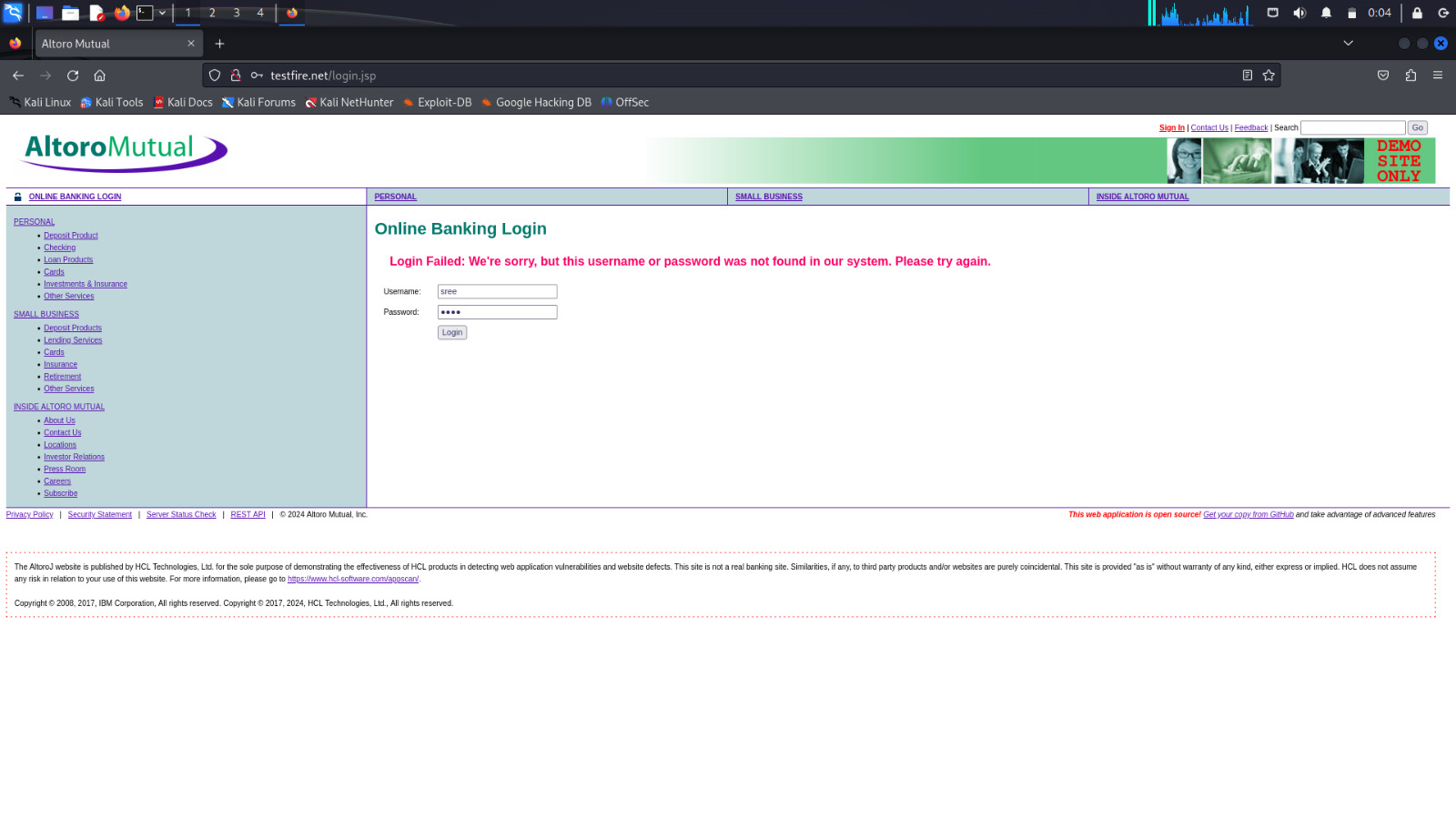
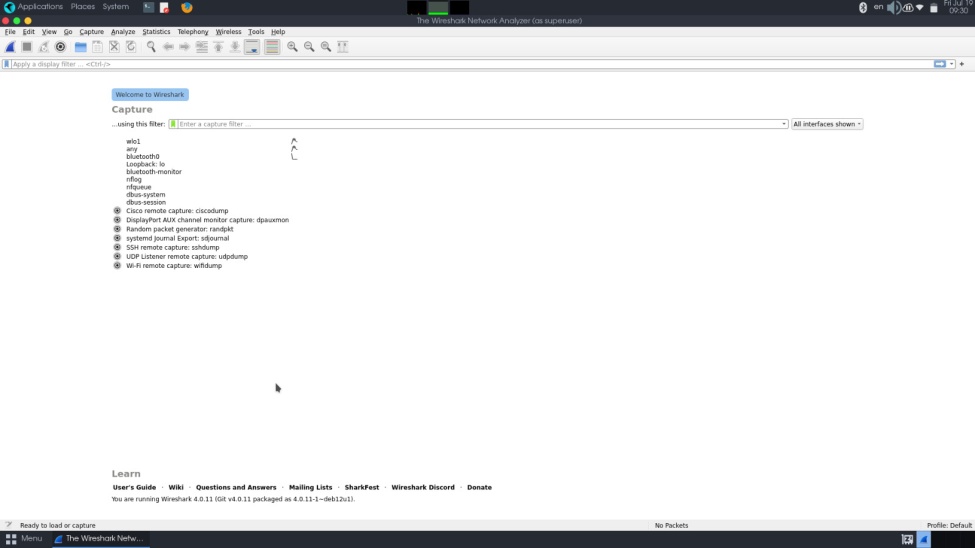
**ASSESSMENT 01**

