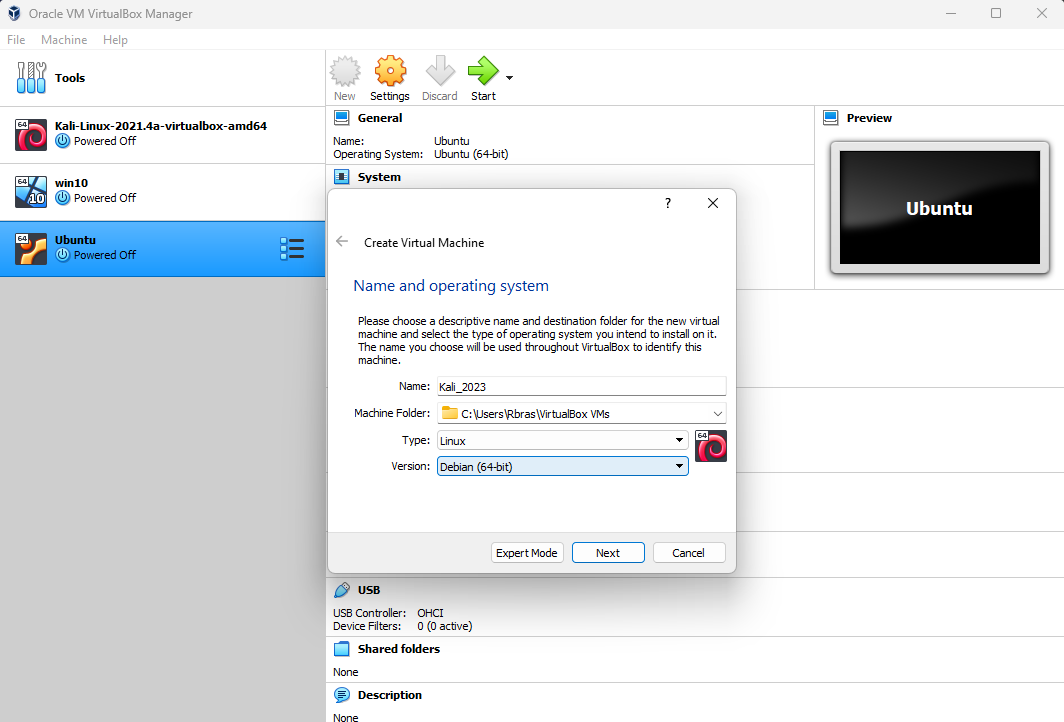
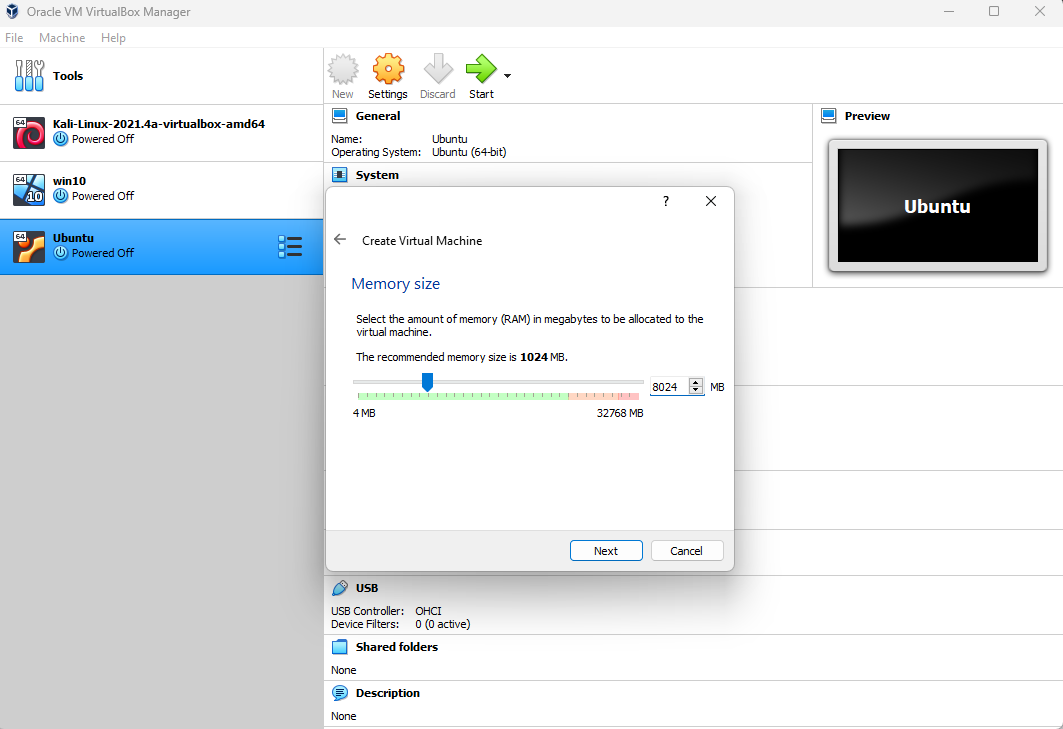
Rodrigo Brasil 18/09

