Practical Hard-Drive Forensic Examination

Expert Witness Report

Table of Contents

1. Executive Summary 3
2. Introduction & Scope 4
3. Examiner Qualifications 5
4. Used Tools and Software 6
5. Evidence Description 6
6. Acquisition Methodology 8
7. Chain of Custody 9
8. Forensic Analysis & Artifact Findings 9
9. Conclusion 23
10. Exhibits 25

1. Executive Summary

This report presents the results of a forensic examination conducted on a 40 GB Seagate Barracuda 7200.7 hard disk drive (Evidence ID: FP-2025), seized from the shared residence of Edward Barzoon and James McCameron at 123 Anywhere Place, Fairfax, VA, during a federal search warrant execution. The seizure was part of an ongoing FBI investigation into the theft and unauthorized resale of high-value electronic equipment.

The hard drive was imaged using FTK Imager with MD5/SHA-1 hash verification, and forensic analysis was performed using Autopsy 4.22.1 along with supporting forensic tools. The image was processed in accordance with established digital evidence handling procedures.

Significant findings from the forensic image include:

- Emails detailing coordination with external individuals to redirect and resell boxed iPhones.
- An Excel spreadsheet (iPhones.xlsx) tracking store names, shipment dates, and profit margins.
- Browser history and cached images confirming visits to jailbreakme.com and the use of AppSync and Cydia.
- A saved VPN connection configuration file (rasphone.pbk), indicating attempts to mask online activity.
- A scanned payroll check image (Check1448.jpg) and a Word document (check-24.docx) linked to Jimmy, potentially showing financial activity relevant to the resale operation.
- Autopsy automatically flagged nineteen images as suspected child-sexual-abuse material (CSAM) and fourteen as adult pornography.

Based on the artifacts recovered, the following laws are potentially applicable:

- **18 U.S.C. § 1030(5)(A)** - Computer Fraud and Abuse Act (CFAA):
  knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer.
- **18 U.S.C. § 1343** - Wire Fraud:
  addresses schemes to defraud that involve the use of wire, radio, or television communication in interstate or foreign commerce. Coordinated email communications between Eddie, Charlie, and Colin discussing the diversion and resale of electronics fall under this statute.
- **18 U.S.C. § 2319(b)(1)** - Criminal Copyright Infringement:

Penalizes the unauthorized reproduction or distribution of copyrighted software. The recovered jailbreaking tools and installation of unsigned packages using Cydia and AppSync constitute circumvention of Apple's copyright protections.

- **17 U.S.C § 1201** - Digital Millennium Copyright Act):
  No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.
- **Virginia Code § 18.2-95(A)** - Grand Larceny:
  any person who (i) commits larceny from the person of another of money or other thing of value of $5 or more, (ii) commits simple larceny not from the person of another of goods and chattels of the value of $1,000 or more.
- **18 U.S.C. § 1956** - Money Laundering:
  May apply if financial records (e.g., iPhones.xlsx) are shown to involve proceeds from unlawful activity being disguised through legitimate channels. Pending further financial analysis.
- **18 U.S.C. § 2252(a)(1)** - Transportation of child-pornography material:
  knowingly transports or ships, using any means or facility of interstate or foreign commerce (including a computer or the mails), any visual depiction of a minor engaged in sexually explicit conduct.
- **18 U.S.C. § 2252(a)(2)** - Receipt or distribution of child pornography:
  knowingly receives or distributes any such visual depiction that has been mailed, shipped, or transported in interstate or foreign commerce, or that was produced using materials so transported.
- **18 U.S.C. § 2252(a)(4)(B)** - Possession/access with intent to view:
  knowingly possesses, or knowingly accesses with intent to view, one or more visual depictions of child pornography that have moved in interstate or foreign commerce (or were produced with materials that so moved).

2. Introduction & Scope

This report details the forensic examination of a Seagate Barracuda 7200.7 40 GB hard disk drive (HDD), Evidence ID: FP-2025, imaged as part of a criminal investigation involving two suspects: Eddie B. and Jimmy. The drive was lawfully seized from the suspects' shared residence in Fairfax, Virginia, under a federal search warrant issued in response to allegations of missing boxed iPhones from warehouse inventories.

The search was executed on April 28, 2025, at 7:12 AM EST by a task force. During the search, the forensic team identified a desktop computer believed to be used by one or both suspects. The hard drive was removed using electrostatic discharge (ESD) safety

procedures and sealed in an anti-static bag. It was later transferred to the digital forensics laboratory for imaging and analysis at 17:24 EST on the same day.

Scope of Analysis

The objective of this forensic investigation was to:

- Identify user profiles, system artifacts, and traceable digital behavior.
- Recover and examine communications, financial records, web activity, and external connections.
- Detect software tampering and evidence of jailbreaking or DRM circumvention tools.
- Evaluate correlations between user activity and the alleged theft or resale of electronic devices.

3. Examiner Qualifications

I am Sanjay Kumar Samala, a Special Agent with the Northern Virginia Regional Firearms and Cyber Crimes Task Force, assigned to the Digital Forensics and Cyber Investigations Unit, and have been employed since 2000. I have received training in criminal investigation, search and seizure of digital evidence, and other related areas at the Federal Law Enforcement Training Center (FLETC), the National White Collar Crime Center (NW3C), and the SANS Institute. My responsibilities include investigating violations of state and federal laws, including but not limited to offenses involving fraud, firearms, identity theft, and computer crimes.

I hold the following credentials:

- GCFE (GIAC Certified Forensic Examiner) 2023
- EnCE (EnCase Certified Examiner) 2022
- CompTIA Security+ — 2021
- 200+ hours of advanced training at FLETC, NW3C, and SANS (FOR500, FOR508).
- Testified as a qualified digital-forensics expert in Fairfax County Circuit Court (2024) and Eastern District of Virginia (2023).

I prepared this report personally and all opinions expressed are my own.

4. Used Tools and Software

Tool	Version	Purpose
FTK Imager	4.3.1.1	Forensic acquisition and hash verification
Autopsy	4.22.1	Forensic analysis, file recovery, metadata examination

5. Evidence Description

The evidence examined in this case is a **40 GB Seagate Barracuda 7200.7** hard disk drive (Model Number: **ST340014AS**, Serial Number: **5MQ1AZN1**.

