

*ISSACK WAITHAKA*  
*cs-sa07-24085*

# INTRO TO OFFENSIVE SECURITY

- Offensive security is breaking into computer systems, exploiting software bugs and finding loopholes in order to gain unauthorized access to them.
- Defensive security is the protecting an organization's network and computer systems by analyzing any potential digital ganger.

## Questions

1.

Answer the questions below

Which of the following options better represents the process where you simulate a hacker's actions to find vulnerabilities in a system?

- Offensive Security
- Defensive Security

Offensive Security

✓ Correct Answer

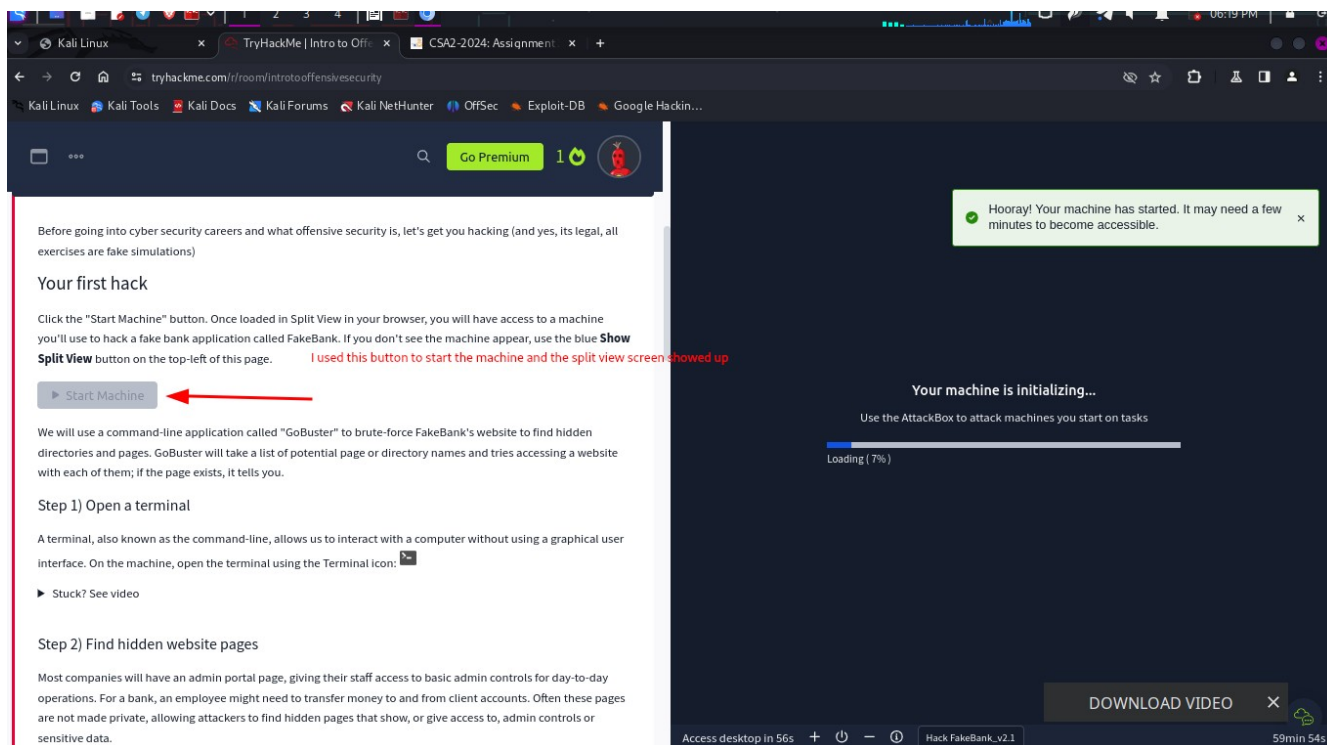
Task 1: What Is Offensive Security?

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!

