

## Digital Forensics



## Contents

Texas College of Management and IT.....	1
Digital Forensics .....	1
Abstract .....	4
Introduction.....	4
Literature Review.....	5
Methodology .....	6
Requirement Analysis .....	6
Tucker Case Summary .....	7
PHASE-1.....	8
Creating the case: .....	8
Verifying the Forensic Image.....	11
Drive Geometry .....	13
Operating System.....	13
Establishing the Time Zone .....	14
Identify Computer User .....	16
Phase - 2 .....	17
User's Personal Data.....	17
LNK Files and JumpLists .....	20
Jumplists .....	22
Recycle Bin .....	27
Attached USB OEM/serial number .....	28
Email-Review .....	28
Internet History .....	31
Hidden or Encrypted Data .....	33

Installed Programs .....	39
Result and Analysis.....	42
Discussion.....	44
Conclusion and Future Works.....	45

## 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. **USBDevview:** 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.

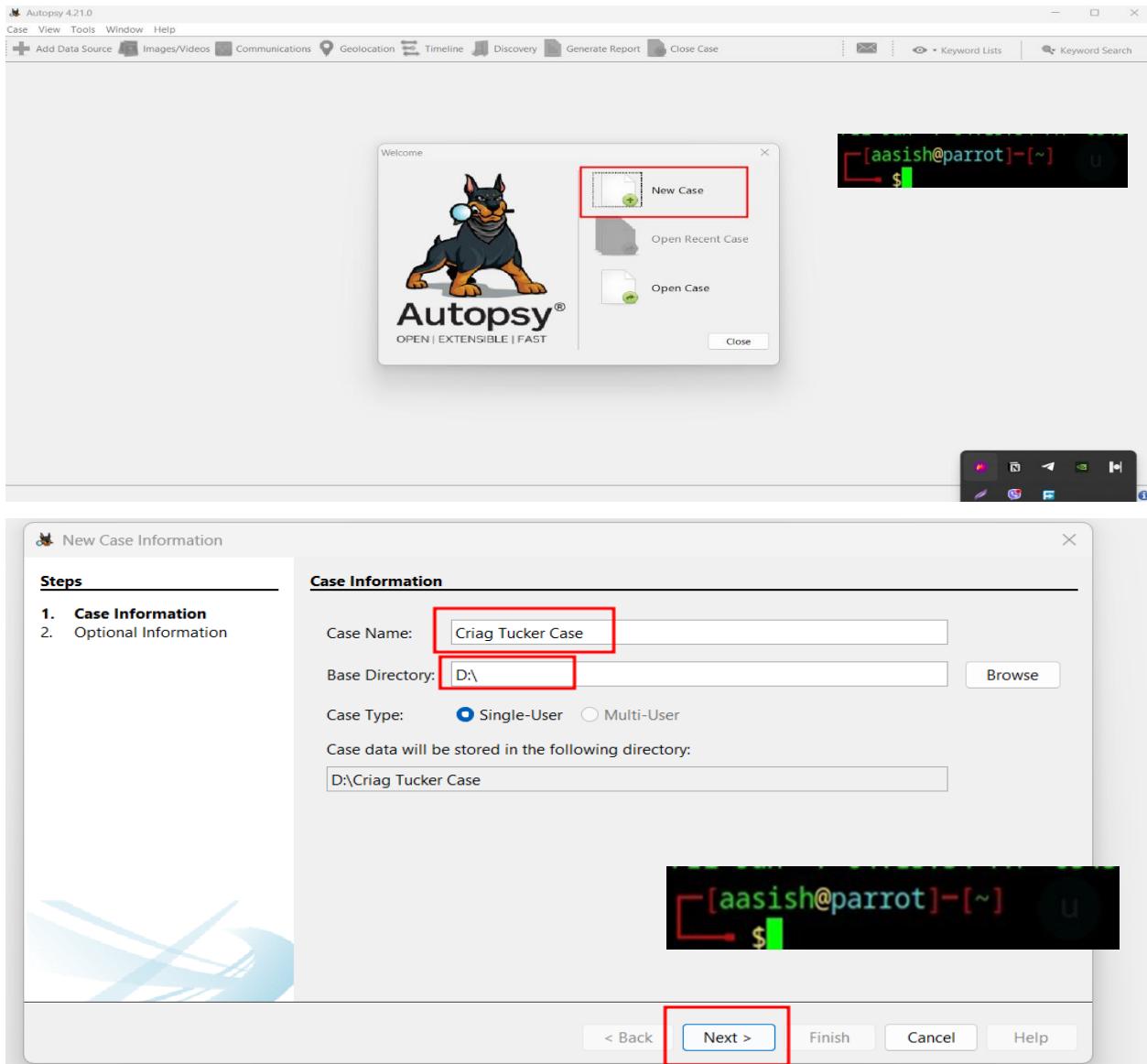
## **Tucker Case Summary**

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

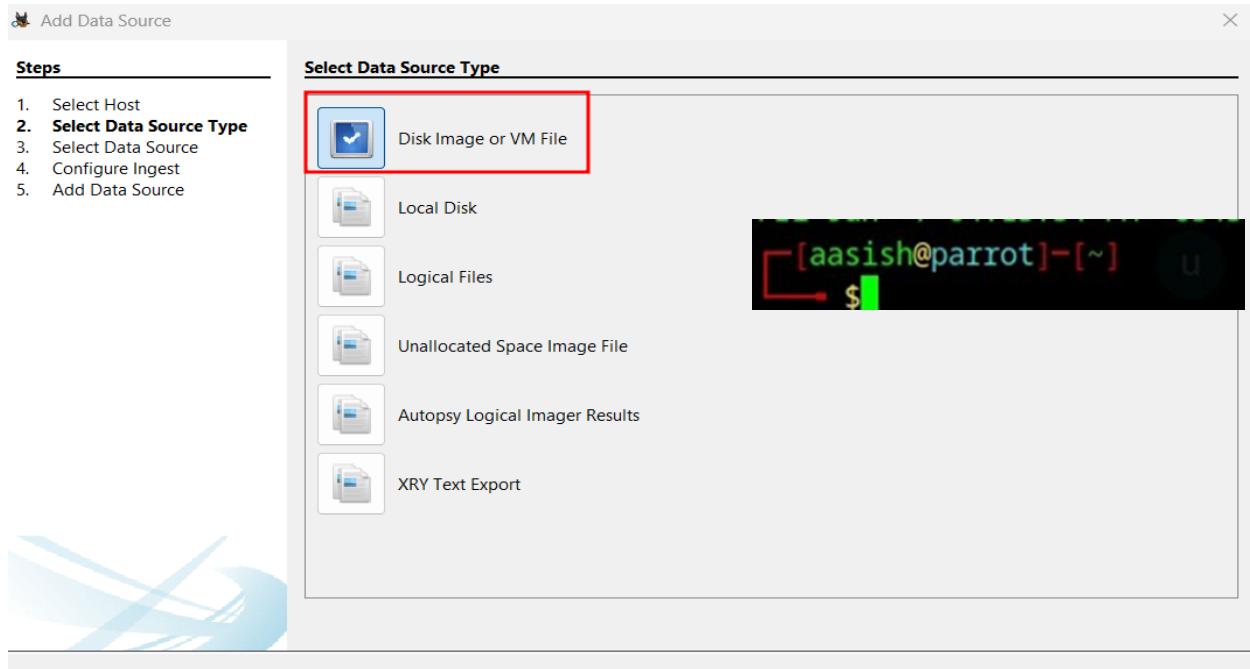
### Creating the case:



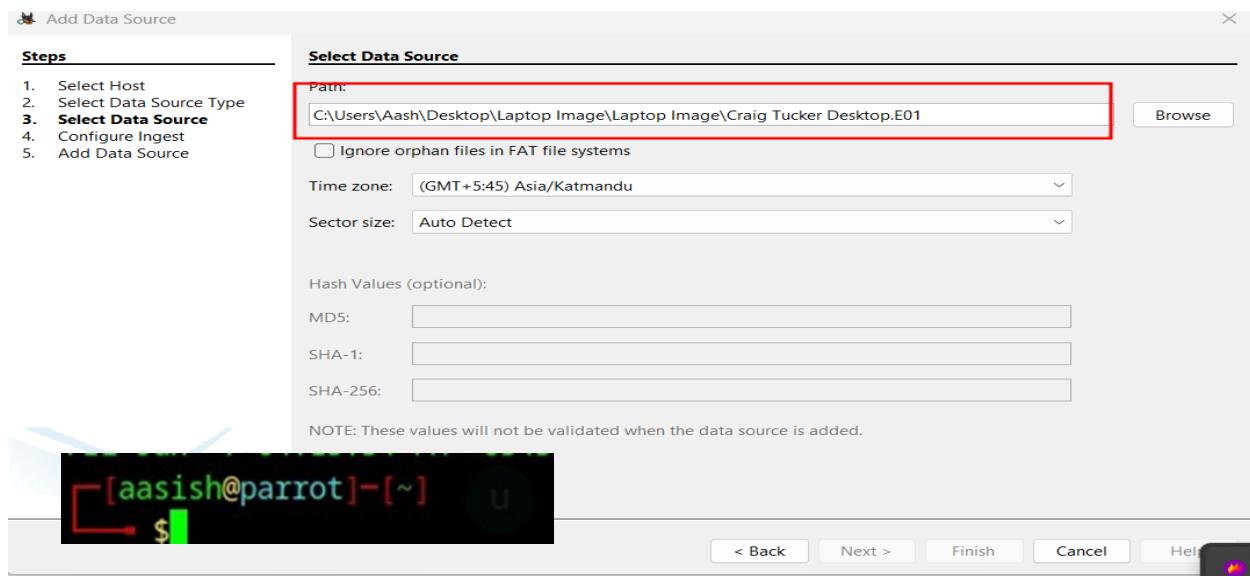
Case name: Criag Tucker Case

Base Directory: D:\

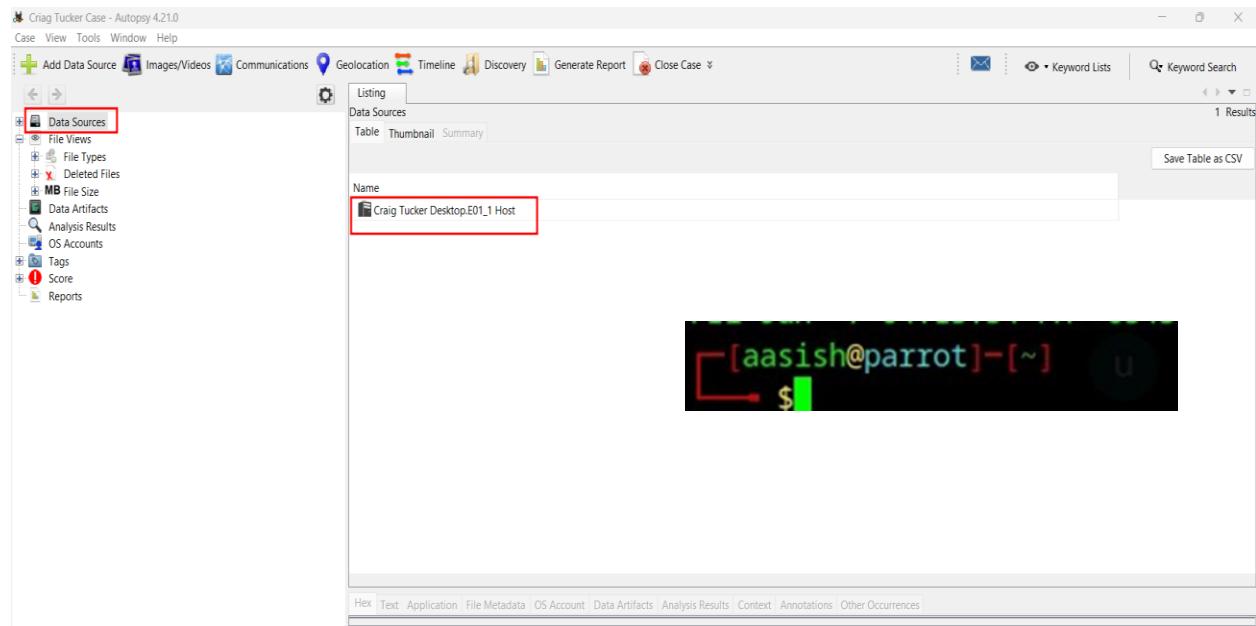
Selecting Disk Image because it's E01 file that is given to us



