```
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-00000445----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 10
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 10, victim: 22, Loss: 0.6154, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:4670.46, Cost:0.00 best_reg:4642.89 avg_loss_reg:4621.30:  23%|███       | 234/1000 [08:22<27:25,  2.15s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: all Trigger Size: 4642.88837890625 Optimization Steps: 235
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 508.9595293998718
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000446----------------------------------------
***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: 16, Loss: 0.2676, Acc: 95.00%, CE_Loss: 0.06, Reg_Loss:91.43, Cost:0.00 best_reg:101.24 avg_loss_reg:91.47:   9%|▉         | 87/1000 [35:04<6:08:04, 24.19s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 101.24027252197266 Optimization Steps: 88
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 2115.3653445243835
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000447----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-1', '3-14', '8-1', '14-3', '14-12', '20-1', '22-1']
***Trigger Reverse Engineering開始***
Target: 22, victim: 1, Loss: 7.8331, Acc: 0.00%, CE_Loss: 7.83, Reg_Loss:2549.89, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2537.14:  11%|▉         | 106/1000 [00:34<04:48,  3.10it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 40.285250663757324
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000448----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.615047216415405
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000449----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.669980764389038
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000450----------------------------------------
***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: 19, Loss: 0.4472, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:3177.85, Cost:0.00 best_reg:3211.57 avg_loss_reg:3147.21:  13%|▉         | 131/1000 [31:48<3:30:57, 14.57s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 3211.5723702566966 Optimization Steps: 132
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1916.7312288284302
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000451----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
```

```
檢測結果: Model是安全的(Benign)
整體耗時: 4.949232578277588
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000452----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 16.315000295639038
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000453----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.186664342880249
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000454----------
***Pre-Screening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', '7-6']
***Trigger Reverse Engineering開始***
Target: 7, victim: 6, Loss: 4.9830, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:422.76, Cost:0.01 best_reg:429.16 avg_loss_reg:423.54:  14%|▉         | 144/1000 [10:12<1:00:40,  4.25s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 6 Trigger Size: 422.7642822265625 Optimization Steps: 134
***Symmetric Check開始***
Target: 6, victim: 7, Loss: 0.0565, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:14010.39, Cost:0.00 best_reg:13939.20 avg_loss_reg:13939.20: 100%|██████████| 134/134 [09:22<00:00,  4.20s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1192.202980041504
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000455----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.389086246490479
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000456----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-13', '9-14', '11-13', '13-11', '14-13', '16-1']
***Trigger Reverse Engineering開始***
Target: 13, victim: 11, Loss: 2.6395, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.63, Cost:0.06 best_reg:48.31 avg_loss_reg:48.31:  23%|██▎       | 230/1000 [15:39<52:25,  4.09s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 11 Trigger Size: 45.63339614868164 Optimization Steps: 68
***Symmetric Check開始***
Target: 11, victim: 13, Loss: 0.3959, Acc: 80.00%, CE_Loss: 0.40, Reg_Loss:8494.80, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:8416.27: 100%|██████████| 68/68 [04:00<00:00,  3.53s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1201.0458145141602
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000457----------
***Pre-Screening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', '1-21', '2-1', '3-1', '4-3', '4-9', '5-9', '11-9', '15-7', '20-1', '20-19', '21-1', '21-19']
***Trigger Reverse Engineering開始***
Target: 1, victim: 21, Loss: 2.4678, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:470.00, Cost:0.01 best_reg:472.34 avg_loss_reg:472.34:  32%|███▏      | 319/1000 [01:25<03:03,  3.71it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 21 Trigger Size: 470.0036315917969 Optimization Steps: 119
***Symmetric Check開始***
Target: 21, victim: 1, Loss: 1.2242, Acc: 90.00%, CE_Loss: 0.45, Reg_Loss:1165.80, Cost:0.00 best_reg:1297.40 avg_loss_reg:1183.93: 100%|██████████| 119/119 [00:30<00:00,  3.92it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 123.52171015739441
