



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Digital Forensics (ACCA7031)

Capture the Flags



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

Lab Activities are based on

TryHackMe, EC Council – CHFI, Digital Forensics Workbook and other Industry Digital Forensic Curriculum

In continuation to our lectures, this hands-on Activity helps in providing you an overview of digital forensic analysis.

As discussed during our lectures, it is very important to adhere to Personal Ethics, Professional Ethics, Computer Ethics and Business Ethics.

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various digital forensic activities. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using these tools for educational purposes on an outside environment, you should contact your lecturer prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

[illegible]

ICONS Used in this document:

Find out the outcome/ Answers/ Solution



Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.



Recommended Screenshot (with Timestamp) for your Coursework.



Recommended to address this part in your Coursework.

Note: For this activity and other upcoming activities, you shall use any relevant screenshots or discussions to your coursework according to your judgement. I will not be recommending Screenshots/ Recommended part to address in the coursework.

Task 1

Capture the Flag

Likely, this is the final activity during this course. You are provided with a ELF Binaries. Capture the flags and document your findings.

Please ensure that every action you take is documented. You are awarded points for even the smallest action. So, if you are not sure you have completed the task, just add evidence explaining what you have done.

If you have done something and there is no evidence (screenshots and written communication), it is to your detriment and thus, you will not be awarded any points.

You will not be marked negatively, but if you do not highlight enough understanding you may not be awarded points. Partial marking is enabled, so even if you do not get the problem, if you are going in the right direction you will be awarded points.

The task involve reverse engineering ELF binaries. You may use the internet.

The tools recommended (but you may use whatever you are comfortable with):

- Static Analysis : Ghidra

The aim of these problems is to get the flag which is in the format: FLAG{...}

Files Required: f3 (available in moodle)

Find the flag. Save your evidence in the table below. If you write any scripts, copy it to this document too, in a new table.

There are multiple flags for this. If it works, it is a valid answer.

Evidence Name	Evidence Description	Evidence Screenshot

-----End of Activity-----