Specifying the disk path "Craig Tucker Desktop.E01"

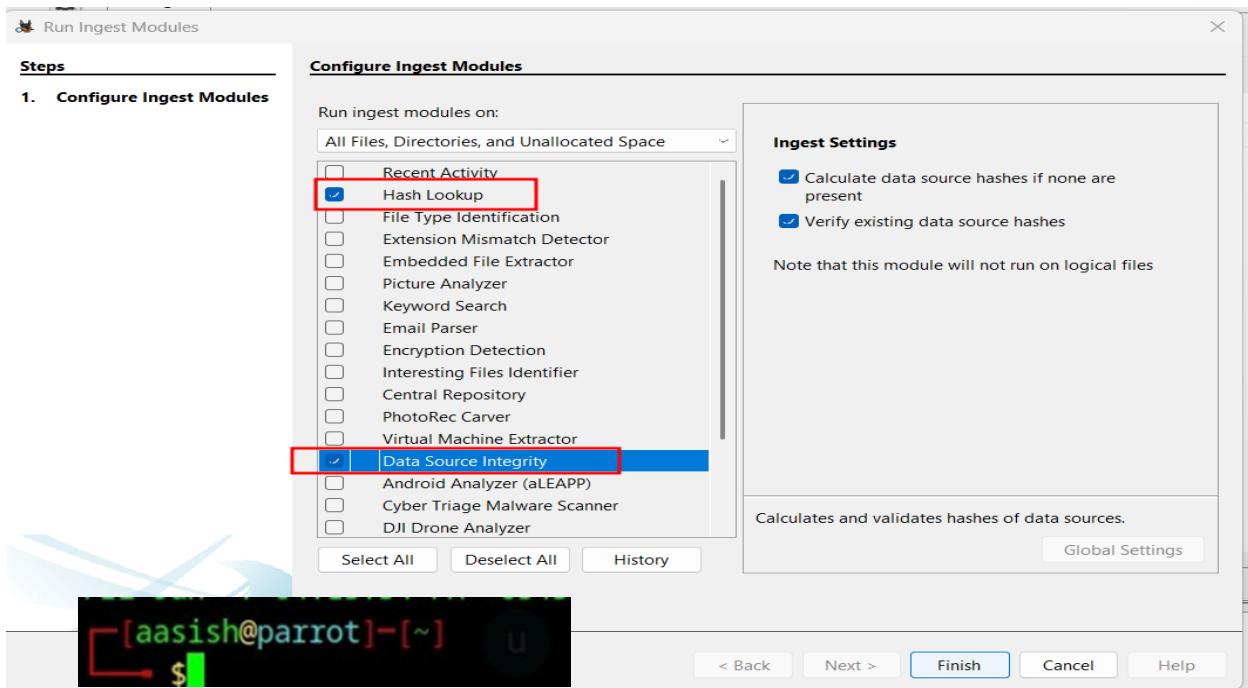


Finally after completing the ingest module here comes the extracted file from the E01 file

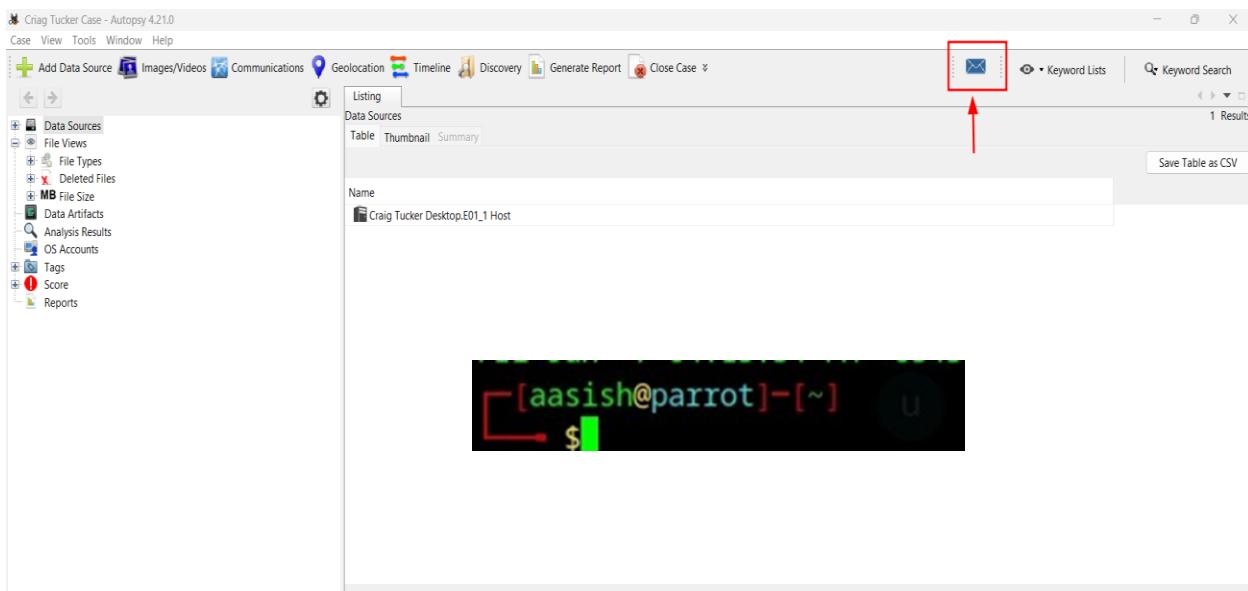


## Verifying the Forensic Image

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 results



Here it is, says verified

Module	Num	New?	Subject	Timestamp
Hash Lookup	1		No notable hash set.	2025/03/10 12:3..
Hash Lookup	1		No known hash set.	2025/03/10 12:3..
Data Source Integrity	1		Starting Craig Tucker Desktop.E01	2025/03/10 12:4..
Data Source Integrity	1	•	Integrity of Craig Tucker Desktop.E01 verified	2025/03/10 12:4..

Let's check and now it's verified!

Data Source Verification Results for Craig Tucker Desktop.E01	
• Result:	verified
• MD5 hash verified	
• Calculated hash:	4e1832956d635ec4e4feba8775a83661
• Stored hash:	4e1832956d635ec4e4feba8775a83661
• SHA-1 hash verified	
• Calculated hash:	12db0624b2c740f3b5195761ab86a85730550a45
• Stored hash:	12db0624b2c740f3b5195761ab86a85730550a45

## Drive Geometry

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

The screenshot shows the Autopsy 4.21.0 interface with the 'Listing' tab selected. In the left sidebar, under 'Data Sources', 'Craig Tucker Desktop.E01\_1 Host' is expanded, showing 'vol1 (Unallocated: 0-2047)', 'vol2 (NTFS / exFAT (0x07); 2048-125827071)' (which is highlighted with a red box), and 'vol3 (Unallocated: 125827072-125829119)'. The main pane displays a table with three rows:

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07); 2048-125827071)	2	2048	125825024	NTFS / exFAT (0x07)	Allocated
vol3 (Unallocated: 125827072-125829119)	3	125827072	2048	Unallocated	Unallocated

At the bottom of the main pane, there is a terminal window showing the text: '[aasish@parrot] - [~] u \$'.

## Operating System

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

The screenshot shows the Autopsy 4.21.0 interface with the 'Listing' tab selected. In the left sidebar, under 'Data Sources', 'Craig Tucker Desktop.E01\_1 Host' is expanded, showing 'vol1 (Unallocated: 0-2047)', 'vol2 (NTFS / exFAT (0x07); 2048-125827071)' (highlighted with a red box), and 'vol3 (Unallocated: 125827072-125829119)'. The main pane displays a table with one row:

Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID	Owner
Craig Tucker Desktop.E01					WIN-BK3J6TFMHL	Windows 8.1 Pro	AMD64	%SystemRoot%\TEMP	C:\Windows	00260-00151-37227-AA229 Wind

At the bottom of the main pane, there is a terminal window showing the text: '[aasish@parrot] - [~] u \$'.

Below the table, the 'Operating System Information' section is expanded, showing details:

Type	Value
Name	WIN-BK3J6TFMHL
Program Name	Windows 8.1 Pro
Processor Architecture	AMD64
Temporary Files Direct	%SystemRoot%\TEMP

## Establishing the Time Zone

Now the time zone specifying the location

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

The screenshot shows the Autopsy interface with the 'Windows\System32' folder selected. The 'config' folder is highlighted with a red box. A context menu is open over the 'config' folder, with the 'Extract File(s)' option highlighted in blue. Other options in the menu include 'Open in External Viewer', 'Save As...', 'Export Selected Rows to CSV', 'Add File Tags', 'Add Files to Hash Set', and 'Properties'. The background shows a terminal window with the text '[aasish@parrot] - [~]'.

Now loading the file into the registry explorer

The screenshot shows the Registry Explorer interface with the 'File' menu open. The 'Load hive' option is selected and highlighted in blue. Other options in the 'File' menu include 'Live system', 'Unload all hives', 'Project', 'Export 'Registry hives'', and 'Exit'. The background shows a terminal window with the text '[aasish@parrot] - [~]'.

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

Key name	# values	# subkeys	Last write time
C:\Users\sachi\Desktop\67970-SAM	==	==	2013-08-21
C:\Users\sachi\Desktop\68025-SYSTEM	2	0	2013-08-21
ControlSet001	12	100	2013-12-31
Control	12	100	2013-12-31
ACPI	1	0	2013-08-21
AGP	7	0	2013-08-21
AppID	0	2	2013-08-21
AppReadiness	1	0	2013-08-21
Arbiters	0	3	2013-08-21
BackupRestore	0	3	2013-08-21
BitLocker	0	0	2013-08-21
CI	0	3	2013-08-21
Class	0	79	2013-12-31
CMF	2	4	2013-12-31
CoDeviceInstallers	3	0	2013-08-21
COM Name Arbitrer	1	0	2013-12-31
Compatibility	0	1	2013-08-21
ComputerName	0	1	2013-12-31
ContentIndex	0	1	2013-08-21
CrashControl	8	1	2013-08-21
Cryptography	0	2	2013-08-21
DeviceClasses	0	81	2013-12-31
DeviceContainerPropertyUpdateEvents	0	1	2013-08-21
DeviceContainers	0	19	2013-12-31
DeviceOverrides	0	1	2013-08-21
DevQuery	0	9	2013-08-21
Diagnostics	0	1	2013-08-21
EarlyLaunch	1	0	2013-08-21
Els	0	1	2013-08-21
Errata	1	1	2013-08-21
FastCache	0	0	2013-08-21
FileSystem	0	0	2013-08-21
FilesystemUtilities	0	0	2013-08-21
GraphicsDrivers	0	0	2013-08-21
GroupOrderList	0	0	2013-08-21
HAL	0	0	2013-08-21
Infrared	0	0	2013-08-21

Value Name	Value Data	Value Data Raw
DaylightBias	0;	0
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	00-00-00-00-01-00-02-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
StandardBias	0	0
StandardName	@tzres.dll,-212	@tzres.dll,-212
Base	480	480
DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds.Milliseconds 2:0:0:0	00-00-03-00-02-00-02-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
TimeZoneKeyName	Pacific Standard Time	Pacific Standard Time
ActiveTimeBias	480	480

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	00-00-08-00-01-00-02-00-00-00-00-00-00-00-00-00
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

User	Full Name	Comments
Administrator	Craig Tucker	Administrator for administering the computer domain
Guest		Guest account for guest access to the computer domain
Craig	Craig Tucker	Administrator, users