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000458----------
***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: 1.7720, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:3917.38, Cost:0.00 best_reg:3821.82 avg_loss_reg:3852.14:   8%|▊         | 77/1000 [03:06<37:11,  2.42s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: all Trigger Size: 3821.816336495536 Optimization Steps: 78
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 192.1087145805359
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000459----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.94709587097168
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000460----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '2-1']
***Trigger Reverse Engineering開始***
Target: 2, victim: 1, Loss: 8.2124, Acc: 0.00%, CE_Loss: 8.21, Reg_Loss:2557.19, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2542.86:   2%|▏         | 21/1000 [00:05<04:00,  4.07it/s]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 2 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 9.722591876983643
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000461----------
***Pre-Screening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', '8-3', '8-9', '8-13', '12-11', '12-13']
***Trigger Reverse Engineering開始***
Target: 8, victim: 3, Loss: 2.3492, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:198.24, Cost:0.01 best_reg:207.35 avg_loss_reg:197.56:  21%|██        | 210/1000 [08:29<31:56,  2.43s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 3 Trigger Size: 198.24041748046875 Optimization Steps: 95
***Symmetric Check開始***
Target: 3, victim: 8, Loss: 0.6461, Acc: 90.00%, CE_Loss: 0.65, Reg_Loss:19142.80, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:19089.80: 100%|██████████| 95/95 [03:49<00:00,  2.42s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 749.9109630584717
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000462----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['20-2', '20-7', '21-2']
***Trigger Reverse Engineering開始***
Target: 20, victim: 7, Loss: 1.4165, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:48.38, Cost:0.03 best_reg:49.62 avg_loss_reg:47.49:  12%|▏         | 122/1000 [00:22<02:41,  5.43it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 20 Victim Class: 7 Trigger Size: 48.37567901611328 Optimization Steps: 103
***Symmetric Check開始***
Target: 7, victim: 20, Loss: 0.5173, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:3983.99, Cost:0.00 best_reg:11195.67 avg_loss_reg:3978.35: 100%|██████████| 103/103 [00:19<00:00,  5.36it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 48.55360150337219
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000463----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 12
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 12, victim: 12, Loss: 0.8067, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:806.73, Cost:0.00 best_reg:808.70 avg_loss_reg:795.52:   9%|▉         | 90/1000 [26:53<4:31:56, 17.93s/it]
early stop 所有
***Trigger Reverse Engineering結束***
```

```
Target Class: 12 Victim Class: all Trigger Size: 808.700341796875 Optimization Steps: 91
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1625.6330347061157
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000464----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.479580402374268
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000465----------
***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: 4, Loss: 1.0341, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:5157.92, Cost:0.00 best_reg:5401.73 avg_loss_reg:5101.63:   5%|▌         | 48/1000 [07:17<2:24:46,  9.12s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 5401.7333984375 Optimization Steps: 49
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 445.0679786205292
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000466----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.631896257400513
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000467----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.522701025009155
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000468----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.749953746795654
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000469----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-11']
***Trigger Reverse Engineering開始***
Target: 6, victim: 11, Loss: 11.1240, Acc: 0.00%, CE_Loss: 11.12, Reg_Loss:2582.18, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2562.63:   1%|          | 10/1000 [00:27<44:37,  2.70s/it]
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 11 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 43.30045461654663
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000470----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.345905065536499
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000471----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 11
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 11, victim: 16, Loss: 0.5763, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:1944.95, Cost:0.00 best_reg:1940.50 avg_loss_reg:1962.71:   8%|▊         | 83/1000 [1:06:52<12:18:51, 48.34s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: all Trigger Size: 1940.5022416548295 Optimization Steps: 84
