Cyberchef
Cyber Intel | Cyberchef | 24/09/2023

Executive Summary

Introduction:

CyberChef is a powerful and versatile open-source tool designed for data analysis, transformation, and encryption/decryption in the field of cybersecurity and digital forensics. This executive summary provides a concise overview of CyberChef's key features, benefits, and applications.

CyberChef is a simple, intuitive web app for carrying out all manner of "cyber" operations within a web browser. These operations include simple encoding like XOR and Base64, more complex encryption like AES, DES and Blowfish, creating binary and hexdumps, compression and decompression of data, calculating hashes and checksums, IPv6 and X.509 parsing, changing character encodings, and much more.

The tool is designed to enable both technical and non-technical analysts to manipulate data in complex ways without having to deal with complex tools or algorithms. It was conceived, designed, built and incrementally improved by an analyst in their 10% innovation time over several years.

Features:

- **Drag and drop**
  - Operations can be dragged in and out of the recipe list, or reorganised.
  - Files up to 2GB can be dragged over the input box to load them directly into the browser.
- **Auto Bake**
  - Whenever you modify the input or the recipe, CyberChef will automatically "bake" for you and produce the output immediately.

    - This can be turned off and operated manually if it is affecting performance (if the input is very large, for instance).
- **Automated encoding detection**
    - CyberChef uses a number of techniques to attempt to automatically detect which encodings your data is under. If it finds a suitable operation that make sense of your data, it displays the 'magic' icon in the Output field which you can click to decode your data.
- **Breakpoints**
    - You can set breakpoints on any operation in your recipe to pause execution before running it.
    - You can also step through the recipe one operation at a time to see what the data looks like at each stage.
- **Save and load recipes**
    - If you come up with an awesome recipe that you know you'll want to use again, just click "Save recipe" and add it to your local storage. It'll be waiting for you next time you visit CyberChef.
    - You can also copy the URL, which includes your recipe and input, to easily share it with others.
- **Search**
    - If you know the name of the operation you want or a word associated with it, start typing it into the search field and any matching operations will immediately be shown.
- **Highlighting**
    - When you highlight text in the input or output, the offset and length values will be displayed and, if possible, the corresponding data will be highlighted in the output or input respectively (example: highlight the word 'question' in the input to see where it appears in the output).
- **Save to file and load from file**
    - You can save the output to a file at any time or load a file by dragging and dropping it into the input field. Files up to around 2GB are supported (depending on your browser), however, some operations may take a very long time to run over this much data.
- **CyberChef is entirely client-side**
    - It should be noted that none of your recipe configuration or input (either text or files) is ever sent to the CyberChef web server - all processing is carried out within your browser, on your own computer.
    - Due to this feature, CyberChef can be downloaded and run locally. You can use the link in the top left corner of the app to download a full copy of CyberChef and drop it into a virtual machine, share it with other people, or host it in a closed network.

Applications:

- **Incident Response**: CyberChef is invaluable for cybersecurity professionals responding to incidents, helping analyse and decode malicious data, extract indicators of compromise, and understand attack vectors.
- **Digital Forensics**: It aids digital forensic experts in parsing and analysing evidence, uncovering hidden information in various file formats, and decrypting secured data.
- **Penetration Testing**: CyberChef assists penetration testers in crafting payloads, encoding and decoding data for exploitation, and analysing results from vulnerability assessments.
- **Threat Intelligence:** Security analysts use CyberChef to dissect threat data, convert indicators, and prepare data for analysis, enhancing threat intelligence capabilities.

Index

1. Introduction

CyberChef is a simple, intuitive web app for carrying out all manner of "cyber" operations within a web browser. These operations include simple encoding like XOR and Base64, more complex encryption like AES, DES and Blowfish,

creating binary and hexdumps, compression and decompression of data, calculating hashes and checksums, IPv6 and X.509 parsing, changing character encodings, and much more.

The tool is designed to enable both technical and non-technical analysts to manipulate data in complex ways without having to deal with complex tools or algorithms. It was conceived, designed, built and incrementally improved by an analyst in their 10% innovation time over several years.

In the ever-evolving landscape of cybersecurity and digital forensics, the need for powerful and adaptable tools has never been greater. CyberChef – a cutting-edge, open-source solution designed to empower professionals and enthusiasts alike with the ability to decipher, transform, and secure digital data effortlessly. In this introduction, we will embark on a journey into the world of CyberChef, unveiling its capabilities, versatility, and the transformative impact it can have in the realm of digital information processing. Whether you're a seasoned cybersecurity expert, a digital investigator, or simply curious about the art of data manipulation, CyberChef is your gateway to unlocking the secrets hidden within the vast digital realm.