Here we get three users,

Administrator, Guest and Craig

## Phase - 2

### User's Personal Data

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

#### Desktop section

Craig Tucker Case - Autopsy 4.2.1.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img\_Craig Tucker Desktop.E01/vol\_voi2/Users/Craig/Desktop

Table Thumbnail Summary

Name S C O Modified Time Change Time Access Time Created Time Size Flags(D)

[current folder] 2013-12-22 00:53:18 NPT 2013-12-22 00:53:18 NPT 2013-12-22 00:53:18 NPT 2013-12-21 06:43:42 NPT 56 Allocat

[parent folder] 2013-12-21 06:43:42 NPT 2013-12-21 06:43:42 NPT 2013-12-21 06:43:42 NPT 2013-12-17 23:56:34 NPT 256 Allocat

AWESOME COUPONS.docx 0 2013-12-21 03:28:05 NPT 2013-12-21 03:28:32 NPT 2013-12-21 03:28:25 NPT 2013-12-21 03:28:25 NPT 632320 Allocat

AWESOME COUPONS.docxZone.Identifier 0 2013-12-21 03:28:05 NPT 2013-12-21 03:28:32 NPT 2013-12-21 03:28:25 NPT 2013-12-21 03:28:25 NPT 26 Allocat

desktop.ini 0 2013-12-18 04:56:25 NPT 2013-12-18 04:56:25 NPT 2013-12-18 04:56:25 NPT 2013-12-18 04:56:25 NPT 282 Allocat

MyCoupons.zip 0 2013-12-22 00:53:18 NPT 2013-12-22 00:53:26 NPT 2013-12-22 00:53:17 NPT 2013-12-22 00:53:17 NPT 8057474 Allocat

Pricing Sheet.ttf 0 2013-12-22 00:38:52 NPT 2013-12-22 00:38:52 NPT 2013-12-22 00:38:52 NPT 2013-12-22 00:38:52 NPT 1550 Allocat

Save Table as CSV

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

Strings Extracted Text Translation

Page: 1 of Page Go to Page: Script: Latin - Basic

Here we found some files name coupons

#### Documents>Guides section

Craig Tucker Case - Autopsy 4.2.1.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img\_Craig Tucker Desktop.E01/vol\_voi2/Users/Craig/Documents/Guides

Table Thumbnail Summary

Name S C O Modified Time Change Time Access Time Created Time Size Flags(D)

[current folder] 2013-12-21 03:12:33 NPT 2013-12-21 03:12:33 NPT 2013-12-21 03:12:33 NPT 2013-12-19 01:26:40 NPT 56 Allocat

[parent folder] 2013-12-19 01:26:40 NPT 2013-12-19 01:26:40 NPT 2013-12-19 01:26:40 NPT 2013-12-17 23:56:34 NPT 56 Allocat

6CommandmentsOfCouponMaking.docx 0 2013-12-21 03:12:33 NPT 2013-12-21 03:12:42 NPT 2013-12-21 03:12:33 NPT 2013-12-21 03:12:33 NPT 371041 Allocat

Guide1.png 0 2013-12-18 08:14:05 NPT 2013-12-18 08:15:59 NPT 2013-12-18 08:15:59 NPT 2013-12-18 08:15:59 NPT 396073 Allocat

Guide2.png 0 2013-12-18 08:14:06 NPT 2013-12-18 08:16:09 NPT 2013-12-18 08:16:09 NPT 2013-12-18 08:16:09 NPT 506409 Allocat

HowToMakeCoupons.jpg 0 2013-12-21 03:11:16 NPT 2013-12-21 03:11:39 NPT 2013-12-21 03:11:38 NPT 2013-12-21 03:11:38 NPT 2089397 Allocat

Save Table as CSV

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

HOW TO MAKE COUPONS

Tags Menu

We found some tutorial that explains how to make coupons

## Documents > My Stuff section

The screenshot shows the 'My Stuff' folder structure under 'Documents'. The folder contains numerous image files, many of which are thumbnails. A specific file named 'MANUFACTURER'S COUPON' is highlighted with a red box. This coupon is for \$200 off Beats headphones and includes a barcode.

Here we found tons of coupons

## Next Downloads section:

The screenshot shows the 'Downloads' section. It lists various files, including several zip files related to coupons. A red box highlights the 'Downloads' folder path. The terminal window at the bottom shows a user session on a 'parrot' machine, with the command 'ls' being run.

Here we found zip files all about coupons

## Next SkyDrive>Documents section

The screenshot shows the Autopsy 4.2.1.0 interface. The left sidebar displays the file system structure under the 'Craig' user profile. A red box highlights the 'Documents' folder within the 'SkyDrive' directory. Another red box highlights the entire 'Documents' folder. The main pane shows a table of file metadata. The columns are: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The table lists numerous files, many of which are coupons from 'Hot Pockets'. The bottom right corner of the interface shows a terminal window with a Parrot OS prompt, displaying the command 'ls'.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
1353036325777.jpg	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:50:57 NPT	2012-11-16 11:41:50 NPT	2012-11-16 11:41:50 NPT	140560	Allocated
1353029875863.jpg	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:50:57 NPT	2012-11-16 11:41:50 NPT	2012-11-16 11:41:50 NPT	442	Allocated
1353029875863.jpggms-properties	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:50:57 NPT	2012-11-16 11:41:50 NPT	2012-11-16 11:41:50 NPT	26	Allocated
1353029875863.jpgZone.Identifier	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:50:57 NPT	2012-11-16 11:41:50 NPT	2012-11-16 11:41:50 NPT	26	Allocated
1353036325777.jpg	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:50:58 NPT	2012-11-16 11:55:22 NPT	2012-11-16 11:55:22 NPT	738852	Allocated
1353036325777.jpggms-properties	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:50:58 NPT	2012-11-16 11:55:22 NPT	2012-11-16 11:55:22 NPT	442	Allocated
1353036325777.jpgZone.Identifier	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:50:58 NPT	2012-11-16 11:55:22 NPT	2012-11-16 11:55:22 NPT	26	Allocated
Bacon2.jpg	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:50:59 NPT	2012-11-16 11:57:26 NPT	2012-11-16 11:57:26 NPT	700347	Allocated
Bacon2.jpggms-properties	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:50:59 NPT	2012-11-16 11:57:26 NPT	2012-11-16 11:57:26 NPT	393	Allocated
Bacon2.jpgZone.Identifier	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:50:59 NPT	2012-11-16 11:57:26 NPT	2012-11-16 11:57:26 NPT	26	Allocated
Hot Pockets.jpg	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:50:59 NPT	2012-11-16 11:57:54 NPT	2012-11-16 11:57:54 NPT	622531	Allocated
Hot Pockets.jpggms-properties	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:50:59 NPT	2012-11-16 11:57:54 NPT	2012-11-16 11:57:54 NPT	442	Allocated
Hot Pockets.jpgZone.Identifier	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:50:59 NPT	2012-11-16 11:57:54 NPT	2012-11-16 11:57:54 NPT	26	Allocated
PizzaRolls.jpg	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:51:00 NPT	2012-11-16 11:58:36 NPT	2012-11-16 11:58:36 NPT	630859	Allocated
PizzaRolls.jpggms-properties	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:51:00 NPT	2012-11-16 11:58:36 NPT	2012-11-16 11:58:36 NPT	393	Allocated
PizzaRolls.jpgZone.Identifier	0		v	2013-12-22 00:50:38 NPT	2013-12-22 00:51:00 NPT	2012-11-16 11:58:36 NPT	2012-11-16 11:58:36 NPT	26	Allocated

Again we found a lots of coupons all under User "Criag"

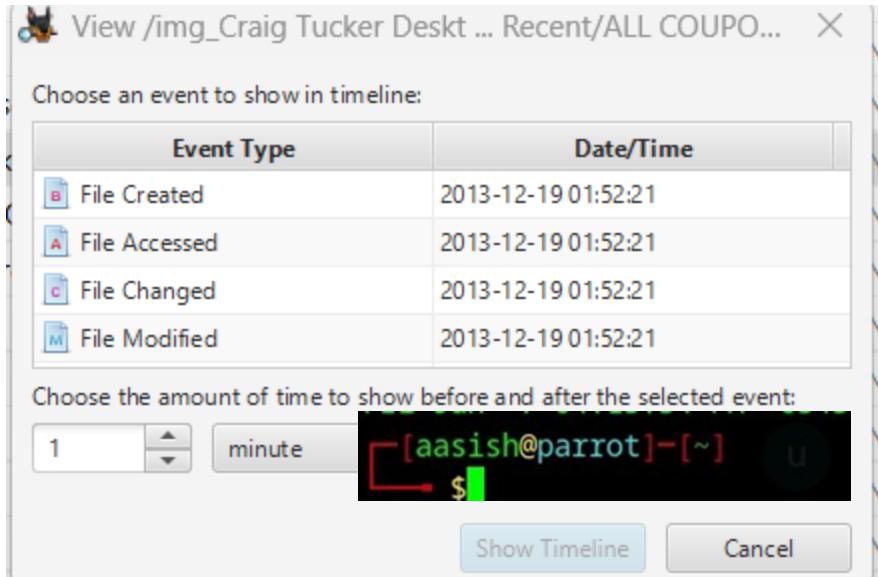
## LNK Files and JumpLists

Link Files:

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

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2013-12-22 01:28:21 NPT	2013-12-22 01:28:21 NPT	2013-12-22 01:28:21 NPT	2013-12-17 23:56:34 NPT	408
[parent folder]				2013-12-18 04:56:25 NPT	2013-12-18 04:56:25 NPT	2013-12-18 04:56:25 NPT	2013-12-17 23:56:34 NPT	56
AutomaticDestinations				2013-12-22 01:27:16 NPT	2013-12-22 01:27:16 NPT	2013-12-18 04:56:25 NPT	2013-12-17 23:56:34 NPT	56
CustomDestinations				2013-12-27 13:28:00 NPT	2013-12-27 13:28:00 NPT	2013-12-27 13:28:00 NPT	2013-12-18 04:56:25 NPT	56
1353033721971.lnk	0			2013-12-19 01:49:22 NPT	2013-12-19 01:49:22 NPT	2013-12-19 01:49:22 NPT	2013-12-19 01:48:45 NPT	2395
1353034600828.lnk	0			2013-12-19 01:48:53 NPT	2013-12-19 01:48:53 NPT	2013-12-19 01:48:53 NPT	2013-12-19 01:48:53 NPT	2395
2000001.lnk	0			2013-12-18 05:17:34 NPT	2013-12-18 05:17:34 NPT	2013-12-18 05:17:34 NPT	2013-12-18 05:16:02 NPT	1929
2000008.lnk	0			2013-12-18 06:31:18 NPT	2013-12-18 06:31:18 NPT	2013-12-18 06:31:18 NPT	2013-12-18 06:30:36 NPT	1929
2000012.lnk	0			2013-12-18 08:16:04 NPT	2013-12-18 08:16:04 NPT	2013-12-18 08:16:04 NPT	2013-12-18 08:14:09 NPT	1929
2000069.lnk	0			2013-12-19 01:49:22 NPT	2013-12-19 01:49:22 NPT	2013-12-19 01:49:22 NPT	2013-12-19 01:48:45 NPT	1929
20000134.lnk	0			2013-12-21 03:11:41 NPT	2013-12-21 03:11:41 NPT	2013-12-21 03:11:41 NPT	2013-12-21 03:11:22 NPT	1929
20000135.lnk	0			2013-12-21 03:28:07 NPT	2013-12-21 03:28:07 NPT	2013-12-21 03:28:07 NPT	2013-12-21 03:28:07 NPT	1929
20000196.lnk	0			2013-12-21 06:59:07 NPT	2013-12-21 06:59:07 NPT	2013-12-21 06:59:07 NPT	2013-12-21 06:59:07 NPT	1929
6CommandmentsofCouponMaking.lnk	0			2013-12-21 03:12:33 NPT	2013-12-21 03:12:33 NPT	2013-12-21 03:12:33 NPT	2013-12-21 03:11:41 NPT	3309
ALL COUPONS.lnk	0			2013-12-19 01:52:21 NPT	2013-12-19 01:52:21 NPT	2013-12-19 01:52:21 NPT	2013-12-19 01:52:21 NPT	617
AWESOME COUPONS.lnk	0			2013-12-21 03:28:33 NPT	2013-12-21 03:28:33 NPT	2013-12-21 03:28:33 NPT	2013-12-21 03:28:33 NPT	563

