University of Advancing Technology
CFR 101 Evidence Chain of Custody Form

Name/Names	Keegan Heaton
Phone	1-800-CALL-FBI
Email	email
Case number	ATMBoA2022
Date	4/25/2024

Name of Persons	Evidence Name	Description	Evidence		Hash	Location	Date	Encryption
			Count (how many)	*Number*				
Example	able2.dd	Email associated with redhat.com, “jbj@redhat.com	1	CFR101-001	884c9cd920aec476c312417daad0f3e	E:\CFR101_LAB\able2.dd	10/17/22	MD5
JAMES	LAPTOP HI_THERE.png	a. Evidence found inside the Text of HI_THERE.png. I discovered the evidence while doing a top-down search of the entire laptop. Evidence includes the location, the route, and the tools used during the robbery. The location is the Bank of America on W Baseline, Tempe and the route was bank of America to Starbucks. Tools used include a script that changes the value of 20$ bills to 1$ bills and a USB drive.	1	CFR101-001	MD5 Hash 2fc157edaa41443b6e07db104a44f8cc SHA-256 Hash 45e1e793cc12a5f43e313340d38c873b4e4c9b91001030a1e0a0810be765ed25	/LogicalFileSet1/CFR101Final.zip/CFR101 CTF-3 Final/UnknownLaptop/C/Users/James/Desktop/Instructions/HI_THERE.png	1:50 P.M 4/18/2024	SHA-256, MD5

University of Advancing Technology
CFR 101 Evidence Chain of Custody Form

		Perpetrators exchanged four hundred for eight thousand and left for the drop off site which was the Starbucks next to UAT on W Baseline Road.						
JAMES, JOHN	iPhone Mesagesfile7.txt	Evidence found inside the text of messagesfile7.txt. I discovered the evidence while doing a top-down search of the confiscated iPhone. The text file has a password from an individual named James to John. The password to an unknown account is Strongone20.	1 of 7	CFR101-001	MD5 Hash -- 50dfd65a4bcb786462336e494f76ddae SHA-256 Hash -- 1e67c54dc79f5ed14c89fca8c0cdc355089cc1941fbd564992f3e7a5d6395ba1	/LogicalFileSet1/CFR101Final.zip/CFR101 CTF-3 Final/iPhone/Messages/messagesfile7.txt	2:13 P.M 4/18/2024	SHA-256, MD5
JAMES, JOHN	iPhone Messagesfile4.txt	Evidence found inside the text of messagefile4.txt. The evidence was discovered while analyzing the Messages directory. The textfile is a conversation between James and John, bringing both individuals to the drop off location of the robbery.	2 of 7	CFR101-001	MD5 Hash 6edb7aea44d126bddf4f766800d362ee SHA-256 Hash 76689fe2febe28566ccb6832b2d7e21f71bfad0b5699efbf52ba2ff2ec237219	/LogicalFileSet1/CFR101Final.zip/CFR101 CTF-3 Final/iPhone/Messages/messagesfile4.txt	2:20 P.M 4/18/2024	SHA-256, MD5
JAMES, UBER DRIVER	iPhone Messagesfile3.txt	Evidence found inside the text of messagefile3.txt. The file was discovered inside the Messages directory. The textfile gives the apartment number and location of	3 of 7	CFR101-001	MD5 Hash def6af974ffacbab94a815e4cb5128ac	/LogicalFileSet1/CFR101Final.zip/CFR101 CTF-3 Final/iPhone/	2:32 P.M 4/18/2024	SHA-256, MD5