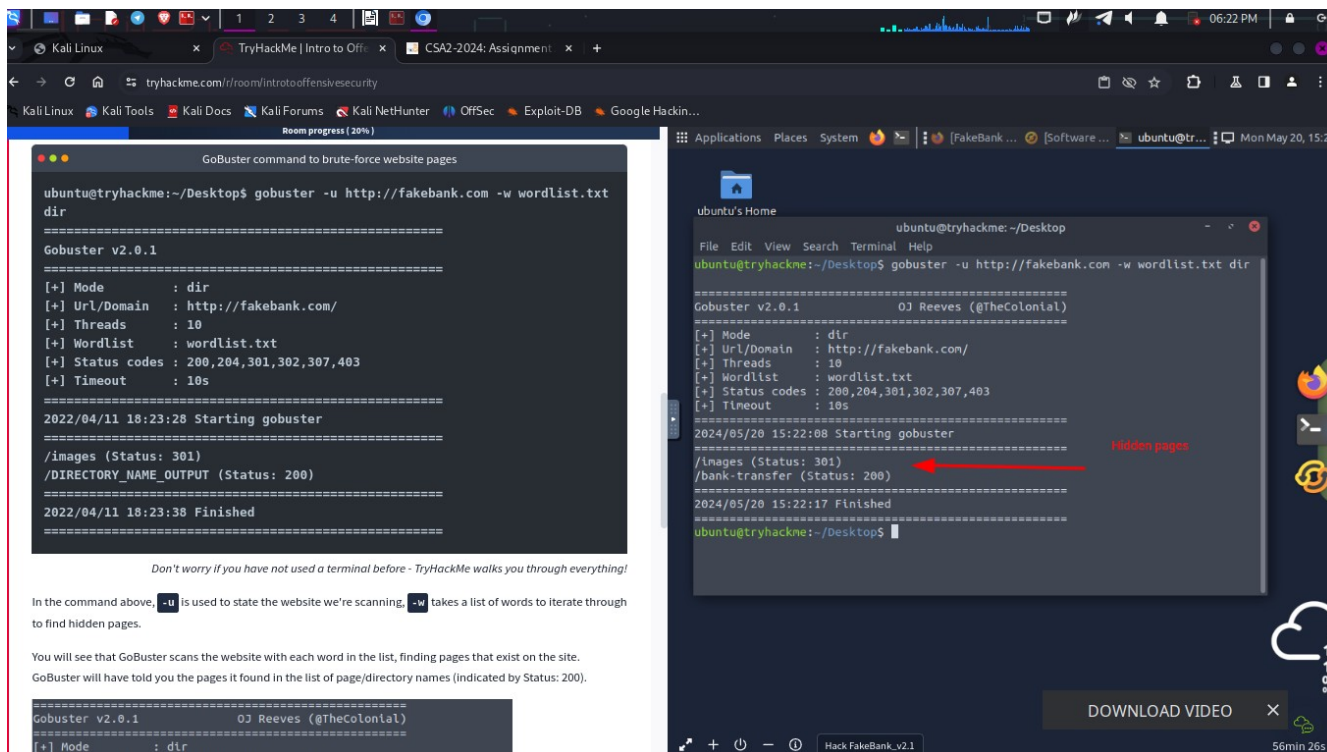
## Hacking your first machine

- The first thing was to start the machine

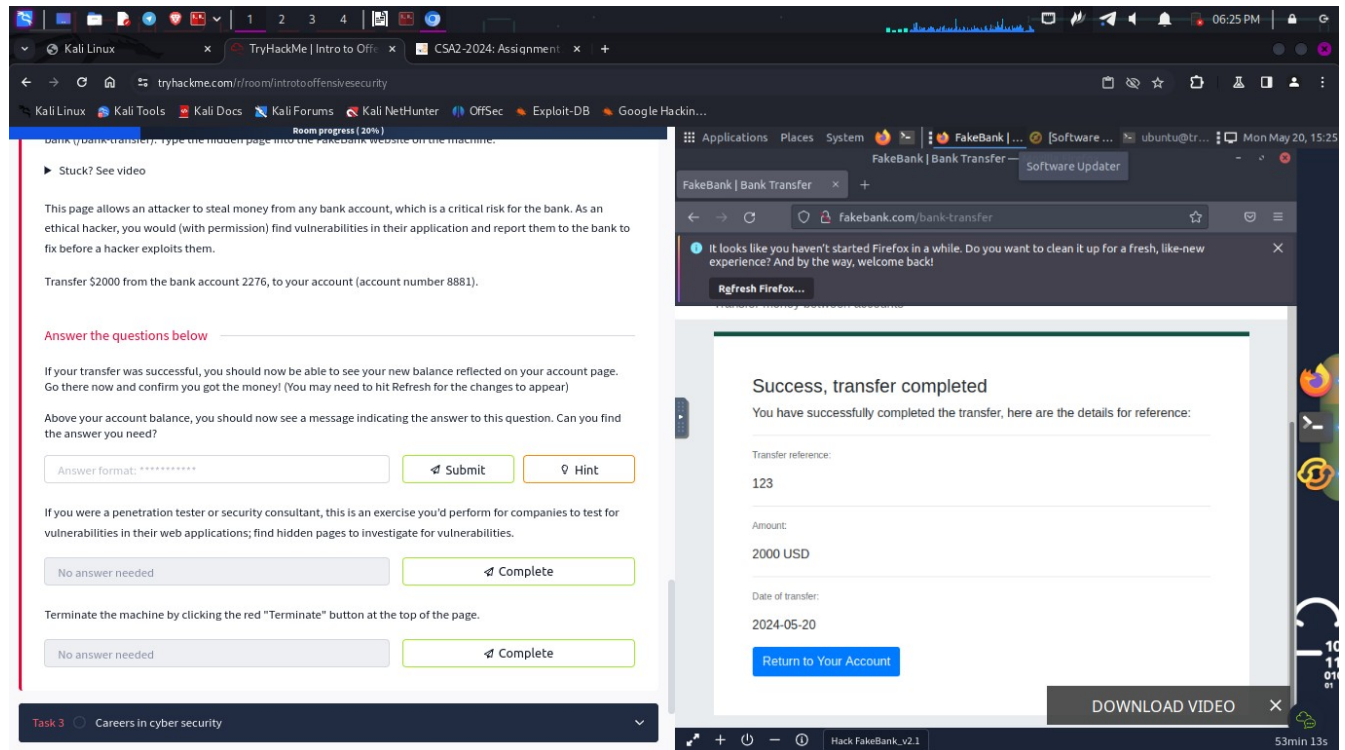


-The second thing was to start the terminal

- The next step was finding hidden websites. We used gobuster command to find the hidden pages



- the last step was to transferred \$2000 from the bank account 2276 to my account



## Questions

1.

Answer the questions below

If your transfer was successful, you should now be able to see your new balance reflected on your account page. Go there now and confirm you got the money! (You may need to hit Refresh for the changes to appear)

