```
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-00000739----------------------------------------
***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: 14.463637590408325
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000740----------------------------------------
***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: 11.918782711029053
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000741----------------------------------------
***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: 11.29201364517212
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000742----------------------------------------
***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', '0-20', '1-2', '1-21', '2-1', '2-21', '3-15', '3-17', '3-18', '4-10', '4-16', '4-21', '5-12', '6-13', '8-16', '9-10', '9-16', '10-16', '13-0', '13-18', '15-3', '15-17', '15-1', '17-19', '20-0']
***Trigger Reverse Engineering開始***
Target: 0, victim: 20, Loss: 1.0485, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:923.24, Cost:0.00 best_reg:923.38 avg_loss_reg:913.63:  50%|[redacted]| 498/1000 [53:53<54:19,  6.49s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 20 Trigger Size: 923.2374267578125 Optimization Steps: 194
***Symmetric Check開始***
Target: 20, victim: 0, Loss: 0.0549, Acc: 95.00%, CE_Loss: 0.05, Reg_Loss:2175.83, Cost:0.00 best_reg:2056.74 avg_loss_reg:2164.89: 100%|[redacted]| 194/194 [20:27<00:00,  6.33s/it]
***Symmetric Check結束***
********************檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 4492.413516521454
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000743----------------------------------------
***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: ['15-20', '16-13', '17-2', '17-9']
***Trigger Reverse Engineering開始***
Target: 17, victim: 9, Loss: 9.8410, Acc: 0.00%, CE_Loss: 9.84, Reg_Loss:2598.01, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2573.26:   4%|[redacted]| 43/1000 [00:54<20:08,  1.26s/it]
***Trigger Reverse Engineering結束***
Target Class: 15 Victim Class: 20 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: 63.71432447433472
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000744----------------------------------------
***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: 11.266184568405151
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000745----------------------------------------
***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: ['1-12', '1-13', '3-12']
***Trigger Reverse Engineering開始***
Target: 3, victim: 12, Loss: 2.3220, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:57.29, Cost:0.04 best_reg:57.67 avg_loss_reg:57.67:  17%|[redacted]| 172/1000 [06:23<30:47,  2.23s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 12 Trigger Size: 57.289920806884766 Optimization Steps: 98
***Symmetric Check開始***
Target: 12, victim: 3, Loss: 3.9909, Acc: 80.00%, CE_Loss: 0.85, Reg_Loss:10608.85, Cost:0.00 best_reg:17686.52 avg_loss_reg:10556.41: 100%|[redacted]| 98/98 [03:37<00:00,  2.22s/it]
***Symmetric Check結束***
********************檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 612.1732649803162
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000746----------------------------------------
***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: 24.231024503707886
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000747----------
***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', '1-21', '1-22', '2-21', '2-23', '3-15', '3-17', '4-8', '4-18', '7-19', '8-0', '8-6', '8-12', '9-0', '10-18', '11-9', '12-6', '12-18', '13-3', '13-6', '14-1', '14-6', '14-8', '15-3', '15-8', '16-8', '17-1', '18-9', '18-12', '20-0', '20-21', '21-1', '21-22', '21-6', '23-0', '23-20', '23-22']
***Trigger Reverse Engineering開始***
Target: 23, victim: 22, Loss: 7.5071, Acc: 0.00%, CE_Loss: 7.51, Reg_Loss:2559.41, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2544.12:  53%|[redacted]| 526/1000 [59:48<53:53,  6.82s/it]
***Trigger Reverse Engineering結束***
Target Class: 0 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: 3634.0702254772186
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000748----------
***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: 24.299894094467163
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000749----------
***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: 7.203389883041382
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000750----------
***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', '15-1', '15-5']
***Trigger Reverse Engineering開始***
Target: 15, victim: 5, Loss: 10.8797, Acc: 0.00%, CE_Loss: 10.88, Reg_Loss:2533.32, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2523.06:   3%|[redacted]| 32/1000 [00:12<06:24,  2.52it/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: 18.310994148254395
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000751----------
***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', '5-6', '8-0', '8-6', '9-2', '11-2', '14-1']
***Trigger Reverse Engineering開始***
Target: 8, victim: 6, Loss: 0.7750, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:145.16, Cost:0.01 best_reg:145.17 avg_loss_reg:145.17:  26%|[redacted]| 265/1000 [02:44<07:36,  1.61it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 6 Trigger Size: 145.16424560546875 Optimization Steps: 134
***Symmetric Check開始***
Target: 6, victim: 8, Loss: 4.2537, Acc: 70.00%, CE_Loss: 0.60, Reg_Loss:2436.57, Cost:0.00 best_reg:2563.51 avg_loss_reg:2455.95: 100%|[redacted]| 134/134 [01:24<00:00,  1.59it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 255.50932121276855
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000752----------
***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: ['0-13', '0-14', '2-14', '13-0']
***Trigger Reverse Engineering開始***
Target: 0, victim: 13, Loss: 2.0598, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:108.70, Cost:0.02 best_reg:109.62 avg_loss_reg:109.62:  17%|[redacted]| 169/1000 [01:03<05:10,  2.67it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 13 Trigger Size: 108.70454406738281 Optimization Steps: 137
