cs-sa07-24019
John_Mbithi_Mutave

Introduction To Cybersecurity

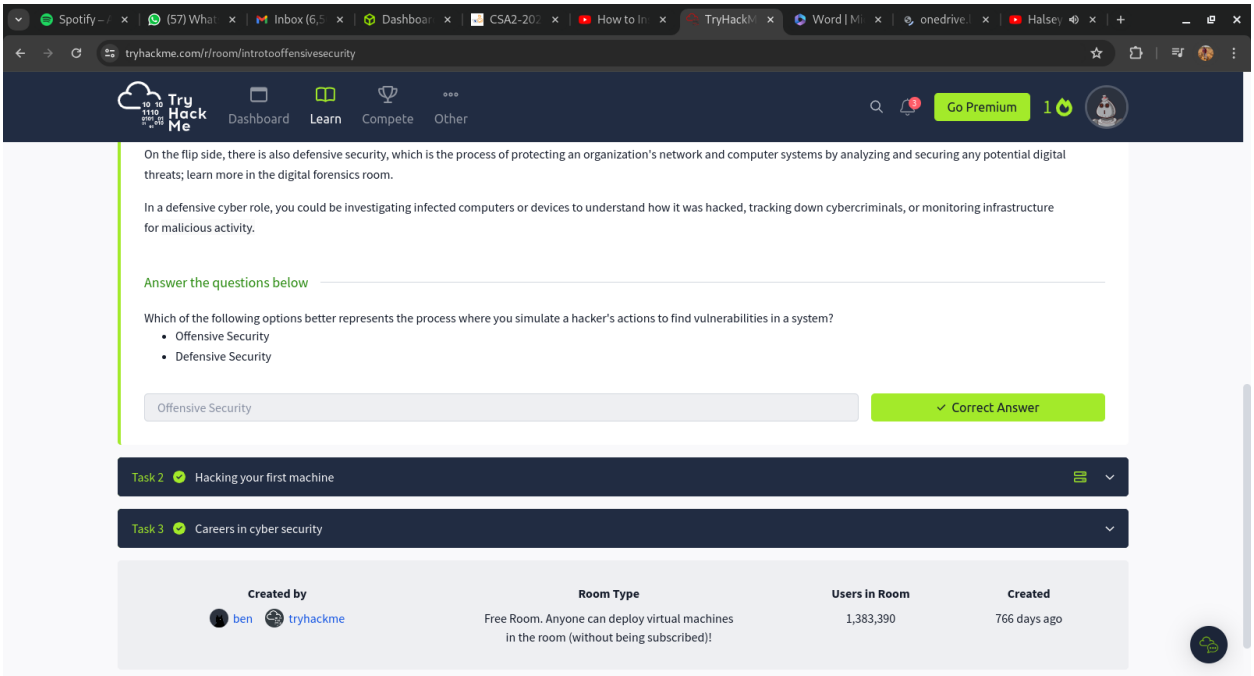
1. Intro to offensive security

In short, offensive security is the process of breaking into computer systems, exploiting software bugs, and finding loopholes in applications to gain unauthorized access to them.

