## Traffic Fingerprint

Pick directories to perform training on from below:

training\_malware training\_protocols

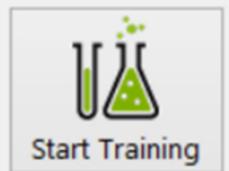
training\_websites

Centroids

25 📥

Threshold

3.0



Status: Ready...



Show quantizations



Show histogram



Fingerprint graphs



Export fingerprint CSVs

90.72%

Capture: cryptlocker1\_gamma\_29

cryptlocker1\_gamma\_290114-17\_42\_37.pcap



Compare capture w/all fingerprints

Fingerprint:

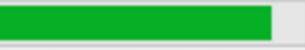
Bladabindi\_alpha\_1



Analyze just this fingerprint

Analysis result:

Tree-Distance (KL) method:



Most likely "cryptlocker\_gamma\_1"

Additional candidates:

"cryptlocker\_gamma\_2" with 90.61,

"cryptlocker\_alpha\_2" with 87.26