***Symmetric Check開始***
Target: 13, victim: 0, Loss: 2.8038, Acc: 100.00%, CE_Loss: 0.46, Reg_Loss:308.37, Cost:0.01 best_reg:310.69 avg_loss_reg:310.69: 100%|[redacted]| 137/137 [00:54<00:00,  2.51it/s]
***Symmetric Check結束***
**********檢測結束**********
```

```
檢測結果: Model是安全的(Benign)
整體耗時: 123.67250084877014
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000753----------
***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: 19.224700450897217
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000754----------
***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', '0-10', '1-0', '1-10', '5-0', '7-1', '8-1', '10-0', '12-10']
***Trigger Reverse Engineering開始***
Target: 1, victim: 0, Loss: 3.1015, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:51.88, Cost:0.06 best_reg:52.69 avg_loss_reg:52.69:  17%|[redacted]        | 174/1000 [02:17<10:54,  1.26it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 0 Trigger Size: 51.879005432128906 Optimization Steps: 73
***Symmetric Check開始***
Target: 0, victim: 1, Loss: 0.9551, Acc: 60.00%, CE_Loss: 0.96, Reg_Loss:13927.54, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:13906.94: 100%|[redacted]| 73/73 [00:57<00:00,  1.26it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 201.69213438034058
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000755----------
***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']
***Trigger Reverse Engineering開始***
Target: 0, victim: 10, Loss: 8.3246, Acc: 0.00%, CE_Loss: 8.32, Reg_Loss:2578.51, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2558.93:   1%|         | 10/1000 [00:31<51:39,  3.13s/it]
***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: 46.552051305770874
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000756----------
***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', '0-5', '0-20', '4-11', '7-4', '7-10', '9-10', '9-16', '10-4', '10-16', '16-10', '18-6', '19-1', '20-4', '21-1']
***Trigger Reverse Engineering開始***
Target: 0, victim: 20, Loss: 3.6779, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:308.73, Cost:0.01 best_reg:309.32 avg_loss_reg:310.01:  43%|[redacted]       | 429/1000 [04:47<06:22,  1.49it/s]
  0%|          | 0/184 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 20 Trigger Size: 308.7345886230469 Optimization Steps: 184
***Symmetric Check開始***
Target: 20, victim: 0, Loss: 0.0909, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:3841.01, Cost:0.00 best_reg:3812.84 avg_loss_reg:3812.84: 100%|[redacted]| 184/184 [01:59<00:00,  1.54it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 414.66723704338074
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000757----------
***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: 2.206376552581787
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000758----------
***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: 32.071468353271484
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000759----------
***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: 16.205012321472168
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000760----------
```

```
***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: ['4-7', '8-7', '11-7', '13-7', '15-4', '15-7']
***Trigger Reverse Engineering開始***
Target: 15, victim: 7, Loss: 8.6291, Acc: 0.00%, CE_Loss: 8.63, Reg_Loss:2552.70, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2539.20:   8%|▉         | 75/1000 [01:10<14:27,  1.07it/s]
***Trigger Reverse Engineering結束***
Target Class: 4 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: 79.27002263069153
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000761----------------------------------------
***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: 15.682577848434448
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000762----------------------------------------
***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: ['7-4']
***Trigger Reverse Engineering開始***
Target: 7, victim: 4, Loss: 2.7750, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:528.10, Cost:0.01 best_reg:528.73 avg_loss_reg:528.73:  16%|▉         | 158/1000 [17:04<1:31:00,  6.48s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 4 Trigger Size: 528.1007080078125 Optimization Steps: 159
***Symmetric Check開始***
Target: 4, victim: 7, Loss: 3.8423, Acc: 70.00%, CE_Loss: 0.45, Reg_Loss:3393.25, Cost:0.00 best_reg:3542.63 avg_loss_reg:3424.00: 100%|██████████| 159/159 [16:57<00:00,  6.40s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 2064.601437330246
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000763----------------------------------------
***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: 9.846359729766846
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000764----------------------------------------
***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: ['14-2']
***Trigger Reverse Engineering開始***
Target: 14, victim: 2, Loss: 7.5442, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:189.11, Cost:0.04 best_reg:190.61 avg_loss_reg:191.65:  12%|▊         | 123/1000 [02:34<18:20,  1.26s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 2 Trigger Size: 189.10995483398438 Optimization Steps: 124
***Symmetric Check開始***
Target: 2, victim: 14, Loss: 0.9953, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:2609.09, Cost:0.00 best_reg:2585.07 avg_loss_reg:2609.31: 100%|██████████| 124/124 [02:34<00:00,  1.24s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 316.583899974823
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000765----------------------------------------