2. Tool Details

Link to Github repo/ Installer source: https://github.com/gchq/CyberChef

Website link: https://gchq.github.io/CyberChef/

Dependencies (if any):

CyberChef is built to fully support Node.js v16.

CyberChef is built to support

- Google Chrome 50+
- Mozilla Firefox 38+

Use Cases List:

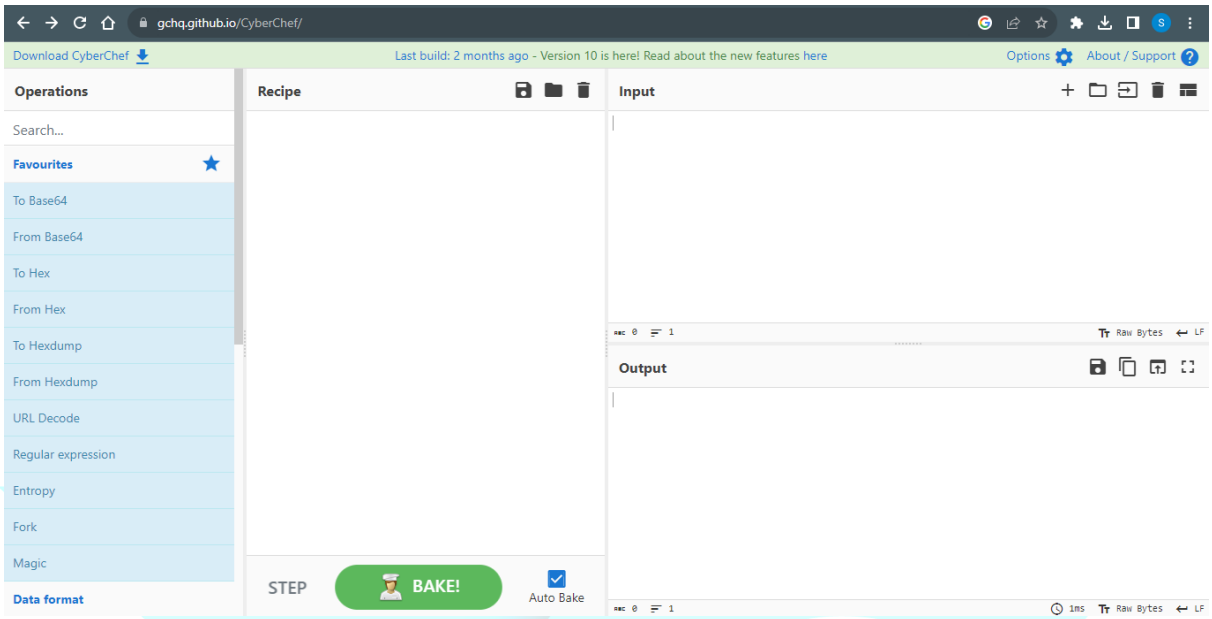
You can use as many operations as you like in simple or complex ways. Some examples are as follows:

- Decode a Base64-encoded string
- Convert a date and time to a different time zone
- Parse a Teredo IPv6 address
- Convert data from a hexdump, then decompress
- Decrypt and disassemble shellcode
- Display multiple timestamps as full dates
- Carry out different operations on data of different types
- Use parts of the input as arguments to operations
- Perform AES decryption, extracting the IV from the beginning of the cipher stream
- Automagically detect several layers of nested encoding