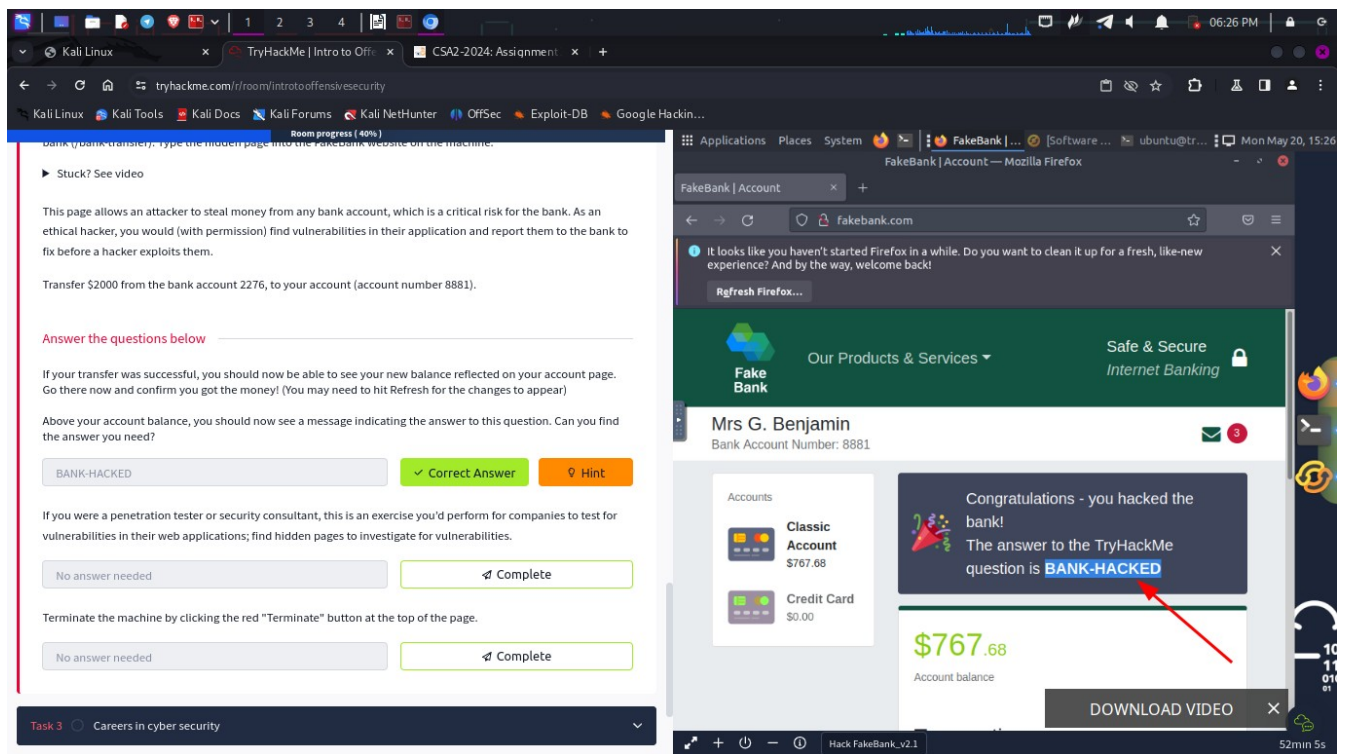
Above your account balance, you should now see a message indicating the answer to this question. Can you find the answer you need?

BANK-HACKED

✓ Correct Answer

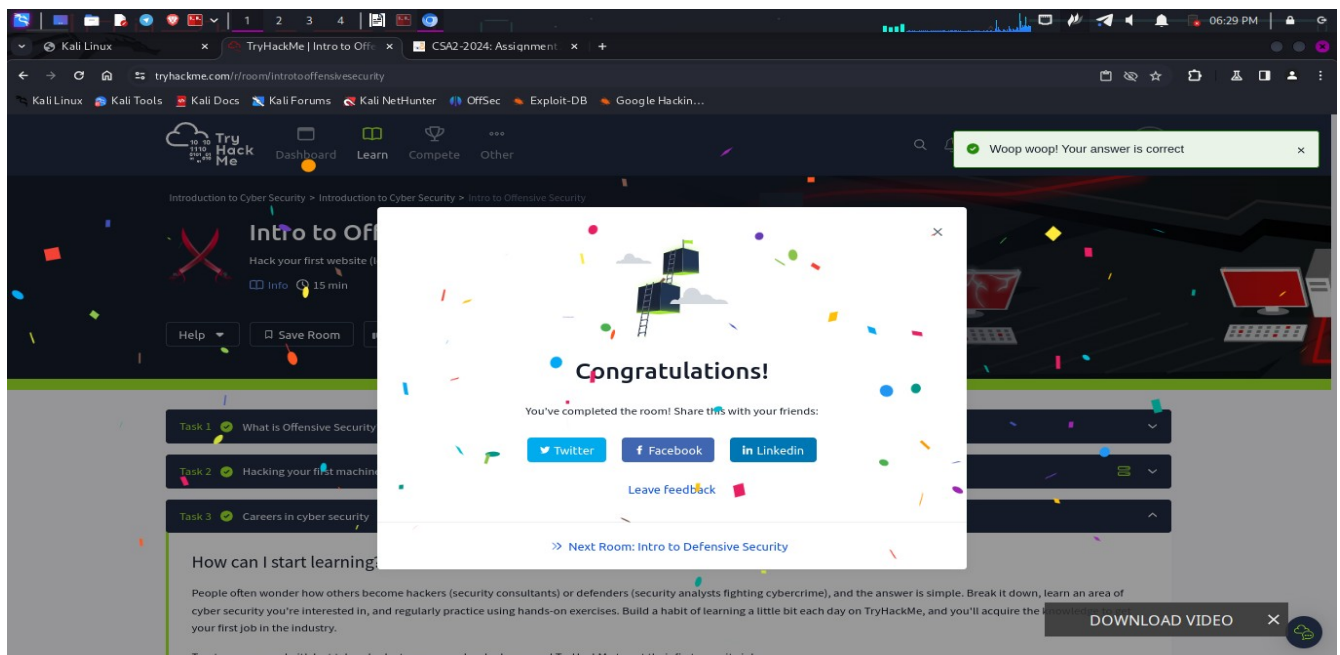
💡 Hint

When I went back to home page I found the flag



## Careers in cyber security

- I learnt that there are various fields in security.
- I read peoples testimonies and how they started their careers in cyber security



# WEB APPLICATION SECURITY

## Introduction

- A web application is a program that is stored on a remote server and is accessible over the internet through a browser like chrome, brave etc.

## Questions

1.

Answer the questions below

What do you need to access a web application?

browser

✓ Correct Answer

## Web Application Security Risks

- The attacker may try to discover your password when you try to login
- An attacker may try to breach system by adding malicious codes to the search bar
- The attacker would check payment details sent in clear text or using weak encryption
- Identification is the ability to identify a user while authentication is proving that the user is whom they claim to be

## Questions

1.

Answer the questions below

You discovered that the login page allows an unlimited number of login attempts without trying to slow down the user or lock the account. What is the category of this security risk?

Identification and Authentication Failure

✓ Correct Answer

We cannot cover everything, but we will present a few formal categories from OWASP Top Ten. Don't worry if these techniques sound alien to you; TryHackMe walks you through each vulnerability.

