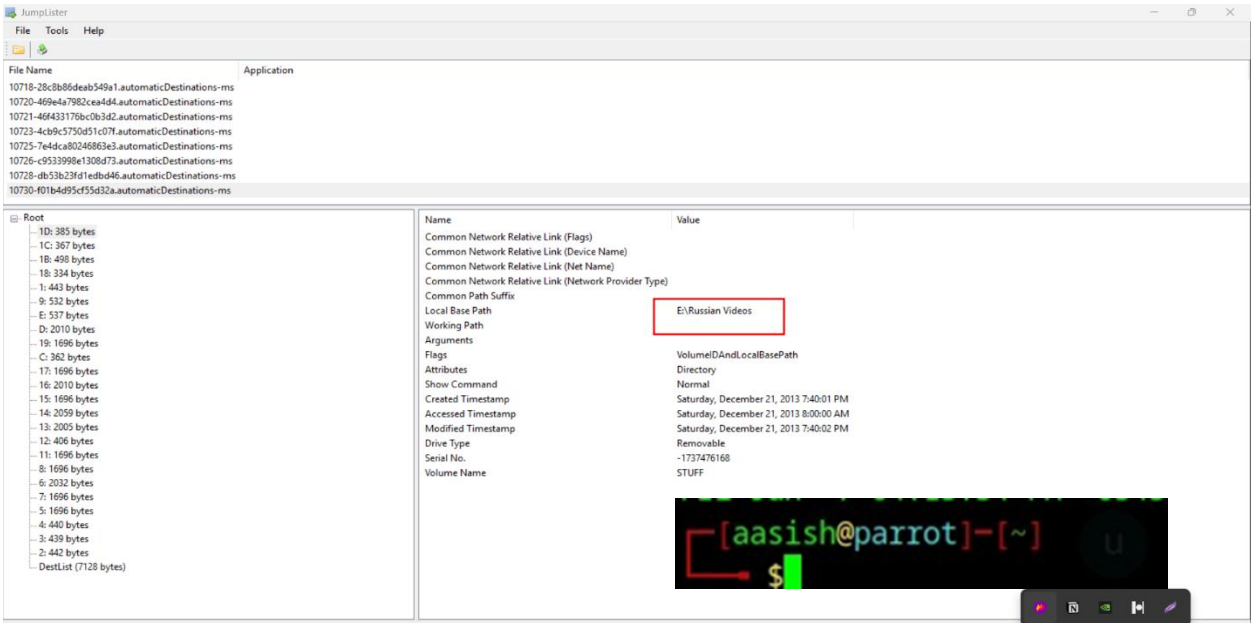


Extracting the jumplist files

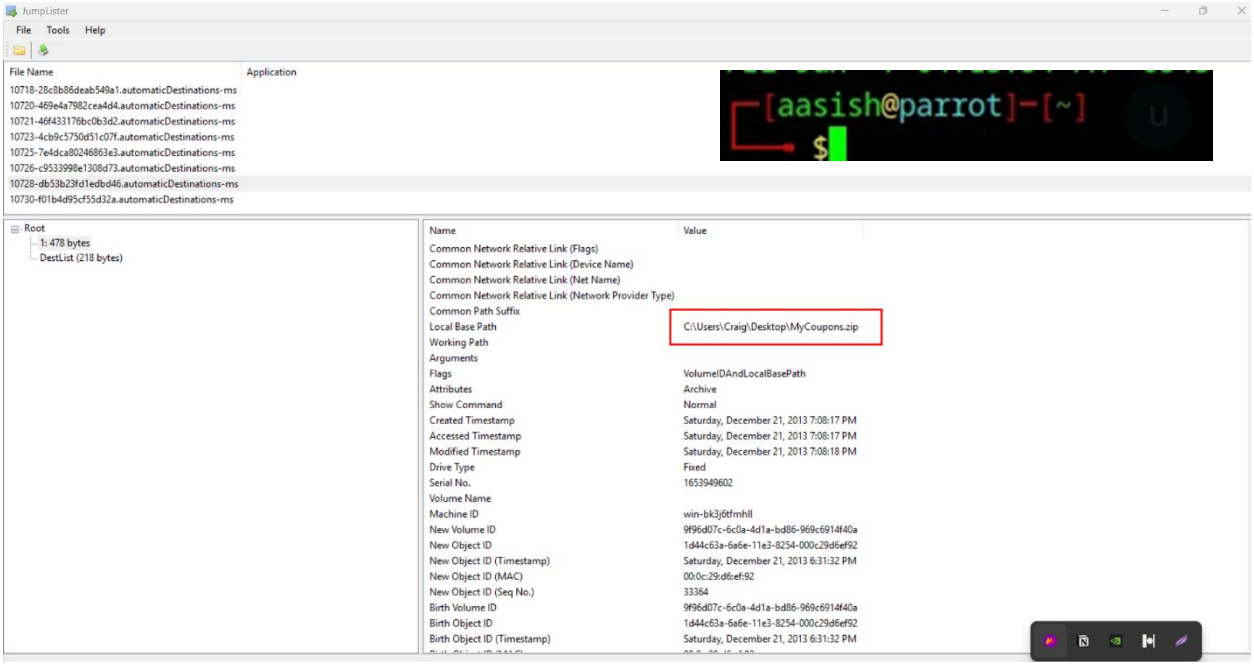


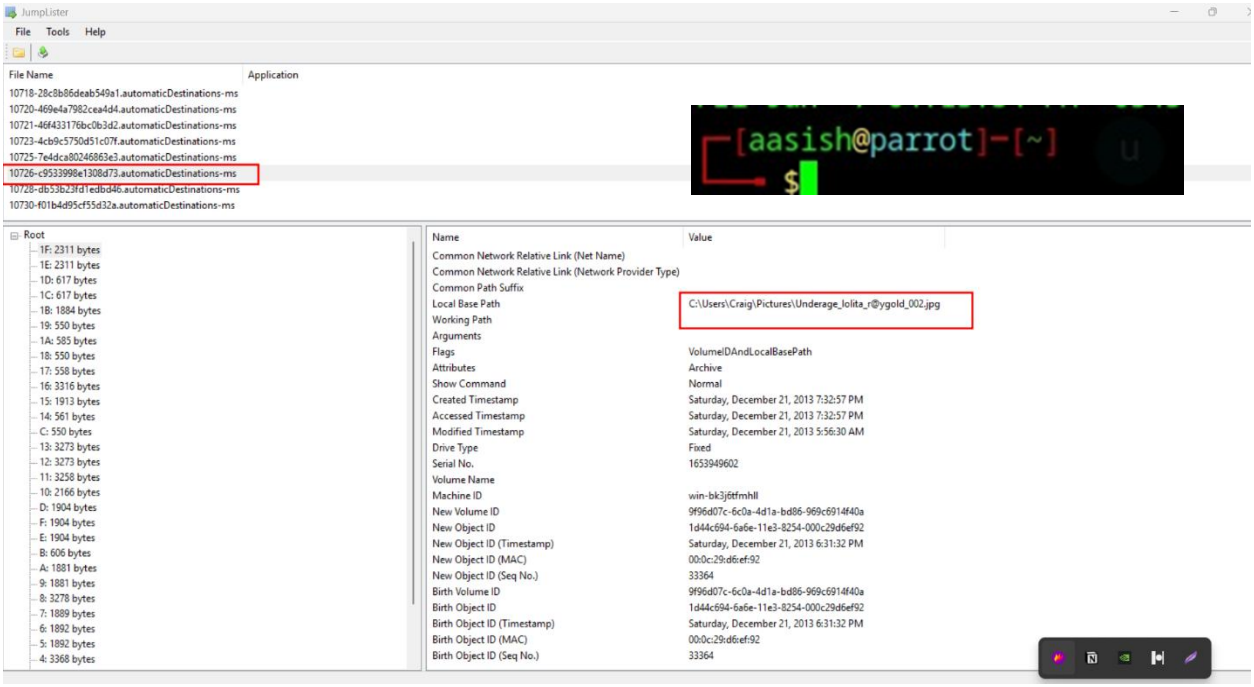
Opening into Jumplister

Here one of the file directs E:\Russian Videos

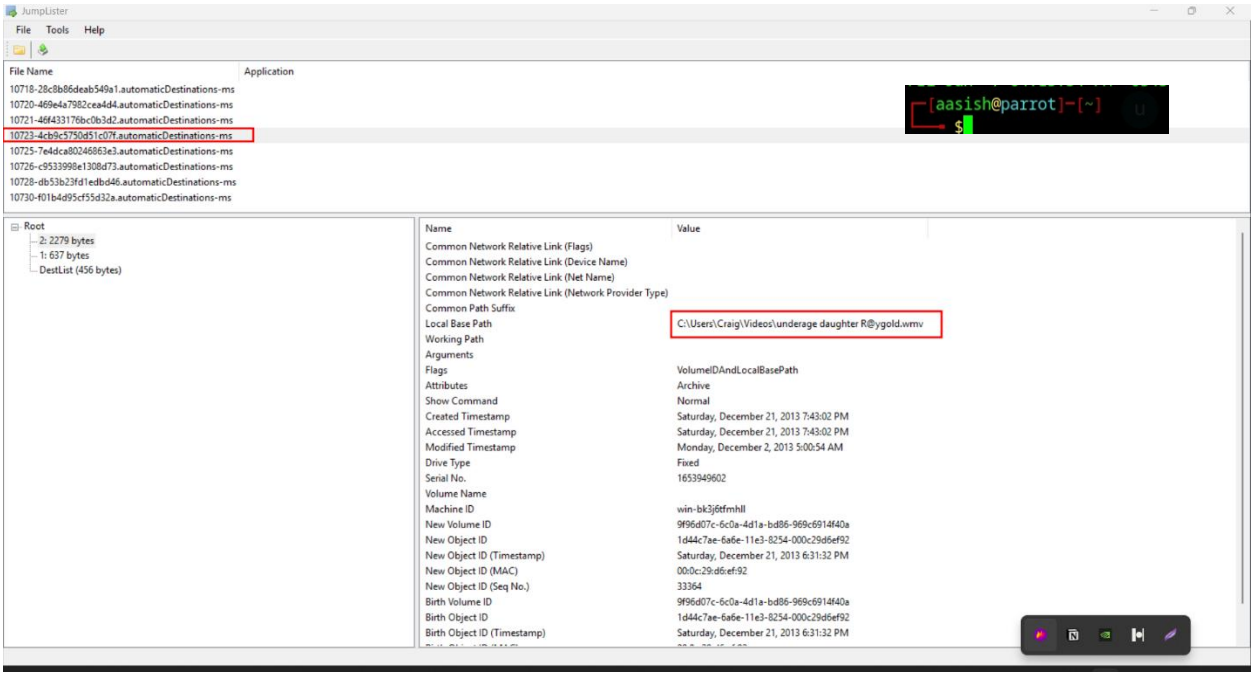


Another one directing into MyCoupns.zip file and all the metadata about the file

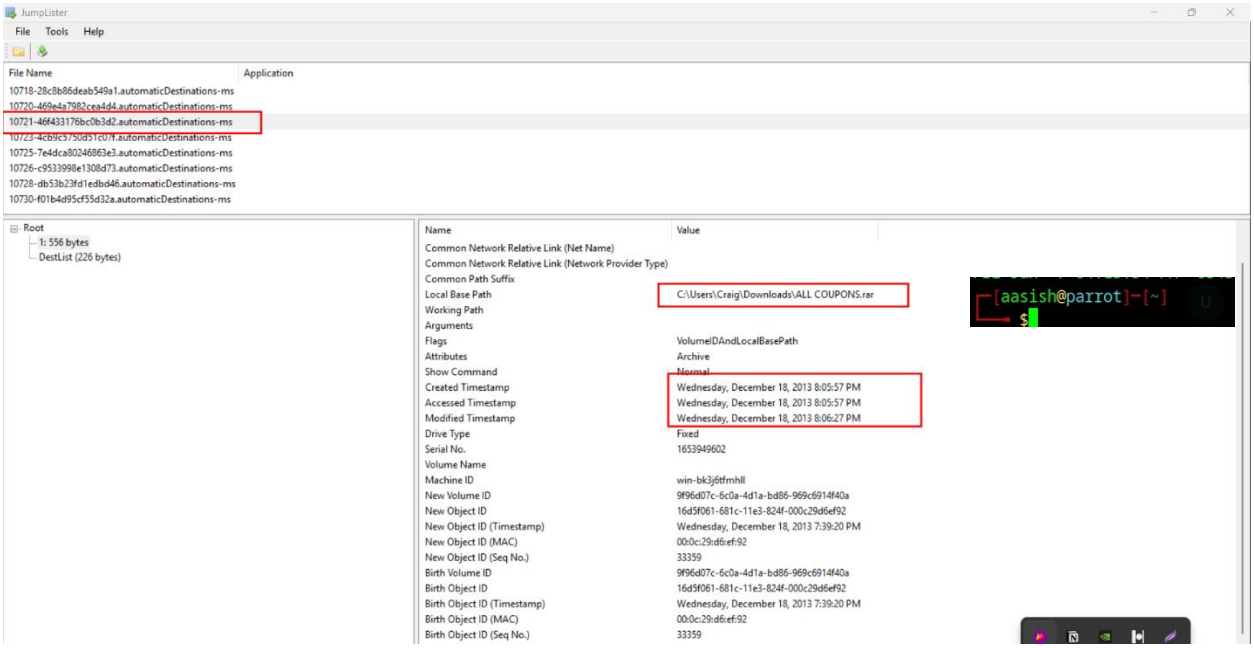




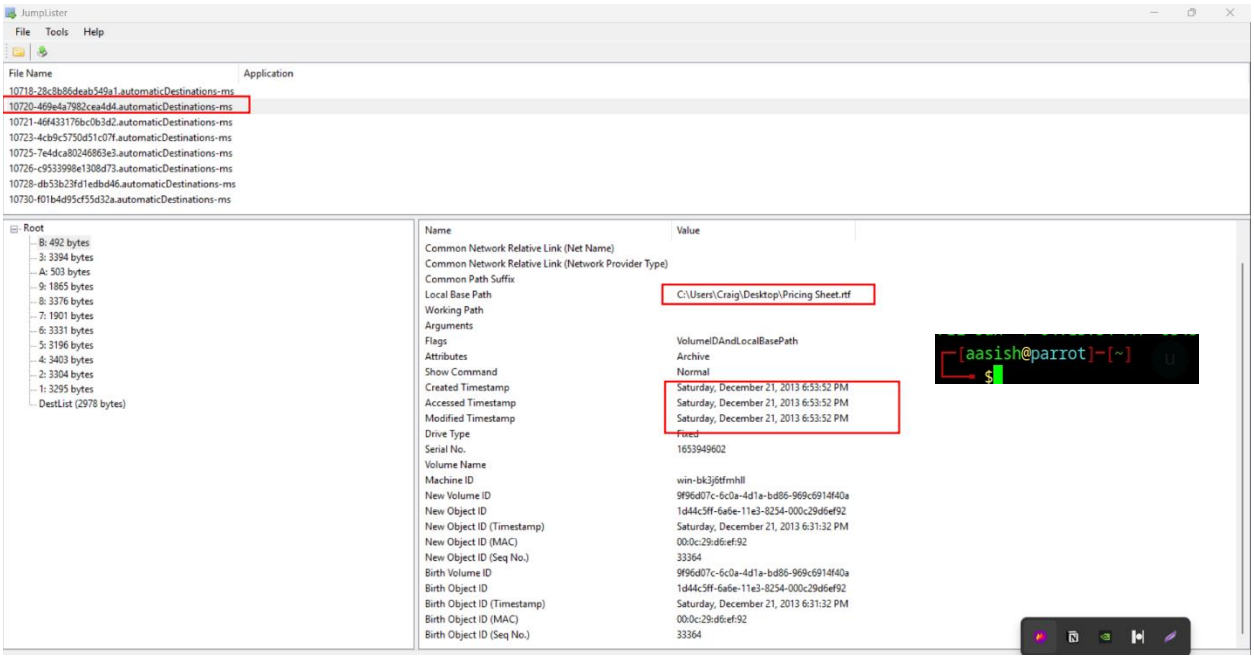
Underage daughter R@ygold.wmv (might be child pornography video)



