Investigation Exam – Forensic Analysis

Case File: Murder by Money	Investigating Agency: IIT

CASE INFORMATION:

Agency Case #:	Exam_MoneyMurder_2022	Forensic Analyst:	Name: Alan Palayil

YOUR ASSIGNMENT:

You are a forensic investigator and have just been assigned your first major case. Your supervisor has personally selected you for this and has privately mentioned that you will make a name for yourself if you correctly solve the case. Cautiously excited (and imagining yourself taking home the company's Forensic Investigator of the Year Award a few months hence), you study the background information with which you've been provided:

- *A crime has been committed with a very unusual weapon.*
- *In spite of the unique nature of the crime, there has been insufficient evidence to apprehend the suspect.*
- *The suspect worked in the IT department and was very computer savvy.*
- *The suspect was known to enjoy digital forensics as a long-time hobby.*
- *The suspect absolutely loves puzzles.*
- *Social media accounts reveal that the suspect has quite a following in the Escape Room Facebook Group.*
- *The suspect is known for designing Escape Room scenarios that are extremely challenging and typically include extraneous information to distract players and clever traps to snag players attempting to take short-cuts.*
- *Though very unlikely, it IS possible the suspect has done nothing wrong and is in fact the wrong target.*

"Well now", you think to yourself, "this could get interesting". After digesting this background, you Zoom call your supervisor and report that you are ready to begin the investigation. You're given one final rather sobering piece of concluding advice: "Remember, now. This suspect loves puzzles and enjoys daring people to solve mysteries. The only way you will succeed is by letting one clue lead to another. Some clues may be more obvious than others. Take no short cuts, follow the trail, be wary of traps, live long and prosper."

Read on for more information about this assignment and the evidence you'll need to submit to complete your investigation.

SUMMARY OF THE CASE:

The police have been called in to respond to a grisly murder. When detectives arrived at the scene, they were puzzled by the nature of the crime. No murder weapon was found. Physical forensic evidence was carefully collected, which was enough to identify a prime suspect for the murder.

Unfortunately, the evidence found thus far is circumstantial. The truly incriminating types of evidence (e.g., the murder weapon, blood-stained clothes) wasn't present at the scene. They did find out from the suspect that he kept a locker at the nearby train station, but he wouldn't give up the combination. Furthermore, the evidence isn't strong enough to get a search warrant for the suspect's locker.

They were, however, able to get a search warrant for the suspect's residence, but extraordinarily little was found that was considered of forensic value. Only two items were identified which seem potentially significant:

- A USB flash drive
- An old coffee-stained scrap of paper with a lot of seemingly random information written on it.

FORENSIC ANALYSIS – MURDER BY MONEY

Forensic technicians have secured the evidence and have taken a forensic raw copy of the suspect's USB flash drive and loaded it on your RADISHng Forensic Workstation. They've copied it to the shared drive at the following path (replace <username> with your actual username:

`R:\student\<username>\Midterm Forensic Exam\InvestigationDiskImage_<username>.001`

They also took a photo of the old scrap of paper and copied it into the same directory with the following name:

`Evidence_SlipOfPaperFound_<username>.pdf`

REQUIREMENTS FOR COMPLETING THE INVESTIGATION EXAM

You are tasked with finding the combination of the locker which hopefully contains evidence linking the suspect to the murder scene. Begin with the forensic disk raw image, the clues that have been left behind, and the background information given by your supervisor and in the case summary.

This investigation will be considered a success if you find legitimate evidence of:

- The 4-number combination to the locker
- A verifiable trail of clues that led you to that account number.

Of course, you **must** log the evidence you find, along with justification as to why you think each piece of evidence is legitimate (remember, the suspect likes to leave a lot of false clues). You will log each piece of evidence you obtain in a Digital Evidence Log, which you can find here:
https://docs.google.com/spreadsheets/d/18jmIsgmT4V0CcsCCW2rTQZSdS6DhLIClQw74_qKoDZ0/edit?usp=sharing

IMPORTANT! Make a copy of the Digital Evidence Log on your own drive BEFORE you begin to fill it out. Be sure to put your name on your log as the Forensic Investigator! DO NOT edit the original version of the Digital Evidence Log!

When your investigation is complete, you must submit three things:

1. a Zip file to your Forensic Investigation assignment on Blackboard containing each item of digital evidence you logged that could be extracted using the Forensic tools you used to discover the evidence. *NOTE: Do NOT do bulk extracts from the disk image; extract only selected items.*
2. The URL of your completed Digital Evidence Log (make sure you have shared the document). You can copy and paste this link into the Comments section when you make your submission.
3. A write-up of your investigation, describing what tools you used, what trail of clues you followed, and what your investigation yielded. Be sure to explain the significance of the result of your investigation (including whether you successfully found the evidence they were hoping to find.) Include screenshots and follow the homework guidelines for this course. Note that a significant portion of your grade will be based on this item as it will demonstrate your understanding.

Final Note: Every student has a unique flash drive image: no two trails are exactly alike. While collaboration is an essential part of forensic investigations, please remember to treat this as if it were an in-class exam: do not share results, ideas, trails, or hints (you may trap another student!).

DUE DATE: Your evidence and Digital Evidence Log link must be submitted by:
Tuesday, October 25 @ 11:59pm (end-of-day) – US Central

If you have any questions regarding this exam, be sure to send them to me no later than Saturday, October 22 (end of day). No questions will be accepted after that as you should be well on your way to completing this investigation by then.