CSCI: 6638-01: Small Scale Digital Forensics

**Week # 8 Google Takeout Lab: CTF**

TC

Contents

[Executive Summary 3](#_Toc149820092)

[Evidence 3](#_Toc149820093)

[Paper Purpose 3](#_Toc149820094)

[Tools 4](#_Toc149820095)

[Laboratory Procedures 4](#_Toc149820096)

[YouTube Subscriptions 4](#_Toc149820097)

[Users Watch History 4](#_Toc149820098)

[User Information (email, name, and gender) 5](#_Toc149820099)

[Video Game User Plays 5](#_Toc149820100)

[Podcasts 6](#_Toc149820101)

[Devices Associated with Account 7](#_Toc149820102)

[User Location 8](#_Toc149820103)

[Twitter Account Details 11](#_Toc149820104)

[Feb 17th Location 12](#_Toc149820105)

[Browser User was Discussing 12](#_Toc149820106)

[Last Data Connection to Device 12](#_Toc149820107)

[Address Near Pier and Nearby Locations 12](#_Toc149820108)

[Bypass Intentions 14](#_Toc149820109)

[Favorite Physical Activities 18](#_Toc149820110)

[Champlain Visits 21](#_Toc149820111)

[Conclusions and Recommendations 23](#_Toc149820112)

[Problem Solving/ Troubleshooting 23](#_Toc149820113)

# Executive Summary

Assigned with doing a filesystem analysis on the IOS platform investigators were tasked with locating the following items. Subscriptions to any YouTube channels, video created by John Hammond that the user had watched (date and time), users full name, email, gender, video games the user plays, podcast subscriptions, number of deices that the user has, physical location of the user and address, Twitter username, specific browser visited by user, event report for February 17th, phones last data connection(IP address), what is the address by the pier where is it close to, what was user trying to bypass, physical activities user enjoys, and number of times Champlain college has been visited and dates associated.

# Evidence

* Users’ subscriptions: PythonMC
* Users Watch History OF John Hammond: 4 times user watched “Minecraft VULNERABLE! (and SO MUCH MORE)"
* Users Name: Ragel Shell, email: ragaelshell1124@gmail.com, gender: male
* Game User plays: Minecraft
* Podcasts User is Subscribed to: Critical Role
* Devices: Mobile phone Pixel 3 running android OS version 9, PC that runs the OS Linux, and PC that runs OS Windows 10
* User Location: Sugarbush Resort, 102 Forest Dr, Warren, VT 05674
* Twitter Account Name: @RafaelShell2
* Feb 17: User is going to New Vegas show on the 17th
* Browser User Downloads: Mozilla Firefox
* Last Data Connection: Date: Feb 9th 2022, Time: 9:33:34 PM, IP: 184.171.159.212
* Address user requested for pier: 1 Maple Street Burlington Vermont, Near Perkins Pier
* Bypass intentions: Wanted to bypass windows hash code by using john the ripper, bypass remote desktop safety to exploit it for remote control over targets computers.
* Disable windows defender, wanted to exploit the La4 java script error within Minecraft to take control over a server,
* The users favorite physical activities: Biking, Skiing/Snowboarding, and LARPing(Live Action Role Playing)
* Champlain Visits: Tue, 25 Jan 2022 17:01:08 -0500 (EST)/ Tue, 1 Feb 2022 19:26:23 -0500 (EST)/ Sun, 6 Feb 2022 14:52:43 -0500 (EST)/ Sat, 12 Feb 2022 16:05:43 -0500 (EST)/ Fri, 28 Jan 2022 21:55:17 -0500 (EST), for a grand total of 5 visits to the college.

# Paper Purpose

To prove and find the items listed above in the introduction and display them in an easy to recreate understandable “How To” format, while displaying all information deemed important to the task.