***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', '5-11', '6-13', '9-13', '10-5']
***Trigger Reverse Engineering開始***
Target: 9, victim: 13, Loss: 3.8025, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:28.38, Cost:0.13 best_reg:30.13 avg_loss_reg:30.13:  16%|▉         | 160/1000 [00:38<03:20,  4.18it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 13 Trigger Size: 28.38150405883789 Optimization Steps: 64
***Symmetric Check開始***
Target: 13, victim: 9, Loss: 1.4509, Acc: 30.00%, CE_Loss: 1.45, Reg_Loss:14291.08, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:14139.52: 100%|██████████| 64/64 [00:14<00:00,  4.37it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 58.130786657333374
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000766----------------------------------------
***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: 6.899338722229004
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000767----------------------------------------
***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', '2-6']
***Trigger Reverse Engineering開始***
Target: 2, victim: 6, Loss: 2.6971, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:70.12, Cost:0.04 best_reg:72.56 avg_loss_reg:68.77:  11%|▉         | 110/1000 [12:31<1:41:22,  6.83s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 6 Trigger Size: 70.12055969238281 Optimization Steps: 83
***Symmetric Check開始***
Target: 6, victim: 2, Loss: 0.3983, Acc: 95.00%, CE_Loss: 0.40, Reg_Loss:13638.58, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:13604.31: 100%|██████████| 83/83 [09:20<00:00,  6.76s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1326.538011789322
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000768----------------------------------------
***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', '21-0']
***Trigger Reverse Engineering開始***
Target: 21, victim: 0, Loss: 11.6559, Acc: 0.00%, CE_Loss: 11.66, Reg_Loss:2580.42, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2560.60:   3%|▎         | 31/1000 [01:36<50:07,  3.10s/it]
***Trigger Reverse Engineering結束***
Target Class: 9 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: 115.56473016738892
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000769----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***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']
***Trigger Reverse Engineering開始***
Target: 1, victim: 8, Loss: 8.2211, Acc: 10.00%, CE_Loss: 8.22, Reg_Loss:3189.18, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3014.48:   2%|▏         | 20/1000 [00:26<21:48,  1.34s/it]
***Trigger Reverse Engineering結束***
Target Class: 1 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: 34.30594301223755
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000770----------------------------------------
***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: 17.935478925704956
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000771----------------------------------------
***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: 6.2525, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:106.59, Cost:0.06 best_reg:106.69 avg_loss_reg:106.69:   8%|▊         | 83/1000 [03:07<34:27,  2.25s/it]
  0%|          | 0/84 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 6 Trigger Size: 106.58892059326172 Optimization Steps: 84
***Symmetric Check開始***
Target: 6, victim: 0, Loss: 0.8821, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:2463.58, Cost:0.00 best_reg:2494.91 avg_loss_reg:2494.91: 100%|██████████| 84/84 [03:02<00:00,  2.18s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 378.4475247859955
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000772----------------------------------------
***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: 14, Loss: 0.1391, Acc: 96.88%, CE_Loss: 0.05, Reg_Loss:93.46, Cost:0.00 best_reg:94.09 avg_loss_reg:92.66:   6%|▌         | 57/1000 [38:22<10:34:44, 40.39s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: all Trigger Size: 94.08768463134766 Optimization Steps: 58
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 2317.1598744392395
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000773----------
***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: ['15-0']
***Trigger Reverse Engineering開始***
Target: 15, victim: 0, Loss: 7.2363, Acc: 20.00%, CE_Loss: 7.24, Reg_Loss:3141.40, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3031.11:   2%|▏         | 20/1000 [02:18<1:52:59,  6.92s/it]
***Trigger Reverse Engineering結束***
Target Class: 15 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: 167.57727789878845
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000774----------
***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: ['9-7']
***Trigger Reverse Engineering開始***
Target: 9, victim: 7, Loss: 2.1305, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:36.66, Cost:0.06 best_reg:37.42 avg_loss_reg:36.11:   8%|▊         | 79/1000 [00:59<11:30,  1.33it/s]
  0%|          | 0/80 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 7 Trigger Size: 36.661293029785156 Optimization Steps: 80
***Symmetric Check開始***
Target: 7, victim: 9, Loss: 1.4239, Acc: 30.00%, CE_Loss: 1.42, Reg_Loss:5385.00, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:5373.69: 100%|██████████| 80/80 [00:59<00:00,  1.35it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 127.45027923583984
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000775----------
***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: 2.869412660598755
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000776----------
***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: ['11-6']
***Trigger Reverse Engineering開始***
Target: 11, victim: 6, Loss: 2.3677, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:2170.13, Cost:0.00 best_reg:2179.99 avg_loss_reg:2171.31:  24%|██▍       | 241/1000 [43:42<2:17:39, 10.88s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 6 Trigger Size: 2170.130859375 Optimization Steps: 242