Type	Value	Source(s)
Path	C:\Users\Craig\Downloads\ALL COUPONS.rar	RecentActivity
Path ID	11053	RecentActivity
Date Accessed	2013-12-19 01:52:21 NPT	RecentActivity
Source File Path	/img_Craig Tucker Desktop.E01/vol_vol2/Users/Craig/AppData/Roaming/Microsoft/Windows/Recent/ALL COUPONS.lnk	
Artifact ID	-922372036854775783	



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

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
20000196.lnk				2013-12-21 06:59:07 NPT	2013-12-21 06:59:07 NPT	2013-12-21 06:59:07 NPT	2013-12-21 06:59:07 NPT	1929
6CommandmentsofCouponMaking.lnk								
ALL COUPONS.lnk								
<b>AWESOME COUPONS.lnk</b>								
Biology and Aggression.lnk								
Cheetos.lnk								
Coca-Cola.lnk								
Coupons (2).lnk								
Coupons.lnk								
Coupons1.lnk								
desktop.ini								
Dinosaur Extinction.lnk								
Downloads.lnk								
GiftCards.lnk								
Guide1.lnk								
Guide2.lnk								

Craig Accessing the Awsome coupons.lnk files timestamp

Name	C	C	O	Modified Time	Change Time	Access Time	Created Time	Si.
20000001.Ink				View /img_Craig Tucker Deskt ... entsofCouponMaki...				
20000008.Ink								
20000012.Ink								
20000069.Ink								
20000134.Ink								
20000135.Ink								
20000196.Ink								
6Commandments								
ALL COUPONS.Ink								
AWESOME COUPON								
Biology and Aggression.Ink								
Cheetos.Ink								
Coca- Cola.Ink								
Coupons (2).Ink								
Coupons.Ink								
Coupons1.Ink								

## Jumplists

Now jumplists

Craig Tucker Case - Autopsy 4.2.1.0								
Case View Tools Window Help								
Timeline Discovery Generate Report Close Case								
Listing								
<a href="#">/img_Craig Tucker Desktop.E01/vol_vol2/Users/Craig/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations</a>								
Table: <a href="#">Thumbnail</a> <a href="#">Summary</a>								
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2013-12-22 01:27:16 NPT	2013-12-22 01:27:16 NPT	2013-12-18 04:56:25 NPT	2013-12-18 04:56:25 NPT	56
(parent folder)				2013-12-22 01:28:21 NPT	2013-12-22 01:28:21 NPT	2013-12-22 01:28:21 NPT	2013-12-17 23:56:34 NPT	408
28c8b06d6eab549a1.automaticDestinations-ms	0			2013-12-18 05:27:05 NPT	2013-12-18 05:27:05 NPT	2013-12-18 05:27:05 NPT	2013-12-18 05:27:05 NPT	2560
46964a7982cea4d4.automaticDestinations-ms	0			2013-12-22 00:38:53 NPT	2013-12-22 00:38:53 NPT	2013-12-19 01:27:59 NPT	2013-12-19 01:27:59 NPT	36864
46f433176bcb63d2.automaticDestinations-ms	0			2013-12-19 01:52:21 NPT	2013-12-19 01:52:21 NPT	2013-12-19 01:52:21 NPT	2013-12-19 01:52:21 NPT	3072
4cb9c5750d51cd7.automaticDestinations-ms	0			2013-12-22 01:28:21 NPT	2013-12-22 01:28:21 NPT	2013-12-22 01:27:16 NPT	2013-12-22 01:27:16 NPT	5632
7e4dc480246863e3.automaticDestinations-ms	0			2013-12-27 13:18:52 NPT	2013-12-27 13:18:52 NPT	2013-12-19 01:52:21 NPT	2013-12-19 01:52:21 NPT	8192
c953399be1308d73.automaticDestinations-ms	0			2013-12-22 01:18:10 NPT	2013-12-22 01:18:10 NPT	2013-12-18 05:16:02 NPT	2013-12-18 05:16:02 NPT	76808
db53b23f1ebd046.automaticDestinations-ms	0			2013-12-22 00:53:26 NPT	2013-12-22 00:53:26 NPT	2013-12-22 00:53:26 NPT	2013-12-22 00:53:26 NPT	3072
f01b4d95c155d32a.automaticDestinations-ms	0			2013-12-22 01:27:16 NPT	2013-12-22 01:27:16 NPT	2013-12-18 04:56:25 NPT	2013-12-18 04:56:25 NPT	46080

## Extracting the jumpelist files

Craig Tucker Case - Autopsy 4.2.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img,Craig Tucker Desktop E01/vol\_voi2/Users/Craig/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations 10 Results

Table Thumbnail Summary Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	File	
[current folder]				2013-12-22 01:27:16 NPT	2013-12-22 01:27:16 NPT	2013-12-18 04:56:25 NPT	2013-12-18 04:56:25 NPT	56	All	
[parent folder]				2013-12-22 01:28:21 NPT	2013-12-22 01:28:21 NPT	2013-12-22 01:28:21 NPT	2013-12-17 23:56:34 NPT	408	All	
28c8b86deab549a1.automaticDestinations-ms	0			2013-12-18 05:27:05 NPT	2013-12-18 05:27:05 NPT	2013-12-18 05:27:05 NPT	2013-12-18 05:27:05 NPT	2560	All	
409ea7a982cead44.automaticDestinations-ms	0			2013-12-22 00:38:53 NPT	2013-12-22 00:38:53 NPT	2013-12-19 01:27:59 NPT	2013-12-19 01:27:59 NPT	36864	All	
46f433176b0b3d2.automaticDestinations-ms	0			2013-12-19 01:52:21 NPT	2013-12-19 01:52:21 NPT	2013-12-19 01:52:21 NPT	2013-12-19 01:52:21 NPT	3072	All	
4cb9c5750d51c07.automaticDestinations-ms	0			2013-12-22 01:28:21 NPT	2013-12-22 01:28:21 NPT	2013-12-22 01:27:16 NPT	2013-12-22 01:27:16 NPT	5632	All	
7e4dcab0246863e3.automaticDestinations-ms				Open in External Viewer Ctrl+E	3:18:52 NPT	2013-12-27 13:18:52 NPT	2013-12-18 04:57:26 NPT	2013-12-18 04:57:26 NPT	8192	All
c953399be130bd73.automaticDestinations-ms				Extract File(s)	11:18:10 NPT	2013-12-22 01:18:10 NPT	2013-12-18 05:16:02 NPT	2013-12-18 05:16:02 NPT	7688	All
db53b231fd1edbd46.automaticDestinations-ms				Export Selected Rows to CSV	10:53:26 NPT	2013-12-22 00:53:26 NPT	2013-12-22 00:53:26 NPT	2013-12-22 00:53:26 NPT	3072	All
f01b4d95c155d32a.automaticDestinations-ms				Add File Tags	>					
				Add Files to Hash Set	>					
				Properties						

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

## Opening into Jumplister

Here one of the file directs E:\Russian Videos

Jumplister

File Tools Help

File Name Application

10718-28c8b86deab549a1.automaticDestinations-ms	Common Network Relative Link (Flags)
10720-469ea7a982cead44.automaticDestinations-ms	Common Network Relative Link (Device Name)
10721-46f433176b0b3d2.automaticDestinations-ms	Common Network Relative Link (Net Name)
10723-4cb9c5750d51c07.automaticDestinations-ms	Common Network Relative Link (Network Provider Type)
10725-7e4dcab0246863e3.automaticDestinations-ms	Common Path Suffix
10726-c953399be130bd73.automaticDestinations-ms	Local Base Path
10728-db53b231fd1edbd46.automaticDestinations-ms	Working Path
10730-f01b4d95c155d32a.automaticDestinations-ms	Arguments

Root

- 10: 395 bytes
- 1C: 362 bytes
- 1B: 498 bytes
- 18: 334 bytes
- 1: 443 bytes
- 9: 532 bytes
- 8: 537 bytes
- D: 2010 bytes
- 19: 1696 bytes
- C: 362 bytes
- 17: 1696 bytes
- 16: 2010 bytes
- 15: 1696 bytes
- 14: 2059 bytes
- 13: 2005 bytes
- 12: 406 bytes
- 11: 1696 bytes
- 8: 1696 bytes
- 6: 2022 bytes
- 7: 1696 bytes
- 5: 1696 bytes
- 4: 440 bytes
- 3: 439 bytes
- 2: 442 bytes
- DestList (7128 bytes)

Name Value

Common Network Relative Link (Flags)	
Common Network Relative Link (Device Name)	
Common Network Relative Link (Net Name)	
Common Network Relative Link (Network Provider Type)	
Common Path Suffix	
Local Base Path	E:\Russian Videos
Working Path	
Arguments	
Flags	
Attributes	
Show Command	
Created Timestamp	Saturday, December 21, 2013 7:40:01 PM
Accessed Timestamp	Saturday, December 21, 2013 8:00:00 AM
Modified Timestamp	Saturday, December 21, 2013 7:40:02 PM
Drive Type	Removable
Serial No.	-173/4/6168
Volume Name	STUFF

Volume/D and Local Base Path

Directory

Normal

Saturday, December 21, 2013 7:40:01 PM

Saturday, December 21, 2013 8:00:00 AM

Saturday, December 21, 2013 7:40:02 PM

Removable

-173/4/6168

STUFF

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

JumpLister

File Tools Help

File Name Application

10718-28c8b86deab549a1.automaticDestinations-ms	Name	Value
10720-469e4a7982cea4d4.automaticDestinations-ms	Common Network Relative Link (Flags)	
10721-464433178bc0b3d2.automaticDestinations-ms	Common Network Relative Link (Device Name)	
10723-4c9c5750d51c07.automaticDestinations-ms	Common Network Relative Link (Net Name)	
10725-7edca80246863e3.automaticDestinations-ms	Common Network Relative Link (Network Provider Type)	
10726-c9533998e1308673.automaticDestinations-ms	Common Path Suffix	
10728-db53b23d1edb4d6.automaticDestinations-ms	Local Base Path	C:\Users\Craig\Desktop\MyCoupons.zip
10730-f01b4d95cf55d32a.automaticDestinations-ms	Working Path	
	Arguments	
	Flags	VolumeIDAndLocalBasePath
	Attributes	Archive
	Show Command	Normal
	Created Timestamp	Saturday, December 21, 2013 7:08:17 PM
	Accessed Timestamp	Saturday, December 21, 2013 7:08:17 PM
	Modified Timestamp	Saturday, December 21, 2013 7:08:18 PM
	Drive Type	Fixed
	Serial No.	1653949602
	Volume Name	win-bk3j6tflmhll
	Machine ID	9f96d07c-6c0a-4d1a-bd86-969c6914f40a
	New Volume ID	1d44c63a-6a6e-11e3-8254-000c29d6ef92
	New Object ID	Saturday, December 21, 2013 6:31:32 PM
	New Object ID (Timestamp)	00:0c:29:d6cef92
	New Object ID (MAC)	33364
	New Object ID (Seq No.)	9f96d07c-6c0a-4d1a-bd86-969c6914f40a
	Birth Volume ID	1d44c63a-6a6e-11e3-8254-000c29d6ef92
	Birth Object ID	Saturday, December 21, 2013 6:31:32 PM
	Birth Object ID (Timestamp)	00:0c:29:d6cef92

Root

- 1: 478 bytes
- DestList (218 bytes)