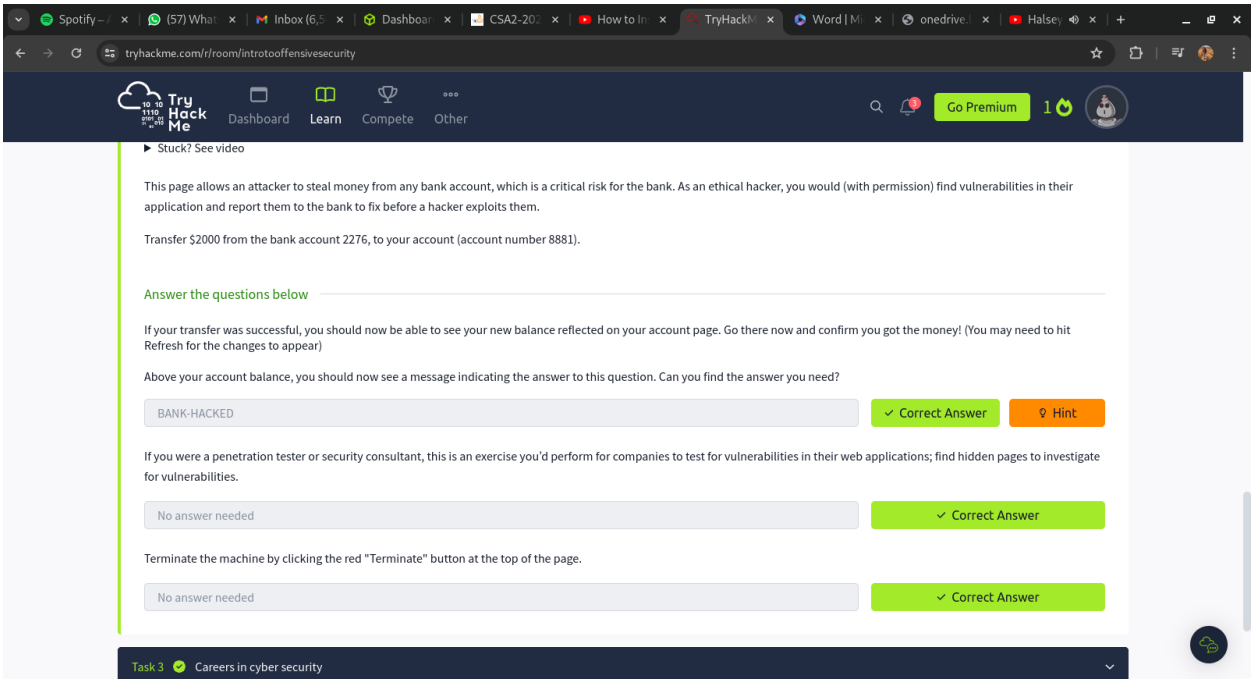
To beat a hacker, you need to behave like a hacker, finding vulnerabilities and recommending patches before a cybercriminal does, as you'll do in this room!

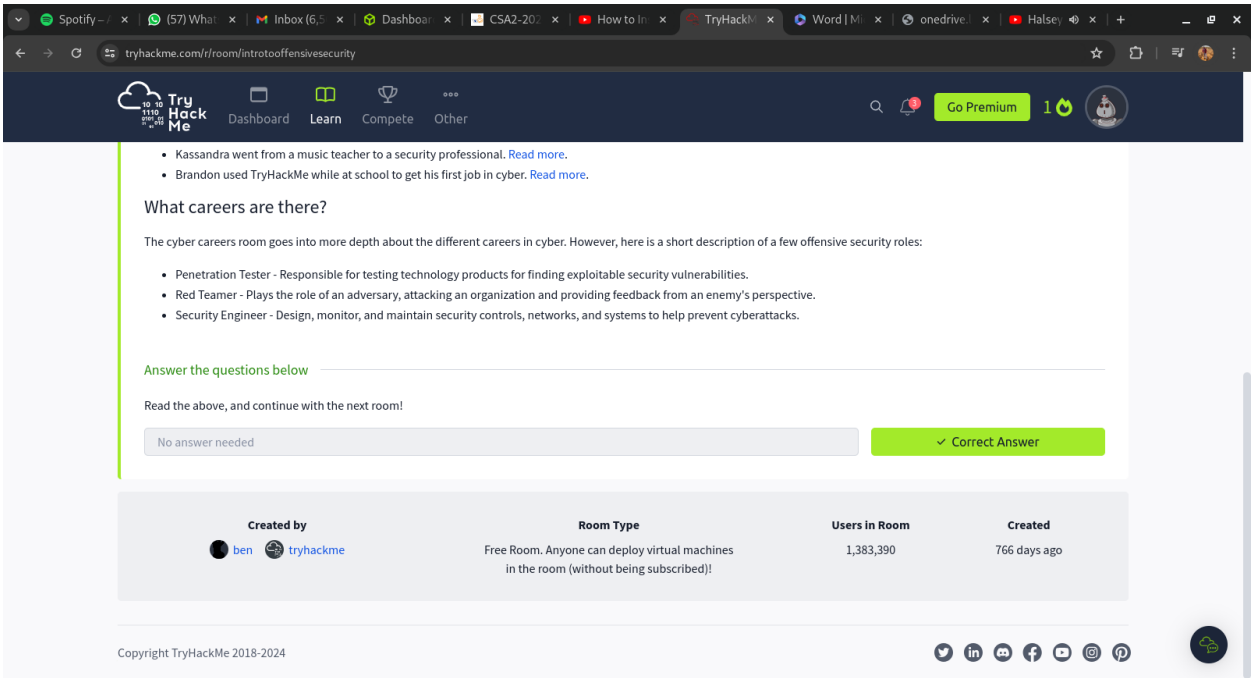
On the flip side, there is also defensive security, which is the process of protecting an organization's network and computer systems by analyzing and securing any potential digital threats; learn more in the digital forensics room.