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 2666.1472220420837
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000777----------
***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', '2-10', '9-5', '10-2', '12-11']
***Trigger Reverse Engineering開始***
Target: 1, victim: 5, Loss: 0.8391, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:688.32, Cost:0.00 best_reg:700.22 avg_loss_reg:687.22:  37%|███▋      | 369/1000 [20:08<34:26,  3.27s/it]
  0%|          | 0/260 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 5 Trigger Size: 688.3182373046875 Optimization Steps: 260
***Symmetric Check開始***
Target: 5, victim: 1, Loss: 1.6722, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:3243.79, Cost:0.00 best_reg:3223.84 avg_loss_reg:3267.67: 100%|██████████| 260/260 [13:59<00:00,  3.23s/it]
***Symmetric Check結束***
```

```
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 2063.03804397583
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000778----------
***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: 2.583286762237549
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000779----------
***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: 2.704631805419922
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000780----------
***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: 19.656209230422974
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000781----------
***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: 12.8363, Acc: 0.00%, CE_Loss: 12.84, Reg_Loss:2577.17, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2558.08:   1%|          | 10/1000 [00:30<50:08,  3.04s/it]
***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: 43.1914324760437
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000782----------
***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: 21.898661136627197
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000783----------
***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: 7.11773419380188
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000784----------
***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: 2.686446189880371
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000785----------
***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: ['7-16', '10-6', '13-8']
***Trigger Reverse Engineering開始***
Target: 13, victim: 8, Loss: 1.7891, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:487.60, Cost:0.00 best_reg:489.38 avg_loss_reg:489.38:  19%|▉         | 189/1000 [05:48<24:53,  1.84s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 8 Trigger Size: 487.60400390625 Optimization Steps: 168
***Symmetric Check開始***
Target: 8, victim: 13, Loss: 0.6030, Acc: 90.00%, CE_Loss: 0.44, Reg_Loss:14243.52, Cost:0.00 best_reg:21949.79 avg_loss_reg:14161.41: 100%|██████████| 168/168 [05:07<00:00,  1.83s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 666.1707537174225
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000786----------
***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: 34.32105898857117
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000787----------
***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: 14.376377582550049
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000788----------
***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: 13.573931455612183
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000789----------
***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: 21.163976907730103
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000790----------
***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: 6.014713287353516
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000791----------
***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: 0.9456, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:578.73, Cost:0.00 best_reg:558.53 avg_loss_reg:565.11:  11%|▉         | 110/1000 [57:07<7:42:14, 31.16s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 558.5330657958984 Optimization Steps: 111
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 3447.483966112137
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000792----------
***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: 13.42529582977295
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000793----------
***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: 0.5168, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:740.33, Cost:0.00 best_reg:730.90 avg_loss_reg:734.34:   8%|▊         | 81/1000 [1:20:20<15:11:28, 59.51s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: all Trigger Size: 730.9016723632812 Optimization Steps: 82
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 4834.056268930435
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000794----------
***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']
***Trigger Reverse Engineering開始***
Target: 6, victim: 1, Loss: 12.7432, Acc: 0.00%, CE_Loss: 12.74, Reg_Loss:2539.56, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2530.27:   1%|         | 10/1000 [01:12<1:59:47,  7.26s/it]
***Trigger Reverse Engineering結束***
Target Class: 6 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: 92.16798639297485
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000795----------
***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', '4-5', '5-0', '5-3']
***Trigger Reverse Engineering開始***
Target: 5, victim: 3, Loss: 9.0277, Acc: 0.00%, CE_Loss: 9.03, Reg_Loss:2542.16, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2532.33:   4%|▌         | 43/1000 [02:21<52:30,  3.29s/it]
***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: 150.16335463523865
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000796----------
***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: 19.273258447647095
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000797----------