JumpLister

File Tools Help

File Name Application

10718-28c8b86deab549a1.automaticDestinations-ms	Name	Value
10720-469e4a7982cea4d4.automaticDestinations-ms	Common Network Relative Link (Net Name)	
10721-464433178bc0b3d2.automaticDestinations-ms	Common Network Relative Link (Network Provider Type)	
10723-4c9c5750d51c07.automaticDestinations-ms	Common Path Suffix	
10725-7edca80246863e3.automaticDestinations-ms	Local Base Path	C:\Users\Craig\Pictures\Underage_loita_r@ygold_002.jpg
10726-c9533998e1308673.automaticDestinations-ms	Working Path	
10728-db53b23d1edb4d6.automaticDestinations-ms	Arguments	
10730-f01b4d95cf55d32a.automaticDestinations-ms	Flags	VolumeIDAndLocalBasePath
	Attributes	Archive
	Show Command	Normal
	Created Timestamp	Saturday, December 21, 2013 7:32:57 PM
	Accessed Timestamp	Saturday, December 21, 2013 7:32:57 PM
	Modified Timestamp	Saturday, December 21, 2013 5:56:30 AM
	Drive Type	Fixed
	Serial No.	1653949602
	Volume Name	win-bk3j6tflmhll
	Machine ID	9f96d07c-6c0a-4d1a-bd86-969c6914f40a
	New Volume ID	1d44c694-6a6e-11e3-8254-000c29d6ef92
	New Object ID	Saturday, December 21, 2013 6:31:32 PM
	New Object ID (Timestamp)	00:0c:29:d6cef92
	New Object ID (MAC)	33364
	New Object ID (Seq No.)	9f96d07c-6c0a-4d1a-bd86-969c6914f40a
	Birth Volume ID	1d44c694-6a6e-11e3-8254-000c29d6ef92
	Birth Object ID	Saturday, December 21, 2013 6:31:32 PM
	Birth Object ID (Timestamp)	00:0c:29:d6cef92
	Birth Object ID (MAC)	33364
	Birth Object ID (Seq No.)	33364

Root

- 1F: 2311 bytes
- 1E: 2311 bytes
- 1D: 617 bytes
- 1C: 617 bytes
- 1B: 1884 bytes
- 19: 550 bytes
- 1A: 585 bytes
- 1B: 550 bytes
- 17: 550 bytes
- 16: 3216 bytes
- 15: 1913 bytes
- 14: 561 bytes
- C: 550 bytes
- 13: 3273 bytes
- 12: 3273 bytes
- 11: 3258 bytes
- 10: 2166 bytes
- D: 1904 bytes
- F: 1904 bytes
- E: 1904 bytes
- B: 606 bytes
- A: 1881 bytes
- 9: 1881 bytes
- 8: 3270 bytes
- 7: 1889 bytes
- 6: 1892 bytes
- 5: 1892 bytes
- 4: 3368 bytes

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

JumpLister

File Tools Help

File Name	Application
10718-28c8b86deab549a1.automaticDestinations-ms	
10720-469e4a7902cea4d4.automaticDestinations-ms	
10721-46433176bc0b3d2.automaticDestinations-ms	
10723-4c99c575051c07.automaticDestinations-ms	
10725-7edca80246863e3.automaticDestinations-ms	
10726-c933998a1308d73.automaticDestinations-ms	
10728-db53b23f1edb4d6.automaticDestinations-ms	
10730-f01b4d95cf55d32a.automaticDestinations-ms	

Root

- 2: 2279 bytes
- 1: 637 bytes
- DestList (456 bytes)

Name	Value
Common Network Relative Link (Flags)	
Common Network Relative Link (Device Name)	
Common Network Relative Link (Net Name)	
Common Network Relative Link (Network Provider Type)	
Common Path Suffix	
Local Base Path	
Working Path	
Arguments	C:\User\Craig\Videos\underage daughter R@ygold.wmv
Flags	
Attributes	
Show Command	
Created Timestamp	Saturday, December 21, 2013 7:43:02 PM
Accessed Timestamp	Saturday, December 21, 2013 7:43:02 PM
Modified Timestamp	Monday, December 2, 2013 5:00:54 AM
Drive Type	Fixed
Serial No.	1653949602
Volume Name	win-bk3j6fmhll
Machine ID	9f96d07c-6c0a-4d1a-bd86-969c6914f40a
New Volume ID	1d44c7ae-6a6e-11e3-8254-000c29d6ef92
New Object ID	Saturday, December 21, 2013 6:31:32 PM
New Object ID (Timestamp)	00:0c:29:d6:ef:92
New Object ID (MAC)	33364
New Object ID (Seq No.)	9f96d07c-6c0a-4d1a-bd86-969c6914f40a
Birth Volume ID	1d44c7ae-6a6e-11e3-8254-000c29d6ef92
Birth Object ID	Saturday, December 21, 2013 6:31:32 PM
Birth Object ID (Timestamp)	00:0c:29:d6:ef:92
Birth Object ID (MAC)	33364
Birth Object ID (Seq No.)	

## Next metadata about the ALL COUPNS.rar file

JumpLister

File Tools Help

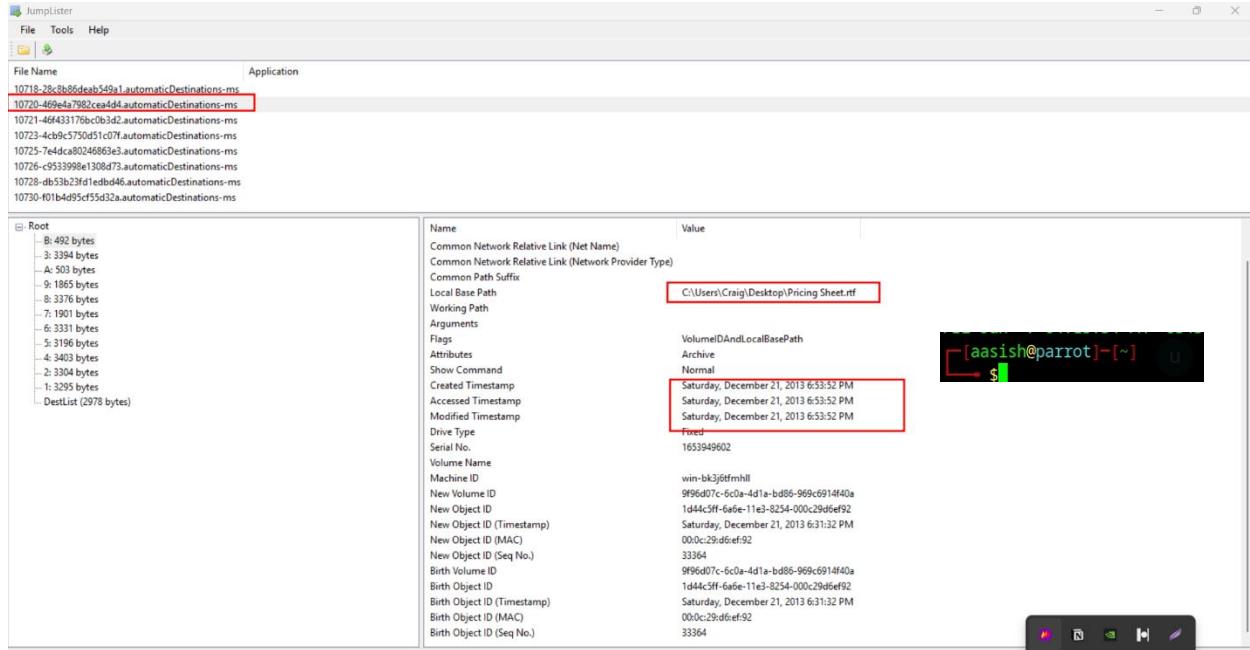
File Name	Application
10718-28c8b86deab549a1.automaticDestinations-ms	
10720-469e4a7902cea4d4.automaticDestinations-ms	
10721-46433176bc0b3d2.automaticDestinations-ms	
10723-4c99c575051c07.automaticDestinations-ms	
10725-7edca80246863e3.automaticDestinations-ms	
10726-c933998a1308d73.automaticDestinations-ms	
10728-db53b23f1edb4d6.automaticDestinations-ms	
10730-f01b4d95cf55d32a.automaticDestinations-ms	

Root

- 1: 556 bytes
- DestList (226 bytes)

Name	Value
Common Network Relative Link (Net Name)	
Common Network Relative Link (Network Provider Type)	
Common Path Suffix	
Local Base Path	
Working Path	
Arguments	C:\Users\Craig\Downloads\ALL COUPONS.rar
Flags	
Attributes	
Show Command	
Created Timestamp	Wednesday, December 18, 2013 8:05:57 PM
Accessed Timestamp	Wednesday, December 18, 2013 8:05:57 PM
Modified Timestamp	Wednesday, December 18, 2013 8:06:27 PM
Drive Type	Fixed
Serial No.	1653949602
Volume Name	win-bk3j6fmhll
Machine ID	9f96d07c-6c0a-4d1a-bd86-969c6914f40a
New Volume ID	1d5f061-681c-11e3-824f-000c29d6ef92
New Object ID	Wednesday, December 18, 2013 7:39:20 PM
New Object ID (Timestamp)	00:0c:29:d6:ef:92
New Object ID (MAC)	33359
New Object ID (Seq No.)	9f96d07c-6c0a-4d1a-bd86-969c6914f40a
Birth Volume ID	1d5f061-681c-11e3-824f-000c29d6ef92
Birth Object ID	Wednesday, December 18, 2013 7:39:20 PM
Birth Object ID (Timestamp)	00:0c:29:d6:ef:92
Birth Object ID (MAC)	33359
Birth Object ID (Seq No.)	

## Next Pricing sheet of the coupons



# Recycle Bin

## Next Recycle bin

Craig Tucker Case - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /Img\_Craig Tucker Desktop.E01/vol\_voi2/\$Recycle.Bin/S-1-5-21-1049150138-4017234595-3791460656-1001

Table Thumbnail Summary Save Table as CSV

9 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
[current folder]				2013-12-27 14:30:34 NPT	2013-12-27 14:30:34 NPT	2013-12-18 04:57:05 NPT	2013-12-18 04:57:05 NPT	56	Allocated	Allocated
[parent folder]				2013-12-18 04:57:05 NPT	2013-12-18 04:57:05 NPT	2013-12-18 04:57:05 NPT	2013-08-22 21:21:31 NPT	328	Allocated	Allocated
\$18MF65.jpg	0			2013-12-27 13:12:06 NPT	2013-12-27 13:12:06 NPT	2013-12-27 13:12:06 NPT	2013-12-27 13:12:06 NPT	544	Allocated	Allocated
\$1GOWXSL.jpg	0			2013-12-27 13:12:09 NPT	2013-12-27 13:12:09 NPT	2013-12-27 13:12:09 NPT	2013-12-27 13:12:09 NPT	544	Allocated	Allocated
\$1VWUORQ.wmv	0			2013-12-27 14:30:34 NPT	2013-12-27 14:30:34 NPT	2013-12-27 14:30:34 NPT	2013-12-27 14:30:34 NPT	544	Allocated	Allocated
\$R8MF65.jpg	0			2013-12-21 11:35:16 NPT	2013-12-27 13:12:06 NPT	2013-12-22 01:17:57 NPT	2013-12-22 01:17:57 NPT	562101	Allocated	Allocated
\$RGOWXSL.jpg	0			2013-12-21 11:41:03 NPT	2013-12-27 13:12:09 NPT	2013-12-22 01:17:57 NPT	2013-12-22 01:17:57 NPT	626337	Allocated	Allocated
\$RVWUORQ.wmv	0			2013-12-02 10:45:54 NPT	2013-12-27 14:30:34 NPT	2013-12-22 01:28:02 NPT	2013-12-22 01:28:02 NPT	8076724	Allocated	Allocated

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

Tags Menu

File Views File Types Deleted Files MB File Size Data Artifacts Chromium Profiles (1) Communication Accounts (2) Installed Programs (64) Operating System Information (1) Recent Documents (106) Recycle Bin (3) Run Programs (1417) Shell Bags (77) USB Device Attached (28) Web Bookmarks (1)