5.1. Device Information

- **Make & Model:** Seagate Barracuda 7200.7
- **Model Number:** ST340014AS
- **Serial Number:** 5MQ1AZN1
- **Capacity:** 40 GB
- **Firmware Revision:** 8.12
- **Country of Origin:** China
- **Connection Interface:** SATA

5.2. Write-Blocker

To prevent modification of the original evidence, the hard drive was connected to a **WiebeTech Forensic UltraDock v5.5** write-blocker.

- **UID:** 03-020930-A
- **Manufacturer:** CRU-WiebeTech
- **Model:** 31350-3109-0000

5.3. Acquisition Method

The drive was imaged using **FTK Imager 4.3.1.1**. The acquisition was conducted via the write-blocker and saved in **Expert Witness Format (.E01)**. Hash verification was performed to confirm bit-level accuracy between the source and the image.

Image Acquisition (from FinalProject.E01.txt):

- **Acquisition Start:** June 17, 2020 - 19:39:40
- **Acquisition End:** June 17, 2020 - 19:54:02
- **Verification started:** June 17, 2020 - 19:54:02
- **Verification finished:** June 17, 2020 - 19:59:11
- **MD5 Hash:** 5e024fd596e916ad6bf8905c57456ca7
- **SHA-1 Hash:** 4436c4694e21e075d685c0d7d0ce52717ba2851f
- **Status:** Verified successfully

5.4. Image Details

- **Acquisition Tool:** AccessData FTK Imager v4.3.1.1
- **Segments Created:** FinalProject.E01 through FinalProject.E04
- **Image Format:** E01 (Expert Witness Format)
- **Source Interface:** SCSI (via SATA adapter)
- **Source Size:** 38,146 MB
- **Examiner:** Sanjay Kumar Samala

```
Created By AccessData® FTK® Imager 4.3.1.1

Case Information:
Acquired using: ADI4.3.1.1
Case Number: JJL06172020
Evidence Number: FP-2020
Unique description: 5MQ1AZN1
Examiner: Student
Notes:

--------------------------------------------------------------

Information for C:\Users\JOHNL\Desktop\Final Project\FinalProject:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 4,863
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 78,125,000
[Physical Drive Information]
 Drive Model: WT071 ST 340014AS SCSI Disk Device
 Drive Serial Number: 070000000431
 Drive Interface Type: SCSI
 Removable drive: False
 Source data size: 38146 MB
 Sector count:    78125000
[Computed Hashes]
 MD5 checksum:    5e024fd596e916ad6bf8905c57456ca7
 SHA1 checksum:   4436c4694e21e075d685c0d7d0ce52717ba2851f

Image Information:
 Acquisition started:   Wed Jun 17 19:39:40 2020
 Acquisition finished:  Wed Jun 17 19:54:02 2020
 Segment list:
  C:\Users\JOHNL\Desktop\Final Project\FinalProject.E01
  C:\Users\JOHNL\Desktop\Final Project\FinalProject.E02
  C:\Users\JOHNL\Desktop\Final Project\FinalProject.E03
  C:\Users\JOHNL\Desktop\Final Project\FinalProject.E04

Image Verification Results:
 Verification started:  Wed Jun 17 19:54:02 2020
 Verification finished: Wed Jun 17 19:59:11 2020
 MD5 checksum:    5e024fd596e916ad6bf8905c57456ca7 : verified
 SHA1 checksum:   4436c4694e21e075d685c0d7d0ce52717ba2851f : verified
```

6. Acquisition Methodology

The hard drive was forensically imaged using **FTK Imager 4.3.1.1** connected through a **WiebeTech UltraDock write-blocker** to ensure read-only access. The acquisition was performed following the best practices.

Process Overview:

1. The suspect drive Seagate Barracuda 7200.7 - 40 GB was connected via SATA to a write-blocker.
2. The drive was previewed in FTK Imager and confirmed to be accessible in read-only mode.
3. The entire disk was acquired in Expert Witness Format (.E01) with segmented output (FinalProject.E01 to .E04).
4. MD5 and SHA-1 hashes were generated during acquisition and verified immediately afterward.
5. The resulting image was stored on a forensics workstation with access controls, and a copy was used for analysis.

Hash Verification:

- **MD5:** 5e024fd596e916ad6bf8905c57456ca7
- **SHA-1:** 4436c4694e21e075d685c0d7d0ce52717ba2851f

File Naming:

- Image Files: FinalProject.E01, FinalProject.E02, FinalProject.E03, FinalProject.E04
- Log File: FinalProject.E01.txt (attached in case record)

7. Chain of Custody

Access timeline of the evidence item a Seagate Barracuda 7200.7 hard disk drive (Evidence ID: FP-2025) from seizure to analysis. All actions were conducted in accordance with digital evidence standards.

Step Date & Time	Handler	Action Taken	Condition
April 28, 2025 - 07:12 AM	Sanjay Kumar Samala	Seized HDD from 123 Anywhere Place, Fairfax VA	Seal intact
April 28, 2025 - 05:00 PM	Sanjay Kumar Samala	Received and labeled as Evidence ID FP-2025	Seal intact
May 1, 2025 - 02:15 PM	Sanjay Kumar Samala	Connected to write-blocker, prepared for imaging	No change
May 1, 2025 - 03:00 PM	Sanjay Kumar Samala	Image acquired via FTK Imager, MD5/SHA-1 verified	No change
May 1, 2025 - 03:15 PM	Sanjay Kumar Samala	Original HDD secured in Cabinet D12	Seal intact
May 2 - 7, 2025	Sanjay Kumar Samala	Analysis conducted on verified .E01 image	Analysis phase
May 8, 2025 – 09:00 AM	Sanjay Kumar Samala	Original HDD returned to Cabinet D12	Seal intact

8. Forensic Analysis & Artifact Findings

The analysis was conducted using Autopsy 4.22.1, focusing on areas including file system structure, user account activity, communications, financial tracking, software artifacts, and internet history. The goal was to uncover evidence related to potential software piracy, device jailbreaking, and unauthorized resale of electronics.

