1. ***D0t5 & D4sh35 :-***

* *First I recorded the morse code from the hardware device.*
* *Then I started learning and listening the various sentences of morse code from youtude and noted them.*
* *Then I started listening morse code which I recorded and wrote down the dots and dash in a letter wise and finally cracked it.*

*wired{IT\_IS\_WHAT\_IT\_IS}*

1. ***Crypto layers :-***

* *They have given a binary code in the challenge.*
* *I decoded that binaryto text using Google.*
* *Then I got to know about a new thing that is “cipher” and that is a cipher text.*
* *Then I identified which type of cipher it is and got that it is a “Caesar cipher”.*
* *According to the hints, I decrypted the cipher 5times and then I got the “Vignere cipher”.*
* *By decoding that vignere cipher, finally I got the flag.*

1. ***Achan’s favorite :-***

* *The challenge is to decode an audio file.*
* *I used sound analyzer online to decode it.*
* *I got a meme templet “Emotional Damage” with the man face who said that.*
* *Hence the flag is*

*wired{Stevens\_He}*

1. ***grep\_it :-***

* *An attachment was also given with it which contain a large symbolic code.*
* *According to description “grep” itself a Linux command which searches for a file for a particular pattern of characters, and displays all lines that contain that pattern.*
* *The pattern that is searched in the file is referred to as the regular expression.*
* *But as I don’t have linux I just got to know that we can use “findstr” command for windows but I just used ctrl+f and searched for wired thing and got the flag.*

1. ***da\_french\_cipher :-***

* *I searched the challenge name in Google and I got that it is a “vignere cipher”.*
* *As per the description given, I copied the given cipher text and decrypted by giving “aeiou”(vowels) as the key.*
* *Then I got the flag which is wired{w3lc0m3\_t0\_th3\_w0rld\_0f\_c1ph3rs}*

1. ***MICH43L5\_P4R4DIS3 :-***

* *I downloaded the given attachment and got .png file which has a photo of a bridge.*
* *I just scanned that photo in my mobile and searched for the name of that bridge and I cracked it.*

*wired{Vespucci\_Boulevard\_Bridge}*

1. ***da\_0n3\_wh3r3\_u\_v1su4l1s3 :-***

* *You have given a text file in the attachment.*
* *I changed the extension of the file to .png and got a image of the flag.*

1. ***simple\_web :--***

* *I clicked on start instance and then it took me to a login page asking username and password.*
* *Then I open the source code of that page.*
* *And that script is “obfuscated” it seems which means difficult to understand.*
* *I deobfuscated it and got the username and password.*
* *I just gave that info in the login page and got the flag.*

1. ***sh0d4n :-***

* *I opened “shodan” website in Google.*
* *Then I searched gas tanks in the search box.*
* *I looked for the various gas tank IP addresses with the specifications given in the description.*
* *Then I gave that IP addresses in the way you mentioned in the description.*

1. ***w!r3d\_sh4rk :-***

* *Downloaded wireshark.*
* *Opened the given. File in wired shark, and the contents opened.*
* *Found the flag amoung the lines in wireshark.*

1. ***what’s\_up\_DoH :-***

* *Opened the file in wireshark*
* *While scanning along the lines, I tried to find out idk567 from the clue given.*
* *Then with the help of seniors, I sorted the lines into script,and then searched for it.*
* *Then I found the flag*

1. ***Find me! :-***

* *According to description searching her profiles in various social media apps can give me the flag.*
* *First I opened twitter and searched for her profile.*
* *There she mentioned her instagram account.*
* *One of her posts is a switch board of specific company.*
* *I Google about that company and got that I was started in Italy.*

*Wired {Italy}*

1. ***L05t\_With1n\_R0bots:-***

* *After connect board to laptop.*
* *Next, I connect corresponding Wi-Fi of the board.*
* *After opening the*

1. ***Web Sleuth! :-***

* *I searched for the repo read.ne written by Esteban lavos in GitHub.*
* *Then I got to know he also went by the name of Escobar lavos and he also we could find him on x.com*
* *I found the flag in the comments of one the post.*

1. ***Micro\_python:-***

* *After connecting the board to my laptop.*
* *Then I opened Arduino IDE and adjusted the frequency.*
* *I entered print(“flag”) and found the flag.*

1. ***Extract: -***
2. ***0R\_bu7\_3xCLus1v3 :-***
3. ***u\_4r7 :-***
4. ***Ain’t no sunshine!***

* *I got circuit from the attachment.*
* *I arranged the connections according to the circuit on the bread board.*
* *Then I found the flag.*

1. ***ESP\_ionage :-***

* *Connected the Esp to the laptop.*
* *Then connected to the espionage Wi-Fi.*
* *Got the Ip address of the Wi-Fi network.*
* *Used the Ip address on the web search bar and found a web page with HTML.*
* *Found the flag within the html code.*