### **Part 1: Deploy Kali Linux**

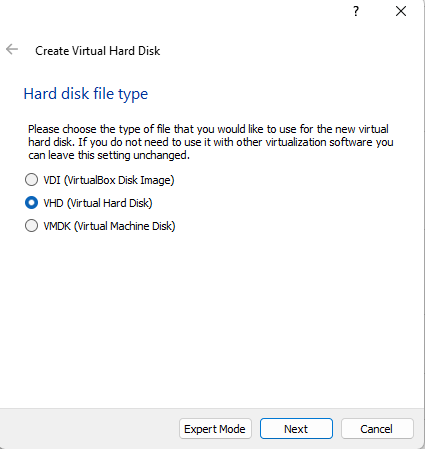
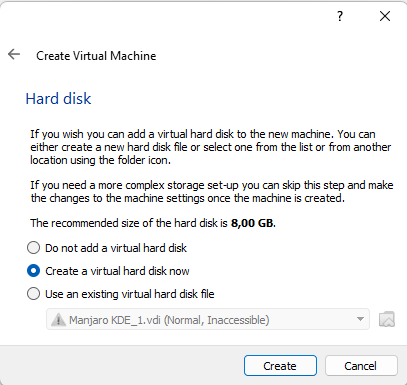
#### **Criação da máquina virtual para instalação do Kali linux**

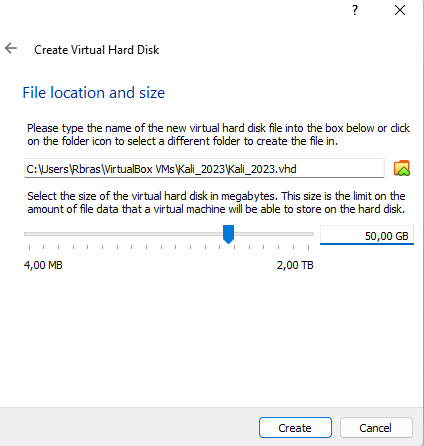


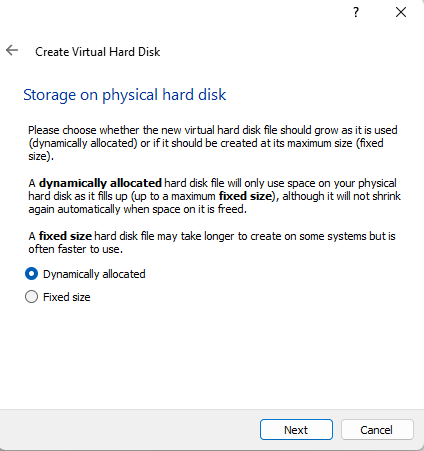
##### Nome e seleção do sistema operativo