Next metadata about the ALL COUPNS.rar file

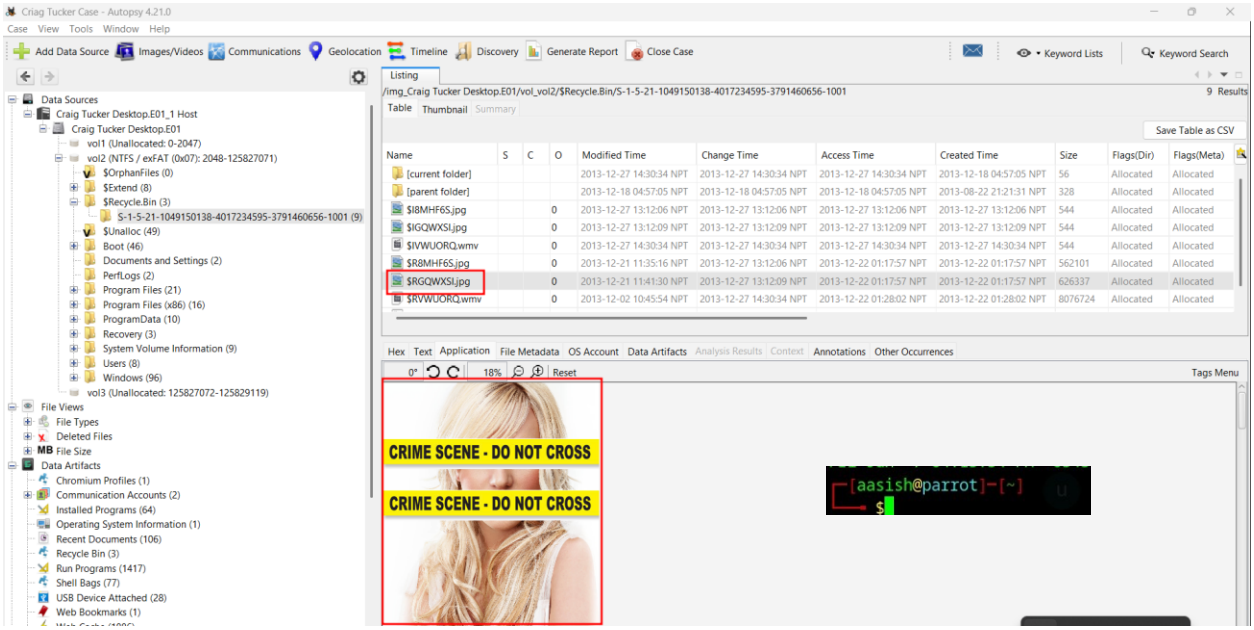


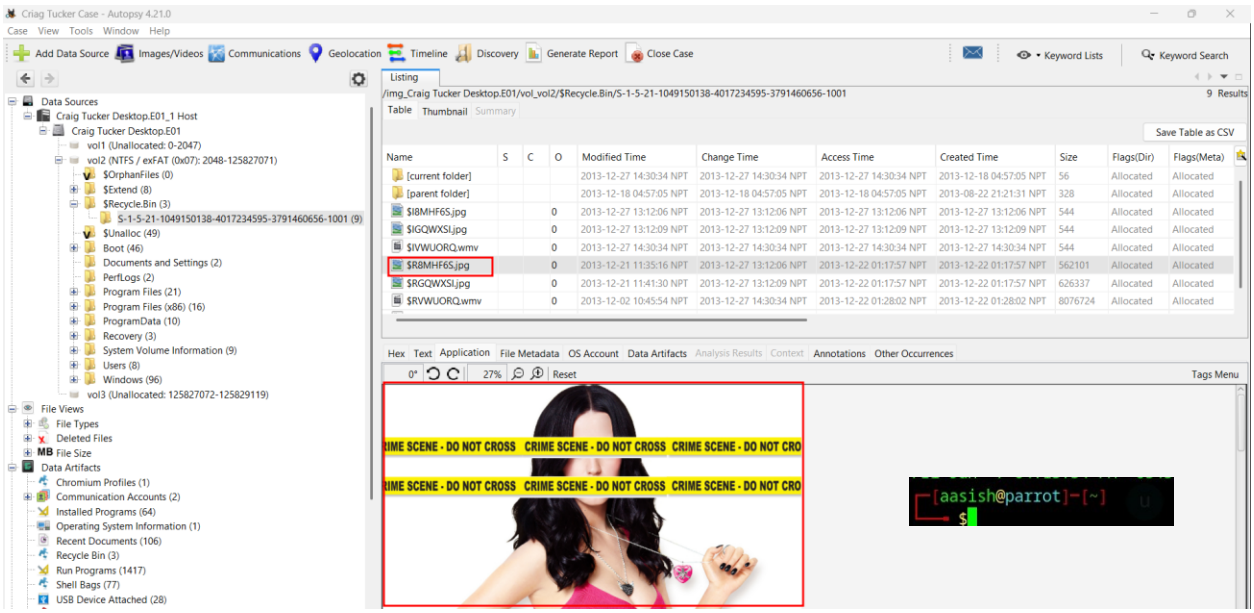
Next Pricing sheet of the coupons



Recycle Bin

Next Recycle bin



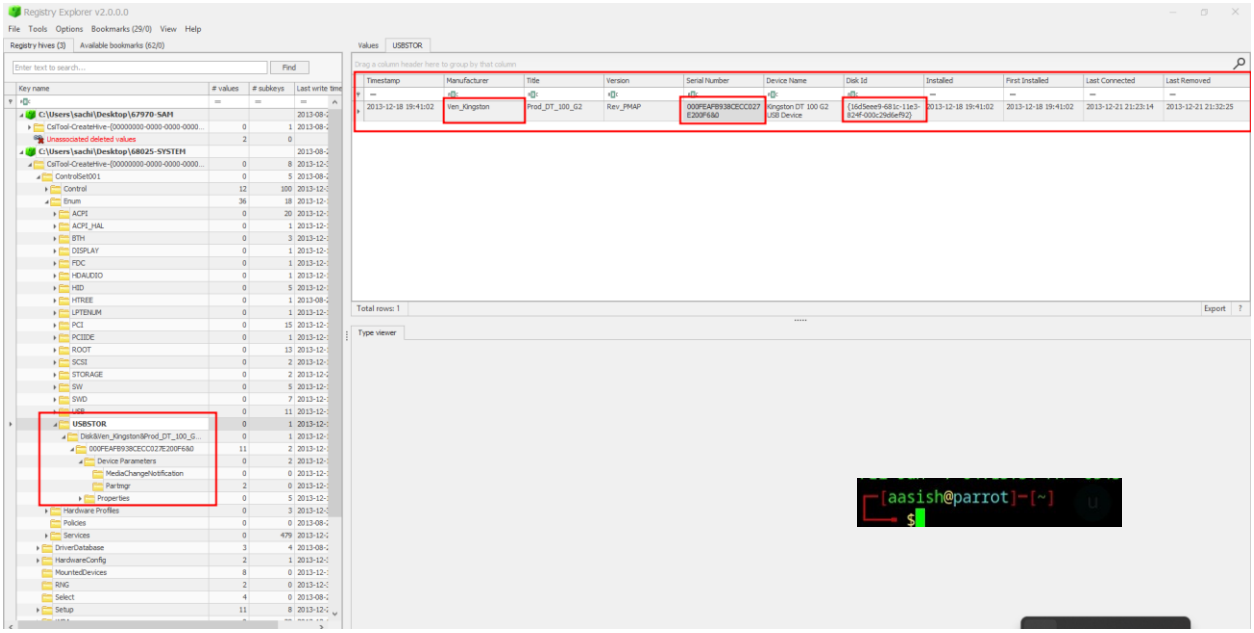


We got some photos that says crime scene- Do not cross and some jpg deleted files

Attached USB OEM/serial number

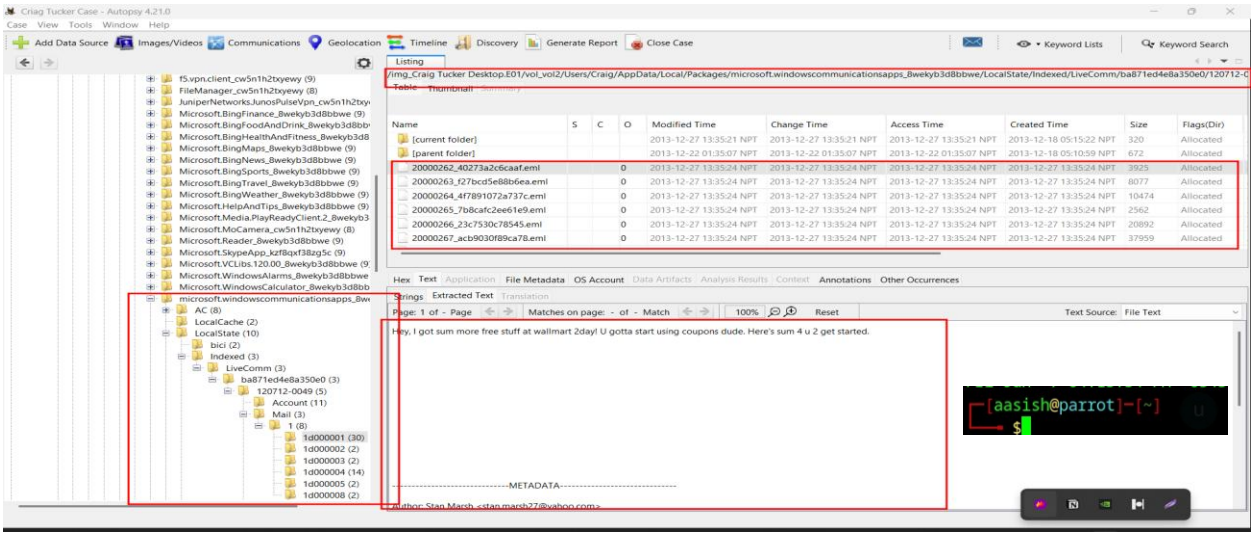
Next up looking for attached USB OEM/serial number

