I propose to build a tool that can describe the structure of a zip file and recover tampered central directories autonomously. When describing the structure, I plan on displaying every field based on these specifications:

Table

Description automatically generated

Table

Description automatically generated

Table

Description automatically generated

In order to parse this information, I plan on using python, and a particular module, Struct; It is a module that performs conversions between Python values and C structs represented as Python bytes objects. Using this I can create an analog directory of the data structures allowing me to view and modify specific fields. From there I can create new binary representations of headers and records and place them at desirable offsets programmatically.

Ultimately, this tool’s goal is to restore tampered central directory headers and provide clarity on the actual Zip file data outside conventional zip applications. To make it user friendly I can incorporate a console interface and a GUI. If making a GUI is preferred, the easiest way for me to do this would be to use Java’s Swing API. Resources like NetBeans IDE makes it super simple to design and create modifiable GUIs on the fly. I could create a java runtime environment that gets extracted and executed by a program in c#, which allows a user to run the application in a single click. I could also create a frontend using the browser and relay information from python through JavaScript, but typically digital forensics applications are built for desktop. If a GUI doesn’t fall within the scope of this project than a console application would serve various flags that would toggle the various behaviors – displaying data, prompting information.