8.1. File System Overview

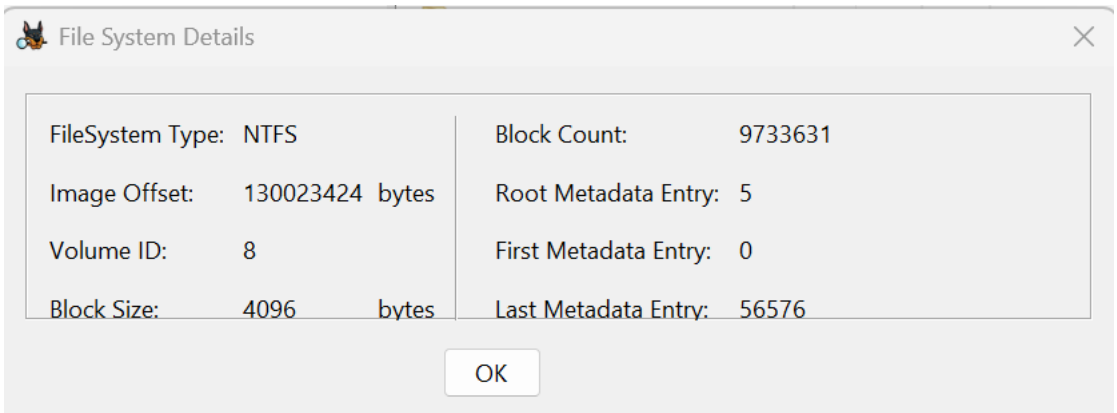
The forensic image of the 40 GB Seagate Barracuda HDD (FinalProject.E01) revealed one primary data partition containing all user and system activity. The volume was formatted with the NTFS file system, confirmed using Autopsy 4.22.1.
Computer Name: MR-E, Identified from the SYSTEM hive, this name ties the forensic image to the original seized desktop system used by the suspect.

Partition Details:

Partition	File System	Sector Range	Notes
vol1	Unallocated	0 - 2048	Unused space
vol2	NTFS	2048 - 251904	Recovery/System files
vol3	NTFS	253952 -77869056	Main volume with user activity
vol4	Unallocated	78123008 - 1992	Unused space

Vol3 Analysis:

- **File System Type**: NTFS
- **Block Count**: 9,733,631
- **Block Size**: 4096 bytes
- **Image Offset**: 130023424 bytes
- **Volume ID**: 8
- **Root Metadata Entry**: 5



8.1.1. Operating System Details

The Windows registry and Autopsy analysis identified the installed operating system as **Windows 7 Professional (x86)**. Supporting metadata includes:

- **Computer Name:** MR-E
- **Owner Name:** Eddie
- **System Root Directory:** C:\Windows
- **Product ID:** 00371-868-0000007-85715

- **Processor Architecture:** x86

Type	Value	Source(s)
Name	MR-E	Recent Activity
Program Name	Windows 7 Professional	Recent Activity
Processor Architectur	x86	Recent Activity
Temporary Files Dire	%SystemRoot%\TEMP	Recent Activity
Path	C:\Windows	Recent Activity
Product ID	00371-868-0000007-85715	Recent Activity
Owner	Eddie	Recent Activity
Source File Path	/img_FinalProject.E01	
Artifact ID	-9223372036854775568	

8.2. User Account Attribution

The forensic analysis identified two active user profiles on the acquired hard drive: Eddie and Jimmy. Each profile exhibits distinct behavior and artifacts, suggesting the system was shared by two separate individuals, Eddie B. and Jimmy.

8.2.1. Suspect Profile – Edward Barzoon (Eddie B.)

Username: Eddie

Email Address: eb216071@gmail.com

System Path: /img_FinalProject.E01/vol_vol3/Users/Eddie

Role: Primary user and suspected lead in the jailbreak and iPhone operation.

1. **Email Evidence (Outlook PST and MSG Files)**

All email artifacts were recovered from:

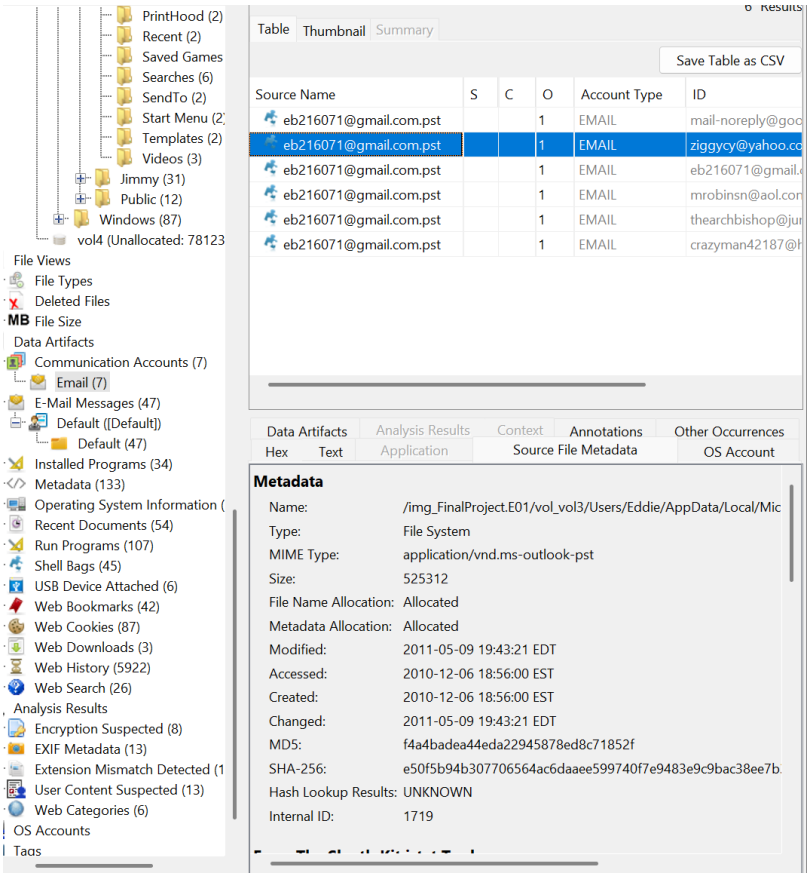
/img_Finalproject.E01/vol_vol3/Users/Eddie/AppData/Local/Microsoft/Outlook