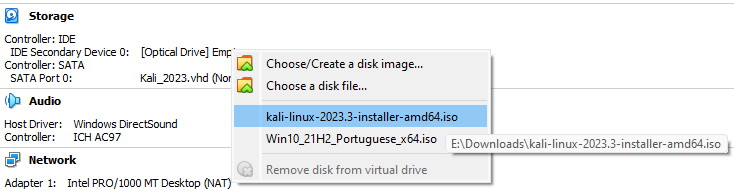
##### Escolha do tamanho da memória RAM da máquina



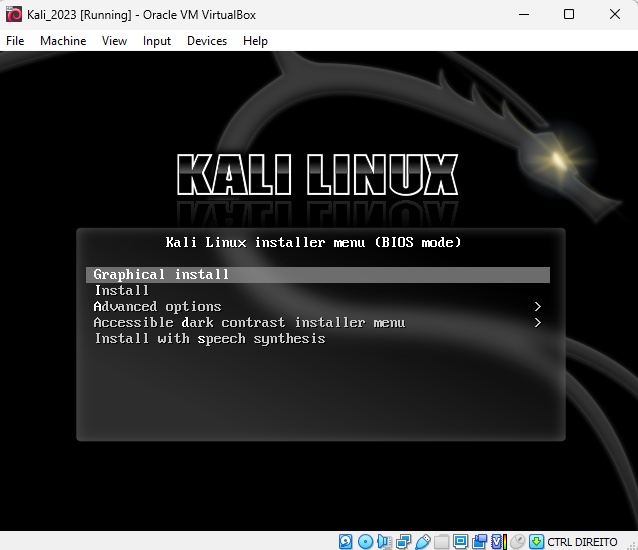




##### Criação do disco virtual



Seleção do ficheiro .iso para a instalação do kali linux no vm



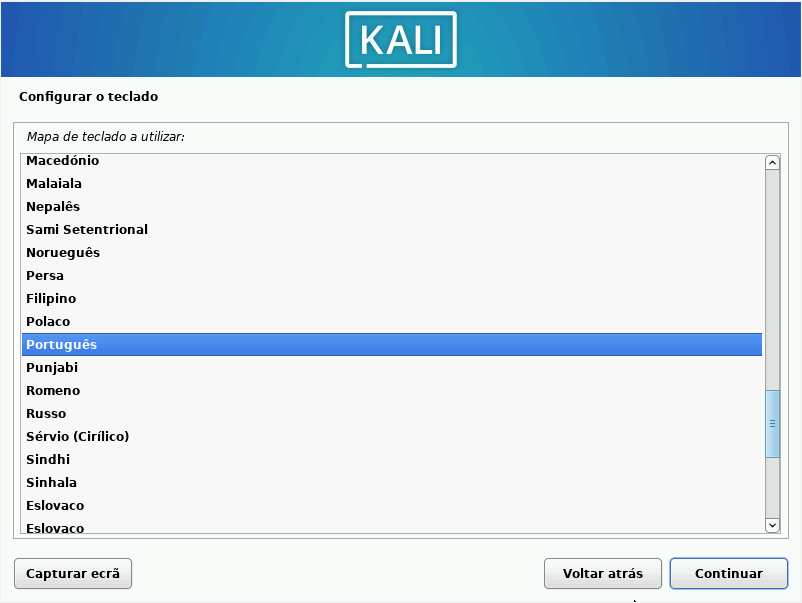