In a defensive cyber role, you could be investigating infected computers or devices to understand how it was hacked, tracking down cybercriminals, or monitoring infrastructure for malicious activity.



cs-sa07-24019
John_Mbithi_Mutave





Shareable Link - http://www.tryhackme.com/r/room/introtooffensivesecurity

Conclusion

The cyber careers room goes into more depth about the different careers in cyber. However, here is a short description of a few offensive security roles:

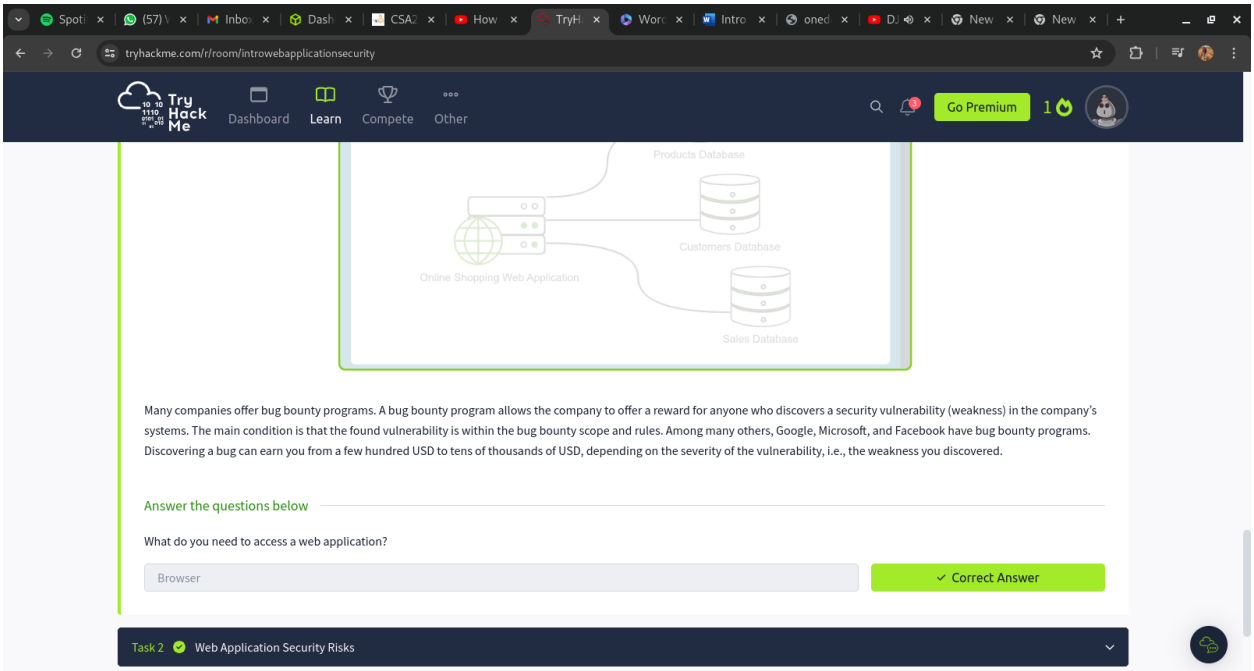
- Penetration Tester - Responsible for testing technology products for finding exploitable security vulnerabilities.
- Red Teamer - Plays the role of an adversary, attacking an organization and providing feedback from an enemy's perspective.
- Security Engineer - Design, monitor, and maintain security controls, networks, and systems to help prevent cyberattacks.

