```
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: 1.2152, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:126.82, Cost:0.01 best_reg:128.16 avg_loss_reg:128.16:  20%|██        | 199/1000 [01:35<06:23,  2.09it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 7 Trigger Size: 126.82107543945312 Optimization Steps: 175
***Symmetric Check開始***
Target: 7, victim: 0, Loss: 1.3250, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:1037.77, Cost:0.00 best_reg:1023.94 avg_loss_reg:1037.90: 100%|██████████| 175/175 [00:41<00:00,  4.19it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 143.3811902999878
----------------------------------------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 [53:03<4:38:35, 19.90s/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: 3192.053612947464
----------------------------------------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: 17.16268491744995
----------------------------------------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: 1, victim: 6, Loss: 7.0571, Acc: 100.00%, CE_Loss: 0.37, Reg_Loss:586.96, Cost:0.01 best_reg:587.16 avg_loss_reg:587.16:  19%|██        | 186/1000 [00:22<01:40,  8.11it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 6 Trigger Size: 586.9552001953125 Optimization Steps: 143
***Symmetric Check開始***
Target: 6, victim: 1, Loss: 2.3611, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:4602.23, Cost:0.00 best_reg:4594.92 avg_loss_reg:4610.98: 100%|██████████| 143/143 [00:17<00:00,  8.13it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 47.97521257400513
----------------------------------------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: 2.0957, Acc: 15.00%, CE_Loss: 2.10, Reg_Loss:10596.28, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:10290.79:   2%|          | 20/1000 [00:01<01:36, 10.14it/s]
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 14 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: 9.749948740005493
----------------------------------------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 [32:50<4:12:42, 17.13s/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: 1981.7125210762024
----------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 [13:09<3:09:13, 12.14s/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: 796.867960691452
----------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: 12.8278, Acc: 0.00%, CE_Loss: 12.83, Reg_Loss:4661.28, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:4187.59:   3%|          | 31/1000 [00:04<02:18,  6.99it/s]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 20 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: 13.618326187133789
----------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: 20.378050804138184
----------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 [1:13:08<8:27:22, 34.83s/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: 4404.524069309235
----------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: 7.029834508895874
----------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: 11.033855676651001
----------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: 19.06214928627014
----------------------------------------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: 10, Loss: 2.2766, Acc: 80.00%, CE_Loss: 0.52, Reg_Loss:347.43, Cost:0.01 best_reg:369.78 avg_loss_reg:347.94: 100%|[redacted]| 1000/1000 [05:50<00:00,  2.85it/s]
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 10 Trigger Size: 369.7843322753906 Optimization Steps: 737
***Symmetric Check開始***
Target: 10, victim: 11, Loss: 1.9861, Acc: 100.00%, CE_Loss: 0.47, Reg_Loss:3406.63, Cost:0.00 best_reg:3517.16 avg_loss_reg:3389.91:  37%|[redacted]      | 270/737 [01:36<02:46,  2.80it/s]
early stop 所有
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 455.95215368270874
----------------------------------------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: 11.162314891815186
----------------------------------------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: 7.533128499984741
----------------------------------------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: 18.214077949523926
----------------------------------------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: 7.3451619148254395
----------------------------------------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: 17.032463312149048
----------------------------------------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: 15.84819483757019
----------------------------------------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: 3.020597457885742
----------------------------------------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: 11.349288940429688
