Sysseclo

Anomaly-stat-V2

forward_tracker.py (ISSUE 1)
↓ .names, .ids
name_freq_counter.py
↓ test.csv
dbg_procs_data.py (ISSUE 2)
↓ programs, .proc
generate_list.py
↓ out
Backtracker-Qi (ISSUE 3)

results

result_analytics.py
↓ noto-fileless-malware-hash.txt
download_similar_mal_hash.py ---- VT Total
↓
.bin

cuckoo C1

cuckooC2

asi-SV2-clone

malware2db_mapping.py (ISSUE 4)
↓ fileless-malware-agent ID-db_mapping.csv
malware DB-query.py
↓ fileless-backtracker-input.tsv
Backtracker-Qi
(ISSUE 3)