**Task-1 WIRESHARK**

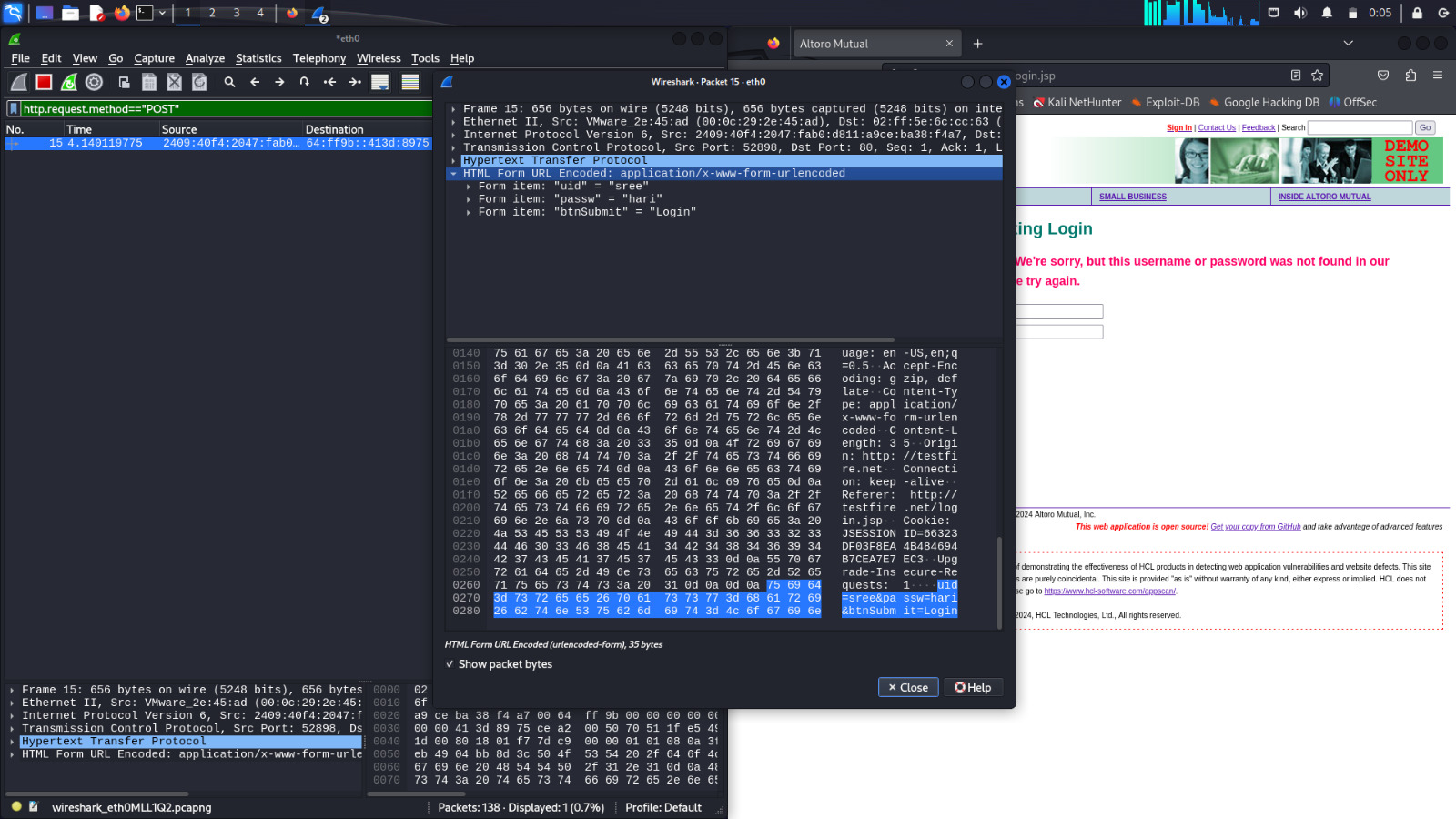
1. First open firefox browser in system (linux or windows)
2. search testfire.net and move to sign.in page.( At the top right there is a sign in option)



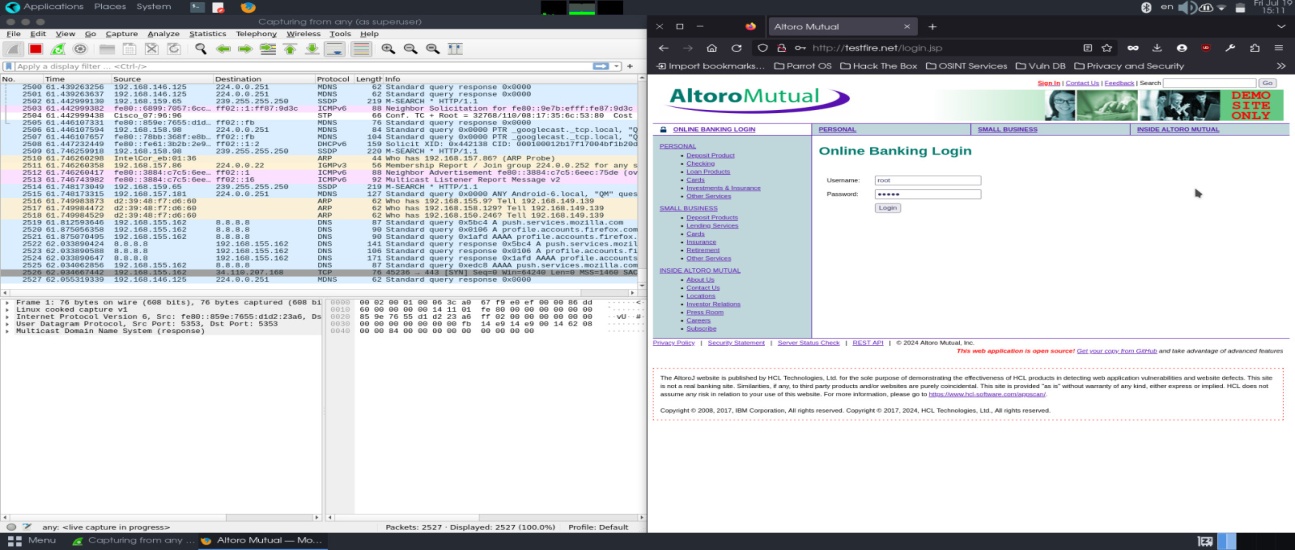
1. Now, open wireshark in your system.