----------------------------------------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: 2.1971, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:52.02, Cost:0.04 best_reg:52.26 avg_loss_reg:49.73:  92%|[redacted] | 921/1000 [01:09<00:05, 13.30it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 6 Trigger Size: 52.01518249511719 Optimization Steps: 99
***Symmetric Check開始***
Target: 6, victim: 5, Loss: 3.0382, Acc: 90.00%, CE_Loss: 0.36, Reg_Loss:2680.72, Cost:0.00 best_reg:2704.34 avg_loss_reg:2704.34: 100%|[redacted]| 99/99 [00:07<00:00, 13.36it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 82.72049069404602
----------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: 9, victim: 6, Loss: 1.9746, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:2619.71, Cost:0.00 best_reg:2606.74 avg_loss_reg:2623.04: 100%|[redacted]| 1000/1000 [03:55<00:00,  4.24it/s]
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 6 Trigger Size: 2606.74072265625 Optimization Steps: 844
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 243.1950716972351
----------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: 10.0454, Acc: 0.00%, CE_Loss: 10.05, Reg_Loss:9443.11, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:8184.87:   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: 91.67607402801514
----------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: 6.068888425827026
----------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: 9.1888, Acc: 0.00%, CE_Loss: 9.19, Reg_Loss:5686.14, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:5189.52:   3%|          | 32/1000 [00:04<02:29,  6.46it/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: 11.62276577949524
----------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 [42:35<10:55:42, 41.90s/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: 2576.4609031677246
----------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: 1.1946, Acc: 100.00%, CE_Loss: 0.34, Reg_Loss:856.11, Cost:0.00 best_reg:825.53 avg_loss_reg:849.33: 100%|██████████| 1000/1000 [47:38<00:00,  2.86s/it]
  0%|          | 0/1000 [00:00<?, ?it/s]***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 8 Trigger Size: 825.5343017578125 Optimization Steps: 1000
***Symmetric Check開始***
Target: 8, victim: 2, Loss: 0.4777, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:4076.33, Cost:0.00 best_reg:4082.44 avg_loss_reg:4068.14:  60%|██████    | 598/1000 [28:32<19:11,  2.86s/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: 4586.448591709137
----------------------------------------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: 9.3851, Acc: 0.00%, CE_Loss: 9.39, Reg_Loss:8232.51, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:7180.10:   2%|▏         | 21/1000 [00:03<02:32,  6.43it/s]
***Trigger Reverse Engineering結束***
Target Class: 8 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: 9.702200174331665
----------------------------------------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: 3.1035, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:6496.22, Cost:0.00 best_reg:6508.56 avg_loss_reg:6591.90:  39%|███▉      | 386/1000 [01:45<02:48,  3.65it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 1 Trigger Size: 6496.22265625 Optimization Steps: 355
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 112.96368670463562
----------------------------------------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: 2.8234, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:1153.52, Cost:0.00 best_reg:1153.74 avg_loss_reg:1170.53:  52%|█████▏    | 525/1000 [19:16<17:26,  2.20s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 3 Trigger Size: 1153.5166015625 Optimization Steps: 494
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1166.993456363678
----------------------------------------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: 8, Loss: 4.1474, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:102.63, Cost:0.04 best_reg:102.68 avg_loss_reg:102.94:  37%|███▋      | 367/1000 [08:05<13:56,  1.32s/it]
  0%|          | 0/328 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 8 Trigger Size: 102.63076782226562 Optimization Steps: 328
***Symmetric Check開始***
Target: 8, victim: 2, Loss: 1.3894, Acc: 90.00%, CE_Loss: 0.53, Reg_Loss:858.46, Cost:0.00 best_reg:854.27 avg_loss_reg:852.34: 100%|██████████| 328/328 [07:10<00:00,  1.31s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 928.2576055526733
----------------------------------------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: 11.457124948501587
```

```
----------------------------------------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: 7.0207507610321045
----------------------------------------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: 6.862086057662964
