```
C:\Users\islab\anaconda3\envs\pytorch1\python.exe D:\UULi\test_code\k_arm_test\main.py
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000000----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-4', '0-7']
***Trigger Reverse Engineering開始***
Target: 0, victim: 7, Loss: 9.1085, Acc: 0.00%, CE_Loss: 9.11, Reg_Loss:2558.18, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2540.18:   3%|          | 31/1000 [00:21<11:20,  1.42it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 32.6272029876709
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000001----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 0
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 0, victim: 4, Loss: 2.8775, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:2877.28, Cost:0.00 best_reg:2917.16 avg_loss_reg:2906.83:  16%|▉         | 160/1000 [27:10<2:22:42, 10.19s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 2885.2230224609375 Optimization Steps: 161
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1643.9113094806671
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000002----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 17.549953937530518
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000003----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-5', '0-8', '1-6']
***Trigger Reverse Engineering開始***
Target: 0, victim: 8, Loss: 2.1476, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:120.41, Cost:0.02 best_reg:121.92 avg_loss_reg:118.75:  13%|▊         | 127/1000 [00:16<01:52,  7.77it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 8 Trigger Size: 120.41090393066406 Optimization Steps: 98
***Symmetric Check開始***
Target: 8, victim: 0, Loss: 1.1514, Acc: 90.00%, CE_Loss: 0.51, Reg_Loss:3254.83, Cost:0.00 best_reg:6717.51 avg_loss_reg:3240.99: 100%|██████████| 98/98 [00:12<00:00,  7.90it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 35.77088284492493
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000004----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['12-14']
***Trigger Reverse Engineering開始***
Target: 12, victim: 14, Loss: 8.0868, Acc: 0.00%, CE_Loss: 8.09, Reg_Loss:2543.81, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2532.46:   1%|          | 10/1000 [00:01<01:51,  8.90it/s]
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 14 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 10.38974905014038
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000005----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 0
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 0, victim: 12, Loss: 1.7018, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:3809.92, Cost:0.00 best_reg:3799.33 avg_loss_reg:3818.20:  12%|▊         | 115/1000 [13:56<1:47:19,  7.28s/it]
early stop 所有
***Trigger Reverse Engineering結束***
```

```
Target Class: 0 Victim Class: all Trigger Size: 3799.326904296875 Optimization Steps: 116
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 848.5646343231201
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000006----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 10
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 10, victim: 12, Loss: 0.3737, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:830.03, Cost:0.00 best_reg:824.60 avg_loss_reg:830.00:   6%|▌         | 65/1000 [02:28<35:35,  2.28s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: all Trigger Size: 824.5954318576389 Optimization Steps: 66
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 157.88350629806519
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000007----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-20', '9-20']
***Trigger Reverse Engineering開始***
Target: 9, victim: 20, Loss: 1.3081, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:514.91, Cost:0.00 best_reg:516.99 avg_loss_reg:517.99:  32%|███▏      | 320/1000 [00:44<01:34,  7.18it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 20 Trigger Size: 514.91015625 Optimization Steps: 310
***Symmetric Check開始***
Target: 20, victim: 9, Loss: 1.8924, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:5364.59, Cost:0.00 best_reg:5274.17 avg_loss_reg:5359.79: 100%|██████████| 310/310 [00:43<00:00,  7.15it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 99.69884490966797
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000008----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 20.20454978942871
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000009----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 4
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 4, victim: 19, Loss: 0.7130, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:93.90, Cost:0.01 best_reg:93.60 avg_loss_reg:93.72:  13%|▏         | 126/1000 [52:39<6:05:16, 25.08s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: all Trigger Size: 93.59891401018415 Optimization Steps: 127
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 3175.2218885421753
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000010----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.298462390899658
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000011----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.590208768844604
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000012----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
```

