CSCI: 6638-01: Small Scale Digital Forensics

**Week # 7 Midterm: Capture the Flag**

TC

MV

EM

RK

KCD

Contents

[Executive Summary 2](#_Toc148954403)

[Evidence 3](#_Toc148954404)

[Paper Purpose 3](#_Toc148954405)

[Tools 3](#_Toc148954406)

[Laboratory Procedures 3](#_Toc148954407)

[Findings 3](#_Toc148954408)

[Conclusions and Recommendations 3](#_Toc148954409)

[Problem Solving/ Troubleshooting 3](#_Toc148954410)

# Executive Summary

Assigned with doing a filesystem analysis on the IOS and Android platform for retrieval of information pertaining to the capture the flag experiment. This would entail the investigator to retrieve IOS information pertaining to users full name, phone number, email address, phone model, software version, devices connected, car play instances, last time phone was unlocked, number of times phone was plugged in, applications installed on device, users signal code, Facebook friend request sent, highest number of culminative steps taken by the user in one day, users weight, Debts to be paid by user, location user was located near, messages between user and contacts, personal information including google calendar and Gmail account, and lastly the users follower interest specifically the lacrosse team. For the android device the required information entails wi-fi networks connected to, name of taco truck and type of tacos being served, the countries the phone was located within, the username and person who asked user to join Kik messaging platform, YouTube history, and the google business account information associated with the device.

# Evidence

# Paper Purpose

No paper was utilized in this lab.

# 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 ++
* ALEAPP For android, Andriller
* IOSLEAPP

# Laboratory Procedures

* Beginning the lab, the investigator booted up the windows virtual machine to ensure the most

# Findings

File Paths for Requested Search

# Conclusions and Recommendations

# Problem Solving/ Troubleshooting