### Identification and Authentication Failure

Identification refers to the ability to identify a user uniquely. In contrast, authentication refers to the ability to prove that the user is whom they claim to be. The online shop must confirm the user's identity and authenticate them before they can use the system. However, this step is prone to different types of weaknesses. Example weaknesses include:

- Allowing the attacker to use brute force, i.e., try many passwords, usually using automated tools, to find valid login credentials.
- Allowing the user to choose a weak password. A weak password is usually easy to guess.
- Storing the users' passwords in plain text. If the attacker manages to read the file containing the passwords, we don't want them to be able to learn the stored password.

Username	Password
----------	----------



2.

You noticed that the username and password are sent in cleartext without encryption. What is the category of this security risk?

Cryptographic Failures

✓ Correct Answer

## Cryptographic Failures

This category refers to the failures related to cryptography. Cryptography focuses on the processes of encryption and decryption of data. Encryption scrambles cleartext into ciphertext, which should be gibberish to anyone who does not have the secret key to decrypt it. In other words, encryption ensures that no one can read the data without knowing the secret key. Decryption converts the ciphertext back into the original cleartext using the secret key. Examples of cryptographic failures include:

- Sending sensitive data in clear text, for example, using HTTP instead of HTTPS. HTTP is the protocol used to access the web, while HTTPS is the secure version of HTTP. Others can read everything you send over HTTP, but not HTTPS.
- Relying on a weak cryptographic algorithm. One old cryptographic algorithm is to shift each letter by one. For instance, "TRY HACK ME" becomes "USZ IBDL NF." This cryptographic algorithm is trivial to break.
- Using default or weak keys for cryptographic functions. It won't be challenging to break the encryption that used 1234 as the secret key.

## Practical Example of Web Application Security

**Task 3 - Practical Example of Web Application Security**

This task will investigate a vulnerable website that uses Insecure Direct Object References (IDOR). IDOR falls under the category of Broken Access Control. Broken access control means that an attacker can access information or perform actions not intended for them. Consider the case where a web server receives user-supplied input to retrieve objects (files, data, documents) and that they are numbered sequentially. Let's say that the user has permission to access a photo named `IMG_1003.JPG`. We might guess that there are also `IMG_1002.JPG` and `IMG_1004.JPG`; however, the web application should not provide us with that image even if we figured out its name. In general, an IDOR vulnerability can occur if too much trust has been placed on that input data. In other words, the web application does not validate whether the user has permission to access the requested object.

Just providing the correct URL for a user or a product does not necessarily mean the user should be able to access that URL. For instance, consider the product page `https://store.tryhackme.thm/products/product?id=52`. We can expect this URL to provide details about product number `52`. In the database, items would be assigned numbers sequentially. The attacker would try other numbers such as `51` or `53` instead of `52`; this might reveal other retired or unreleased products if the web application is vulnerable.

Let's consider a more critical example; the URL `https://store.tryhackme.thm/customers/user?id=10` would return the user with `id=10`. Again, we expect the users to have sequential ID numbers. The attacker would try other numbers and possibly access other user accounts. This vulnerability might work with sequential files; for instance, if the attacker sees `007.txt`, the attacker might try other numbers such as `001.txt`, `006.txt`, and `008.txt`. Similarly, if you were ID number 16 and ID number 17 was another user, by changing the ID to 17, you could see sensitive data that belongs to another user. Likewise, they can change the ID to 16 and see sensitive data that belongs to you. (Of course, we assume here that the system is vulnerable to IDOR.)

Click on "View Site," and let's see this in action. You will see a page showing an Inventory Management System. If you click on the "Planned Shipments" tab, you will discover that an attacker has managed to mix things up as part of sabotage plans. Notice how they send the wrong tires to each assembly line; for instance, they assign scooter tires and motorcycle tires to bike assembly! If left unfixed, all tires will go to the wrong assembly.

We will hack the system back and undo the attacker's steps. On "Your Activity," you can see the activity of one of the users. We have reason to believe that this website has an IDOR vulnerability.

[View Site](#)

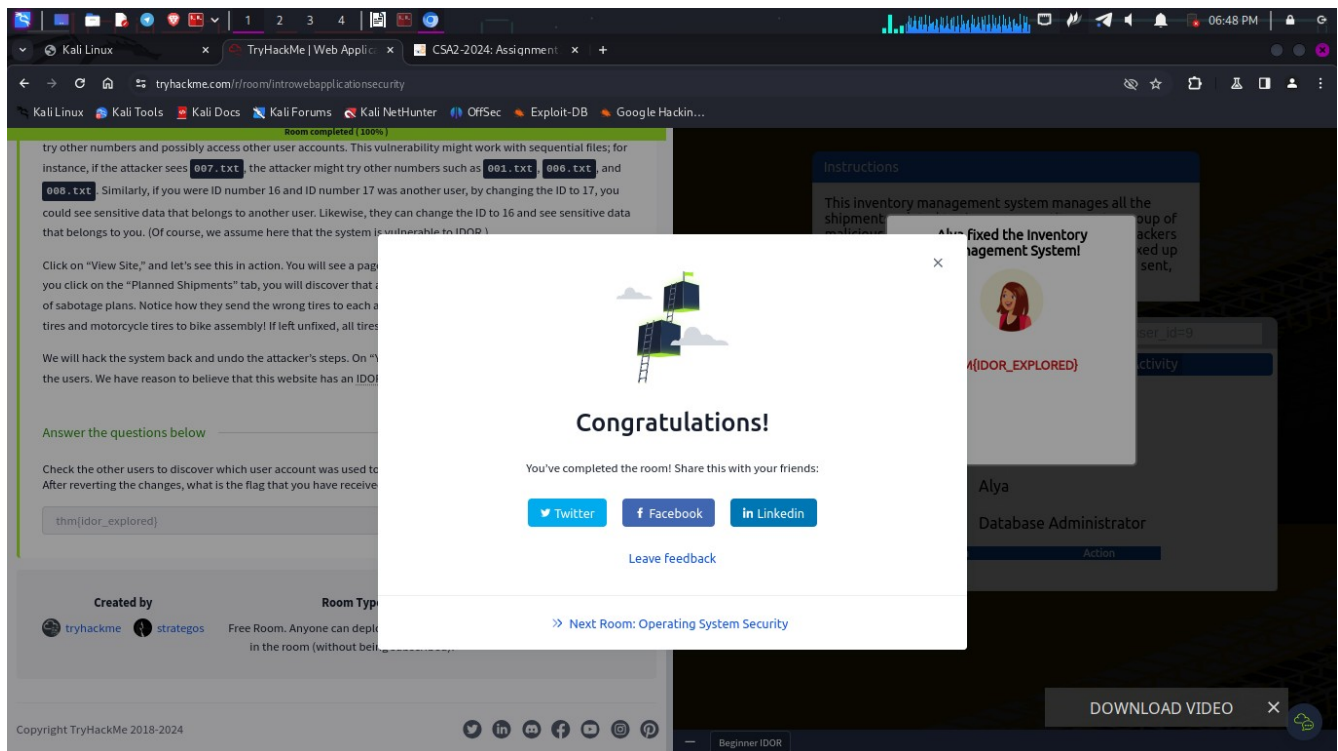
[DOWNLOAD VIDEO](#)

