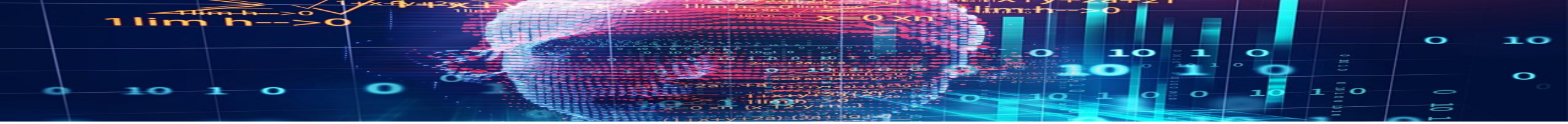
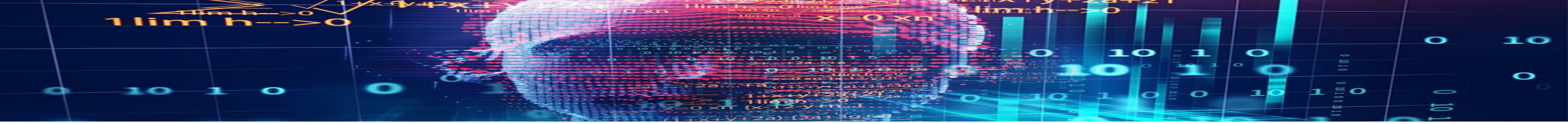
SENG 460 – ECE 579
Practice of Information Security & Privacy Lab
Lab Assignment



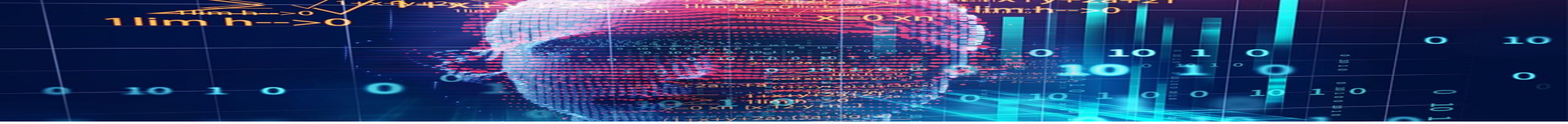
Lab Assignment

- demonstrate your familiarity with the concepts covered in weekly labs
- responding to security incidents requires rapid gathering of information
- automating tasks saves effort and precious minutes



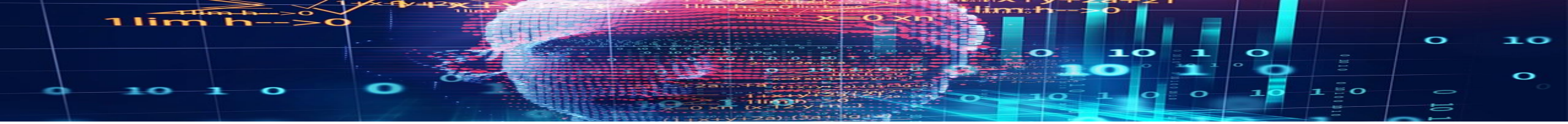
Lab Assignment

- cybercriminals are typosquatting or otherwise trying to defraud your customers with a domain that is very similar to yours and infringing on your brand
- they have been sending malicious emails to your clients in an effort to compromise them
- your website is www.xyzincorporated.com and they registered www.xyzincorporate.com and are hosting fake login pages designed to steal your employee credentials
- you need to process necessary information to report to the following abuse departments: domain registrar, web hosting provider, DNS hosting provider, network provider