整體耗時: 20.46985673904419
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000013----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-15', '2-1', '2-10', '3-4', '4-14', '5-10', '7-1', '7-9', '11-1', '11-10', '11-15', '12-4', '12-14', '15-14', '16-4']
Trigger Reverse Engineering開始
Target: 11, victim: 15, Loss: 1.5402, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:124.50, Cost:0.01 best_reg:124.67 avg_loss_reg:124.77: 43%|[redacted]| 427/1000 [03:05<04:09, 2.30it/s]
early stop 所有
Trigger Reverse Engineering結束
Target Class: 11 Victim Class: 15 Trigger Size: 124.50299835205078 Optimization Steps: 127
Symmetric Check開始
Target: 15, victim: 11, Loss: 7.2660, Acc: 80.00%, CE_Loss: 0.75, Reg_Loss:9769.91, Cost:0.00 best_reg:15144.27 avg_loss_reg:10184.31: 100%|[redacted]| 127/127 [00:46<00:00, 2.71it/s]
Symmetric Check結束
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 241.6618514060974
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000014----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 11.132597923278809
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000015----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 8.272382497787476
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000016----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 17.52834439277649
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000017----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 8.810150861740112
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000018----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 16.901154279708862
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000019----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 16.05219841003418
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000020----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 3.6919925212860107
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000021----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 12.595725774765015
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000022----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-11', '1-6', '1-7', '1-9', '2-0', '2-10', '3-11', '5-6', '5-8', '6-5', '7-1', '7-8', '9-3', '10-2']
Trigger Reverse Engineering開始

```
Target: 5, victim: 6, Loss: 2.3234, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:54.84, Cost:0.04 best_reg:54.97 avg_loss_reg:54.97:  27%|███       | 266/1000 [00:19<00:54, 13.57it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 6 Trigger Size: 54.83860778808594 Optimization Steps: 103
***Symmetric Check開始***
Target: 6, victim: 5, Loss: 1.6170, Acc: 90.00%, CE_Loss: 0.32, Reg_Loss:1945.85, Cost:0.00 best_reg:2060.69 avg_loss_reg:1978.39: 100%|██████████| 103/103 [00:07<00:00, 13.40it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 33.65658688545227
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000023----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-8', '9-6', '12-1', '12-8', '13-0']
***Trigger Reverse Engineering開始***
Target: 12, victim: 8, Loss: 1.3848, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:389.15, Cost:0.00 best_reg:390.60 avg_loss_reg:387.86:  34%|███▍      | 340/1000 [01:19<02:34,  4.28it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 8 Trigger Size: 389.1537170410156 Optimization Steps: 201
***Symmetric Check開始***
Target: 8, victim: 12, Loss: 1.8964, Acc: 95.00%, CE_Loss: 0.25, Reg_Loss:3712.50, Cost:0.00 best_reg:4129.94 avg_loss_reg:3708.70: 100%|██████████| 201/201 [00:46<00:00,  4.30it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 136.11167430877686
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000024----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['8-5', '8-9']
***Trigger Reverse Engineering開始***
Target: 8, victim: 9, Loss: 13.2254, Acc: 0.00%, CE_Loss: 13.23, Reg_Loss:2587.64, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2561.44:   2%|▏         | 21/1000 [01:16<59:13,  3.63s/it]
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 92.06118702888489
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000025----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.430930852890015
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000026----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['9-10', '9-16', '11-16']
***Trigger Reverse Engineering開始***
Target: 11, victim: 16, Loss: 6.6376, Acc: 0.00%, CE_Loss: 6.64, Reg_Loss:2525.99, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2518.81:   3%|▎         | 32/1000 [00:03<01:57,  8.21it/s]
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 10 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 11.79649543762207
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000027----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 6
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 6, victim: 19, Loss: 0.7005, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:1043.19, Cost:0.00 best_reg:1035.95 avg_loss_reg:1048.86:   6%|▌         | 61/1000 [32:39<8:22:36, 32.12s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: all Trigger Size: 1035.9530290876116 Optimization Steps: 62
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1979.9323785305023
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000028----------------------------------------
```

```
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-8']
***Trigger Reverse Engineering開始***
Target: 2, victim: 8, Loss: 4.8791, Acc: 0.00%, CE_Loss: 4.88, Reg_Loss:2577.06, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2559.87:   1%|          | 10/1000 [00:30<50:21,  3.05s/it]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 8 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 45.83541822433472
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000029----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['8-2', '8-6']
***Trigger Reverse Engineering開始***
Target: 8, victim: 6, Loss: 13.5948, Acc: 0.00%, CE_Loss: 13.59, Reg_Loss:2591.59, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2569.47:   3%|▎         | 31/1000 [00:03<01:59,  8.11it/s]
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 2 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 10.320770502090454
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000030----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-3', '1-5', '4-1']
***Trigger Reverse Engineering開始***
Target: 4, victim: 1, Loss: 8.2156, Acc: 0.00%, CE_Loss: 8.22, Reg_Loss:2585.05, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2565.52:   3%|▎         | 32/1000 [00:08<04:28,  3.60it/s]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 3 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 17.183552503585815
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000031----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-0', '3-4', '4-3']
***Trigger Reverse Engineering開始***
Target: 4, victim: 3, Loss: 0.4180, Acc: 95.00%, CE_Loss: 0.08, Reg_Loss:1734.67, Cost:0.00 best_reg:1736.45 avg_loss_reg:1733.61: 100%|██████████| 1000/1000 [34:22<00:00,  2.06s/it]
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 3 Trigger Size: 1736.4454345703125 Optimization Steps: 978
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 2072.59046626091
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000032----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-4', '2-8', '8-4']
***Trigger Reverse Engineering開始***
Target: 2, victim: 4, Loss: 1.6283, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:91.62, Cost:0.02 best_reg:92.03 avg_loss_reg:92.03:  12%|▏         | 122/1000 [02:00<14:30,  1.01it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 4 Trigger Size: 91.61526489257812 Optimization Steps: 96
***Symmetric Check開始***
Target: 4, victim: 2, Loss: 1.5548, Acc: 90.00%, CE_Loss: 0.49, Reg_Loss:1069.46, Cost:0.00 best_reg:1111.77 avg_loss_reg:1088.98: 100%|██████████| 96/96 [01:33<00:00,  1.03it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 227.4209806919098
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000033----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.049734830856323
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000034----------
***Pre-Screening開始***
```

```
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.609855651855469
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000035----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.713872909545898
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000036----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-8', '2-9', '3-4', '3-6', '4-7', '5-7', '6-7', '8-1', '8-10', '8-11', '9-2', '9-6', '10-1', '10-8', '10-14', '13-11', '14-0', '14-13', '15-14']
***Trigger Reverse Engineering開始***
Target: 15, victim: 14, Loss: 14.4300, Acc: 0.00%, CE_Loss: 14.43, Reg_Loss:2586.78, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2565.79:  25%|███       | 248/1000 [18:33<56:17,  4.49s/it]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 8 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1140.3475620746613
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000037----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['10-13', '14-4']
***Trigger Reverse Engineering開始***
Target: 14, victim: 4, Loss: 3.1206, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:120.69, Cost:0.03 best_reg:122.70 avg_loss_reg:122.70:  10%|▉         | 104/1000 [00:33<04:44,  3.14it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 4 Trigger Size: 120.689697265625 Optimization Steps: 84
***Symmetric Check開始***
Target: 4, victim: 14, Loss: 1.8288, Acc: 0.00%, CE_Loss: 1.83, Reg_Loss:17365.15, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:17288.30: 100%|██████████| 84/84 [00:26<00:00,  3.21it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 69.78644633293152
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000038----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 16.580349445343018
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000039----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '1-5', '8-5', '12-5']
***Trigger Reverse Engineering開始***
Target: 12, victim: 5, Loss: 10.9263, Acc: 0.00%, CE_Loss: 10.93, Reg_Loss:2546.80, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2534.95:   4%|▍         | 43/1000 [00:03<01:09, 13.70it/s]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 2 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 11.188262224197388
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000040----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 9, Loss: 0.2163, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:96.13, Cost:0.00 best_reg:116.95 avg_loss_reg:96.81:  10%|▉         | 104/1000 [09:36<1:22:45,  5.54s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 116.95089530944824 Optimization Steps: 105
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 586.1445779800415
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000041----------
```

```
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-20', '7-11', '8-1', '8-7', '8-11', '10-0', '10-19', '12-9', '13-1', '13-3', '13-19', '14-5', '14-9', '15-7', '17-19', '20-0']
***Trigger Reverse Engineering開始***
Target: 20, victim: 0, Loss: 1.2312, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:695.26, Cost:0.00 best_reg:697.03 avg_loss_reg:699.13:  60%|[redacted]  | 599/1000 [02:26<01:37,  4.09it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 20 Victim Class: 0 Trigger Size: 695.2594604492188 Optimization Steps: 279
***Symmetric Check開始***
Target: 0, victim: 20, Loss: 0.6636, Acc: 95.00%, CE_Loss: 0.27, Reg_Loss:1316.27, Cost:0.00 best_reg:1335.39 avg_loss_reg:1313.22: 100%|[redacted]| 279/279 [01:07<00:00,  4.13it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 226.33615922927856
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000042----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-9', '4-10', '11-10']
***Trigger Reverse Engineering開始***
Target: 4, victim: 10, Loss: 1.9583, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:33.41, Cost:0.06 best_reg:34.13 avg_loss_reg:34.13:  11%|[redacted]  | 110/1000 [06:21<51:27,  3.47s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 10 Trigger Size: 33.41248321533203 Optimization Steps: 69
***Symmetric Check開始***
Target: 10, victim: 4, Loss: 0.7188, Acc: 65.00%, CE_Loss: 0.72, Reg_Loss:12533.46, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:12407.27: 100%|[redacted]| 69/69 [03:53<00:00,  3.39s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 631.8594088554382
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000043----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.047940492630005
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000044----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-6']
***Trigger Reverse Engineering開始***
Target: 0, victim: 6, Loss: 2.0927, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:895.77, Cost:0.00 best_reg:898.52 avg_loss_reg:898.52:  25%|[redacted]  | 246/1000 [01:18<04:02,  3.11it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 6 Trigger Size: 895.7700805664062 Optimization Steps: 247
***Symmetric Check開始***
Target: 6, victim: 0, Loss: 0.4522, Acc: 95.00%, CE_Loss: 0.08, Reg_Loss:833.02, Cost:0.00 best_reg:844.83 avg_loss_reg:832.32: 100%|[redacted]| 247/247 [01:19<00:00,  3.10it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 165.35660219192505
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000045----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 17.712972164154053
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000046----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.463090419769287
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000047----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.469682455062866
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000048----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-7']
***Trigger Reverse Engineering開始***
Target: 5, victim: 7, Loss: 2.7606, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:101.61, Cost:0.03 best_reg:101.66 avg_loss_reg:101.66:  10%|          | 102/1000 [01:27<12:48,  1.17it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 7 Trigger Size: 101.61225128173828 Optimization Steps: 103
***Symmetric Check開始***
Target: 7, victim: 5, Loss: 2.2136, Acc: 80.00%, CE_Loss: 0.37, Reg_Loss:2766.08, Cost:0.00 best_reg:3081.28 avg_loss_reg:2768.00: 100%|██████████| 103/103 [01:27<00:00,  1.18it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 186.49200868606567
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000049----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-2', '6-1']
***Trigger Reverse Engineering開始***
Target: 6, victim: 1, Loss: 1.9192, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:106.27, Cost:0.02 best_reg:106.95 avg_loss_reg:106.95:  10%|          | 99/1000 [00:07<01:05, 13.74it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 1 Trigger Size: 106.26641845703125 Optimization Steps: 79
***Symmetric Check開始***
Target: 1, victim: 6, Loss: 1.6441, Acc: 40.00%, CE_Loss: 1.64, Reg_Loss:17481.23, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:17302.98: 100%|██████████| 79/79 [00:05<00:00, 13.43it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 19.07635188102722
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000050----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.913066864013672
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000051----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.256797313690186
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000052----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-4', '2-6']
***Trigger Reverse Engineering開始***
Target: 2, victim: 6, Loss: 1.5610, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:26.97, Cost:0.06 best_reg:27.69 avg_loss_reg:27.69:   9%|          | 89/1000 [00:21<03:41,  4.12it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 6 Trigger Size: 26.973079681396484 Optimization Steps: 79
***Symmetric Check開始***
Target: 6, victim: 2, Loss: 1.1480, Acc: 50.00%, CE_Loss: 1.15, Reg_Loss:16848.31, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:16727.95: 100%|██████████| 79/79 [00:19<00:00,  4.15it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 47.6233868598938
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000053----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 1
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 1, victim: 22, Loss: 1.4065, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:10502.64, Cost:0.00 best_reg:10413.47 avg_loss_reg:10432.45:  16%|          | 165/1000 [1:07:33<5:41:52, 24.57s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 10413.472778320312 Optimization Steps: 166
```

```
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 4068.8110830783844
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000054----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 14.109715700149536
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000055----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['14-12']
***Trigger Reverse Engineering開始***
Target: 14, victim: 12, Loss: 7.5283, Acc: 10.00%, CE_Loss: 7.53, Reg_Loss:2715.90, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2680.33:   2%|         | 20/1000 [00:02<02:06,  7.77it/s]
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 12 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 14.277221441268921
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000056----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-7', '1-8', '1-16', '2-11', '6-10', '7-8', '16-7']
***Trigger Reverse Engineering開始***
Target: 1, victim: 8, Loss: 2.2877, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:2028.92, Cost:0.00 best_reg:2031.48 avg_loss_reg:2031.48:  32%|[redacted]       | 325/1000 [00:39<01:22,  8.22it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 8 Trigger Size: 2028.91552734375 Optimization Steps: 239
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 47.49352955818176
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000057----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['10-1']
***Trigger Reverse Engineering開始***
Target: 10, victim: 1, Loss: 13.6979, Acc: 0.00%, CE_Loss: 13.70, Reg_Loss:2543.86, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2533.13:   1%|         | 10/1000 [00:01<02:33,  6.46it/s]
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 11.388310194015503
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000058----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['8-1', '11-15', '17-4', '18-1']
***Trigger Reverse Engineering開始***
Target: 18, victim: 1, Loss: 8.3917, Acc: 0.00%, CE_Loss: 8.39, Reg_Loss:2490.44, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2492.27:   6%|         | 63/1000 [00:15<03:53,  4.02it/s]
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 28.06581687927246
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000059----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 14.115655899047852
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000060----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-9', '6-1', '6-2', '6-9', '9-2']
***Trigger Reverse Engineering開始***
Target: 9, victim: 2, Loss: 9.5228, Acc: 10.00%, CE_Loss: 9.52, Reg_Loss:3092.37, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2998.41:   9%|         | 94/1000 [05:06<49:15,  3.26s/it]
```

```
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 9 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 324.40434288978577
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000061----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-12', '2-6', '3-12', '12-0', '12-3']
***Trigger Reverse Engineering開始***
Target: 12, victim: 3, Loss: 1.2220, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:227.29, Cost:0.01 best_reg:228.85 avg_loss_reg:230.24:  28%|███       | 276/1000 [00:34<01:30,  8.01it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 3 Trigger Size: 227.2919158935547 Optimization Steps: 178
***Symmetric Check開始***
Target: 3, victim: 12, Loss: 1.5988, Acc: 95.00%, CE_Loss: 0.30, Reg_Loss:578.02, Cost:0.00 best_reg:591.45 avg_loss_reg:574.87: 100%|██████████| 178/178 [00:22<00:00,  8.05it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 66.93280124664307
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000062----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '1-22', '2-1', '2-23', '3-14', '3-15', '3-23', '4-8', '5-8', '6-8', '10-8', '14-2', '15-3', '15-14', '17-15', '18-12', '21-15', '21-19', '21-22', '22-1']
***Trigger Reverse Engineering開始***
Target: 22, victim: 1, Loss: 1.3573, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:334.49, Cost:0.00 best_reg:334.99 avg_loss_reg:335.30:  46%|████▋     | 459/1000 [00:43<00:51, 10.57it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 22 Victim Class: 1 Trigger Size: 334.48626708984375 Optimization Steps: 163
***Symmetric Check開始***
Target: 1, victim: 22, Loss: 1.9003, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:728.96, Cost:0.00 best_reg:720.74 avg_loss_reg:726.78: 100%|██████████| 163/163 [00:15<00:00, 10.64it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 67.13302826881409
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000063----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-1', '5-3']
***Trigger Reverse Engineering開始***
Target: 5, victim: 3, Loss: 12.4081, Acc: 0.00%, CE_Loss: 12.41, Reg_Loss:2550.73, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2538.93:   2%|▏         | 21/1000 [00:02<01:48,  9.06it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 8.242540121078491
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000064----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 1
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 1, victim: 9, Loss: 0.3352, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:219.82, Cost:0.00 best_reg:216.37 avg_loss_reg:218.93:   8%|▊         | 81/1000 [13:35<2:34:12, 10.07s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 216.37274932861328 Optimization Steps: 82
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 824.5776777267456
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000065----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 17.090968132019043
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000066----------------------------------------
***Pre-Screening開始***
```

```
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['7-8']
***Trigger Reverse Engineering開始***
Target: 7, victim: 8, Loss: 7.2764, Acc: 0.00%, CE_Loss: 7.28, Reg_Loss:2550.48, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2537.07:   1%|         | 10/1000 [00:07<12:27,  1.33it/s]
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 8 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 17.749913692474365
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000067----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 1
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 1, victim: 16, Loss: 0.0364, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:888.93, Cost:0.00 best_reg:862.01 avg_loss_reg:894.71:   7%|▋         | 70/1000 [54:13<12:00:31, 46.49s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 862.007246537642 Optimization Steps: 71
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 3281.07292509079
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000068----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 0
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 0, victim: 3, Loss: 21.5826, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:561.41, Cost:0.04 best_reg:591.35 avg_loss_reg:591.35:  11%|█         | 114/1000 [11:06<1:26:21,  5.85s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 567.5093383789062 Optimization Steps: 115
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 678.1912469863892
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000069----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-15', '4-13', '15-3']
***Trigger Reverse Engineering開始***
Target: 4, victim: 13, Loss: 6.9052, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:174.77, Cost:0.04 best_reg:175.98 avg_loss_reg:175.98:  13%|█▎        | 133/1000 [00:16<01:47,  8.05it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 13 Trigger Size: 174.76739501953125 Optimization Steps: 101
***Symmetric Check開始***
Target: 13, victim: 4, Loss: 3.3441, Acc: 60.00%, CE_Loss: 1.06, Reg_Loss:5132.66, Cost:0.00 best_reg:11446.18 avg_loss_reg:5152.19: 100%|██████████| 101/101 [00:12<00:00,  8.18it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 37.879610776901245
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000070----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 14.030179500579834
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000071----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.382782459259033
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000072----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2']
```

```
***Trigger Reverse Engineering開始***
Target: 1, victim: 2, Loss: 7.2326, Acc: 10.00%, CE_Loss: 7.23, Reg_Loss:2849.44, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2790.99:   2%|          | 20/1000 [00:02<02:07,  7.69it/s]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 2 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 9.793334245681763
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000073----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.73539113998413
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000074----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 12, Loss: 0.1760, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:78.20, Cost:0.00 best_reg:77.17 avg_loss_reg:77.29:   5%|▌         | 50/1000 [01:47<34:09,  2.16s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 77.1730228000217 Optimization Steps: 51
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 116.48888731002808
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000075----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-3', '5-7']
***Trigger Reverse Engineering開始***
Target: 5, victim: 7, Loss: 3.2535, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:52.87, Cost:0.06 best_reg:52.89 avg_loss_reg:52.93:  10%|▉         | 95/1000 [00:09<01:26, 10.44it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 7 Trigger Size: 52.868919372558594 Optimization Steps: 87
***Symmetric Check開始***
Target: 7, victim: 5, Loss: 10.0595, Acc: 70.00%, CE_Loss: 0.73, Reg_Loss:13994.41, Cost:0.00 best_reg:19791.03 avg_loss_reg:14401.38: 100%|██████████| 87/87 [00:08<00:00, 10.49it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 23.511597156524658
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000076----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['8-9']
***Trigger Reverse Engineering開始***
Target: 8, victim: 9, Loss: 10.2534, Acc: 0.00%, CE_Loss: 10.25, Reg_Loss:2544.21, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2532.22:   1%|          | 10/1000 [00:03<05:21,  3.08it/s]
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 9 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 11.785981893539429
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000077----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.593531608581543
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000078----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.021196365356445
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000079----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
```

```
可能的 target-victim 配對: ['9-1', '21-1']
***Trigger Reverse Engineering開始***
Target: 21, victim: 1, Loss: 2.3981, Acc: 0.00%, CE_Loss: 2.40, Reg_Loss:3145.84, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2998.16:   3%|          | 31/1000 [01:48<56:29,  3.50s/it]
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 131.03706431388855
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000080----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-10', '13-10']
***Trigger Reverse Engineering開始***
Target: 13, victim: 10, Loss: 2.0125, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:114.49, Cost:0.02 best_reg:114.69 avg_loss_reg:114.69:   9%|▉         | 92/1000 [04:16<42:14,  2.79s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 10 Trigger Size: 114.49464416503906 Optimization Steps: 82
***Symmetric Check開始***
Target: 10, victim: 13, Loss: 2.9464, Acc: 90.00%, CE_Loss: 0.32, Reg_Loss:3940.23, Cost:0.00 best_reg:6668.54 avg_loss_reg:4001.40: 100%|██████████| 82/82 [03:46<00:00,  2.76s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 500.08529710769653
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000081----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 14.089277744293213
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000082----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 9, Loss: 0.1716, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:255.17, Cost:0.00 best_reg:5811.71 avg_loss_reg:318.77:   2%|▏         | 17/1000 [00:27<26:31,  1.62s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 5811.7144775390625 Optimization Steps: 18
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 34.564368724823
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000083----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-7']
***Trigger Reverse Engineering開始***
Target: 2, victim: 7, Loss: 2.8437, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:48.77, Cost:0.06 best_reg:50.43 avg_loss_reg:50.43:   7%|▋         | 72/1000 [00:07<01:39,  9.31it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 7 Trigger Size: 48.77121353149414 Optimization Steps: 73
***Symmetric Check開始***
Target: 7, victim: 2, Loss: 3.3430, Acc: 95.00%, CE_Loss: 0.38, Reg_Loss:2963.41, Cost:0.00 best_reg:4572.58 avg_loss_reg:3095.16: 100%|██████████| 73/73 [00:07<00:00,  9.71it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 22.688708543777466
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000084----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 0
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 0, victim: 6, Loss: 0.6189, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:171.54, Cost:0.00 best_reg:171.89 avg_loss_reg:171.05:  11%|█         | 106/1000 [14:49<2:04:58,  8.39s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 171.70403442382812 Optimization Steps: 107
```

```
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 897.533429145813
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000085----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '0-18', '0-19', '8-7', '8-16', '12-17', '19-18']
***Trigger Reverse Engineering開始***
Target: 8, victim: 16, Loss: 4.0465, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:346.96, Cost:0.01 best_reg:347.53 avg_loss_reg:347.53:  23%|██▎        | 233/1000 [13:03<42:57,  3.36s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 16 Trigger Size: 346.96417236328125 Optimization Steps: 98
***Symmetric Check開始***
Target: 16, victim: 8, Loss: 1.5069, Acc: 25.00%, CE_Loss: 1.51, Reg_Loss:16616.27, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:16525.87: 100%|██████████| 98/98 [05:15<00:00,  3.22s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1123.6005647182465
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000086----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 17.34115505218506
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000087----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.498942852020264
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000088----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '0-23', '3-4', '3-19', '9-4', '11-4', '11-19', '16-2', '17-3', '17-9', '18-4', '18-19', '19-4', '23-0']
***Trigger Reverse Engineering開始***
Target: 18, victim: 19, Loss: 0.9857, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:384.85, Cost:0.00 best_reg:384.91 avg_loss_reg:385.41:  39%|███▉       | 392/1000 [00:43<01:08,  8.92it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 18 Victim Class: 19 Trigger Size: 384.85443115234375 Optimization Steps: 151
***Symmetric Check開始***
Target: 19, victim: 18, Loss: 2.8095, Acc: 90.00%, CE_Loss: 0.55, Reg_Loss:1003.34, Cost:0.00 best_reg:1152.97 avg_loss_reg:1009.49: 100%|██████████| 151/151 [00:16<00:00,  9.08it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 73.36021900177002
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000089----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 9
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 9, victim: 19, Loss: 0.1386, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:264.28, Cost:0.00 best_reg:339.97 avg_loss_reg:265.44:   3%|▎          | 27/1000 [02:13<1:20:04,  4.94s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: all Trigger Size: 339.9654017857143 Optimization Steps: 28
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 142.23385548591614
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000090----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-0']
***Trigger Reverse Engineering開始***
Target: 1, victim: 0, Loss: 9.1544, Acc: 0.00%, CE_Loss: 9.15, Reg_Loss:2586.48, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2565.96:   1%|          | 10/1000 [00:01<02:12,  7.46it/s]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
```

```
檢測結果: Model是安全的(Benign)
整體耗時: 7.880602598190308
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000091----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.620845079421997
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000092----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-5']
***Trigger Reverse Engineering開始***
Target: 0, victim: 5, Loss: 12.8185, Acc: 0.00%, CE_Loss: 12.82, Reg_Loss:2546.30, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2534.92:   1%|          | 10/1000 [00:05<09:20,  1.77it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 13.490098476409912
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000093----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-6', '10-6', '11-13']
***Trigger Reverse Engineering開始***
Target: 11, victim: 13, Loss: 6.4381, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:246.54, Cost:0.03 best_reg:250.94 avg_loss_reg:243.85:  14%|▉          | 136/1000 [00:19<02:06,  6.83it/s]
  0%|          | 0/77 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 13 Trigger Size: 246.5424041748047 Optimization Steps: 77
***Symmetric Check開始***
Target: 13, victim: 11, Loss: 9.5785, Acc: 70.00%, CE_Loss: 0.79, Reg_Loss:8785.65, Cost:0.00 best_reg:12632.95 avg_loss_reg:9457.98: 100%|██████████| 77/77 [00:11<00:00,  6.64it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 38.07493352890015
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000094----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '2-9', '2-22', '3-15', '4-20', '5-11', '5-20', '6-3', '7-3', '8-2', '8-22', '9-19', '11-20', '12-20', '13-12', '13-20', '15-3', '15-11', '18-15', '18-5', '18-22', '20-5', '21-2', '21-8']
***Trigger Reverse Engineering開始***
Target: 3, victim: 15, Loss: 1.3984, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:856.57, Cost:0.00 best_reg:862.66 avg_loss_reg:862.66:  55%|█████▌    | 548/1000 [08:17<06:50,  1.10it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 15 Trigger Size: 856.5682373046875 Optimization Steps: 245
***Symmetric Check開始***
Target: 15, victim: 3, Loss: 1.0406, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:3950.15, Cost:0.00 best_reg:3827.92 avg_loss_reg:3965.08: 100%|██████████| 245/245 [04:21<00:00,  1.07s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 772.6253283023834
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000095----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-3', '2-4', '2-5']
***Trigger Reverse Engineering開始***
Target: 2, victim: 5, Loss: 11.3240, Acc: 0.00%, CE_Loss: 11.32, Reg_Loss:2581.18, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2561.07:   4%|▍          | 42/1000 [00:18<06:50,  2.33it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 3 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 22.240153551101685
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000096----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-3']
***Trigger Reverse Engineering開始***
Target: 2, victim: 3, Loss: 3.9951, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:149.60, Cost:0.03 best_reg:149.94 avg_loss_reg:149.94:  11%|▉          | 111/1000 [00:16<02:15,  6.55it/s]
```

```
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 3 Trigger Size: 149.59913635253906 Optimization Steps: 112
***Symmetric Check開始***
Target: 3, victim: 2, Loss: 1.3048, Acc: 70.00%, CE_Loss: 0.50, Reg_Loss:6105.99, Cost:0.00 best_reg:12299.64 avg_loss_reg:6139.63: 100%|[redacted]| 112/112 [00:17<00:00,  6.53it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 37.55736589431763
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000097----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 17.50396156311035
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000098----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-3', '1-7', '2-3', '2-6', '4-10', '7-1', '7-4', '7-12', '8-5', '8-6', '11-12']
***Trigger Reverse Engineering開始***
Target: 1, victim: 7, Loss: 1.8698, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:520.50, Cost:0.00 best_reg:524.70 avg_loss_reg:524.70:  43%|[redacted]| 430/1000 [00:55<01:13,  7.77it/s]
  0%|          | 0/185 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 7 Trigger Size: 520.50244140625 Optimization Steps: 185
***Symmetric Check開始***
Target: 7, victim: 1, Loss: 2.4374, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:451.53, Cost:0.01 best_reg:456.84 avg_loss_reg:456.84:  74%|[redacted]| 137/185 [00:17<00:06,  7.76it/s]
early stop 所有
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 79.86445927619934
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000099----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-7', '3-1']
***Trigger Reverse Engineering開始***
Target: 3, victim: 1, Loss: 8.7771, Acc: 5.00%, CE_Loss: 8.78, Reg_Loss:3219.60, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3078.77:   3%|[redacted]| 31/1000 [00:10<05:33,  2.91it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 7 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 18.66694450378418
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000100----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 20.267292261123657
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000101----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 4
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 4, victim: 17, Loss: 0.1802, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:270.06, Cost:0.00 best_reg:282.12 avg_loss_reg:277.22:   3%|[redacted]| 30/1000 [02:54<1:33:59,  5.81s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: all Trigger Size: 282.1248524983724 Optimization Steps: 31
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 185.93014001846313
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000102----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-1', '6-2']
***Trigger Reverse Engineering開始***
Target: 6, victim: 2, Loss: 2.0319, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:22.00, Cost:0.09 best_reg:23.01 avg_loss_reg:23.01:   8%|[redacted]| 76/1000 [00:38<07:48,  1.97it/s]
```