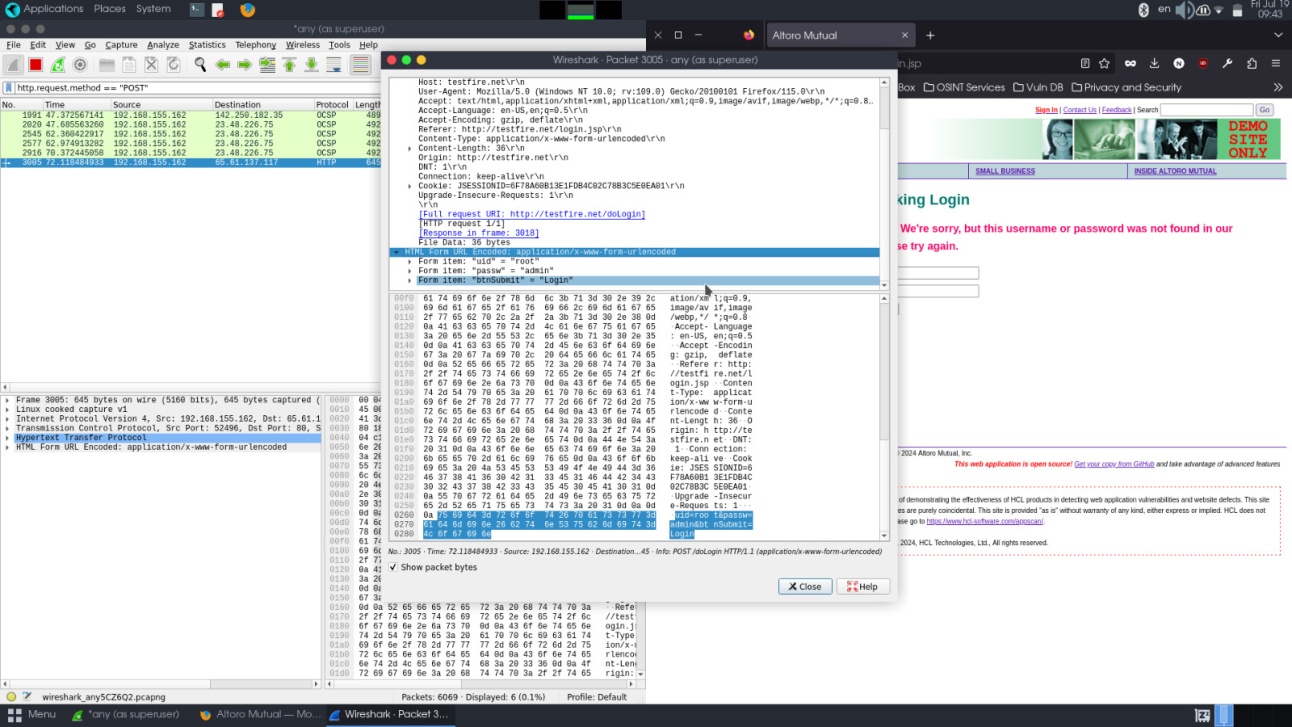


1. In wireshark, click on eth() on that goes to that official terminal of the wireshark.
2. This shows that the scanning process in the wireshark.
3. Now go to the sign in page , enter the username, password and sign in to the website
4. The image below shows the result, after clicking “login” , Navigate to wireshark tool and enter the command in search bar. http.request.method=="POST"



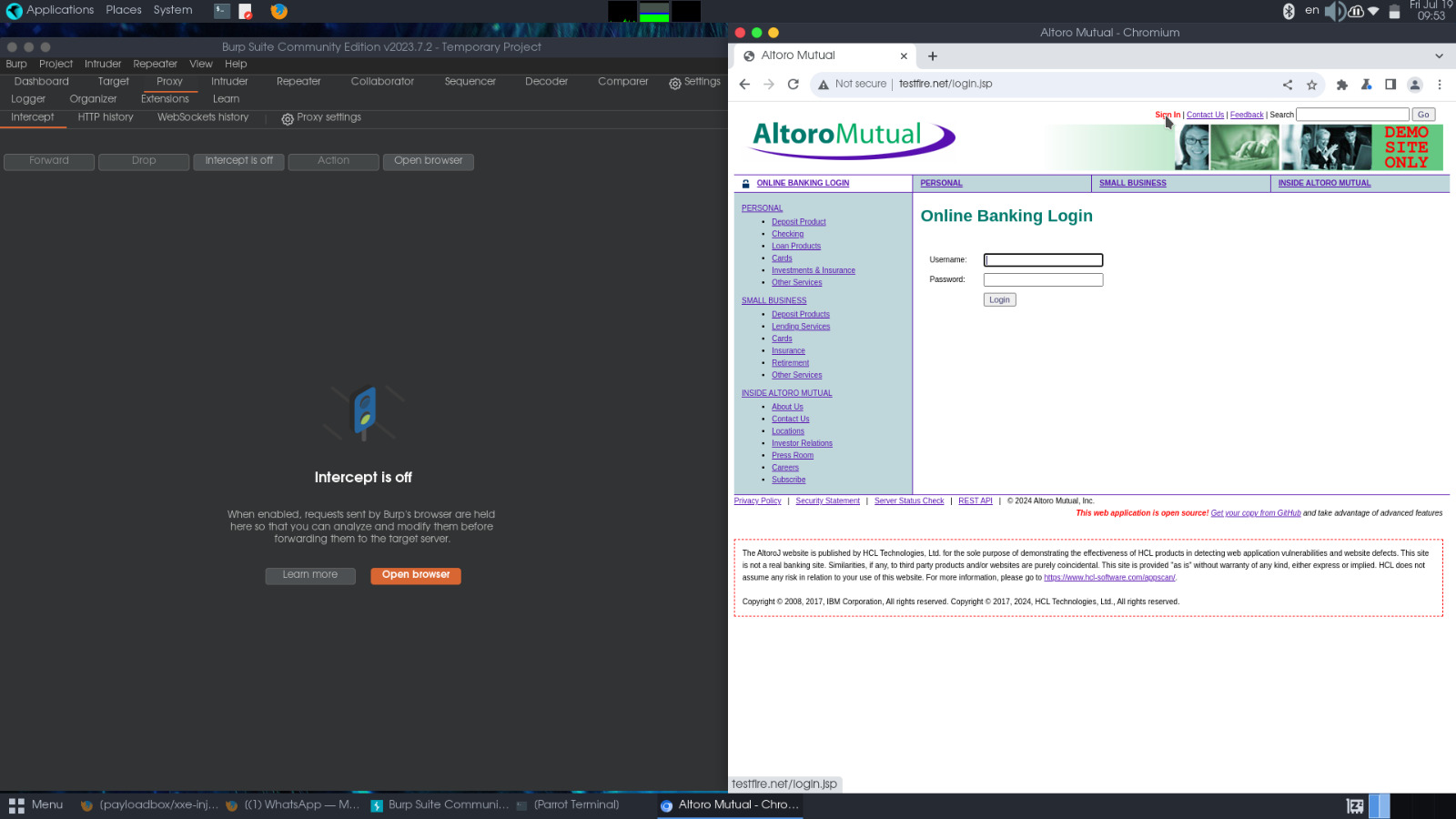
1. Now search for the HTTP requests and click on it to get the result as shown below. This parameter has captured the username and password given by the user.



