• **What is OS Fingerprinting:**
  – Process of detecting OSes of remote machines.

• **What we are doing:**
  – We are developing an OS fingerprinting system
  – The system employs Genetic Algorithm (GA) and Machine Learning (ML) techniques

• **Methodology:**
  – **Data:** instances of different OSes.
  – **Genetic Algorithm:** to select relevant features.
  – **Machine Learning algorithms:** to extract rules for OS Fingerprinting.
OS Fingerprinting using ML

- **Advantages:**
  - The system is a single-packet classification system.
  - The system is the first OS classifier to adopt GA.
  - The system is completely machine learning dependant.

- **Algorithms being tested:**
  - J48, JRip, Ridor, PART

- **Fitness Function:**

\[
Fitness = 0.80 \times \text{Accuracy} + \\
0.15 \times \left(1 - \frac{|\text{SelectedFeatures}| - 1}{|\text{AllFeatures}| - 1}\right) + \\
0.05 \times \left(1 - \frac{|\text{SelectedRules}| - 1}{|\text{AllRules}| - 1}\right)
\]