----------------------------------------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: 8, victim: 1, Loss: 0.7839, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:3420.82, Cost:0.00 best_reg:3425.66 avg_loss_reg:3417.02:  82%|████████▏ | 816/1000 [1:01:43<13:55,  4.54s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 1 Trigger Size: 3420.816162109375 Optimization Steps: 360
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 3728.9489817619324
----------------------------------------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: 3.2437, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:122.09, Cost:0.03 best_reg:123.58 avg_loss_reg:123.58:  13%|▏         | 129/1000 [00:45<05:07,  2.83it/s]
  0%|          | 0/119 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 4 Trigger Size: 122.093017578125 Optimization Steps: 119
***Symmetric Check開始***
Target: 4, victim: 14, Loss: 2.0966, Acc: 95.00%, CE_Loss: 0.49, Reg_Loss:5436.89, Cost:0.00 best_reg:6240.88 avg_loss_reg:5482.51: 100%|██████████| 119/119 [00:41<00:00,  2.84it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 95.08255219459534
----------------------------------------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: 17.49670171737671
----------------------------------------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: 1, victim: 5, Loss: 11.0995, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:187.10, Cost:0.06 best_reg:187.90 avg_loss_reg:187.90:  13%|▏         | 132/1000 [00:11<01:12, 11.89it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 5 Trigger Size: 187.09918212890625 Optimization Steps: 88
***Symmetric Check開始***
Target: 5, victim: 1, Loss: 2.9641, Acc: 100.00%, CE_Loss: 0.49, Reg_Loss:1100.89, Cost:0.00 best_reg:1134.87 avg_loss_reg:1111.82: 100%|██████████| 88/88 [00:06<00:00, 12.86it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 24.501861095428467
----------------------------------------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 [27:53<4:00:15, 16.09s/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: 1683.2260296344757
----------------------------------------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: 0, victim: 20, Loss: 0.8362, Acc: 95.00%, CE_Loss: 0.15, Reg_Loss:1024.87, Cost:0.00 best_reg:1035.90 avg_loss_reg:1019.59: 100%|██████████| 1000/1000 [04:18<00:00,  3.87it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 20 Trigger Size: 1035.896728515625 Optimization Steps: 253
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 267.22953629493713
----------------------------------------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: 1.2234, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:28.89, Cost:0.04 best_reg:29.29 avg_loss_reg:29.29:  13%|█▎        | 133/1000 [07:51<51:12,  3.54s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 10 Trigger Size: 28.88616943359375 Optimization Steps: 101
***Symmetric Check開始***
Target: 10, victim: 4, Loss: 1.3092, Acc: 90.00%, CE_Loss: 0.50, Reg_Loss:6149.09, Cost:0.00 best_reg:13050.65 avg_loss_reg:6123.76: 100%|██████████| 101/101 [05:52<00:00,  3.49s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 840.2945759296417
----------------------------------------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: 12.33970832824707
----------------------------------------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: 9.3379, Acc: 0.00%, CE_Loss: 9.34, Reg_Loss:7412.15, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:6636.06:   1%|          | 10/1000 [00:04<06:39,  2.48it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 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: 10.744796514511108
----------------------------------------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: 17.440627574920654
----------------------------------------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: 6.48016095161438
----------------------------------------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: 6.277478456497192
----------------------------------------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: 2.6458, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:93.91, Cost:0.03 best_reg:94.40 avg_loss_reg:95.16:  15%|          | 150/1000 [02:26<13:50,  1.02it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 7 Trigger Size: 93.91307067871094 Optimization Steps: 151
***Symmetric Check開始***
Target: 7, victim: 5, Loss: 2.7724, Acc: 90.00%, CE_Loss: 0.50, Reg_Loss:2272.82, Cost:0.00 best_reg:2371.15 avg_loss_reg:2278.85: 100%|| 151/151 [02:19<00:00,  1.08it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 298.35584568977356
----------------------------------------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: 3, victim: 2, Loss: 1.3675, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:355.85, Cost:0.00 best_reg:358.17 avg_loss_reg:358.17:  19%|          | 187/1000 [00:20<01:27,  9.29it/s]
