

Before we start the class...

BRIEFING FOR ASSIGNMENT 1

- **ASSIGNMENT 1 GROUPING**

- Assignment 1 released on 23th Oct 23 (Monday)
- Form group and submit your group **member names** and **research topic** to tutor by end of week 2 (27th Oct 23).
- Please ensure that everyone has an assignment group

- **OBJECTIVES OF ASSIGNMENT 1**

- To research the concept and principles of **Mobile Forensics**.

- **TASKS FOR ASSIGNMENT 1**

- **Conduct a research on an assigned topic as thorough as possible.**
- Present and produce a report (Team)
- Will be good if can do a simple demon during presentation. i.e tools used

Before we start the class... (cont)

PLEASE HELP TO KEEP THE LAB CLEAN...

NO DRINK AND FOOD IN LAB...



Important concepts to note for week2 lecture (e-learning)

CHAIN OF CUSTODY

- Refers to the **order** in which items of evidence have been handled during the investigation of a case.
- Why “Chain of Custody” is required?

PRIVATE AND PUBLIC INVESTIGATOR

- **Private Investigator** – Resource abuse case, misuse of company resources. Usually within company
- **Public Investigator** – Involve police officer, criminal

WRITE BLOCKER – IMPORTANT DEVICE

- **To avoid altering evidence – Most important in DFI!**
- i.e enable you to boot to windows without writing data to the evidence drive
- Under “learning Resources” folder in BrightSpace, there is a sub folder named “Other Resources”. In this sub-folder, we have a video created by ex-DISM students regarding write blocker. Take a look if possible.

Quizzes for chapter 2

Chapter 2 – “Understanding DFI”

► Quiz 1

1. A form that helps you document what has been done with the original evidence and its forensics copies is also known as:

- ☒ Chain-of-evidence form
- ☐ Software Configuration form
- ☐ System admin form
- ☐ Forensic lab form



Quizzes for chapter 2 (Cont)

Chapter 2 – “Understanding DFI”

► Quiz 2

1. For E-mail Abuse Investigation, as a forensic investigator, you need to:

- ☐ Use appropriate tools to extract all Web page URL information
- ☐ Compare the data recovered from forensic analysis to the proxy server log
- ☐ Access to the computer so that you can perform a forensic analysis on it
- ☐ All of the above



Quizzes for chapter 2 (Cont)

Chapter 2 – “Understanding DFI”

► Quiz 3

1. What device is required to avoid altering the evidence when perform evidence acquisition?

- ☐ Hard disk storage device
- ☒ Write-blockers device
- ☐ Digital forensic work station
- ☐ Forensic lab evidence tape



Week 1 Lab Exercise – We completed the following last week...

Setup DFI VM on D drive (1A) and explore Magnet software (1B)

- ▶ Practical 1A
 - ▶ Setup DFI VM that contains DFI Software Magnet (ForensicV6)
- ▶ Create DFI VM “Forensicv6”
 - ▶ Read instructions in Practical 1A
 - ▶ Create working folder in D drive
 - ▶ Go to C drive “Baseimages” and copy folder “Forensicv6” to your D drive folder or your own Personal Computers to work on your Practical Labs
 - ▶ Try to run DFI VM “Forensic” from your D drive or your own Personal Computers to ensure that your VM is working properly.

Week 1 Lab Exercise – We completed the following last week...

► Work on Lab 1B – Explore DFI software Magnet

► Practical 1B

► Read instructions in Practical 1B

- In this Practical, you will be able to process the **acquire data** called **image files** (. E01 - an encase proprietary format). **Creating a case file** and **process** it to verify image file (. E01) to ensure that the acquired image is a bit-for-bit copy of the original copy by generating a hash value within AXIOM Process.

Week 2 Lab Exercise

- ▶ Basic functions in Magnet.
 - ▶ Lab 2A
 - ▶ How to access a “**Case**” in Magnet
 - ▶ Perform **Google Searches** artifact group
 - ▶ Perform **Parsed Search** Queries
 - ▶ Lab 2B
 - ▶ Learn to recover **emails** and **email attachments** from mail clients supported by Magnet AXIOM.
- ▶ Follow the steps on your lab documents and work on Week 2 Lab 2A and 2B – Document your answers in a word document and submit lab exercises **individually** to BrightSpace
- ▶ Start to work on **assignment 1** if got time...