***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: 1.2937, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:6532.86, Cost:0.00 best_reg:6585.44 avg_loss_reg:6503.59:  12%|▋         | 122/1000 [44:12<5:18:10, 21.74s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 6585.442731584822 Optimization Steps: 123
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 2668.064249277115
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000798----------
***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: 31.05341386795044
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000799----------
***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', '0-3', '0-4']
***Trigger Reverse Engineering開始***
Target: 0, victim: 3, Loss: 5.4244, Acc: 100.00%, CE_Loss: 0.37, Reg_Loss:295.78, Cost:0.02 best_reg:299.45 avg_loss_reg:299.45:  18%|▊         | 185/1000 [00:44<03:14,  4.19it/s]
  0%|          | 0/163 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 3 Trigger Size: 295.7810363769531 Optimization Steps: 163
***Symmetric Check開始***
Target: 3, victim: 0, Loss: 2.0759, Acc: 100.00%, CE_Loss: 0.37, Reg_Loss:1701.28, Cost:0.00 best_reg:1701.88 avg_loss_reg:1701.88: 100%|██████████| 163/163 [00:38<00:00,  4.23it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 84.23969006538391
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000800----------
***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: 20, Loss: 0.1459, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:1024.20, Cost:0.00 best_reg:1026.09 avg_loss_reg:1008.44:   7%|▏         | 72/1000 [1:31:07<19:34:36, 75.94s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 1026.0934491838727 Optimization Steps: 73
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 5484.463182926178
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000801----------
***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: 8.984658002853394
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000802----------
***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: 1.7590, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:19.43, Cost:0.09 best_reg:19.59 avg_loss_reg:19.59:   6%|▌         | 63/1000 [03:14<48:16,  3.09s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 19.48233127593994 Optimization Steps: 64
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 196.71590375900269
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000803----------
***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', '11-0']
***Trigger Reverse Engineering開始***
Target: 11, victim: 0, Loss: 7.0466, Acc: 0.00%, CE_Loss: 7.05, Reg_Loss:2556.58, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2542.14:   2%|▏         | 21/1000 [02:04<1:36:47,  5.93s/it]
***Trigger Reverse Engineering結束***
Target Class: 9 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: 143.06681632995605
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000804----------
***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', '1-11', '10-8', '12-11', '15-9']
***Trigger Reverse Engineering開始***
Target: 1, victim: 11, Loss: 1.5253, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:390.88, Cost:0.00 best_reg:392.85 avg_loss_reg:392.85:  30%|███       | 301/1000 [03:00<07:00,  1.66it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 11 Trigger Size: 390.88421630859375 Optimization Steps: 257
***Symmetric Check開始***
Target: 11, victim: 1, Loss: 1.8034, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:1025.44, Cost:0.00 best_reg:1020.51 avg_loss_reg:1025.47: 100%|██████████| 257/257 [02:29<00:00,  1.72it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 337.3044583797455
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000805----------
***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: 9, Loss: 0.4463, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:126.55, Cost:0.00 best_reg:127.59 avg_loss_reg:126.11:   7%|▋         | 72/1000 [38:16<8:13:23, 31.90s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: all Trigger Size: 127.58805847167969 Optimization Steps: 73
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 2310.836585044861
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000806----------
***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: 2.7551, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:490.34, Cost:0.01 best_reg:496.34 avg_loss_reg:496.34:  14%|▏         | 144/1000 [08:47<52:18,  3.67s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 8 Trigger Size: 490.33782958984375 Optimization Steps: 145
***Symmetric Check開始***
```

```
Target: 8, victim: 7, Loss: 3.3355, Acc: 90.00%, CE_Loss: 0.41, Reg_Loss:4394.37, Cost:0.00 best_reg:4504.04 avg_loss_reg:4424.29: 100%|| 145/145 [08:46<00:00,  3.63s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1071.4055304527283
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000807----------------------------------------
***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: 25.581960439682007
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000808----------------------------------------
***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: ['1-17', '1-22', '2-17', '3-17', '4-8', '4-21', '5-11', '12-9', '13-8', '14-10', '15-17', '18-11', '23-1', '23-7']
***Trigger Reverse Engineering開始***
Target: 23, victim: 1, Loss: 1.3568, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:161.31, Cost:0.01 best_reg:162.18 avg_loss_reg:161.61:  46%|     | 464/1000 [1:01:06<1:10:35,  7.90s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 23 Victim Class: 1 Trigger Size: 161.30975341796875 Optimization Steps: 213
***Symmetric Check開始***
Target: 1, victim: 23, Loss: 5.9114, Acc: 100.00%, CE_Loss: 0.36, Reg_Loss:730.72, Cost:0.01 best_reg:732.96 avg_loss_reg:732.08:  86%|  | 184/213 [24:14<03:49,  7.91s/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: 5157.744780778885