- We start by clicking the view site button

- We used broken access to alter with the URL and manage to get the id of the employee whose user's account was used to make malicious changes.







## INTRO TO DIGITAL FORENSICS

### Introduction

- This is identifying, analyzing. Processing and reporting data stored electronically
- It was born due to the usage and spread of digital systems like computers and smartphone

## Questions

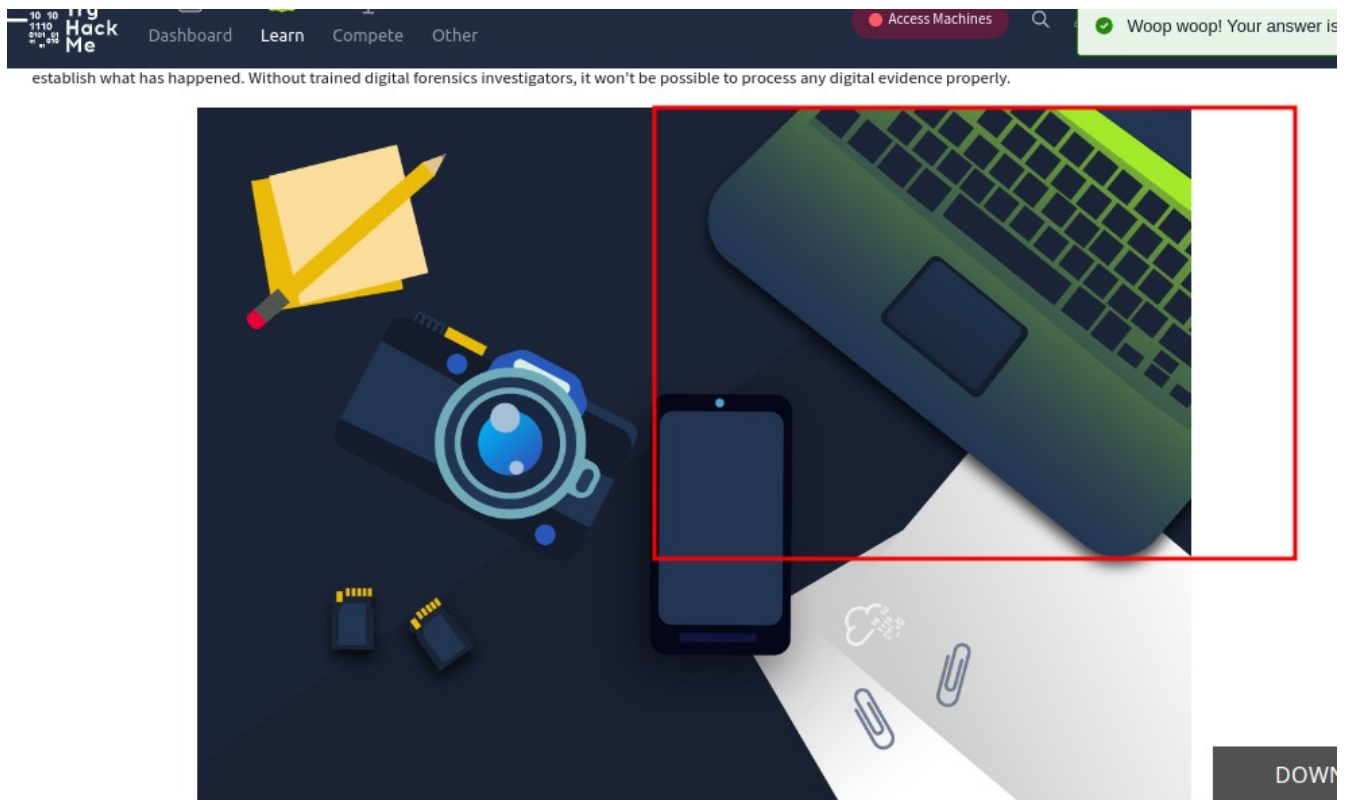
1.

Consider the desk in the photo above. In addition to the smartphone, camera, and SD cards, what would be interesting for digital forensics?

laptop

✓ Correct Answer

🔍 Hint



## Digital Forensics Process

When you arrive at the scene you:

- Acquire evidence – collecting digital devices
- Establish chain of custody – fill out forms
- Place evidence in a safe container
- Transport evidence to the lab

- At the lab:

- Retrieve digital evidence from the container
- Create a forensic copy
- Return digital evidence into the container
- Start processing the copy on the workstation

## Questions

1.

Answer the questions below

It is essential to keep track of who is handling it at any point in time to ensure that evidence is admissible in the court of law. What is the name of the documentation that would help establish that?

Chain of custody

✓ Correct Answer

3. Return the digital evidence to the secure container: You will be working on the copy. If you damage the copy, you can always create a new one.
4. Start processing the copy on your forensics workstation.

The above steps have been adapted from [Guide to Computer Forensics and Investigations, 6th Edition](#).

More generally, according to the former director of the Defense Computer Forensics Laboratory, Ken Zatyko, digital forensics includes:

- ~~Proper search authority. Investigators cannot commence without the proper legal authority.~~
- Chain of custody: This is necessary to keep track of who was holding the evidence at any time.
- Validation with mathematics: Using a special kind of mathematical function, called a hash function, we can confirm that a file has not been modified.
- Use of validated tools: The tools used in digital forensics should be validated to ensure that they work correctly. For example, if you are creating an image of a disk, you want to ensure that the forensic image is identical to the data on the disk.
- Repeatability: The findings of digital forensics can be reproduced as long as the proper skills and tools are available.
- Reporting: The digital forensics investigation is concluded with a report that shows the evidence related to the case that was discovered.