early stop 所有
Trigger Reverse Engineering結束
Target Class: 6 Victim Class: 2 Trigger Size: 22.000186920166016 Optimization Steps: 70
Symmetric Check開始
Target: 2, victim: 6, Loss: 0.4768, Acc: 80.00%, CE_Loss: 0.48, Reg_Loss:14025.84, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:13936.54: 100%|[redacted]| 70/70 [00:34<00:00, 2.01it/s]
Symmetric Check結束
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 77.21825766563416
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000103----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 7
可能的 victim classes: ALL
Trigger Reverse Engineering開始
Target: 7, victim: 19, Loss: 0.2759, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:77.38, Cost:0.00 best_reg:83.56 avg_loss_reg:77.14:   7%|[redacted]| 68/1000 [08:03<1:50:31, 7.11s/it]
early stop 所有
Trigger Reverse Engineering結束
Target Class: 7 Victim Class: all Trigger Size: 83.5587397984096 Optimization Steps: 69
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 494.19460344314575
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000104----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 13.409391403198242
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000105----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 17.283063650131226
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000106----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '2-1', '2-17', '3-13', '4-9', '10-3', '12-3', '12-16', '13-3', '17-1', '17-2']
Trigger Reverse Engineering開始
Target: 2, victim: 1, Loss: 0.7579, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:117.03, Cost:0.01 best_reg:117.45 avg_loss_reg:117.45: 51%|[redacted]| 508/1000 [00:39<00:37, 13.02it/s]
early stop 所有
Trigger Reverse Engineering結束
Target Class: 2 Victim Class: 1 Trigger Size: 117.02783203125 Optimization Steps: 187
Symmetric Check開始
Target: 1, victim: 2, Loss: 0.9814, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:233.92, Cost:0.00 best_reg:229.88 avg_loss_reg:230.70: 100%|[redacted]| 187/187 [00:13<00:00, 14.05it/s]
Symmetric Check結束
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 58.980252265930176
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000107----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-12', '1-0', '9-2', '12-0', '13-0']
Trigger Reverse Engineering開始
Target: 13, victim: 0, Loss: 0.8043, Acc: 100.00%, CE_Loss: 0.47, Reg_Loss:1137.55, Cost:0.00 best_reg:1105.72 avg_loss_reg:1135.88: 100%|[redacted]| 1000/1000 [03:40<00:00, 4.54it/s]
Trigger Reverse Engineering結束
Target Class: 13 Victim Class: 0 Trigger Size: 1105.718505859375 Optimization Steps: 956
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 229.24896478652954
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000108----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 9
可能的 victim classes: ALL
Trigger Reverse Engineering開始
Target: 9, victim: 14, Loss: 0.2802, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:280.18, Cost:0.00 best_reg:283.14 avg_loss_reg:279.21:   8%|[redacted]| 82/1000 [07:25<1:23:02, 5.43s/it]

```
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: all Trigger Size: 283.13702087402345 Optimization Steps: 83
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 455.85304403305054
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000109----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-8', '0-10', '2-7']
***Trigger Reverse Engineering開始***
Target: 0, victim: 8, Loss: 1.5482, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:283.75, Cost:0.01 best_reg:283.88 avg_loss_reg:284.07:  18%|██        | 183/1000 [00:38<02:53,  4.71it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 8 Trigger Size: 283.7460021972656 Optimization Steps: 139
***Symmetric Check開始***
Target: 8, victim: 0, Loss: 1.1270, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:1277.02, Cost:0.00 best_reg:1289.05 avg_loss_reg:1289.05: 100%|██████████| 139/139 [00:30<00:00,  4.63it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 76.43703031539917
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000110----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 3
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 3, victim: 12, Loss: 0.2555, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:75.68, Cost:0.00 best_reg:73.78 avg_loss_reg:75.26:   8%|▊         | 82/1000 [33:08<6:11:01, 24.25s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: all Trigger Size: 73.77916717529297 Optimization Steps: 83
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 2003.1719031333923
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000111----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.94533109664917
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000112----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '16-11']
***Trigger Reverse Engineering開始***
Target: 16, victim: 11, Loss: 5.8819, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:99.19, Cost:0.06 best_reg:99.62 avg_loss_reg:97.54:  13%|█▎        | 126/1000 [02:59<20:42,  1.42s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 16 Victim Class: 11 Trigger Size: 99.1943359375 Optimization Steps: 116
***Symmetric Check開始***
Target: 11, victim: 16, Loss: 1.2934, Acc: 90.00%, CE_Loss: 0.27, Reg_Loss:7774.00, Cost:0.00 best_reg:8254.67 avg_loss_reg:7815.20: 100%|██████████| 116/116 [02:42<00:00,  1.40s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 358.08257007598877
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000113----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 18.308409214019775
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000114----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '2-1', '4-2', '4-16', '14-3']
***Trigger Reverse Engineering開始***
Target: 1, victim: 2, Loss: 2.7199, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:757.11, Cost:0.00 best_reg:765.92 avg_loss_reg:765.92:  28%|██▊       | 282/1000 [03:08<07:59,  1.50it/s]
```

```
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 2 Trigger Size: 757.11474609375 Optimization Steps: 140
***Symmetric Check開始***
Target: 2, victim: 1, Loss: 2.5011, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:1010.18, Cost:0.00 best_reg:1012.91 avg_loss_reg:1012.91: 100%|██████████| 140/140 [01:41<00:00,  1.38it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 301.6820764541626
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000115----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 17.45164656639099
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000116----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 1
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 1, victim: 19, Loss: 1.6342, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:5515.40, Cost:0.00 best_reg:5533.82 avg_loss_reg:5706.35:  12%|▉         | 115/1000 [53:53<6:54:41, 28.11s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 5533.819266183035 Optimization Steps: 116
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 3248.550849914551
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000117----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-0', '2-3', '2-4']
***Trigger Reverse Engineering開始***
Target: 2, victim: 4, Loss: 10.8851, Acc: 0.00%, CE_Loss: 10.89, Reg_Loss:2546.01, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2534.08:   3%|▎         | 32/1000 [00:03<01:49,  8.81it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 13.00511121749878
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000118----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 25.40241551399231
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000119----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.926257133483887
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000120----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-8', '0-21', '1-7', '1-16', '2-11', '2-13', '2-16', '3-10', '6-19', '7-13', '7-16', '8-0', '8-19', '10-11', '10-16', '11-16', '11-13', '11-10', '12-14', '12-5', '12-4', '15-5', '15-21', '15-14', '16-10', '16-11', '17-5', '19-21', '20-13', '21-0', '21-5', '21-19']
***Trigger Reverse Engineering開始***
Target: 16, victim: 11, Loss: 0.8928, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:1051.67, Cost:0.00 best_reg:1069.50 avg_loss_reg:1041.51:  61%|██████    | 610/1000 [36:39<23:26,  3.61s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 16 Victim Class: 11 Trigger Size: 1051.6719970703125 Optimization Steps: 219
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 2226.367737531662
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000121----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-14', '6-2', '14-1']
```

```
***Trigger Reverse Engineering開始***
Target: 14, victim: 1, Loss: 5.3068, Acc: 10.00%, CE_Loss: 5.31, Reg_Loss:3549.48, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3309.52:   4%|▍         | 42/1000 [00:27<10:29,  1.52it/s]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 14 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 39.74085736274719
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000122----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 14, Loss: 0.5384, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:97.46, Cost:0.01 best_reg:97.95 avg_loss_reg:95.25:   9%|▊         | 86/1000 [07:19<1:17:54,  5.11s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 97.94744415283203 Optimization Steps: 87
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 449.74557733535767
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000123----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.765231847763062
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000124----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.506844997406006
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000125----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-3', '8-3']
***Trigger Reverse Engineering開始***
Target: 4, victim: 3, Loss: 4.3082, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:813.26, Cost:0.01 best_reg:814.77 avg_loss_reg:814.77:  19%|█▉        | 189/1000 [01:20<05:46,  2.34it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 3 Trigger Size: 813.263427734375 Optimization Steps: 179
***Symmetric Check開始***
Target: 3, victim: 4, Loss: 5.4069, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:2283.56, Cost:0.00 best_reg:2285.21 avg_loss_reg:2285.21:  94%|█████████▍| 168/179 [01:26<00:05,  1.95it/s]
early stop 所有
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 175.42600464820862
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000126----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-4', '2-4', '9-10', '10-0', '10-9']
***Trigger Reverse Engineering開始***
Target: 10, victim: 0, Loss: 2.1735, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:266.33, Cost:0.01 best_reg:268.43 avg_loss_reg:268.43:  26%|██▌       | 258/1000 [00:39<01:53,  6.56it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 0 Trigger Size: 266.32720947265625 Optimization Steps: 214
***Symmetric Check開始***
Target: 0, victim: 10, Loss: 1.4214, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:1727.01, Cost:0.00 best_reg:1700.06 avg_loss_reg:1723.15: 100%|██████████| 214/214 [00:30<00:00,  7.04it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 76.22197437286377
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000127----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-1', '11-21', '14-21', '15-21', '22-21']
```

```
***Trigger Reverse Engineering開始***
Target: 22, victim: 21, Loss: 10.5746, Acc: 0.00%, CE_Loss: 10.57, Reg_Loss:2523.19, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2517.02:   6%|▌         | 64/1000 [03:34<52:16,  3.35s/it]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 230.7379150390625
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000128----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '4-1', '5-1', '8-2', '8-5', '8-7', '9-7']
***Trigger Reverse Engineering開始***
Target: 8, victim: 2, Loss: 4.3483, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:244.42, Cost:0.02 best_reg:244.57 avg_loss_reg:245.15:  27%|██▋       | 271/1000 [00:29<01:19,  9.12it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 2 Trigger Size: 244.42417907714844 Optimization Steps: 121
***Symmetric Check開始***
Target: 2, victim: 8, Loss: 1.0276, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:3700.98, Cost:0.00 best_reg:3777.15 avg_loss_reg:3777.15: 100%|██████████| 121/121 [00:13<00:00,  8.80it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 49.69510793685913
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000129----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 17.729063034057617
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000130----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.131453275680542
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000131----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-15', '1-15', '8-13', '10-16', '13-8', '17-0', '17-16']
***Trigger Reverse Engineering開始***
Target: 1, victim: 15, Loss: 1.2195, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:1684.62, Cost:0.00 best_reg:1684.99 avg_loss_reg:1684.92:  50%|█████     | 501/1000 [21:41<21:36,  2.60s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 15 Trigger Size: 1684.616455078125 Optimization Steps: 405
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1317.3795902729034
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000132----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-19', '8-4', '12-1', '18-19']
***Trigger Reverse Engineering開始***
Target: 18, victim: 19, Loss: 11.2953, Acc: 0.00%, CE_Loss: 11.30, Reg_Loss:2563.41, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2548.16:   5%|▌         | 53/1000 [00:09<02:43,  5.77it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 19 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 16.73827886581421
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000133----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.230655193328857
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000134----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
```

```
整體耗時: 11.668393850326538
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000135----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-4', '5-1', '9-7']
***Trigger Reverse Engineering開始***
Target: 5, victim: 1, Loss: 1.6850, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:1508.55, Cost:0.00 best_reg:1508.78 avg_loss_reg:1510.42:  29%|[redacted]      | 290/1000 [00:33<01:21,  8.73it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 1 Trigger Size: 1508.553955078125 Optimization Steps: 258
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 40.61774826049805
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000136----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.451930999755859
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000137----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-13', '3-2', '3-13', '4-8', '5-4', '5-8', '5-13', '6-8', '10-4', '12-3']
***Trigger Reverse Engineering開始***
Target: 3, victim: 2, Loss: 1.8443, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:223.28, Cost:0.01 best_reg:223.78 avg_loss_reg:223.60:  35%|[redacted]      | 349/1000 [06:24<11:57,  1.10s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 2 Trigger Size: 223.28207397460938 Optimization Steps: 177
***Symmetric Check開始***
Target: 2, victim: 3, Loss: 0.0896, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:4697.78, Cost:0.00 best_reg:4744.28 avg_loss_reg:4761.69: 100%|[redacted]| 177/177 [03:16<00:00,  1.11s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 589.9502079486847
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000138----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-10']
***Trigger Reverse Engineering開始***
Target: 4, victim: 10, Loss: 2.6461, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:719.37, Cost:0.00 best_reg:726.31 avg_loss_reg:719.76:  14%|[redacted]        | 142/1000 [01:00<06:04,  2.35it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 10 Trigger Size: 719.365234375 Optimization Steps: 143
***Symmetric Check開始***
Target: 10, victim: 4, Loss: 3.7186, Acc: 90.00%, CE_Loss: 0.26, Reg_Loss:5187.67, Cost:0.00 best_reg:5232.50 avg_loss_reg:5232.50: 100%|[redacted]| 143/143 [01:02<00:00,  2.30it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 130.94886660575867
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000139----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 2.6243269443511963
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000140----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-0', '10-0', '13-3', '16-0']
***Trigger Reverse Engineering開始***
Target: 16, victim: 0, Loss: 8.1876, Acc: 0.00%, CE_Loss: 8.19, Reg_Loss:3158.33, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3017.95:   5%|[redacted]        | 53/1000 [04:17<1:16:46,  4.86s/it]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 287.01466703414917
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000141----------------------------------------
```

```
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-20', '4-17', '19-12']
***Trigger Reverse Engineering開始***
Target: 19, victim: 12, Loss: 3.7116, Acc: 100.00%, CE_Loss: 0.40, Reg_Loss:193.74, Cost:0.02 best_reg:194.30 avg_loss_reg:194.98:  19%|██        | 194/1000 [13:04<54:17,  4.04s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 19 Victim Class: 12 Trigger Size: 193.73573303222656 Optimization Steps: 163
***Symmetric Check開始***
Target: 12, victim: 19, Loss: 1.5044, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:6376.17, Cost:0.00 best_reg:6496.78 avg_loss_reg:6496.78: 100%|██████████| 163/163 [10:49<00:00,  3.99s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1456.4605922698975
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000142----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-3', '2-1', '2-4', '2-9', '3-0', '6-5', '6-16', '8-1', '8-5', '9-5', '10-5', '11-4', '17-0']
***Trigger Reverse Engineering開始***
Target: 2, victim: 1, Loss: 2.1220, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:4378.35, Cost:0.00 best_reg:4382.39 avg_loss_reg:4424.00:  60%|██████    | 597/1000 [30:17<20:26,  3.04s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 4378.3525390625 Optimization Steps: 425
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1844.2108731269836
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000143----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-5', '1-3', '7-6']
***Trigger Reverse Engineering開始***
Target: 1, victim: 3, Loss: 3.5995, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:1479.17, Cost:0.00 best_reg:1479.24 avg_loss_reg:1479.24:  24%|██        | 237/1000 [01:29<04:49,  2.63it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 3 Trigger Size: 1479.166748046875 Optimization Steps: 205
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 97.24881386756897
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000144----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 2.788980722427368
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000145----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.539626121520996
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000146----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.664697885513306
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000147----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 19.98484516143799
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000148----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-18', '7-10', '11-16', '15-16', '17-16']
***Trigger Reverse Engineering開始***
```

```
Target: 17, victim: 16, Loss: 9.7743, Acc: 0.00%, CE_Loss: 9.77, Reg_Loss:2534.12, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2521.15:   7%|▋         | 74/1000 [05:44<1:11:51,  4.66s/it]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 18 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 373.0696756839752
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000149----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.46427845954895
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000150----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.986953973770142
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000151----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 2.916640043258667
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000152----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.358924388885498
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000153----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 19
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 19, victim: 22, Loss: 0.4862, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:1641.07, Cost:0.00 best_reg:1636.47 avg_loss_reg:1614.44:   6%|▌         | 62/1000 [09:27<2:23:09,  9.16s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 19 Victim Class: all Trigger Size: 1636.4735026041667 Optimization Steps: 63
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 580.8192658424377
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000154----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 3.025019407272339
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000155----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.072980403900146
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000156----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-12', '2-5', '4-8', '4-10', '6-10', '10-6']
***Trigger Reverse Engineering開始***
Target: 10, victim: 6, Loss: 7.3118, Acc: 20.00%, CE_Loss: 7.31, Reg_Loss:2981.55, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2887.85:  10%|▉         | 95/1000 [00:10<01:38,  9.21it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 12 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 18.1731595993042
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000157----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
```

```
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.449477434158325
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000158----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-0']
***Trigger Reverse Engineering開始***
Target: 4, victim: 0, Loss: 10.9118, Acc: 0.00%, CE_Loss: 10.91, Reg_Loss:2565.98, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2547.86:   1%|          | 10/1000 [00:04<07:55,  2.08it/s]
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 12.471770286560059
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000159----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['8-5']
***Trigger Reverse Engineering開始***
Target: 8, victim: 5, Loss: 1.4055, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:54.59, Cost:0.03 best_reg:56.84 avg_loss_reg:56.84:  10%|▉         | 102/1000 [05:05<44:53,  3.00s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 5 Trigger Size: 54.58509826660156 Optimization Steps: 103
***Symmetric Check開始***
Target: 5, victim: 8, Loss: 0.8852, Acc: 100.00%, CE_Loss: 0.75, Reg_Loss:3463.38, Cost:0.00 best_reg:3247.45 avg_loss_reg:3441.00: 100%|██████████| 103/103 [05:12<00:00,  3.03s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 635.8410024642944
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000160----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-12', '7-4']
***Trigger Reverse Engineering開始***
Target: 7, victim: 4, Loss: 9.6687, Acc: 5.00%, CE_Loss: 9.67, Reg_Loss:4071.68, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3698.69:   3%|▎         | 31/1000 [00:09<04:56,  3.27it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 12 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 19.996350288391113
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000161----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.556492328643799
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000162----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.457389116287231
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000163----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-10', '7-6', '10-2']
***Trigger Reverse Engineering開始***
Target: 0, victim: 10, Loss: 4.4090, Acc: 100.00%, CE_Loss: 0.34, Reg_Loss:804.56, Cost:0.01 best_reg:806.51 avg_loss_reg:806.51:  17%|▋         | 169/1000 [09:58<49:03,  3.54s/it]
  0%|          | 0/138 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 10 Trigger Size: 804.5567626953125 Optimization Steps: 138
***Symmetric Check開始***
Target: 10, victim: 0, Loss: 3.4626, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:655.82, Cost:0.01 best_reg:657.53 avg_loss_reg:657.53: 100%|██████████| 138/138 [08:05<00:00,  3.52s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1099.481012582779
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000164----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 18
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 18, victim: 22, Loss: 0.3491, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:784.08, Cost:0.00 best_reg:777.31 avg_loss_reg:769.15:  16%|          | 160/1000 [42:20<3:42:17, 15.88s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 18 Victim Class: all Trigger Size: 777.3056869506836 Optimization Steps: 161
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 2552.3722443580627
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000165----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['9-4']
***Trigger Reverse Engineering開始***
Target: 9, victim: 4, Loss: 9.1343, Acc: 0.00%, CE_Loss: 9.13, Reg_Loss:2595.83, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2574.84:   1%|          | 10/1000 [00:02<04:25,  3.73it/s]
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 10.258039712905884
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000166----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.502660512924194
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000167----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.112302780151367
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000168----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.316439151763916
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000169----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.106948614120483
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000170----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-0']
***Trigger Reverse Engineering開始***
Target: 2, victim: 0, Loss: 0.7838, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:916.85, Cost:0.00 best_reg:919.26 avg_loss_reg:920.08:  38%|███▊      | 377/1000 [03:58<06:33,  1.58it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 0 Trigger Size: 916.8477783203125 Optimization Steps: 378
***Symmetric Check開始***
Target: 0, victim: 2, Loss: 1.5438, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:6714.46, Cost:0.00 best_reg:6733.06 avg_loss_reg:6702.65: 100%|██████████| 378/378 [03:58<00:00,  1.58it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 484.760906457901
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000171----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
```

```
整體耗時: 9.399004220962524
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000172----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.118836164474487
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000173----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 3.993023157119751
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000174----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.443248748779297
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000175----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.17429494857788
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000176----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.700076580047607
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000177----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 5
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 5, victim: 6, Loss: 0.1988, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:670.80, Cost:0.00 best_reg:664.12 avg_loss_reg:669.98:  13%|▉         | 133/1000 [33:56<3:41:18, 15.31s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: all Trigger Size: 664.12333984375 Optimization Steps: 134
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 2049.607510328293
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000178----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 2.6641976833343506
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000179----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 16.523897886276245
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000180----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '0-2', '6-5']
***Trigger Reverse Engineering開始***
Target: 0, victim: 2, Loss: 2.4812, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:690.61, Cost:0.00 best_reg:695.37 avg_loss_reg:695.37:  25%|██▌       | 251/1000 [14:18<42:41,  3.42s/it]
  0%|          | 0/178 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 2 Trigger Size: 690.60888671875 Optimization Steps: 178
***Symmetric Check開始***
Target: 2, victim: 0, Loss: 0.8426, Acc: 60.00%, CE_Loss: 0.84, Reg_Loss:14700.95, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:14688.43: 100%|██████████| 178/178 [10:06<00:00,  3.41s/it]
***Symmetric Check結束***
**********檢測結束**********
```

```
檢測結果: Model含有後門(Abnormal)
整體耗時: 1477.6634047031403
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000181----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-5', '2-14', '4-7', '5-14', '10-7', '15-14']
***Trigger Reverse Engineering開始***
Target: 2, victim: 14, Loss: 2.0464, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:33.64, Cost:0.06 best_reg:35.25 avg_loss_reg:33.22:  15%|▉         | 148/1000 [04:46<27:28,  1.93s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 14 Trigger Size: 33.63653564453125 Optimization Steps: 69
***Symmetric Check開始***
Target: 14, victim: 2, Loss: 7.8493, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:7527.38, Cost:0.00 best_reg:8052.60 avg_loss_reg:8144.33: 100%|██████████| 69/69 [02:12<00:00,  1.92s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 434.2893204689026
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000182----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 18.230083465576172
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000183----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-17', '1-12', '1-20', '1-21', '2-0', '2-1', '2-10', '3-2', '4-5', '4-9', '4-12', '5-12', '6-8', '6-11', '6-12', '7-18', '8-6', '8-9', '8-11', '9-8', '9-11', '11-8', '11-19', '13-10', '17-0', '18-1', '18-7', '19-2', '20-21', '21-1', '21-12', '21-11']
***Trigger Reverse Engineering開始***
Target: 21, victim: 11, Loss: 2.2823, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:425.56, Cost:0.01 best_reg:427.07 avg_loss_reg:427.07:  68%|██████▊   | 677/1000 [36:52<17:35,  3.27s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 21 Victim Class: 11 Trigger Size: 425.5569763183594 Optimization Steps: 156
***Symmetric Check開始***
Target: 11, victim: 21, Loss: 0.9748, Acc: 70.00%, CE_Loss: 0.97, Reg_Loss:22108.08, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:22042.08: 100%|██████████| 156/156 [08:34<00:00,  3.30s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 2747.7031893730164
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000184----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.955691814422607
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000185----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.551476240158081
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000186----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.198354005813599
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000187----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-20', '3-8', '3-6', '3-15', '4-13', '4-20', '6-3', '8-6', '9-3', '9-6', '9-11', '10-11', '10-12', '11-3', '11-8', '11-12', '13-1', '14-13', '15-3', '15-6', '16-13', '16-20', '20-1']
***Trigger Reverse Engineering開始***
Target: 20, victim: 1, Loss: 1.0046, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:737.39, Cost:0.00 best_reg:740.88 avg_loss_reg:740.88:  54%|█████▍    | 541/1000 [01:10<00:59,  7.70it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 20 Victim Class: 1 Trigger Size: 737.390625 Optimization Steps: 178
***Symmetric Check開始***
Target: 1, victim: 20, Loss: 0.9989, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:317.94, Cost:0.00 best_reg:310.50 avg_loss_reg:318.45: 100%|██████████| 178/178 [00:26<00:00,  6.74it/s]
***Symmetric Check結束***
```

```
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 104.32757019996643
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000188----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-7', '1-3', '2-1', '2-9', '4-5', '4-12', '5-4', '5-12', '7-0', '9-1', '9-3', '9-6', '13-14', '15-14']
***Trigger Reverse Engineering開始***
Target: 13, victim: 14, Loss: 1.2788, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:1096.02, Cost:0.00 best_reg:1096.28 avg_loss_reg:1082.27:  72%|[redacted]  | 723/1000 [23:35<09:02,  1.96s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 14 Trigger Size: 1096.019775390625 Optimization Steps: 526
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1430.7862091064453
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000189----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-3', '0-18']
***Trigger Reverse Engineering開始***
Target: 0, victim: 18, Loss: 1.7949, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:13.74, Cost:0.13 best_reg:15.65 avg_loss_reg:15.65:  10%|[redacted]  | 97/1000 [00:18<02:56,  5.12it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 18 Trigger Size: 13.73945426940918 Optimization Steps: 77
***Symmetric Check開始***
Target: 18, victim: 0, Loss: 5.0626, Acc: 90.00%, CE_Loss: 0.26, Reg_Loss:4806.15, Cost:0.00 best_reg:7334.80 avg_loss_reg:5236.66: 100%|[redacted]| 77/77 [00:15<00:00,  5.04it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 48.667075634002686
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000190----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-9', '7-8', '8-10', '10-8']
***Trigger Reverse Engineering開始***
Target: 10, victim: 8, Loss: 2.3022, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:82.88, Cost:0.03 best_reg:83.56 avg_loss_reg:82.70:  17%|[redacted]  | 167/1000 [09:26<47:04,  3.39s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 8 Trigger Size: 82.87805938720703 Optimization Steps: 125
***Symmetric Check開始***
Target: 8, victim: 10, Loss: 4.7076, Acc: 75.00%, CE_Loss: 0.62, Reg_Loss:9203.32, Cost:0.00 best_reg:16200.26 avg_loss_reg:9537.62: 100%|[redacted]| 125/125 [06:54<00:00,  3.31s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1000.4495198726654
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000191----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '0-6', '0-15', '1-15', '2-17', '3-2', '3-5', '5-17', '6-1', '6-4', '6-19', '7-14', '7-19', '8-6', '10-4', '10-13', '11-10', '11-15', '12-13', '12-17', '13-10', '16-0', '16-9', '16-18', '17-12', '17-1', '17-2', '18-6', '19-4', '20-12', '20-13', '21-4', '21-19', '22-1', '22-4', '22-6']
***Trigger Reverse Engineering開始***
Target: 7, victim: 14, Loss: 2.8302, Acc: 100.00%, CE_Loss: 0.43, Reg_Loss:711.31, Cost:0.00 best_reg:711.46 avg_loss_reg:708.78:  65%|[redacted]  | 650/1000 [10:15<05:31,  1.06it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 14 Trigger Size: 711.3124389648438 Optimization Steps: 235
***Symmetric Check開始***
Target: 14, victim: 7, Loss: 2.3942, Acc: 100.00%, CE_Loss: 0.39, Reg_Loss:4502.24, Cost:0.00 best_reg:4448.60 avg_loss_reg:4500.33: 100%|[redacted]| 235/235 [03:11<00:00,  1.23it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 821.4709134101868
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000192----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-13', '2-1', '3-0', '3-2', '4-13', '5-0', '5-4', '5-10', '6-11', '6-12', '7-5', '7-10', '8-0', '8-10', '9-12', '9-13', '10-7', '11-6', '11-12', '12-6', '12-11', '13-1']
***Trigger Reverse Engineering開始***
Target: 13, victim: 1, Loss: 1.9356, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:747.32, Cost:0.00 best_reg:747.93 avg_loss_reg:747.93:  63%|[redacted]  | 633/1000 [02:08<01:14,  4.94it/s]
```

```
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 1 Trigger Size: 747.3206787109375 Optimization Steps: 383
***Symmetric Check開始***
Target: 1, victim: 13, Loss: 2.0207, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:3836.43, Cost:0.00 best_reg:3832.30 avg_loss_reg:3865.17: 100%|██████████| 383/383 [01:16<00:00,  5.02it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 212.6898331642151
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000193----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 20.411783695220947
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000194----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 14.62452483177185
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000195----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 7
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 7, victim: 6, Loss: 1.6562, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:3674.95, Cost:0.00 best_reg:3665.24 avg_loss_reg:3666.75:  16%|██        | 155/1000 [04:21<23:45,  1.69s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: all Trigger Size: 3664.0279134114585 Optimization Steps: 156
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 265.77352237701416
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000196----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-11', '0-13', '11-0', '11-5', '11-13', '13-12']
***Trigger Reverse Engineering開始***
Target: 13, victim: 12, Loss: 3.4855, Acc: 25.00%, CE_Loss: 3.49, Reg_Loss:3068.03, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2970.85:   8%|▊         | 75/1000 [03:39<45:11,  2.93s/it]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 11 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 240.72338366508484
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000197----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.923811912536621
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000198----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 1
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 1, victim: 16, Loss: 4.2168, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:1249.43, Cost:0.00 best_reg:1249.23 avg_loss_reg:1249.23:  14%|█▍        | 135/1000 [1:16:19<8:09:05, 33.92s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 1248.2555042613637 Optimization Steps: 136
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 4593.790768146515
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000199----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
```

```
可能的 target class: 4
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 4, victim: 12, Loss: 0.6873, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:305.28, Cost:0.00 best_reg:306.10 avg_loss_reg:303.25:  14%|▉         | 143/1000 [49:22<4:55:52, 20.71s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: all Trigger Size: 306.10232883029516 Optimization Steps: 144
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 2974.5973365306854
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000200----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['19-0']
***Trigger Reverse Engineering開始***
Target: 19, victim: 0, Loss: 0.4071, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:1174.83, Cost:0.00 best_reg:1175.85 avg_loss_reg:1177.57:  22%|██        | 215/1000 [13:28<49:13,  3.76s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 19 Victim Class: 0 Trigger Size: 1174.829833984375 Optimization Steps: 216
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 835.3701615333557
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000201----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 19.869332790374756
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000202----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-7', '2-9', '5-9']
***Trigger Reverse Engineering開始***
Target: 2, victim: 7, Loss: 4.5071, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:828.98, Cost:0.01 best_reg:832.61 avg_loss_reg:833.69:  24%|██        | 241/1000 [04:38<14:36,  1.15s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 7 Trigger Size: 828.98046875 Optimization Steps: 200
***Symmetric Check開始***
Target: 7, victim: 2, Loss: 8.1691, Acc: 90.00%, CE_Loss: 0.64, Reg_Loss:2230.39, Cost:0.00 best_reg:2239.86 avg_loss_reg:2232.29: 100%|██████████| 200/200 [03:35<00:00,  1.08s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 504.65786504745483
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000203----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 17.48613667488098
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000204----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['17-9']
***Trigger Reverse Engineering開始***
Target: 17, victim: 9, Loss: 5.9559, Acc: 10.00%, CE_Loss: 5.96, Reg_Loss:3294.17, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3048.43:   2%|▏         | 20/1000 [01:06<54:08,  3.31s/it]
***Trigger Reverse Engineering結束***
Target Class: 17 Victim Class: 9 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 81.09473729133606
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000205----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 9
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 9, victim: 9, Loss: 0.4088, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:35.54, Cost:0.01 best_reg:35.57 avg_loss_reg:35.10:   5%|▌         | 53/1000 [01:21<24:23,  1.55s/it]
```

