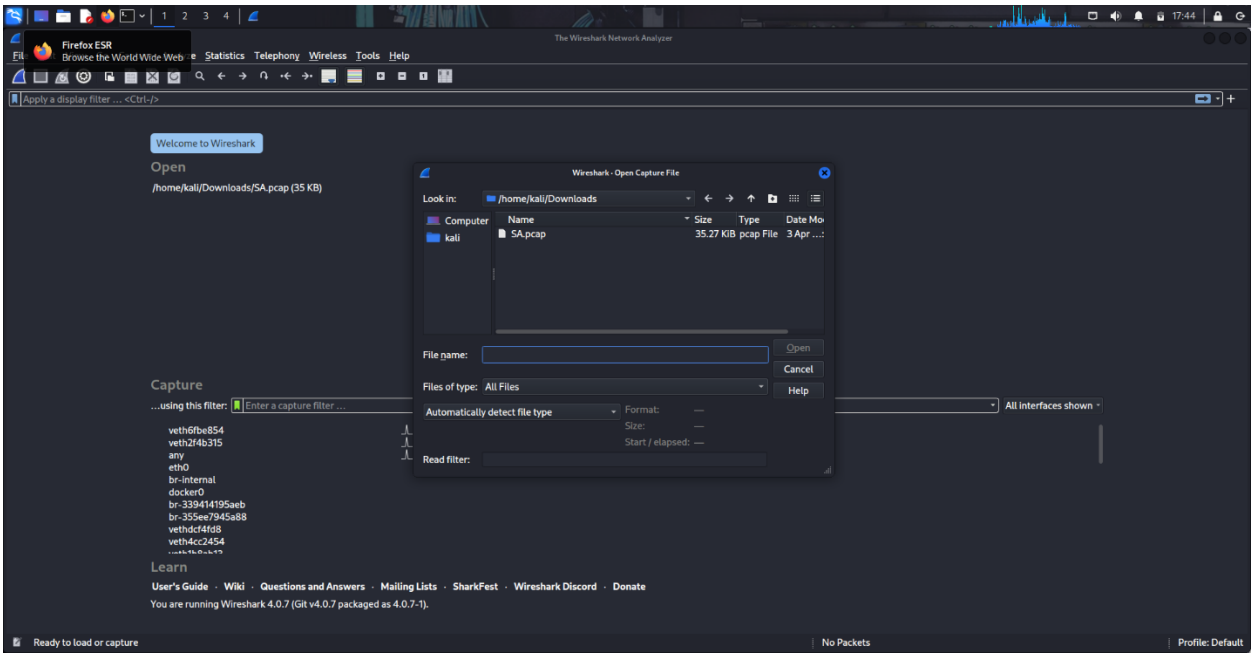
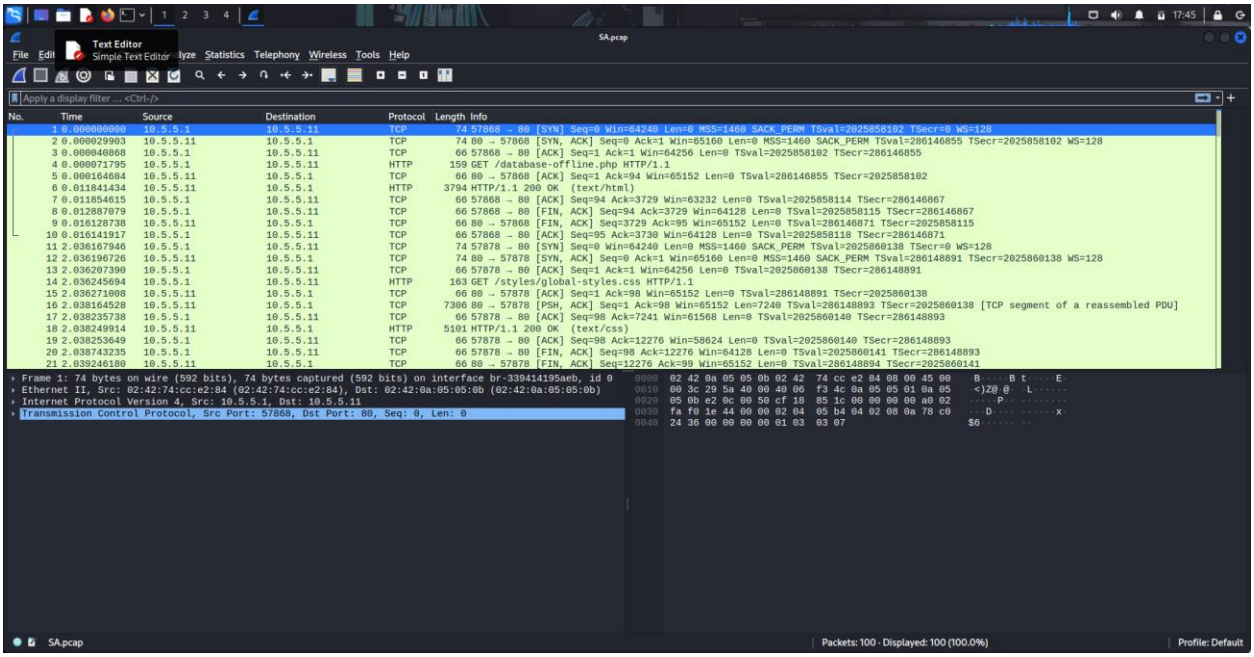
Challenge 4: Analyze a PCAP File to Find Information.