We found it under SYSTEM hive

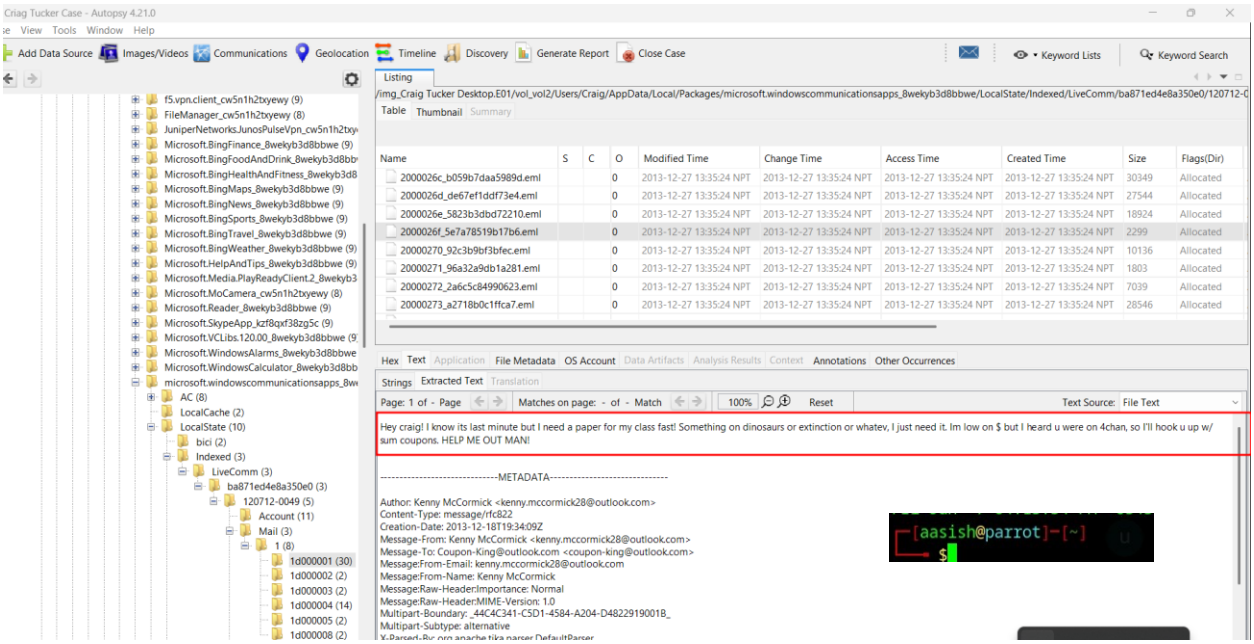


Email-Review

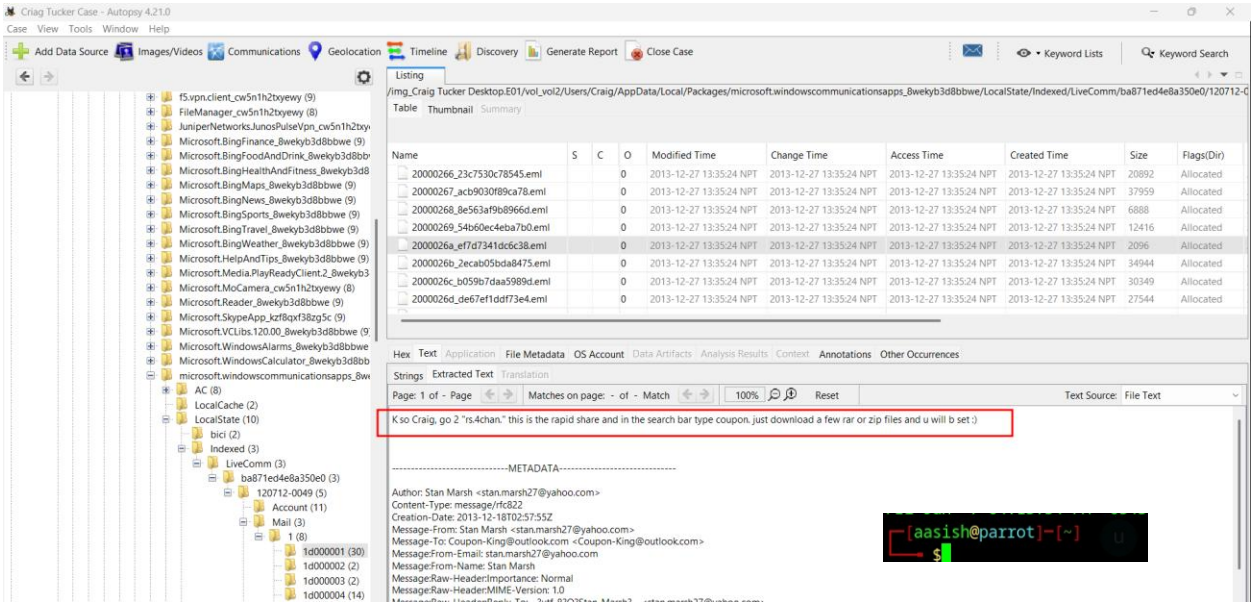
Next up looking for emails

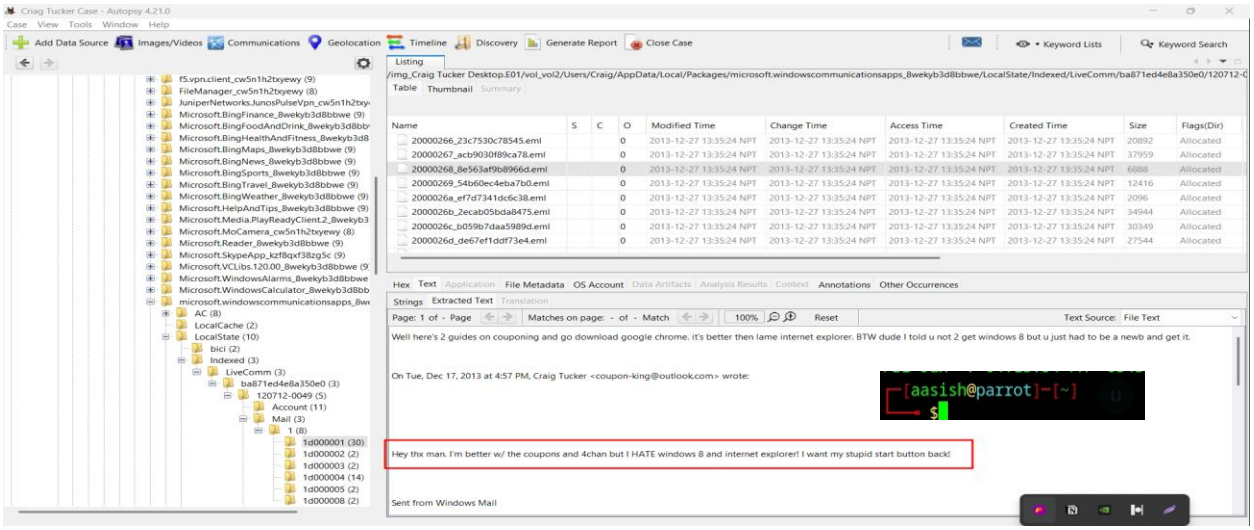


This indicates the usage of coupons

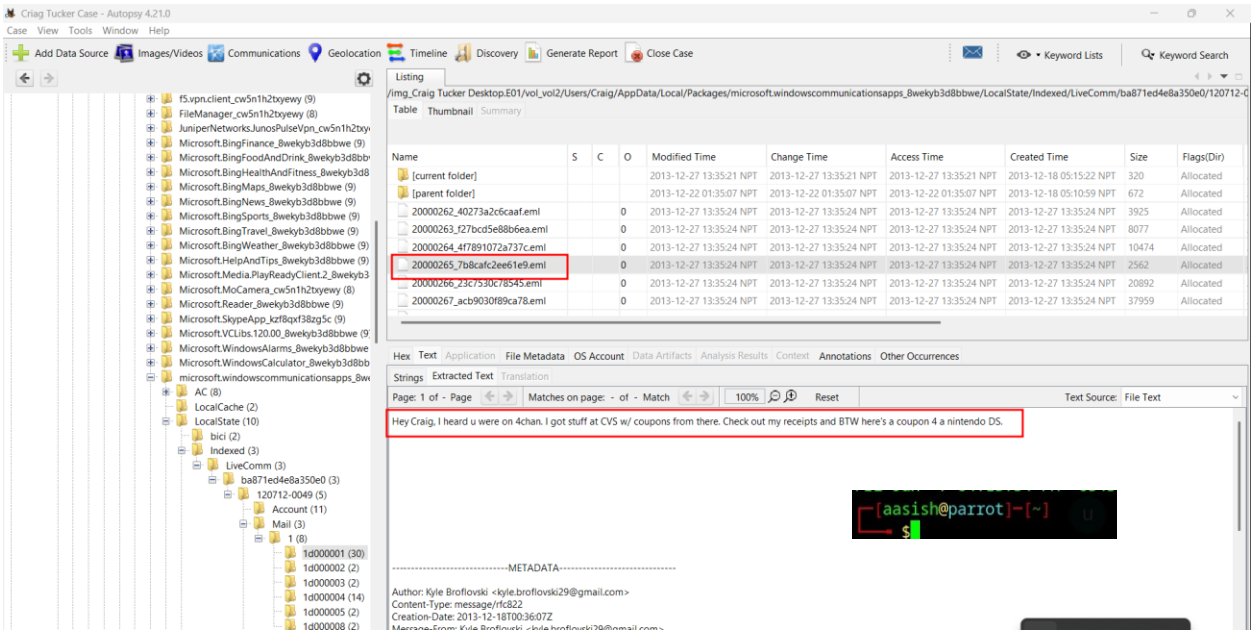


This indicates Kenny McCormic is asking for some coupons





Next Criag Mailed about he is good at coupns

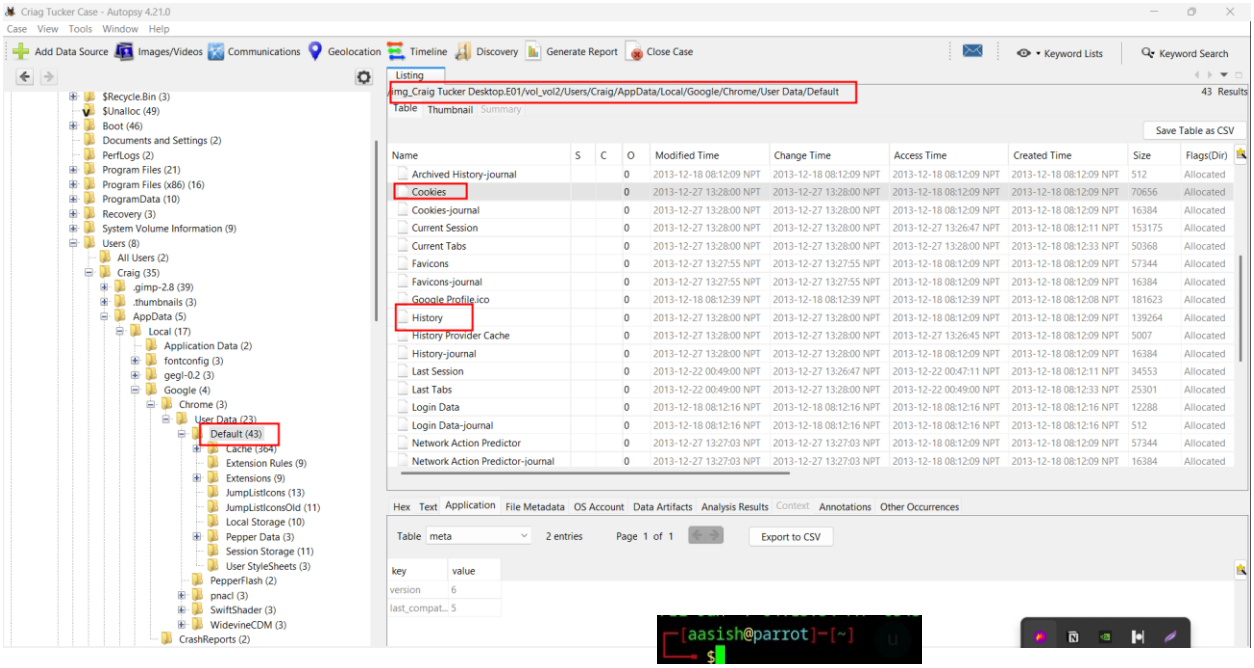


Next Kyle Broflovvski mailed about coupons dealing