```

```
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 4027.8936009407043
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000472----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-10', '2-3', '3-2', '3-10', '4-14', '5-11', '5-13', '6-13', '7-9', '8-18', '9-11', '10-3', '12-5', '14-4', '16-9', '16-11', '16-13', '19-3', '19-10', '20-1', '20-2']
***Trigger Reverse Engineering開始***
Target: 2, victim: 3, Loss: 4.2976, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:796.70, Cost:0.01 best_reg:797.06 avg_loss_reg:797.34:  60%|[redacted]  | 602/1000 [19:07<12:38,  1.91s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 3 Trigger Size: 796.70166015625 Optimization Steps: 195
***Symmetric Check開始***
Target: 3, victim: 2, Loss: 3.5176, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:968.04, Cost:0.00 best_reg:981.31 avg_loss_reg:981.31:  73%|[redacted]  | 142/195 [03:36<01:20,  1.52s/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: 1379.2330272197723
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000473----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.054565191268921
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000474----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-18', '5-18', '8-9', '22-21']
***Trigger Reverse Engineering開始***
Target: 22, victim: 21, Loss: 7.7380, Acc: 0.00%, CE_Loss: 7.74, Reg_Loss:2525.05, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2516.91:   5%|[redacted]  | 53/1000 [01:30<26:57,  1.71s/it]
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 18 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 107.49298167228699
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000475----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['16-0']
***Trigger Reverse Engineering開始***
Target: 16, victim: 0, Loss: 4.3915, Acc: 20.00%, CE_Loss: 4.39, Reg_Loss:2943.35, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2877.14:   2%|[redacted]  | 20/1000 [01:13<1:00:04,  3.68s/it]
***Trigger Reverse Engineering結束***
Target Class: 16 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: 100.53090262413025
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000476----------------------------------------
***Pre-Screening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', '1-0', '1-2', '1-22', '2-1', '2-3', '2-6', '3-1', '3-16', '4-2', '4-5', '5-6', '5-11', '6-5', '6-13', '6-2', '7-5', '7-22', '7-21', '8-13', '8-9', '8-18', '9-16', '10-3', '10-16', '11-5', '11-13', '11-18', '12-18', '12-7', '12-20', '13-0', '13-19', '14-19', '15-0', '15-17', '17-15', '17-19', '17-22', '18-11', '18-20', '19-13', '19-15', '19-20', '20-1', '20-21', '21-7', '21-20', '21-22', '22-1']
***Trigger Reverse Engineering開始***
Target: 1, victim: 22, Loss: 2.2814, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:1329.19, Cost:0.00 best_reg:1343.86 avg_loss_reg:1343.86:  91%|[redacted] | 911/1000 [39:39<03:52,  2.61s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 22 Trigger Size: 1329.1861572265625 Optimization Steps: 203
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 2393.9243268966675
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000477----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 32.64503526687622
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000478----------------------------------------
```

```
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.31959342956543
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000479----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.60225772857666
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000480----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.6397130489349365
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000481----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-9', '5-16', '11-0', '13-5', '15-16']
***Trigger Reverse Engineering開始***
Target: 1, victim: 9, Loss: 1.6601, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:1024.46, Cost:0.00 best_reg:1029.03 avg_loss_reg:1029.03:  23%|██        | 233/1000 [18:54<1:02:13,  4.87s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 9 Trigger Size: 1024.458740234375 Optimization Steps: 190
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1158.3292882442474
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000482----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 18.340771436691284
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000483----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 18
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 18, victim: 19, Loss: 0.2427, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:363.81, Cost:0.00 best_reg:357.10 avg_loss_reg:361.13:  10%|▉         | 99/1000 [38:49<5:53:17, 23.53s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 18 Victim Class: all Trigger Size: 357.10140119280135 Optimization Steps: 100
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 2341.3998906612396
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000484----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-6']
