

Traffic Fingerprint

Pick directories to perform training on from below:

training_malware
training_protocols
training_websites

Centroids

25

Threshold

3.0



Start Training

Status: **Ready...**



Show quantizations



Show histogram



Fingerprint graphs



Export fingerprint CSVs

Capture:

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:



90.72%

Most likely "cryptlocker_gamma_1"

Additional candidates:

"cryptlocker_gamma_2" with 90.61,
"cryptlocker_alpha_2" with 87.26



All fingerprints