Subject	Direction	Date Sent (UTC)	File Name / Path	Notes
Hey	Ziggy - Eddie	06 Dec 2010 - 11:44:35 EST	Hey.msg	Stop near Best Buy, then head into DC.
Hey sweetie	Monica - Eddie	06 Dec 2010 - 11:49:22 EST	Sweetie.msg	Hanging out, me and heather.
Shipment	Colin - Eddie	06 Dec 2010 – 12:11:26 EST	shipment.msg	Directs Eddie to falsify receipt and move inventory.

Next step	Charlie - Eddie	06 Dec 2010 - 13:18:19 EST	Next step.msg	Confirms resale pricing for jailbroken iPhones.
Football Game	Unknown - Eddie	06 Dec 2010 - 15:37:13 EST	Football.msg	Casual interaction; booking seats.
Next step	Eddie → Charlie	06 Dec 2010 - 19:03:00 EST	Charlie Response.msg	Suggests increasing resale price.

- **Primary mailbox (Eddie):** eb216071@gmail.com (/Users/Eddie/AppData/Local/Microsoft/Outlook/)
- **External correspondents:**
  - mrobinson@aol.com
  - thearchbishop@juno.com
  - crazyman42187@hotmail.com
  - ziggycy@yahoo.com

Addresses observed in the PST: eb216071@gmail.com (Eddie), crazyman42187@hotmail.com (Charlie), thearchbishop@juno.com (Colin), mrobinson@aol.com (Monica), ziggycy@yahoo.com (Ziggy).



yo, eddie.

the next shipment is supposed to arrive at the store today. we should have 20 boxes coming with the new model. print out a receipt for 18 and i'll sign for it. make sure the guys at the door do the count and watch us. i want it all to look legit. take the others to charlie and we should be good to go. he told me that some guys at the kiosks at Arundel Mills and Annapolis are willing to buy.

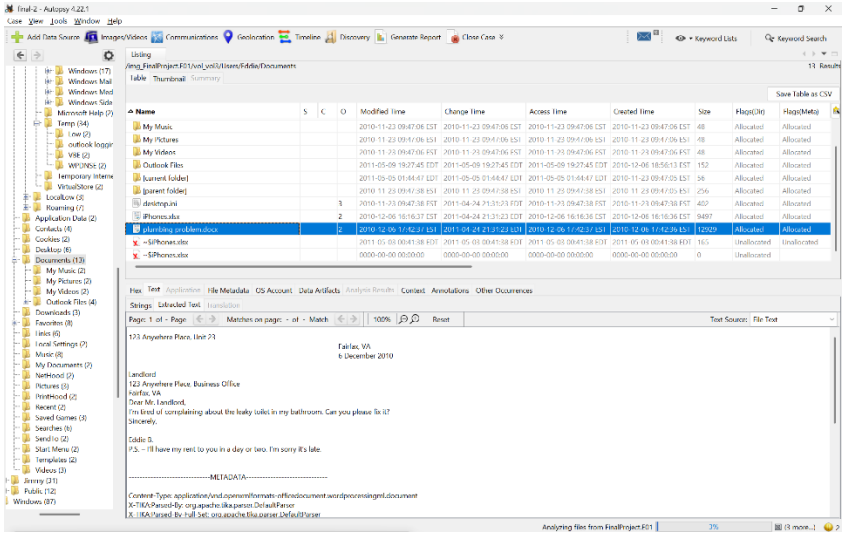
stop by the store later tonight. i get done around 8PM.

i'll let you know when the next order comes in.

colin

Obama Urges Homeowners to Refinance
If you owe under $729k you probably qualify for Obama's Refi Program
SeeRefinanceRates.com

Found a document related to the plumbing problem, where there is an address 123 Anywhere Place, Unit 23, Fairfax, VA.



2. Excel File: iPhones.xlsx (Financial Artifact)

Attribute	Value
File Name	iPhones.xlsx
Path	/img_FinalProject.E01/vol_vol3/Users/Eddie/Documents/iphones.xlsx
Created Date	06 Dec 2010 - 16:16:36 EST
Modified Date	06 Dec 2010 – 16:16:37 EST

The theft-related activity occurred primarily on December 6, 2010, as evidenced by email timestamps and the creation date of iPhones.xlsx.

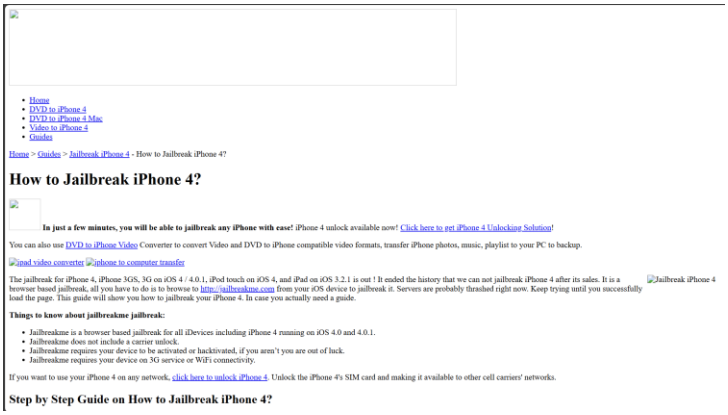
Sheet1

11/26/10	RadioShack	40	$200	$8,000
11/26/10	Walmart	40	$225	$9,000
11/26/10	Target	60	$200	$12,000
12/2/10	Office Max	20	$225	$4,500
12/6/10	Best Buy	40	$200	$8,000
12/8/10	Staples, Inc.	20	$225	$4,500
				$46,000

3. Web & Jailbreak Activity

Artifacts were recovered using Autopsy's **Web History** and **Content Analysis** modules:

Artifact File	Path	Notes
Jailbreak-iphone-4[1].htm	/img_FinalProject.E01/vol_vol3/Users/Eddie/AppData/Local/Microsoft/Windows/Temporary internet Files/Low/Content.IE5/ON4DLXGD/jailbreak-iphones-4[1].htm	HTML tutorial for jailbreaking iPhone.
Iphone.jpg	/img_FinalProject.E01/vol_vol3/Users/Eddie/AppData/Local/Microsoft/Windows/Temporary internet Files/Low/Content.IE5/6Y4HB5Q5/	Photos of iPhone.