File Views File Types Deleted Files MB File Size Data Artifacts Chromium Profiles (1) Communication Accounts (2) Installed Programs (64) Operating System Information (1) Recent Documents (106) Recycle Bin (3) Run Programs (1417) Shell Bags (77) USB Device Attached (28) Web Bookmarks (1)

Craig Tucker Case - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /Img\_Craig Tucker Desktop.E01/vol\_voi2/\$Recycle.Bin/S-1-5-21-1049150138-4017234595-3791460656-1001

Table Thumbnail Summary Save Table as CSV

9 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
[current folder]				2013-12-27 14:30:34 NPT	2013-12-27 14:30:34 NPT	2013-12-18 04:57:05 NPT	2013-12-18 04:57:05 NPT	56	Allocated	Allocated
[parent folder]				2013-12-18 04:57:05 NPT	2013-12-18 04:57:05 NPT	2013-12-18 04:57:05 NPT	2013-08-22 21:21:31 NPT	328	Allocated	Allocated
\$18MF65.jpg	0			2013-12-27 13:12:06 NPT	2013-12-27 13:12:06 NPT	2013-12-27 13:12:06 NPT	2013-12-27 13:12:06 NPT	544	Allocated	Allocated
\$1GOWXSL.jpg	0			2013-12-27 13:12:09 NPT	2013-12-27 13:12:09 NPT	2013-12-27 13:12:09 NPT	2013-12-27 13:12:09 NPT	544	Allocated	Allocated
\$1VWUORQ.wmv	0			2013-12-27 14:30:34 NPT	2013-12-27 14:30:34 NPT	2013-12-27 14:30:34 NPT	2013-12-27 14:30:34 NPT	544	Allocated	Allocated
\$R8MF65.jpg	0			2013-12-21 11:35:16 NPT	2013-12-27 13:12:06 NPT	2013-12-22 01:17:57 NPT	2013-12-22 01:17:57 NPT	562101	Allocated	Allocated
\$RGOWXSL.jpg	0			2013-12-21 11:41:03 NPT	2013-12-27 13:12:09 NPT	2013-12-22 01:17:57 NPT	2013-12-22 01:17:57 NPT	626337	Allocated	Allocated
\$RVWUORQ.wmv	0			2013-12-02 10:45:54 NPT	2013-12-27 14:30:34 NPT	2013-12-22 01:28:02 NPT	2013-12-22 01:28:02 NPT	8076724	Allocated	Allocated

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

Tags Menu

File Views File Types Deleted Files MB File Size Data Artifacts Chromium Profiles (1) Communication Accounts (2) Installed Programs (64) Operating System Information (1) Recent Documents (106) Recycle Bin (3) Run Programs (1417) Shell Bags (77) USB Device Attached (28) Web Bookmarks (1)

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

Timestamp	Manufacturer	Title	Version	Serial Number	Device Name	Disk Id	Installed	First Installed	Last Connected	Last Removed	
2013-12-18 19:41:02	Ven_Kington	Prod_DT_100_G2	Rev_JMAP	000FEEFB938ECC027E200F6A0	Western Digital WD Blue DT 100 G2	E200F6A0	000f6eeb938eccc027e200f6a0	2013-12-18 19:41:02	2013-12-18 19:41:02	2013-12-21 21:23:14	2013-12-21 21:32:25

## Email-Review

Next up looking for emails

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]				2013-12-27 13:35:21 NPT	2013-12-27 13:35:21 NPT	2013-12-27 13:35:21 NPT	2013-12-18 05:15:22 NPT	320	Allocated
[parent folder]				2013-12-22 01:35:07 NPT	2013-12-22 01:35:07 NPT	2013-12-22 01:35:07 NPT	2013-12-18 05:10:59 NPT	672	Allocated
20000262_40273a2c5cafaeml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	3925	Allocated
20000263_27bc5c58876ea.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	8077	Allocated
20000264_4f89107a737c.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	10474	Allocated
20000265_7b6cafc2e66fe9.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2562	Allocated
20000266_23c7530c78545.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	20892	Allocated
20000267_acb9030ff9ca78.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	37959	Allocated

This indicates the usage of coupons

Craig Tucker Case - Autopsy 4.21.0

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

**Listing** /img\_Craig Tucker Desktop.E01.vol\_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps\_8wekyb3d8bbwe/LocalState/Indexed/LiveComm/ba871ed4e8a350e0/120712-0

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
2000026c_b059b7daa5989d.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	30349	Allocated
2000026d_de67ef1dd7f3e4.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	27544	Allocated
2000026e_5823b3d0bf72210.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	18924	Allocated
2000026f_5e7a78519b17b6.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2299	Allocated
20000270_92c3b9fb3fbfec.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	10136	Allocated
20000271_9632a9bf281.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	1803	Allocated
20000272_2a6c5c84990623.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	7039	Allocated
20000273_a271b0c1fcfa7.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	28546	Allocated

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

Page: 1 of - Page Matches on page: - of - Match 100%   Reset Text Source: File Text

Hey craig! I know its last minute but I need a paper for my class fast! Something on dinosaurs or extinction or whatev, I just need it. Im low on \$ but I heard u were on 4chan, so I'll hook u up w/ sum coupons. HELP ME OUT MAN!

-----METADATA-----

```

Author: Kenny McCormick <kenny.mccormick28@outlook.com>
Content-Type: message/rfc822
Creation-Date: 2013-18T19:34:09Z
Message-From: Kenny McCormick <kenny.mccormick28@outlook.com>
Message-To: Coupon-King<coupon-king@outlook.com>
Message-From-Email: kenny.mccormick28@outlook.com
Message-From-Name: Kenny McCormick
Message-Raw-Header-Importance: Normal
Message-Raw-Header-MIME-Version: 1.0
Multipart-Boundary: 444C4341-CSD1-1048-A204-D4822919001B
Multipart-Subtype: alternative
Y_Parser:Bur runn smarthka nancr DfauitPancar

```

[aasish@parrot] - [~]

This indicates Kenny McCormick is asking for some coupons

Craig Tucker Case - Autopsy 4.21.0

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

**Listing** /img\_Craig Tucker Desktop.E01.vol\_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps\_8wekyb3d8bbwe/LocalState/Indexed/LiveComm/ba871ed4e8a350e0/120712-0

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
20000266_23c7530c78545.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	20892	Allocated
20000267_acb9030f9ca78.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	37959	Allocated
20000268_ae563a9b896661.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	6888	Allocated
20000269_54b60c4eba7b0.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	12416	Allocated
2000026a_ef1f741d6c38.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2096	Allocated
2000026b_2ecab5bda475.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	3494	Allocated
2000026c_b059b7daa5989d.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	30349	Allocated
2000026d_de67ef1dd7f3e4.eml	0			2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	27544	Allocated

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

Page: 1 of - Page Matches on page: - of - Match 100%   Reset Text Source: File Text

K so Craig, go 2 "r4chan." this is the rapid share and in the search bar type coupon, just download a few rar or zip files and u will b set :)

-----METADATA-----

```

Author: Stan Marsh <stan.marsh27@yahoo.com>
Content-Type: message/rfc822
Creation-Date: 2013-18T02:57:52Z
Message-From: Stan Marsh <stan.marsh27@yahoo.com>
Message-To: Coupon-King<coupon-king@outlook.com>
Message-From-Email: stan.marsh27@yahoo.com
Message-From-Name: Stan Marsh
Message-Raw-Header-Importance: Normal
Message-Raw-Header-MIME-Version: 1.0

```

[aasish@parrot] - [~]

Craig Tucker Case - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img\_Craig Tucker Desktop.E01/vol\_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps\_bwekyb3d8bbwe/LocalState/Indexed/LiveComm/ba871ed4ea350e0/120712-0

Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
20000266_23c7530c78545.eml	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	20892	Allocated
20000267_act9030f9ca78.eml	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	37959	Allocated
20000268_be563a49b896d6.eml	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	6688	Allocated
20000269_b5460e4c9eba7b.eml	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	12416	Allocated
2000026a_f7d741dcf38.eml	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2096	Allocated
2000026b_2ecab05dab475.eml	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	34944	Allocated
2000026c_b05967da5989d.eml	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	30349	Allocated
2000026d_de67ef1ddf73e4.eml	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	27544	Allocated

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

Strings Extracted Text Translation

Page: 1 of - Page Matches on page: - of - Match 100% ⌂ ⌂ Reset Text Source: File Text

Well here's 2 guides on couponing and go download google chrome. it's better than internet explorer. BTW dude I told u not 2 get windows 8 but u just had to be a newb and get it.

On Tue, Dec 17, 2013 at 4:57 PM, Craig Tucker <coupon-king@outlook.com> wrote:

[aashish@parrot] ~

Hey thx man. I'm better w/ the coupons and 4chan but I HATE windows 8 and internet explorer! I want my stupid start button back!

Sent from Windows Mail

## Next Criag Mailed about he is good at coupns

Craig Tucker Case - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img\_Craig Tucker Desktop.E01/vol\_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps\_bwekyb3d8bbwe/LocalState/Indexed/LiveComm/ba871ed4ea350e0/120712-0

Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]				2013-12-27 13:35:21 NPT	2013-12-27 13:35:21 NPT	2013-12-27 13:35:21 NPT	2013-12-18 05:15:22 NPT	320	Allocated
[parent folder]				2013-12-22 01:35:07 NPT	2013-12-22 01:35:07 NPT	2013-12-22 01:35:07 NPT	2013-12-18 05:10:59 NPT	672	Allocated
b0000262_40273a2c6caa.eml	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	3925	Allocated
b0000263_272bcd5e88b6e.eml	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	8077	Allocated
b0000264_4f7891072a737.eml	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	10474	Allocated
<b>b0000265_7b6caf2ee6fe9.eml</b>	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2562	Allocated
b0000266_23c7530c78545.eml	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	20892	Allocated
b0000267_act9030f9ca78.eml	0	0	0	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	2013-12-27 13:35:24 NPT	37959	Allocated

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

Strings Extracted Text Translation

Page: 1 of - Page Matches on page: - of - Match 100% ⌂ ⌂ Reset Text Source: File Text

Hey Craig. I heard u were on 4chan. I got stuff at CVS w/ coupons from there. Check out my receipts and BTW here's a coupon 4 a nintendo DS.

[aashish@parrot] ~

-----METADATA-----

Author: Kyle Broflovski <kyle.broflovski29@gmail.com>  
Content-Type: message/rfc822  
Creation-Date: 2013-12-18T00:36:07Z  
Message-From: Kyle Broflovski <kyle.broflovski29@gmail.com>

## Next Kyle Broflovvski mailed about coupons dealing

# Internet History

Let's explore internet history

First lets open google hive

The screenshot shows the Autopsy 4.2.1 interface with the 'Google' case open. The left sidebar lists various file types and their counts. The main pane displays a table of artifacts under the 'History' category. The table includes columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags/Dir. Several rows are highlighted with red boxes, including 'Cookies', 'History', and 'Default'. A detailed view of the 'Default' folder is shown below, listing sub-folders like Cache, Extension Rules, and Session Storage. At the bottom, a key-value pair 'version: 6' is displayed.

And next to internet explorer

The screenshot shows the Autopsy 4.2.1 interface with the 'Microsoft' case open. The left sidebar lists various file types and their counts. The main pane displays a table of artifacts under the 'Windows' category. The table includes columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags/Dir. Several rows are highlighted with red boxes, including 'History', 'IECompatCache', 'INetCookies', and 'Temporary Internet Files'. A detailed view of the 'Temporary Internet Files' folder is shown below, listing sub-folders like 1033, Application Shortcuts, and Themes. At the bottom, a key-value pair 'version: 6' is displayed.