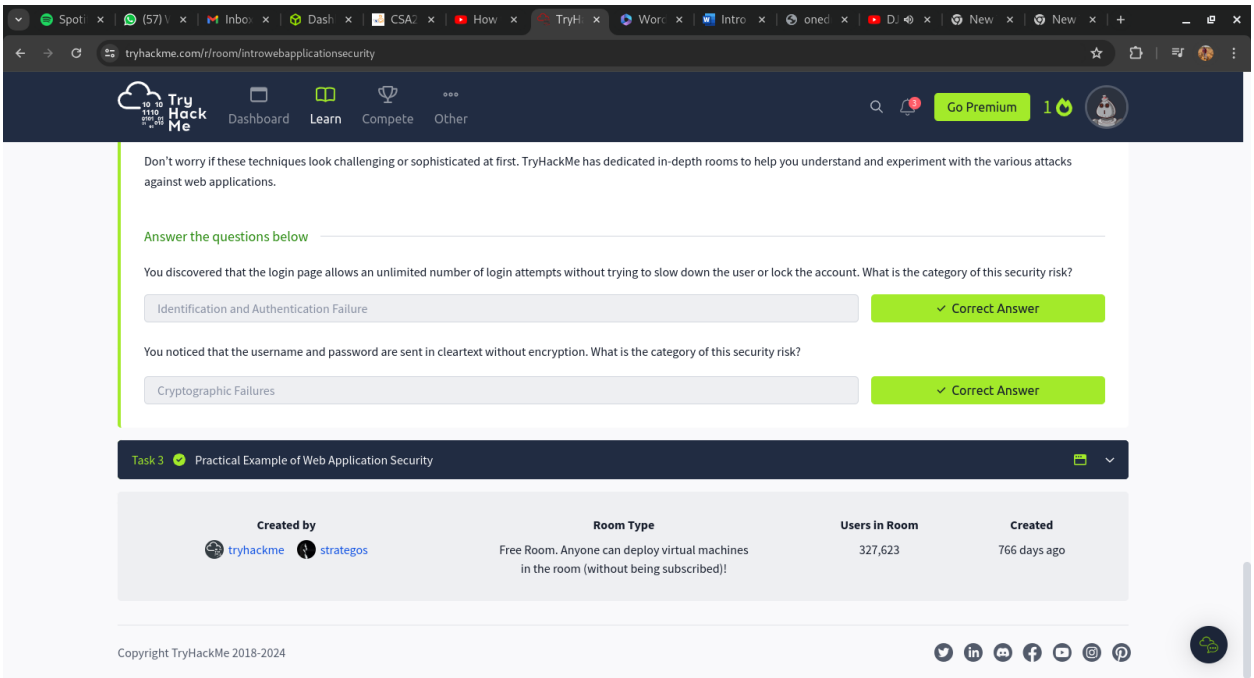
2. Web application security

A web application is like a “program” that we can use without installation as long as we have a modern standard web browser, such as Firefox, Safari, or Chrome. Consequently, instead of installing every program you need, you only need to browse the related page. The following are some examples of web applications:

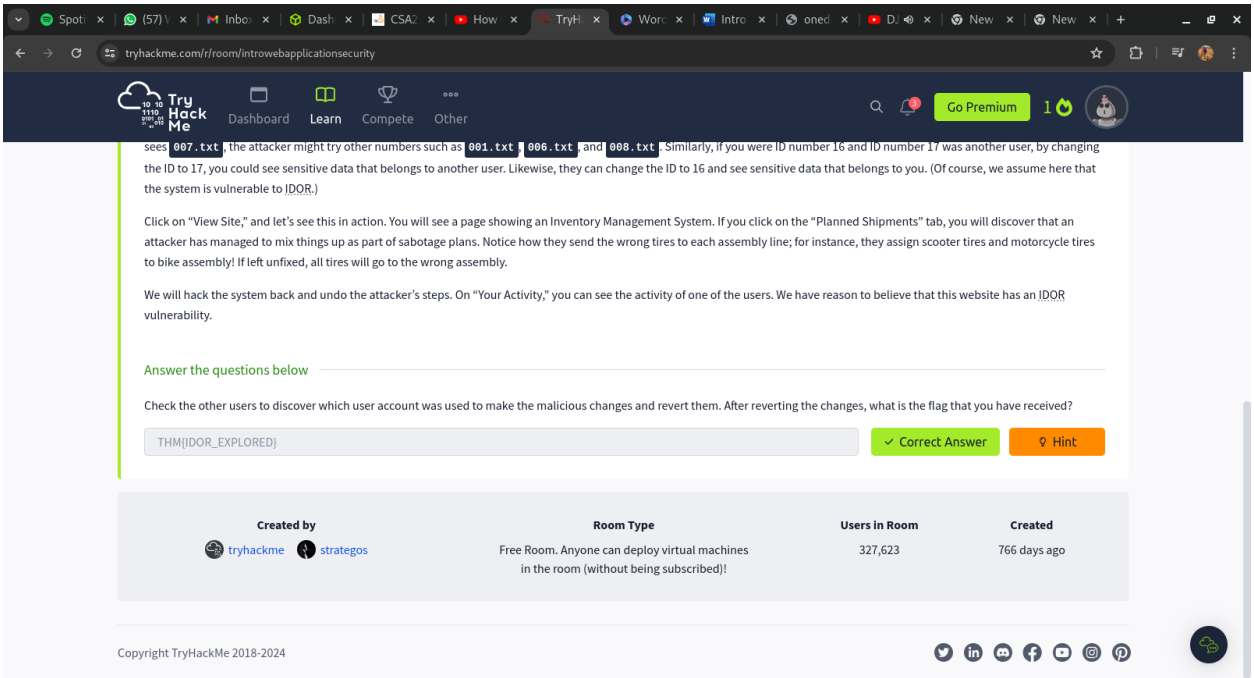
- Webmail such as Tutanota, Protonmail, Outlook, and Gmail
- Online office suites such as Microsoft Office 365 (Word, Excel, and PowerPoint), Google Drive (Docs, Sheets, and Slides), and Zoho Office (Writer, Sheet, and Show)
- Online shopping such as Amazon.com, AliExpress, and Etsy

cs-sa07-24019
John_Mbithi_Mutave





cs-sa07-24019
John_Mbithi_Mutave



Conclusion

The idea of a web application is that it is a program running on a remote server. A server refers to a computer system running continuously to "serve" the clients. In this case, the server will run a specific type of program that can be accessed by web browsers.