Seleção do método de instalação



Seleção da linguagem do sistema operativo



Localização



Língua do teclado



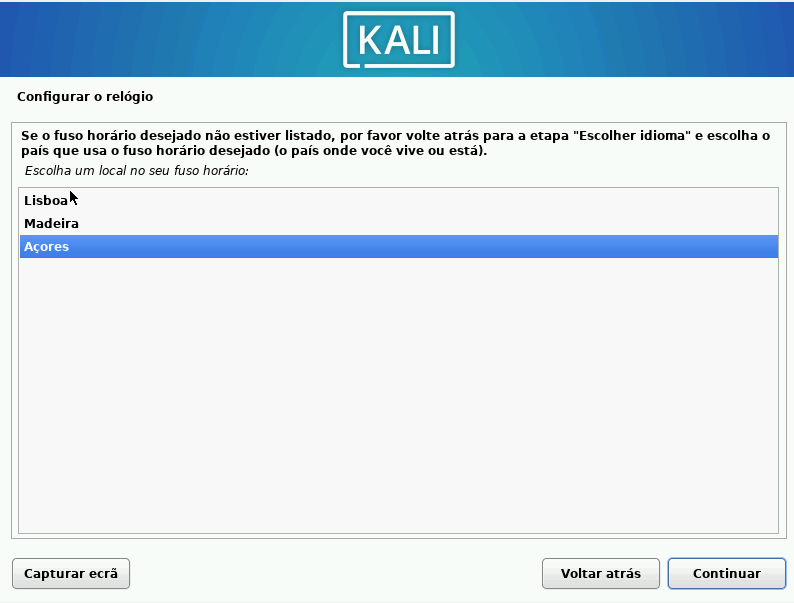
Nome do computador



Criação do utilizador



Criação da palavra pass do utilizador