  0%|          | 0/177 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 2 Trigger Size: 355.851806640625 Optimization Steps: 177
***Symmetric Check開始***
Target: 2, victim: 3, Loss: 3.0817, Acc: 90.00%, CE_Loss: 0.68, Reg_Loss:1068.52, Cost:0.00 best_reg:1072.62 avg_loss_reg:1068.78: 100%|| 177/177 [00:16<00:00, 10.54it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 43.169769048690796
----------------------------------------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: 6.67685866355896
----------------------------------------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: 9.778457880020142
----------------------------------------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: 2.9305, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:33.25, Cost:0.09 best_reg:33.77 avg_loss_reg:33.77:  18%|          | 182/1000 [00:55<04:08,  3.29it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 6 Trigger Size: 33.24592208862305 Optimization Steps: 77
***Symmetric Check開始***
Target: 6, victim: 2, Loss: 1.3824, Acc: 100.00%, CE_Loss: 0.52, Reg_Loss:9792.31, Cost:0.00 best_reg:9257.17 avg_loss_reg:9785.06: 100%|| 77/77 [00:23<00:00,  3.31it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 85.99053597450256
----------------------------------------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 [2:11:04<11:03:21, 47.67s/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: 7882.579081535339
----------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: 15.206706047058105
----------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: 2.1084, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:869.05, Cost:0.00 best_reg:872.22 avg_loss_reg:872.22:  20%|██        | 196/1000 [00:34<02:22,  5.63it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 12 Trigger Size: 869.0472412109375 Optimization Steps: 197
***Symmetric Check開始***
Target: 12, victim: 14, Loss: 3.9850, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:493.30, Cost:0.01 best_reg:493.49 avg_loss_reg:494.81:  67%|██████▋   | 132/197 [00:23<00:11,  5.66it/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: 65.45136713981628
----------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: 7, Loss: 3.0634, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:375.17, Cost:0.01 best_reg:375.33 avg_loss_reg:377.98:  44%|████▍     | 442/1000 [01:00<01:16,  7.28it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 7 Trigger Size: 375.1672668457031 Optimization Steps: 198
***Symmetric Check開始***
Target: 7, victim: 1, Loss: 0.3828, Acc: 90.00%, CE_Loss: 0.38, Reg_Loss:16837.65, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:16780.40: 100%|██████████| 198/198 [00:29<00:00,  6.63it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 97.91662311553955
----------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: 1.7425, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:1598.79, Cost:0.00 best_reg:1599.59 avg_loss_reg:1601.99:  33%|███▎      | 327/1000 [01:11<02:26,  4.58it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 1 Trigger Size: 1598.789306640625 Optimization Steps: 328
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 79.20686292648315
----------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: 8, victim: 1, Loss: 1.1323, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:2106.23, Cost:0.00 best_reg:2106.46 avg_loss_reg:2116.32:  45%|████▌     | 450/1000 [02:13<02:42,  3.38it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 1 Trigger Size: 2106.2275390625 Optimization Steps: 341
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 141.95744490623474
----------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: 15.082679986953735
----------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: 9.7215, Acc: 20.00%, CE_Loss: 9.72, Reg_Loss:8111.38, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:7699.41:  10%|          | 104/1000 [06:08<52:58,  3.55s/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: 387.7729549407959
----------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: 2.1712, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:116.54, Cost:0.02 best_reg:117.78 avg_loss_reg:115.16:  31%|          | 311/1000 [00:47<01:44,  6.58it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 3 Trigger Size: 116.53671264648438 Optimization Steps: 160
***Symmetric Check開始***
Target: 3, victim: 12, Loss: 1.6584, Acc: 90.00%, CE_Loss: 0.32, Reg_Loss:593.10, Cost:0.00 best_reg:612.83 avg_loss_reg:595.38: 100%|          | 160/160 [00:24<00:00,  6.41it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 78.82564687728882
----------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: 1, victim: 22, Loss: 4.5194, Acc: 100.00%, CE_Loss: 0.38, Reg_Loss:818.42, Cost:0.01 best_reg:807.95 avg_loss_reg:818.14: 100%|          | 1000/1000 [01:45<00:00,  9.46it/s]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 22 Trigger Size: 807.9522094726562 Optimization Steps: 385