early stop 所有
Trigger Reverse Engineering結束
Target Class: 9 Victim Class: all Trigger Size: 35.573119163513184 Optimization Steps: 54
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 88.10036444664001
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000206----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-2', '0-15', '2-8', '2-12', '3-17', '4-14', '5-12', '6-12', '8-2', '9-2', '10-3', '11-0', '11-17', '13-3', '13-10', '13-17', '16-3']
Trigger Reverse Engineering開始
Target: 4, victim: 14, Loss: 2.4853, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:1518.05, Cost:0.00 best_reg:1520.34 avg_loss_reg:1522.93: 52%|[redacted]| 519/1000 [04:49<04:27, 1.80it/s]
early stop 所有
Trigger Reverse Engineering結束
Target Class: 4 Victim Class: 14 Trigger Size: 1518.04931640625 Optimization Steps: 343
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 299.2864797115326
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000207----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['7-3']
Trigger Reverse Engineering開始
Target: 7, victim: 3, Loss: 6.1714, Acc: 5.00%, CE_Loss: 6.17, Reg_Loss:2977.46, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2889.50:   2%|[redacted]| 20/1000 [01:04<52:30, 3.21s/it]
Trigger Reverse Engineering結束
Target Class: 7 Victim Class: 3 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 79.0871148109436
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000208----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 14.67023491859436
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000209----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 6.318421840667725
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000210----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 8.353721618652344
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000211----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 18.184931755065918
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000212----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-3', '4-5']
Trigger Reverse Engineering開始
Target: 1, victim: 3, Loss: 2.2081, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:899.46, Cost:0.00 best_reg:906.49 avg_loss_reg:906.49: 22%|[redacted]| 215/1000 [00:18<01:05, 11.90it/s]
  0%| | 0/205 [00:00<?, ?it/s]early stop 所有
Trigger Reverse Engineering結束
Target Class: 1 Victim Class: 3 Trigger Size: 899.4613037109375 Optimization Steps: 205
Symmetric Check開始
Target: 3, victim: 1, Loss: 4.6158, Acc: 80.00%, CE_Loss: 0.49, Reg_Loss:2753.29, Cost:0.00 best_reg:2788.24 avg_loss_reg:2755.98: 100%|[redacted]| 205/205 [00:16<00:00, 12.33it/s]
Symmetric Check結束
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 37.454235792160034

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000213----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['9-4']
***Trigger Reverse Engineering開始***
Target: 9, victim: 4, Loss: 4.7633, Acc: 20.00%, CE_Loss: 4.76, Reg_Loss:3176.36, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2993.18:   2%|          | 20/1000 [00:52<42:52,  2.62s/it]
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 66.2883768081665
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000214----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.622028589248657
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000215----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 16.186407804489136
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000216----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.229387998580933
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000217----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.2376015186309814
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000218----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 2.434854507446289
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000219----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-0']
***Trigger Reverse Engineering開始***
Target: 6, victim: 0, Loss: 6.9811, Acc: 0.00%, CE_Loss: 6.98, Reg_Loss:2589.08, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2567.88:   1%|          | 10/1000 [00:35<59:10,  3.59s/it]
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 50.39560651779175
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000220----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.060251951217651
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000221----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 21.524623155593872
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000222----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
```

```
整體耗時: 10.246219158172607
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000223----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['9-5', '13-6']
***Trigger Reverse Engineering開始***
Target: 13, victim: 6, Loss: 9.3001, Acc: 0.00%, CE_Loss: 9.30, Reg_Loss:2572.66, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2558.02:   2%|▏          | 21/1000 [00:23<18:09,  1.11s/it]
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 32.411505937576294
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000224----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-12', '11-12']
***Trigger Reverse Engineering開始***
Target: 11, victim: 12, Loss: 13.3322, Acc: 0.00%, CE_Loss: 13.33, Reg_Loss:2513.85, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2509.87:   2%|▏          | 21/1000 [00:02<02:08,  7.64it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 12 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 9.7119460105896
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000225----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.680684328079224
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000226----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.77011227607727
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000227----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.14785099029541
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000228----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-0']
***Trigger Reverse Engineering開始***
Target: 2, victim: 0, Loss: 4.6806, Acc: 0.00%, CE_Loss: 4.68, Reg_Loss:2531.97, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2521.27:   1%|          | 10/1000 [00:33<56:03,  3.40s/it]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 42.158549308776855
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000229----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 16.701091766357422
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000230----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-5']
***Trigger Reverse Engineering開始***
Target: 4, victim: 5, Loss: 5.7675, Acc: 20.00%, CE_Loss: 5.77, Reg_Loss:3354.54, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3172.22:   2%|▏          | 20/1000 [00:02<01:48,  9.05it/s]
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
```

