CSCI: 6638-01: Small Scale Digital Forensics

**Final Week Final Project: Puttin on the Ritz**

TC/MV

Contents

[Executive Summary 3](#_Toc148009436)

[Evidence 3](#_Toc148009437)

[Paper Purpose 4](#_Toc148009438)

[Tools 4](#_Toc148009439)

[Laboratory Procedures 4](#_Toc148009440)

[Build Info 4](#_Toc148009441)

[SMS/MMS Messages 6](#_Toc148009442)

[Accounts Associated with Device 7](#_Toc148009443)

[Calendar Information 8](#_Toc148009444)

[Wi-Fi Information 8](#_Toc148009445)

[Time Zone information 12](#_Toc148009446)

[Photos Found on Device 12](#_Toc148009447)

[Application Downloads on Device 13](#_Toc148009448)

[Contacts On Device 13](#_Toc148009449)

[Findings 14](#_Toc148009450)

[Conclusions and Recommendations 15](#_Toc148009451)

[Problem Solving/ Troubleshooting 16](#_Toc148009452)

# Executive Summary

Investigators are tasked with looking into a case with foreign relations and to prove the accused did in fact have intention to “embarrass” America. Alex the wealthy businessman has agreed to carry through with sending ‘tourists’ to the museum. The person Carry, who is working with Alex has to devise a plan in order to get them into the museum with tools to damage the work. The investigation was tasked with determining evidence to determine which suspects are responsible and if carry has any evidence looping it back to her orchestrating all of this. This will be done by searching through the files and devices associated with Tracy, Pat, Joe, Alex, Carry, and Terry.

# Evidence

Breakdown of all information found via manual search through autopsy, notepad++, SQLDBrowser, and windows filesystem/cmd manual search

# Paper Purpose

This papers purpose is to provide the current evidence to corroborate the criminal involvement between the suspects in order to prove that one is at fault this paper will highlight certain evidence that corroborate towards any of the suspects and outline the following paths and procedure taken to acquire the evidence as to be easily replicated when necessary.

# Tools

* Virtual Box: Virtual Windows 11 OS, 12GB RAM s, Version: WinDev2309Eval
* Host Computer: Windows 10 OS, 16GB RAM, Version: 22H2
* Windows CMD
* Windows Filesystem
* DB Browser (SQLite)
* Notepad ++
* Andriller
* ALEAPP
* IOSleapp

# Laboratory Procedures

Carry tablet Data Extraction

* First being with navigating towards the file for the table system titled “carr-tablet-2012-07-16-final” this is to be extracted to the respective folder with the same name. Once file has been extracted begin to work on locating evidence
* To begin start by searching the systems sdcard associated with the tablet, navigate towards file path “ carr-taablet-2012-07-16-final.tar/mnt/sdcard/Download” evidence has been found of a museum brochure from the same Museum as the picture on terry’s phone (pictured in next section)
* A person with curly hair

  Description automatically generated
* Scrolling through this image you can also see the map attached proving to be useful information for someone who would be breaking and entering to deface certain art A screenshot of a computer screen

  Description automatically generated
* Within the same folder path you can find the file titled “securedownload-1.pdf” this file contains the security personal schedule describing when certain shifts will begin and end for each set of security teams
* A document with text on it

  Description automatically generated
* A building with trees in front of it

  Description automatically generatedFollowing this investigators further researched other images stored on the device to place carry physically in Washington and found was Bethesda bagels this is a bagel chain within Washington DC with physical address being 120 M St SE, Washington, DC 20003
* Further investigation led to the path carry-tablet-2012-07-16-final.tar/mnt/sdcard/supernote/100 this reveals the note 1\_00 which discusses a plan and a certain frequency to be on specifically this should be noted as the security operate at a specific frequency as well, pictured below text information from file.
* A screenshot of a computer

  Description automatically generated

Tracy-Phone Logical

* Navigate back to the root folder where each of the files is contained within this folder there is a zip file with the title “Tracy-Phone\_Logical\_2021-07-15-1317” within this folder there is the DCIM folder click on this to reveal the following
* A screenshot of a computer

  Description automatically generated
* This is the photos associated on the device path taken Desktop \Tracy-phone-logical-2012-07-15-1317.zip\Tracy-Phone-Logical-2012-07-15-1317\DCIM\800AAAAA
* File on interest contains the national gallery of art sculpture garden the place in question is in fact located in Washington DC and is in the museum.
* A wall with text on it

  Description automatically generated
* The physical address of this location is Constitution Ave NW &, 7th St NW, Washington, DC 20408 which can put the person at this address at the time of the image.
* Some other items of note within Tracys phone photo library are found within the IMG\_0057.JPG file with a US local post stamp this stamp upon further research is worth $325 USD \*Pictured underneath original stamp, which begs the question why many pictures of “collectable stamps”. Brings the question why they would need these are they bribing postal authorities to ship tools for the defacing of museum property. A close up of a label

  Description automatically generated
* A yellow post stamp with red writing

  Description automatically generated
* Following this there is multiple items

# Findings

File Paths for Requested Search

# Conclusions and Recommendations

To conclude,

# Problem Solving/ Troubleshooting

No issues