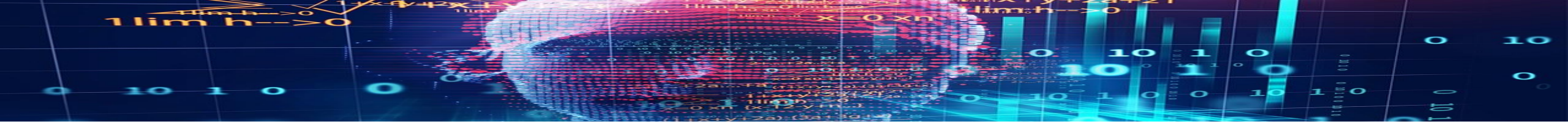
Lab Assignment

- you must build a shell script that takes a domain as input and gathers as much information about it as possible using commands like WHOIS and dig
- you will need to test the script to ensure that it works across a variety of domains and **presents the information in a meaningful way (more useful)**
- include information that is relevant to an incident responder and present efficiently so an analyst would prefer to use your script than run commands themselves
- goal is to gather as much information as possible but be thoughtful about what you provide to the analyst – make their job as easy as possible



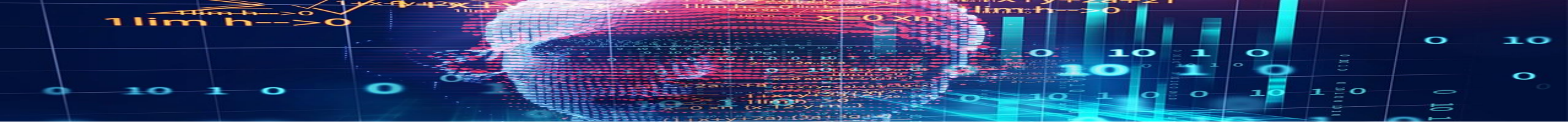
Lab Assignment

- the script should accept the following as input:
  - domain eg. yahoo.com
  - email address eg. bob@yahoo.com
  - URL eg. www.yahoo.com
- the script is better if it accepts the following:
  - IP address eg. 98.137.11.163



Lab Assignment

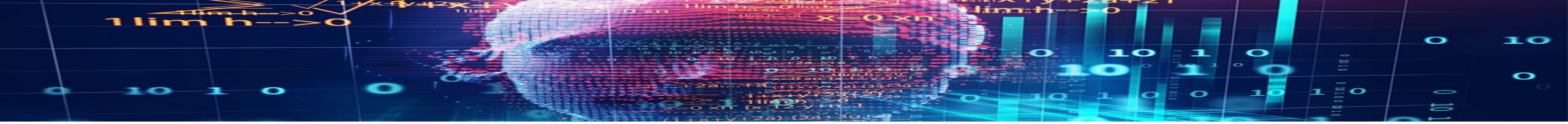
- the script will run a series of commands and present the output accordingly
- **whois** is the most important command to be run
- leverage linux, vi, network tools, shell scripting, sed/awk, cut, grep, as necessary



Lab Assignment

- you will be required to provide a copy of the script and sample output for the following domains:
  - cnn.com
  - yahoo.ca
  - uvic.ca

- the TA's will take your script and may run it against additional unspecified domains



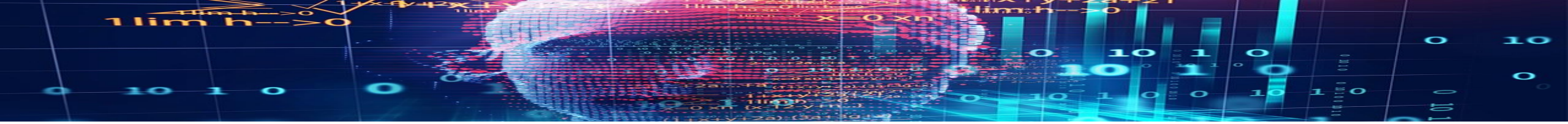
Lab Assignment

- the individual lab assignment will be marked as follows:

  5 marks for functionality
  5 marks for quality of output

…for a total of 10 marks and represents 10% of the course grade

- the lab assignment is due March 18th, 2022 submitted on BrightSpace



End of Lab