***Trigger Reverse Engineering開始***
Target: 3, victim: 6, Loss: 2.6270, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:19.56, Cost:0.13 best_reg:20.36 avg_loss_reg:20.36:   6%|▌         | 65/1000 [00:07<01:52,  8.28it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 6 Trigger Size: 19.558185577392578 Optimization Steps: 66
***Symmetric Check開始***
Target: 6, victim: 3, Loss: 3.9893, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:2520.09, Cost:0.00 best_reg:2581.22 avg_loss_reg:2581.22: 100%|██████████| 66/66 [00:07<00:00,  8.54it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 17.868822813034058
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000485----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['10-11']
```

```
***Trigger Reverse Engineering開始***
Target: 10, victim: 11, Loss: 9.1305, Acc: 0.00%, CE_Loss: 9.13, Reg_Loss:2543.78, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2532.51:   1%|          | 10/1000 [00:03<06:22,  2.59it/s]
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 11 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 9.986019611358643
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000486----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-3']
***Trigger Reverse Engineering開始***
Target: 4, victim: 3, Loss: 11.2577, Acc: 0.00%, CE_Loss: 11.26, Reg_Loss:2591.12, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2570.44:   1%|          | 10/1000 [00:01<03:01,  5.47it/s]
***Trigger Reverse Engineering結束***
Target Class: 4 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: 4.39846396446228
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000487----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 16.589495182037354
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000488----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.584741353988647
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000489----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.06437373161316
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000490----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.690270185470581
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000491----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-10', '5-12', '5-14', '9-14', '11-14', '13-3', '13-12', '14-8', '14-9', '17-0']
***Trigger Reverse Engineering開始***
Target: 14, victim: 8, Loss: 2.3006, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:2136.66, Cost:0.00 best_reg:2160.59 avg_loss_reg:2187.44:  36%|[redacted]       | 362/1000 [17:45<31:17,  2.94s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 8 Trigger Size: 2136.660888671875 Optimization Steps: 243
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1086.8663012981415
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000492----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-19', '2-11', '13-0', '13-4', '14-4', '16-9', '19-1', '20-1', '20-22', '22-0']
***Trigger Reverse Engineering開始***
Target: 13, victim: 4, Loss: 1.2602, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:157.08, Cost:0.01 best_reg:157.26 avg_loss_reg:157.16:  31%|[redacted]       | 308/1000 [02:19<05:13,  2.20it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 4 Trigger Size: 157.07608032226562 Optimization Steps: 179
***Symmetric Check開始***
Target: 4, victim: 13, Loss: 2.6631, Acc: 95.00%, CE_Loss: 0.37, Reg_Loss:2289.50, Cost:0.00 best_reg:2335.35 avg_loss_reg:2304.50: 100%|[redacted]| 179/179 [01:21<00:00,  2.20it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
```

```
整體耗時: 228.1006999015808
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000493----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.041424751281738
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000494----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 32.34579849243164
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000495----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-17', '7-8', '13-18', '18-19']
***Trigger Reverse Engineering開始***
Target: 0, victim: 17, Loss: 2.6233, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:44.27, Cost:0.06 best_reg:45.01 avg_loss_reg:45.01:  13%|          | 133/1000 [04:38<30:18,  2.10s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 17 Trigger Size: 44.26556396484375 Optimization Steps: 91
***Symmetric Check開始***
Target: 17, victim: 0, Loss: 2.0320, Acc: 5.00%, CE_Loss: 2.03, Reg_Loss:14961.56, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:14797.46: 100%|| 91/91 [03:11<00:00,  2.10s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 480.39882802963257
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000496----------
***Pre-Screening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', '4-2']
***Trigger Reverse Engineering開始***
Target: 4, victim: 2, Loss: 7.6594, Acc: 0.00%, CE_Loss: 7.66, Reg_Loss:2536.81, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2528.22:   2%|          | 21/1000 [00:02<01:42,  9.52it/s]
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 7.097445964813232
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000497----------
***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: 9, Loss: 0.2679, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:79.35, Cost:0.00 best_reg:85.46 avg_loss_reg:78.87:   5%|          | 49/1000 [05:40<1:50:06,  6.95s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: all Trigger Size: 85.46172768729073 Optimization Steps: 50
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 345.83332085609436