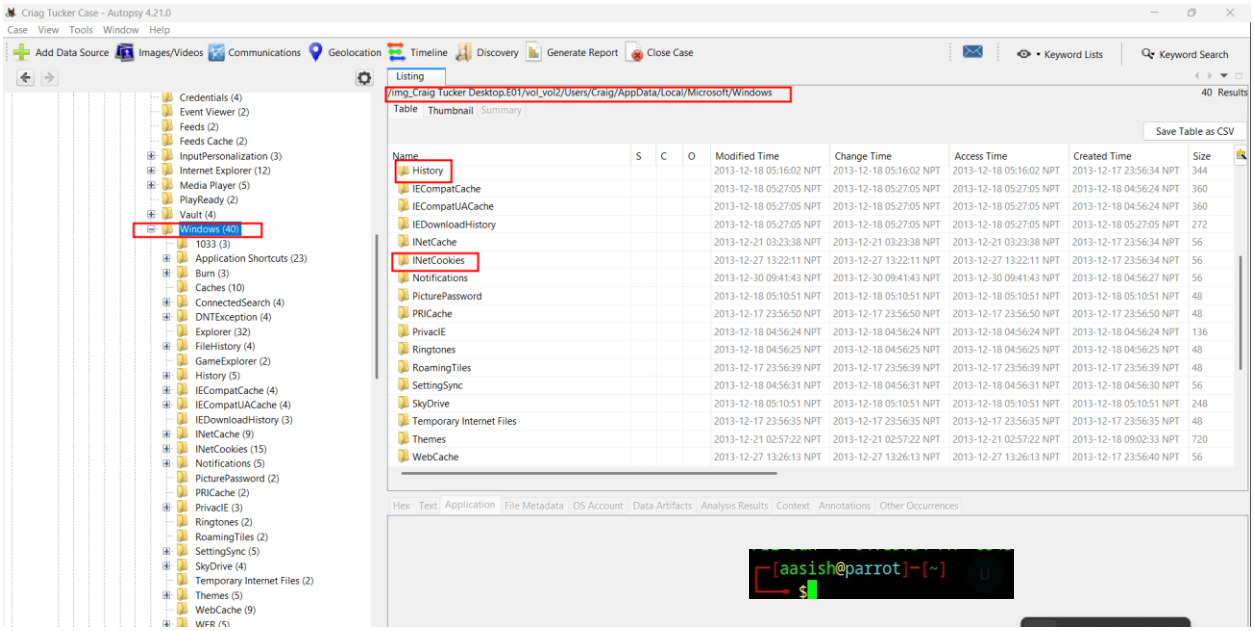
Internet History

Let’s explore internet history

First lets open google hive

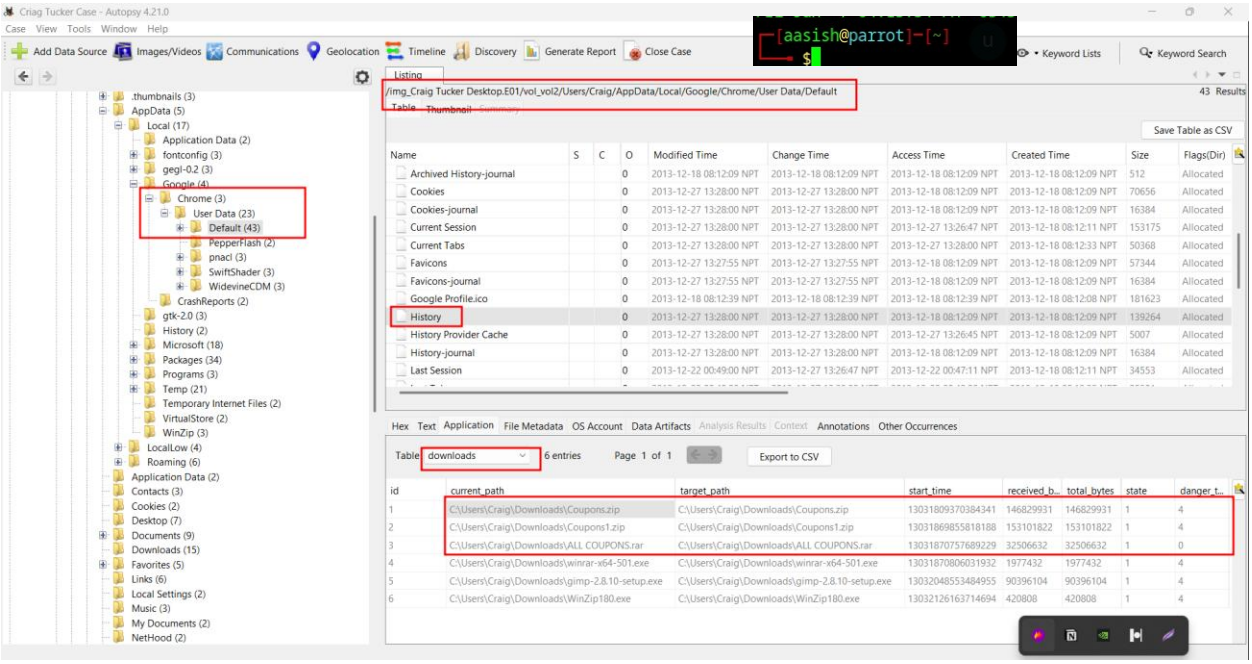


And next to internet explorer

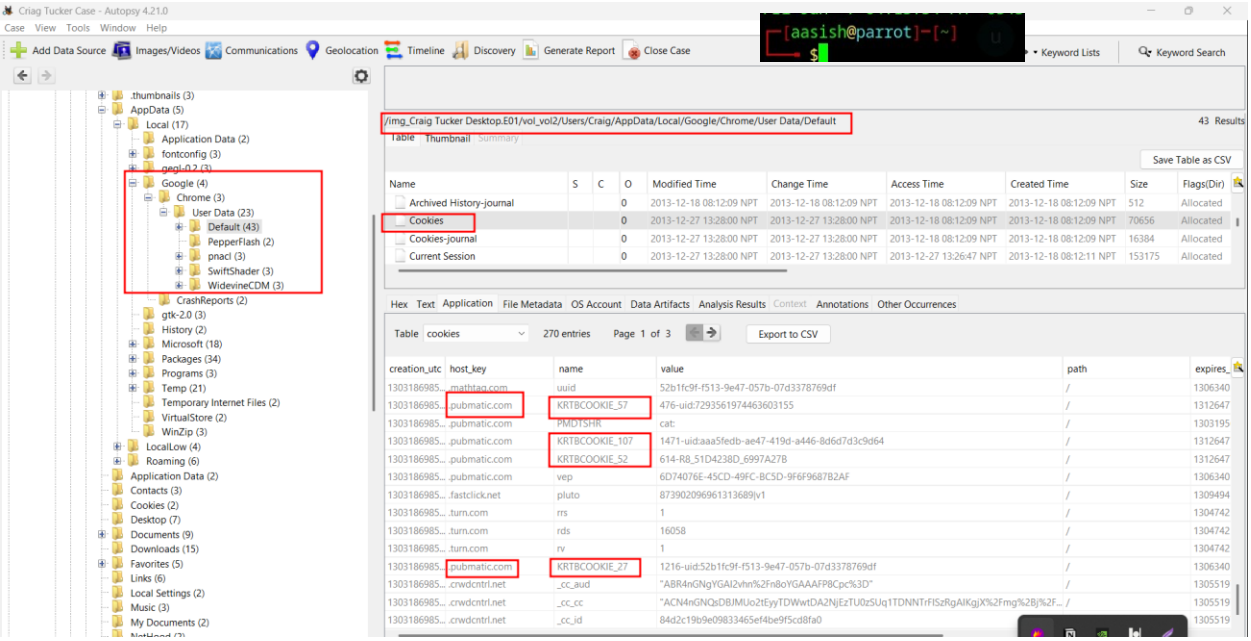


Next SQLite view

For google chrome



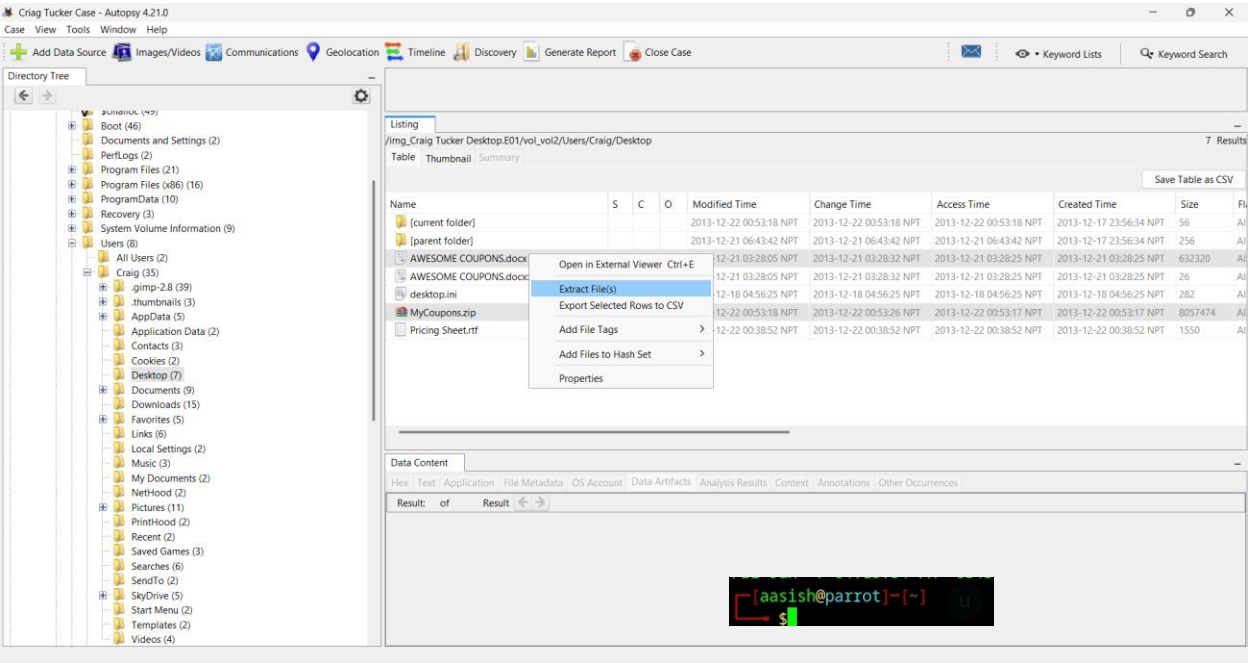
Here the coupons zip files are downloaded



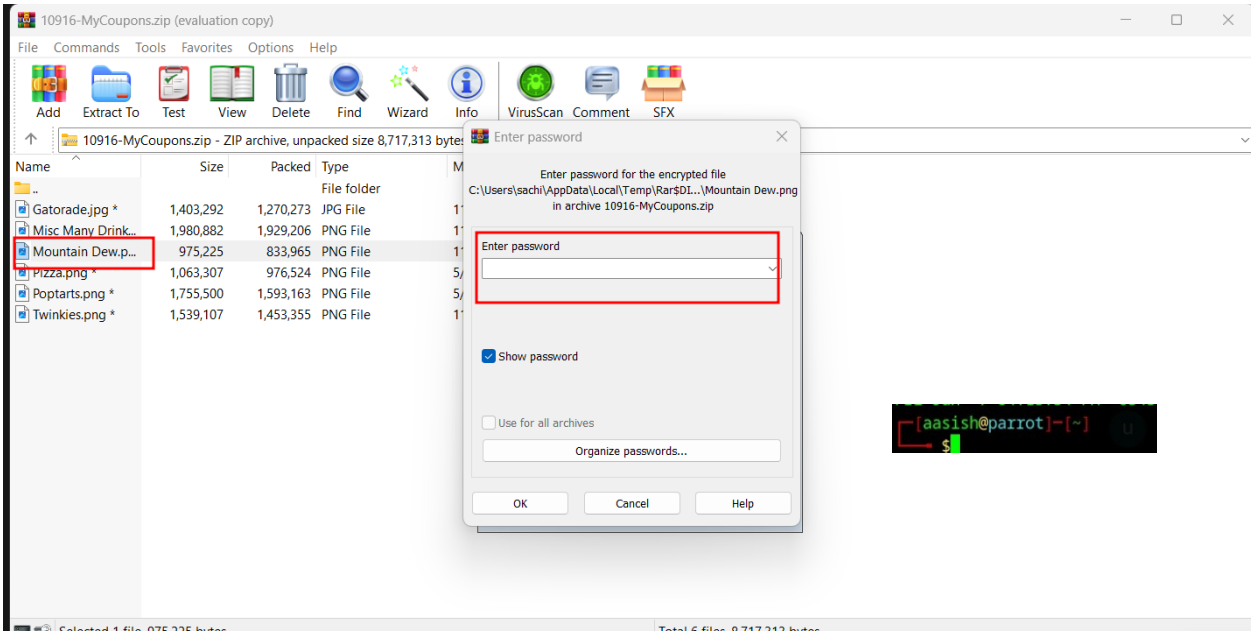
Here the pubmatic.com is preety suspicious having the name KRTBCOKIE_27