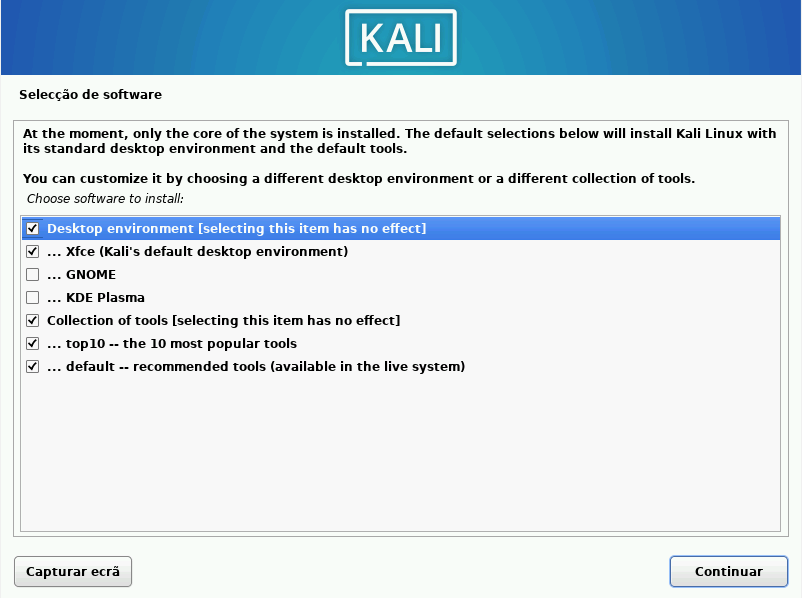
Seleção do fuso horário



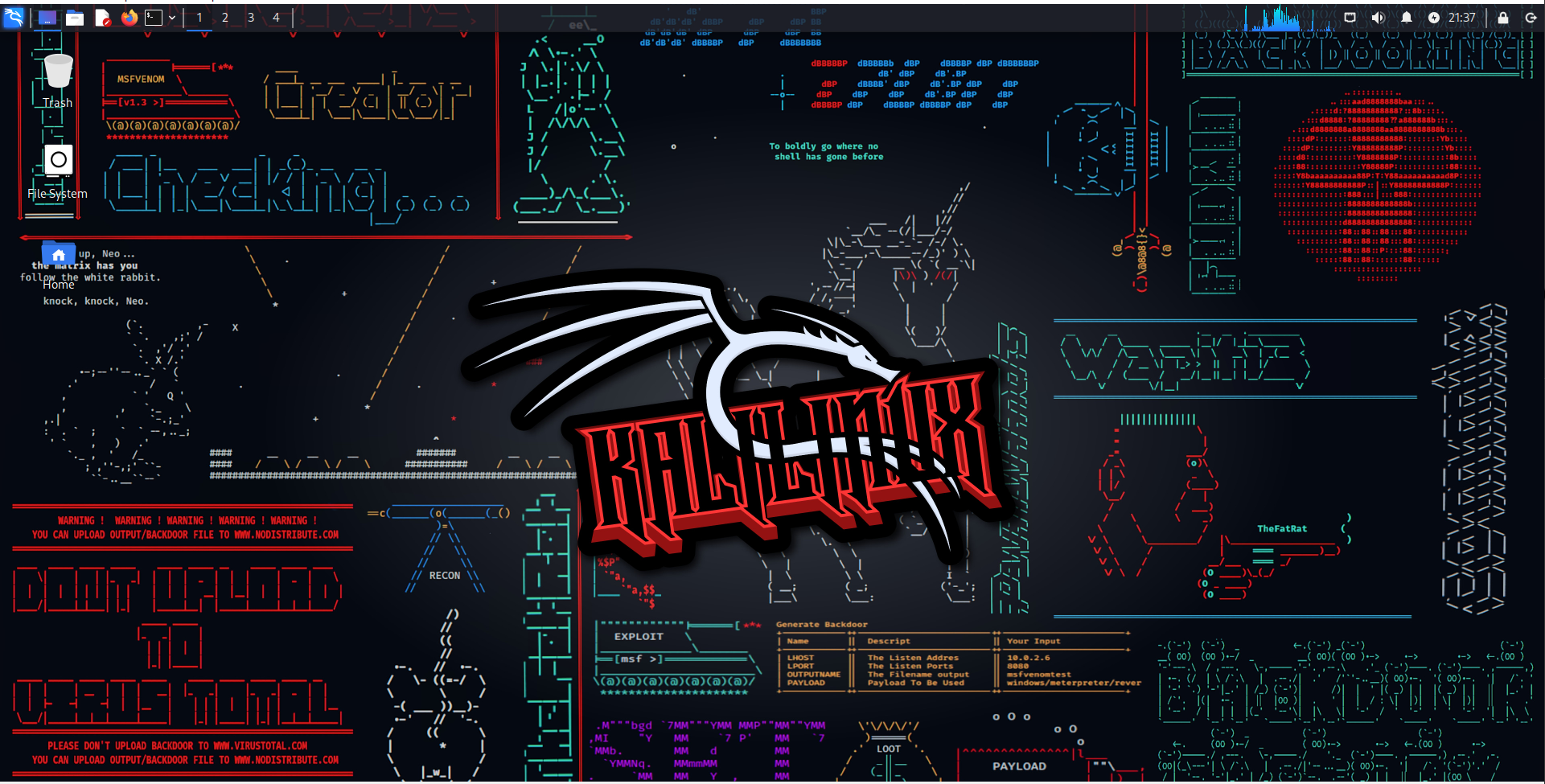




Criação e configuração das partições do disco



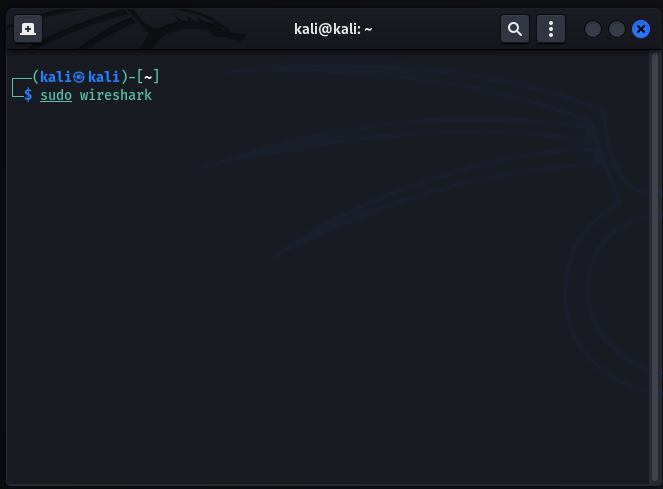
Selecionar o desktop environment e software recomendado