Answer the questions below

It is essential to keep track of who is handling it at any point in time to ensure that evidence is admissible in the court of law. What is the name of the documentation that would help establish that?

## Practical Example of Digital Forensics

**Task 3** Practical Example of Digital Forensics

Everything we do on our digital devices, from smartphones to computers, leaves traces. Let's see how we can use this in the subsequent investigation.

Our cat, Gado, has been kidnapped. The kidnapper has sent us a document with their requests in MS Word Document format. We have converted the document to PDF format and extracted the image from the MS Word file for your convenience.

You can download the attached file to your local machine for inspection; however, for your convenience we have added the files to the AttackBox. To follow along, open the terminal on the AttackBox, then go to the directory `/root/Rooms/introdigitalforensics` as shown below. In the following terminal output, we changed to the directory containing the case files.

```
root# cd /root/Rooms
root# cd introdigitalforensics
root# ls
letter-image.jpg  ransom-letter.doc  ransom-letter.pdf  ransom-lettter-2.zip
```

**Document Metadata**

When you create a text file, `.TXT`, some metadata gets saved by the Operating System, such as file creation date and last modification date. However, much information gets kept within the file's metadata when you use a more advanced editor, such as MS Word. There are various ways to read the file metadata; you might open them within their official viewer/editor or use a suitable forensic tool. Note that exporting the file to other formats, such as `.PDF`, would maintain most of the metadata of the original document, depending on the PDF tool used.

[Download Task Files](#)

[PDF DOWNLOAD VIDEO](#)

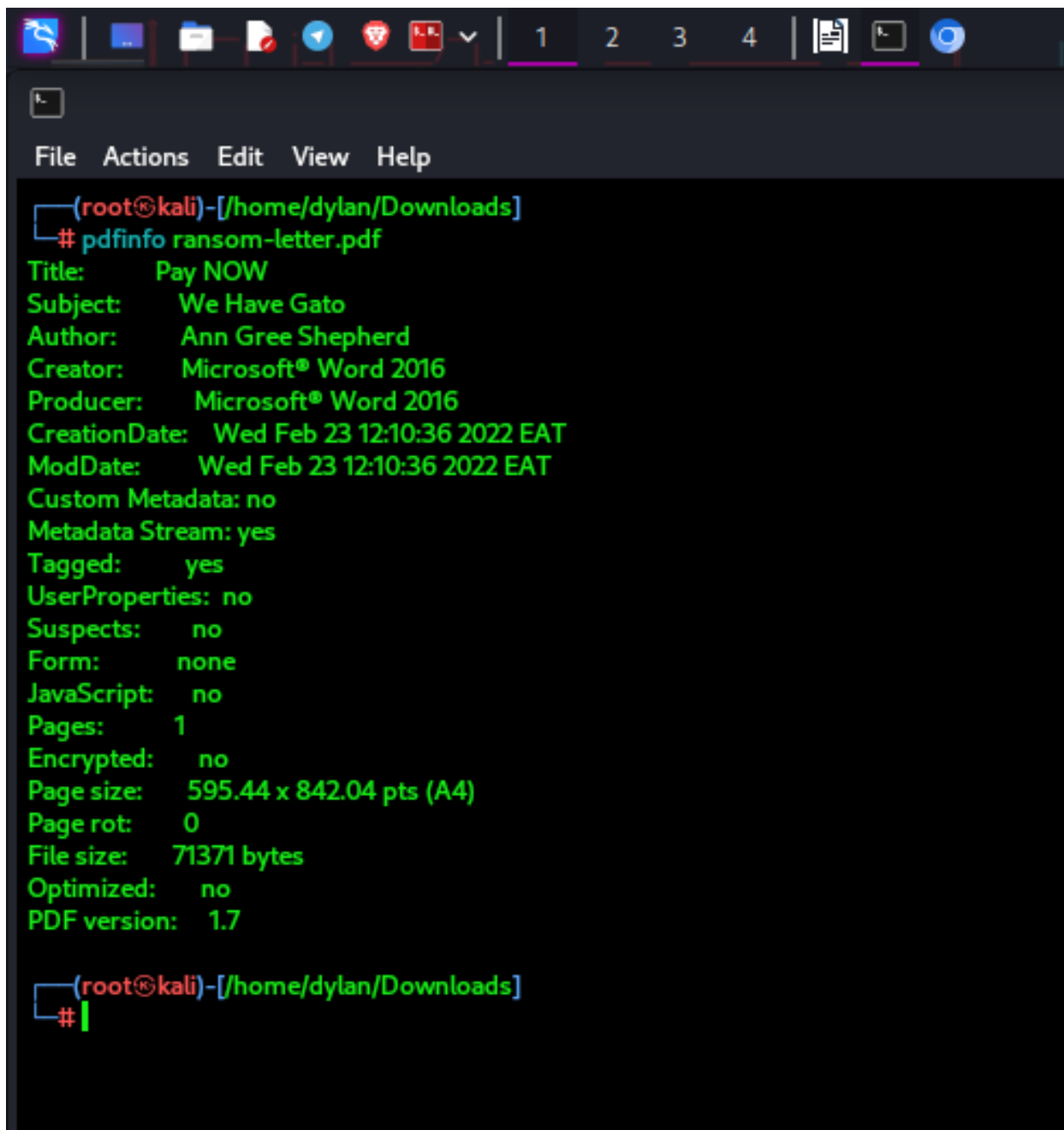
- I download these files in my local machine

```
root@kali:~# unzip ransom-lettter-2-1645608985174.zip
Archive: ransom-lettter-2-1645608985174.zip
  inflating: letter-image.jpg
  inflating: ransom-letter.doc
  inflating: ransom-letter.pdf

root@kali:~#
```

- I unzipped the file and got three other files

- I used `pdfinfo` tool to find the metadata of the `inflating-letter.pdf` and here are the results



```
(root@kali)-[/home/dylan/Downloads]
# pdftinfo ransom-letter.pdf
Title:      Pay NOW
Subject:     We Have Gato
Author:      Ann Gree Shepherd
Creator:     Microsoft® Word 2016
Producer:    Microsoft® Word 2016
CreationDate: Wed Feb 23 12:10:36 2022 EAT
ModDate:     Wed Feb 23 12:10:36 2022 EAT
Custom Metadata: no
Metadata Stream: yes
Tagged:      yes
UserProperties: no
Suspects:    no
Form:        none
JavaScript:   no
Pages:       1
Encrypted:    no
Page size:    595.44 x 842.04 pts (A4)
Page rot:     0
File size:    71371 bytes
Optimized:    no
PDF version:  1.7

(root@kali)-[/home/dylan/Downloads]
#
```

## Question

1.