## Next SQLite view

For google chrome

The screenshot shows the Autopsy 4.2.1 interface with a search result for 'History' in the 'Google Chrome/User Data/Default' folder. The results table displays the following columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The first two rows are highlighted in red:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Archived History-journal	0			2013-12-18 08:12:09 NPT	2013-12-18 08:12:09 NPT	2013-12-18 08:12:09 NPT	2013-12-18 08:12:09 NPT	512	Allocated
Cookies	0			2013-12-27 13:28:00 NPT	2013-12-27 13:28:00 NPT	2013-12-18 08:12:09 NPT	2013-12-18 08:12:09 NPT	70656	Allocated

Here the coupons zip files are downloaded

The screenshot shows the Autopsy 4.2.1 interface with a search result for 'Cookies' in the 'Google Chrome/User Data/Default' folder. The results table displays the following columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The first three rows are highlighted in red:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Archived History-journal	0			2013-12-18 08:12:09 NPT	2013-12-18 08:12:09 NPT	2013-12-18 08:12:09 NPT	2013-12-18 08:12:09 NPT	512	Allocated
Cookies	0			2013-12-27 13:28:00 NPT	2013-12-27 13:28:00 NPT	2013-12-18 08:12:09 NPT	2013-12-18 08:12:09 NPT	70656	Allocated
Cookie-journal	0			2013-12-27 13:28:00 NPT	2013-12-27 13:28:00 NPT	2013-12-18 08:12:09 NPT	2013-12-18 08:12:09 NPT	16384	Allocated

Here the pubmatic.com is pretty suspicious having the name KRTBCOKIE\_27

## Hidden or Encrypted Data

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

Craig Tucker Case - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Directory Tree

Listing /Img.Craig Tucker Desktop.E01/vol.vol2/Users/Craig/Desktop

Table Thumbnail Summary Save Table as CSV

Name S C O Modified Time Change Time Access Time Created Time Size File

[current folder] 2013-12-22 0053:18 NPT 2013-12-22 0053:18 NPT 2013-12-21 06:43:42 NPT 2013-12-17 23:56:34 NPT 56 AI

[parent folder] 2013-12-21 06:43:42 NPT 2013-12-21 06:43:42 NPT 2013-12-21 06:43:42 NPT 2013-12-17 23:56:34 NPT 256 AI

AWESOME COUPONS.docx 12-21 03:28:05 NPT 2013-12-21 03:28:32 NPT 2013-12-21 03:28:25 NPT 2013-12-21 03:28:25 NPT 632320 AI

AWESOME COUPONS.docx 12-18 04:56:25 NPT 2013-12-18 04:56:25 NPT 2013-12-18 04:56:25 NPT 2013-12-18 04:56:25 NPT 26 AI

desktop.ini Extract File(s) 12-18 04:56:25 NPT 2013-12-18 04:56:25 NPT 2013-12-18 04:56:25 NPT 2013-12-18 04:56:25 NPT 282 AI

MyCoupons.zip Export Selected Rows to CSV 12-22 00:53:18 NPT 2013-12-22 00:53:26 NPT 2013-12-22 00:53:17 NPT 2013-12-22 00:53:17 NPT 8057474 AI

Pricing Sheet.xls Add file Tags 12-22 00:38:52 NPT 2013-12-22 00:38:52 NPT 2013-12-22 00:38:52 NPT 2013-12-22 00:38:52 NPT 1550 AI

Pricing Sheet.xls Add Files to Hash Set 12-22 00:38:52 NPT 2013-12-22 00:38:52 NPT 2013-12-22 00:38:52 NPT 2013-12-22 00:38:52 NPT 1550 AI

Pricing Sheet.xls Properties

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

Result: of Result ↺ ↻

[aasish@parrot]-[~] \$

Extracting the files

10916-MyCoupons.zip (evaluation copy)

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX

10916-MyCoupons.zip - ZIP archive, unpacked size 8,717,313 bytes

Name Size Packed Type M Enter password

-. 1,403,292 1,270,273 JPG File

Gatorade.jpg \* 1,980,882 1,929,206 PNG File

Misc Many Drink... 975,225 833,965 PNG File

Mountain Dew.p... 1,063,307 976,524 PNG File

Poptarts.png \* 1,755,500 1,593,163 PNG File

Twinkies.png \* 1,539,107 1,453,355 PNG File

Enter password for the encrypted file  
C:\Users\sachi\AppData\Local\Temp\Rar\$O...\\Mountain Dew.png  
in archive 10916-MyCoupons.zip

Enter password

Show password

Use for all archives Organize passwords...

OK Cancel Help

[aasish@parrot]-[~] \$

Now let's crack the password

## Using ophcrack

The screenshot shows the ophcrack application window. At the top, there's a menu bar with 'ophcrack' and icons for Load, Delete, Save, Tables, Crack, Help, Exit, and About. Below the menu is a toolbar with similar icons. A navigation bar at the top has tabs for Progress, Statistics, and Preferences, with 'Progress' selected. The main area displays a table of user accounts and their hashes:

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
*disabled* Administrator	31d6cfe0d16ae931b73c59d7e0c089c0				empty
*disabled* Guest	31d6cfe0d16ae931b73c59d7e0c089c0				empty
Craig		85786ac88f59806d085ff414553fae6e			hungry123

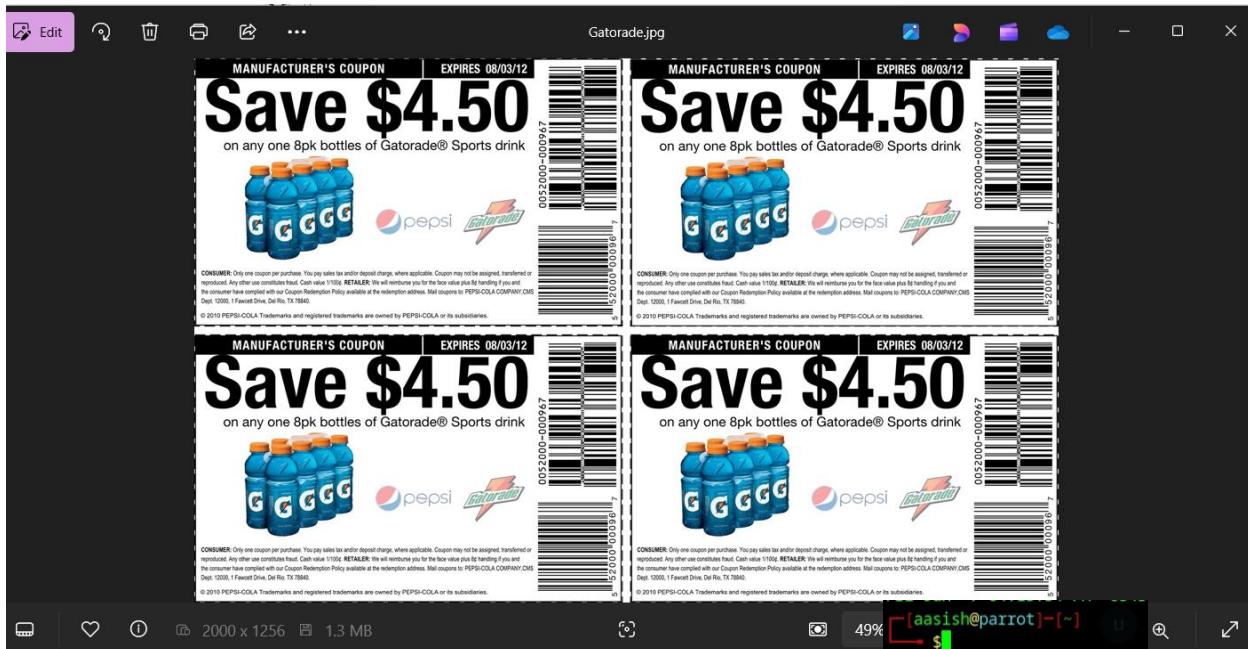
Below the table, there's a progress bar labeled 'Preload' showing '100% in RAM'. To the right of the progress bar is a terminal window with the text: '[aasish@parrot] ~ \$'. At the bottom, there are status indicators: Preload: done, Brute force: done, Pwd found: 3/3, Time elapsed: 0h 0m 28s.

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

**Run Ingest Modules**

**Steps**

**1. Configure Ingest Modules**

Configure Ingest Modules

Run ingest modules on:

All Files, Directories, and Unallocated Space

Recent Activity

Hash Lookup

File Type Identification

Extension Mismatch Detector

Embedded File Extractor

Picture Analyzer

Keyword Search

Email Parser

Encryption Detection

Interesting Files Identifier

Central Repository

PhotoRec Carver

Virtual Machine Extractor

Data Source Integrity

Android Analyzer (aLEAPP)

Cyber Triage Malware Scanner

DJI Drone Analyzer

Select All   Deselect All   History

Check all file types

Check all file types except text files

Check only multimedia and executable files

Skip files without extensions

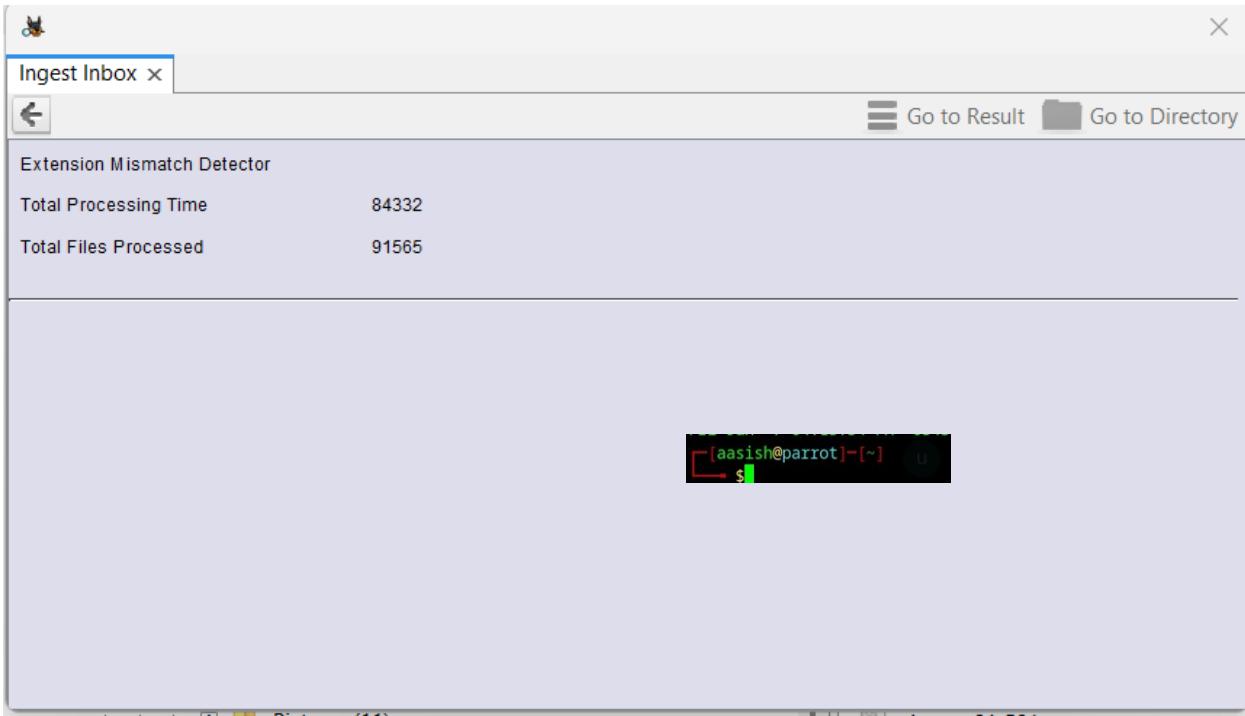
Skip known files

[aasish@parrot] - [~]

Flags files that have a non-standard extension based on the

Global Settings

< Back   Next >   Finish   Cancel   Help



## Hidden files:

The screenshot shows the Autopsy 4.21.0 interface with the 'Extension Mismatch Detected' analysis results table highlighted by a red box. The table lists 39 results with columns for Source Name, S, C, O, Source Type, Score, Conclusion, Configuration, and Justification.