Hidden or Encrypted Data

Now let’s try to open encrypted zip files that we have got before

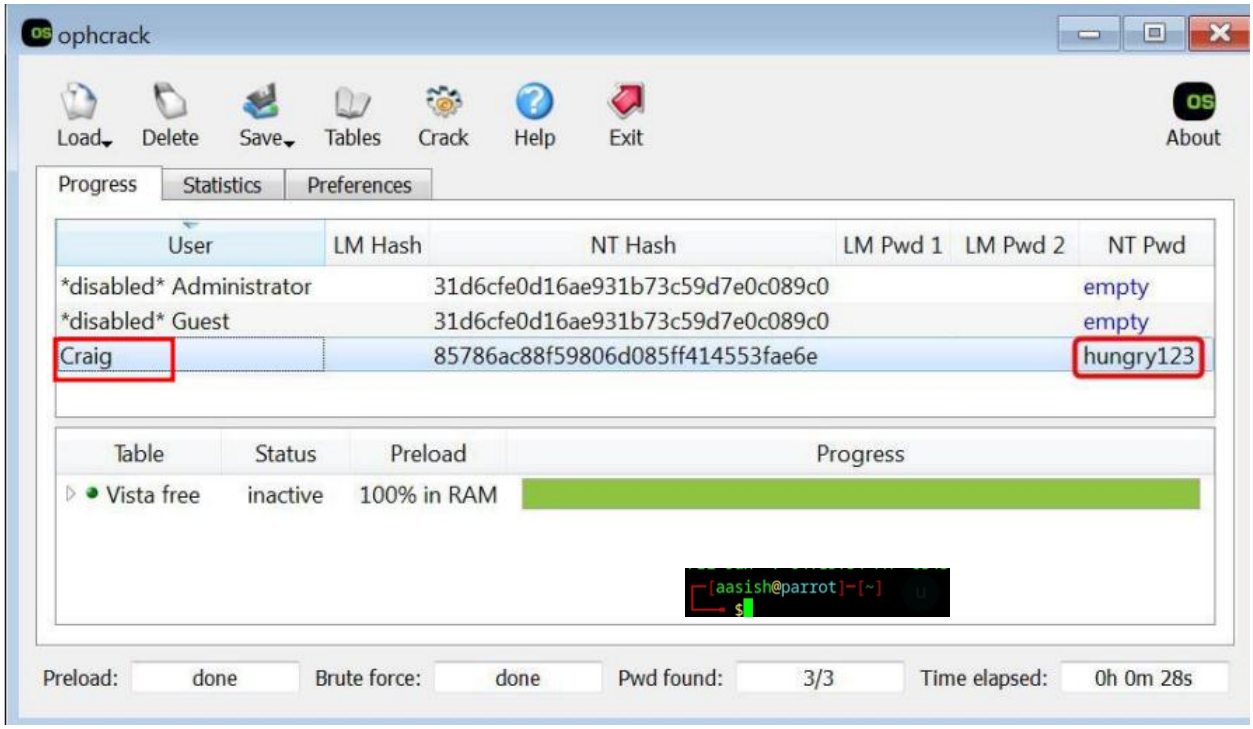


Extracting the files



Now let’s crack the password

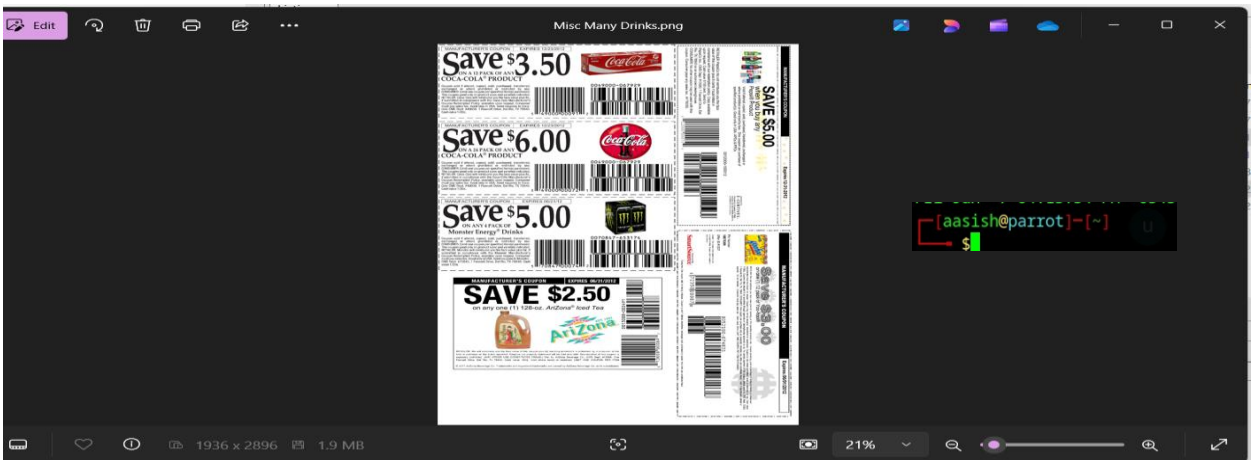
Using ophcrack

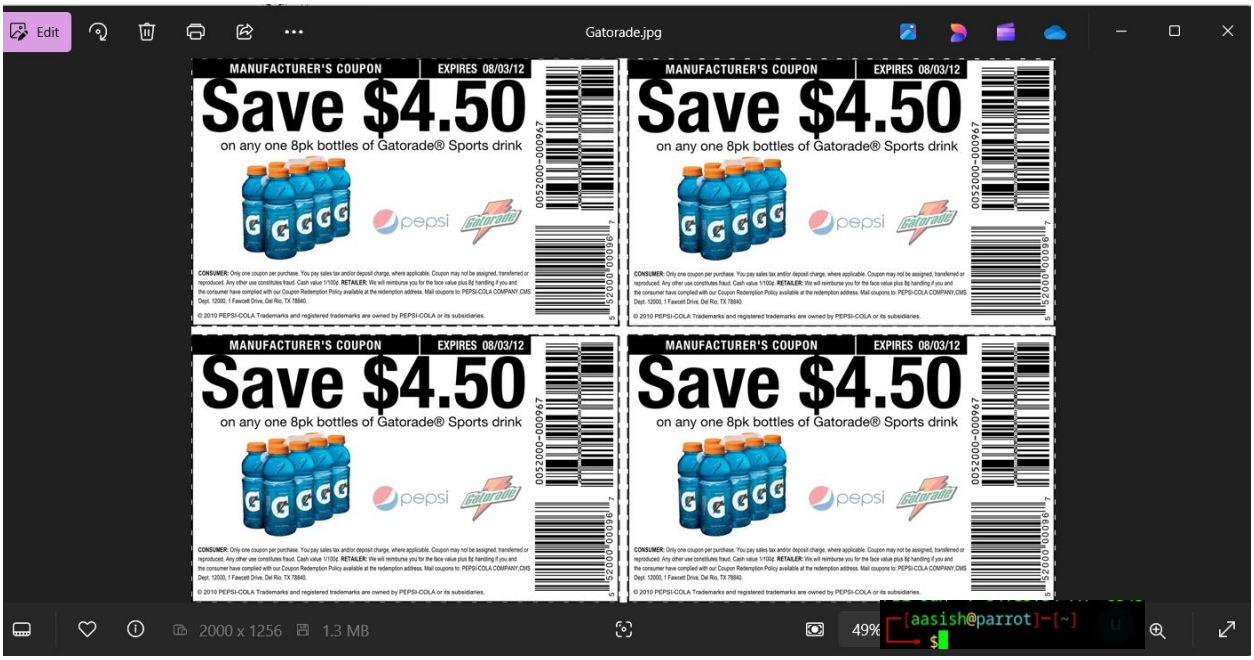


We got “hungry123” as password

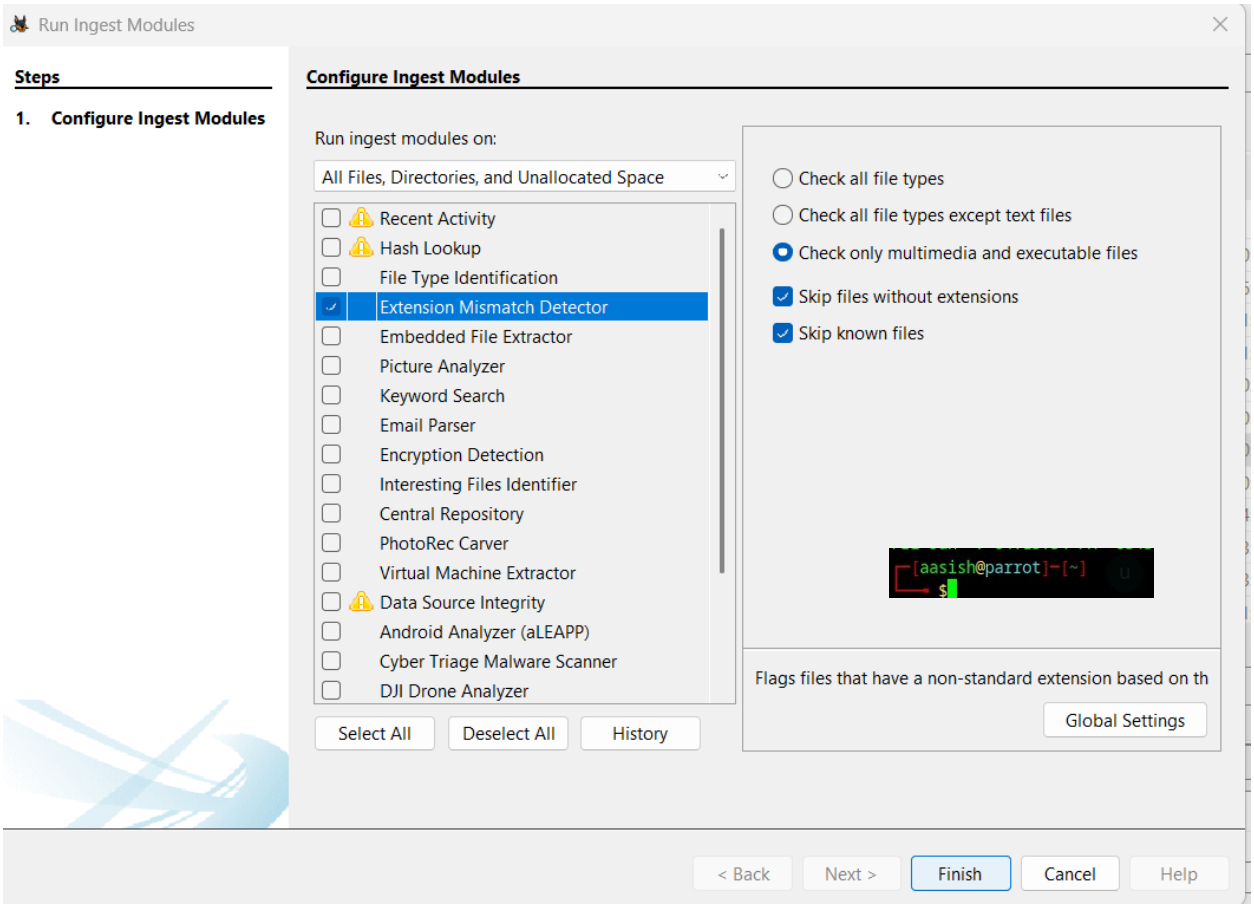
Now using it to decrypting the zip files

