CYBER SLEUTH
SCIENCE LAB

MISSION 1
INVESTIGATOR BRIEF

To solve this Mission and complete your Digital Forensics Report you will uncover information in the **Portable Case Files (found in the Virtual Toolkit)** and **Data Collection Reports (found in the Lab Resources).**

You will uncover evidence using digital forensic copies or Portable Case Files of 001 Kara's phone, 002 Backup of Kara's phone and 003 Suspect Phone. You will want to review each one of them **STARTING with 001 Kara's Phone.**

As you review the data in the **Portable Case Files** look for the answers to the following investigator questions and record them in your Notebook. Finding these answers will help you reconstruct the sequence of events involved in this investigation.

NOTE: Key to an investigation is exploring the data and tagging evidence you believe to be related to the case. **Begin the investigation by using the Digital Data Scavenger Hunt on page 2 to help you find different ways of searching the data in the Portable Case Files.**

INVESTIGATOR QUESTIONS

Answering the following questions will help you collect Information you will need to complete your Digital Forensics Report:

1. What Type of phone does Kara have?

2. What type of phone does the Cyberbully Suspect have?

3. Where did you locate a copy of the bullying messages sent to Kara's phone?
(ie. Email, Backup of Phone, SD Card, Cloud)

4. What is the MD5 Hash Value of the **Case.mdfb file** for Kara's Phone Backup?

5. What is the MD5 Hash Value of the **Case.mdfb file** for Kara's Phone?

6. Which phone number was used to send bullying messages?

7. Where is the most data stored on the cyberbully suspect's phone?
(i.e documents, chat, media, mobile)

8. What was the bullying message sent to Kara from the cyberbully suspect's phone?
(Be sure to include the message as a part of the evidence in your Digital Forensics Report)

9. Did you find any evidence of the photo that was used to bully Kara on the cyberbully suspect's phone? (If so, be sure to include the photo as a part of the evidence in your Digital Forensics Report.)

DIGITAL DATA SCAVENGER HUNT

INVESTIGATION PART 1

After exploring the 2 Portable Case Files of Kara's Phone you should be able to: 1) identify the phone number of the suspected bully, and 2) have tagged evidence of the bullying message(s) and image.

001 Kara Phone

How Many "Artifact" types can you choose from in Magnet Axiom? Name two of them.

What Artifact type shows the most results in Kara's phone?

How many ways are there to "View" evidence in Axiom? Name two of them.

What is the best way to View Media artifacts?

002 Kara Back-up

How many Chat Artifacts are there in the 002 Back-up of Kara's phone? How does this compare to 001 Kara's Phone?

How many Applications does the Back-up show are installed on Kara's phone?

To look for a group of messages from a specific phone number how can you sort the evidence?

How do you "Add a New Tag" in Axiom Examine? Where do you view a list of the items you have tagged?

How do you export items you have tagged? Export your evidence as different export types to determine how they might be used for your Digital Forensic Report.

INVESTIGATION PART 2

After exploring the Portable Case File of the Suspect Phone you should determine IF YOU HAVE FOUND evidence that corresponds to what was found on Kara's phone.

003 Suspect Phone

How many "Identifiers" are shown on the Suspects Phone?

Where is the information about "Installed Applications" artifacts stored?

How do you Clear a "Search" Filter in Axiom?

EXTRA CREDIT
Is there any evidence of Social Media activity on the Suspects phone?

If so, what Social Media Applications left traces on the phone?