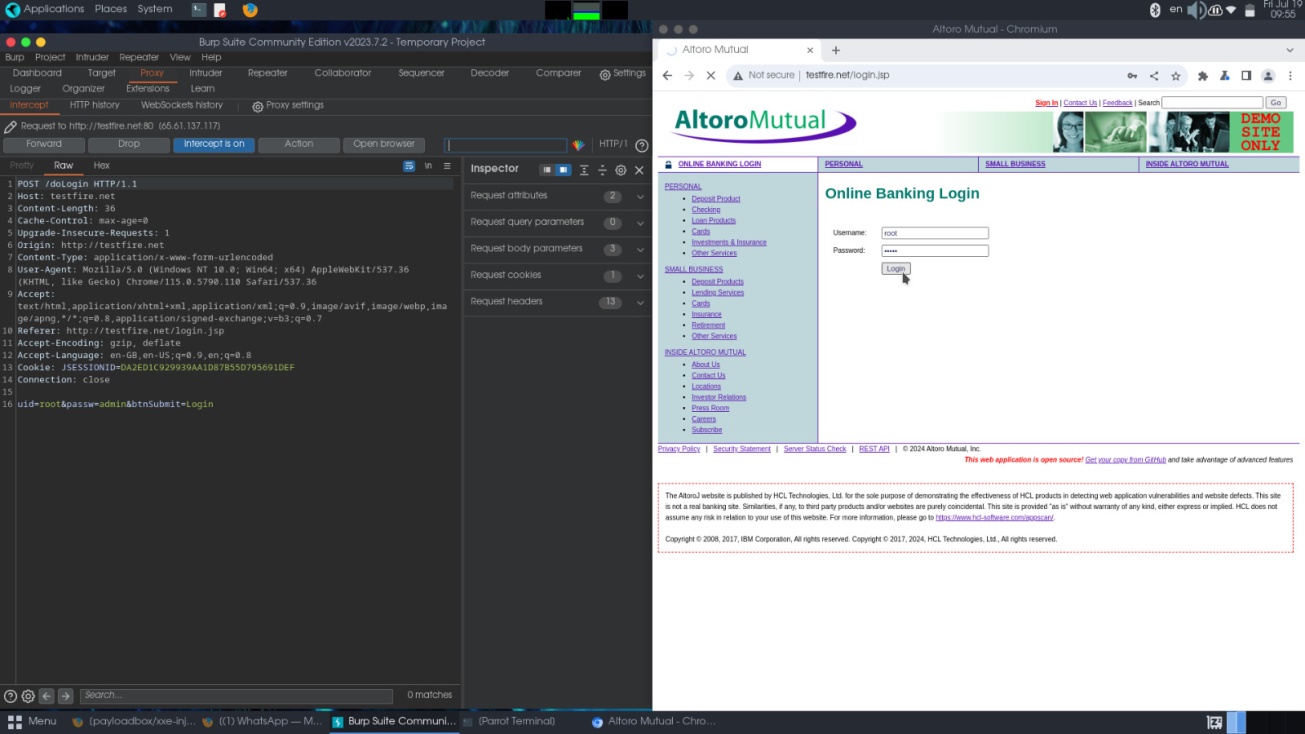


**Task – 2 BURPSUITE**

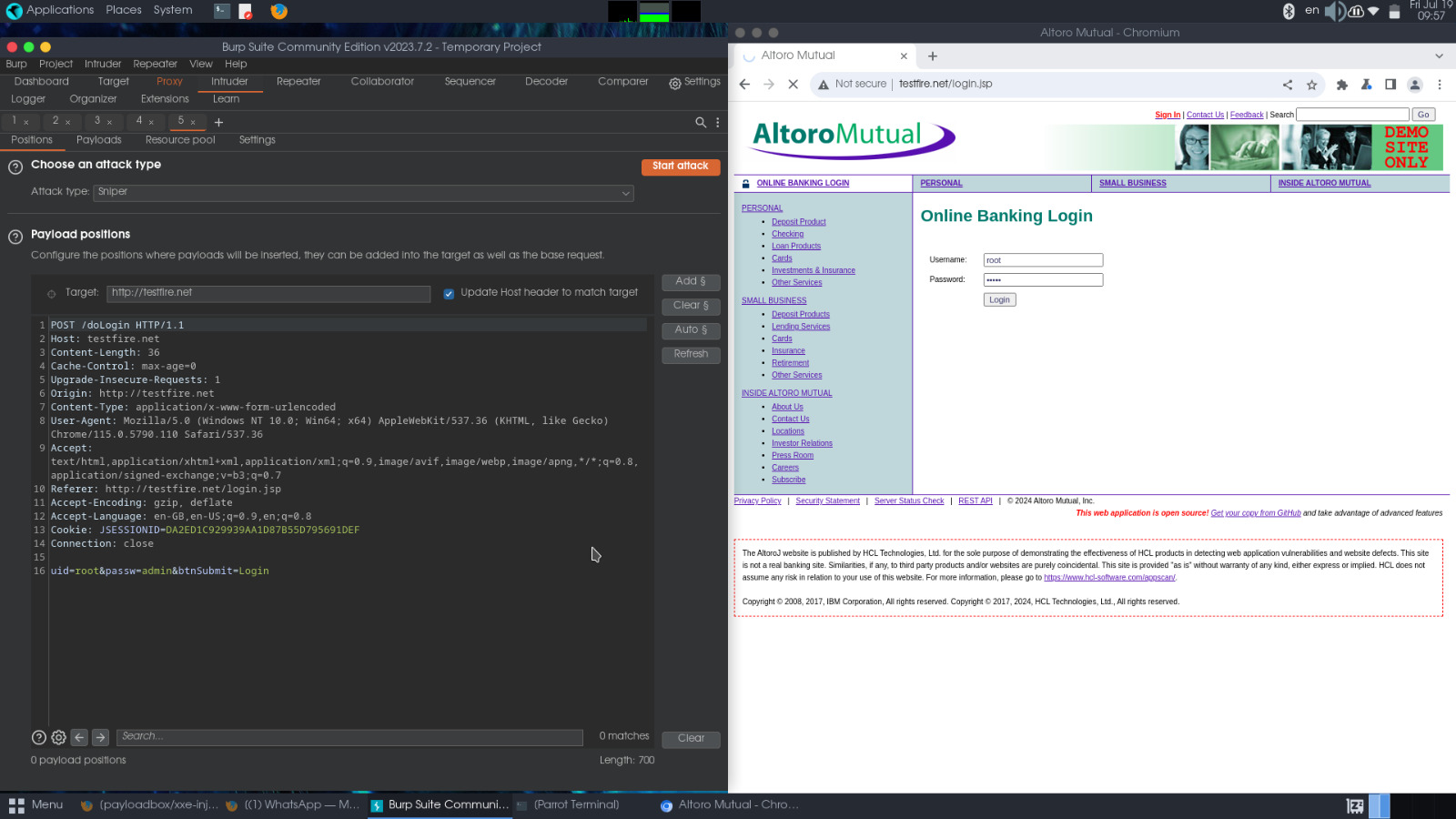
1. Open the Burpsuite in your linux, move to proxy tab and off the intercepter