***Symmetric Check開始***
Target: 22, victim: 1, Loss: 2.9883, Acc: 100.00%, CE_Loss: 0.38, Reg_Loss:343.09, Cost:0.01 best_reg:345.20 avg_loss_reg:344.14:  70%|          | 271/385 [00:34<00:14,  7.94it/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: 146.68693208694458
----------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: 2, victim: 1, Loss: 1.7349, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:688.51, Cost:0.00 best_reg:666.02 avg_loss_reg:689.23: 100%|          | 1000/1000 [02:08<00:00,  7.81it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 666.021728515625 Optimization Steps: 601
***Symmetric Check開始***
Target: 1, victim: 2, Loss: 1.4397, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:374.66, Cost:0.00 best_reg:389.78 avg_loss_reg:372.44:  21%|          | 128/601 [00:16<00:59,  7.99it/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: 150.4124014377594
----------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 [29:25<5:33:45, 21.79s/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: 1774.000016450882
----------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: 18.231248140335083
----------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: 1.9397, Acc: 20.00%, CE_Loss: 1.94, Reg_Loss:9182.88, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:8865.10:   2%|         | 20/1000 [00:16<13:25,  1.22it/s]
***Trigger Reverse Engineering結束***
Target Class: 7 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: 27.21014904975891
----------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 [1:15:06<16:37:58, 64.39s/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: 4533.974607229233
----------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 [21:06<2:44:06, 11.11s/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: 1274.459157705307
----------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: 2.2120, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:77.73, Cost:0.03 best_reg:79.74 avg_loss_reg:79.74:  14%|▉         | 144/1000 [00:22<02:13,  6.39it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 13 Trigger Size: 77.72793579101562 Optimization Steps: 94
***Symmetric Check開始***
Target: 13, victim: 4, Loss: 1.6180, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:6628.50, Cost:0.00 best_reg:6571.07 avg_loss_reg:6684.57: 100%|██████████| 94/94 [00:15<00:00,  6.26it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 45.588940143585205
----------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: 14.260638236999512
----------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: 13.7104651927948
----------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: 3.4264, Acc: 100.00%, CE_Loss: 0.44, Reg_Loss:262.37, Cost:0.01 best_reg:263.63 avg_loss_reg:263.63:  15%|          | 153/1000 [00:19<01:49,  7.72it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 2 Trigger Size: 262.37188720703125 Optimization Steps: 154
***Symmetric Check開始***
Target: 2, victim: 1, Loss: 2.7897, Acc: 100.00%, CE_Loss: 0.34, Reg_Loss:727.15, Cost:0.00 best_reg:724.93 avg_loss_reg:726.05: 100%|| 154/154 [00:20<00:00,  7.67it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 46.706992864608765
----------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: 10.553327798843384
----------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 [10:04<3:11:23, 12.09s/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: 610.8321437835693
----------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: 3, Loss: 6.3245, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:105.18, Cost:0.06 best_reg:105.94 avg_loss_reg:105.94:  12%|          | 119/1000 [00:12<01:29,  9.82it/s]
  0%|          | 0/93 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 3 Trigger Size: 105.18342590332031 Optimization Steps: 93
***Symmetric Check開始***
Target: 3, victim: 5, Loss: 5.7649, Acc: 90.00%, CE_Loss: 0.46, Reg_Loss:3534.16, Cost:0.00 best_reg:3607.45 avg_loss_reg:3607.45: 100%|| 93/93 [00:09<00:00,  9.97it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 27.79301691055298
----------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: 2.5488, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:1030.73, Cost:0.00 best_reg:1030.82 avg_loss_reg:1061.13:  38%|          | 378/1000 [03:19<05:27,  1.90it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 9 Trigger Size: 1030.734619140625 Optimization Steps: 379
**********檢測結束**********
```

```
檢測結果: Model是安全的(Benign)
整體耗時: 207.6089973449707
----------------------------------------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: 6.6446568965911865