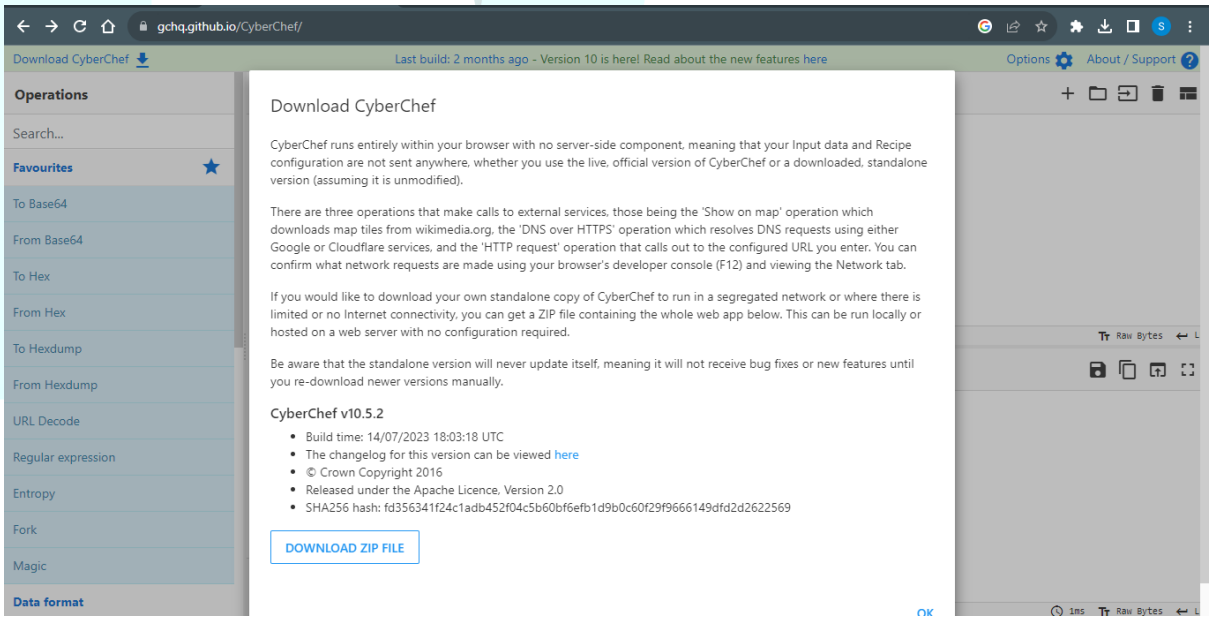
Version worked on in the report: v10.5.2
Date of installation and run: 24/09/2023
Interface: Web Interface

3. Installation

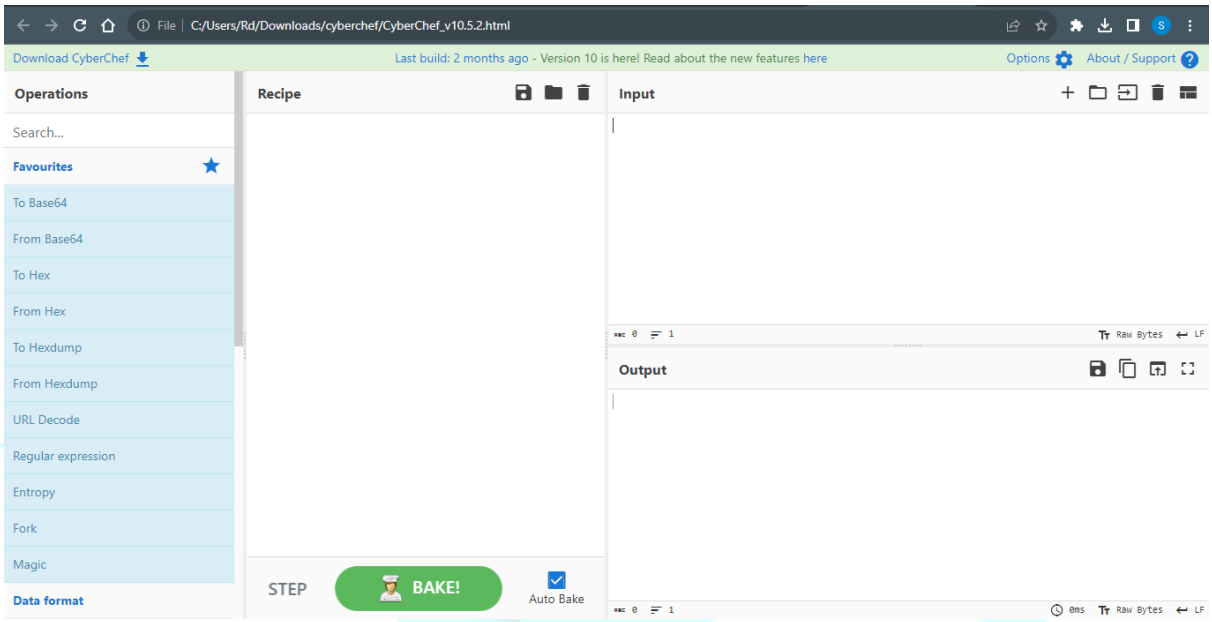
Step 1. User can either directly open the web interface from https://gchq.github.io/CyberChef/ or they can also download the application zip file from the website.