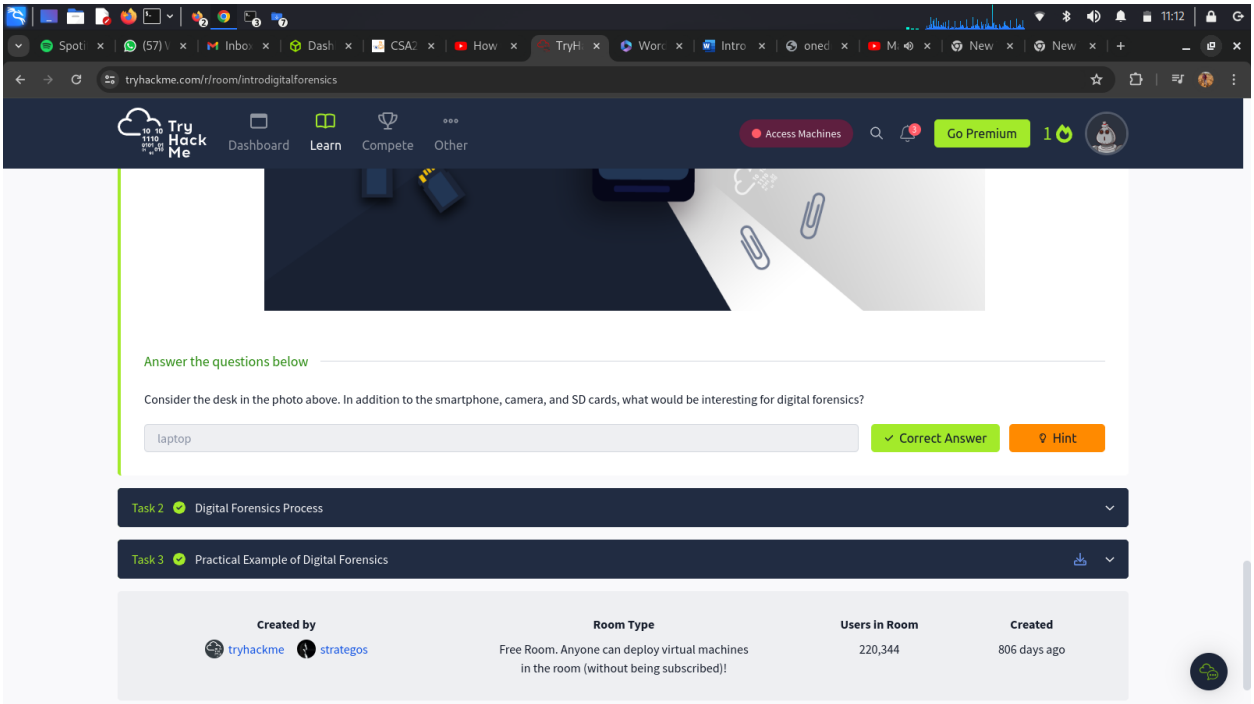
3. Intro to Digital Forensics

Forensics is the application of science to investigate crimes and establish facts. With the use and spread of digital systems, such as computers and smartphones, a new branch of forensics was born to investigate related crimes: computer forensics, which later evolved into, *digital forensics*.

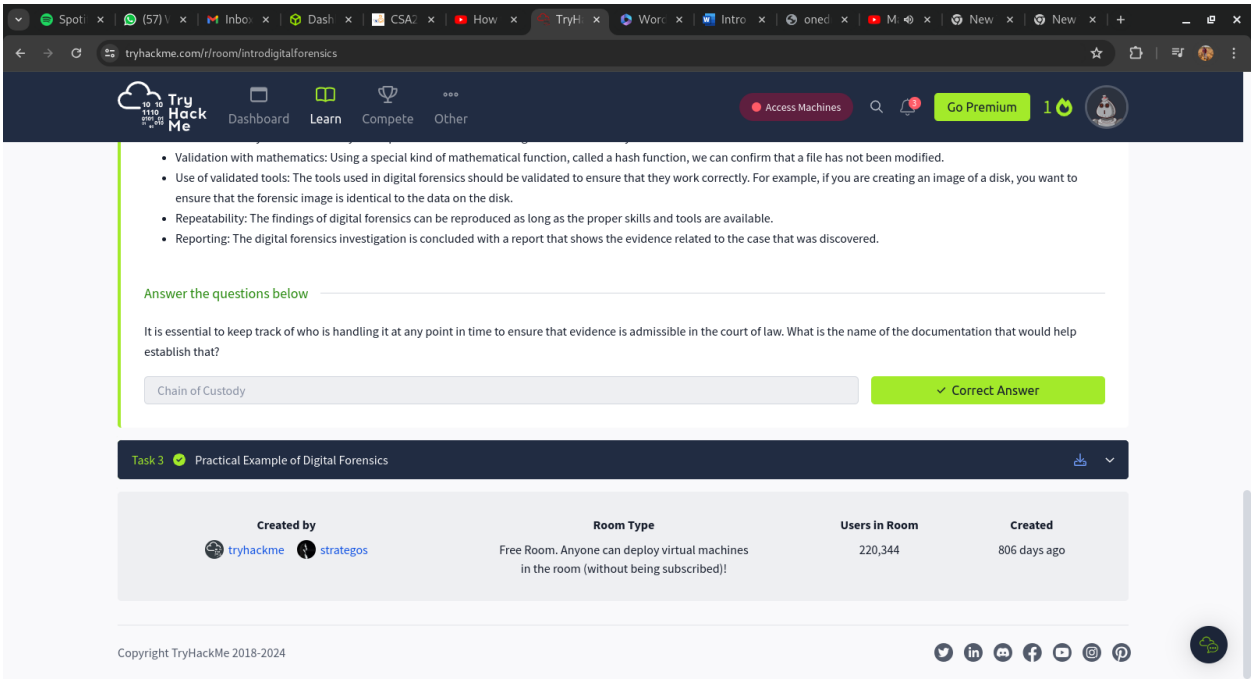
Think about the following scenario. The law enforcement agents arrive at a crime scene; however, part of this crime scene includes digital devices and media. Digital devices include desktop computers, laptops, digital cameras, music players, and