```
檢測結果: Model是安全的(Benign)
整體耗時: 10.612811803817749
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000231----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 2.4224913120269775
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000232----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.676013708114624
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000233----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.888827085494995
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000234----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-11']
***Trigger Reverse Engineering開始***
Target: 6, victim: 11, Loss: 2.2984, Acc: 100.00%, CE_Loss: 0.33, Reg_Loss:873.91, Cost:0.00 best_reg:874.07 avg_loss_reg:870.95:  29%|███       | 294/1000 [10:34<25:22,  2.16s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 11 Trigger Size: 873.9107666015625 Optimization Steps: 295
***Symmetric Check開始***
Target: 11, victim: 6, Loss: 2.1714, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:6579.38, Cost:0.00 best_reg:6557.29 avg_loss_reg:6584.63: 100%|██████████| 295/295 [10:34<00:00,  2.15s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1278.9124207496643
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000235----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 14.617265939712524
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000236----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-5', '1-6', '6-1']
***Trigger Reverse Engineering開始***
Target: 1, victim: 6, Loss: 4.2543, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:108.79, Cost:0.04 best_reg:109.89 avg_loss_reg:109.89:  13%|▏         | 132/1000 [06:39<43:47,  3.03s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 6 Trigger Size: 108.79255676269531 Optimization Steps: 77
***Symmetric Check開始***
Target: 6, victim: 1, Loss: 0.3218, Acc: 90.00%, CE_Loss: 0.32, Reg_Loss:10620.24, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:10516.87: 100%|██████████| 77/77 [03:51<00:00,  3.00s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 640.2766888141632
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000237----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-13', '11-5', '13-3']
***Trigger Reverse Engineering開始***
Target: 13, victim: 3, Loss: 7.8710, Acc: 15.00%, CE_Loss: 7.87, Reg_Loss:3437.10, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3234.26:   6%|▌         | 62/1000 [00:39<09:51,  1.59it/s]
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 13 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 49.253036975860596
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000238----------
```

```
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-6', '3-11', '6-20', '10-19', '10-21', '10-8', '17-16', '17-20', '19-20', '20-6', '20-19']
***Trigger Reverse Engineering開始***
Target: 17, victim: 20, Loss: 1.5537, Acc: 100.00%, CE_Loss: 0.38, Reg_Loss:1170.23, Cost:0.00 best_reg:1163.46 avg_loss_reg:1178.88: 100%|| 1000/1000 [47:57<00:00,  2.88s/it]
***Trigger Reverse Engineering結束***
Target Class: 17 Victim Class: 20 Trigger Size: 1163.456298828125 Optimization Steps: 661
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 2903.5240228176117
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000239----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '1-23', '5-23', '14-23', '22-23']
***Trigger Reverse Engineering開始***
Target: 5, victim: 23, Loss: 2.0553, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:34.07, Cost:0.06 best_reg:35.86 avg_loss_reg:34.49:  19%|        | 193/1000 [00:50<03:30,  3.83it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 23 Trigger Size: 34.07093048095703 Optimization Steps: 80
***Symmetric Check開始***
Target: 23, victim: 5, Loss: 0.8172, Acc: 40.00%, CE_Loss: 0.82, Reg_Loss:13663.40, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:13562.97: 100%|| 80/80 [00:20<00:00,  3.86it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 82.85792303085327
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000240----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.328764200210571
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000241----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-9', '2-3', '2-9', '8-3', '8-9', '14-3', '15-9']
***Trigger Reverse Engineering開始***
Target: 2, victim: 9, Loss: 0.9825, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:226.58, Cost:0.00 best_reg:226.96 avg_loss_reg:226.96:  24%|        | 239/1000 [00:16<00:53, 14.12it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 9 Trigger Size: 226.57591247558594 Optimization Steps: 153
***Symmetric Check開始***
Target: 9, victim: 2, Loss: 2.3870, Acc: 100.00%, CE_Loss: 0.50, Reg_Loss:1886.10, Cost:0.00 best_reg:1894.00 avg_loss_reg:1894.00: 100%|| 153/153 [00:10<00:00, 14.58it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 34.32163858413696
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000242----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 3.92148494720459
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000243----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.76967191696167
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000244----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['7-0', '14-0', '16-0']
***Trigger Reverse Engineering開始***
Target: 16, victim: 0, Loss: 12.3398, Acc: 0.00%, CE_Loss: 12.34, Reg_Loss:2546.67, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2533.22:   3%|         | 32/1000 [00:37<18:48,  1.17s/it]
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
```

```
檢測結果: Model是安全的(Benign)
整體耗時: 50.18550157546997
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000245----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-8', '1-3', '1-4', '1-5', '5-3', '8-0', '10-4']
***Trigger Reverse Engineering開始***
Target: 10, victim: 4, Loss: 8.6155, Acc: 15.00%, CE_Loss: 8.62, Reg_Loss:3579.00, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3339.31:  12%|          | 116/1000 [00:16<02:05,  7.06it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 8 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 25.71719741821289
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000246----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.339779138565063
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000247----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 7
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 7, victim: 12, Loss: 0.1830, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:76.55, Cost:0.00 best_reg:80.21 avg_loss_reg:75.58:   6%|          | 57/1000 [21:18<5:52:27, 22.43s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: all Trigger Size: 80.21017150878906 Optimization Steps: 58
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1289.224137544632
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000248----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.279832363128662
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000249----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-0', '1-4', '1-22', '2-3', '4-15', '6-11', '10-0', '10-5', '13-4', '15-4', '17-15', '18-0', '21-1', '21-4', '22-1']
***Trigger Reverse Engineering開始***
Target: 13, victim: 4, Loss: 1.8781, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:1673.97, Cost:0.00 best_reg:1684.14 avg_loss_reg:1684.14:  47%|          | 467/1000 [21:42<24:46,  2.79s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 4 Trigger Size: 1673.97412109375 Optimization Steps: 263
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1329.2443466186523
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000250----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.342945098876953
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000251----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-10', '3-8', '12-2', '12-14', '13-8', '15-8', '20-14', '21-18', '22-1']
***Trigger Reverse Engineering開始***
Target: 22, victim: 1, Loss: 8.5412, Acc: 0.00%, CE_Loss: 8.54, Reg_Loss:2566.56, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2550.08:  14%|          | 138/1000 [00:34<03:36,  3.97it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 10 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 45.78194832801819
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000252----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-6', '1-20', '1-21', '3-14', '4-8', '5-15', '7-8', '8-15', '11-8', '11-10', '12-15', '13-19', '13-20', '14-3', '14-19', '14-20', '15-5', '15-8', '16-19', '19-16', '21-1', '22-19']
***Trigger Reverse Engineering開始***
Target: 21, victim: 1, Loss: 2.2654, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:620.62, Cost:0.00 best_reg:624.65 avg_loss_reg:631.27:  60%|[redacted]  | 603/1000 [24:15<15:58,  2.41s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 21 Victim Class: 1 Trigger Size: 620.6196899414062 Optimization Steps: 246
***Symmetric Check開始***
Target: 1, victim: 21, Loss: 2.1914, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:117.07, Cost:0.02 best_reg:119.15 avg_loss_reg:119.15:  54%|[redacted]  | 134/246 [04:26<03:43,  1.99s/it]
early stop 所有
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1741.2192630767822
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000253----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 16.017282247543335
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000254----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.957149028778076
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000255----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 6, Loss: 0.2611, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:559.69, Cost:0.00 best_reg:555.96 avg_loss_reg:557.36:  14%|[redacted]  | 145/1000 [09:44<57:23,  4.03s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 555.9589029947916 Optimization Steps: 146
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 592.8882167339325
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000256----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-10', '3-11', '4-10', '11-3']
***Trigger Reverse Engineering開始***
Target: 2, victim: 10, Loss: 2.7357, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:102.52, Cost:0.03 best_reg:102.59 avg_loss_reg:102.59:  13%|[redacted]  | 132/1000 [00:32<03:32,  4.08it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 10 Trigger Size: 102.52171325683594 Optimization Steps: 90
***Symmetric Check開始***
Target: 10, victim: 2, Loss: 2.2862, Acc: 90.00%, CE_Loss: 0.76, Reg_Loss:5142.69, Cost:0.00 best_reg:10939.42 avg_loss_reg:5261.17: 100%|[redacted]| 90/90 [00:21<00:00,  4.28it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 61.55465626716614
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000257----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-0', '3-15', '4-7', '4-8', '4-9', '5-7', '5-8', '5-10', '7-10', '8-7', '8-9', '11-9', '12-7', '12-8', '12-10', '13-8', '15-10', '15-12', '17-14', '17-0', '17-2']
***Trigger Reverse Engineering開始***
Target: 15, victim: 12, Loss: 0.6338, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:844.27, Cost:0.00 best_reg:844.85 avg_loss_reg:844.85:  55%|[redacted]  | 550/1000 [03:08<02:34,  2.92it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 15 Victim Class: 12 Trigger Size: 844.2669677734375 Optimization Steps: 173
***Symmetric Check開始***
Target: 12, victim: 15, Loss: 0.2086, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:9038.80, Cost:0.00 best_reg:8755.17 avg_loss_reg:9030.10: 100%|[redacted]| 173/173 [00:59<00:00,  2.91it/s]
```

```
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 258.7712004184723
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000258----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-0']
***Trigger Reverse Engineering開始***
Target: 6, victim: 0, Loss: 2.3055, Acc: 100.00%, CE_Loss: 0.33, Reg_Loss:879.72, Cost:0.00 best_reg:880.66 avg_loss_reg:876.25:  19%|██        | 194/1000 [00:26<01:51,  7.21it/s]
  0%|          | 0/195 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 0 Trigger Size: 879.718017578125 Optimization Steps: 195
***Symmetric Check開始***
Target: 0, victim: 6, Loss: 1.3552, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:4031.27, Cost:0.00 best_reg:3960.17 avg_loss_reg:3996.11: 100%|██████████| 195/195 [00:28<00:00,  6.74it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 59.23349142074585
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000259----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 14.57260537147522
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000260----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-5']
***Trigger Reverse Engineering開始***
Target: 3, victim: 5, Loss: 8.5477, Acc: 20.00%, CE_Loss: 8.55, Reg_Loss:3872.52, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3559.12:   2%|▏         | 20/1000 [00:53<43:31,  2.66s/it]
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 63.87156558036804
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000261----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-0', '4-0', '7-13', '10-1', '14-0']
***Trigger Reverse Engineering開始***
Target: 7, victim: 13, Loss: 2.4544, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:294.99, Cost:0.01 best_reg:295.21 avg_loss_reg:295.36:  26%|██▌       | 258/1000 [15:06<43:27,  3.51s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 13 Trigger Size: 294.993408203125 Optimization Steps: 157
***Symmetric Check開始***
Target: 13, victim: 7, Loss: 0.6540, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:10113.93, Cost:0.00 best_reg:9741.82 avg_loss_reg:10099.10: 100%|██████████| 157/157 [08:54<00:00,  3.41s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1461.9326655864716
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000262----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-18', '0-19', '1-18', '17-18', '18-0', '18-1', '19-0', '19-1']
***Trigger Reverse Engineering開始***
Target: 19, victim: 0, Loss: 2.8555, Acc: 100.00%, CE_Loss: 0.43, Reg_Loss:213.08, Cost:0.01 best_reg:214.11 avg_loss_reg:214.11:  20%|██        | 202/1000 [00:14<00:55, 14.37it/s]
  0%|          | 0/125 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 19 Victim Class: 0 Trigger Size: 213.077880859375 Optimization Steps: 125
***Symmetric Check開始***
Target: 0, victim: 19, Loss: 1.9032, Acc: 70.00%, CE_Loss: 0.46, Reg_Loss:427.91, Cost:0.00 best_reg:451.58 avg_loss_reg:426.96: 100%|██████████| 125/125 [00:08<00:00, 14.62it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 30.69347596168518
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000263----------------------------------------
```

```
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 22.036527395248413
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000264----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.798579454421997
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000265----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-9', '2-12', '7-9', '12-9']
***Trigger Reverse Engineering開始***
Target: 2, victim: 12, Loss: 2.6690, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:68.85, Cost:0.04 best_reg:69.87 avg_loss_reg:69.87:  21%|██        | 211/1000 [09:57<37:15,  2.83s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 12 Trigger Size: 68.85238647460938 Optimization Steps: 72
***Symmetric Check開始***
Target: 12, victim: 2, Loss: 4.9122, Acc: 0.00%, CE_Loss: 4.91, Reg_Loss:14389.06, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:14262.21: 100%|██████████| 72/72 [03:23<00:00,  2.83s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 831.7977221012115
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000266----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 7
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 7, victim: 6, Loss: 0.4118, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:255.91, Cost:0.00 best_reg:253.00 avg_loss_reg:254.95:  10%|▉         | 102/1000 [25:09<3:41:32, 14.80s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: all Trigger Size: 253.00390625 Optimization Steps: 103
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1529.5436279773712
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000267----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-13', '3-13', '4-6', '8-7', '10-3', '11-6']
***Trigger Reverse Engineering開始***
Target: 8, victim: 7, Loss: 0.9015, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:71.14, Cost:0.01 best_reg:71.90 avg_loss_reg:71.90:  45%|████▌     | 452/1000 [00:51<01:02,  8.77it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 7 Trigger Size: 71.13677215576172 Optimization Steps: 127
***Symmetric Check開始***
Target: 7, victim: 8, Loss: 8.2422, Acc: 80.00%, CE_Loss: 0.49, Reg_Loss:11632.27, Cost:0.00 best_reg:16824.35 avg_loss_reg:12409.88: 100%|██████████| 127/127 [00:14<00:00,  8.48it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 75.29008531570435
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000268----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 0
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 0, victim: 6, Loss: 1.4364, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:177.48, Cost:0.01 best_reg:179.58 avg_loss_reg:185.24:  14%|▏         | 144/1000 [15:17<1:30:52,  6.37s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 179.34065755208334 Optimization Steps: 145
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 924.2564198970795
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000269----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-0', '2-4', '3-7', '7-3']
***Trigger Reverse Engineering開始***
Target: 7, victim: 3, Loss: 9.2558, Acc: 0.00%, CE_Loss: 9.26, Reg_Loss:2598.33, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2571.89:   6%|▌         | 63/1000 [02:46<41:09,  2.64s/it]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 182.42415857315063
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000270----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.4649529457092285
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000271----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-12', '1-14', '2-7', '5-12']
***Trigger Reverse Engineering開始***
Target: 5, victim: 12, Loss: 5.4542, Acc: 0.00%, CE_Loss: 5.45, Reg_Loss:2599.28, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2574.66:   5%|▍         | 53/1000 [00:27<08:18,  1.90it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 12 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 40.54869723320007
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000272----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['10-1']
***Trigger Reverse Engineering開始***
Target: 10, victim: 1, Loss: 7.1734, Acc: 0.00%, CE_Loss: 7.17, Reg_Loss:2576.56, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2557.39:   1%|          | 10/1000 [00:01<02:57,  5.57it/s]
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 10.090167760848999
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000273----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-13', '7-8', '8-7', '11-7', '13-2', '14-2']
***Trigger Reverse Engineering開始***
Target: 11, victim: 7, Loss: 3.9573, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:216.81, Cost:0.02 best_reg:217.18 avg_loss_reg:217.14:  17%|▏        | 169/1000 [00:24<02:00,  6.91it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 7 Trigger Size: 216.81166076660156 Optimization Steps: 114
***Symmetric Check開始***
Target: 7, victim: 11, Loss: 3.0480, Acc: 80.00%, CE_Loss: 0.89, Reg_Loss:4864.62, Cost:0.00 best_reg:10320.57 avg_loss_reg:4963.81: 100%|██████████| 114/114 [00:19<00:00,  5.99it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 50.286834955215454
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000274----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 24.034883737564087
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000275----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 23.880672931671143
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000276----------------------------------------
```

```
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.835036754608154
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000277----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['7-8']
***Trigger Reverse Engineering開始***
Target: 7, victim: 8, Loss: 9.1221, Acc: 0.00%, CE_Loss: 9.12, Reg_Loss:2574.99, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2555.77:   1%|         | 10/1000 [00:04<07:54,  2.08it/s]
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 8 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 15.46074914932251
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000278----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 28.607166528701782
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000279----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.633477449417114
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000280----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-12']
***Trigger Reverse Engineering開始***
Target: 4, victim: 12, Loss: 10.8191, Acc: 0.00%, CE_Loss: 10.82, Reg_Loss:2537.32, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2526.63:   1%|         | 10/1000 [00:03<06:22,  2.59it/s]
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 12 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 13.260554552078247
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000281----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 14.600788354873657
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000282----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 36.816036224365234
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000283----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.614709377288818
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000284----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '2-1', '4-3', '4-11', '9-3', '14-11', '19-2', '22-1', '22-2']
***Trigger Reverse Engineering開始***
Target: 4, victim: 11, Loss: 2.5807, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:43.90, Cost:0.06 best_reg:44.19 avg_loss_reg:43.36:  22%|[redacted]         | 222/1000 [03:38<12:46,  1.02it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 11 Trigger Size: 43.900657653808594 Optimization Steps: 91
***Symmetric Check開始***
Target: 11, victim: 4, Loss: 0.4296, Acc: 85.00%, CE_Loss: 0.43, Reg_Loss:19473.90, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:19374.88: 100%|[redacted]| 91/91 [01:21<00:00,  1.12it/s]
```