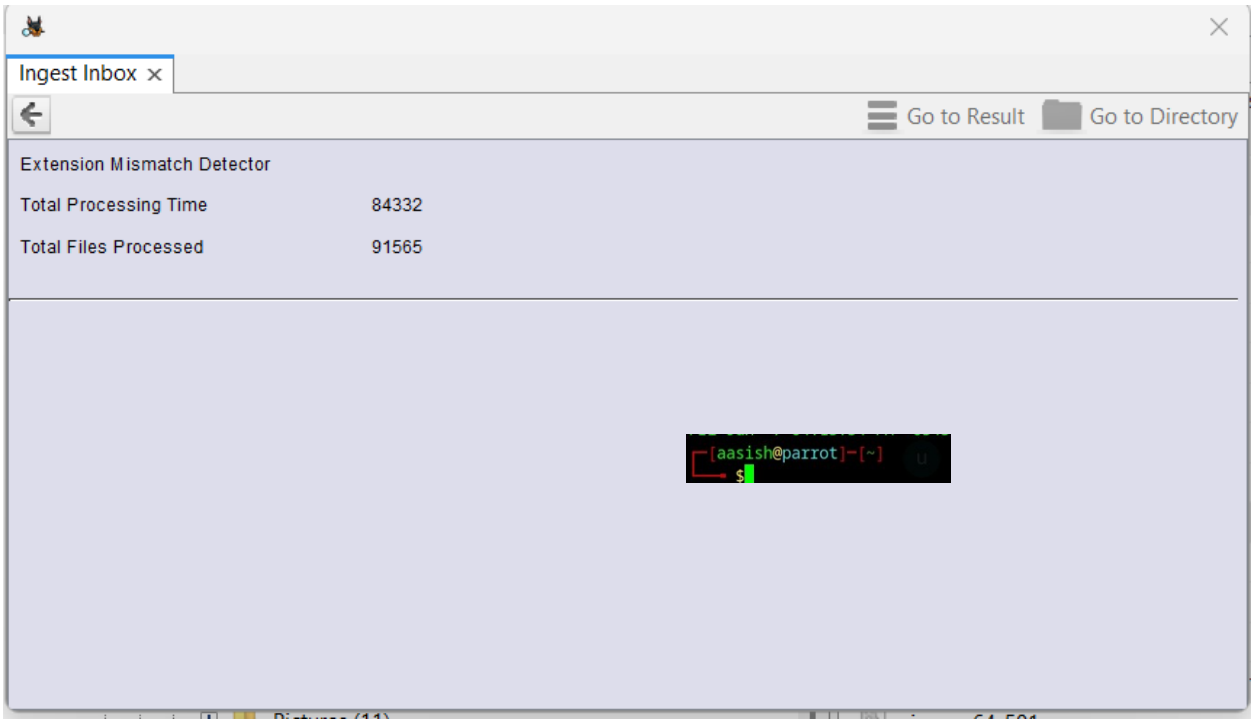
After using password we got the coupons



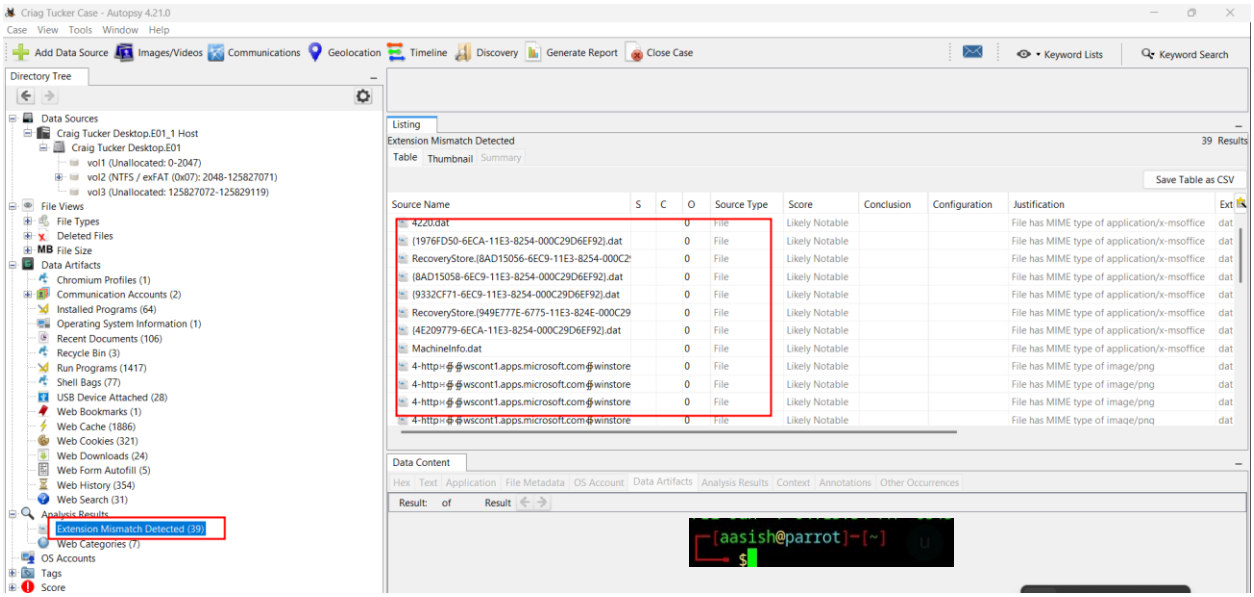


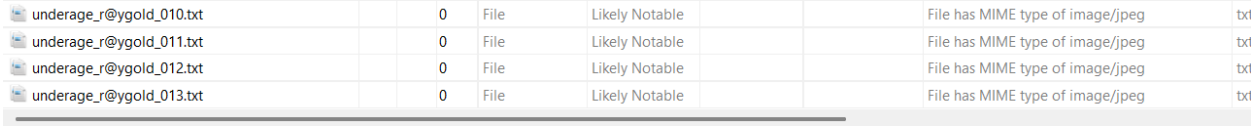
So for hidden files running ingest module



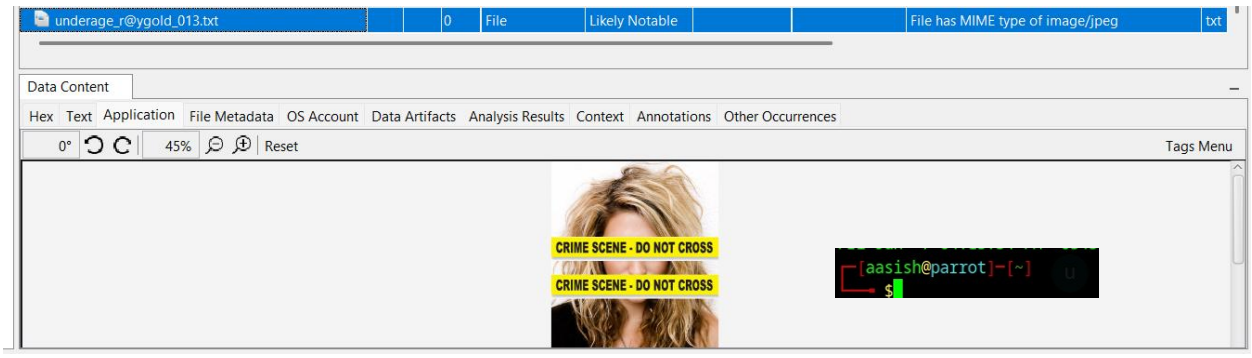


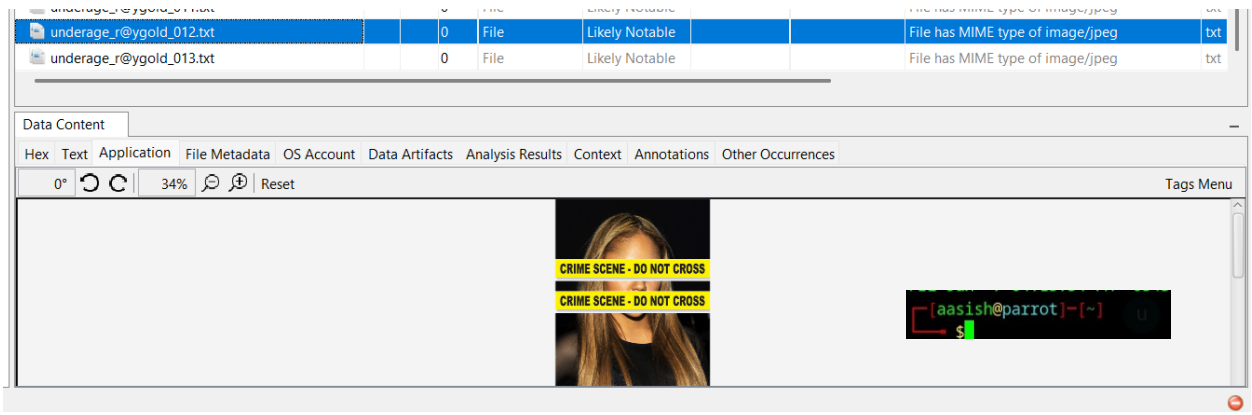
Hidden files:

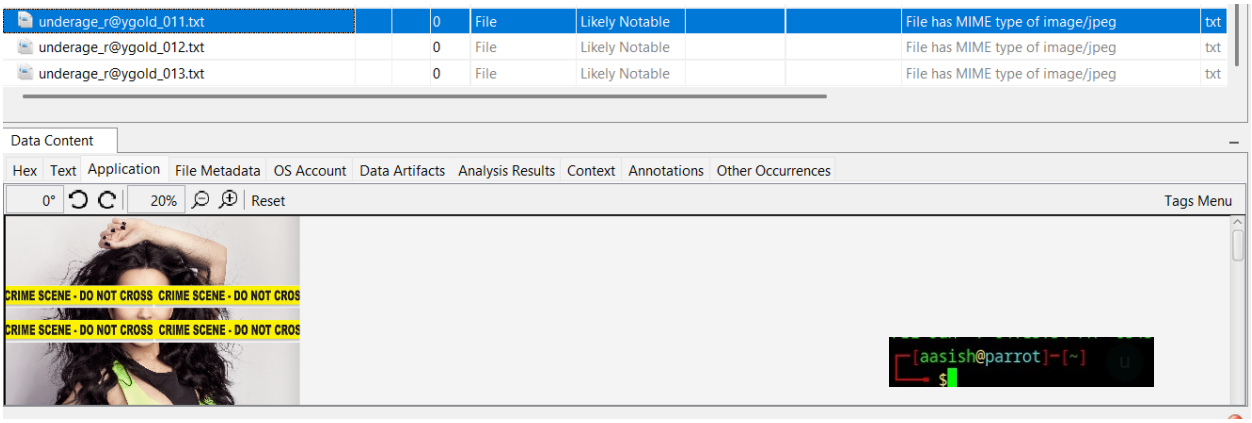


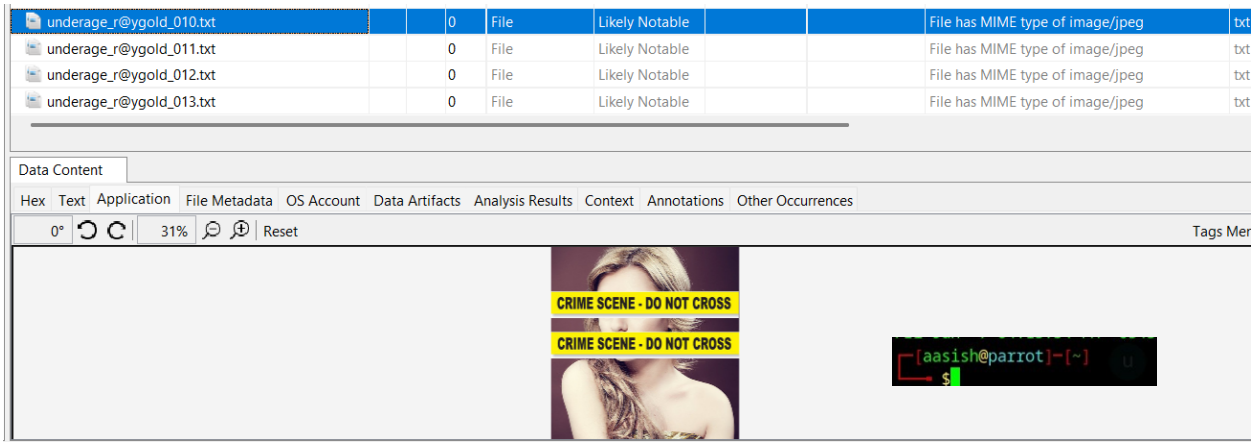


Here we get the text files


underage_r@ygold_013.txt 0 File Likely Notable File has MIME type of image/jpeg txt
Data Content
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
0° 45% Reset Tags Menu
CRIME SCENE - DO NOT CROSS
CRIME SCENE - DO NOT CROSS
[aasish@parrot]-[~]
$


underage_r@ygold_012.txt 0 File Likely Notable File has MIME type of image/jpeg txt
underage_r@ygold_013.txt 0 File Likely Notable File has MIME type of image/jpeg txt
Data Content
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
0° 34% Reset Tags Menu
CRIME SCENE - DO NOT CROSS
CRIME SCENE - DO NOT CROSS
[aasish@parrot]-[~]
$


underage_r@ygold_011.txt 0 File Likely Notable File has MIME type of image/jpeg txt
underage_r@ygold_012.txt 0 File Likely Notable File has MIME type of image/jpeg txt
underage_r@ygold_013.txt 0 File Likely Notable File has MIME type of image/jpeg txt
Data Content
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
0° 20% Reset Tags Menu
CRIME SCENE - DO NOT CROSS CRIME SCENE - DO NOT CROS
CRIME SCENE - DO NOT CROSS CRIME SCENE - DO NOT CROS
[aasish@parrot]-[~]
$


underage_r@ygold_010.txt 0 File Likely Notable File has MIME type of image/jpeg txt
underage_r@ygold_011.txt 0 File Likely Notable File has MIME type of image/jpeg txt
underage_r@ygold_012.txt 0 File Likely Notable File has MIME type of image/jpeg txt
underage_r@ygold_013.txt 0 File Likely Notable File has MIME type of image/jpeg txt
Data Content
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
0° 31% Reset
CRIME SCENE - DO NOT CROSS
CRIME SCENE - DO NOT CROSS
[aasish@parrot]-[~]
$

