**MGMT 646 Project Instructions (Fall 2022)**

***Reminder: This is an individual assignment and not a group project. Given the nature of the course it is not very difficult to detect if this requirement is violated based on the deliverables that you will turn in. If this requirement is not met you will receive no points for this assignment and may be subject to additional penalties.***

# Background

ACME is a multinational corporation with offices in the US, Europe and Malaysia. The company provides a multitude of services and products which include electronics, chemicals and medical equipment. Additionally, the company has several contracts with the US department of defense and department of energy, however any service or products provided to DoD/DoE are not listed in the company’s public records.

As a forensic examiner for ACME you are tasked from time to time to support corporate investigations. Last week you received the paperwork to complete the ***remote acquisition*** of a system belonging to Mr. Ocho Pelota and to retrieve any evidence regarding the possible exfiltration of company data. Based on corporate policy all computer systems are setup with a standard image, which includes a remote acquisition agent, and a locked down configuration of the operating system so that employees ***cannot install or store any type of information on their boot drive***, including any browser data. All digital work products are stored on network file servers which will be examined by a different team. However, there are no countermeasures in place to prevent employees from accessing their system’s USB interfaces and connect keys or external drives to the system. Next time Mr. Pelota’s system accesses an external USB device you will be notified to retrieve any evidence attached to his system.

# Instructions

When you are ready to start your project delete/destroy all other vApps and only keep the main class vApp (MGMT 646 vApp) then contact me via email. I will then deploy a copy of your Project vApp. In the Project vApp you will have a copy of the Win10 and Kali VMs from class along with the suspect’s VM. You can safely assume that at this time Mr. Pelota has access to a USB device on his system. You can use any set of tools you choose to complete the work, whether it’s part of the software located on your Z: drive or downloaded from the web.

# Management Support

I will play the role of your direct supervisor in this project. If you need assistance, you'll be able to escalate a request by communicating directly with me via email what your needs are (do not message via Canvas). In my responses I will provide you with options on how to proceed which may include suggestions, answers or possible ‘next steps’.

Each option will require a certain amount of knowledge and time to which points will be assigned in place of financial cost. These points will be deducted from your final project grade. For example, if you need assistance to get past a certain hurdle, I may respond by saying that an info bulletin (instructions on what you need to do next) will cost 70 points and that if you want me to step in and apply the bulletin the cost will be 120 points. No points or actions are taken until I receive an email confirming that you agree to the terms or cost of the support call. ***Please note that it costs you nothing to ask questions, only after you’ve agreed on points, etc. and you’ve received the help will there be a***

***deduction. After I respond with a points’ amount you can very well reply with a “no thanks”. So DO ASK questions when you’re not sure about something as the worst thing that can happen is that I reply with “the answer would cost XX points”. Often times I can answer questions with no charge, particularly when something is not functioning as expected. You want to avoid regretting not asking a question when you had the opportunity before the due date.***

All communications, assistance, bulletins, etc. are to remain private since the project is an individual assignment. If you share information regarding the project that originates from a support call, you’ll be in violation of the project’s requirements (see the “Reminder” section at the beginning of this document). Additionally, given that there are different versions of the project, with different evidence, you would risk giving someone the wrong instructions, damaging their project, and automatically flagging a violation.

Based on the work and tools you’ve used in class thus far you should be aware that there are often different paths you can take to retrieve the same evidence. You may use Hex Workshop or Winhex to view raw data, Autopsy for imaging, etc. As your supervisor I have developed my own set of tools for this examination. This is one of the possible

“packages” that can be used to complete this investigation, it certainly isn’t the only one and it’s possibly not the best one, but it works. If at some point you are interested in purchasing the tool set the cost is 200 points. The tool set will not include instructions, but the presence and capabilities of each tool should tip you as to the nature and location of the evidence you are working to retrieve.

# Deliverables

Your final report is to be addressed the company’s legal counsel office and will include:

1. An executive report of your findings no longer than 2 pages.
2. To meet the digital forensics standard of reproducibility of results, provide a timeline (step by step) document which catalogues the process you applied in your examination. The document should be organized by day and time displaying which activities were conducted at what time and what the outcomes were. Another forensics examiner must be able to follow your instructions and produce the same results, thus your instructions must be clear and easy to follow. Additionally, consider that the more detail you include in your instructions the better the likelihood of successfully supporting your findings during trial several months from now. Any information regarding the validity of the evidence must be included in this document (hashes). ***Do not include screen captures (points will be deducted if you do)***, rather be descriptive and detailed in the steps you took.
3. If you choose to, you can add an appendix section for all detailed reports generated by the applications you used. These should not be included in your timeline document as they will easily clutter your instructions for reproducibility of results.
4. An archive of all digital evidence found, mostly files and any additional data about those files.

Four separate (if you include an appendix section) files must be uploaded to UNM Learn with the following naming convention:

* *LastName*Executive.docx
* *LastName*Timeline.docx
* *LastName*Appendices.docx (Optional)
* *LastName*Archive.zip

All files must be uploaded by the deadline listed in the course website.

# READ CAREFULLY

**OCHO’S SYSTEM: You should not interact directly with Ocho’s system under any circumstance. You do not have physical access to his system. If you try to login to the VM, reset it, etc. he’ll be on to you and will permanently destroy any evidence. *IF YOU RESET, REBOOT OR TAKE OFFLINE OCHO’S SYSTEM/VM YOU WILL HAVE FAILED THE PROJECT AS HE WILL KNOW THAT SOMEONE IS TRYING TO ACCESS HIS USB DRIVE AND WILL REMOVE AND DESTROY THE DRIVE AND EVIDENCE.***

**IMPORTANT: Please remember that evidence is indeed available in this project. If you state that there's no evidence or that this is a decoy to the investigation, it will result in 0 points. Additionally, you are expected to retrieve all the evidence that you can. Simply stating that you suspect there is incriminating evidence and that you recommend this investigation be escalated to senior examiners will also result in a failing grade.**

**Finally, when you are not sure about a goal, expectation, procedure, etc. ask. It does not cost anything to ask. Worst case scenario I determine that you require a bulletin and before taking any action I will confirm that you are agreeing to pay the fee in points.**

**TIME MANAGEMENT: Having observed students over the years working on these types of projects let me strongly encourage you not to wait until a few days before it’s due to work on this project. This is the type of project you want to start as soon as you can. You will need to digest several components and work through different challenges. There will be times when stepping away from the project for a couple of days will help you regain some clarity or help you consider other possibilities. If you wait until the end, these ‘pockets’ of reflection are severely compressed, stress will increase, and your ability to think clearly and calmly will be impacted. Also, the last day to request the ‘tool set’ or submit a support ticket is 5 PM on October 9, 2022. You should spend the last week of the project tying up loose ends, confirming that you can replicate your findings and putting the finishing touches on your deliverables.**