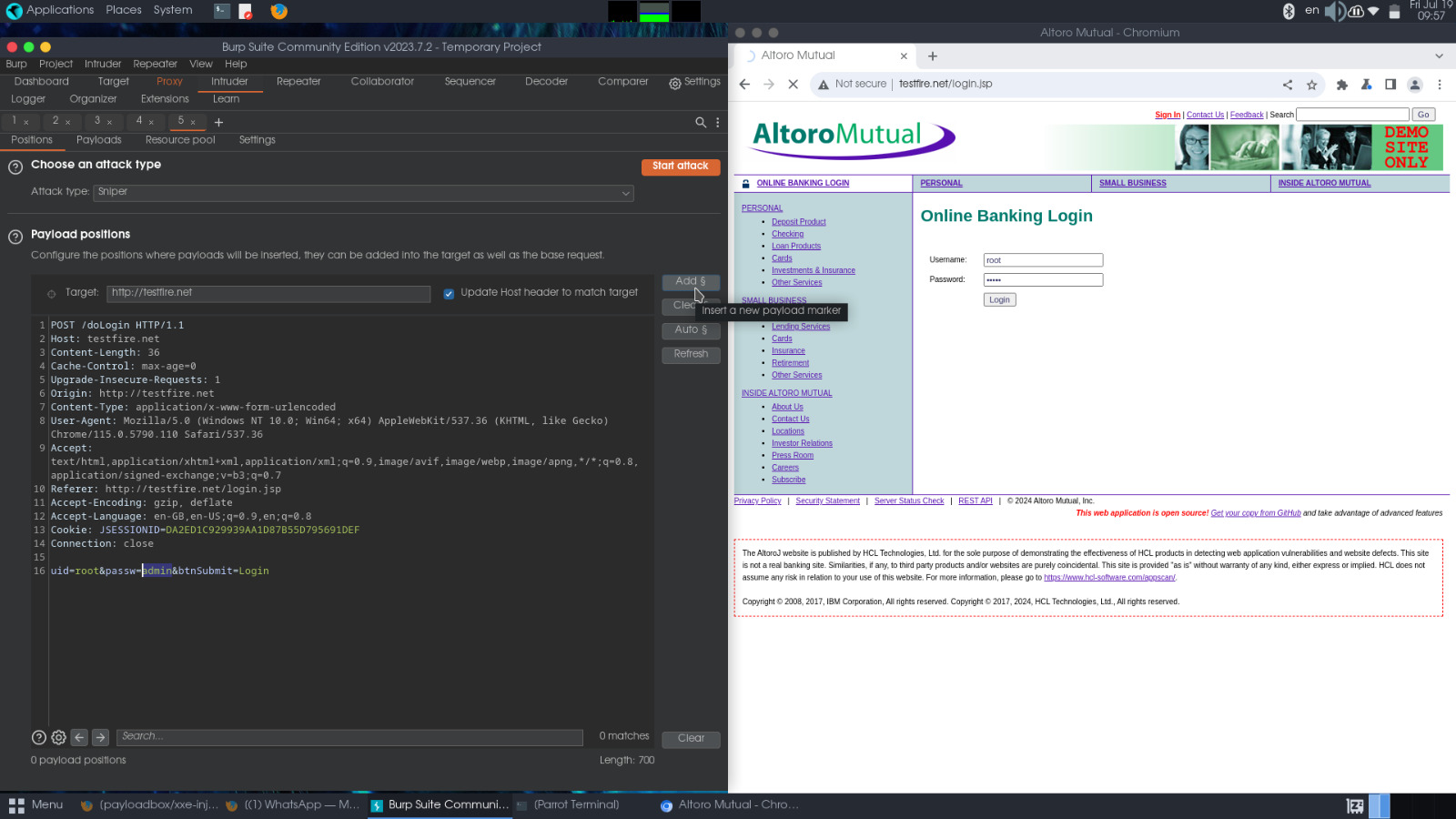
1. Also open the browser and search testfire.net. There is a sign in tab enter the username and password, go to the burpsuite and turn on the intercept, then click login.