Listing

Extension Mismatch Detected — 39 Results

Table | Thumbnail | Summary

Save Table as CSV

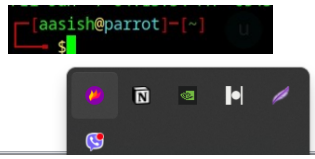
Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Ext
{DEAC9D0B-6774-11E3-824E-000C29D6EF92}.dat			0	File	Likely Notable			File has MIME type of application/x-msoffice	dat
{D5506EEE-6774-11E3-824E-000C29D6EF92}.dat			0	File	Likely Notable			File has MIME type of application/x-msoffice	dat
{F687F41F-6774-11E3-824E-000C29D6EF92}.dat			0	File	Likely Notable			File has MIME type of application/x-msoffice	dat
{F687F420-6774-11E3-824E-000C29D6EF92}.dat			0	File	Likely Notable			File has MIME type of application/x-msoffice	dat
comempty.dat			0	File	Likely Notable			File has MIME type of application/x-msoffice	dat
comempty.dat			0	File	Likely Notable			File has MIME type of application/x-msoffice	dat
comempty.dat			0	File	Likely Notable			File has MIME type of application/x-msoffice	dat
comempty.dat			0	File	Likely Notable			File has MIME type of application/x-msoffice	dat
underage_r@ygold_010.txt			0	File	Likely Notable			File has MIME type of image/jpeg	txt
underage_r@ygold_011.txt			0	File	Likely Notable			File has MIME type of image/jpeg	txt
underage_r@ygold_012.txt			0	File	Likely Notable			File has MIME type of image/jpeg	txt
underage_r@ygold_013.txt			0	File	Likely Notable			File has MIME type of image/jpeg	txt

Data Content

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Page: 1 of 8 Page Go to Page: 1 Jump to Offset Launch in HxD

```
0x00000000: FF D8 FF E0  00 10 4A 46   49 46 00 01  01 01 00 5F   ......JFIF....._
0x00000010: 00 5F 00 00  FF DB 00 43   00 03 02 02  03 02 02 03   ._.....C........
0x00000020: 03 03 03 04  03 03 04 05   08 05 05 04  04 05 0A 07   ................
0x00000030: 07 06 08 0C  0A 0C 0C 0B   0A 0B 0B 0D  0E 12 10 0D   ................
0x00000040: 0E 11 0E 0B  0B 10 16 10   11 13 14 15  15 15 0C 0F   ................
0x00000050: 17 18 16 14  18 12 14 15   14 FF DB 00  43 01 03 04   ............C...
0x00000060: 04 05 04 05  09 05 05 09   14 0D 0B 0D  14 14 14 14   ................
0x00000070: 14 14 14 14  14 14 14 14   14 14 14 14  14 14 14 14   ................
0x00000080: 14 14 14 14  14 14 14 14   14 14 14 14  14 14 14 14   ................
```



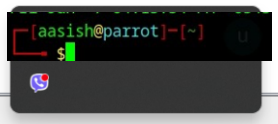
[current folder]				2013-12-27 13:42:34 NPT	2013-12-27 13:42:49 NPT	2013-12-27 13:42:34 NPT	2013-12-27 13:39:50 NPT	56	Al
[parent folder]				2013-12-30 09:45:47 NPT	2013-12-30 09:45:47 NPT	2013-12-30 09:45:47 NPT	2013-08-22 19:21:16 NPT	56	Al
underage_r@ygold_010.txt			0	2013-12-27 13:35:33 NPT	2013-12-27 13:42:49 NPT	2013-12-27 13:36:10 NPT	2013-12-27 13:36:10 NPT	124385	Al
underage_r@ygold_010.txt:Zone.Identifier			0	2013-12-27 13:35:33 NPT	2013-12-27 13:42:49 NPT	2013-12-27 13:36:10 NPT	2013-12-27 13:36:10 NPT	26	Al
underage_r@ygold_011.txt			0	2013-12-27 13:35:42 NPT	2013-12-27 13:42:49 NPT	2013-12-27 13:36:17 NPT	2013-12-27 13:36:17 NPT	383370	Al
underage_r@ygold_011.txt:Zone.Identifier			0	2013-12-27 13:35:42 NPT	2013-12-27 13:42:49 NPT	2013-12-27 13:36:17 NPT	2013-12-27 13:36:17 NPT	26	Al
underage_r@ygold_012.txt			0	2013-12-27 13:35:44 NPT	2013-12-27 13:42:49 NPT	2013-12-27 13:36:21 NPT	2013-12-27 13:36:21 NPT	92801	Al
underage_r@ygold_012.txt:Zone.Identifier			0	2013-12-27 13:35:44 NPT	2013-12-27 13:42:49 NPT	2013-12-27 13:36:21 NPT	2013-12-27 13:36:21 NPT	26	Al
underage_r@ygold_013.txt			0	2013-12-27 13:35:47 NPT	2013-12-27 13:42:49 NPT	2013-12-27 13:36:26 NPT	2013-12-27 13:36:26 NPT	68992	Al
underage_r@ygold_013.txt:Zone.Identifier			0	2013-12-27 13:35:47 NPT	2013-12-27 13:42:49 NPT	2013-12-27 13:36:26 NPT	2013-12-27 13:36:26 NPT	26	Al

Data Content

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Page: 1 of 8 Page Go to Page: 1 Jump to Offset Launch in HxD

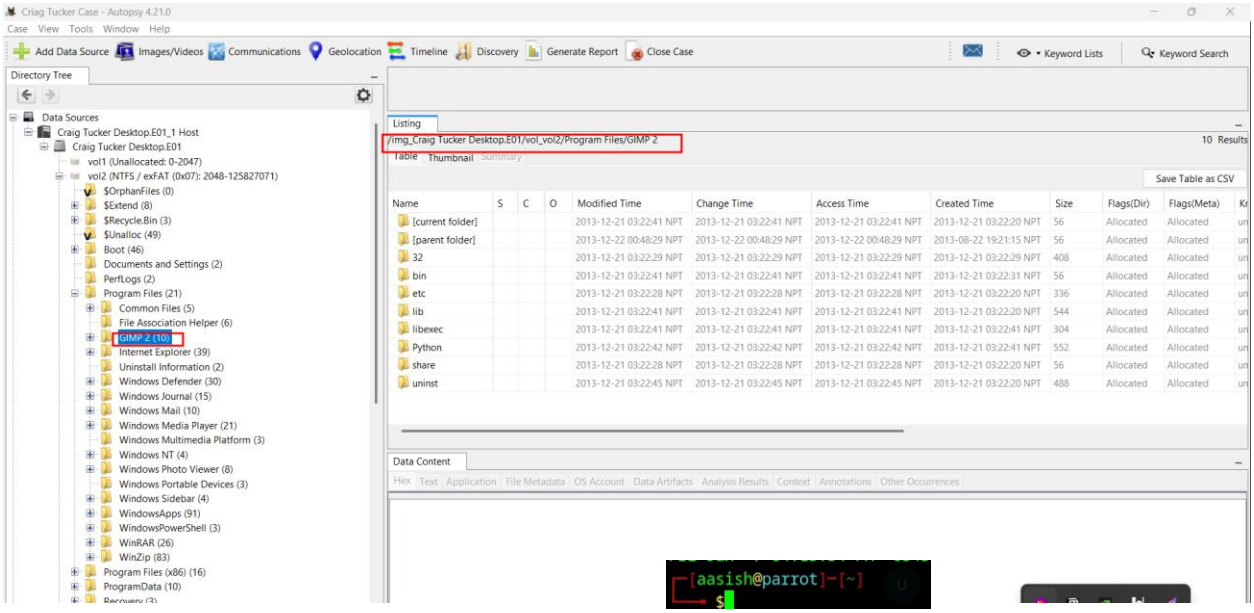
```
0x00000000: FF D8 FF E0  00 10 4A 46   49 46 00 01  01 01 00 5F   ......JFIF....._
0x00000010: 00 5F 00 00  FF DB 00 43   00 03 02 02  03 02 02 03   ._.....C........
0x00000020: 03 03 03 04  03 03 04 05   08 05 05 04  04 05 0A 07   ................
0x00000030: 07 06 08 0C  0A 0C 0C 0B   0A 0B 0B 0D  0E 12 10 0D   ................
0x00000040: 0E 11 0E 0B  0B 10 16 10   11 13 14 15  15 15 0C 0F   ................
0x00000050: 17 18 16 14  18 12 14 15   14 FF DB 00  43 01 03 04   ............C...
0x00000060: 04 05 04 05  09 05 05 09   14 0D 0B 0D  14 14 14 14   ................
0x00000070: 14 14 14 14  14 14 14 14   14 14 14 14  14 14 14 14   ................
0x00000080: 14 14 14 14  14 14 14 14   14 14 14 14  14 14 14 14   ................
```



