Due: 4/24/2017 5:30 PM EDT

# CIS 484-75-4172 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 on March 2, 2016, 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?
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 his 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 him? If so, can you determine the identity of the accomplice?
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)?

It's very important to identify the basis for your answers to the above questions. 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 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 tegrity sessions and PowerPoints, as you will need to use nearly all the skills and artifacts discussed to fully complete this project.

***Present your group's findings to the class on 4/24/2017, highlighting the methodology and steps used during the forensic examination (including tools used), the answers to the above questions, and the evidence your group found to support its findings. In addition, submit a write-up (one per group) that details the group's methodology, findings, and supporting evidence (e.g. file names and paths, specific registry keys/values, timestamps embedded in particular artifacts, etc.) used to answer the questions above. Turn both the PowerPoint and write-up in via BlackBoard prior to 4/24/2017 5:30 PM EDT.***

Due: 4/24/2017 5:30 PM EDT

**Project Guidelines**

- There are two parts to this project. The first part is a maximum 10 written pages. The paper should cover the following:
  - The group's 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 (i.e. what you did any why you did it)
  - Tools used throughout the project

- The second part is a 10-15 minute PowerPoint presentation. The presentation should highlight the paper. Each group member must speak in front of the class.
  - Presentations should be professional, organized, and easy to follow.
  - A penalty will be imposed for each minute under or over a presentation runs.

- **The grade for this assignment will be made up of two parts**:
  - **70% for the written paper**
  - **30% for the presentation**

- ***Each individual group member's grade will be adjusted according to his or her peer evaluation.***

- The written paper should have the following format:
  - Typed, 12pt, Times New Roman, Use normal margin (1" on all sides) - When naming files to be submitted, use assignment, group #, and extension: (CIS484Project_Group#.docx).

- Presentation:
  - Presentation: 4/24/17 (Mon)
  - Submit the PowerPoint presentation along with the write-up

Due: 4/24/2017 5:30 PM EDT

- Paper evaluation criteria:

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

- Submission
  - Project write-up (one submission per group)
  - Peer evaluation (each individual)