# Tools

* Virtual Box: Virtual Windows 11 OS, 12GB RAM s, Version: WinDev2309Eval
* Host Computer: Windows 10 OS, 16GB RAM, Version: 22H2
* Laptop: Acer Predator Helios 300, Windows 10 OS, 16 GB RAM, Version: 22H2
* Windows CMD
* Windows Filesystem
* DB Browser (SQLite)
* Notepad ++
* Google Earth

# Laboratory Procedures

* Beginning the lab, the investigator booted up the windows virtual machine to ensure the most security when working on the documentation containing it within an isolated environment.
* Once located in isolated environment begin to work towards navigate to gather the required information as stated in the task.
* This will be assuming that you have saved the file to your desktop and therefore the file path will always start with C:/Users/\*name\*/desktop/takeout-20220222T154448Z/Takeout

## YouTube Subscriptions

* Start first by navigating to the location in which you extracted the data from the zip file in which case you can navigate to the folder once the zip file is extracted to find the first item look at the YouTube Subscriptions list and there you will find a csv file that contains one subscription to PyhtonMC
* A screenshot of a computer

  Description automatically generated

## Users Watch History

* Following this navigate towards YouTube watch history to find the John Hammond titled video the user had watched the video titled “Minecraft VULNERABLE! (and SO MUCH MORE)” user had watched this video a total of 4 timesA screenshot of a computer

  Description automatically generated

## User Information (email, name, and gender)

* Next navigate towards the parent folder Takeout to find the folder titled “Profile” open this folder up to reveal the profile.json file and open it within notepad++.
* A screenshot of a computer screen

  Description automatically generated
* Users name is Rafel Shell, his email is known as [rafaelshell1124@gmail.com](mailto:rafaelshell1124@gmail.com), and his gender is male.

## Video Game User Plays

* Once done within this folder navigate back to the parent folder of Takeout and look for the video games the user seems to be playing, investigator found through YouTube watch history the user enjoys playing Minecraft as his YouTube watch history solidifies it.
* A screenshot of a video chat

  Description automatically generated

## Podcasts

* To find out what podcast the user is listening to navigate back to the parent fold “Takeout” and then click on my activity this will then lead you to Podcasts folder containing the MyActivcity.html document.
* A screenshot of a computer

  Description automatically generated
* Within this folder once file clicked website will open displaying the following informationA screenshot of a web page

  Description automatically generated

## Devices Associated with Account

* To locate the devices user has, the first device can be found via the path Takeout/Google Play Store/Devices.json
* A screenshot of a computer

  Description automatically generated
* To find the other devices that are associated with the account navigate to the path Takeout/Access Log Activity/Devices- A list of Devices…csv this will reveal the devices associated with the user to be Mobile phone Pixel 3 running android OS version 9, PC that runs the OS Linux, and PC that runs OS Windows 10
* A screenshot of a computer

  Description automatically generated

## User Location

* The user location can be found via some extra work investigator navigated via the path Takeout/Fit/Daily activity metrics/2022-02-12.csv this will reveal a list of the users fit analytics but will also reveal a set of coordinates navigating through multiple files I search for the common latitude and longitude to show up that points to the same house, lat: 44.478145 Longitude: -73.2133 A screenshot of a computer

  Description automatically generated
* This when plugged into google earth will reveal an apartment building (pictured below)A screenshot of a phone

  Description automatically generated
* A screenshot of a google maps

  Description automatically generated
* Looking further into the files if you navigate back to the Takeout/Fit/2022-01-30.csv file you can see more latitude and longitude data, this points in the direction of two potential points of a user location as all activity data is from around this location.
* A screenshot of a cell phone

  Description automatically generated
* A map of a house with a road and a road

  Description automatically generated
* Lastly is the following which seems to most likely be the users house located Latitude: 44.14157104 Longitude: 72.89542389
* A aerial view of a house and trees

  Description automatically generated
* This area is around Sugarbush Resort, 102 Forest Dr, Warren, VT 05674 found by the path Takeout/MyActivity/Maps/MyActivity.html

## Twitter Account Details

* The twitter account that is associated with the device is @RafaelShell2 this can be found via the path Takeout/Mail/All mail Including Spam and Trash.mbox and right clicking to edit with notepad+
* A computer code with numbers and symbols

  Description automatically generated

## Feb 17th Location

* The location here the user is going Feb. 17 can be found by taking the following path to the keep folder Takeout/Keep/2022-02-13T03\_21\_04.819-05\_00.json top find that the user is attending a show in New Vegas and needs a flight.
* A screenshot of a computer

  Description automatically generated

## Browser User was Discussing

* To find the browser that the user was discussing look into the path Takeout/My Activity/GoogleAnalytics/MyActivity.html to find a download the user visiting firefoxs website to download the browser navigating through google chrome to downloaded mozilla firefox
* A black and white text

  Description automatically generated

## Last Data Connection to Device

* To find the last data connection on the device navigate toward the path Takeout\Android Device Configuration Service to find the last connection was on Feb 9 2022, at 9:33:34 PM UTC, from IP Address 184.171.159.212
* A white background with black text

