Due: 04/23/2025 11:59 PM

CIS-484-50-4252 Project 4

Scenario:
You are a digital forensic examiner working for the Louisville Metro Police Department. A drug enforcement team has been after a suspected drug dealer, Perry Winkler, for several months. After finally obtaining a warrant to search Mr. Winkler's residence, LMPD arrives at the residence only to find an abandoned home. A first response team scours the home for any evidence as to Mr. Winkler's whereabouts, but the residence has been cleared of any useful evidence. After searching the dumpster outside the residence, a desktop PC is located and recovered. The desktop tower had been damaged – possibly in an attempt to render the data from the computer unreadable – but the hard drive is luckily intact. The hard drive from the computer is imaged using forensically sound measures and turned over to you in order to conduct a digital forensic examination. The lead investigator believes that the key to Mr. Winkler's whereabouts lies somewhere in the data collected from the computer. You are tasked with determining answers to the following questions regarding the computer recovered from the dumpster:

1. What identifying information did you find on the hard drive to help determine the owner or user of the computer? Does the computer appear to have used by Perry Winkler?
2. Is there any evidence on the computer that the user may have been associated with drugs or other illegal activities?
3. Is there any evidence that the user may have been trying to cover their tracks or delete evidence from the computer?
4. Can you identify any additional items (such as USB devices) that may contain pertinent evidence? If so, what are they? Include as much identifying information about each device as possible.
5. Is there any evidence on the computer that the user may have been planning to go on the run? If so, can you determine where the user was planning to go?
    a. If the user was planning to run, is there evidence that anyone might be traveling with them? If so, can you determine the identity of the accomplice(s)?
6. What other evidence did you locate on the computer that may assist LMPD in its investigation (e.g. files that point to additional leads, accomplices, or any other activity not targeted by the initial investigation)?

<u>It's very important to identify the basis for your answers to the above questions.</u> Since you may be called on to testify regarding your findings, you need to be sure that your opinions and the answers to the questions above are based on a sound forensic examination. For example, if you found a particular piece of information in the registry, be sure to note the registry hive where you found the information, the specific subkey/value of interest, and why it's important. It is highly recommended that you revisit the Windows artifacts class recordings and PowerPoints, as you will need to use nearly all the skills and artifacts discussed to fully complete this project.

Project Guidelines

- ***Submit a written report of your findings via Blackboard, highlighting the methodology and steps used during the forensic examination (including tools used), the answers to the above questions, and the evidence you uncovered to support your findings (e.g. file names and paths, specific registry keys/values, timestamps embedded in particular artifacts, etc.).***

- Your written report should be a **maximum** 20 written pages and should cover the following:
  - Your answer to each question
  - Details regarding the evidence that supports each answer (i.e. where you located your answer – SOFTWARE registry hive, Microsoft Excel jump list, etc.)
  - The methodology used to find the evidence (what you did & why you did it)
  - Tools used throughout the project

- The written paper should have the following format:
  - Typed, 12pt, Times New Roman, Double Spaced, Use normal margin (1" on all sides)

- Evaluation criteria:

Criteria	**Points**
Provided Answers	30%
Supporting Evidence	30%
Logical Methodology	15%
Description of Methodology	15%
Grammar	10%
Total	*100%*

Project 4 Tips

- Suggested Steps:
  1. Verify E01 file using FTK Imager (make sure image file you downloaded is complete)
  2. Determine the operating system version and other basic facts about the system:
     - OS install date, user accounts, computer name, time zone, etc.
  2. Analyze each question of Project 4 and plan out what you'll need to answer each.
     - Err on the side of including too much information
- Questions:
  1. What identifying information did you find on the hard drive to help determine the owner of the computer?
  2. Is there any evidence on the computer that the user may have been associated with drugs or other illegal activities?
     - Incriminating images, "client" lists, web history related to illegal activity, etc.
  3. Is there any evidence that the user may have been trying to cover his tracks or delete evidence from the computer?
     - Running secure erase programs, deleting files, etc.
  4. Can you identify any additional items (such as USB devices) that may contain pertinent evidence?
     - Identify any devices and evidence of any files accessed on those devices
  5. Is there any evidence on the computer that the user may have been planning to go on the run? If so, where?
     - If the user was planning to run, is there evidence that anyone might be traveling with him? If so, who?
     - Planning documents, itineraries, contacts, emails, web history, etc.
  6. Identify any other evidence that you located on the computer that may assist LMPD in its investigation.
     - If you're not sure whether or not it's important, include it!
- Think about the different artifacts we've learned about this semester and the information that each can provide (LNK files, prefetch files, registry hives, etc.)