

University of Advancing Technology

CFR 101 Evidence Chain of Custody Form

Name Keegan Heaton

Phone _____

Email Kheaton84226@uat.edu

Case number CFR101

Date 02/08/2024

Name of Persons	Evidence Name	Description	Evidence		Hash	Location	Date	Encryption
			Count(how many)	Number				
Keegan Heaton	Password for encryption	Download.jfif is a picture of a smoking gun. At the bottom of the hex code is an encryption key.	1	10110	f8d54a0847769fa962869b6c8007104d	/LogicalFileSet2/One Drive_2024-02-08 (1).zip/CFR101 CTF - Copy/memes/New folder/Dont Look Here/download.jfif	02/08/2024	None
Keegan Heaton	The plan.docx	Encrypted file of the robbers detailed plan	1	10111	4d8140df9de2e0c7b09ded03c6823881	/LogicalFileSet2/One Drive_2024-02-08 (1).zip/CFR101 CTF - Copy/Docs/The plan.docx	02/08/2024	yes

Double click in Footer to put School Name here and update logo



University of Advancing Technology

CFR 101 Evidence Chain of Custody Form

Evidence Lab and Report

1. Case CFR 101 – Bank Robbery001

a. Downloaded files and ran file through Autopsy Ver. 4.19.3

i. Date 02/08/2024

2. Found file Download.jfif on 02/08/2024



a. Location: /LogicalFileSet2/OneDrive_2024-02-08 (1).zip/CFR101 CTF - Copy/memes/New folder/Dont Look

Here/download.jfif

University of Advancing Technology

CFR 101 Evidence Chain of Custody Form

i. Date 02/08/2024

Hex										Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences	
Page: 1 of 1		Page						Go to Page: 1		Jump to Offset				Launch in HxD					
0x000017d0: 00 A5 00 81 0C E0 8A 9C 0D E2 2E 8E D4 B3 2C 41									U.v...A									
0x000017c0: 41 CF 0C 72 C7 22 AA 8C 4E 3B B9 D7 33 BA A2 5A										A..r."..N;..3..Z									
0x000017d0: A5 2D BA B9 5E D5 76 34 B3 DB C6 F1 E7 69 79 53										..-..^..v4.....iyS									
0x000017e0: 70 07 A8 28 09 38 3E EA 84 B3 E8 17 91 AB 5C F1										p..(.8>.....\.									
0x000017f0: 0C E9 F7 71 C9 64 87 6B A8 19 F6 B8 DB 71 F3 FF										...q.d.k....q..									
0x00001800: 00 5E 5B 76 3C 2A D9 3C 34 B7 5F 71 6F 7B 73 AB										..^[v<*.<4._qo{s.									
0x00001810: 45 A7 7D 3C 4D C3 86 DE 33 15 BA 65 C0 66 DD 24										E..}<M...3...e.f.\$									
0x00001820: 8E 72 37 C8 DE 3E 15 44 B5 4E E4 FD E6 3C 15 7F										..r7...>.D.N...<..									
0x00001830: D6 B0 66 AA 24 4D 46 94 A0 52 94 A0 52 94 A0 52										..f.\$MF..R..R..R									
0x00001840: 94 A0 53 26 94 A0 F4 13 52 C9 F1 A5 28 3D 04 D7										..S&....R...(<=..									
0x00001850: B4 A5 07 B5 E8 CD 29 40 C9 AF 72 69 4A 06 4D 01									)@...riJ.M.									
0x00001860: 26 94 A0 F3 26 BD C9 A5 28 19 35 E6 4F 8D 29 41										&...&...(.5.O.)A									
0x00001870: E1 CD 79 93 CA 94 A0 F0 93 5E 1C D2 94 1E 12 6A										..y.....^.....j									
0x00001880: 39 34 A5 07 AB CD 94 1E 85 80 3F 1A BA C3 74 BC										94.....?....t.									
0x00001890: FB 9B 97 A5 29 41 5A E3 F6 9E F5 15 8A 94 A0 52									)AZ.....R									
0x000018a0: 94 A0 CD 6F 1A 4A EC AD 9C 05 27 97 8E 40 A5 29									o.J....'..@.)									
0x000018b0: 41 FF D9 50 61 73 73 77 6F 72 64 31 21 0D 0A										A..Passwordl!..									

University of Advancing Technology

CFR 101 Evidence Chain of Custody Form

3. Found file The plan.docx on 02/08/2024

a. Location: /LogicalFileSet2/OneDrive_2024-02-08 (1).zip/CFR101 CTF - Copy/Docs/The plan.docx

i. Date 02/08/2024

University of Advancing Technology

CFR 101 Evidence Chain of Custody Form

The plan!