Installed Programs

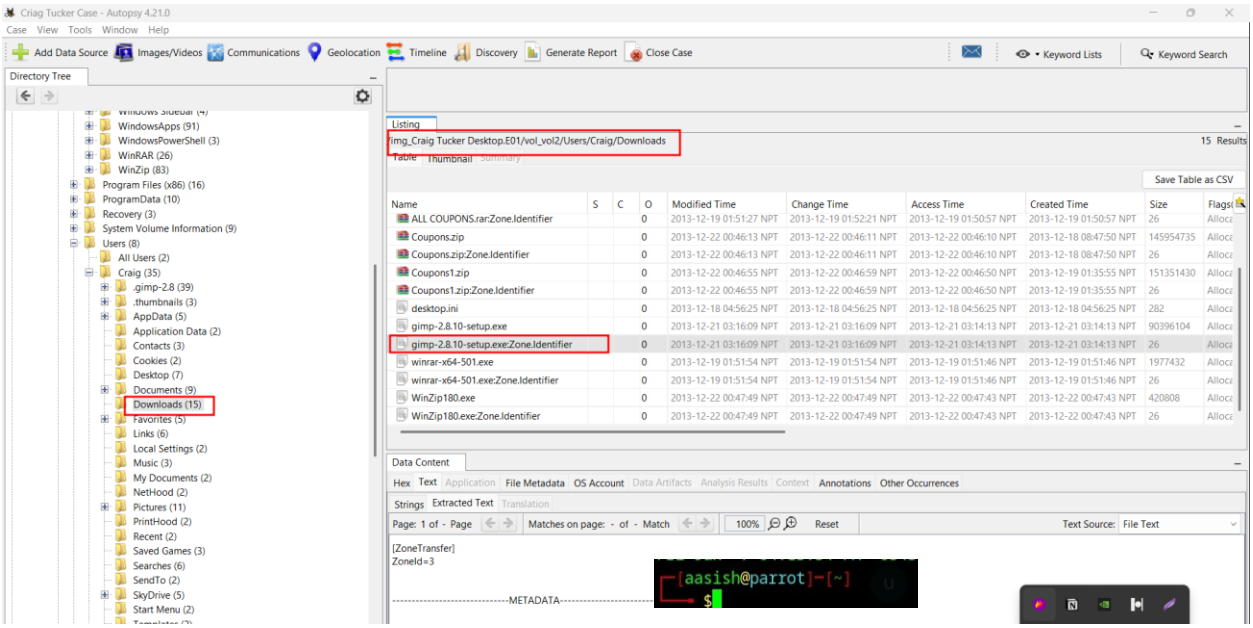
First look into program files

First one is GIMP2



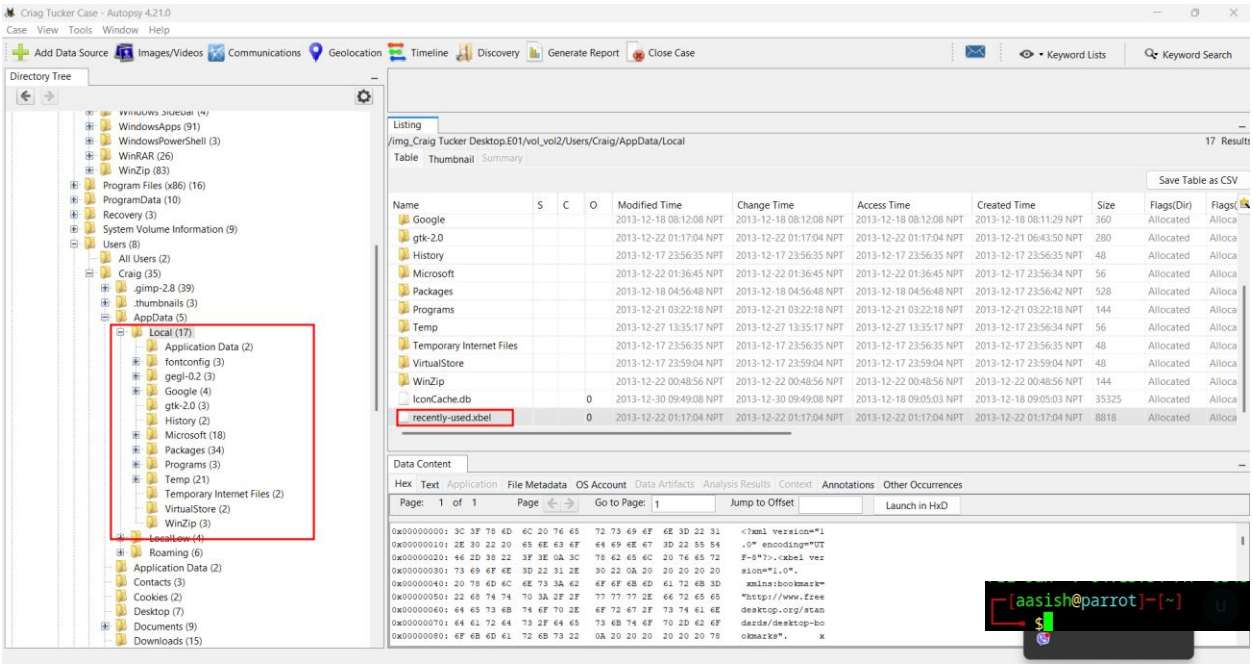
GIMP: GIMP is a freeware graphic manipulation tool. You can alter pictures and add layers to a photo with it. If you look at Craig's email, there is one called "Re: Coupon Making" from Stan Marsh. Craig had asked him how to make his own coupons, and then Stan attached two guides and told him to download GIMP.

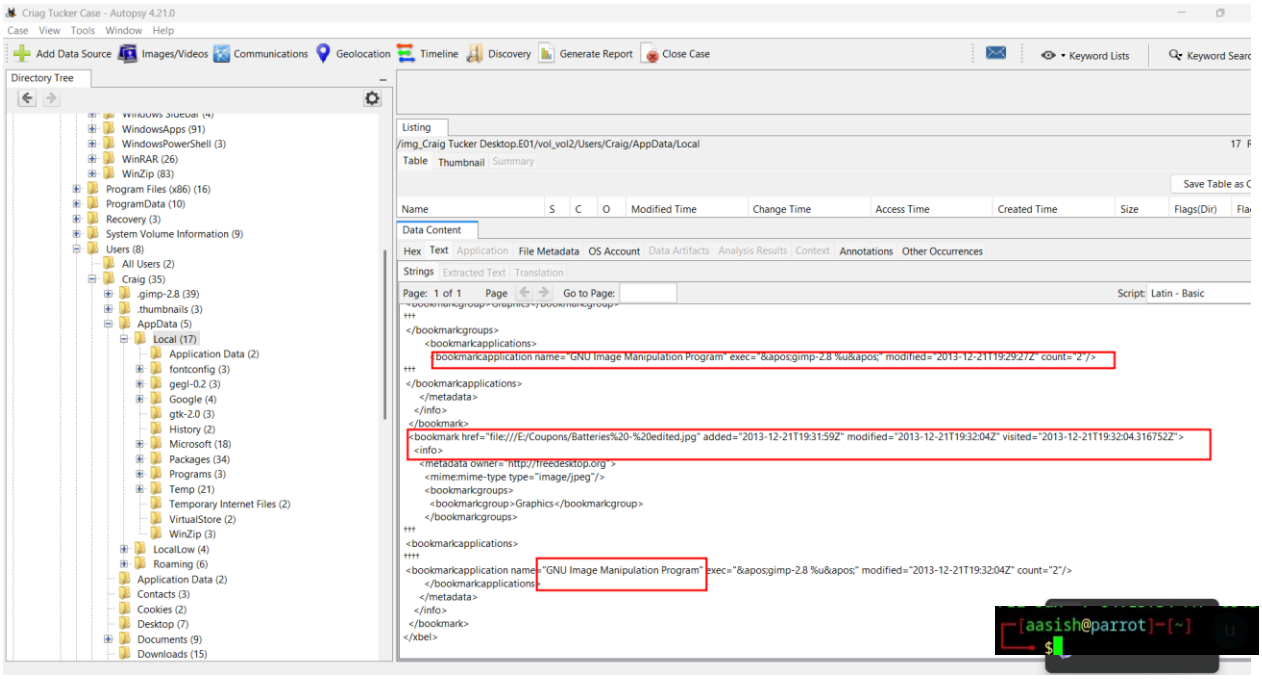
Again in the downloads folder



cirag has downloaded it

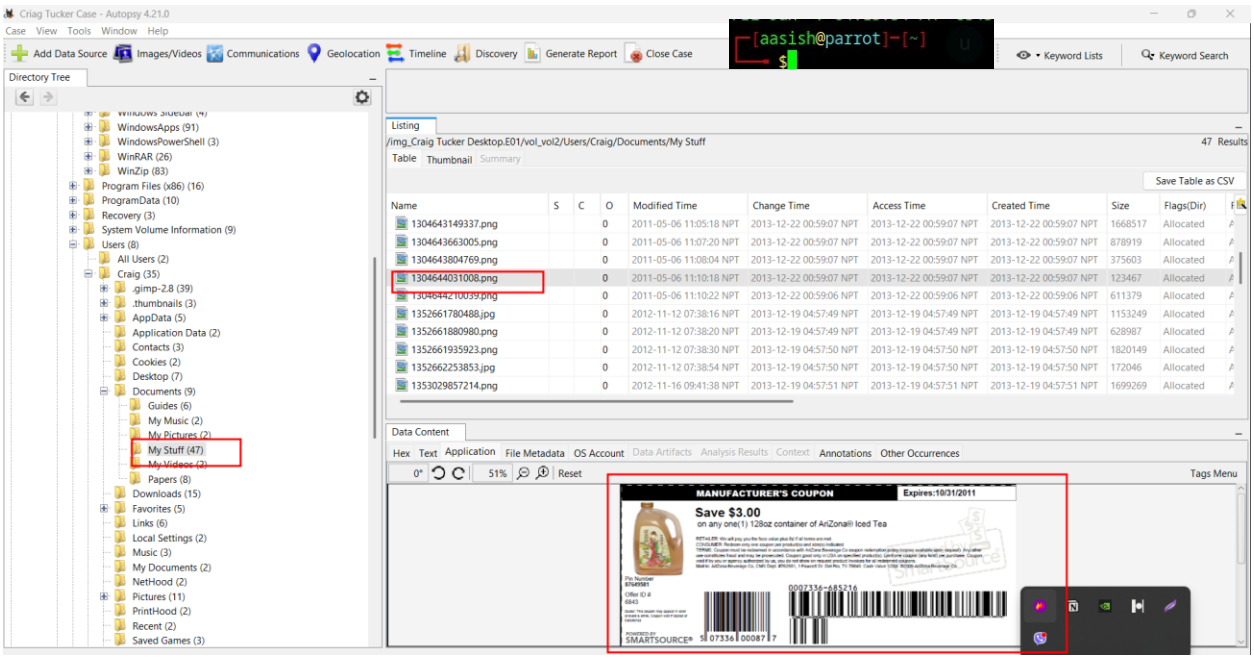
Now again explore document history






```
</bookmark>
<bookmark href="file:///C:/Users/Craig/Documents/My%20Stuff/Iced%20tea%20-%20edited.png" added="2013-12-21T19:19:52Z" modified="2013-12-21T19:19:58Z" visited="2013-12-21T19:19:52Z">
  <info>
    <metadata owner="http://freedesktop.org">
+++
```

And the file is:



Result and Analysis

Phase 1: Forensic Image Analysis

Creating the Case and Verifying Forensic Image

- A forensic image of Craig Tucker's computer was analyzed using Autopsy and FTK Imager.
- The integrity of the forensic image (E01 file) was verified using SHA-256 hash validation, ensuring that the data was unaltered and admissible in legal proceedings.

Drive Geometry and Operating System Information

- The drive was formatted in NTFS/exFAT file system.
- The system was identified as **Windows 8.1 Pro**, which helped determine relevant artifacts and system logs for analysis.

Establishing Time Zone and User Identification

- The time zone was determined to be **Pacific Standard Time (PST)** using Registry Explorer.
- The system had three users: **Administrator, Guest, and Craig**, with Craig's account being the primary suspect.

Phase 2: Evidence Discovery and Analysis

User's Personal Data

- A large number of **coupon-related files** were found across various directories, including **Desktop, My Documents, Downloads, and SkyDrive**.
- Tutorial files explaining **how to make coupons** were recovered.
- Multiple compressed files (.zip, .rar) containing coupon data were found in the Downloads folder.

LNK Files and JumpLists

- **Shortcut files (.lnk) and JumpLists** showed that Craig accessed coupon-related files multiple times.
- Some JumpLists indicated access to external storage devices and specific files, such as **MyCoupons.zip** and **Russian Videos**.

Recycle Bin Analysis

- Deleted images with **crime scene indicators** were recovered.
- Other deleted coupon-related documents were found in the Recycle Bin, suggesting an attempt to remove evidence.

USB Device Analysis

- The **USB device history** indicated multiple external drives were connected, possibly used for transferring data.
- Registry analysis provided OEM and serial numbers of the attached USB devices.

Email Review

- Emails indicated that Craig was **communicating about coupon deals** with multiple individuals, including Kenny McCormic and Kyle Broflovski.
- One email from Stan Marsh included **instructions on how to create fake coupons** and recommended **GIMP** as a tool.

Internet History Analysis

- **Downloaded coupon files** were found in browser history logs.
- Suspicious website activity, including **Pubmatic.com**, was discovered, possibly linked to fraudulent activities.

Hidden or Encrypted Data Analysis

- Multiple **encrypted ZIP files** were recovered.
- The password **"hungry123"** was cracked using **Ophcrack**, revealing more counterfeit coupon files.

Installed Programs Analysis

- Craig had installed **GIMP 2**, a graphics editing tool used for modifying images.
- Files related to **coupon editing and creation** were found in the document history and downloads folder.

Discussion

The forensic investigation into Craig Tucker's digital activities provides a clear example of how digital evidence can be systematically collected, analyzed, and interpreted in cybercrime cases. The findings highlight several key aspects, including the suspect's digital footprint and intent, data concealment, forensic challenges, and implications for cybercrime investigations. The extensive presence of coupon-related files, combined with tutorial guides on coupon creation, indicates premeditated involvement in fraudulent activities. The forensic timeline and metadata suggest that the suspect intentionally accessed and modified counterfeit coupons. Additionally, the use of encrypted ZIP files and the presence of deleted data in the Recycle Bin demonstrate an effort to hide evidence. The suspect's browsing history and email exchanges suggest collaboration or communication with other individuals potentially involved in similar fraudulent activities.

While forensic tools such as Autopsy, FTK Imager, and Registry Explorer were effective in uncovering digital artifacts, challenges such as data encryption, deleted file recovery, and verifying user intent were encountered. The presence of potentially illicit content raised legal and ethical concerns, emphasizing the need for strict adherence to forensic investigation protocols. This case also highlights the importance of time zone verification, USB device tracking, and LNK/JumpList analysis in reconstructing digital activities. The successful password recovery and decryption of hidden files reinforce the role of advanced forensic techniques in obtaining crucial evidence.

Overall, this forensic analysis provides a strong basis for legal proceedings against the suspect. The findings reinforce the critical role of digital forensics in bridging gaps between physical and electronic evidence, ensuring that cybercrimes can be thoroughly investigated and prosecuted.

Conclusion and Future Works

This investigation successfully demonstrated the importance of digital forensics in uncovering fraudulent activities and securing digital evidence for legal proceedings. By utilizing a structured forensic approach, including disk imaging, metadata analysis, and email tracing, the investigation effectively reconstructed the suspect's actions and identified key evidence. The case highlights the necessity of proper forensic methodologies in ensuring data integrity and maintaining the chain of custody for legal admissibility.

Future work in this domain should focus on advancing forensic tools to better handle encrypted and deleted data, improving AI-driven analysis for faster and more accurate detection of suspicious activities, and enhancing cybersecurity measures to prevent such digital fraud cases from occurring. Additionally, incorporating machine learning algorithms for anomaly detection and integrating blockchain-based evidence authentication could further strengthen digital forensic investigations. Continued research and collaboration between law enforcement agencies, cybersecurity experts, and forensic analysts will be crucial in keeping pace with evolving cyber threats.