```
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 311.3421742916107
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000285----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-18', '13-3', '14-18', '16-3']
***Trigger Reverse Engineering開始***
Target: 14, victim: 18, Loss: 2.5877, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:94.10, Cost:0.03 best_reg:95.52 avg_loss_reg:95.52:  14%|█         | 145/1000 [00:16<01:39,  8.59it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 18 Trigger Size: 94.09506225585938 Optimization Steps: 112
***Symmetric Check開始***
Target: 18, victim: 14, Loss: 5.2238, Acc: 90.00%, CE_Loss: 0.67, Reg_Loss:3033.36, Cost:0.00 best_reg:3112.93 avg_loss_reg:3070.61: 100%|██████████| 112/112 [00:13<00:00,  8.46it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 35.91523265838623
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000286----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['10-12', '10-13']
***Trigger Reverse Engineering開始***
Target: 10, victim: 13, Loss: 8.9809, Acc: 0.00%, CE_Loss: 8.98, Reg_Loss:2543.81, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2530.32:   2%|▏         | 21/1000 [00:03<02:57,  5.50it/s]
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 12 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 9.533351182937622
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000287----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-10', '6-3', '10-0']
***Trigger Reverse Engineering開始***
Target: 0, victim: 10, Loss: 1.4801, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:575.54, Cost:0.00 best_reg:576.44 avg_loss_reg:575.33:  24%|██        | 235/1000 [12:05<39:22,  3.09s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 10 Trigger Size: 575.5419921875 Optimization Steps: 194
***Symmetric Check開始***
Target: 10, victim: 0, Loss: 0.9422, Acc: 95.00%, CE_Loss: 0.26, Reg_Loss:1027.04, Cost:0.00 best_reg:1060.54 avg_loss_reg:1020.31: 100%|██████████| 194/194 [09:56<00:00,  3.07s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1332.5574412345886
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000288----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 8
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 8, victim: 16, Loss: 0.3565, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:70.43, Cost:0.01 best_reg:81.13 avg_loss_reg:70.85:   7%|▋         | 66/1000 [04:06<58:12,  3.74s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: all Trigger Size: 81.12675603230794 Optimization Steps: 67
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 253.48026180267334
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000289----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['13-0']
***Trigger Reverse Engineering開始***
Target: 13, victim: 0, Loss: 7.3209, Acc: 0.00%, CE_Loss: 7.32, Reg_Loss:2553.39, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2540.90:   1%|         | 10/1000 [00:22<36:33,  2.22s/it]
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
```

```
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 35.53170442581177
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000290----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-8']
***Trigger Reverse Engineering開始***
Target: 0, victim: 8, Loss: 3.3472, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:1408.71, Cost:0.00 best_reg:1414.26 avg_loss_reg:1405.70:  15%|▉         | 149/1000 [11:52<1:07:49,  4.78s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 8 Trigger Size: 1408.7076416015625 Optimization Steps: 150
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 735.323009967804
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000291----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 0
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 0, victim: 9, Loss: 0.2001, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:58.89, Cost:0.00 best_reg:57.97 avg_loss_reg:58.59:   8%|▊         | 77/1000 [16:59<3:23:36, 13.24s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 57.970904214041575 Optimization Steps: 78
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1030.4302251338959
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000292----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.500859260559082
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000293----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 1.9401400089263916
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000294----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 0
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 0, victim: 9, Loss: 0.2176, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:319.79, Cost:0.00 best_reg:316.05 avg_loss_reg:318.34:   9%|▉         | 90/1000 [01:01<10:19,  1.47it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 316.0466766357422 Optimization Steps: 91
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 66.52274012565613
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000295----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.0246827602386475
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000296----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.946580410003662
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000297----------
***Pre-Screening開始***
***Pre-Screening結束***
```

```
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['7-0', '7-5']
***Trigger Reverse Engineering開始***
Target: 7, victim: 0, Loss: 1.5542, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:284.63, Cost:0.01 best_reg:285.20 avg_loss_reg:285.53:  17%|▉         | 172/1000 [03:39<17:35,  1.27s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 0 Trigger Size: 284.62506103515625 Optimization Steps: 155
***Symmetric Check開始***
Target: 0, victim: 7, Loss: 8.3136, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:476.59, Cost:0.02 best_reg:483.70 avg_loss_reg:483.70: 100%|██████████| 155/155 [03:21<00:00,  1.30s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 427.1314253807068
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000298----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-20', '1-8', '4-8', '5-7', '7-11', '9-14', '9-12', '9-15', '10-18', '10-4', '10-9', '12-6', '12-8', '13-6', '15-12', '16-5', '16-6', '17-11', '18-2', '18-19', '19-14', '19-20', '20-0']
***Trigger Reverse Engineering開始***
Target: 0, victim: 20, Loss: 4.0837, Acc: 100.00%, CE_Loss: 0.34, Reg_Loss:218.92, Cost:0.02 best_reg:219.43 avg_loss_reg:219.43:  41%|████▏     | 412/1000 [16:21<23:20,  2.38s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 20 Trigger Size: 218.91944885253906 Optimization Steps: 119
***Symmetric Check開始***
Target: 20, victim: 0, Loss: 6.4806, Acc: 90.00%, CE_Loss: 0.34, Reg_Loss:1819.57, Cost:0.00 best_reg:2016.21 avg_loss_reg:1850.03: 100%|██████████| 119/119 [04:11<00:00,  2.11s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1249.1257319450378
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000299----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 2.0644288063049316
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000300----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-9', '4-5', '4-8', '7-0', '7-6', '8-3', '8-4']
***Trigger Reverse Engineering開始***
Target: 7, victim: 0, Loss: 1.1127, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:1432.11, Cost:0.00 best_reg:1436.21 avg_loss_reg:1433.47:  42%|████▏     | 419/1000 [22:46<31:34,  3.26s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 0 Trigger Size: 1432.1094970703125 Optimization Steps: 343
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1377.9544868469238
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000301----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 1.9250075817108154
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000302----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.963806867599487
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000303----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.616626024246216
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000304----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
```

```
整體耗時: 6.236108303070068
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000305----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 6
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 6, victim: 6, Loss: 0.2643, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:6.85, Cost:0.04 best_reg:6.75 avg_loss_reg:6.82:   9%|▉         | 93/1000 [02:29<24:18,  1.61s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: all Trigger Size: 6.747086906433106 Optimization Steps: 94
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 154.31021928787231
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000306----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['9-12']
***Trigger Reverse Engineering開始***
Target: 9, victim: 12, Loss: 12.5037, Acc: 0.00%, CE_Loss: 12.50, Reg_Loss:2532.20, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2524.50:   1%|         | 10/1000 [00:01<02:50,  5.81it/s]
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 12 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 7.7492430210113525
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000307----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-21', '23-1']
***Trigger Reverse Engineering開始***
Target: 23, victim: 1, Loss: 5.7499, Acc: 0.00%, CE_Loss: 5.75, Reg_Loss:2592.91, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2568.80:   2%|▏         | 21/1000 [00:07<06:02,  2.70it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 21 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 14.38970685005188
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000308----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.02915334701538
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000309----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.687676668167114
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000310----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 6
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 6, victim: 14, Loss: 0.3528, Acc: 90.62%, CE_Loss: 0.13, Reg_Loss:151.66, Cost:0.00 best_reg:152.74 avg_loss_reg:149.77:   8%|▊         | 80/1000 [13:40<2:37:16, 10.26s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: all Trigger Size: 152.74190826416014 Optimization Steps: 81
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 829.546571969986
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000311----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.035828590393066
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000312----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 0
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 0, victim: 6, Loss: 2.5409, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:5694.87, Cost:0.00 best_reg:5736.33 avg_loss_reg:5723.15:  13%|          | 130/1000 [31:42<3:32:15, 14.64s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 5736.3283203125 Optimization Steps: 131
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1913.6277701854706
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000313----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-16', '2-1', '2-16', '4-6', '7-4', '7-6', '7-10', '8-4', '9-3', '9-12', '10-4', '10-6', '10-8', '14-5', '14-9', '14-3']
***Trigger Reverse Engineering開始***
Target: 2, victim: 1, Loss: 0.4673, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:326.49, Cost:0.00 best_reg:326.97 avg_loss_reg:329.15:  63%|          | 634/1000 [14:25<08:19,  1.37s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 326.4883728027344 Optimization Steps: 426
***Symmetric Check開始***
Target: 1, victim: 2, Loss: 1.3830, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:1838.50, Cost:0.00 best_reg:1843.37 avg_loss_reg:1843.37:  72%|          | 305/426 [06:33<02:36,  1.29s/it]
early stop 所有
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1274.3152511119843
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000314----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-4', '1-3', '1-5', '4-0', '5-1']
***Trigger Reverse Engineering開始***
Target: 5, victim: 1, Loss: 6.8003, Acc: 15.00%, CE_Loss: 6.80, Reg_Loss:3458.16, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3256.90:   6%|          | 64/1000 [03:12<47:01,  3.01s/it]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 206.88228225708008
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000315----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-21']
***Trigger Reverse Engineering開始***
Target: 2, victim: 21, Loss: 7.8032, Acc: 0.00%, CE_Loss: 7.80, Reg_Loss:2552.49, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2539.31:   1%|          | 10/1000 [00:02<03:30,  4.69it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 21 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 8.86907434463501
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000316----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-0', '11-0']
***Trigger Reverse Engineering開始***
Target: 11, victim: 0, Loss: 6.7771, Acc: 0.00%, CE_Loss: 6.78, Reg_Loss:2515.07, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2512.11:   2%|          | 21/1000 [00:31<24:07,  1.48s/it]
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 40.993611335754395
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000317----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
```

```
檢測結果: Model是安全的(Benign)
整體耗時: 6.335360288619995
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000318----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.53815484046936
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000319----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['7-9']
***Trigger Reverse Engineering開始***
Target: 7, victim: 9, Loss: 9.3304, Acc: 10.00%, CE_Loss: 9.33, Reg_Loss:2970.36, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2847.66:   2%|          | 20/1000 [00:30<24:38,  1.51s/it]
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 9 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 43.0543429851532
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000320----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.648034334182739
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000321----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 4
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 4, victim: 9, Loss: 0.2310, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:230.64, Cost:0.00 best_reg:237.42 avg_loss_reg:228.67:   9%|▉         | 93/1000 [01:14<12:06,  1.25it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: all Trigger Size: 237.4216423034668 Optimization Steps: 94
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 79.00211191177368
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000322----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-8', '1-3', '2-1', '2-5', '2-6', '3-6', '5-2', '5-6', '6-2', '6-5', '9-3', '10-3', '12-18', '17-8']
***Trigger Reverse Engineering開始***
Target: 2, victim: 5, Loss: 2.9384, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:110.89, Cost:0.03 best_reg:113.64 avg_loss_reg:109.01:  69%|[redacted]  | 688/1000 [08:05<03:40,  1.42it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 5 Trigger Size: 110.89006042480469 Optimization Steps: 75
***Symmetric Check開始***
Target: 5, victim: 2, Loss: 1.9302, Acc: 35.00%, CE_Loss: 1.93, Reg_Loss:10730.96, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:10618.96: 100%|[redacted]| 75/75 [00:51<00:00,  1.44it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 545.1646373271942
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000323----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['9-0']
***Trigger Reverse Engineering開始***
Target: 9, victim: 0, Loss: 4.0282, Acc: 15.00%, CE_Loss: 4.03, Reg_Loss:3579.64, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3358.63:   2%|          | 20/1000 [00:06<05:40,  2.88it/s]
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 12.6623215675354
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000324----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
```

```
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['17-0']
***Trigger Reverse Engineering開始***
Target: 17, victim: 0, Loss: 9.3512, Acc: 0.00%, CE_Loss: 9.35, Reg_Loss:2514.84, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2508.08:   1%|         | 10/1000 [00:27<45:03,  2.73s/it]
***Trigger Reverse Engineering結束***
Target Class: 17 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 40.362021684646606
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000325----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 6
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 6, victim: 12, Loss: 0.4586, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:601.37, Cost:0.00 best_reg:598.59 avg_loss_reg:596.63:   8%|▊         | 79/1000 [29:55<5:48:49, 22.73s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: all Trigger Size: 598.5869018554688 Optimization Steps: 80
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1809.007972240448
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000326----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['8-7']
***Trigger Reverse Engineering開始***
Target: 8, victim: 7, Loss: 8.4096, Acc: 0.00%, CE_Loss: 8.41, Reg_Loss:2575.97, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2556.88:   1%|         | 10/1000 [00:01<02:28,  6.66it/s]
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 7 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 6.764363765716553
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000327----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 18.185552835464478
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000328----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['11-5', '11-6']
***Trigger Reverse Engineering開始***
Target: 11, victim: 5, Loss: 3.4726, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:299.28, Cost:0.01 best_reg:299.37 avg_loss_reg:299.92:  12%|▏        | 117/1000 [09:18<1:10:16,  4.78s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 5 Trigger Size: 299.2782287597656 Optimization Steps: 103
***Symmetric Check開始***
Target: 5, victim: 11, Loss: 0.2988, Acc: 95.00%, CE_Loss: 0.30, Reg_Loss:14243.00, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:14197.04: 100%|██████████| 103/103 [08:13<00:00,  4.79s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1071.2411034107208
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000329----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 15.622506380081177
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000330----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 5
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 5, victim: 6, Loss: 0.5990, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:265.72, Cost:0.00 best_reg:265.91 avg_loss_reg:263.88:   8%|▊         | 85/1000 [11:31<2:04:04,  8.14s/it]
```

```
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: all Trigger Size: 265.90570678710935 Optimization Steps: 86
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 700.4093108177185
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000331----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-6', '6-4', '14-5']
***Trigger Reverse Engineering開始***
Target: 14, victim: 5, Loss: 12.6698, Acc: 0.00%, CE_Loss: 12.67, Reg_Loss:2538.88, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2529.34:   3%|          | 32/1000 [00:13<06:55,  2.33it/s]
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 6 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 19.45664691925049
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000332----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 16
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 16, victim: 17, Loss: 0.3459, Acc: 96.43%, CE_Loss: 0.09, Reg_Loss:874.24, Cost:0.00 best_reg:886.97 avg_loss_reg:887.27:  12%|          | 120/1000 [51:10<6:15:16, 25.59s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 16 Victim Class: all Trigger Size: 886.9656219482422 Optimization Steps: 121
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 3083.6483561992645
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000333----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-5', '15-2', '22-0', '23-1']
***Trigger Reverse Engineering開始***
Target: 22, victim: 0, Loss: 0.9291, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:48.74, Cost:0.02 best_reg:52.24 avg_loss_reg:48.55:  22%|          | 219/1000 [00:21<01:15, 10.30it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 22 Victim Class: 0 Trigger Size: 48.737030029296875 Optimization Steps: 114
***Symmetric Check開始***
Target: 0, victim: 22, Loss: 1.5909, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:258.60, Cost:0.01 best_reg:259.68 avg_loss_reg:259.68: 100%|          | 114/114 [00:11<00:00, 10.04it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 42.551265716552734
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000334----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.497998476028442
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000335----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.792309522628784
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000336----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-5', '3-7', '9-10', '12-1', '12-0', '12-8']
***Trigger Reverse Engineering開始***
Target: 12, victim: 8, Loss: 12.5223, Acc: 0.00%, CE_Loss: 12.52, Reg_Loss:2484.50, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2479.38:   6%|          | 65/1000 [01:01<14:48,  1.05it/s]
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
```

```
整體耗時: 68.87157225608826
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000337----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-7', '7-9']
***Trigger Reverse Engineering開始***
Target: 7, victim: 9, Loss: 12.4700, Acc: 0.00%, CE_Loss: 12.47, Reg_Loss:2593.65, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2570.58:   2%|         | 21/1000 [00:17<13:34,  1.20it/s]
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 7 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 26.603146076202393
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000338----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.014855623245239
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000339----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['16-10']
***Trigger Reverse Engineering開始***
Target: 16, victim: 10, Loss: 3.5172, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:299.20, Cost:0.01 best_reg:299.87 avg_loss_reg:299.87:  16%|██        | 160/1000 [08:32<44:53,  3.21s/it]
  0%|          | 0/161 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 16 Victim Class: 10 Trigger Size: 299.2015380859375 Optimization Steps: 161
***Symmetric Check開始***
Target: 10, victim: 16, Loss: 2.3431, Acc: 95.00%, CE_Loss: 0.25, Reg_Loss:3140.07, Cost:0.00 best_reg:3183.31 avg_loss_reg:3055.32: 100%|██████████| 161/161 [09:44<00:00,  3.63s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1113.8228380680084
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000340----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-7', '3-1', '6-7', '9-3', '10-3', '10-6', '10-15', '11-1', '11-17', '11-15', '14-16', '18-19', '19-1']
***Trigger Reverse Engineering開始***
Target: 10, victim: 3, Loss: 1.8873, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:1140.20, Cost:0.00 best_reg:1142.91 avg_loss_reg:1151.57:  46%|████▋     | 463/1000 [00:49<00:56,  9.43it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 3 Trigger Size: 1140.197021484375 Optimization Steps: 201
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 54.143009185791016
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000341----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.157269477844238
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000342----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.143176794052124
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000343----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.981877565383911
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000344----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['17-5', '19-5', '22-5']
```