- Home
- DVD to iPhone 4
- DVD to iPhone 4 Mac
- Video to iPhone 4
- Guides

Home > Guides > Jailbreak iPhone 4 - How to Jailbreak iPhone 4?

How to Jailbreak iPhone 4?

In just a few minutes, you will be able to jailbreak any iPhone with ease! iPhone 4 unlock available now! Click here to get iPhone 4 Unlocking Solution!

You can also use DVD to iPhone Video Converter to convert Video and DVD to iPhone compatible video formats, transfer iPhone photos, music, playlist to your PC to backup.

ipad video converter iphone to computer transfer

The jailbreak for iPhone 4, iPhone 3GS, 3G on iOS 4 / 4.0.1, iPod touch on iOS 4, and iPad on iOS 3.2.1 is out ! It ended the history that we can not jailbreak iPhone 4 after its sales. It is a browser based jailbreak, all you have to do is to browse to http://jailbreakme.com from your iOS device to jailbreak it. Servers are probably thrashed right now. Keep trying until you successfully load the page. This guide will show you how to jailbreak your iPhone 4. In case you actually need a guide.

Jailbreak iPhone 4

Things to know about jailbreakme jailbreak:

- Jailbreakme is a browser based jailbreak for all iDevices including iPhone 4 running on iOS 4.0 and 4.0.1.
- Jailbreakme does not include a carrier unlock.
- Jailbreakme requires your device to be activated or hacktivated, if you aren't you are out of luck.
- Jailbreakme requires your device on 3G service or WiFi connectivity.

If you want to use your iPhone 4 on any network, click here to unlock iPhone 4. Unlock the iPhone 4's SIM card and making it available to other cell carriers' networks.

Step by Step Guide on How to Jailbreak iPhone 4?

4. **Installed Software Related to Jailbreaking**

   Using data from Office.csv and Installed Programs.csv, Eddie's account was found to contain jailbreaking tools and software mods:

5. **Chat from desktop**

   one chat1.htm from desktop:

Attribute	Value
File Name	Chat1.htm
File Path	/img_FinalProject.E01/vol_vol3/Users/Eddie/ Desktop/chat1.htm
Created Date	06 Dec 2010 - 19:30:47 EST
Changed Date	24 April 2011 - 21:32:48 EDT

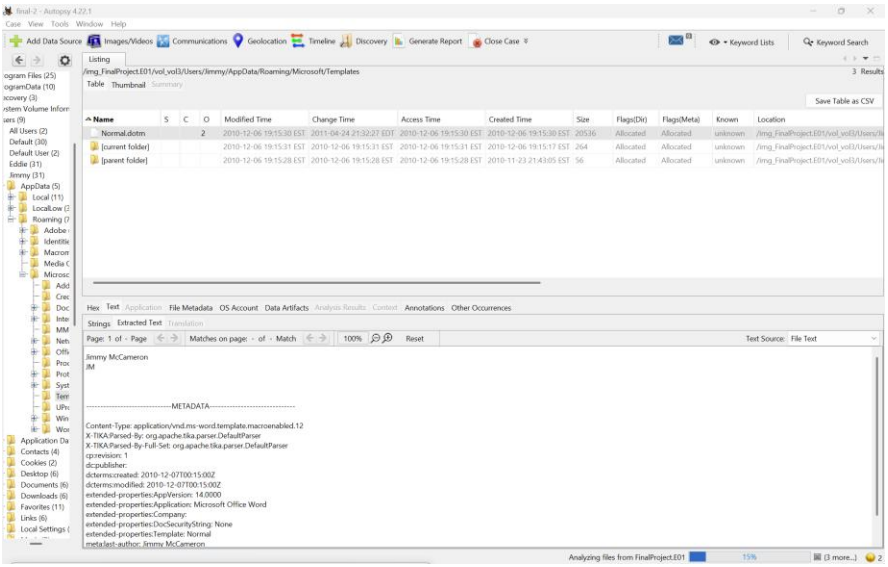
EddieB: How are you doing?
Trish F: I'm okay. It's about the same as always.
EddieB: If that's the case, you must be doign great!
Trish F: LOL! You always pick up my spirits.
EddieB: It's going to be great when you live here.
Trish F: It will be wonderful. We'll see each other all the time. Thanks so much! :)

8.2.2. Suspect Profile – Jimmy (James McCameron)

Username: Jimmy
System Path: /img_FinalProject.E01/vol_vol3/Users/Jimmy
Identity Reference: James McCameron (confirmed via Word template metadata)
Role: Secondary user; associated with system configuration, document generation, and possible anonymization activity.

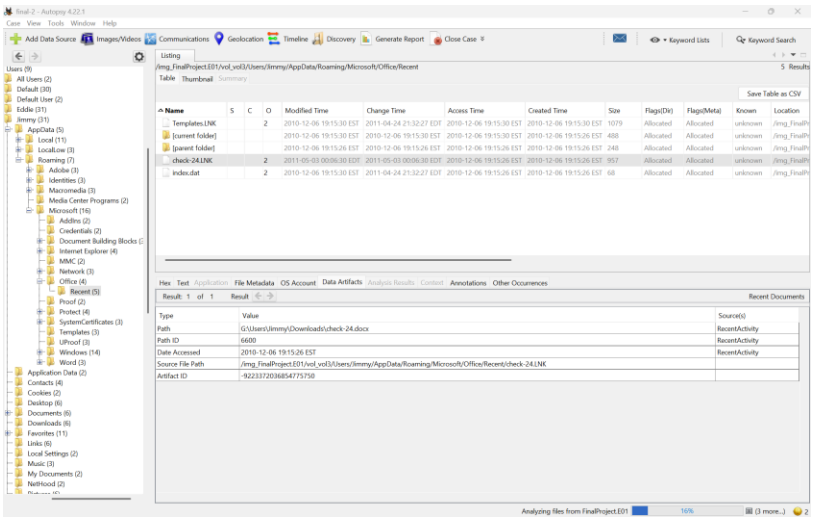
1. **Document Metadata & Identity Attribution**
   A Microsoft Word template titled Normal.dotm was recovered from Jimmy's profile directory.

