PekoeCTF 2021 Writeup:

Problem Name (link to files)	Category	Point Value	Flag	Description	Hint	Author
The Slack point	General Skills	1	pekoe{english_breakfast_d0dfb0}	Join our slack to find teams, hangout, or even DM the mods for hints	HEY SLACKER, WHY HAVEN'T YOU DONE THIS ALREADY?	Toby
Glass [glass.docx]	General Skills	50	pekoe{chai_a17c36}	Somehow I feel like there is more to this document than meets the eye	Try checking inside	Toby
Fruit [fruit.pages]	General Skills	50	pekoe{fruits_d'alsace_634adc}	Somehow I feel like there is more to this document than meets the eye	Try checking inside	Toby
(a grep problem)	General Skills	50				Ezra
Not a Nintendo64 [notendo64.txt]	General Skills	50	pekoe{earl_grey_54d520}	I asked my Uncle for a Nintendo64 and he replied with this... This doesn't look like normal text	it should be pretty straight forward to convert this to text	Toby
NAME THAT LANGUAGE!	General Skills	50		Take this quiz to win the flag (website here)		Toby and John?
Hello World [HelloWorld.zip]	Web Exploitation	50	pekoe{peach_ginger_46a962}	This is my hello world site. It's very impressive	What makes up a site?	John
Making hash browns? [hash]	General Skills	50	732f4459fc7476646640910b855db1d7	Someone told me to hash this file but I don't think I can do that because I am not a very good chef. Can you help me?	The flag is not in the usual format	Toby
eS Que eL [fancylogin.html]	Web Exploitation	50	pekoe{tisane_89f4n6}	Can you help me login to this site?	Do you speak spanish?	Owen
Rolling, rolling on a CTF [playlist.txt]	General Skills	50	pekoe{cranberry_autumn_f312ac}	Find the flag	You could probably do it manually but it might be easier if you clear away the garbage	Toby
Driving a Tractor [tractor.java]	Reverse Engineering	100	pekoe{ruby_black_39k8ds}	Can you put this tractor in reverse? It's license plate is "s¤hµnrèh~æuÎxðe1|æbWekoÒdºf,n©bC6Þ<Fn©;g/võ"	You may want to write a program that can turn the license plate into the flag.	Owen
Ceaser1.txt	Cryptography	25	pekoe{name_of_the_exploration_rover}	I am doing a project on a planet, will you help me?		Francesca
Ceaser2.txt	Cryptography	50	pekoe{nickname_of_mars}	goes with 1	Keyword is the answer of Ceaser1	Francesca
Cesear3.txt	Cryptography	75	pekoe{lets_go_live_in_mars}	goes with 1	keyword is the answer of Caesar 2	Francesca
Tar and feather [500.tar.gz]	General Skills	100	pekoe{moroccan_mint_dc55ea}	I wanted to save some disk space so I compressed the flag	I may have compressed it 500 times	Toby
Try my cookie cookie [https://pekoe-try-my-cookie-cookie.herokuapp.com/]	Web Exploitation	100	pekoe{chamomile_dba943}	Only 99 cents plus tax (For testing: you have to run this one in firefox if running locally)	The title says it all	John
A very broken image [broken_image.png]	Forensics	100	pekoe{oolong_c4c13a}	This image file has the flag, but I can't open it	If only it was this easy to repair the world's problems in a hex editor	[redacted]
Bitcoin is very volitile [https://pekoe-bitcoin-is-very-volatile.herokuapp.com/]	Web Exploitation	100	pekoe{passionfruit_mango_b5048e}	Bitcoin is very volatile today.	There are a few types of requests	John
Dogecoin to the moon [https://pekoe-dogecoi	Web Exploitation	100	pekoe{orange_50b3c2}	"One word: Doge" - Elon Musk's Twitter	Next stop: Dogecoin moon **base** (For testing: you have to run this one in firefox if running locally)	John