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000809----------------------------------------
***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', '6-9', '7-14', '13-1']
***Trigger Reverse Engineering開始***
Target: 13, victim: 1, Loss: 3.7780, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:1586.43, Cost:0.00 best_reg:1586.75 avg_loss_reg:1587.19:  24%|     | 243/1000 [18:19<57:04,  4.52s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 1 Trigger Size: 1586.426513671875 Optimization Steps: 211
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1125.8866560459137
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000810----------------------------------------
***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: 18.07299256324768
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000811----------------------------------------
***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: 11.91101622581482
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000812----------------------------------------
***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: 10.990734338760376
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000813----------------------------------------
***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: ['3-1', '3-4', '3-9', '4-12', '4-16', '4-3', '5-3', '5-11', '8-16', '8-3', '8-12', '10-9', '11-12', '11-16', '12-11', '16-11', '16-12', '19-1']
***Trigger Reverse Engineering開始***
Target: 16, victim: 12, Loss: 2.3299, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:408.74, Cost:0.01 best_reg:415.49 avg_loss_reg:411.85:  34%|     | 338/1000 [21:05<41:19,  3.74s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 16 Victim Class: 12 Trigger Size: 408.7350769042969 Optimization Steps: 121
***Symmetric Check開始***
Target: 12, victim: 16, Loss: 1.0892, Acc: 60.00%, CE_Loss: 1.09, Reg_Loss:13665.04, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:13660.21: 100%| 121/121 [07:22<00:00,  3.65s/it]
```

```
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1726.4608261585236
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000814----------------------------------------
***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: 8.278771162033081
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000815----------------------------------------
***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: 17.821948289871216
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000816----------------------------------------
***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: ['5-6']
***Trigger Reverse Engineering開始***
Target: 5, victim: 6, Loss: 7.1757, Acc: 5.00%, CE_Loss: 7.18, Reg_Loss:3142.62, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3009.77:   2%|          | 20/1000 [00:16<13:32,  1.21it/s]
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 6 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: 22.332966566085815
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000817----------------------------------------
***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: 6, Loss: 0.7965, Acc: 96.88%, CE_Loss: 0.33, Reg_Loss:138.17, Cost:0.00 best_reg:136.75 avg_loss_reg:138.10:   9%|▉         | 86/1000 [22:19<3:57:12, 15.57s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: all Trigger Size: 136.74974365234374 Optimization Steps: 87
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1345.1702678203583
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000818----------------------------------------
***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', '1-2', '1-11', '3-2', '6-4', '7-4', '7-11', '8-4', '9-10', '12-1', '12-2', '13-1', '13-11', '14-13']
***Trigger Reverse Engineering開始***
Target: 8, victim: 4, Loss: 3.8578, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:1052.67, Cost:0.00 best_reg:1053.39 avg_loss_reg:1069.02:  43%|████▎     | 431/1000 [04:04<05:22,  1.77it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 4 Trigger Size: 1052.66552734375 Optimization Steps: 268
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 249.66332411766052
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000819----------------------------------------
***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: 15.670140266418457
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000820----------------------------------------
***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: ['13-2']
***Trigger Reverse Engineering開始***
Target: 13, victim: 2, Loss: 3.8271, Acc: 100.00%, CE_Loss: 0.39, Reg_Loss:1019.13, Cost:0.00 best_reg:1020.10 avg_loss_reg:1020.10:  28%|██▊       | 277/1000 [03:45<09:49,  1.23it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 2 Trigger Size: 1019.133056640625 Optimization Steps: 278
```

```
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 232.1439459323883
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000821----------
***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: 12.125516414642334
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000822----------
***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: 9.0563, Acc: 15.00%, CE_Loss: 9.06, Reg_Loss:3852.34, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3518.61:   2%|         | 20/1000 [02:23<1:56:53,  7.16s/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: 163.78042578697205
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000823----------
***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: ['2-15', '9-15', '10-15', '19-1']
***Trigger Reverse Engineering開始***
Target: 19, victim: 1, Loss: 10.3378, Acc: 0.00%, CE_Loss: 10.34, Reg_Loss:2542.22, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2532.59:   4%|▍         | 43/1000 [00:41<15:33,  1.03it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 15 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: 50.26493692398071