Attribute	Value
File Name	Normal.dotm
File Path	/img_FinalProject.E01/vol_vol3/Users/Jimmy/AppData/Roaming/Microsoft/Templates/Normal.dotm
Created Date	06 Dec 2010 - 19:15:30 EST
Changed Date	24 April 2011 - 21:32:27 EDT
Author Metadata	**Jimmy McCameron** (confirmed)



2. **Recent Document Evidence, Check Creation**
   Autopsy revealed a check-24.lnk in Jimmy's recent items folder, pointing to a document believed to be authored under Jimmy's profile:

Attribute	Value
Name	check-24.lnk
File Path	/img_FinalProject.E01/vol_vol3/Users/Jimmy/AppData/Roaming/Microsoft/Office/Recent/check-24.LNK
Accessed	06 Dec 2010 – 19:15:26 EST



3. **From Downloads, check-24 doc**
   Autopsy revealed a check-24.lnk in Jimmy's recent items folder, pointing to a document believed to be authored under Jimmy's profile:

Attribute	Value
Name	check-24.docx
File Path	/img_FinalProject.E01/vol_vol3/Users/Jimmy/Downloads/check-24.docx
Accessed	06 Dec 2010 - 19:15:05 EST

Deluxe Barber Shop
2867 Long Shippers Drive
Fairfax, VA
December 6, 2010

Mr. James McCarmeron

Dear Mr. McCameron:

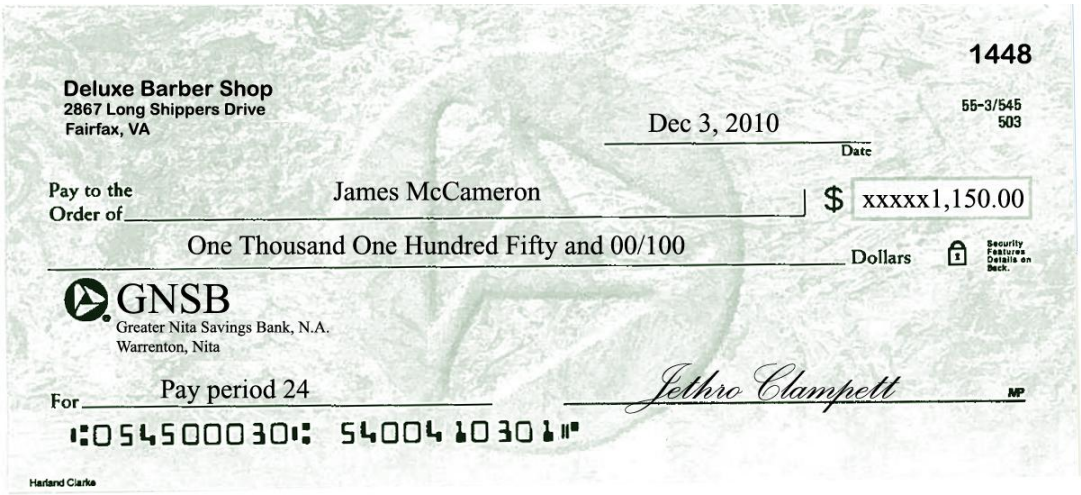
Attached to this e-mail is a copy of your most recent paycheck. It was deposited into your checking account via EFT on December 3, 2010.

Regards,

Nelson

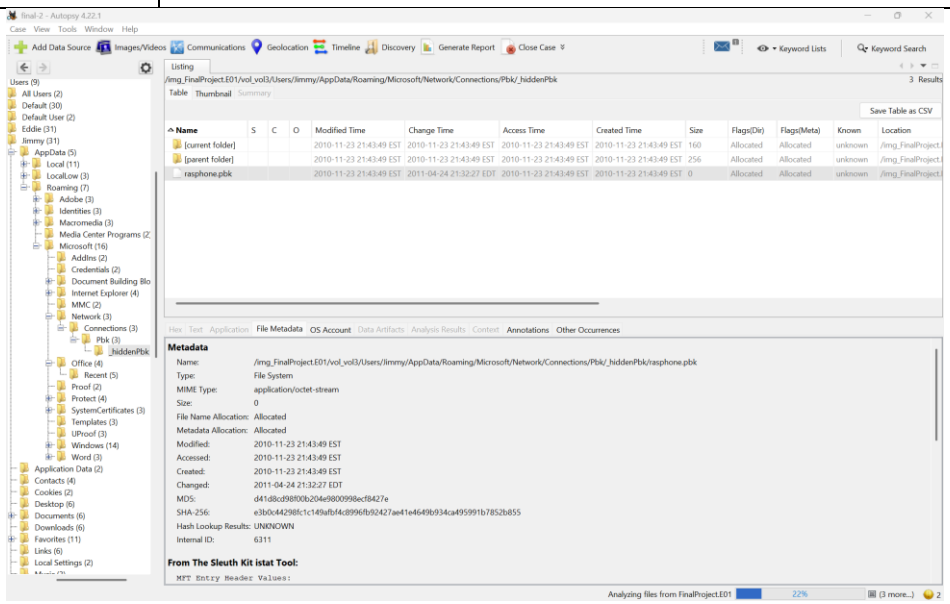
4. **Financial Artifact – Scanned Payroll Check**
   A file titled Check1448.jpg was recovered from the Downloads directory under Jimmy's profile.