```
***Trigger Reverse Engineering開始***
Target: 22, victim: 5, Loss: 10.0402, Acc: 0.00%, CE_Loss: 10.04, Reg_Loss:2555.11, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2542.00:   3%|▌         | 32/1000 [00:30<15:09,  1.06it/s]
***Trigger Reverse Engineering結束***
Target Class: 17 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 38.2461199760437
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000345----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-2', '0-6']
***Trigger Reverse Engineering開始***
Target: 0, victim: 6, Loss: 1.5478, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:180.21, Cost:0.01 best_reg:181.40 avg_loss_reg:181.40:  16%|██        | 164/1000 [08:01<40:55,  2.94s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 6 Trigger Size: 180.20608520507812 Optimization Steps: 121
***Symmetric Check開始***
Target: 6, victim: 0, Loss: 0.5100, Acc: 90.00%, CE_Loss: 0.51, Reg_Loss:8921.35, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:8947.13: 100%|██████████| 121/121 [05:56<00:00,  2.95s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 846.6174244880676
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000346----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-5', '3-4', '4-1', '4-3']
***Trigger Reverse Engineering開始***
Target: 4, victim: 3, Loss: 6.9602, Acc: 15.00%, CE_Loss: 6.96, Reg_Loss:2812.63, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2759.34:   6%|▋         | 63/1000 [02:22<35:19,  2.26s/it]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 149.1050362586975
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000347----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.385232925415039
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000348----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 0
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 0, victim: 6, Loss: 3.3575, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:3290.78, Cost:0.00 best_reg:3272.15 avg_loss_reg:3345.69:  28%|██▊       | 278/1000 [46:42<2:01:18, 10.08s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 3272.1532389322915 Optimization Steps: 279
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 2809.8104202747345
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000349----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 20, Loss: 2.1570, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:4845.65, Cost:0.00 best_reg:4851.19 avg_loss_reg:4861.34:  17%|█▋        | 166/1000 [1:03:27<5:18:51, 22.94s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 4841.870989118303 Optimization Steps: 167
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 3821.095847129822
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000350----------------------------------------
***Pre-Screening開始***
```

```
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-7', '1-10']
***Trigger Reverse Engineering開始***
Target: 1, victim: 7, Loss: 3.2053, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:54.42, Cost:0.06 best_reg:54.83 avg_loss_reg:54.83:  10%|          | 104/1000 [00:15<02:13,  6.72it/s]
  0%|          | 0/83 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 7 Trigger Size: 54.4190559387207 Optimization Steps: 83
***Symmetric Check開始***
Target: 7, victim: 1, Loss: 1.3867, Acc: 35.00%, CE_Loss: 1.39, Reg_Loss:15893.03, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:15759.57: 100%|[redacted]| 83/83 [00:12<00:00,  6.56it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 33.74845600128174
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000351----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.537317991256714
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000352----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-10', '1-0', '1-7', '1-10', '5-0', '7-1', '8-1', '10-0', '12-10']
***Trigger Reverse Engineering開始***
Target: 1, victim: 0, Loss: 4.7732, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:54.51, Cost:0.09 best_reg:56.07 avg_loss_reg:56.07:  17%|          | 167/1000 [00:16<01:20, 10.35it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 0 Trigger Size: 54.510581970214844 Optimization Steps: 68
***Symmetric Check開始***
Target: 0, victim: 1, Loss: 0.4796, Acc: 80.00%, CE_Loss: 0.48, Reg_Loss:17405.35, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:17260.42: 100%|[redacted]| 68/68 [00:06<00:00, 10.26it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 27.55863118171692
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000353----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.758951663970947
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000354----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.725831031799316
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000355----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-5', '6-8']
***Trigger Reverse Engineering開始***
Target: 6, victim: 8, Loss: 10.2825, Acc: 0.00%, CE_Loss: 10.28, Reg_Loss:2576.66, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2556.35:   2%|          | 21/1000 [00:02<02:01,  8.04it/s]
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 7.385179042816162
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000356----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.305670499801636
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000357----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
```

整體耗時: 7.878838062286377
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000358----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-1', '3-4', '7-10', '7-12', '10-12', '17-1']
Trigger Reverse Engineering開始
Target: 7, victim: 12, Loss: 1.6455, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:975.52, Cost:0.00 best_reg:980.22 avg_loss_reg:980.22: 36%|[redacted]| 356/1000 [11:24<20:38, 1.92s/it]
  0%| | 0/251 [00:00<?, ?it/s]early stop 所有
Trigger Reverse Engineering結束
Target Class: 7 Victim Class: 12 Trigger Size: 975.5238037109375 Optimization Steps: 251
Symmetric Check開始
Target: 12, victim: 7, Loss: 2.9300, Acc: 90.00%, CE_Loss: 0.64, Reg_Loss:5160.49, Cost:0.00 best_reg:5196.58 avg_loss_reg:5166.26: 100%|[redacted]| 251/251 [07:53<00:00, 1.89s/it]
Symmetric Check結束
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1167.7012283802032
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000359----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 8
可能的 victim classes: ALL
Trigger Reverse Engineering開始
Target: 8, victim: 22, Loss: 0.2151, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:483.02, Cost:0.00 best_reg:486.89 avg_loss_reg:480.74:   8%|[redacted]| 82/1000 [30:57<5:46:38, 22.66s/it]
early stop 所有
Trigger Reverse Engineering結束
Target Class: 8 Victim Class: all Trigger Size: 486.88933715820315 Optimization Steps: 83
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1873.4004418849945
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000360----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-1', '3-13', '13-3', '18-0']
Trigger Reverse Engineering開始
Target: 18, victim: 0, Loss: 0.0839, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:118.10, Cost:0.00 best_reg:118.65 avg_loss_reg:119.16: 32%|[redacted]| 317/1000 [00:22<00:48, 13.94it/s]
early stop 所有
Trigger Reverse Engineering結束
Target Class: 18 Victim Class: 0 Trigger Size: 118.10191345214844 Optimization Steps: 237
Symmetric Check開始
Target: 0, victim: 18, Loss: 2.5557, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:435.88, Cost:0.01 best_reg:440.90 avg_loss_reg:440.90: 61%|[redacted]| 144/237 [00:09<00:06, 15.14it/s]
early stop 所有
Symmetric Check結束
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 41.28732872009277
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000361----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 15
可能的 victim classes: ALL
Trigger Reverse Engineering開始
Target: 15, victim: 17, Loss: 0.3861, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:571.10, Cost:0.00 best_reg:567.83 avg_loss_reg:571.29:   9%|[redacted]| 91/1000 [04:57<49:27, 3.26s/it]
early stop 所有
Trigger Reverse Engineering結束
Target Class: 15 Victim Class: all Trigger Size: 567.8334452311198 Optimization Steps: 92
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 302.4981861114502
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000362----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-16', '8-1', '11-1']
Trigger Reverse Engineering開始
Target: 0, victim: 16, Loss: 2.5543, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:697.10, Cost:0.00 best_reg:715.03 avg_loss_reg:704.37: 21%|[redacted]| 213/1000 [02:11<08:05, 1.62it/s]
  0%| | 0/172 [00:00<?, ?it/s]early stop 所有
Trigger Reverse Engineering結束

```
Target Class: 0 Victim Class: 16 Trigger Size: 697.10009765625 Optimization Steps: 172
***Symmetric Check開始***
Target: 16, victim: 0, Loss: 1.1219, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:921.77, Cost:0.00 best_reg:917.25 avg_loss_reg:921.78: 100%|██████████| 172/172 [01:45<00:00,  1.63it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 243.44098162651062
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000363----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.68360710144043
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000364----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-3', '1-4', '1-13', '3-0', '7-3', '7-13', '9-12', '11-0', '14-9']
***Trigger Reverse Engineering開始***
Target: 7, victim: 13, Loss: 1.0191, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:177.72, Cost:0.01 best_reg:180.13 avg_loss_reg:173.70:  32%|████      | 317/1000 [03:15<07:01,  1.62it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 13 Trigger Size: 177.72308349609375 Optimization Steps: 148
***Symmetric Check開始***
Target: 13, victim: 7, Loss: 5.3910, Acc: 95.00%, CE_Loss: 0.33, Reg_Loss:1499.19, Cost:0.00 best_reg:1537.90 avg_loss_reg:1501.97: 100%|██████████| 148/148 [01:30<00:00,  1.63it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 292.8055000305176
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000365----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 0
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 0, victim: 12, Loss: 0.4519, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:3354.73, Cost:0.00 best_reg:3307.56 avg_loss_reg:3286.58:   8%|▊         | 85/1000 [05:39<1:00:55,  3.99s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 3307.563818359375 Optimization Steps: 86
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 346.6965730190277
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000366----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.257125616073608
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000367----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 11
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 11, victim: 12, Loss: 0.2309, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:346.29, Cost:0.00 best_reg:348.40 avg_loss_reg:342.99:   7%|▋         | 70/1000 [45:00<9:57:51, 38.57s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: all Trigger Size: 348.4009704589844 Optimization Steps: 71
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 2713.2469820976257
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000368----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.642746210098267
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000369----------------------------------------
***Pre-Screening開始***
```

```
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-1', '6-4']
***Trigger Reverse Engineering開始***
Target: 6, victim: 4, Loss: 4.8886, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:179.35, Cost:0.03 best_reg:179.76 avg_loss_reg:178.64:  15%|          | 150/1000 [01:08<06:25,  2.20it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 4 Trigger Size: 179.3450927734375 Optimization Steps: 121
***Symmetric Check開始***
Target: 4, victim: 6, Loss: 0.7534, Acc: 90.00%, CE_Loss: 0.46, Reg_Loss:4982.47, Cost:0.00 best_reg:9232.01 avg_loss_reg:4939.88: 100%|| 121/121 [00:51<00:00,  2.35it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 123.55148339271545
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000370----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.930258512496948
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000371----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-7', '1-10', '4-7', '6-5']
***Trigger Reverse Engineering開始***
Target: 1, victim: 7, Loss: 1.8228, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:1113.65, Cost:0.00 best_reg:1116.76 avg_loss_reg:1116.76:  31%|       | 313/1000 [02:09<04:43,  2.43it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 7 Trigger Size: 1113.651123046875 Optimization Steps: 239
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 135.52325963974
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000372----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-10', '3-13', '4-13', '7-13']
***Trigger Reverse Engineering開始***
Target: 7, victim: 13, Loss: 3.0903, Acc: 20.00%, CE_Loss: 3.09, Reg_Loss:3235.27, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3052.37:   5%|          | 53/1000 [00:49<14:41,  1.07it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 10 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 56.9391188621521
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000373----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-6']
***Trigger Reverse Engineering開始***
Target: 2, victim: 6, Loss: 9.9193, Acc: 0.00%, CE_Loss: 9.92, Reg_Loss:2606.60, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2578.62:   1%|          | 10/1000 [00:09<14:53,  1.11it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 6 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 17.979365587234497
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000374----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 15.113564491271973
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000375----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-10', '2-16', '2-12', '2-13', '3-17', '3-1', '3-9', '4-7', '5-17', '6-20', '7-5', '7-12', '7-17', '8-0', '8-20', '9-3', '9-7', '10-1', '10-9', '11-4', '11-5', '11-12', '13-2', '14-1', '16-2', '17-5', '17-7', '17-12', '18-1', '18-9', '18-20', '19-6', '20-6', '21-15', '21-20', '21-19']
***Trigger Reverse Engineering開始***
Target: 11, victim: 12, Loss: 2.0982, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:1215.98, Cost:0.00 best_reg:1217.94 avg_loss_reg:1227.84:  83%|  | 830/1000 [01:43<00:21,  8.00it/s]
early stop 所有
```

```
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 12 Trigger Size: 1215.9766845703125 Optimization Steps: 405
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 109.23744702339172
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000376----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.0404393672943115
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000377----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-2', '1-0', '1-4', '2-1', '3-5']
***Trigger Reverse Engineering開始***
Target: 3, victim: 5, Loss: 4.6918, Acc: 0.00%, CE_Loss: 4.69, Reg_Loss:2557.34, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2542.31:   6%|▌         | 64/1000 [00:29<07:10,  2.17it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 2 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 33.2822949886322
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000378----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.759771108627319
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000379----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '8-2']
***Trigger Reverse Engineering開始***
Target: 1, victim: 2, Loss: 1.1429, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:454.84, Cost:0.00 best_reg:458.83 avg_loss_reg:449.87:  25%|██▍       | 248/1000 [02:45<08:22,  1.50it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 2 Trigger Size: 454.83990478515625 Optimization Steps: 238
***Symmetric Check開始***
Target: 2, victim: 1, Loss: 1.6893, Acc: 100.00%, CE_Loss: 0.55, Reg_Loss:508.24, Cost:0.00 best_reg:485.99 avg_loss_reg:508.10: 100%|██████████| 238/238 [02:42<00:00,  1.46it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 334.1624011993408
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000380----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['15-1', '15-7']
***Trigger Reverse Engineering開始***
Target: 15, victim: 1, Loss: 3.0122, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:810.54, Cost:0.00 best_reg:811.22 avg_loss_reg:804.46:  19%|█▉        | 193/1000 [00:27<01:54,  7.05it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 15 Victim Class: 1 Trigger Size: 810.542724609375 Optimization Steps: 183
***Symmetric Check開始***
Target: 1, victim: 15, Loss: 1.6863, Acc: 70.00%, CE_Loss: 0.79, Reg_Loss:4562.24, Cost:0.00 best_reg:10118.81 avg_loss_reg:4587.21: 100%|██████████| 183/183 [00:26<00:00,  6.97it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 58.86849761009216
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000381----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 3.062547206878662
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000382----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
```

```
可能的 target class: 7
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 7, victim: 16, Loss: 0.3407, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:511.07, Cost:0.00 best_reg:505.86 avg_loss_reg:507.27:  16%|▉         | 163/1000 [1:00:26<5:10:19, 22.25s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: all Trigger Size: 505.8648274739583 Optimization Steps: 164
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 3638.8696393966675
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000383----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-14', '10-5', '10-18', '21-1']
***Trigger Reverse Engineering開始***
Target: 10, victim: 18, Loss: 2.5464, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:315.79, Cost:0.01 best_reg:316.40 avg_loss_reg:316.40:  19%|▊         | 191/1000 [00:24<01:43,  7.84it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 18 Trigger Size: 315.7879943847656 Optimization Steps: 128
***Symmetric Check開始***
Target: 18, victim: 10, Loss: 3.1301, Acc: 70.00%, CE_Loss: 0.94, Reg_Loss:7379.08, Cost:0.00 best_reg:14340.97 avg_loss_reg:7468.34: 100%|██████████| 128/128 [00:16<00:00,  7.70it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 46.70122241973877
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000384----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '0-16', '1-16', '2-12', '7-8', '10-12', '12-2', '14-15', '15-16', '16-1', '16-15']
***Trigger Reverse Engineering開始***
Target: 16, victim: 1, Loss: 2.0948, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:824.44, Cost:0.00 best_reg:825.00 avg_loss_reg:827.18:  71%|███████   | 714/1000 [01:12<00:28,  9.88it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 16 Victim Class: 1 Trigger Size: 824.4365234375 Optimization Steps: 574
***Symmetric Check開始***
Target: 1, victim: 16, Loss: 6.3692, Acc: 100.00%, CE_Loss: 0.33, Reg_Loss:1789.55, Cost:0.00 best_reg:1790.88 avg_loss_reg:1798.32:  95%|█████████▍| 544/574 [00:55<00:03,  9.80it/s]
early stop 所有
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 132.87911128997803
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000385----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.34387731552124
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000386----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 1
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 1, victim: 12, Loss: 5.2271, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:3484.75, Cost:0.00 best_reg:3487.93 avg_loss_reg:3488.08:  21%|▋         | 208/1000 [52:49<3:21:08, 15.24s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 3484.59853515625 Optimization Steps: 209
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 3180.5453498363495
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000387----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 17.066123485565186
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000388----------------------------------------
***Pre-Screening開始***
```

```
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 11
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 11, victim: 16, Loss: 0.6910, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:460.67, Cost:0.00 best_reg:465.29 avg_loss_reg:470.59:  15%|          | 152/1000 [1:38:16<9:08:15, 38.79s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: all Trigger Size: 465.29006125710225 Optimization Steps: 153
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 5912.958165884018
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000389----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 4
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 4, victim: 14, Loss: 0.1276, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:25.19, Cost:0.01 best_reg:25.11 avg_loss_reg:24.55:   6%|          | 57/1000 [33:18<9:11:07, 35.07s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: all Trigger Size: 25.106945419311522 Optimization Steps: 58
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 2013.7501435279846
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000390----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.823410749435425
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000391----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-0', '1-2', '1-4']
***Trigger Reverse Engineering開始***
Target: 1, victim: 4, Loss: 9.4199, Acc: 0.00%, CE_Loss: 9.42, Reg_Loss:2574.83, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2558.21:   4%|          | 42/1000 [02:17<52:13,  3.27s/it]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 146.41415405273438
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000392----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.122389316558838
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000393----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-5']
***Trigger Reverse Engineering開始***
Target: 1, victim: 5, Loss: 10.9795, Acc: 0.00%, CE_Loss: 10.98, Reg_Loss:2566.29, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2549.80:   1%|          | 10/1000 [00:01<02:20,  7.03it/s]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 6.40530800819397
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000394----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.03056025505066
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000395----------
***Pre-Screening開始***
***Pre-Screening結束***
```

