VMIFF - Visualization Metrics for the Identification of File Fragments

Visualization of complex data, such as a file system or file, allows a forensic analyst or reverse engineer to rapidly locate areas of interest amidst a large quantity of data. While visualization provides a promising form of analysis, is the subject of much skepticism, as human interaction is required in order for this method to be successful. As a result of this, visualization methods face two major obstacles: tediousness and time.

As our contribution, we propose a unique method of graphing visual information into a measurable format suitable for use with machine learning algorithms. This method will still utilize the visual layout of the data but streamline this form into one that can be rapidly processed by a machine.

In this work we examine existing methods of file fragment analysis, determine how to apply visualization to this analysis, and transform this visual data into a measurable format for machine leaning algorithms using our tool called VMIFF (Visualization Metrics for the Identification of File Fragments). In its breadth, this work aims to demonstrate that such transformations will still yield meaningful results.