Step 2: Download the zip file from the top left corner of the webpage where the download link exists.



Step 3: Extract the zip file and open the html file contained in the extracted folder



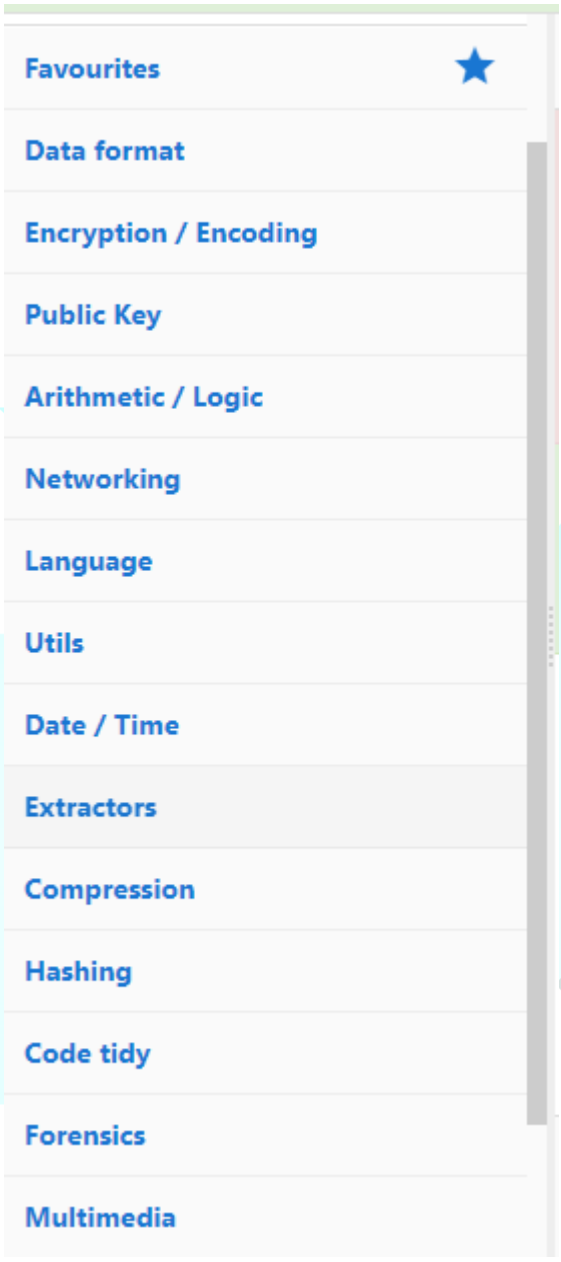
4. Execution

Step 1: If user wants to see sample test cases and examples, then they can directly run the predetermined inputs using the links given on the github page of the tool

You can use as many operations as you like in simple or complex ways. Some examples are as follows:

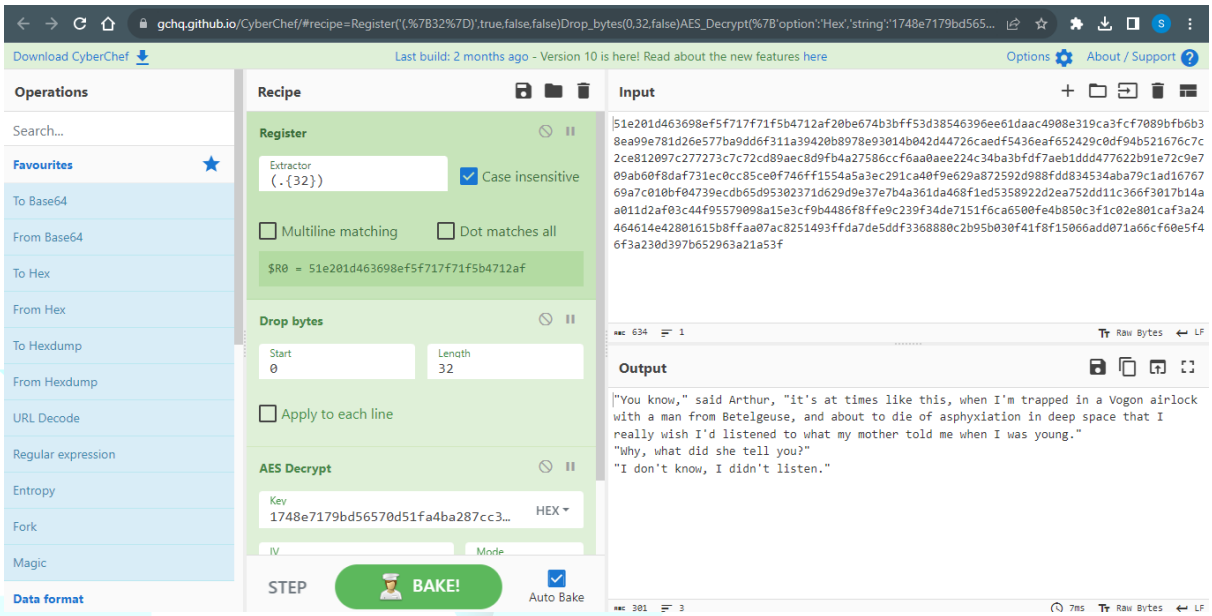
- Decode a Base64-encoded string
- Convert a date and time to a different time zone
- Parse a Teredo IPv6 address
- Convert data from a hexdump, then decompress
- Decrypt and disassemble shellcode
- Display multiple timestamps as full dates
- Carry out different operations on data of different types
- Use parts of the input as arguments to operations
- Perform AES decryption, extracting the IV from the beginning of the cipher stream
- Automagically detect several layers of nested encoding

Step 2: There is a wide variety of options available on the website to perform any operation

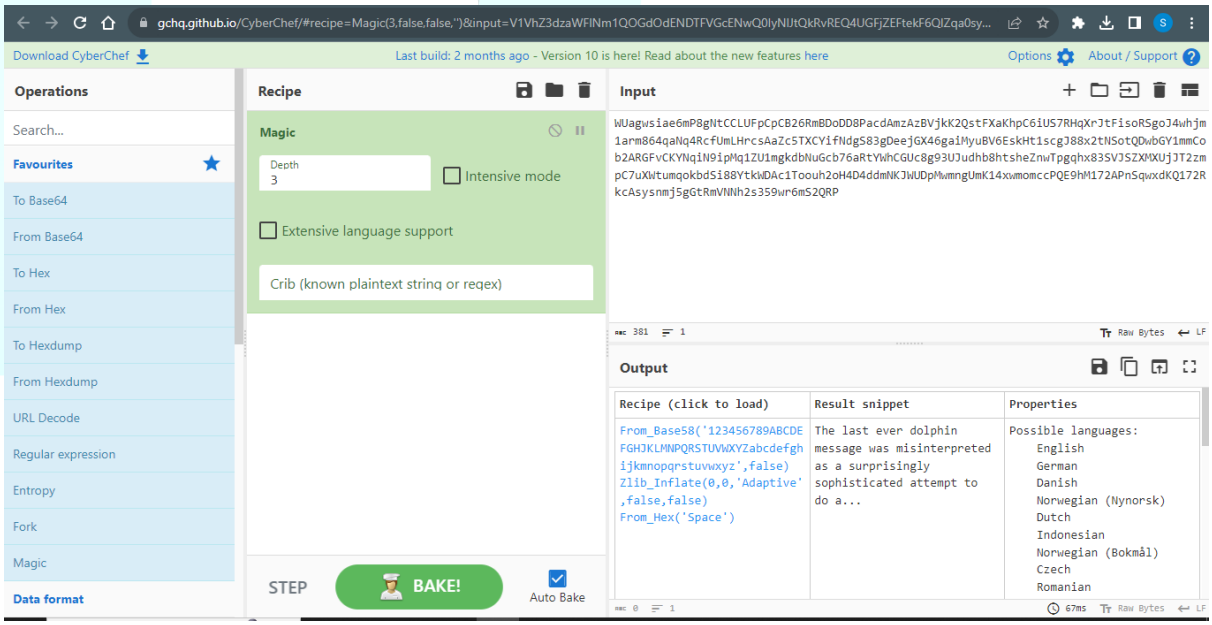


Some examples of tool:

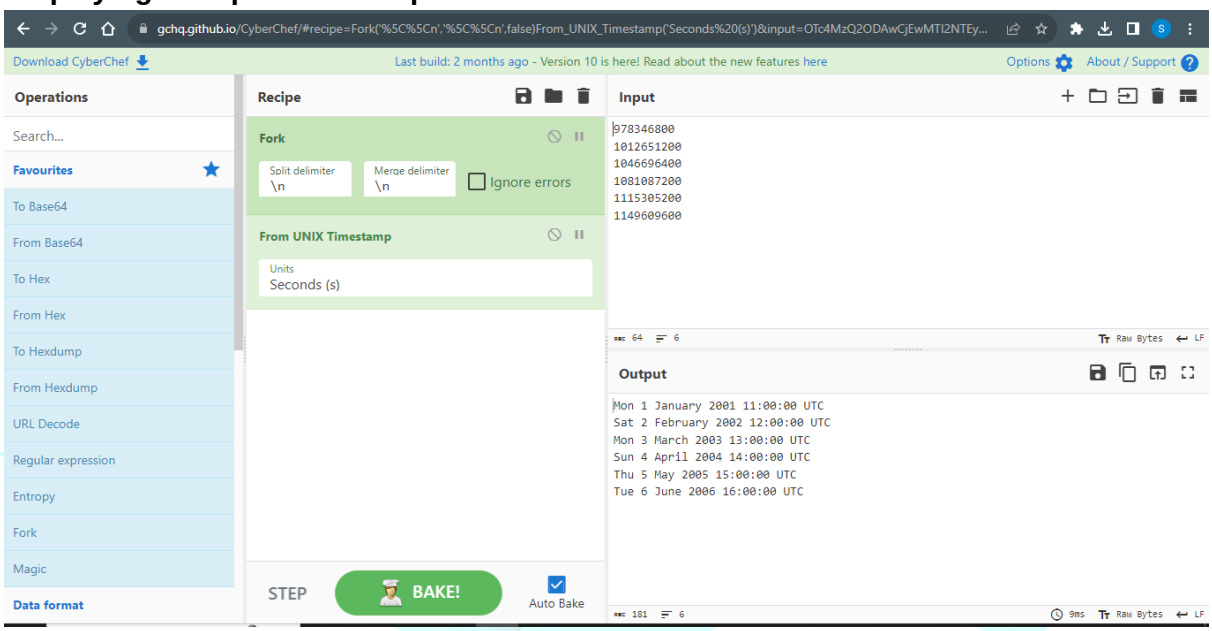
AES Decryption



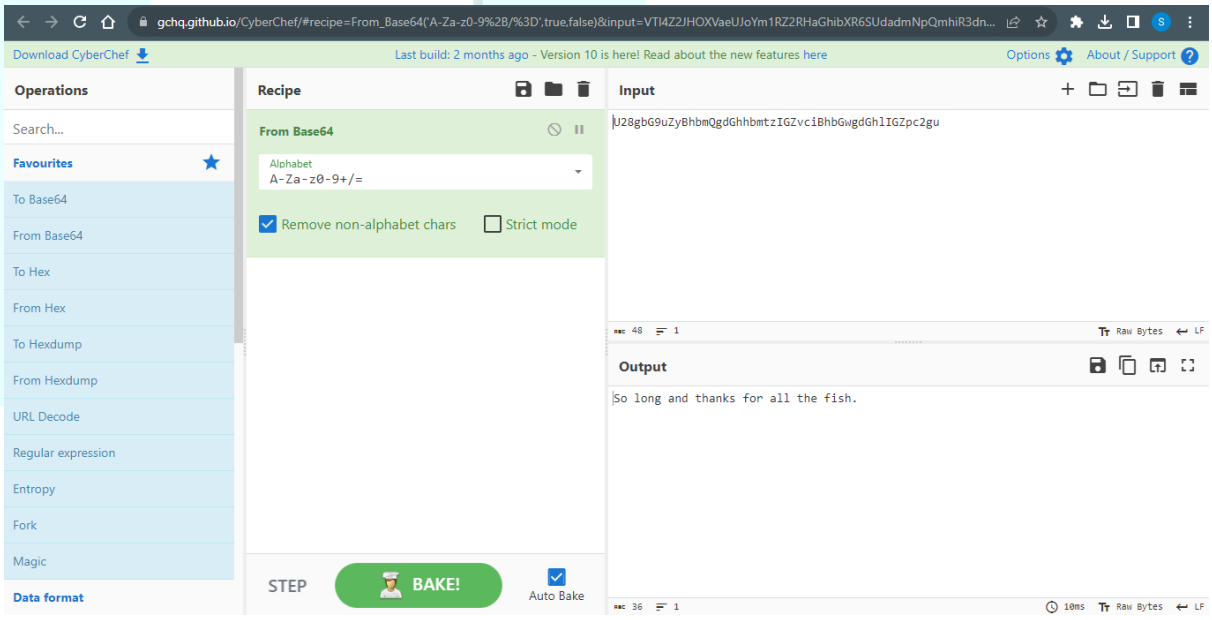
Detecting several layers of nested encoding



