Practical case statement

Before addressing this forensic investigation, Autopsy tool should be installed.

Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. (http://www.sleuthkit.org/autopsy/)

The general way to install and execute the tool is described below:

Windows: http://www.sleuthkit.org/autopsy/download.php

a. Install

b. Open the application

Linux and Mac: http://www.sleuthkit.org/autopsy/v2/download.php

a. Download the file

b. Decompress and compile

c. Execute ./autopsy

d. Open a browser http://localhost:9999/29026328457131899 3/autopsy

Scenario

Marcus, 26, was arrested yesterday on charges of selling illegal drugs to high school students. A local police officer posed as a high school student was approached by Marcus in the parking lot of Smith Hill High School. Marcus asked the undercover cop if he would like to buy some marijuana. Before the undercover cop could answer, Marcus pulled some out of his pocket and showed it to the officer. Marcus said to the officer "Look at this stuff, Colombians couldn't grow it better! My supplier not only sells it direct to me, he grows it himself."

Marcus has been seen on numerous occasions hanging out at various local high school parking lots around 2:30pm, the time school usually ends for the day. School officials from multiple high schools have called the police regarding Marcus's

presence at their school and noted an increase in drug use among students, since his arrival.

The police need your help. They want to try and determine if Marcus has been selling drugs to students at other schools besides Smith Hill. The problem is no students will come forward and help the police. Based on Marcus's comment regarding the Colombians, the police are interested in finding Marcus's supplier/producer of marijuana.

Marcus has denied selling drugs at any other school besides Smith Hill and refuses to provide the police with the name of his drug supplier/producer. Marcus also refuses to validate the statement that he made to the undercover officer right before his arrest. Upon issuing a search warrant and searching of the suspect's house the police were able to obtain a small amount of marijuana. The police also seized a USB device, but no computer and/or other media was present in the house.

The police have imaged the suspect's USB and have provided you with a copy. They would like you to examine the USB and provide answers to the following questions. The police would like you to pay special attention to any information that might prove that Marcus was in fact selling drugs at other high schools besides Smith Hill. They would also like you to try and determine if possible who Marcus's supplier is.

Marcus posted bail set at $20,000.00. Afraid he may skip town, the police would like to get him locked up as soon as possible. To do so, the police have asked that you have the results fully completed and submitted within 3 days. Please provide the police with a strong case consisting of your specific findings related to the questions, where the findings are located on the disk, processes and techniques used, and any actions that the suspect may have taken to intentionally delete, hide and/or alter data on the USB. Good Luck!

Any names, locations, and situations presented are completely made up. Any resemblance to any name, locations and/or situation is purely coincidence.

Objetive

Your mission is to analyse a recovered USB device and answer the questions below. The dd image of the recovered USB device can be downloaded using the following link:

http://www.honeynet.onofri.org/scans/scan24/image.zip

MD5 (image.zip) = b676147f63923e1f428131d59b1d6a72

Note: *the integrity of the download file should be checked.*
Note: *If the zip file does not open for you, please use this alternative source instead: https://www.honeynet.onofri.org/scans/scan24/sol/carrier/index.html*

Questions:

1. Who is Marcus's supplier of marijuana and what is the address listed for the supplier?
2. What crucial data is available within the coverpage.jpg file and why is this data crucial?
3. What (if any) other high schools besides Smith Hill does Marcus frequent?
4. For each file, what processes were taken by the suspect to mask them from others?
5. What processes did you (the investigator) use to successfully examine the entire contents of each file?

Your answers:

Please provide answers to these questions at:
https://acehacker.com/microsoft/cybersecurity/assignment2.html