**InfoSec Project Idea: All-in-One Cyber Tool**

This document outlines the concept for a web-based information security tool that combines the data manipulation capabilities of CyberChef with a suite of steganography and forensic analysis features.

**## Part 1: The "CyberChef" Core** 🧑‍🍳

The foundation of the project is a tool for encoding, decoding, and transforming data on the fly.

* **Concept:** A three-panel web interface:
  1. **Input Panel:** For pasting raw data.
  2. **Operations Panel:** A list of functions to apply.
  3. **Output Panel:** Shows the transformed data in real-time.
* **Core Functions to Implement:**
  1. **Encoding/Decoding:** Base64, Hexadecimal, ROT13, URL Encoding.
  2. **Hashing (One-Way):** MD5, SHA-1, SHA-256.
  3. **Logical Operations:** XOR, AND, OR for byte-level manipulation.
  4. **Compression:** Gzip, Zlib.

**## Part 2: Steganography Features** 🤫

This module focuses on hiding data within other files.

* **Image Steganography (LSB):**
  + **Concept:** Hide a secret message in the Least Significant Bits (LSB) of an image's pixels. The change is visually undetectable.
  + **Implementation:** An interface to upload a "carrier" image, input a secret message, and download the new image with the hidden data. A corresponding "decode" function is also needed.
* **Text Steganography:**
  + **Zero-Width Characters:** Hide binary data using invisible Unicode characters.
  + **Whitespace Steganography:** Use unique combinations of spaces and tabs to encode information within a body of text.

**## Part 3: Advanced Features (To Make it More Interesting)**

These features elevate the project from a simple utility to a more comprehensive analysis suite.

**###** 🕵️‍♂️ **Forensic and Analysis Tools**

* **Steganalysis (Detecting Hidden Data):**
  + **LSB Visualizer:** An impressive tool that processes an image and displays only its LSB data. This can visually reveal patterns or shapes of hidden messages that are otherwise invisible.
  + **Chi-Square Attack:** A statistical test to detect if an image's pixel data has been unnaturally altered, which is a common side effect of LSB steganography.
* **Magic Byte Analyzer:**
  + A tool to read the first few bytes of any uploaded file to determine its *true* file type, regardless of its extension (e.g., detecting an .exe disguised as a .jpg).

**###** ✨ **Enhanced "CyberChef" Experience**

* **"Magic" Auto-Detection:** The tool intelligently analyzes the input and suggests the most likely decoding operation (e.g., suggests "From Base64" if the input ends with an = sign).
* **Regular Expression (Regex) Tester:** A dedicated module to build, test, and apply regex patterns to extract data from the input.
* **Classical Ciphers:** Add fun, historical ciphers like Caesar, Vigenère, and Atbash.

**###** 🔊 **Expanded Steganography Methods**

* **Audio Steganography:** Hide data in the LSB of audio samples in .wav files.
* **Metadata (EXIF) Steganography:** Hide messages in the metadata fields of a photo, such as the "Comments" or "Camera Model" fields.