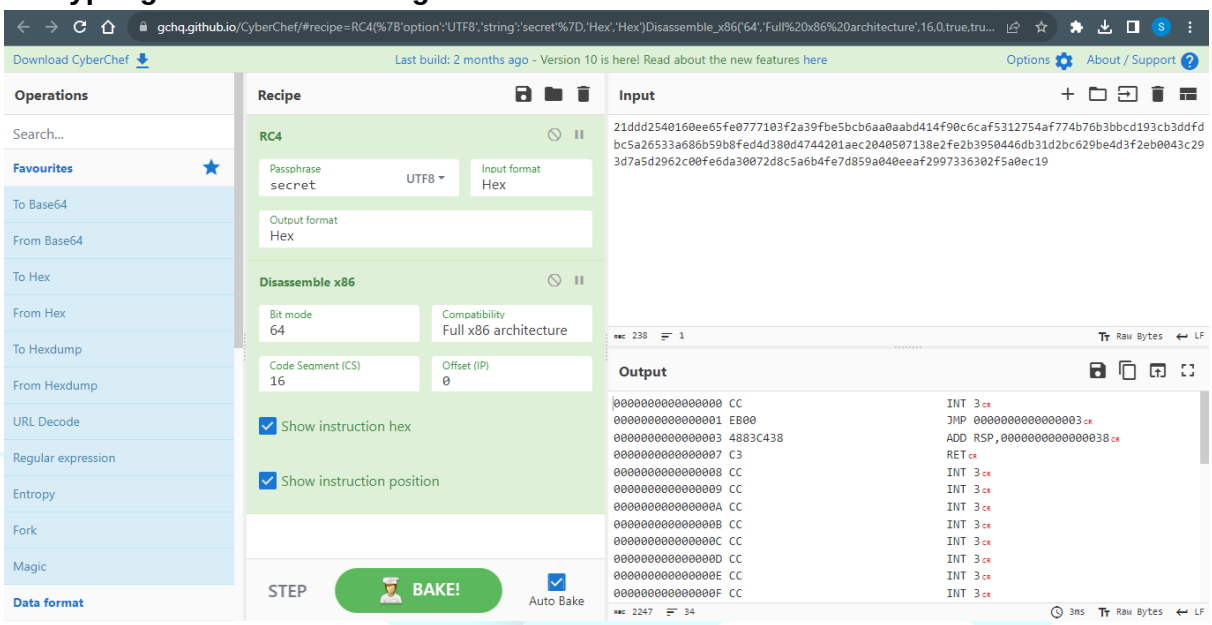
Displaying multiple timestamps as dates:



Decrypting base-64 encoded string:

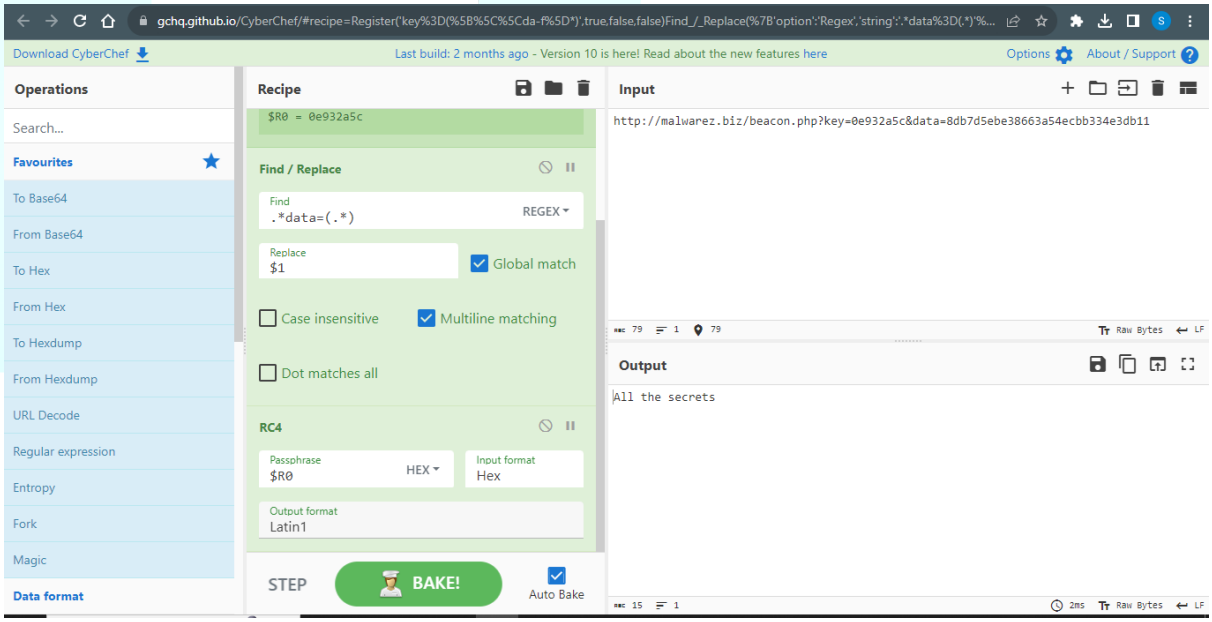


Decrypting and disassembling shellcode:



Using part of the input as argument for the operation:

(data=8db7d5ebe38663a54ecbb334e3db11 : All the secrets)



5. Scope and Limitations

Scope and features:

- **Data Transformation and Manipulation:** CyberChef excels at transforming data from one format to another. It supports a wide range of encoding, decoding, hashing, encryption, and decryption operations. This makes it invaluable for tasks such as data conversion, data obfuscation, and data normalization.

- **Batch Processing**: CyberChef allows users to process multiple pieces of data simultaneously, making it suitable for tasks involving large datasets or repetitive operations. This can significantly improve efficiency in data analysis and processing workflows.

- **Customization**: Users can create custom "recipes" in CyberChef, which are reusable sets of operations tailored to specific tasks. This feature enhances productivity and ensures consistency in data processing.

- **Data Visualization**: CyberChef provides tools for visualizing data, such as generating histograms and previewing data formats. These capabilities aid in better understanding and interpreting data.

- **Security and Privacy:** CyberChef operates entirely on the client side, meaning that sensitive data stays on the user's device. This enhances security and privacy, making it suitable for handling sensitive information.

- **Web-Based Access:** Being web-based, CyberChef is accessible from any device with a web browser, promoting collaboration among cybersecurity teams and ensuring accessibility across various platforms.

Limitations:

- **Complexity**: While CyberChef is user-friendly, some of its advanced operations may require a good understanding of data formats, encoding

schemes, and cryptography principles. Novice users may need time to learn and effectively utilize these features.

- **Dependency on Pre-built Operations:** CyberChef relies on a library of pre-built operations. If a specific operation is not available out of the box, users may need to implement it themselves or seek alternative tools.

- **Not a Complete Forensics Solution**: While CyberChef is useful for data manipulation and analysis, it is not a comprehensive digital forensics tool. It lacks features such as disk imaging, file system analysis, and registry examination, which are essential for a complete forensic investigation.

- **Limited Automation:** While it supports batch processing, CyberChef does not provide advanced automation capabilities found in dedicated scripting or programming languages. Users looking for complex automation tasks may need to integrate CyberChef with other tools or write scripts separately.

- **Internet Dependency**: While CyberChef's web-based nature is advantageous, it also means that users need internet access to use the tool. In situations with limited or no connectivity, this may be a limitation.

6. Conclusion

In conclusion, CyberChef stands as a formidable asset in the arsenal of professionals and enthusiasts navigating the intricate realms of cybersecurity, digital forensics, and data analysis.

CyberChef's user-friendly interface and customization options empower users to decode, encode, and manipulate data with ease, making it accessible to both experts and novices. Its invaluable role in incident response, digital investigations, penetration testing, and threat intelligence is undeniable, as it equips users with the agility to dissect, decipher, and secure digital information swiftly and effectively.

While CyberChef shines brightly in its domain, it is important to acknowledge its limitations, such as the need for some familiarity with data formats and encoding

schemes, as well as its dependency on pre-built operations. Nonetheless, these limitations are overshadowed by its capacity to streamline complex tasks, enhance data analysis, and promote collaboration among cybersecurity teams.

7. References

https://github.com/gchq/CyberChef

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