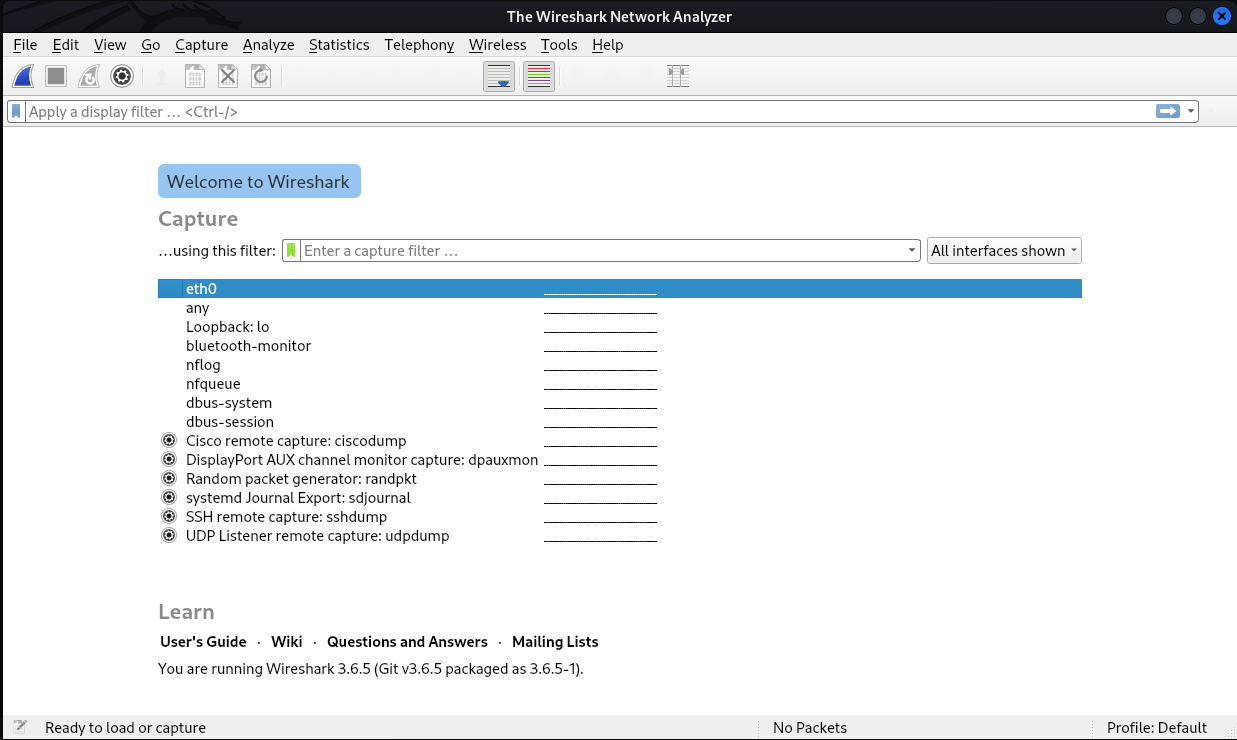
E está instalado!