```
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.8176820278167725
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000396----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 22, Loss: 0.1062, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:354.49, Cost:0.00 best_reg:348.38 avg_loss_reg:346.73:   8%|▉         | 78/1000 [48:01<9:27:41, 36.94s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 348.3751907348633 Optimization Steps: 79
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 2900.604240655899
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000397----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 1
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 1, victim: 9, Loss: 1.2414, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:163.45, Cost:0.01 best_reg:163.82 avg_loss_reg:162.64:   9%|▉         | 87/1000 [01:49<19:04,  1.25s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 163.8156509399414 Optimization Steps: 88
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 117.99328184127808
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000398----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['9-1']
***Trigger Reverse Engineering開始***
Target: 9, victim: 1, Loss: 8.7729, Acc: 0.00%, CE_Loss: 8.77, Reg_Loss:2574.31, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2557.49:   1%|          | 10/1000 [00:05<09:46,  1.69it/s]
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 11.585622310638428
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000399----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 14.854406595230103
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000400----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-23', '16-4', '20-18']
***Trigger Reverse Engineering開始***
Target: 2, victim: 23, Loss: 1.0036, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:780.74, Cost:0.00 best_reg:784.12 avg_loss_reg:784.12:  23%|██▎       | 231/1000 [00:34<01:56,  6.61it/s]
  0%|          | 0/210 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 23 Trigger Size: 780.7389526367188 Optimization Steps: 210
***Symmetric Check開始***
Target: 23, victim: 2, Loss: 3.1949, Acc: 100.00%, CE_Loss: 0.33, Reg_Loss:376.78, Cost:0.01 best_reg:379.88 avg_loss_reg:379.88:  88%|████████▊ | 185/210 [00:29<00:04,  6.20it/s]
early stop 所有
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 70.99684596061707
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000401----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
```

```
整體耗時: 5.263123512268066
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000402----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 3.311382532119751
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000403----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 11
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 11, victim: 12, Loss: 0.3512, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:156.09, Cost:0.00 best_reg:165.57 avg_loss_reg:154.15:   5%|▌         | 48/1000 [07:16<2:24:17,  9.09s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: all Trigger Size: 165.57279052734376 Optimization Steps: 49
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 442.98185300827026
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000404----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['7-0', '7-2']
***Trigger Reverse Engineering開始***
Target: 7, victim: 2, Loss: 2.3866, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:41.25, Cost:0.06 best_reg:42.38 avg_loss_reg:42.38:   8%|▊         | 79/1000 [02:57<34:24,  2.24s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 2 Trigger Size: 41.25117874145508 Optimization Steps: 69
***Symmetric Check開始***
Target: 2, victim: 7, Loss: 1.2989, Acc: 95.00%, CE_Loss: 0.46, Reg_Loss:2846.08, Cost:0.00 best_reg:6141.67 avg_loss_reg:2873.37: 100%|██████████| 69/69 [02:32<00:00,  2.21s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 336.5531601905823
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000405----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.637441873550415
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000406----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-3']
***Trigger Reverse Engineering開始***
Target: 4, victim: 3, Loss: 7.1372, Acc: 10.00%, CE_Loss: 7.14, Reg_Loss:3155.50, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2996.66:   2%|▏         | 20/1000 [00:06<05:36,  2.91it/s]
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 3 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 12.280215501785278
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000407----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-3', '0-5', '0-9', '9-0', '9-3']
***Trigger Reverse Engineering開始***
Target: 9, victim: 3, Loss: 8.9303, Acc: 0.00%, CE_Loss: 8.93, Reg_Loss:2566.66, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2551.13:   5%|▌         | 54/1000 [00:25<07:24,  2.13it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 3 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 31.771421909332275
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000408----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
```

```
檢測結果: Model是安全的(Benign)
整體耗時: 12.038453817367554
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000409----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.768537282943726
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000410----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-4', '3-5', '4-3']
***Trigger Reverse Engineering開始***
Target: 3, victim: 5, Loss: 1.4301, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:171.93, Cost:0.01 best_reg:172.52 avg_loss_reg:172.18:  12%|          | 117/1000 [00:14<01:47,  8.19it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 5 Trigger Size: 171.92515563964844 Optimization Steps: 100
***Symmetric Check開始***
Target: 5, victim: 3, Loss: 1.8552, Acc: 50.00%, CE_Loss: 1.86, Reg_Loss:9442.78, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:9370.38: 100%|| 100/100 [00:12<00:00,  8.28it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 28.233701467514038
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000411----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.866551876068115
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000412----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 9, Loss: 0.1640, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:109.36, Cost:0.00 best_reg:119.03 avg_loss_reg:108.64:   5%|          | 54/1000 [00:42<12:26,  1.27it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 119.02754974365234 Optimization Steps: 55
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 46.95885968208313
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000413----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-5', '3-0', '3-5', '4-8', '5-2', '5-3', '7-8', '7-9', '10-0']
***Trigger Reverse Engineering開始***
Target: 7, victim: 9, Loss: 3.1831, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:267.62, Cost:0.01 best_reg:270.47 avg_loss_reg:266.60:  30%|       | 299/1000 [00:36<01:24,  8.26it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 9 Trigger Size: 267.62371826171875 Optimization Steps: 144
***Symmetric Check開始***
Target: 9, victim: 7, Loss: 3.6260, Acc: 20.00%, CE_Loss: 1.38, Reg_Loss:7591.18, Cost:0.00 best_reg:14895.91 avg_loss_reg:7643.52: 100%| 144/144 [00:17<00:00,  8.25it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 58.883779525756836
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000414----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 14.39618968963623
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000415----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
```

```
整體耗時: 13.509204149246216
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000416----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.237755298614502
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000417----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '2-3', '4-1', '10-3', '12-1', '12-5', '12-16', '17-16']
***Trigger Reverse Engineering開始***
Target: 17, victim: 16, Loss: 10.2244, Acc: 0.00%, CE_Loss: 10.22, Reg_Loss:2563.50, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2548.03:  10%|         | 97/1000 [00:11<01:51,  8.11it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 17.779464721679688
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000418----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-18', '2-16', '18-1']
***Trigger Reverse Engineering開始***
Target: 18, victim: 1, Loss: 8.7006, Acc: 0.00%, CE_Loss: 8.70, Reg_Loss:2539.63, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2529.47:   4%|         | 42/1000 [00:13<05:11,  3.08it/s]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 18 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 20.849449396133423
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000419----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.909383773803711
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000420----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 1
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 1, victim: 12, Loss: 0.4286, Acc: 96.88%, CE_Loss: 0.13, Reg_Loss:5022.23, Cost:0.00 best_reg:4718.50 avg_loss_reg:5132.37:   9%|         | 89/1000 [12:42<2:10:04,  8.57s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 4718.504296875 Optimization Steps: 90
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 772.5430574417114
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000421----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.237573146820068
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000422----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '1-0', '3-0', '3-8', '5-21', '10-1', '10-14', '17-8', '20-0', '22-0', '23-0', '23-1']
***Trigger Reverse Engineering開始***
Target: 0, victim: 1, Loss: 1.0628, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:255.48, Cost:0.00 best_reg:255.68 avg_loss_reg:256.08:  41%|     | 408/1000 [00:34<00:50, 11.70it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 255.48068237304688 Optimization Steps: 196
***Symmetric Check開始***
Target: 1, victim: 0, Loss: 1.7400, Acc: 90.00%, CE_Loss: 0.33, Reg_Loss:278.34, Cost:0.01 best_reg:284.07 avg_loss_reg:279.10: 100%|| 196/196 [00:16<00:00, 11.88it/s]
***Symmetric Check結束***
**********檢測結束**********
```

```
檢測結果: Model是安全的(Benign)
整體耗時: 57.083882093429565
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000423----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 3
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 3, victim: 16, Loss: 0.9905, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:57.97, Cost:0.02 best_reg:58.31 avg_loss_reg:58.15:  10%|          | 100/1000 [31:29<4:43:29, 18.90s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: all Trigger Size: 58.17532857259115 Optimization Steps: 101
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1905.0320341587067
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000424----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 9
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 9, victim: 9, Loss: 0.1102, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:246.55, Cost:0.00 best_reg:254.01 avg_loss_reg:244.57:   5%|          | 53/1000 [05:41<1:41:40,  6.44s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: all Trigger Size: 254.0085950578962 Optimization Steps: 54
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 353.878351688385
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000425----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 17.767489671707153
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000426----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-7', '7-1']
***Trigger Reverse Engineering開始***
Target: 7, victim: 1, Loss: 9.5066, Acc: 0.00%, CE_Loss: 9.51, Reg_Loss:2551.13, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2538.44:   3%|          | 31/1000 [00:02<01:11, 13.64it/s]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 7 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 6.997875928878784
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000427----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.52353811264038
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000428----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.410531759262085
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000429----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '1-2', '2-1', '5-7']
***Trigger Reverse Engineering開始***
Target: 2, victim: 1, Loss: 2.8085, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:20.10, Cost:0.13 best_reg:20.13 avg_loss_reg:20.49:  15%|          | 149/1000 [07:27<42:34,  3.00s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 20.09794044494629 Optimization Steps: 96
***Symmetric Check開始***
```

```
Target: 1, victim: 2, Loss: 0.1070, Acc: 95.00%, CE_Loss: 0.11, Reg_Loss:11699.47, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:11596.09: 100%|██████████| 96/96 [04:46<00:00,  2.99s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 752.6907222270966
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000430----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 15.926489114761353
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000431----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.127343416213989
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000432----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 0
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 0, victim: 12, Loss: 2.3083, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:5166.56, Cost:0.00 best_reg:5139.15 avg_loss_reg:5144.94:  10%|▉         | 96/1000 [27:08<4:15:33, 16.96s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 5139.151953125 Optimization Steps: 97
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1640.0265655517578
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000433----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-7', '12-2', '12-6', '12-7']
***Trigger Reverse Engineering開始***
Target: 12, victim: 7, Loss: 0.9666, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:11.17, Cost:0.09 best_reg:11.92 avg_loss_reg:11.92:  10%|▉         | 104/1000 [00:07<01:02, 14.45it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 7 Trigger Size: 11.17060661315918 Optimization Steps: 72
***Symmetric Check開始***
Target: 7, victim: 12, Loss: 2.5084, Acc: 100.00%, CE_Loss: 0.40, Reg_Loss:4742.68, Cost:0.00 best_reg:7876.27 avg_loss_reg:4828.02: 100%|██████████| 72/72 [00:04<00:00, 15.11it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 16.65692925453186
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000434----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-1']
***Trigger Reverse Engineering開始***
Target: 2, victim: 1, Loss: 6.9982, Acc: 10.00%, CE_Loss: 7.00, Reg_Loss:4033.58, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3634.46:   2%|▏         | 20/1000 [01:23<1:08:26,  4.19s/it]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 92.40736222267151
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000435----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.887247800827026
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000436----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-6', '1-7', '1-8', '3-5', '6-5', '8-7', '10-0']
***Trigger Reverse Engineering開始***
```

```
Target: 1, victim: 6, Loss: 2.0491, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:252.65, Cost:0.01 best_reg:253.94 avg_loss_reg:249.45:  24%|     | 240/1000 [00:29<01:32,  8.23it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 6 Trigger Size: 252.6473388671875 Optimization Steps: 120
***Symmetric Check開始***
Target: 6, victim: 1, Loss: 2.2023, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:1898.09, Cost:0.00 best_reg:1950.49 avg_loss_reg:1950.49: 100%|| 120/120 [00:14<00:00,  8.33it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 48.54423785209656
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000437----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.665287733078003
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000438----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-18', '18-1']
***Trigger Reverse Engineering開始***
Target: 18, victim: 1, Loss: 4.1972, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:775.25, Cost:0.01 best_reg:784.13 avg_loss_reg:786.13:  28%|     | 280/1000 [02:54<07:27,  1.61it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 18 Victim Class: 1 Trigger Size: 775.2532958984375 Optimization Steps: 202
***Symmetric Check開始***
Target: 1, victim: 18, Loss: 0.5824, Acc: 95.00%, CE_Loss: 0.14, Reg_Loss:669.40, Cost:0.00 best_reg:676.06 avg_loss_reg:668.62: 100%|| 202/202 [02:05<00:00,  1.61it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 306.3106610774994
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000439----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['13-1']
***Trigger Reverse Engineering開始***
Target: 13, victim: 1, Loss: 5.6023, Acc: 0.00%, CE_Loss: 5.60, Reg_Loss:2536.24, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2527.87:   1%|         | 10/1000 [00:01<02:46,  5.94it/s]
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 6.431513071060181
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000440----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-1', '15-18', '19-10', '20-0']
***Trigger Reverse Engineering開始***
Target: 20, victim: 0, Loss: 7.6356, Acc: 5.00%, CE_Loss: 7.64, Reg_Loss:3740.49, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3413.21:   6%|         | 63/1000 [00:20<05:01,  3.11it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 26.27037024497986
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000441----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.197281837463379
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000442----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '2-1', '2-3']
***Trigger Reverse Engineering開始***
Target: 2, victim: 3, Loss: 1.6487, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:457.70, Cost:0.00 best_reg:459.04 avg_loss_reg:463.26:  41%|     | 410/1000 [21:54<31:31,  3.21s/it]
early stop 所有
***Trigger Reverse Engineering結束***
```

```
Target Class: 2 Victim Class: 3 Trigger Size: 457.69580078125 Optimization Steps: 337
***Symmetric Check開始***
Target: 3, victim: 2, Loss: 1.4711, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:6887.11, Cost:0.00 best_reg:6785.85 avg_loss_reg:6881.59: 100%|[redacted]| 337/337 [18:38<00:00,  3.32s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 2443.038028717041
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000443----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-0', '9-8']
***Trigger Reverse Engineering開始***
Target: 9, victim: 8, Loss: 6.6005, Acc: 0.00%, CE_Loss: 6.60, Reg_Loss:2557.31, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2543.30:   2%|         | 21/1000 [00:02<02:06,  7.74it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 7.605119943618774
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000444----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-10', '3-12', '7-3', '8-3', '10-14', '11-1', '14-15', '16-12', '16-6', '16-11', '17-1']
***Trigger Reverse Engineering開始***
Target: 16, victim: 12, Loss: 0.4516, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:182.44, Cost:0.00 best_reg:183.94 avg_loss_reg:183.94:  28%|[redacted]       | 279/1000 [05:36<14:29,  1.21s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 16 Victim Class: 12 Trigger Size: 182.4385986328125 Optimization Steps: 144
***Symmetric Check開始***
Target: 12, victim: 16, Loss: 0.7762, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:1603.96, Cost:0.00 best_reg:1609.60 avg_loss_reg:1625.29: 100%|[redacted]| 144/144 [03:00<00:00,  1.25s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 523.8364114761353
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000445----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 10
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 10, victim: 19, Loss: 0.4989, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:5138.34, Cost:0.00 best_reg:33452.80 avg_loss_reg:5059.68:   3%|          | 34/1000 [10:51<5:08:40, 19.17s/it]
Traceback (most recent call last):
  File "D:\UULi\test_code\k_arm_test\main.py", line 158, in <module>
    trigger_reverse_engineering(target_classes, victim_classes, backdoor_type, model, DATA_PATH,
  File "D:\UULi\test_code\k_arm_test\k_arm\reverse.py", line 54, in trigger_reverse_engineering
    pattern, mask, l1_norm, time_cost = scanner.scanning(
  File "D:\UULi\test_code\k_arm_test\k_arm\scanner.py", line 123, in scanning
    for images, labels in data_loaders[target_index]:
  File "C:\Users\islab\anaconda3\envs\pytorch1\lib\site-packages\torch\utils\data\dataloader.py", line 435, in __next__
    data = self._next_data()
  File "C:\Users\islab\anaconda3\envs\pytorch1\lib\site-packages\torch\utils\data\dataloader.py", line 475, in _next_data
    data = self._dataset_fetcher.fetch(index)  # may raise StopIteration
  File "C:\Users\islab\anaconda3\envs\pytorch1\lib\site-packages\torch\utils\data\_utils\fetch.py", line 44, in fetch
    data = [self.dataset[idx] for idx in possibly_batched_index]
  File "C:\Users\islab\anaconda3\envs\pytorch1\lib\site-packages\torch\utils\data\_utils\fetch.py", line 44, in <listcomp>
    data = [self.dataset[idx] for idx in possibly_batched_index]
  File "D:\UULi\test_code\k_arm_test\k_arm\dataset.py", line 35, in __getitem__
    image = Image.open(img_path).convert('RGB')
  File "C:\Users\islab\anaconda3\envs\pytorch1\lib\site-packages\PIL\Image.py", line 937, in convert
    self.load()
  File "C:\Users\islab\anaconda3\envs\pytorch1\lib\site-packages\PIL\ImageFile.py", line 269, in load
    n, err_code = decoder.decode(b)
KeyboardInterrupt

Process finished with exit code -1073741510 (0xC000013A: interrupted by Ctrl+C)
```