Answer the questions below

Using `pdftinfo`, find out the author of the attached PDF file, `ransom-letter.pdf`.

Ann Gree Shepherd

✓ Correct Answer

```
(root@kali)~[/home/dylan/Downloads]
# pdftools ransom-letter.pdf
Title:      Pay NOW
Subject:    We Have Gato
Author:     Ann Gree Shepherd
Creator:    Microsoft® Word 2016
Producer:   Microsoft® Word 2016
CreationDate:  Wed Feb 23 12:10:36 2022 EAT
ModDate:    Wed Feb 23 12:10:36 2022 EAT
Custom Metadata: no
Metadata Stream: yes
Tagged:     yes
UserProperties: no
Suspects:   no
Form:       none
JavaScript: no
Pages:      1
Encrypted:   no
Page size:   595.44 x 842.04 pts (A4)
Page rot:    0
File size:   71371 bytes
Optimized:   no
PDF version: 1.7

(root@kali)~[/home/dylan/Downloads]
#
```



## questions

1.

we typed `51.30 51.9 W 0 00 38.7 W` in the map search bar.

Using `exiftool` or any similar tool, try to find where the kidnappers took the image they attached to their document. What is the name of the street?

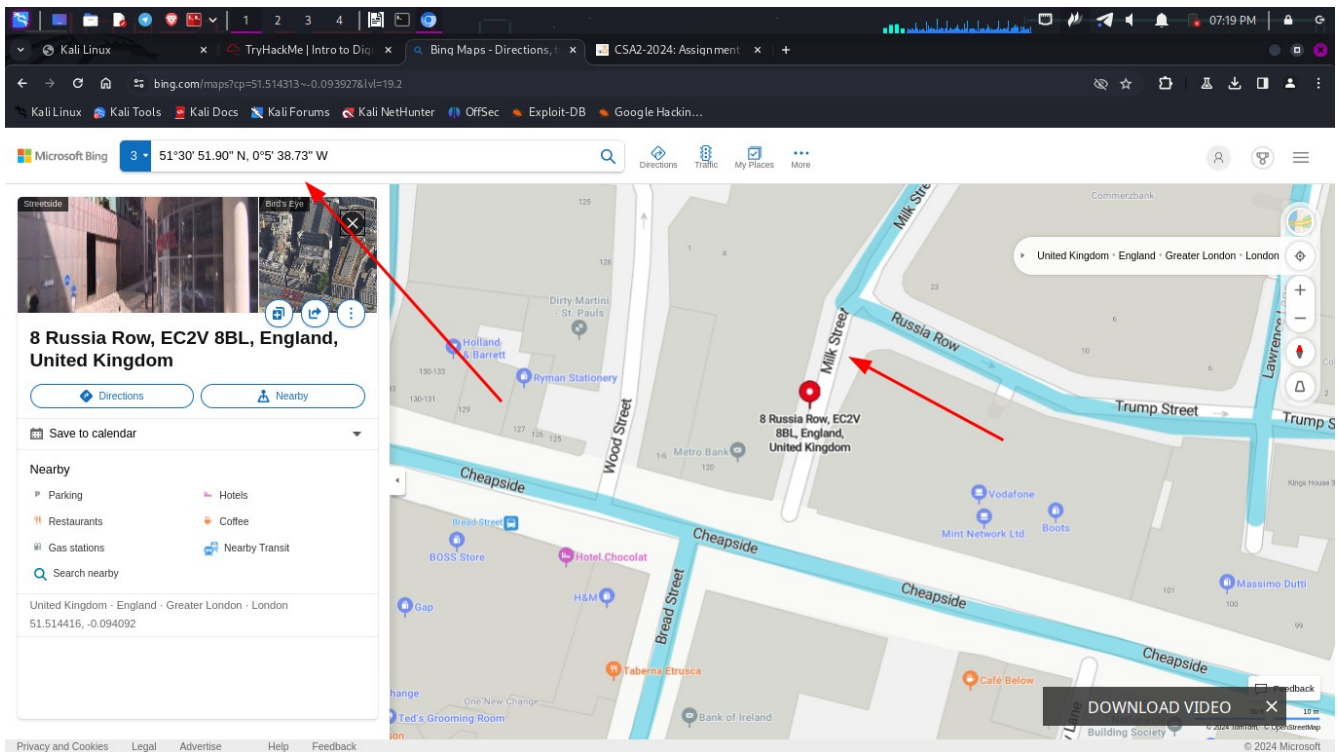
milk street

✓ Correct Answer

🔍 Hint

- I used the exiftool tool to get more information about the image
- To get the location I took the GPS latitude and longitude from the results

