Assignment 4 Scenario: Team Rocket

FTK 1.8 will not work for this assignment (over 5,000 files). You must use Autopsy or another option.

Questions:

1. What user account is related to SID 1004?

TeamRocket

1. What is the email account associated with this user account?

[James39933@outlook.com](mailto:James39933@outlook.com)

1. What is the Make of a USB drive that was connected to this device?

Alcor Micro Corp.

Internet:

1. What search term(s) were used on FireFox?

“How to get on the dark web”

1. List (2) Chrome bookmarks and (2) Firefox bookmarks.

Chrome:  
<https://connect.secure.wellsfargo.com/auth/login/present>   
<https://secure.bankofamerica.com/login/sign-in/signONV2Screen.go>

Firefox:  
<https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html>   
<https://mozilla.org/en-US/about/>

1. What file was downloaded at 08:08:34 on 11 Apr 2021?

TunnelBear-Installer.exe

Recycle Bin

1. What time was Motto.txt deleted?

2021-04-11 08:29:36 PST

Regex

1. Locate and export a suspicious Office document. Who authored this document?

Target List 1.xlsx – Author: Meowth Created on 4/11/2021 8:49:05 PST.

1. Review the bank accounts. Write a regular expression to locate additional accounts based on account number patterns.

Bank Of America: ([a-z]+[0-9]{5}+-[0-9]{6})

([a-z]+[0-9]{3}+-[0-9]{3}+[a-z])

Prefetch

1. Locate the prefetch file for “Protonvpn.exe” What is the number of executions and what is the date/time for the first execution?

3 Executions. First Execution: 2021-04-11 08:30:50 PST