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000498----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 17.476946115493774
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000499----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.314077377319336
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000500----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
```

```
檢測結果: Model是安全的(Benign)
整體耗時: 6.391058921813965
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000501----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 18
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 18, victim: 20, Loss: 0.2463, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:554.00, Cost:0.00 best_reg:557.91 avg_loss_reg:551.87:  12%|          | 119/1000 [2:51:48<21:12:01, 86.63s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 18 Victim Class: all Trigger Size: 557.9116908482143 Optimization Steps: 120
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 10335.603230714798
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000502----------
***Pre-Screening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', '4-3', '5-0']
***Trigger Reverse Engineering開始***
Target: 5, victim: 0, Loss: 0.9095, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:528.48, Cost:0.00 best_reg:533.69 avg_loss_reg:526.46:  38%|      | 384/1000 [00:56<01:30,  6.82it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 0 Trigger Size: 528.4754028320312 Optimization Steps: 353
***Symmetric Check開始***
Target: 0, victim: 5, Loss: 1.1086, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:2260.90, Cost:0.00 best_reg:2263.79 avg_loss_reg:2260.75:  57%|      | 200/353 [00:29<00:22,  6.82it/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: 94.84227633476257
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000503----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.296743392944336
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000504----------
***Pre-Screening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', '20-4']
***Trigger Reverse Engineering開始***
Target: 20, victim: 4, Loss: 10.2242, Acc: 0.00%, CE_Loss: 10.22, Reg_Loss:2563.23, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2546.65:   2%|          | 21/1000 [00:10<08:05,  2.02it/s]
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 18.445801734924316
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000505----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-4']
***Trigger Reverse Engineering開始***
Target: 1, victim: 4, Loss: 5.8203, Acc: 5.00%, CE_Loss: 5.82, Reg_Loss:4032.35, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3714.88:   2%|          | 20/1000 [00:43<35:19,  2.16s/it]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 51.48796224594116
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000506----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-7', '0-19', '2-12', '2-15', '3-4', '3-9', '4-3', '5-6', '5-11', '6-3', '6-5', '8-11', '9-3', '12-2', '15-2', '15-18', '16-0', '16-1', '16-7', '17-14', '18-16', '18-19', '18-20', '19-18', '20-1', '20-16']
***Trigger Reverse Engineering開始***
Target: 19, victim: 18, Loss: 1.5233, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:1797.57, Cost:0.00 best_reg:1800.22 avg_loss_reg:1800.22:  64%|      | 644/1000 [07:06<03:55,  1.51it/s]
early stop 所有
```

```
***Trigger Reverse Engineering結束***
Target Class: 19 Victim Class: 18 Trigger Size: 1797.567626953125 Optimization Steps: 319
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 434.56749844551086
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000507----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-3']
***Trigger Reverse Engineering開始***
Target: 6, victim: 3, Loss: 13.0298, Acc: 0.00%, CE_Loss: 13.03, Reg_Loss:2567.32, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2550.86:   1%|         | 10/1000 [00:01<01:40,  9.80it/s]
***Trigger Reverse Engineering結束***
Target Class: 6 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: 6.01404333114624
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000508----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.146109104156494
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000509----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 23.142169952392578
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000510----------------------------------------
***Pre-Screening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', '3-20', '10-15', '15-20', '17-20', '20-15', '21-20']
***Trigger Reverse Engineering開始***
Target: 21, victim: 20, Loss: 15.1456, Acc: 0.00%, CE_Loss: 15.15, Reg_Loss:2496.88, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2491.75:   9%|▉         | 86/1000 [03:49<40:42,  2.67s/it]
***Trigger Reverse Engineering結束***
Target Class: 0 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: 251.00414991378784
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000511----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.085107803344727