and paste them into google bing to get the exact location



and got the location where the image was taken

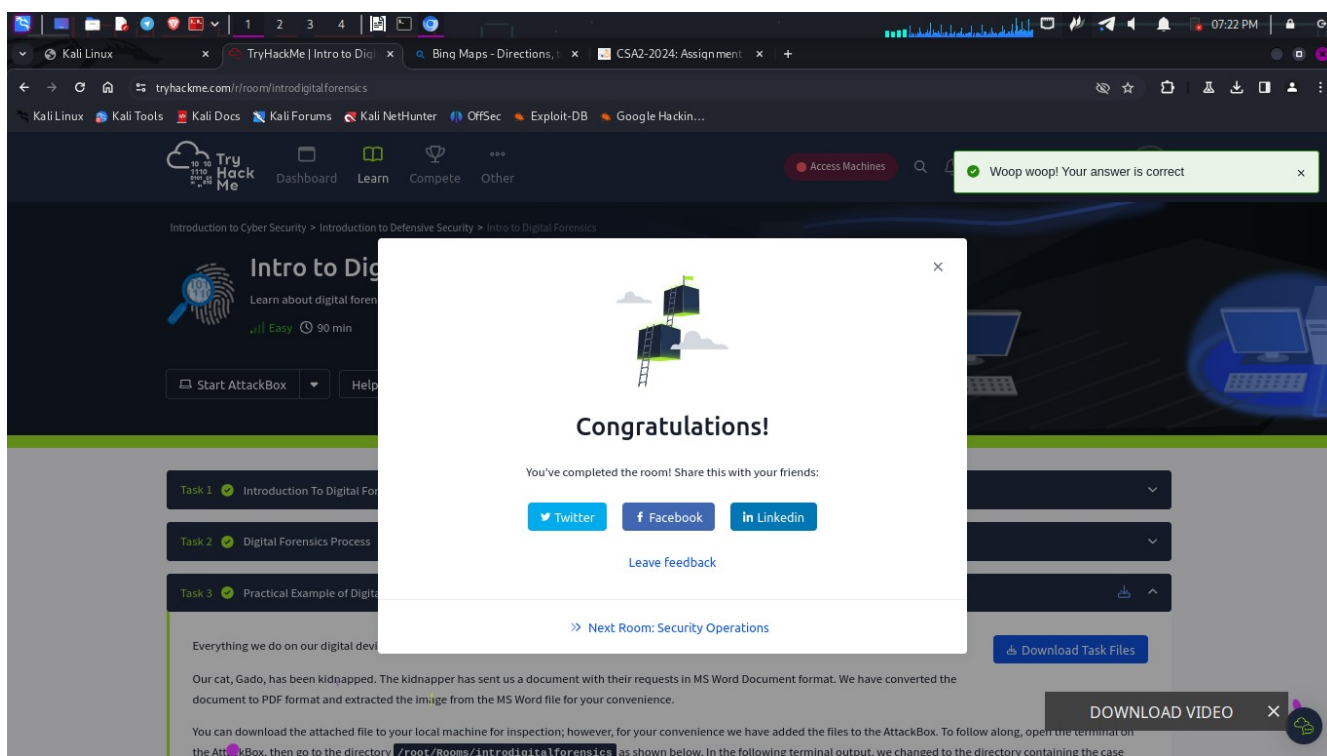
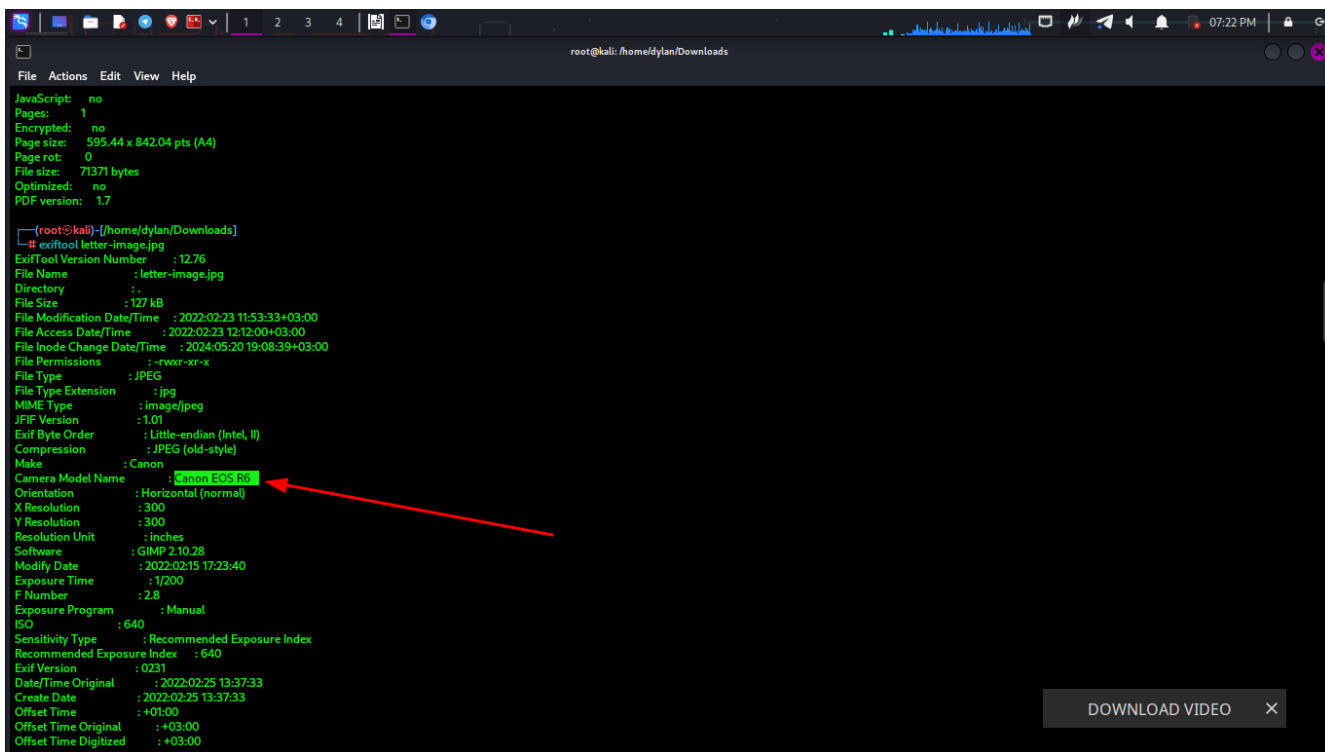
2.

What is the model name of the camera used to take this photo?

Canon EOS R6

✓ Correct Answer

🔑 Hint



## **Conclusion**

- In this modules I learn the basic that I need to start my cyber security journey. I have learnt the different cyber security careers. I now know the steps one takes to conduct digital forensics and some of the tools used.