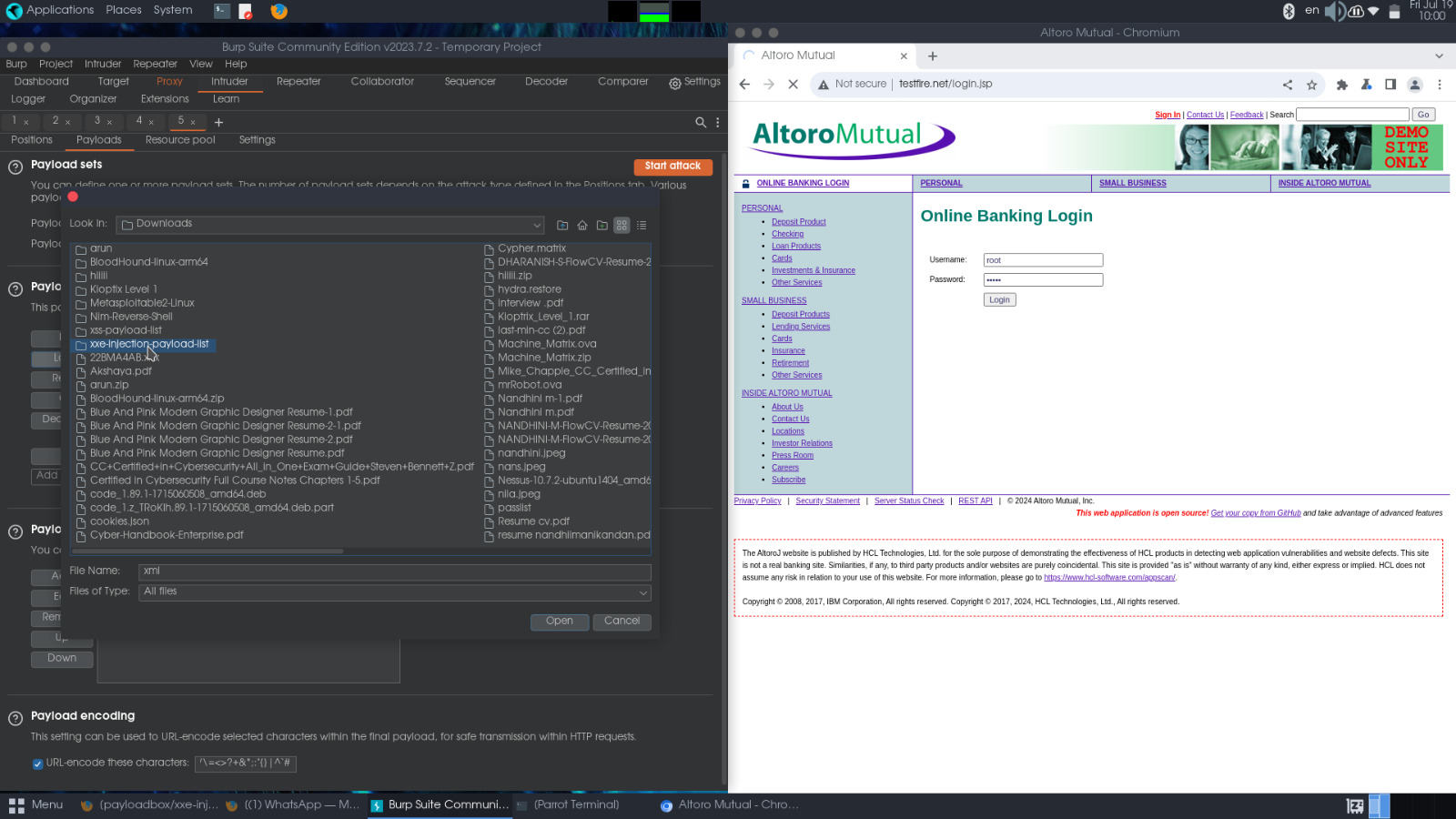
1. In burpsuite, the proxy has captured the login details. Now right click on the screen and select “ send to the intruder” .