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000824----------
***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: 27.854203701019287
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000825----------
***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: 17.87335991859436
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000826----------
***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: 23.094658374786377
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000827----------
***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: ['3-9', '5-9', '6-8']
***Trigger Reverse Engineering開始***
Target: 6, victim: 8, Loss: 10.1556, Acc: 20.00%, CE_Loss: 10.16, Reg_Loss:2931.77, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2841.27:   6%|▌         | 62/1000 [00:36<09:08,  1.71it/s]
***Trigger Reverse Engineering結束***
Target Class: 3 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: 42.6524178981781
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000828----------
***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: 12.439329147338867
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000829----------
***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', '1-4', '1-20', '8-7', '12-7', '13-20', '19-20', '20-1', '21-7', '21-8']
***Trigger Reverse Engineering開始***
Target: 21, victim: 8, Loss: 6.5099, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:111.47, Cost:0.06 best_reg:113.53 avg_loss_reg:113.53:  37%|████      | 371/1000 [02:21<04:00,  2.61it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 21 Victim Class: 8 Trigger Size: 111.47022247314453 Optimization Steps: 89
***Symmetric Check開始***
Target: 8, victim: 21, Loss: 4.2790, Acc: 70.00%, CE_Loss: 0.54, Reg_Loss:328.55, Cost:0.01 best_reg:471.52 avg_loss_reg:336.53: 100%|██████████| 89/89 [00:34<00:00,  2.57it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 182.84737586975098
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000830----------
***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: 11, Loss: 0.2723, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:53.79, Cost:0.01 best_reg:53.38 avg_loss_reg:53.76:   6%|▌         | 64/1000 [1:03:08<15:23:25, 59.19s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: all Trigger Size: 53.376094818115234 Optimization Steps: 65
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 3802.1978306770325
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000831----------
***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: 12.931822061538696
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000832----------
***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: ['12-10', '13-9', '16-1']
***Trigger Reverse Engineering開始***
Target: 13, victim: 9, Loss: 0.8185, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:43.14, Cost:0.02 best_reg:43.39 avg_loss_reg:43.39:  13%|▏         | 132/1000 [01:22<09:05,  1.59it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 9 Trigger Size: 43.13946533203125 Optimization Steps: 100
***Symmetric Check開始***
Target: 9, victim: 13, Loss: 3.0269, Acc: 95.00%, CE_Loss: 0.62, Reg_Loss:714.14, Cost:0.00 best_reg:735.42 avg_loss_reg:735.42: 100%|██████████| 100/100 [01:02<00:00,  1.61it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 152.39497065544128
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000833----------
***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: 2.233386993408203
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000834----------
***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: 13.179946422576904
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000835----------
***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', '4-2', '4-3', '6-0']
***Trigger Reverse Engineering開始***
Target: 4, victim: 2, Loss: 1.2223, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:215.50, Cost:0.01 best_reg:215.96 avg_loss_reg:215.96:  31%|███       | 312/1000 [55:47<2:03:01, 10.73s/it]
early stop 所有
***Trigger Reverse Engineering結束***
```

```
Target Class: 4 Victim Class: 2 Trigger Size: 215.4962158203125 Optimization Steps: 149
***Symmetric Check開始***
Target: 2, victim: 4, Loss: 1.0330, Acc: 75.00%, CE_Loss: 1.03, Reg_Loss:13045.16, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:13099.90: 100%|[redacted]| 149/149 [26:53<00:00, 10.83s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 4988.310601949692
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000836----------
***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', '2-5']
***Trigger Reverse Engineering開始***
Target: 2, victim: 5, Loss: 9.9563, Acc: 0.00%, CE_Loss: 9.96, Reg_Loss:2576.96, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2559.31:   3%|▌         | 31/1000 [00:07<04:00,  4.02it/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: 9.753085613250732
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000837----------
***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']
***Trigger Reverse Engineering開始***
Target: 8, victim: 2, Loss: 11.4747, Acc: 0.00%, CE_Loss: 11.47, Reg_Loss:2502.02, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2495.25:   1%|          | 10/1000 [00:24<40:55,  2.48s/it]
***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: 33.46728014945984
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000838----------
***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: 11.3692, Acc: 0.00%, CE_Loss: 11.37, Reg_Loss:2559.86, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2547.47:   1%|          | 10/1000 [00:45<1:15:53,  4.60s/it]
***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: 53.54767107963562
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000839----------