n-to-the-moon.herokuapp.com/]						
Pekoemon [https://pekoe-pekoemon.herokuapp.com/]	Web Exploitation	100	pekoe{refresher_mint_bab305}	Gotta catchem all	You're going to want to use a program called Postman for this problem	John
Where's my backup? [backup2.img]	Forensics	100	pekoe{mango_fruit_26a9f2}	I asked a friend to backup a very important file on my flash drive, but instead of sending me the file they sent me this strange thing	Knowing the filesystem (and where it starts) would be helpful	Toby
(An RSA problem)	Cryptography	100				
Secret SSH	General Skills			I may have used the default password on my tiny fruit themed computer but atleast I secured it by changing the port... Right????	First you have to find what port the service is actually on, then you have to "guess" the username and password - many of you likely know what it is already.	Toby
Dr.Java [drjava.jar]	Forensics	100	pekoe{darjeeling_fa5bd8}	Dr.Java knows all, including the flag	I hid the flag somewhere in this IDE	Toby
normal gcode [flag.gcode]	General Skills	100	pekoe{lemon_7567a}	I wanted to 3D print the flag	I said this gcode is normal, but I didn't say what kind of normal it was. If you are having issues it might help to check that	Toby
the missing link	General Skills	100	pekoe{Wulong_56bfda}	The flag is on my website. It should be easy enough to get there [the_missing_link.jpg]	How could you get a link from a picture?	Toby
the magic colors	Forensics	100	pekoe{tea_476a}	A friend sent me this strange image. I wonder what it could mean.	How could you get a flag (text) from this picture. If you seem to be on the right track but are having issues ask in Slack, there may be some inconsistency	Toby
inception	Forensics					
Arduino_Bitmap [flag.ino]	Forensics	200	pekoe{mint_a128}	The flag is embedded somewhere in this Arduino program	You don't need any special hardware for this.	Toby
The droid you are looking for [flag_app.apk]	Forensics	200	pekoe{rooibos_1afcb5}	This app isn't the droid you are looking for, or is it?	If you don't have an Android phone setting up a VM might be helpful, but shouldn't be necessary	Toby
Super Secure Gcode? [flag.gcode.cubepro]	Cryptography	200	pekoe{brisk_berry_f17b23}	I just got a "new" 3D printer that uses encrypted gcode for some reason???? ¯_(ツ)_/¯ anyways I tried to create a file for it and hid the flag somewhere in it	You need to get it down to plain text. The file uses a blowfish scheme, some tools exist to make this trivial. If you are still stuck the file extension might help	Toby
dictionary skills	Cryptography	200	pekoe{goji_berry_b1faf3}	can you decode this message: U2FsdGVkX189XzZma1XalqGG0jwB8IERFj8UuzlFrcFwp727lETxrUuJP06LaLWF	in some ways this is similar to the super secure gcode problem... The message is encrypted with DES	Toby
Recovery Image image recovery [lineage-17.1-recovery-polaris.img]	Forensics	200	pekoe{ginger_76adb5}	Can you help me recover an image from my recovery image?	This is not a standard disk image	Toby
Noise 1 [output.wav]	Forensics	150	pekoe{tisane_14f7a9}	When my friend was driving through Kansas City they recorded this off the radio on to a cassette, what could it mean?	file is encoded in mono with a framerate of 9600 Hz.	Toby
Noise 2[flag.au]	Forensics	250	pekoe{tisane_a25ab9}	Even though it may seem like I am just hamming it up you simply can't ignore the fax. The flag is in this file somewhere	if you are struggling then the settings I encoded it with are as follows. The carrier is 1900hz the deviation is 400hz, modulation FM, filter middle, apt start (5s) /apt stop 300hz IPM 120, phasing line 20, normal, mono	Toby

Captcha the flag [https://pekoe-captcha-the-flag.herokuapp.com/]	General Skills	350	pekoe{chamomile_mango_cef460}	This website needs a 3 digit pin to login... that shouldn't be too hard to brute force, except for the pesky captcha	Maybe you can teach your computer to read the captcha...	John & Toby
sudo random? -1	Reverse Engineering	200	0.8229855101	a friend, who lives in a house on Wichmann Hill, told me that they could generate random numbers. They have 3 seeds that are each 100. They want me to guess the 5th random number	the number (the flag) is between 0 and 1 and should have at least 10 sig figs	Toby
sudo random? -2	Reverse Engineering	250	720469842	My friend said was very impressed that I guessed their random number, now they want me to guess the seed. They generated the following output.	The seeds are between 0-999	Toby
Easy_Java	Reverse Engineering	50	832807	I found this strange program, and a log of the output from when it first ran. The program outputed 895205. What was the input?	This should be a pretty straightforward problem	
MAX SCORE		4151				

1 - The Slack Point.

Join slack, find the pinned message in #announcements, solve the challenge. Serves as a way to encourage members to join the slack and familizare them with the CTFd portal and the flag format

2 - Glass

Change the .docx file to .zip and extract. Find the flag file. Tests knowledge of file extensions.

3- Fruit

Change the .pages file to .zip and extract. Companion problem to glass, aims to make it the same level of difficulty for people familiar with Mac or PC

4 - Not a Nintendo 64

Decode the base64 text. This can be done with an online tool.

5 - Hello World

Use inspect element to find the three pieces of the flag in the html, CSS, and JS.