As part of your reconnaissance effort, your team captured traffic using Wireshark. The capture file, **SA.pcap**, is located in the **Downloads** subdirectory within the **kali** user home directory.

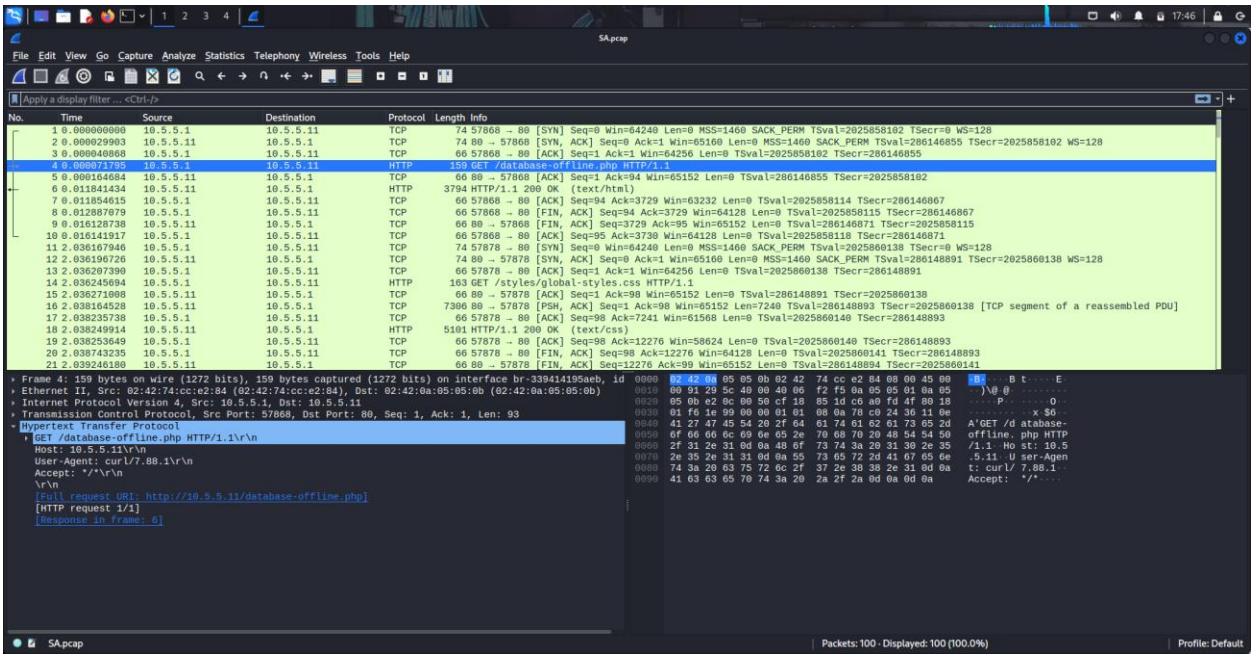
Step 1: Find and analyze the SA.pcap file.



Analyze the content of the PCAP file to determine the IP address of the target computer and the URL location of the file with the Challenge 4 code.