***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', '2-1', '16-1', '17-1']
***Trigger Reverse Engineering開始***
Target: 2, victim: 1, Loss: 1.3686, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:47.84, Cost:0.03 best_reg:47.88 avg_loss_reg:47.96:  14%|▍         | 145/1000 [00:58<05:44,  2.49it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 47.83894348144531 Optimization Steps: 102
***Symmetric Check開始***
Target: 1, victim: 2, Loss: 7.4418, Acc: 90.00%, CE_Loss: 0.44, Reg_Loss:922.16, Cost:0.01 best_reg:939.39 avg_loss_reg:924.98: 100%|[redacted]| 102/102 [00:41<00:00,  2.48it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 105.92292761802673
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000840----------
***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: 24.68047022819519
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000841----------
***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: 14.541155815124512
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000842----------------------------------------
***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', '7-3', '9-2']
***Trigger Reverse Engineering開始***
Target: 9, victim: 2, Loss: 4.8228, Acc: 20.00%, CE_Loss: 4.82, Reg_Loss:2972.18, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2853.69:   4%|▍          | 42/1000 [00:10<03:49,  4.17it/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: 15.0741286277771
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000843----------------------------------------
***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: 5.521037578582764
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000844----------------------------------------
***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: 6.8390, Acc: 0.00%, CE_Loss: 6.84, Reg_Loss:2612.02, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2587.21:   1%|          | 10/1000 [01:15<2:04:44,  7.56s/it]
***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: 96.07770109176636
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000845----------------------------------------
***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: ['13-4']
***Trigger Reverse Engineering開始***
Target: 13, victim: 4, Loss: 2.0004, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:73.89, Cost:0.03 best_reg:73.89 avg_loss_reg:73.89:  10%|▉          | 102/1000 [07:48<1:08:47,  4.60s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 4 Trigger Size: 73.89019775390625 Optimization Steps: 103
***Symmetric Check開始***
Target: 4, victim: 13, Loss: 9.0002, Acc: 40.00%, CE_Loss: 0.75, Reg_Loss:12377.69, Cost:0.00 best_reg:17592.12 avg_loss_reg:13215.54: 100%|██████████| 103/103 [07:49<00:00,  4.55s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 959.9967269897461
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000846----------------------------------------
***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: ['11-1', '12-9']
***Trigger Reverse Engineering開始***
Target: 12, victim: 9, Loss: 2.3953, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:1008.55, Cost:0.00 best_reg:1012.11 avg_loss_reg:1007.04:  18%|█▊         | 177/1000 [19:49<1:32:10,  6.72s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 9 Trigger Size: 1008.5536499023438 Optimization Steps: 157
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1215.2177982330322
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000847----------------------------------------
***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: 9.37430739402771
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000848----------------------------------------
***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: 8.862825870513916
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000849----------------------------------------
***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: 5.9735, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:3982.34, Cost:0.00 best_reg:3997.50 avg_loss_reg:3997.50:  20%|██        | 199/1000 [1:04:12<4:18:26, 19.36s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 3976.3284301757812 Optimization Steps: 200
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 3864.3802876472473
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000850----------------------------------------
***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: 7.794076919555664
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000851----------------------------------------
***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', '3-7', '5-0', '5-6']
***Trigger Reverse Engineering開始***
Target: 3, victim: 7, Loss: 1.3944, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:2737.53, Cost:0.00 best_reg:2747.88 avg_loss_reg:2720.13:  32%|███▏      | 317/1000 [56:41<2:02:09, 10.73s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 7 Trigger Size: 2737.52734375 Optimization Steps: 274
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 3435.0818412303925
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000852----------------------------------------
***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: 11.437893390655518
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000853----------------------------------------
***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: 9.214526176452637
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000854----------------------------------------
***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: ['9-3']
***Trigger Reverse Engineering開始***
Target: 9, victim: 3, Loss: 8.6953, Acc: 0.00%, CE_Loss: 8.70, Reg_Loss:2502.26, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2501.90:   1%|          | 10/1000 [00:24<40:37,  2.46s/it]
***Trigger Reverse Engineering結束***
Target Class: 9 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: 33.60719013214111
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000855----------------------------------------
***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***
```