### **Part 2: Traffic Capture**

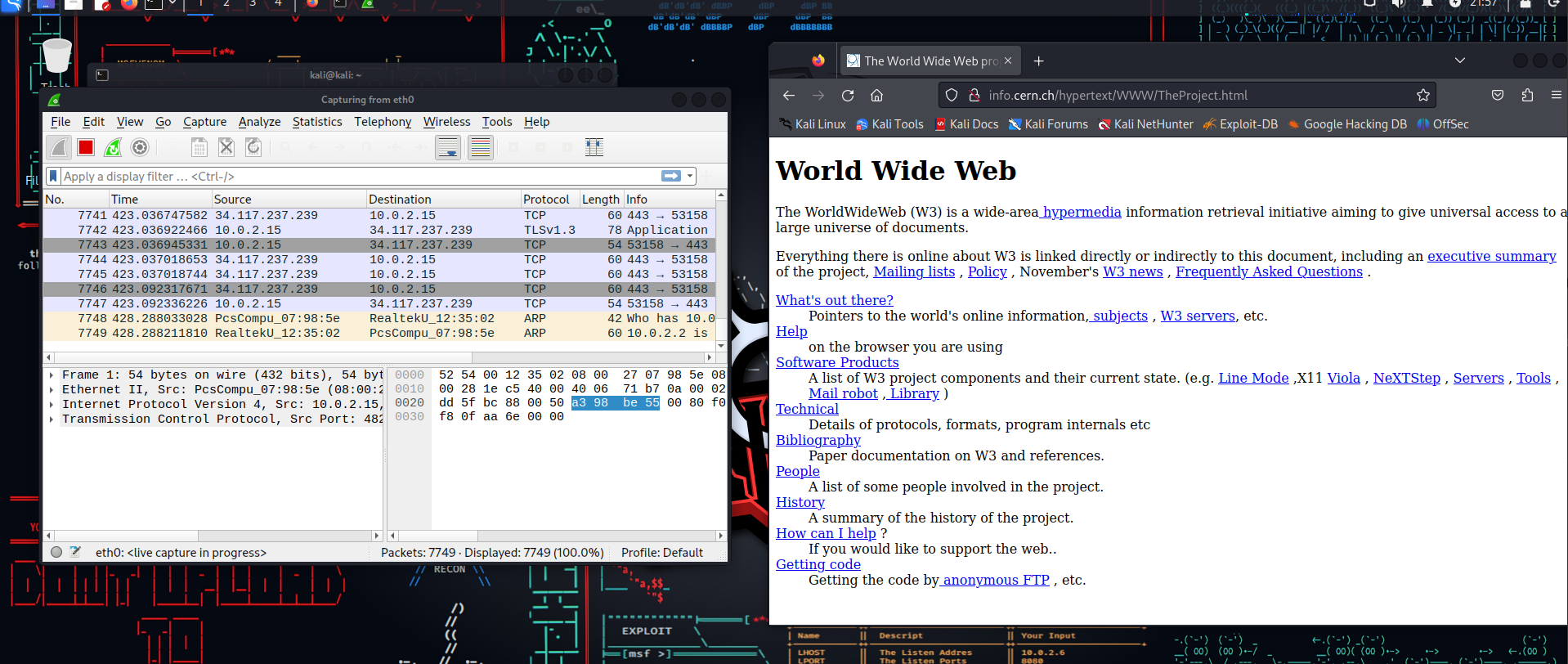
Captura de packets com wireshark



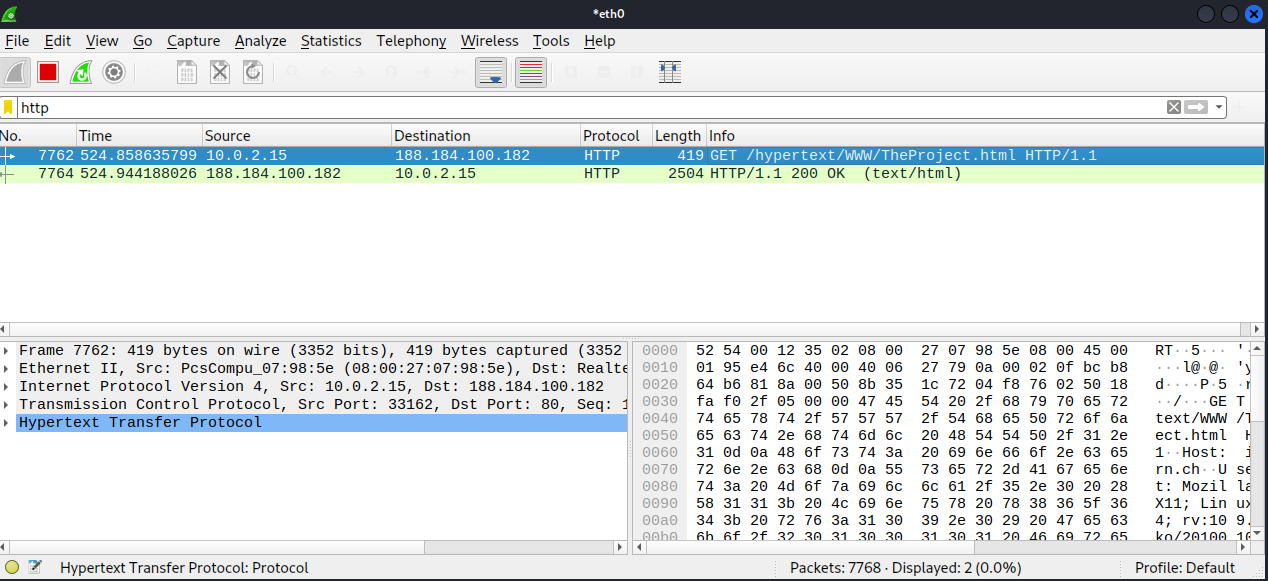
Iniciar o wireshark com privilégios root



Selecionar o adaptador de rede eth0



Capturar packets



Packets filtrados por http

* What is the difference between the various colors of packets that you see?

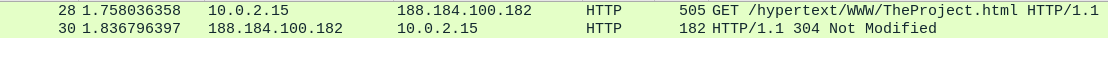
A diferença que identifiquei entre as várias cores mostradas foi o protocolo, o protocolo DNS é azul enquanto o TCP é verde.

### **Part 3: TCP Analysis**

* How many segments are used here?
  + 11
* What is the length in bytes of each segment? (Remember: The segment length is the size of the data contained in the packet)
  + 1 - 40 bytes
  + 2 - 24 bytes
  + 3 - 20 bytes
  + 4 - 20 bytes
  + 5 - 20 bytes
  + 6 - 20 bytes
  + 7 - 20 bytes
  + 8 - 20 bytes
  + 9 - 20 bytes
  + 10 - 20 bytes
  + 11 - 20 bytes
