Information Security (CP3404)
Chapter 13 practical

- This practical consists of some quick quiz questions, tutorial type questions, and hands-on projects relevant to (chosen from) Chapter 13 of the textbook (i.e., Mark Ciampa, *CompTIA® Security + Guide to Network Security Fundamentals, Fifth Edition*, USA, 2015).
- You may not be able to complete this practical within the scheduled one-hour practical session for this subject. You are strongly recommended to complete it in your own time (note that you are expected to work 10 hours per week on this subject, including 3 hours of contact time).

Section A – Quick-Quiz/Multiple-Choice Questions:

- Each week, complete the test on LearnJCU within the time allocated, which is before the next practical session.
- These on-line tests are worth 20% of the total marks for this subject.

Section B – Short Answer (Tutorial-Type) Questions:

- Answers to this set of questions are available at the end of this document (Section D).
- Effective learning implies you answer the questions before seeing the answer.

1. Describe the purpose of a disaster recovery plan.
2. What are the three (3) objectives of disaster exercises?
3. What are the steps in damage control?
4. Explain how to best capture volatile data.
5. Discuss the purpose and importance of the chain of custody.
6. What does Windows do if a file being saved is not long enough to fill up the last sector on the disk?
7. When creating a data backup plan or policy, what five (5) basic questions should be answered?

Section C – Hands-On Projects:

Due to security issues, you may not be allowed to practise hands-on projects with university's computers. Interested students are encouraged to do these projects on their own computers (if available). You will not be assessed for utilities/commands that cannot be practised on university computers. Note that you may still be assessed for descriptions/definitions that are provided in this section.

Creating a Disk Image Backup[1]

To backup programs and operating system files in addition to user files, one solution is to create a disk image. a Disk image is created by performing a complete sector-by-sector copy of the hard drive instead of backing up using the drive's file system.

In this project, you download Macrium Reflect to create an image backup.

1. Use your web browser to go to www.macrium.com[2].
2. Click **DOWNLOADS** and the click **Download Now**. At the download site, also click **Download Now**.
3. Run the file and then click **Trial software**. Select **Professional** from the drop-down list.
4. Click **Download**.
5. Accept the default settings to download, and then install this program onto your computer. Launch the program by double-checking the icon.
6. When Reflect launches, click **Backup** if necessary.
7. Click **Create an image of the partition(s) required to backup and restore windows**.
8. Under **Source** select the disk that contains the operating system and data for this computer.
9. elect the location to store the backup. You cannot store the backup on the same hard drive on which you are creating the image; you must store it on another hard drive in that computer or on an external USB hard drive. Under **Destination**, select the appropriate location. Click **Next**.
10. Review the settings that are displayed. Note that, depending on the size of the data to be backed up and the speed of the computer, it will take several minutes to perform the backup. Click **Finish** and then **OK**. Click **OK** and then **Close**.
11. Leave Macrium Reflect open for the next project.

It is important to test the steps necessary to restore a disk image in case a hard drive stops functioning.

In this project you will go through the steps of restoring the Macrium reflect image backup in previous project, although you will stop short of actually restoring the image.

1. Once the backup in previous project has finished, you will create a Rescue CD. This CD will allow you to boot your computer if the hard drive becomes corrupt and restore the backup. Click **Other Tasks** and then **Create bootable Rescue media**.
2. Select **Linux - Select this option to create a Linux based recovery media**. Click **Next**.
3. Click **Finish**.
4. When prompted, place a blank CD disk in the tray, and then click **OK**. Reflect will now create a recovery CD.
5. When the recovery CD has been created, close all windows.
6. Now boot from the recovery CD. Be sure the recovery CD is in the disk drive, and restart your computer. If it does not boot from the recovery CD, check the instructions for your computer to boot from a CD.

[1] If you are concern about installing any of the software in this project on your regular computer, you can instead install the software in the Windows virtual machine created in practical-1. Software installed within the virtual machine will not impact the host computer.

[2] It is not unusual for websites to change the location of files. If the URL above no longer functions, open a search engine and search for "Macrium Reflect"

7. hen the Restore Wizard dialog box is displayed, click **Next**.
8. In the left pane, click the location where you stored the image backup.
9. In the right pane, select the backup image that appears.
10. If you are actually restoring your image backup, you would continue to proceed. However, click the **Close** button.
11. Remove the CD.
12. Click **OK** to reboot your computer.

Section D – Answers to Short Answer (Tutorial-Type) Questions:

1. Describe the purpose of a disaster recovery plan.

   Answer:
   A disaster recovery plan (DRP) is a written document that details the process for restoring IT resources following an event that causes a significant disruption in service. Comprehensive in its scope, a DRP is intended to be a detailed document that is updated regularly.

2. What are the three (3) objectives of disaster exercises?

   Answer:
   The three objectives of disaster exercises are:

   (i) Test the efficiency of interdepartmental planning and coordination in managing a disaster.
   (ii) Test current procedures of the DRP.
   (iii) Determine the strengths and weaknesses in responses.

3. What are the steps in damage control?

   Answer:
   Report the incident to security or the police.
   Confront any suspects (if the situation allows).
   Neutralize the suspected perpetrator from harming others (if necessary).
   Secure physical security features.
   Quarantine electronic equipment.
   Contact the response team.

4. Explain how to best capture volatile data.

   Answer:
   Capturing volatile information can best be performed by capturing the entire system image, which is a snapshot of the current state of the computer that contains all current settings and data.

5. Discuss the purpose and importance of the chain of custody.

   Answer:
   The chain of custody documents that the evidence was under strict control at all times and no unauthorized person was given the opportunity to corrupt the evidence. A chain of custody includes documenting all of the serial numbers of the systems involved, who handled and had custody of the systems and for what length of time, how the computer was shipped, and any other steps in the process. In short, a chain of

custody is a detailed document describing where the evidence was at all times. Gaps in this chain of custody can result in severe legal consequences. Courts have dismissed cases involving computer forensics because a secure chain of custody could not be verified.

6. What does Windows do if a file being saved is not long enough to fill up the last sector on the disk?

   Answer:
   When a file that is being saved is not long enough to fill up the last sector on a disk (a common occurrence because a file size only rarely matches the sector size), Windows pads the remaining cluster space with data that is currently stored in RAM. This padding creates RAM slack, which can contain any information that has been created, viewed, modified, downloaded, or copied since the computer was last booted.

7. When creating a data backup plan or policy, what five (5) basic questions should be answered?

   Answer:
   The five (5) basic questions that should be answred are:

   (i) What information should be backed up?

   (ii) How frequently should it be backed up?

   (iii) What media should be used?

   (iv) Where should the backup be stored?

   (v) What hardware or software should be used?