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification
4230.dat	0	File	Likely Notable	File has MIME type of application/x-msoffice dat				
(1976F050-6ECA-11E3-8254-000C29D6EF92).dat	0	File	Likely Notable	File has MIME type of application/x-msoffice dat				
RecoveryStore.(8AD15056-6EC9-11E3-8254-000C29D6EF92).dat	0	File	Likely Notable	File has MIME type of application/x-msoffice dat				
(8AD15058-6EC9-11E3-8254-000C29D6EF92).dat	0	File	Likely Notable	File has MIME type of application/x-msoffice dat				
(9332CF71-6EC9-11E3-8254-000C29D6EF92).dat	0	File	Likely Notable	File has MIME type of application/x-msoffice dat				
RecoveryStore.(949E777E-6775-11E3-824E-000C29	0	File	Likely Notable	File has MIME type of application/x-msoffice dat				
(4E209779-6EC4-11E3-8254-000C29D6EF92).dat	0	File	Likely Notable	File has MIME type of application/x-msoffice dat				
MachineInfo.dat	0	File	Likely Notable	File has MIME type of application/x-msoffice dat				
4- <a href="http://\$wscont1.lapps.microsoft.com/\$winstore">http://\$wscont1.lapps.microsoft.com/\$winstore</a>	0	File	Likely Notable	File has MIME type of image/png dat				
4- <a href="http://\$wscont1.lapps.microsoft.com/\$winstore">http://\$wscont1.lapps.microsoft.com/\$winstore</a>	0	File	Likely Notable	File has MIME type of image/png dat				
4- <a href="http://\$wscont1.lapps.microsoft.com/\$winstore">http://\$wscont1.lapps.microsoft.com/\$winstore</a>	0	File	Likely Notable	File has MIME type of image/png dat				

underage_r@ygold_010.txt	0	File	Likely Notable	File has MIME type of image/jpeg	btx
underage_r@ygold_011.txt	0	File	Likely Notable	File has MIME type of image/jpeg	btx
underage_r@ygold_012.txt	0	File	Likely Notable	File has MIME type of image/jpeg	btx
underage_r@ygold_013.txt	0	File	Likely Notable	File has MIME type of image/jpeg	btx

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% 34% 31% 0° 45% 34% 31% | Tags Menu

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

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° 45% 34% 31% 0° 45% 34% 31% | Tags Menu

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

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° 45% 20% 31% 0° 45% 20% 31% | Tags Menu

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

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° 45% 34% 31% 0° 45% 34% 31% | Tags Menu

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

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	0	File	Likely Notable				File has MIME type of application/x-msoffice dat	dat
(D5506EEE-6774-11E3-824E-000C29D6EF92).dat	0	0	File	Likely Notable				File has MIME type of application/x-msoffice dat	dat
(F687F41F-6774-11E3-824E-000C29D6EF92).dat	0	0	File	Likely Notable				File has MIME type of application/x-msoffice dat	dat
(F687F420-6774-11E3-824E-000C29D6EF92).dat	0	0	File	Likely Notable				File has MIME type of application/x-msoffice dat	dat
comempty.dat	0	0	File	Likely Notable				File has MIME type of application/x-msoffice dat	dat
comempty.dat	0	0	File	Likely Notable				File has MIME type of application/x-msoffice dat	dat
comempty.dat	0	0	File	Likely Notable				File has MIME type of application/x-msoffice dat	dat
comempty.dat	0	0	File	Likely Notable				File has MIME type of application/x-msoffice dat	dat
underage_r@ygold_010.txt	0	0	File	Likely Notable				File has MIME type of image/jpeg	txt
underage_r@ygold_011.txt	0	0	File	Likely Notable				File has MIME type of image/jpeg	txt
underage_r@ygold_012.txt	0	0	File	Likely Notable				File has MIME type of image/jpeg	txt
underage_r@ygold_013.txt	0	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: | 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 .._.C...  
0x00000080: 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 .._.C...
```

[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	AI
[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	AI
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	AI	
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	AI	
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	AI	
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	AI	
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	AI	
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	AI	
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	AI	
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	AI	

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: | 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 .._.C...  
0x00000080: 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 .._.C...
```

## Installed Programs

First look into program files

First one is GIMP2

The screenshot shows the Autopsy 4.2.1.0 interface. In the Directory Tree, under 'Data Sources' and 'Craig Tucker Desktop.E01\_1 Host', the 'vol2 (NTFS / exFAT (0x07); 2048-125827071)' volume is selected. Inside, the 'Program Files/GIMP 2' folder is highlighted with a red box. The 'Listing' tab in the center pane shows a table of file details:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Ki
[current folder]				2013-12-21 03:22:41 NPT	2013-12-21 03:22:41 NPT	2013-12-21 03:22:20 NPT	2013-12-21 03:22:20 NPT	56	Allocated	Allocated	un
[parent folder]				2013-12-22 00:48:29 NPT	2013-12-22 00:48:29 NPT	2013-12-22 00:48:29 NPT	2013-08-22 19:21:15 NPT	56	Allocated	Allocated	un
32				2013-12-21 03:22:29 NPT	2013-12-21 03:22:29 NPT	2013-12-21 03:22:29 NPT	2013-12-21 03:22:29 NPT	408	Allocated	Allocated	un
bin				2013-12-21 03:22:41 NPT	2013-12-21 03:22:41 NPT	2013-12-21 03:22:28 NPT	2013-12-21 03:22:41 NPT	56	Allocated	Allocated	un
etc				2013-12-21 03:22:28 NPT	2013-12-21 03:22:28 NPT	2013-12-21 03:22:28 NPT	2013-12-21 03:22:20 NPT	336	Allocated	Allocated	un
lib				2013-12-21 03:22:41 NPT	2013-12-21 03:22:41 NPT	2013-12-21 03:22:41 NPT	2013-12-21 03:22:20 NPT	544	Allocated	Allocated	un
libexec				2013-12-21 03:22:41 NPT	2013-12-21 03:22:41 NPT	2013-12-21 03:22:41 NPT	2013-12-21 03:22:41 NPT	304	Allocated	Allocated	un
Python				2013-12-21 03:22:42 NPT	2013-12-21 03:22:42 NPT	2013-12-21 03:22:42 NPT	2013-12-21 03:22:41 NPT	552	Allocated	Allocated	un
share				2013-12-21 03:22:28 NPT	2013-12-21 03:22:28 NPT	2013-12-21 03:22:28 NPT	2013-12-21 03:22:20 NPT	56	Allocated	Allocated	un
uninst				2013-12-21 03:22:45 NPT	2013-12-21 03:22:45 NPT	2013-12-21 03:22:45 NPT	2013-12-21 03:22:20 NPT	488	Allocated	Allocated	un

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.

The screenshot shows an email message in the Autopsy interface. The subject is 'Subject: Re: Coupon Making'. The message is from 'Stan Marsh <stan.marsh27@yahoo.com>' to 'Craig Tucker <coupon-king@outlook.com>' on 'Date: 20/12/2013 13:25:40'. The attachments listed are '(3) [Noname], HowtoMakeCoupons.jpg, 6CommandmentsofCouponMaking.docx'.

Here r sum guides but just warning u that u r getting in 2 a whole new deal by making them urself. u get caught using them, not so bad and u can make up an excuse...u get caught making them, u r doomed. So dont be a newb and get caught. BTW u need GIMP 2 make ur own, so go download it.

Again in the downloads folder



Craig Tucker Case - Autopsy 4.2.1.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img\_Craig Tucker Desktop.E01/vol\_vol2/Users/Craig/AppData/Local

Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags

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

Strings Extracted Text Translation

```

Page: 1 of 1 Page Go to Page: Script: Latin - Basic
+++
</bookmarkgroups>
<bookmarkapplications>
<bookmarkapplication name="GNU Image Manipulation Program" exec="&apos;gimp-2.8 %&apos;" modified="2013-12-21T19:29:27Z" count="2"/>
+++
</bookmarkapplications>
</metaadata>
</info>
</bookmark>
<bookmark href="file:///E/Coupons/Batteries%20-%20edited.jpg" added="2013-12-21T19:31:59Z" modified="2013-12-21T19:32:04Z" visited="2013-12-21T19:32:04Z">
<info>
<metadata owner="http://freedesktop.org">
<mime:mime-type type="image/jpeg">
<bookmarkgroups>
<bookmarkgroup>Graphics</bookmarkgroup>
</bookmarkgroups>
+++
<bookmarkapplications>
+++
<bookmarkapplication name="GNU Image Manipulation Program" exec="&apos;gimp-2.8 %&apos;" modified="2013-12-21T19:32:04Z" count="2"/>
</metaadata>
</info>
</bookmark>
<xbel>
```

[aasish@parrot] - [~]

</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:

Craig Tucker Case - Autopsy 4.2.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img\_Craig Tucker Desktop.E01/vol\_vol2/Users/Craig/Documents/My Stuff

Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags
1304643149337.png	0			2011-05-06 11:05:18 NPT	2013-12-22 00:59:07 NPT	2013-12-22 00:59:07 NPT	2013-12-22 00:59:07 NPT	1668517	Allocated	A
1304643663005.png	0			2011-05-06 11:07:20 NPT	2013-12-22 00:59:07 NPT	2013-12-22 00:59:07 NPT	2013-12-22 00:59:07 NPT	878919	Allocated	A
1304643804769.png	0			2011-05-06 11:08:04 NPT	2013-12-22 00:59:07 NPT	2013-12-22 00:59:07 NPT	2013-12-22 00:59:07 NPT	375603	Allocated	A
<b>1304644031008.png</b>	0			2011-05-06 11:10:18 NPT	2013-12-22 00:59:07 NPT	2013-12-22 00:59:07 NPT	2013-12-22 00:59:07 NPT	123467	Allocated	A
1304644210039.png	0			2011-05-06 11:10:22 NPT	2013-12-22 00:59:06 NPT	2013-12-22 00:59:06 NPT	2013-12-22 00:59:06 NPT	611379	Allocated	A
1352661780468.jpg	0			2012-11-12 07:38:20 NPT	2013-12-19 04:57:49 NPT	2013-12-19 04:57:49 NPT	2013-12-19 04:57:49 NPT	1153249	Allocated	A
1352661880980.png	0			2012-11-12 07:38:20 NPT	2013-12-19 04:57:49 NPT	2013-12-19 04:57:49 NPT	2013-12-19 04:57:49 NPT	628987	Allocated	A
1352661935923.png	0			2012-11-12 07:38:20 NPT	2013-12-19 04:57:50 NPT	2013-12-19 04:57:50 NPT	2013-12-19 04:57:50 NPT	1820149	Allocated	A
135266223853.jpg	0			2012-11-12 07:38:54 NPT	2013-12-19 04:57:50 NPT	2013-12-19 04:57:50 NPT	2013-12-19 04:57:50 NPT	172046	Allocated	A
1353029857214.png	0			2012-11-16 09:41:38 NPT	2013-12-19 04:57:51 NPT	2013-12-19 04:57:51 NPT	2013-12-19 04:57:51 NPT	1699269	Allocated	A

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

0% 51% Tags Menu

MANUFACTURER'S COUPON Expires: 10/31/2011

Save \$3.00 on any one(1) 1.28oz container of Arizona Iced Tea.

Arizona Iced Tea and the Arizona logo are trademarks of The Quaker Oats Company. © 2011 Quaker Oats Company. All rights reserved. Arizona Iced Tea is a registered trademark of The Quaker Oats Company. © 2011 Quaker Oats Company. All rights reserved. This coupon entitles the bearer to a discount on purchases of Arizona Iced Tea products at participating grocery stores. Limit one coupon per household per purchase. One coupon per transaction. Not valid at gas bars or convenience stores. Not valid with other offers or discounts. Not valid where prohibited by law. Void where prohibited. Offer subject to change without notice.

For more information about this offer, visit [www.azicedtea.com](http://www.azicedtea.com).

Printed by SMARTSOURCE® 000877 007336 000877

# 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.