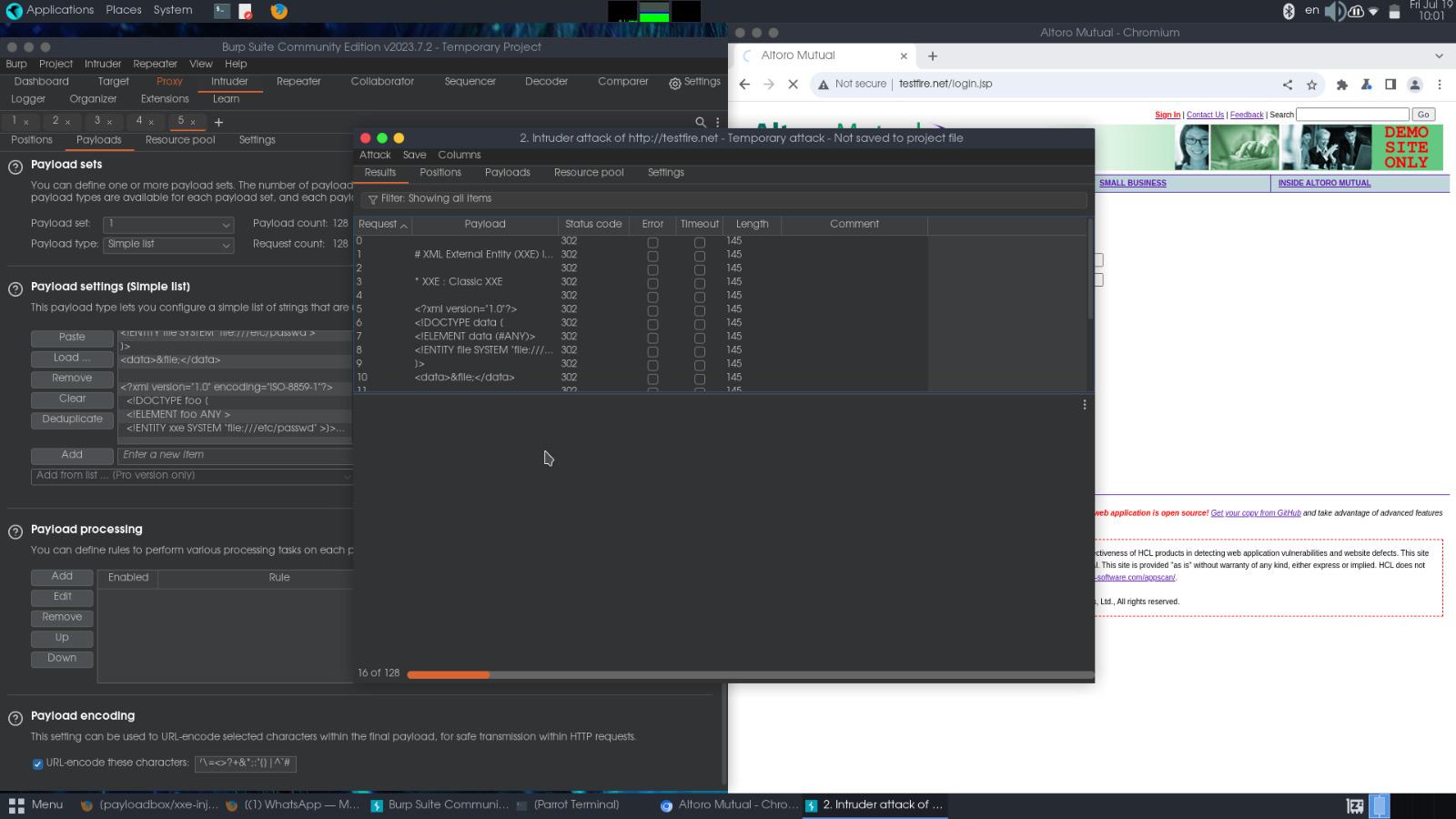
1. Now highlight the password and click the add button.



1. Navigate to payload tab and upload the xml payload-list from the download folder . (You can get the payload list from github source).



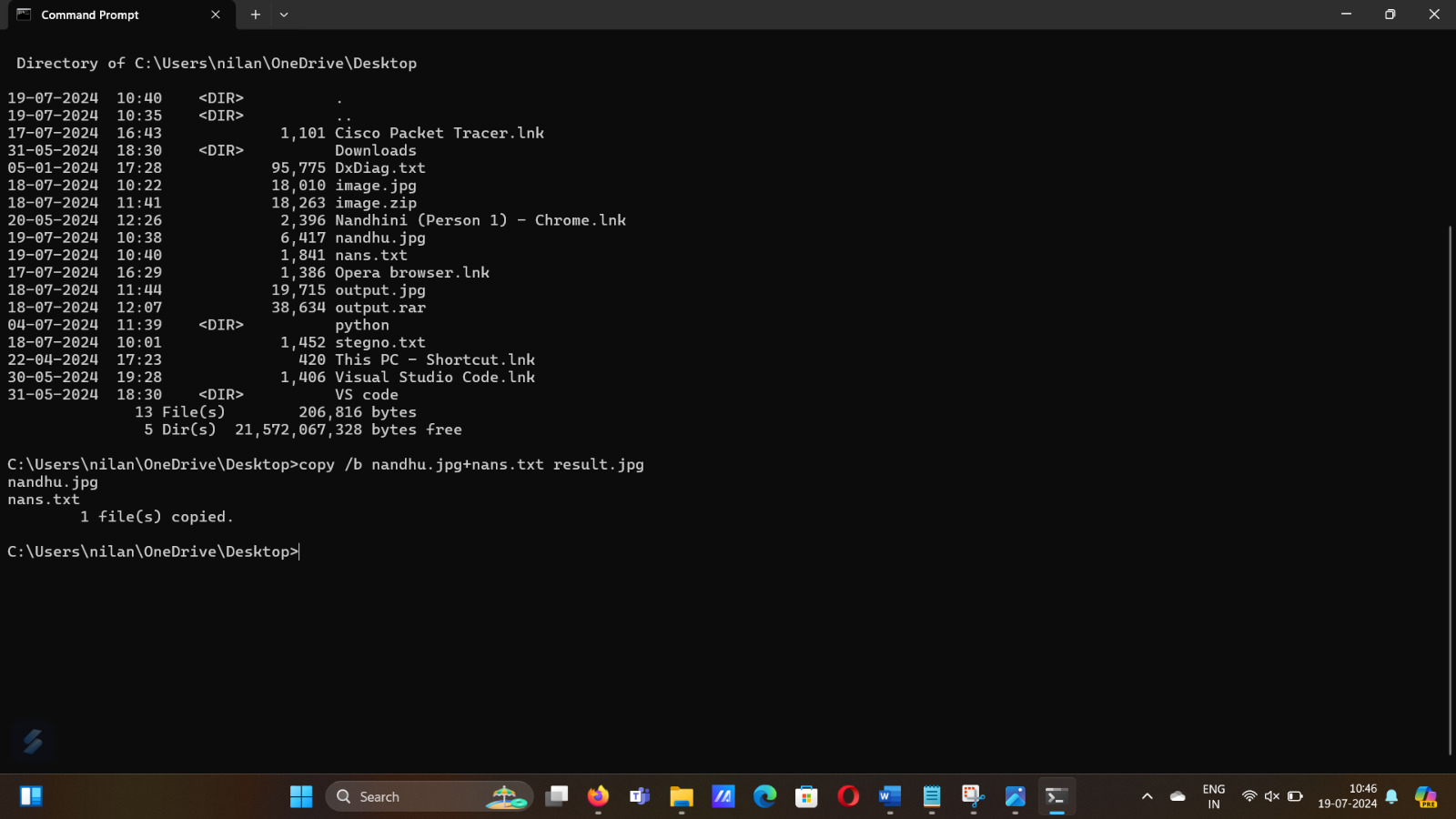
1. Click the 'start attack' button and watch scanning process. You can see the list of requests passing with length and status code. When the length value varies the password will change accordingly.