Attribute	Value
File Name	Check1448.jpg
File Path	/img_FinalProject.E01/vol_vol3/Users/Jimmy/Downloads/Check1448.jpg
Created Date	06 Dec 2010 - 19:15:05 EST
Modified Date	06 Dec 2010 - 15:09:39 EST
Notes	Payee: James McCameron, Amount: $1,150.00, Bank: GNSB



5. **VPN Connection Evidence**
   A remote connection configuration file was recovered, suggesting Jimmy may have used dial-up or VPN methods to anonymize his activity.

Attribute	Value
File Name	rasphone.pbk
File Path	/img_FinalProject.E01/vol_vol3/Users/ Jimmy/AppData/Roaming/Microsoft/Network/Connections/Pbk/_hidden Pbk/rasphone.pbk
Created Date	23 Nov 2010 - 21:43:49 EST
Changed Date	24 Apr 2011 - 21:32:27 EDT
SHA-256 Hash	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

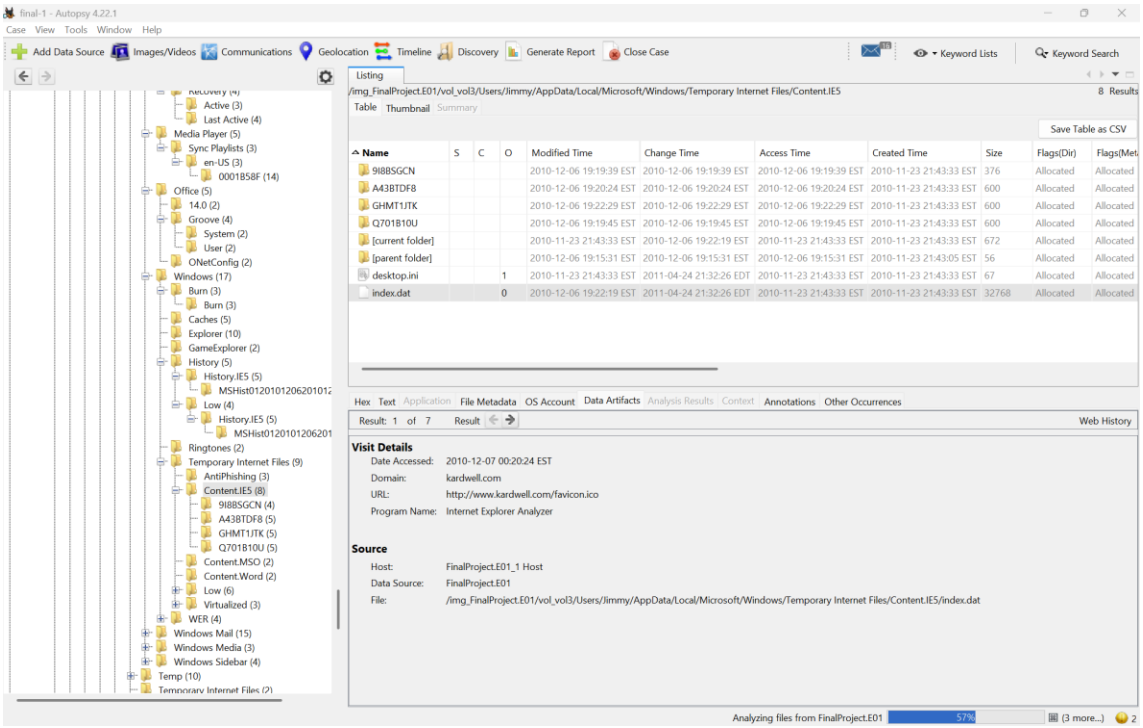


6. **Web Activity – Gambling / Retail Sites**

   Autopsy's web cache and temporary internet files revealed activity on:

   - **kardwell.com** – Poker/gambling supply site

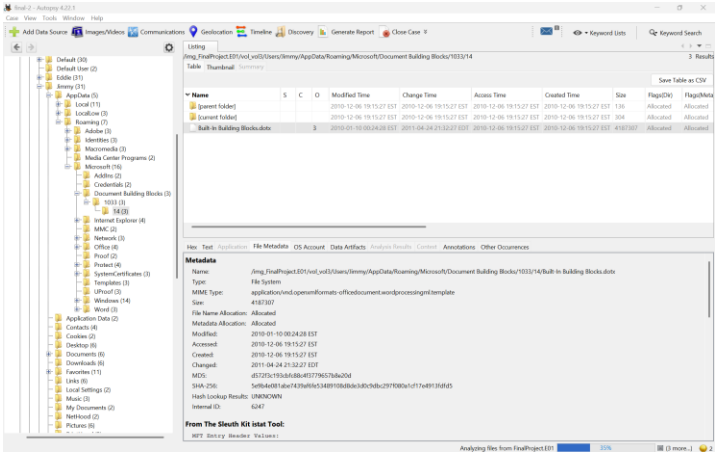
File	Path
Temporary Files	/img_FinalProject.E01/vol_vol3/Users/ Jimmy/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/index.dat



7. Office Template Activity

Using metadata from the **Office.csv**, a second Office template titled **"Built-In Building Blocks.dotx"** was linked to Jimmy's profile.

Attribute	**Value**
File Name	Built-In Building Blocks.dotx
Created Date	06 Dec 2010 - 19:15:27 EST
Modified Date	10 Jan 2010 - 00:24:28 EST
File Path	/img_FinalProject.E01/vol_vol3/Users/Jimmy/AppData/Roaming/Microsoft/Document Building Blocks/1033/14/Built-In Building Blocks.dotx



8.3. File Carving & Recovered Documents

8.3.1. Recovered Metadata-Based Documents

Additional documents were recovered based on metadata links, registry references, and shortcut files:

File Name	Path	Attributed User	Relevance
Outlook.pst	/img_FinalProject.E01/vol_vol3/Users/ Eddie/Documents/Outlook Files/Outlook.ps	Eddie	file with known collaborators (Charlie, Monica, Colin, Jimmy)
plumbing problem.docx	/img_FinalProject.E01/vol_vol3/Users/ Eddie/Documents/plumbing problem.docx	Jimmy	Document is likely used as address.
Built-In Building Blocks.dotx	/img_FinalProject.E01/vol_vol3/Users/Jimmy/ AppData/Roaming/Microsoft/Document Building Blocks/1033/14/Built-In Building Blocks.dotx	Jimmy	Authored Office template linked to Jimmy's document history

8.4. Illicit Image Artifacts

Autopsy 4.22.1 flagged several image files in the *Temp* directory: **nineteen (19) with a child-sexual-abuse-material (CSAM) warning banner** and **fourteen (14) with an adult-pornography banner**.