  Description automatically generated

## Address Near Pier and Nearby Locations

* The address the user requested for the pier can be found by navigating to Takeout/My Activity/ Discover/MyActivity.html this will reveal a list of searches the user made specifically the ones with Weather at Location
* A screenshot of a map

  Description automatically generated
* Upon closer inspection this is Burlington Vermont 05401 and the pier that is close to this is Burlington Fishing Pier or the Perkins Pier which is the closest to the coordinates listed in the picture below. Location also being 1 Maple Street found via the following path Taketout/MyActivcity/Maps/MYActivity.html
* A screenshot of a computer

  Description automatically generated

## Bypass Intentions

* Navigate to Takeout/My Activity/Search/MyActicity.html to reveal the users intentions of bypassing the following web searches that have the user interested in using john the ripper to crack Microsoft passwords, the user also has search of disabling windows defender through PowerShell and utilizing exploit within the remote desktop framework Microsoft has to launch attacks.
* A screenshot of a computer

  Description automatically generated
* A screenshot of a web page

  Description automatically generated
* A screenshot of a computer

  Description automatically generated
* A screenshot of a search engine

  Description automatically generated
* The user also seems to be quite interested in bypassing the server security within the video game Minecraft, this can also be seen through the users search history and the bookmarked website.
* A screenshot of a computer

  Description automatically generated
* A screenshot of a computer

  Description automatically generated
* This website being a tutorial on how to hack Minecraft servers using an exploit within the java logging system Log4Shell.
* A screenshot of a computer

  Description automatically generated

## Favorite Physical Activities

* To find the sporting activity that the user enjoys doing navigate to the path Takeout/Fit/Activities and investigate any of the files listed by right clicking them to edit with notepad++ to view that Biking is the users favorite physical activity.
* A screenshot of a computer

  Description automatically generated
* Along with this located from the path Takeout/Google Play Store/Library.json displays an All Trails hiking app along with a snowboard skiing appA screenshot of a computer code

  Description automatically generated
* The last physical activity can be found by looking through the chrome browser history and brief research from the investigator of “LARP” multiple searches with LARP are logges with techniques, shield builds, and other general searches. This is Live Action RolePlayin and is considered another physical activity path take is Takeout/Chrom/BroswerHistory.json

## Champlain Visits

* A screenshot of a computer

  Description automatically generated
* The user data on champlain college can be found by navigating to the location of the mail Takeout/Mail/All mail Including Spam and Trash.mbox and crtl+ f to look for champlain to reveal the guest Wi-Fi networks and how many times user connected first date Tue, 25 Jan 2022 17:01:08 -0500 (EST), Tue, 1 Feb 2022 19:26:23 -0500 (EST), Sun, 6 Feb 2022 14:52:43 -0500 (EST), Sat, 12 Feb 2022 16:05:43 -0500 (EST), Fri, 28 Jan 2022 21:55:17 -0500 (EST), for a grand total of 5 visits to the college.
* A screenshot of a computer

  Description automatically generated
* A screenshot of a computer

  Description automatically generated
* A screenshot of a computer screen

  Description automatically generated
* A screenshot of a computer code

  Description automatically generated

# Conclusions and Recommendations

To conclude, each of the required tasks was accomplished by being able to locate and find the correct information for the requested services. A conclusion about the user can be made that he has intentions on bypassing multiple security breaches is a vulnerability researcher and exploiter. We can see that he either has malicious intentions or is trying to take preventative measures for himself in this situation. This takeout image of user’s phone shows that some sort of misconduct should be going on especially or it can be assumed that this is just a penetration tester that is researching and staying on top of what vulnerabilities to expect in the field. However final thoughts are that the user has malicious intent towards the Microsoft, java, and other platforms as multiple web searches and other articles are found that explicitly determine how to hack the listed above and how to exploit these vulnerabilities. No searches are based on protecting against these vulnerabilities leading to my conclusion the user had malicious intent to hack Minecraft servers and windows computers.

# Problem Solving/ Troubleshooting

No issues with the set-up and successful processing of the data, however the only item that required more effort than searching through file structures. For the user’s location extra effort was needed by searching latitude and longitude within google earth in order to find the users location or what could lead to the location as the last step was found within the maps section of the users google takeout file showing them to be visiting Vermont at the Sugarbush Resort.