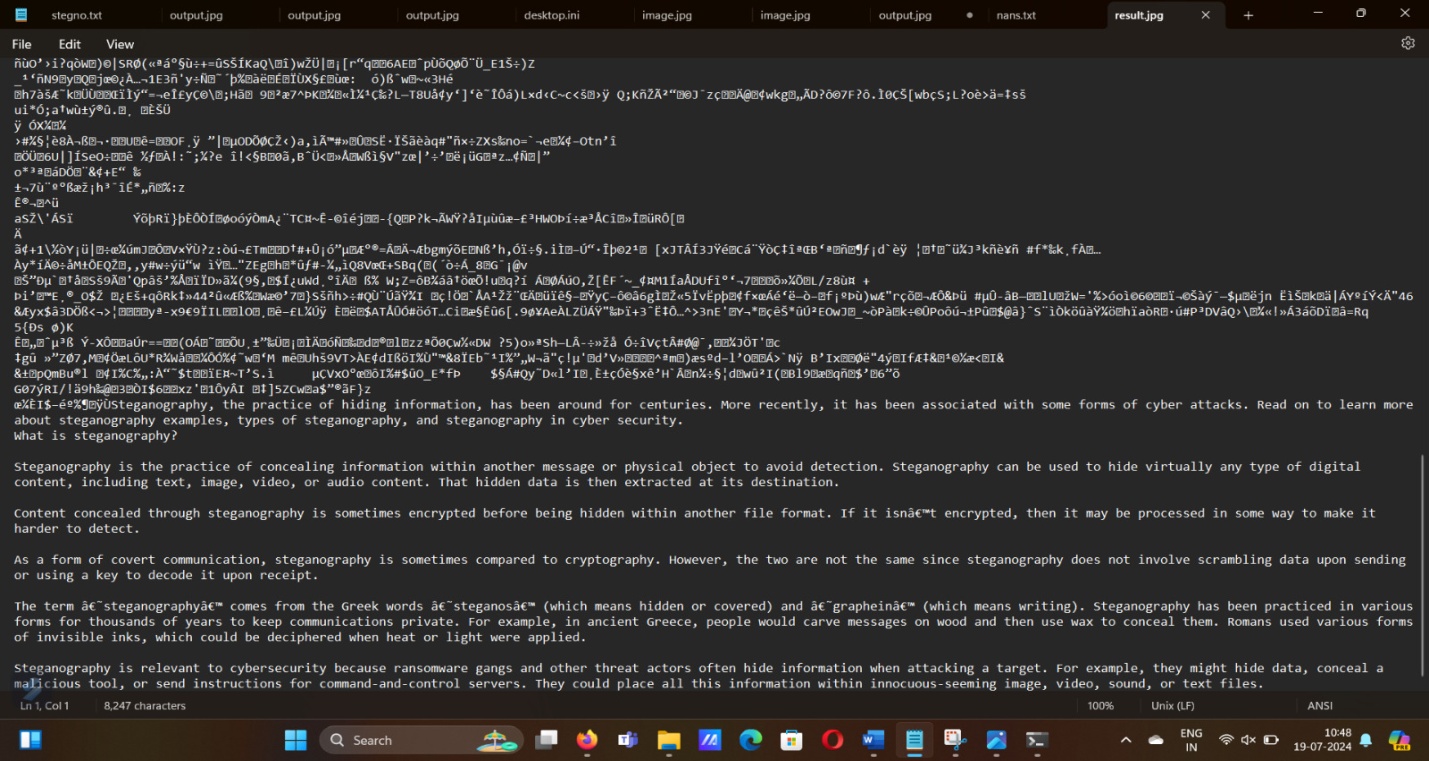


**Task – 3 STEGANOGRAPHY**

Steganography is **the technique of hiding data within an ordinary, nonsecret file or message to avoid detection; the hidden data is then extracted at its destination**. Steganography use can be combined with encryption as an extra step for hiding or protecting data

1. Open command prompt in your window. Move to desktop directory.
2. Before that create any text file and download any image to perform setganography.
3. Use the command: copy /b “image name”.”format”+”Textfile name.txt” “Ouput file name”.”Format”
4. Eg : copy /b image.jpg+file.txt output.jpg
5. After entering this command the text file is copied to the image, Now you can view the image by selecting “open with notepad” option. This shows you the hidden text content.





**Task - 4 NMAP SCANNING**

Nmap is **a network scanning tool—an open source Linux command-line tool—used for network exploration, host discovery, and security auditing**.

* **-A (Aggressive Scan):**

-A is like a super detailed scan that tries to learn everything possible about the target. It finds the operating system, software versions, runs scripts for more info, and traces the network path.

* **-O (OS Detection):**

-O is used to figure out what operating system the target is running. It's like asking, "What kind of computer are you?"