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000512----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.267090797424316
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000513----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['13-8', '14-1']
***Trigger Reverse Engineering開始***
Target: 13, victim: 8, Loss: 1.4495, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:179.81, Cost:0.01 best_reg:180.59 avg_loss_reg:180.59:  16%|▋         | 155/1000 [06:22<34:45,  2.47s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 8 Trigger Size: 179.80850219726562 Optimization Steps: 145
***Symmetric Check開始***
Target: 8, victim: 13, Loss: 0.4692, Acc: 85.00%, CE_Loss: 0.47, Reg_Loss:15403.12, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:15347.84: 100%|██████████| 145/145 [05:57<00:00,  2.47s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 751.1787374019623
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000514----------------------------------------
***Pre-Screening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', '2-6']
***Trigger Reverse Engineering開始***
Target: 2, victim: 3, Loss: 1.7907, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:67.55, Cost:0.03 best_reg:67.63 avg_loss_reg:67.63:  10%|          | 102/1000 [00:36<05:17,  2.83it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 3 Trigger Size: 67.55159759521484 Optimization Steps: 93
***Symmetric Check開始***
Target: 3, victim: 2, Loss: 1.8897, Acc: 95.00%, CE_Loss: 0.28, Reg_Loss:5423.27, Cost:0.00 best_reg:12199.41 avg_loss_reg:5503.18: 100%|| 93/93 [00:32<00:00,  2.87it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 73.57213521003723
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000515----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-1', '4-2', '4-5', '5-0']
***Trigger Reverse Engineering開始***
Target: 5, victim: 0, Loss: 3.3136, Acc: 20.00%, CE_Loss: 3.31, Reg_Loss:3948.22, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3649.38:   5%|          | 53/1000 [01:02<18:30,  1.17s/it]
***Trigger Reverse Engineering結束***
Target Class: 4 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: 67.69993734359741
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000516----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.565248250961304
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000517----------------------------------------
***Pre-Screening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', '4-3', '5-2']
***Trigger Reverse Engineering開始***
Target: 4, victim: 3, Loss: 4.3456, Acc: 100.00%, CE_Loss: 0.39, Reg_Loss:781.24, Cost:0.01 best_reg:782.48 avg_loss_reg:782.48:  27%|          | 271/1000 [10:06<27:11,  2.24s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 3 Trigger Size: 781.23681640625 Optimization Steps: 249
***Symmetric Check開始***
Target: 3, victim: 4, Loss: 2.5840, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:1057.22, Cost:0.00 best_reg:1031.29 avg_loss_reg:1057.62: 100%|| 249/249 [09:07<00:00,  2.20s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1164.1218991279602
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000518----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-4', '8-10', '10-8']
***Trigger Reverse Engineering開始***
Target: 10, victim: 8, Loss: 5.2189, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:649.29, Cost:0.01 best_reg:650.68 avg_loss_reg:650.68:  19%|          | 191/1000 [00:20<01:27,  9.25it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 8 Trigger Size: 649.28515625 Optimization Steps: 170
***Symmetric Check開始***
Target: 8, victim: 10, Loss: 3.1938, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:895.27, Cost:0.00 best_reg:894.97 avg_loss_reg:894.97: 100%|| 170/170 [00:17<00:00,  9.99it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 42.49762296676636
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000519----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-13', '9-13', '11-18', '21-2']
***Trigger Reverse Engineering開始***
Target: 21, victim: 2, Loss: 8.1945, Acc: 0.00%, CE_Loss: 8.19, Reg_Loss:2571.05, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2554.36:   5%|          | 53/1000 [01:27<26:08,  1.66s/it]
```

```
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 13 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: 104.89127492904663
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000520----------------------------------------
***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: 4.6352, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:4633.54, Cost:0.00 best_reg:4591.62 avg_loss_reg:4600.78:  16%|██          | 162/1000 [1:34:30<8:08:52, 35.00s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 4591.620465959822 Optimization Steps: 163
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 5689.902697563171
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000521----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 16
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 16, victim: 16, Loss: 0.1710, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:114.01, Cost:0.00 best_reg:118.79 avg_loss_reg:113.04:   5%|▌          | 54/1000 [11:12<3:16:26, 12.46s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 16 Victim Class: all Trigger Size: 118.78918711344402 Optimization Steps: 55