Players

Tom "The Cat" Cruse

Jerry "the mouse" Jackson

Bank robbery plan

Step 1 Go to the Bank

Step 2 Rob the Bank

Step 3 Get away with it

Step 4 or no

Bank Address

Address 1164 west UAT Tempe AZ 85001

Phone numbers

8309311819

Double click in Footer to put
here and update logo



University of Advancing Technology

CFR 101 Evidence Chain of Custody Form

Summary

On 02/08/2024, I acquired the folder “OneDrive_2024-02-08”. This file is believed to have evidence about the Robbery and the participants. Upon opening the folder with Autopsy Ver. 4.19.3, it contained a list of folders, the main folder being named “CFR101 CTF – Copy”. The “CFR101 CTF – Copy” folder contained more folders named “Docs”, “junk”, “memes”, “New folder”, and “pictures”. The “Docs” folder contained an encrypted document titled “The plan”. The file couldn’t be opened and there wasn’t any apparent password document along with it. This is one of the major artifacts found inside the file. The “junk” folder had memes. After searching each memes Hex code, there was nothing abnormal. The “memes” folder had memes, screenshots, and more folders. After searching each file in the first directory, there was nothing abnormal. In the “memes” > “New Folder” was a “Don’t Look Here” folder, which had a file named “Download.jfif” and was a JIF of a smoking gun. This was a very suspicious file and a major artifact. In the second “New Folder” was pictures of more memes. Each file in the second “New folder” was searched and had no abnormal results. The “New folder (2)” had nothing inside and “CFR101 CTF – Copy” > “New folder” had nothing as well. The folder “pictures” had nine pictures; all the pictures were about an aspect of cyber security, but all were searched, and none had any significant evidence. To access the document in the “Docs” folder, an encryption key was needed. Upon inspecting “Download.jfif”, there was an encryption key hidden in the hex code, at the very

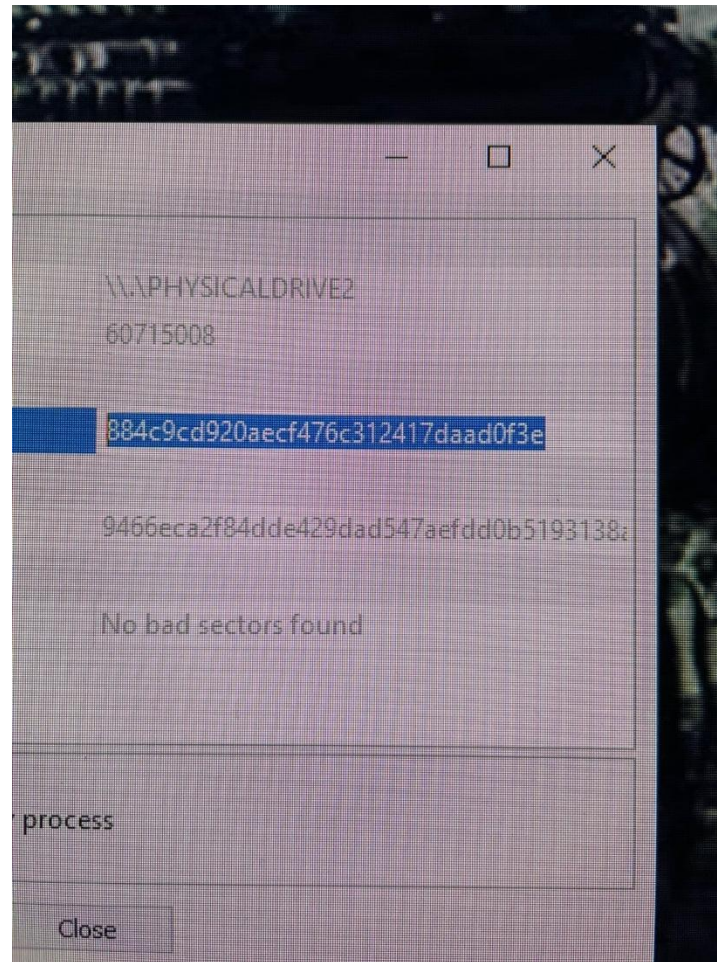
University of Advancing Technology

CFR 101 Evidence Chain of Custody Form

bottom of the code. After inputting the encryption code “Password1!”, the document detailed who was participating in the robbery and the location of the bank they would rob. The Bank Robbers planned out three steps, step 1: Go to the Bank, step 2: Rob the Bank, step 3: Get away with it. The “Players” of the Robbery were Tom “The Cat” Cruise and Jerry “The Mouse” Jackson and they planned to rob the bank on West Baseline Road, In Tempe Arizona. All findings were recorded, tagged, and reported for collection.

University of Advancing Technology

CFR 101 Evidence Chain of Custody Form



University of Advancing Technology

CFR 101 Evidence Chain of Custody Form

References:

<https://www.youtube.com/watch?v=QBRFS-fnA7I&t=2026s>

<https://www.linuxleo.com/>

[https://www.exterro.com/ftk-imager#:~:text=FTK%C2%AE%20Imager%20is%20a,\(FTK%C2%AE\)%20is%20warranted.](https://www.exterro.com/ftk-imager#:~:text=FTK%C2%AE%20Imager%20is%20a,(FTK%C2%AE)%20is%20warranted.)

<https://www.7-zip.org/download.html>