

# Computer and Network Forensics CA Technical Challenge

**Important Instructions:** “*This report should entirely reflect your individual efforts and findings. Please refrain from requesting findings or sharing your own with fellow students. Any students found to be involved in asking for or sharing answers will be subject to an automatic zero grade. All submissions will undergo thorough scrutiny for unoriginal and copied content*”.

— Michael Hegarty.

## Computer Forensics Assignment: Analysing Evidence

**The Challenge:** Your mission involves conducting an in-depth analysis of a retrieved disk. Your objective is to address the questions provided and produce a meticulously structured forensic report. This forensic report must adhere to the **principles and standards** integral to the scope of digital forensics. The essential information required for compiling this report has been presented throughout our lectures and labs over the previous weeks. To effectively undertake this task, it is important that you review the lecture materials and lab sessions.

**Prologue: Reading the Police Report** At the onset of this forensic investigation, like the commencement of real-world investigations, you are granted access to a police report. This document furnishes you with initial background information and a trace of potential evidence. However, it is mandatory upon you to employ your technical prowess to extract the essential answers. Just as in actual investigations, your findings are essential to uncovering the truth.

**The Investigative Kit: Recovered Disk Image** Contained within the designated folder is the digital image of the retrieved disk. This forms the base of your investigation. It is your responsibility to meticulously document every step of your investigative process and all discoveries made during this analysis. The principles of the Chain of Custody are of paramount importance in upholding the integrity and admissibility of evidence. It is, indeed, the foundation upon which a successful forensic case is built.

**Task Assignment: Addressing the Questions** Your primary task revolves around addressing the questions presented. The questions serve as a guiding your path through the maze of digital data and potentially hidden evidence.

**Compilation of a Professional Forensic Report** The culmination of your efforts is the creation of a professional forensic report. This report should not only answer the questions but also meticulously detail the process you undertook, the tools you utilized, and the discoveries you made. It must adhere to established forensic standards and reflect the highest levels of professionalism. Remember, the quality of your forensic report and your adherence to the Chain of Custody and forensic process could be the condition(s) that either strengthens or jeopardizes the case.

Throughout this challenge, demonstrate the highest standards of ethics and professionalism. Uphold the rules of digital forensics, ensuring that your findings and analysis stand up to the strictest scrutiny and cross examination.

**Image MD5 = AC3F7B85816165957CD4867E62CF452B**

Write up a **professional report** (review lectures/labs and Moodle/Brightspace) of your findings *and* include answers to the following questions. Remember it is your investigation so propose any additional evidence. Your report should be professional.

You may use any open/closed source tools you have available.

#### **The Challenge:**

Your mission is to perform an analysis on a retrieved disk and respond to the inquiries presented below. Prior to commencing the examination of the image, it is essential to thoroughly review the police report. Just as in the commencement of a real-world investigation, you possess some initial information and a certain amount of evidence, yet it is crucial for you to employ your technical ability to unearth the answers.

Contained within the directory is the dd image of the recovered disk. It is important to meticulously document all your activities and findings throughout this investigation. Please consult the Moodle/Brightspace platform, comprising lecture notes and supplementary educational materials, for guidance.

**Image MD5 = AC3F7B85816165957CD4867E62CF452B**

Your task is to compose a **professional forensic report** detailing the outcomes of your inquiry and providing responses to the following questions (in addition to any supplementary

**Any shared answers will be automatically awarded a grade of zero**

evidence of illicit activities). You may cite TU-Dublin Lab-A11 as the forensic lab where you conducted your forensic analysis.

### **Police Report - Computer and Network Forensics TU-Dublin Michael Hegarty**

A recent arrest has been made involving an individual suspected of drug distribution to students. The apprehension transpired when a local police officer, operating undercover as a school student, encountered Joe Jacobs in the vicinity of Smith Hill High School. During this encounter, Jacobs, unaware of the officer's identity, offered to sell marijuana. Showing the illicit substance, Jacobs boasted, "*Look at this stuff, Colombians couldn't grow it better! My supplier not only sells it direct to me, but he also grows it himself.*"

Jacobs has been sighted frequently, loitering near various local schools around 2:30 pm, the typical time for a to school finish. Multiple high school administrators have alerted the police to Jacobs' unwarranted presence and reported an increase in student drug usage since his appearance.

To ascertain whether Joe Jacobs has engaged in drug transactions with students from other institutions apart from Smith Hill, the police have initiated an investigation. Regrettably, students have been slow in coming forward to assist the authorities. Of particular interest to the police is the identification of Joe Jacobs' supplier or marijuana producer, based on his reference to Colombians.

Despite subsequent investigations, Jacobs strongly denied any involvement in drug sales at schools other than Smith Hill and has refrained from disclosing the identity of his supplier/producer. He also withdrew his prior statement regarding the quality of the marijuana. Following the execution of a search warrant at the suspect's residence, the police secured a small quantity of marijuana and seized a *single disk*. However, no computers or additional media were found on-site.

The police, in their pursuit of concrete evidence linking Joe Jacobs to drug distribution at schools beyond Smith Hill and the identification of his supplier, have imaged the suspect's disk and furnished you with a copy for examination. They have urged you to focus on uncovering any information that may substantiate his involvement with other high schools and identify

**Any shared answers will be automatically awarded a grade of zero**

his supplier. Notably, Jacobs has posted bail, set at €10,000.00, and due to concerns of potential flight, the police wish to expedite the case. Hence, they have requested a comprehensive report containing specific findings in line with the posed questions. It is imperative that your findings withstand cross-examination, as the case will ultimately be presented in a court of law.

**Questions Section A (All Questions and Answers should be added to the end of your report)**

1. Where was the analysis of evidence conducted?

When did the analysis commence?

What evidence supports this timeline?

Who, if anyone, aided during the process?

How can the authenticity of your evidence be verified?

What forensic tools were utilized for evidence analysis?

- Are these tools admissible in court?
- How can their admissibility be determined?

2. Outline the procedures involved in uploading the evidence for analysis.
3. How many files are presented in the complete image?
4. What specific file system is currently in use?

**Questions Section B: (All Questions and Answers should be added to the end of your report)**

1. Who is the supplier of marijuana for Joe Jacobs, and what address is associated with the supplier? Identify the key individuals involved in this case.
2. Within the coverpage.jpg file, what critical data is contained, and why is this data considered pivotal to the investigation?

**Any shared answers will be automatically awarded a grade of zero**

3. Besides Smith Hill, which, if any, other high schools did Joe Jacobs frequently visit?
4. In each file, what methods did the suspect employ to conceal them from prying eyes?
5. What investigative techniques were employed to comprehensively examine the entire contents of each file?
6. Which Microsoft program was utilized in the creation of the Cover Page file, and what evidence supports this claim?
7. Are there any additional findings or information that could be instrumental in ensuring a conviction?

**ANSWER ALL QUESTIONS AND PRESENT YOUR PROFESSIONAL REPORT IN A SINGLE MS WORD DOCUMENT AND UPLOAD TO MOODLE BY DUE DATE**

*All names, locations, and scenarios presented in this case are entirely fictional and bear no connection to actual individuals, places, or events.*

*This investigation should be conducted using your independent methods and available resources and tools.*

### **Plagiarism Checks**

- 1. All work is processed through plagiarism checkers**
- 2. All work is processed through Large Language Models such as chatGPT checkers**

**Any shared answers will be automatically awarded a grade of zero**