6 - Making Hash Browns

Hash the provided text using MD5

7 - eS Que eL

SQL Injection use - ‘ or 1=1#

8 - Rolling, rolling on a CTF

Use find and replace to identify the correct link - flag is in description

9 - Driving a tractor

Write a program that takes the “license plate”, and outputs every other symbol, but shifted up 3 places in ASCII, which should give the flag.

10 - Caesar0.txt

Use an online Caesar cipher decoded (the shift is 11)

11 - Caesar1.txt

To be filled by fini

12 - Caesar2.txt

To be filled by fini

13 - Caesar3.txt

To be filled by fini

14 - Tar and feather

Use a script (bash is IMO the easiest, but I have seen people do it with Python or even Java) to untar all the files.
Example script: here

15 - Pekoemon

1. You’re going to need to install Postman (or some other program for analysing network requests)

2. Once Postman is installed and running go to “file” in the top right corner and select “new tab”
3. A new tab should appear with a search bar that says “Enter request URL”
4. In the search bar enter “https://pekoe-pekoemon.herokuapp.com/”, set the request type to post, and click send
5. Now click on the “Headers” tab above where the HTML output appears
6. The flag should appear with the corresponding key “Flag”

16 - A very broken image

-Basically unsolvable (see https://github.com/bhscomputerscienceclub/ctf-writeups/tree/master/pekoe/2021)
Sorry, it didn’t end up getting properly tested. The unbroken image is here so you can see what the unaltered headers are

17 - Try my cookie cookie

Check the cookies, and there should be a cookie with the name flag, and the value of the flag

18 - Dogecoin to the Moon

1. Under cookies there will be a cookie with the name “important-information”
2. This cookies value is encoded in base64, and if you decode it you’ll get the following JSON: {dogecoin-target: "$1"}
3. Change the target from "$1" to "moon", re-encode it and set the cookie to the new value
4. Reload the page, and there should be a cookie with the flag

19 - Captcha the Flag

To solve this problem you need to train a basic image recognition algorithm to solve the captcha each time, and then with that brute force the password -> or exploit a design flaw in the problem (see https://github.com/bhscomputerscienceclub/ctf-writeups/tree/master/pekoe/2021)

20 - Bitcoin is very Volatile

In index.js you’ll see the following XHTTP request

```
`
var xhttp = new XMLHttpRequest();
xhttp.onreadystatechange = function() {
    if (this.readyState == 4 && this.status == 200) {
        if(xhttp.responseText == 'true'){
            console.log('Bitcoin is very volatile today');
        }
        else{
            console.log(xhttp.responseText);
        }

    }
};

xhttp.open("GET", "./is-bitcoin-volatile", true);
xhttp.send();
`
```

Copy that code into the inspect element console, change the GET to POST, press enter, and the flag should log. You can also solve this problem by sending a post request to "https://pekoe-bitcoin-is-very-volatile.herokuapp.com/is-bitcoin-volatile" in postman

21 - Where's my backup

Mount the image file by using fdisk -l to find out the correct details and then using mount -o loop...

22 - Dr.Java!

Rename to .zip and open

23 - Normal gcode

Use a gcode viewer to see the flag drawn out

24 - The missing link

Reverse image search with Google or Bing

25 - The magic colors

Use a color picker to get the RGB values for the colors, convert to ascii, get flag

26 - Arduino Bitmap

Convert the image array to a bitmap to reveal the flag

27 - The Droid you are looking for?

Either install the APK on android and use “activity launcher” to open the flag screen, or use an APK deconstruction tool to extract the flag png

28 - Super Secure Gcode

Use either codeX or cube-utils in order to decrypt the gcode. Flag is at top of file in plain text.

29 - Dictionary skills

Use rockyou.txt with john the ripper or similar tool to solve for flag

30 - Recovery image image recovery

Unpack the recovery image using a recovery image unpacking tool such as the one linked here (https://forum.xda-developers.com/t/tutorial-edit-recovery-ramdisk-change-images-etc-n00b-friendly-tuto.2491791/)

31 - Noise 1

Use pyKCS or other KCS decoder tool to decode the flag text

32 - Noise 2

Use Hamfax or other WEFAX-IOC576 decoder to get the image

33 - Sudo Random? - 1

Use a wichmann hill algorithm with each seed set to 100. Enter the 5th number generated. (random note. This problem was inspired by this video)
Example algorithm is here

34 - Sudo Random? - 2

Use the algorithm for part 1 to brute force all the possible seeds (0-999) for each, compare the first output of the algorithm to the first output provided.

35 - Easy_Java

You can try to trace the code, but using brute force is definitely easier. Loop throw possible inputs to see what gives the correct output.