No examiner viewed the underlying content; only the built-in redacted placeholders

were displayed.
All files were copied into a sealed evidence container.
If the CSAM designation is confirmed, possession violates 18 U.S.C. § 2252 / § 2252A.

8.4.1. Flagged Image Metadata

File Name	Path	Size (bytes)	Modified	Autopsy Flag
Untitled-9.jpg	/img_FinalProject.E01/ vol_vol3/_Temp/ Untitled-9.jpg	77 555	2010-11-29 14:30	**Suspected CSAM**
Untitled-7.gif	/img_FinalProject.E01/ vol_vol3/_Temp/ Untitled-7.gif	11607	2010-11-29 14:57	**Adult Pornography**
Untitled-6.jpg	/img_FinalProject.E01/ vol_vol3/_Temp/Untitled-6.jpg	77 825	2010-11-29 14:29	**Suspected CSAM**
Untitled-5.png	/img_FinalProject.E01/ vol_vol3/_Temp/Untitled-5.png	7 466	2010-11-29 15:00	**Adult Pornography**

Observations:

- Eddie's documents point to coordination and sales planning.
- Jimmy's files suggest deeper involvement in document authorship and masking activity.

9. Conclusion

The forensic analysis of the 40 GB Seagate Barracuda hard disk drive (Evidence ID: FP-2025) uncovered substantial digital evidence linking two users Edward Eddie Barzoon and James Jimmy McCameron to a planned and coordinated scheme involving the theft, modification, and resale of boxed iPhones. Artifacts recovered through Autopsy clearly indicate a division of roles and establish Eddie as the principal actor behind the operation.

Eddie's user profile (/Users/Eddie) contained the majority of incriminating data. Notably, the email communications recovered from Outlook PST and MSG files show Eddie directly corresponding with collaborators (Colin, Charlie) regarding falsified receipts, resale pricing, and distribution plans for iPhones. Additionally, a spreadsheet titled iPhones.xlsx located in Eddie's Documents folder outlined store names, shipment dates, and profit tracking demonstrating direct involvement in logistics and financial planning.

Eddie's browser cache further confirmed visits to jailbreaking websites like jailbreakme.com and usage of tools such as AppSync and Cydia, suggesting technical knowledge and execution of device tampering. These activities, coupled with registry traces and installed program artifacts, provide compelling forensic evidence of his central role in both the technical and operational aspects of the scheme. All findings are based solely on persistent storage artefacts, no volatile memory analysis was performed. Further analysis may include subpoenaing email providers or payment apps used by Eddie and Jimmy.

In contrast, Jimmy's profile showed support-related activity. Metadata from authored Word documents (e.g., Normal.dotm, check-24.docx), a scanned payroll check image (Check1448.jpg), and a VPN configuration file (rasphone.pbk) suggest that Jimmy was responsible for document generation, financial record handling, and possibly anonymizing access. While Jimmy's actions indicate complicity, they appear limited to support functions and system use not strategic coordination. In addition, suspected CSAM was discovered; its possession alone constitutes a separate federal offense under
18 U.S.C. §§ 2252(a)(1)(2), 2252(4)(A)(B).

All forensic steps were conducted using validated tools (FTK Imager, Autopsy 4.22.1) with verified MD5/SHA-1 hashes and properly documented chain of custody procedures. The evidence supports the conclusion that Edward Barzoon was the primary individual responsible, while James McCameron acted in a secondary, supporting capacity. These findings may assist further investigative action or legal proceedings.

Prepared by:

Sanjay Kumar Samala

Special Agent, Digital Forensics

ssamala3@gmu.edu

Executed on: *May 8, 2025*

Signature: sanjay kumar samala

10.Exhibits

Page No.	Exhibit ID	Description	Section
6	Exhibit 5.1	Photo - HDD Top Label (Seagate Barracuda 40GB)	Section 5
7	Exhibit 5.3	Photo - Write Blocker (WiebeTech UltraDock v5.5)	Section 5
8	Exhibit 5.4	Screenshot - Acquisition Log (FinalProject.E01.txt in FTK Imager)	Section 5
10	Exhibit 8.1	Vol3 Analysis	Section 8.1
11	Exhibit 8.1.1	Operating System Details	Section 8.1.1
12	Exhibit 8.2.1a	Screenshot - Outlook Folder Tree (Eddie)	Section 8.2.1
11	Exhibit 8.2.1b	shipment.msg email preview (Eddie to Colin)	Section 8.2.1
13	Exhibit 8.2.1c	plumbing problem & address	Section 8.2.1
14	Exhibit 8.2.1d	Screenshot - iPhones.xlsx spreadsheet with store & profit data	Section 8.2.1
14-15	Exhibit 8.2.1e	Screenshot – Jailbreak HTML (jailbreak-iphone-4[1].htm)	Section 8.2.1
15	Exhibit 8.2.1f	Screenshot – Registry key for Cydia/AppSync	Section 8.2.1
16	Exhibit 8.2.1g	Chat from desktop	Section 8.2.1
16	Exhibit 8.2.2a	Screenshot – Word Metadata (Normal.dotm) showing Jimmy as author	Section 8.2
17	Exhibit 8.2.2b	revealed a check-24.lnk	Section 8.2
18	Exhibit 8.2.2c	Screenshot - check-24 doc	Section 8.2
18	Exhibit 8.2.2d	Scanned payroll check	Section 8.2
19	Exhibit 8.2.2e	Screenshot - rasphone.pbk VPN configuration file in AppData	Section 8.2
20	Exhibit 8.2.2f	Photo of website	Section 8.2
22	Exhibit 8.4	CSAM placeholder/ adult-pornography	Section 8.4