Mission Name

DataCardForensics

History Background

Claire found Ethan at Skytech, interrogating to a suspected information trader on the black market. The suspect (SkytechMole named Anderson) is connected, and Claire acquire his datacard.

Technical High-Level Overview

A file system is provided that is linked to a memory module within the datacard. The aim is to get a location, in this case in South America (Paraguay).
Player will have to analyse datacard filesystem in order to find out two parameters: latitude and longitude. These parameters can be found inside a picture of Asuncion (Paraguay).

Short Description

You´re going to analyse Skytech Mole´s datacard, your goal is to find a location in terms of latitude and longitude.

Mission Description

A file system is provided that is linked to a memory module within the datacard. You´re going to analyse this Skytech Mole´s datacard and your goal is to find a location in terms of latitude and longitude.

Location

SYLVARCON | SKYTECH HQ

Tools

- Arsenal image mounter
- exiftool

Questions

Which is the header of the picture that you have located? Please insert the whole header in HEX

- FFD8FFE000104A464946000101000001

Which was the software used to store the picture before the datacard?

- Picasa

Which was the last month that Anderson Vegas received the vaccine?

- July

Hints

1. Mount the Encase image E01 using Arsenal Image Mounter
2. Locate pictures from Paraguay.
3. Use Exiftool analyse picture and extract coordinates.

Write Up

Linux Method: - root required

https://www.andreafortuna.org/2018/04/11/how-to-mount-an-ewf-image-file-e01-on-linux/

- apt install ewf-tools
- mkdir rawimage
- ewfmount IMAGE.E01 ./rawimage/
- mkdir mountpoint
- mount rawimage/ewf1 mountpoint
- apt install exiftool

exiftool

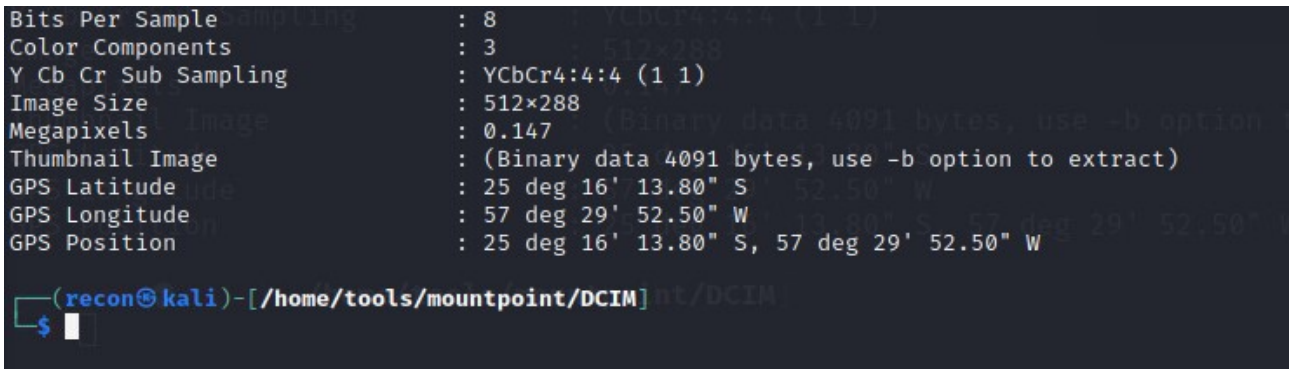

Figure 1

Windows Method:

First of all, player should mount the E01 image to access filesystem, using Arsenal Image Mounter:

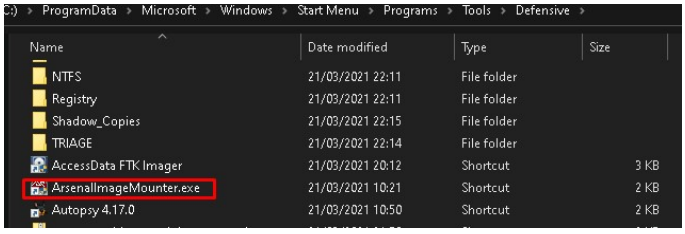

Figure 2

Then select “Mount Disk image file”

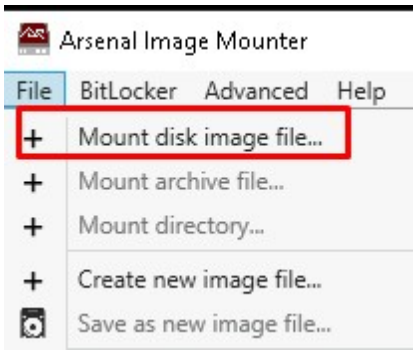

Figure 3

And finally select “Read only disk device” and press “ok”:

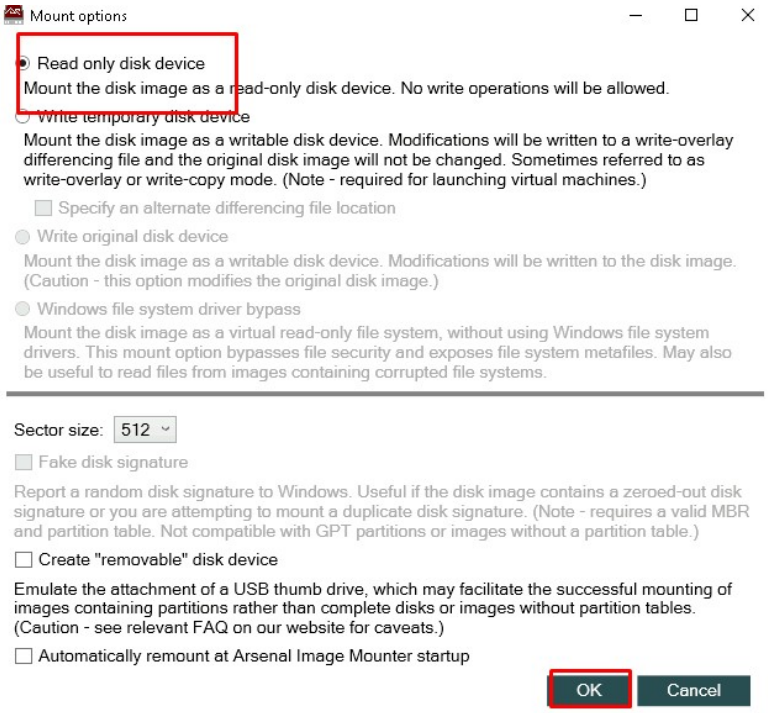

Figure 4

Your system will have mounted the evidence like this:

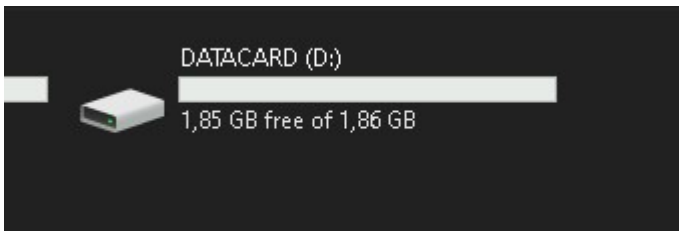

Figure 5

Player must analyse folders to get a latitude and a longitude. These parameters are usually found inside pictures as metadata.

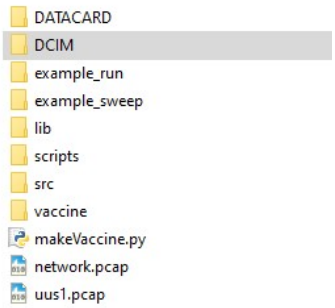

Figure 6

Once player has found folder called DCIM, he can identify three pictures, but one of them has GPS coordinates:

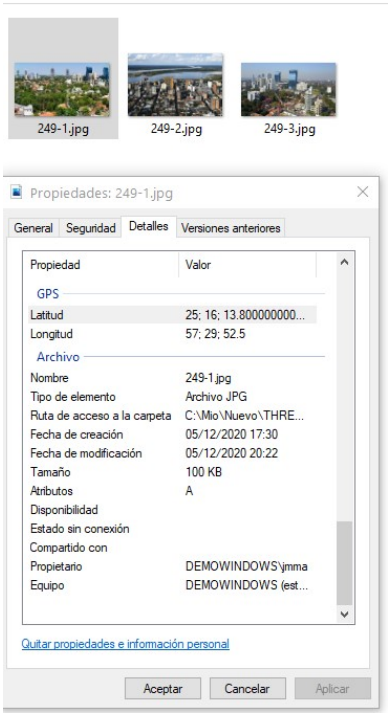

Figure 7

And finally, player will able to get latitude and longitude with ExifTool:

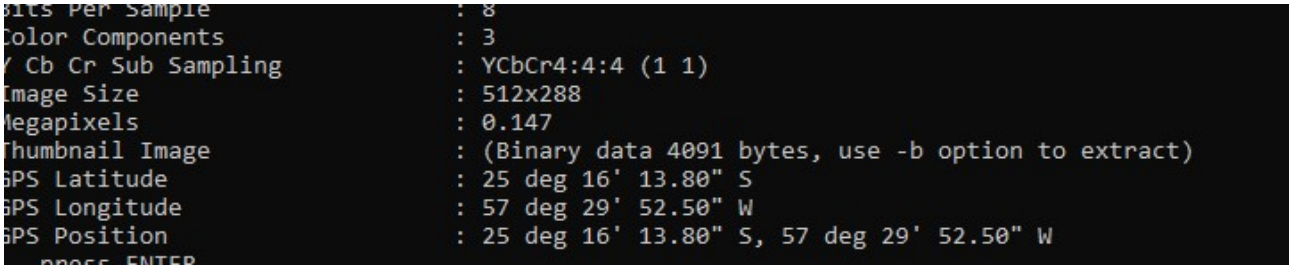

Figure 8

Latitude: 25 deg 16' 13.80" S
Longitude: 57 deg 29' 52.50" W

Flag Information

flag{Latitude: 25 deg 16' 13.80" S | Longitude: 57 deg 29' 52.50" W}