A Brief Summary:

* The reproduction of MalConv they use (EMBER) is available on GitHub
* Their dataset is 700 samples in size at roughly 50/50 malware/benign
* Their analysis is four separate sections:
  + The first is concerned with the content of the binary files and their "gradient" (which I assume is meant to relate to Gradient Descent but I am unsure as it is unclear in the paper)
  + The second is a line of experimentation involving interpolation between benign and malicious files to generate new samples to classify with the model-- the authors then state that their results hint that machine learning models learn to classify by linearly interpolating (?) which strikes me as strange (pg 5; just below Fig 6)
  + The third seems strange as well as what it appears is that they train two convolutional filter's parameters (presumably from the same data) and then demonstrate that the two filters are correlated which would be obvious if they were indeed trained on the same data
  + The fourth then only adds to my confusion as apparently both filters perform differently when applied, having vastly different accuracy. Additionally, the standard MalConv uses 128 filters, so testing the performance of a single filter doesn't seem useful to me (?)