* Can you identify all three packets involved in the TCP three-way handshake? Include a screencap of them.
* How much data is typically acknowledged per ACK?

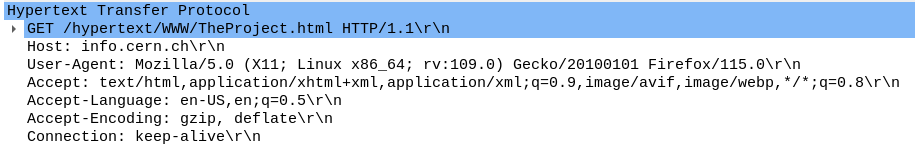
### **Part 4: HTTP Analysis**

* Filter traffic to HTTP from source Kali Linux to destination CERN. Include a screenshot of the filtered view.



* Locate the GET method that precedes a series of HTTP headers.





### 

### 

### 

### **Part 5: Wrap Up**

When you are finished, save a PCAP file of the network traffic capture for future reference.

Search your favorite job site, such as [Indeed](https://www.indeed.com/), for the keyword “wireshark.”

* What did you find?

I found that wireshark is a tool used widely in many different areas.

* Why is network traffic analysis a relevant skill to have?

Network traffic analysis is relevant because it helps organizations maintain the security, reliability, and efficiency of their networks.

* Do you see yourself working in this type of job in the future?

No.