----------------------------------------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: 12.439175367355347
----------------------------------------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: 9, victim: 1, Loss: 0.9025, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:4501.87, Cost:0.00 best_reg:4506.67 avg_loss_reg:4512.84:  61%|[redacted]  | 611/1000 [34:53<22:12,  3.43s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 1 Trigger Size: 4501.8662109375 Optimization Steps: 591
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 2115.706630706787
----------------------------------------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: 1.4792, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:6869.00, Cost:0.00 best_reg:6873.51 avg_loss_reg:6873.51:  56%|[redacted]  | 565/1000 [31:56<24:35,  3.39s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 10 Trigger Size: 6869.001953125 Optimization Steps: 394
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1937.7479786872864
----------------------------------------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: 15.795825004577637
----------------------------------------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 [03:54<3:46:15, 13.81s/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: 242.2243571281433
----------------------------------------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: 0.8094, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:311.98, Cost:0.00 best_reg:313.97 avg_loss_reg:313.97:  15%|[redacted]  | 146/1000 [00:18<01:47,  7.94it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 7 Trigger Size: 311.98199462890625 Optimization Steps: 147
***Symmetric Check開始***
```

```
Target: 7, victim: 2, Loss: 0.9666, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:1638.13, Cost:0.00 best_reg:1666.78 avg_loss_reg:1666.78: 100%|██████████| 147/147 [00:17<00:00,  8.46it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 42.177544832229614
----------------------------------------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 [38:08<5:21:40, 21.59s/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: 2296.520660877228
----------------------------------------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: 19, victim: 18, Loss: 1.4830, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:1167.94, Cost:0.00 best_reg:1182.68 avg_loss_reg:1171.06:  41%|████      | 409/1000 [24:45<35:47,  3.63s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 19 Victim Class: 18 Trigger Size: 1167.9443359375 Optimization Steps: 205
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1512.9597244262695
----------------------------------------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: 17.805039882659912
----------------------------------------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: 6.194135665893555
----------------------------------------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: 4, Loss: 4.4473, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:73.16, Cost:0.06 best_reg:73.45 avg_loss_reg:73.45:  50%|█████     | 496/1000 [01:14<01:15,  6.67it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 18 Victim Class: 4 Trigger Size: 73.15617370605469 Optimization Steps: 81
***Symmetric Check開始***
Target: 4, victim: 18, Loss: 0.5927, Acc: 80.00%, CE_Loss: 0.59, Reg_Loss:29864.18, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:29799.39: 100%|██████████| 81/81 [00:14<00:00,  5.74it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 95.38706994056702
----------------------------------------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 [07:45<4:39:32, 17.24s/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: 474.0966110229492
----------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: 5.0626, Acc: 100.00%, CE_Loss: 0.37, Reg_Loss:926.21, Cost:0.01 best_reg:927.14 avg_loss_reg:927.14:  19%|██        | 187/1000 [00:37<02:41,  5.03it/s]
  0%|          | 0/188 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 0 Trigger Size: 926.2102661132812 Optimization Steps: 188
***Symmetric Check開始***
Target: 0, victim: 1, Loss: 6.2260, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:1739.66, Cost:0.00 best_reg:1739.85 avg_loss_reg:1739.85:  76%|███████▌  | 143/188 [00:27<00:08,  5.18it/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: 71.55773138999939
----------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: 7.3559253215789795
----------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: 2.8211, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:2600.79, Cost:0.00 best_reg:2554.50 avg_loss_reg:2552.52: 100%|██████████| 1000/1000 [11:44<00:00,  1.42it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 5 Trigger Size: 2554.49853515625 Optimization Steps: 1000
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 712.7076923847198