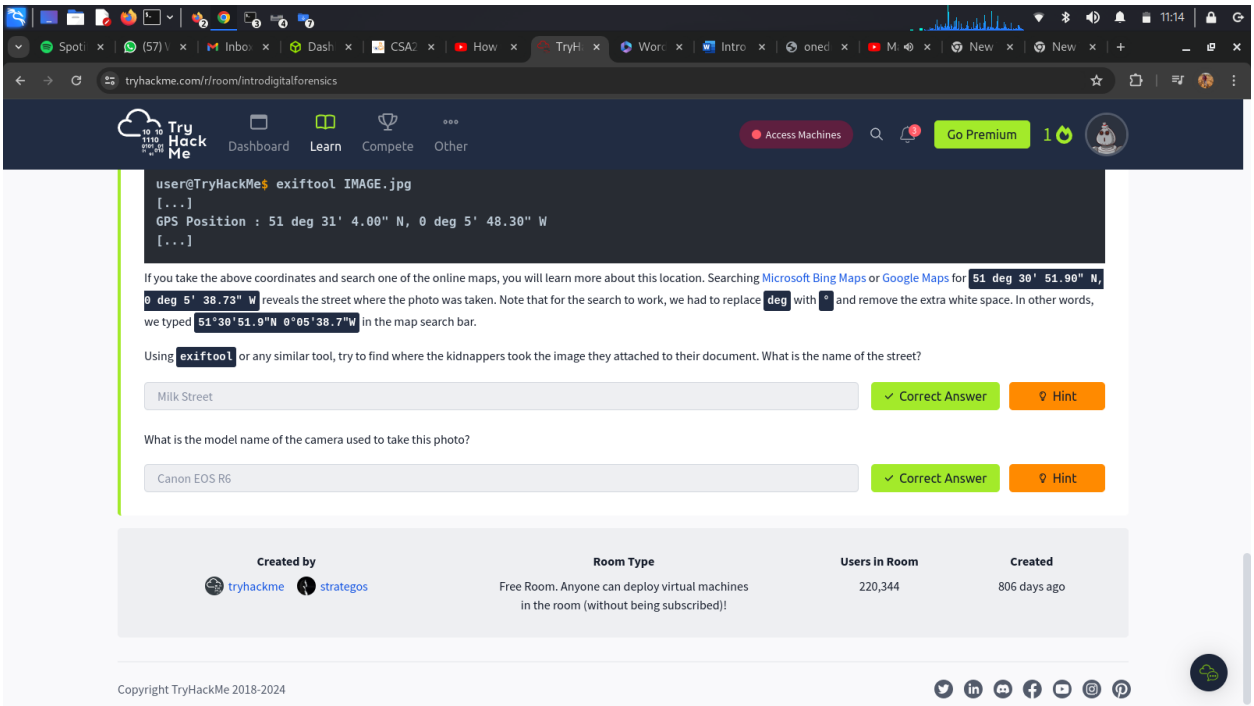
smartphones, to name a few. Digital media includes CDs, DVDs, USB flash memory drives, and external storage. A few questions arise:

- How should the police collect digital evidence, such as smartphones and laptops? What are the procedures to follow if the computer and smartphone are running?
- How to transfer the digital evidence? Are there certain best practices to follow when moving computers, for instance?
- How to analyze the collected digital evidence? Personal device storage ranges between tens of gigabytes to several terabytes; how can this be analyzed?



cs-sa07-24019
John_Mbithi_Mutave





Shareable link - https://t.co/tzfS5tMXwv

Conclusion

cs-sa07-24019
John_Mbithi_Mutave

Digital forensics is the application of computer science to investigate digital evidence for a legal purpose. Digital forensics is used in two types of investigations:

1. **Public-sector investigations** refer to the investigations carried out by government and law enforcement agencies. They would be part of a crime or civil investigation.
2. **Private-sector investigations** refer to the investigations carried out by corporate bodies by assigning a private investigator, whether in-house or outsourced. They are triggered by corporate policy violations.

Whether investigating a crime or a corporate policy violation, part of the evidence is related to digital devices and digital media. This is where digital forensics comes into play and tries to establish what has happened. Without trained digital forensics investigators, it won’t be possible to process any digital evidence properly.