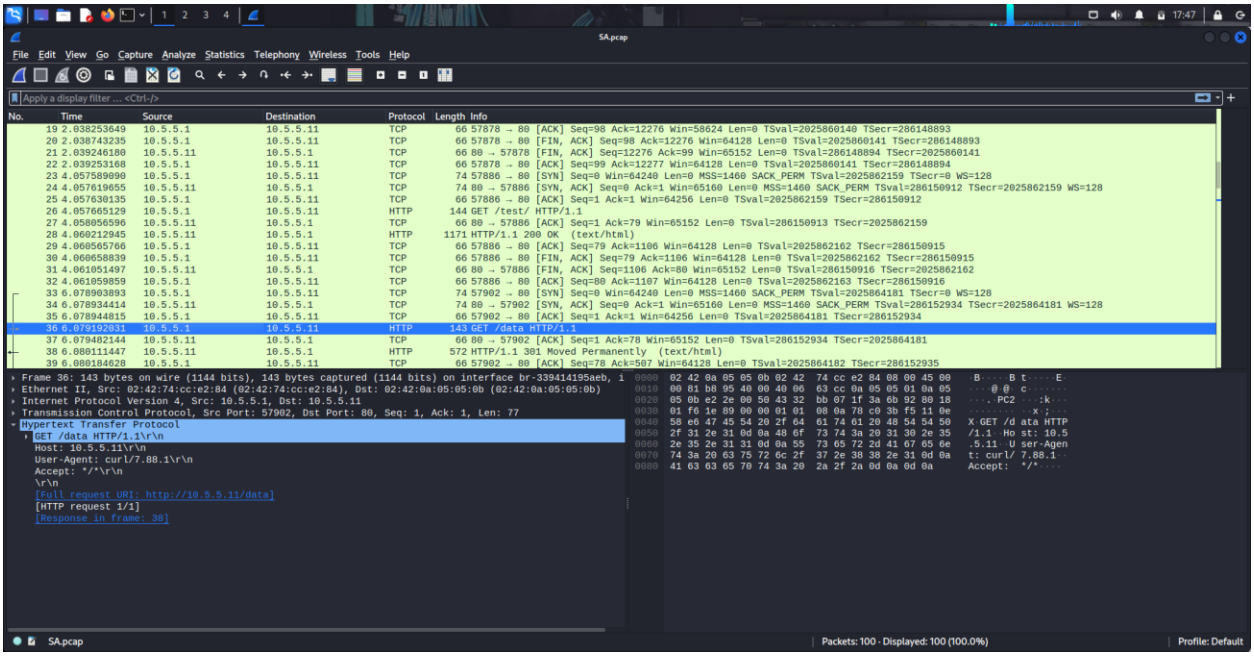


What is the IP address of the target computer? **10.5.5.11**



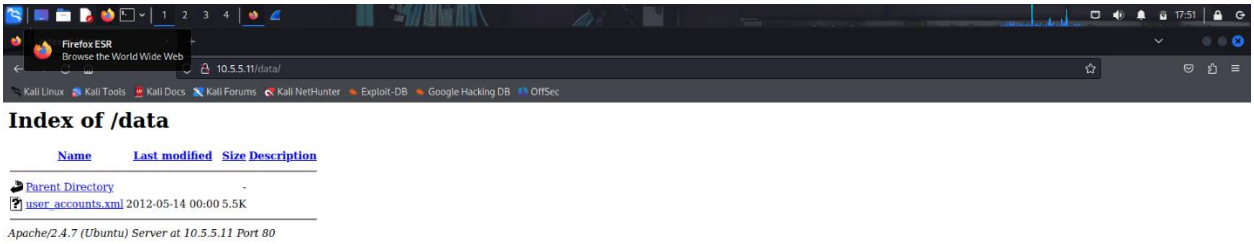
What directories on the target are revealed in the PCAP?

In the http packets, the paths 10.5.5.11/database-offline.php/, 10.5.5.11/data/, and 10.5.5.11/test/ were discovered.



Step 2: Use a web browser to display the contents of the directories on the target computer.