----------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: 9.5290, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:242.52, Cost:0.04 best_reg:243.42 avg_loss_reg:240.30:  14%|█         | 141/1000 [00:23<02:23,  6.00it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 13 Trigger Size: 242.5188751220703 Optimization Steps: 120
***Symmetric Check開始***
Target: 13, victim: 11, Loss: 4.4305, Acc: 100.00%, CE_Loss: 0.53, Reg_Loss:1154.45, Cost:0.00 best_reg:1151.29 avg_loss_reg:1154.90: 100%|██████████| 120/120 [00:20<00:00,  5.82it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 51.25985503196716
----------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: 9, victim: 19, Loss: 1.4410, Acc: 90.00%, CE_Loss: 0.75, Reg_Loss:2331.50, Cost:0.00 best_reg:2390.04 avg_loss_reg:2325.86: 100%|██████████| 1000/1000 [18:32<00:00,  1.11s/it]
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 19 Trigger Size: 2390.04443359375 Optimization Steps: 528
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1127.5095200538635
----------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: 13.6150, Acc: 0.00%, CE_Loss: 13.62, Reg_Loss:5354.46, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:4800.22:   3%|▌         | 32/1000 [00:19<09:57,  1.62it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 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: 23.362310647964478
----------------------------------------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: 1.7051, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:1068.46, Cost:0.00 best_reg:1069.58 avg_loss_reg:1069.70:  18%|██        | 183/1000 [00:38<02:53,  4.71it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 3 Trigger Size: 1068.4608154296875 Optimization Steps: 184
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 42.21012806892395
----------------------------------------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: 18.003498315811157
----------------------------------------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: 1.7547, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:324.98, Cost:0.01 best_reg:326.56 avg_loss_reg:326.56:  44%|████▍     | 440/1000 [00:58<01:13,  7.58it/s]
  0%|          | 0/146 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 7 Trigger Size: 324.9828796386719 Optimization Steps: 146
***Symmetric Check開始***
Target: 7, victim: 1, Loss: 4.0716, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:334.25, Cost:0.01 best_reg:335.66 avg_loss_reg:335.66:  69%|██████▉   | 101/146 [00:15<00:06,  6.58it/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: 80.1291229724884
----------------------------------------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: 2, victim: 7, Loss: 2.6102, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:2426.16, Cost:0.00 best_reg:2426.65 avg_loss_reg:2427.65:  41%|████      | 414/1000 [02:22<03:22,  2.90it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 7 Trigger Size: 2426.15771484375 Optimization Steps: 365
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 150.3266522884369
----------------------------------------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: 20.945130109786987
----------------------------------------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%|▎         | 30/1000 [08:57<4:49:27, 17.90s/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: 546.2802238464355
----------------------------------------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: 3.8521, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:42.26, Cost:0.09 best_reg:43.79 avg_loss_reg:42.37:   9%|▉         | 88/1000 [00:48<08:23,  1.81it/s]
  0%|          | 0/73 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 2 Trigger Size: 42.26390075683594 Optimization Steps: 73
***Symmetric Check開始***
Target: 2, victim: 6, Loss: 1.4916, Acc: 90.00%, CE_Loss: 0.58, Reg_Loss:4612.52, Cost:0.00 best_reg:10515.01 avg_loss_reg:4601.79: 100%|██████████| 73/73 [00:43<00:00,  1.69it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 95.27344012260437
----------------------------------------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: 16, Loss: 0.7842, Acc: 96.88%, CE_Loss: 0.27, Reg_Loss:102.49, Cost:0.01 best_reg:115.48 avg_loss_reg:105.86:   3%|▎         | 34/1000 [11:01<5:13:15, 19.46s/it]
Traceback (most recent call last):
  File "D:\UULi\test_code\k_arm_test\main.py", line 87, 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 153, in scanning
    f'Target: {target_classes[target_index]}, victim: {labels[0]}, Loss: {loss:.4f},'
  File "C:\Users\islab\anaconda3\envs\pytorch1\lib\site-packages\torch\tensor.py", line 534, in __format__
    return self.item().__format__(format_spec)
KeyboardInterrupt

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

```