National College of Ireland

BSc (Hons) in Computing (Cybersecurity) – Year 4 – Full-time (BSHCYB4)
BSc (Hons) in Computing (Cybersecurity) – Year 4 – Part-time (BSCCYBE4)

Semester 2, 2024/25

Release Date: Thursday 3rd April 2025
Due Date: Thursday 17th April 2025 @ 23:55

Lecturers:
Arghir-Nicolae Moldovan, Michael Prior

Digital Forensics

CA Type: Individual Assessment (TABA)

WEIGHT: 50% of overall marks for this module. The assignment will be marked out of 100.

INTRUCTIONS:

- This is an **individual assessment**, so you are not allowed to collaborate or share your CA work with other colleagues.
- Read each question carefully as they usually ask you to do a few things.
- Answer **all** questions in a **Word document** (use single column format).
- **Add your name and student ID** at the top of page 1.
- Clearly **indicate the question part and number** (e.g., Question A1), but **DO NOT** include the question text as that will increase the Turnitin similarity.
- This is an **open-book** assessment so you can use any resources (e.g., on Moodle, Internet).
- You **must include references** to all resources that you have consulted for your answers (e.g., books, articles, tutorials, videos, etc.).
- **Theoretical questions** will focus on comprehension, discussion and exemplification. You should not copy paste text from lecture notes or external resources. Instead, you should discuss and write the answers in your own words. Some questions will require you to do some research (e.g., search online and reference a few articles to support your answers).
- **Practical questions** will focus on the application of the digital forensic skills. The **answers will be personalised** (e.g., based on student ID), to ensure that each student does them independently. The lecturer can award **0 marks** for generic non-personalised answers.
- You must **include screenshots** to demonstrate that you completed the practical questions.
- **Relevant information must be highlighted** in the screenshots to demonstrate your comprehension and that you know what you are looking for.

SUBMISSION DETAILS:
Check the Moodle page for instructions and submission links. Upload the Word document to Moodle before the deadline.
Late submissions are normally not allowed as the TABA is an exam replacement. Any student that has relevant personal circumstances should apply for an individual extension through NCI360.

TURNITIN: All report submissions will be electronically screened for evidence of academic misconduct (e.g., plagiarism and collusion).

AI Acknowledgement: All students must fill and submit the AI acknowledgement form and confirm if they used AI tools for any aspect of the TABA work such as report writing (including but not limited to ChatGPT, Copilot, etc.). If you use any AI tools you must provide details and screenshots of the prompts and answers in the form.

Attachments: None

Part A – Theoretical Essay Questions (50 marks)

Answer **all** questions from Part A.

Each question answer should be clear and concise (approx. 3 pages long for A1 and 3 pages for A2 excluding references). Personalise the answers by providing examples based on your independent reading, reference real-world digital forensics cases, etc. All references should be included at the end of the corresponding question answer.

A1) Device and filesystem forensics:

- Discuss the forensic methodology, principles, techniques and legal aspects that you would consider when conducting file system forensics on a suspect USB drive.
- Contrast and exemplify the wealth of forensic information that could be extracted from a laptop's internal HDD/SSD as compared to a USB drive.
- Research and discuss some challenges newer file systems (e.g., NTFS vs. FAT, APFS vs HFS+, ext4 vs. ext3, etc.) and newer storage technologies (e.g., SSD vs. HDD), present for forensic investigators and how they can overcome these challenges.
- Discuss the challenges posed for forensic investigations by data encryption, as well as the forensic imaging/acquisition methods one can use depending on if encryption is used or not.

(25 marks)

A2) Network, cloud and device forensics:

- Discuss why other forms of digital forensics such as memory, network, cloud, IoT and mobile are becoming increasingly important (support your answer with market statistics and some real-world examples of forensic cases).
- Imagine and briefly describe (i.e., in approx. half a page) a scenario where a user of cloud computing services is being the suspect in a digital forensic investigation. Provide specific details such as the role of the user (e.g., manager/employee of company Y), what cloud services they use, the type of service (e.g., IaaS/PaaS/SaaS), some activities they did, end user devices used (e.g., laptop, smartphone, OS, if BYOD or owned by the company), etc.
- Briefly discuss the main forensic methods you would use in this scenario (e.g., filesystem, memory, network, cloud, mobile). Research and provide 3 examples of complementary forensic tools and discuss how you would use them in your scenario (e.g., prerequisites, capabilities and limitations of the tools, what forensic information you would extract, etc.).
- Select 3 cloud forensic challenges specified by NISTIR 8006, discuss how they apply to your scenario and if these are unique or exacerbated by the cloud environment, as compared to other types of digital forensics (e.g., computer, mobile, network, etc.).

(25 marks)

Part B – Practical Questions (50 marks)

Answer **all** questions from Part B.
For each question, include step-by-step descriptions of the process you followed (and/or computations), as well as screenshots that clearly highlight the relevant information as evidence that you did the work.

B1) Use a software tool to take a raw memory dump of your Windows PC/VM and name it based on your **student ID** (e.g., x12345678_Win11_Memdump.raw). Compress the dump with ZIP, then compare its raw size vs. compressed size vs. used memory displayed by Task Manager. Analyse the dump using command line and/or GUI-based tools to find any 3 pieces of information (e.g., Message output to CMD: echo "My student ID is x12345678", OS info, processes, open ports, files loaded, URLs opened, etc.). Include screenshots of other apps taken immediately before creating the memory dump to verify the info (e.g., CMD of echo, System Info for OS, Task Manager for processes, Netstat for ports, browser for URLs, relevant app for files, etc.).

(10 marks)

B2) Explore your Windows PC/VM Registry to find any 5 interesting pieces of info about your activity on the PC that could be relevant forensic evidence (may include but are not limited to: your user SID and profile image path, user login activity, recent files, last time the PC was turned on, last activity view, last USB drive you connected to the PC, last time you connected to the WiFi network, recent searches in File Explorer, etc.). Some screenshots must show **personal info** (e.g., name, student ID). The screenshots and/or text description should clearly indicate the registry key where the information is located. If the information is in hexadecimal you should convert it to readable text (i.e., manually or using software tools like a Hex data interpreter / decoder).

(10 marks)

B3) Create a PowerPoint presentation containing your brief bio and photo and rename the file to include your **student ID** in the file name (e.g**.,** x12345678_Bio.pptx). Open the file and while it is open, find the corresponding temporary file starting with ~$ and discuss what useful information this contains. Delete the file by pressing the Delete key. Locate the corresponding $I and $R files in the Recycle Bin and analyse and discuss their contents.

(10 marks)

B4) Use a network forensic tool (e.g., Wireshark or Network Miner) to capture the traffic as you visit an unsecure website (e.g., http://zero.webappsecurity.com/login.html). Browse through the different pages. Attempt to login by using your **first name** for username and **student ID** for password (do not register just fill the details and click on Login). Stop the packet capture and analyse the traffic capture to extract the following 4 pieces of information: the login credentials and login timestamp, one image, one html file and access timestamp, server IP and its location (i.e., city and country, may require the use of additional tools).

(10 marks)

B5) Create a Linux instance in Amazon Web Services and name it using your **student ID** (e.g., x12345678_OSversion_DIGFOR). Create a LiME kernel object and use a cloud forensic tool (e.g., Margarita Shotgun) to remotely take a memory dump of the AWS instance. Use the Strings utility to search the memory dump for the Linux version information.

(10 marks)