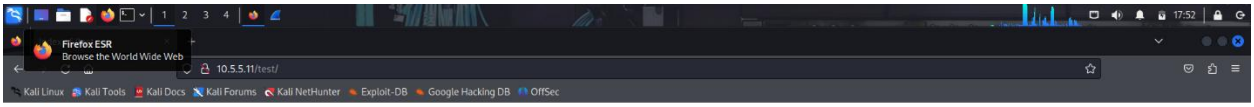
Use a web browser to investigate the URLs listed in the Wireshark output. Find the file with the code for Challenge 4.



Index of /data

Name	Last modified	Size	Description
Parent Directory		-	
user_accounts.xml	2012-05-14 00:00	5.5K	

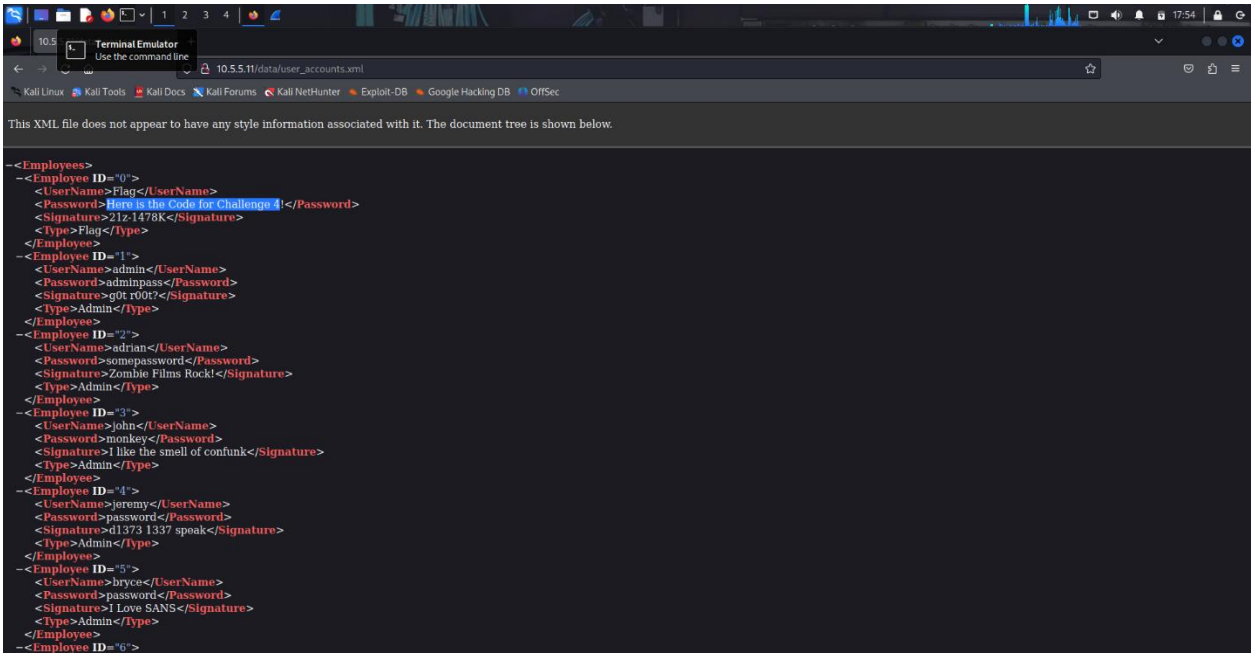
Apache/2.4.7 (Ubuntu) Server at 10.5.5.11 Port 80



Index of /test

Name	Last modified	Size	Description
Parent Directory		-	
testoutput/	2018-05-14 21:24	-	

Apache/2.4.7 (Ubuntu) Server at 10.5.5.11 Port 80



What is the URL of the file? http://10.5.5.11/data/user_accounts.xml

What is the content of the file? username, password and signatures

What is the code for Challenge 4? 21z-1478K

Step 3: Research and propose remediation that would prevent file content from being transmitted in clear text.

What are two remediation methods that can prevent unauthorized persons from viewing the content of the files?

Two effective remediation methods to prevent unauthorized persons from viewing the content of files are:

1. **Data Encryption (At-Rest and In-Transit):** Encrypting data converts it into unreadable code that cannot be viewed or interpreted without the proper decryption key, making the content useless even if accessed.
2. **Access Control and Permissions (e.g., ACLs or RBAC):** Implementing strict Access Control Lists (ACLs) or Role-Based Access Control (RBAC) at the operating system level restricts file access to authorized users only, denying unauthorized users the ability to read or edit the files.