University of Advancing Technology
CFR 101 Evidence Chain of Custody Form

		James house. The location being 2625 W baseline road, Tempe, AZ, 85283, room 909.			SHA-256 Hash c9aa6a4eeae951f2457a6bb4e2076a38ac272bd0889db71f6457e4c856ea9f56	Messages/messagesfile3.txt		
JAMES, MARY	iPhone Messagesfile1.txt	Evidence found inside the text of messagefile1.txt while analyzing the Messages directory. The textfile is a conversation between James and Marry. James wants Mary back, but Mary wants money, which James doesn't have. Mary blocks James because he is broke. The conversation gives the motive behind the ATM robberies.	4 of 7	CFR101-001	MD5 Hash 1951a3ddfb9aad443d37f019eb364f1e SHA-256 Hash 22eabfd2c41f5ebb0567d2935582c496ac8dc604b2740cc1142678e26b61778c	/LogicalFileSet1/CFR101Final.zip/CFR101 CTF-3 Final/iPhone/Messages/messagesfile1.txt	2:36 P.M 4/18/2024	SHA-256, MD5
JAMES	TABLET Nothing.txt	Evidence found inside the text of Nothing.txt. The evidence was discovered during the top-down analysis of the tablet. The evidence is a string with unknown relevance. The string is PTPX7-N4M62-232PB-QKT4P-76GYC	1	CFR101-001	MD5 Hash 3bf336850920309c946d5e4b19b7672d SHA-256 Hash 3d6b5af1f672916552be21fa088feba37d249d0a21a4933d71def305b6cac225	/LogicalFileSet1/CFR101Final.zip/CFR101 CTF-3 Final/tablet/C/Users/Guest/Nothing.txt	2:36 P.M 4/18/2024	SHA-256, MD5
JAMES	LAPTOP Jackpotting.ty	Evidence found inside the James User account, hidden inside the document directory. The .py file is a	1	CFR101-001	MD5 Hash 76123af76d838bf031d6e9226d3c4ba3	File Path /LogicalFileSet1/CFR101Final.z	2:10 P.M 4/25/2024	MD5

University of Advancing Technology
CFR 101 Evidence Chain of Custody Form

		computerkiller in disquise, the program was referenced inside the HI_THERE.png.				ip/CFR101 CTF-3 Final/UnknownLaptop/C/Users/James/Documents/New folder/jackpotting.py		
BRANDON, KYLE	LAPTOP, TABLET ComputerKiller.py	Evidence found in multiple locations. One was found on BRANDON's account on the desktop, and another was found on KYLE's account on the tablet. ComputerKiller.py installs itself in startup folders and slowly destroys the computer.	2	CFR101-001	BRANDON MD5 Hash 50d1aed1129a5805a979df627ff951de KYLE MD5 Hash 50d1aed1129a5805a979df627ff951de	BRANDON File Path /LogicalFileSet1/CFR101Final.zip/CFR101 CTF-3 Final/UnknownLaptop/C/Users/Brandon/Desktop/New folder/ComputerKiller.py KYLE File Path /LogicalFileSet1/CFR101Final.zip/CFR101 CTF-3 Final/tablet/C/Users/Kyle/Desktop/New folder/ComputerKiller.py	2:15 P.M 4/25/2024	MD5

University of Advancing Technology
CFR 101 Evidence Chain of Custody Form

JAMES	James1.jfif, James2.jfif, James3.jfif	Evidence found inside James user account, inside the Pictures directory. The evidence was found while doing a top-down analysis of the laptop. The evidence is a picture of James committing the robbery. He is in striped black and white clothing with a gun.	3	CFR101-001	James1 MD5 Hash 9b0364ebcd8aa98902e7c9a9717bbd68 James2 MD5 Hash e915dd73e3bf4cd4689a8e5e8c139498 James3 MD5 Hash 29bb95b3924de32776fb419042e1cfca	**James1 Location** /LogicalFileSet1/CFR101Final.zip/CFR101 CTF-3 Final/UnknownLaptop/C/Users/James/Pictures/james1.jfif **James2 Location** /LogicalFileSet1/CFR101Final.zip/CFR101 CTF-3 Final/UnknownLaptop/C/Users/James/Pictures/James2.jfif **James3**	2:20 P.M 4/25/2024	

University of Advancing Technology
CFR 101 Evidence Chain of Custody Form

						Location /LogicalFileSet1/CFR101Final.zip/CFR101 CTF-3 Final/UnknownLaptop/C/Users/James/Pictures/james3.jfif		
JOHN	John1.jfif	Evidence found in James user account, inside the Pictures directory. The evidence was found while doing a top-down analysis of the laptop. John1.jfif is a picture of john with handcuffs, wearing an orange shirt with no disguise.	1	CFR101-001	MD5 Hash edb8292a801b2a5912c4e80e2541b15a	Location /LogicalFileSet1/CFR101Final.zip/CFR101 CTF-3 Final/UnknownLaptop/C/Users/James/Pictures/John1.jfif	2:20 P.M 4/25/2024	MD5

University of Advancing Technology
CFR 101 Evidence Chain of Custody Form

Evidence Lab and Report

University of Advancing Technology
CFR 101 Evidence Chain of Custody Form