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 684.5530257225037
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000522----------------------------------------
***Pre-Screening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', '1-18', '17-18']
***Trigger Reverse Engineering開始***
Target: 17, victim: 18, Loss: 0.3620, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:874.48, Cost:0.00 best_reg:877.01 avg_loss_reg:864.72:  24%|██▍         | 236/1000 [10:54<35:18,  2.77s/it]
  0%|          | 0/215 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 17 Victim Class: 18 Trigger Size: 874.4785766601562 Optimization Steps: 215
***Symmetric Check開始***
Target: 18, victim: 17, Loss: 0.7516, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:902.30, Cost:0.00 best_reg:896.43 avg_loss_reg:901.21: 100%|██████████| 215/215 [09:54<00:00,  2.77s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1266.2277092933655
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000523----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.091041088104248
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000524----------------------------------------
***Pre-Screening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', '6-5']
***Trigger Reverse Engineering開始***
Target: 6, victim: 5, Loss: 10.6030, Acc: 0.00%, CE_Loss: 10.60, Reg_Loss:2575.43, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2556.40:   2%|▏          | 21/1000 [00:23<17:52,  1.10s/it]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 13 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 31.139619827270508
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000525----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
```

```
可能的 target-victim 配對: ['4-3']
***Trigger Reverse Engineering開始***
Target: 4, victim: 3, Loss: 5.8719, Acc: 25.00%, CE_Loss: 5.87, Reg_Loss:3329.36, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3133.80:   2%|          | 20/1000 [00:10<08:26,  1.93it/s]
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 3 Trigger Size: 10000000000.0 Optimization Steps: 21
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 16.903932809829712
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000526----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.114787578582764
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000527----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 21.072645902633667
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000528----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.481308937072754
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000529----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-17']
***Trigger Reverse Engineering開始***
Target: 3, victim: 17, Loss: 12.1405, Acc: 0.00%, CE_Loss: 12.14, Reg_Loss:2548.70, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2532.64:   1%|          | 10/1000 [00:03<06:34,  2.51it/s]
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 17 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: 10.650186538696289
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000530----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-19', '4-12', '4-0', '13-19', '16-19']
***Trigger Reverse Engineering開始***
Target: 16, victim: 19, Loss: 13.0143, Acc: 0.00%, CE_Loss: 13.01, Reg_Loss:2552.64, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2537.83:   5%|▌         | 54/1000 [01:21<23:49,  1.51s/it]
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 19 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 93.31725883483887
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000531----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-19', '0-23', '1-7', '1-8', '1-13', '2-4', '2-8', '2-13', '3-20', '4-5', '4-7', '4-8', '8-4', '8-7', '9-21', '10-21', '10-20', '10-8', '12-9', '12-14', '13-2', '13-7', '13-8', '14-20', '14-21', '15-6', '15-7', '17-20', '19-23', '21-22', '22-19', '22-21', '22-23', '23-0', '23-19']
***Trigger Reverse Engineering開始***
Target: 15, victim: 6, Loss: 0.9246, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:810.35, Cost:0.00 best_reg:812.94 avg_loss_reg:812.94:  70%|███████   | 704/1000 [37:06<15:36,  3.16s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 15 Victim Class: 6 Trigger Size: 810.35009765625 Optimization Steps: 172
***Symmetric Check開始***
Target: 6, victim: 15, Loss: 0.5054, Acc: 95.00%, CE_Loss: 0.24, Reg_Loss:10224.56, Cost:0.00 best_reg:18157.05 avg_loss_reg:10174.34: 100%|██████████| 172/172 [08:47<00:00,  3.07s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 2773.907059907913
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000532----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
```

```
整體耗時: 18.164676904678345
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000533----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['12-0']
***Trigger Reverse Engineering開始***
Target: 12, victim: 0, Loss: 0.9127, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:796.95, Cost:0.00 best_reg:797.85 avg_loss_reg:798.12:  21%|██        | 210/1000 [02:01<07:35,  1.73it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 0 Trigger Size: 796.9490356445312 Optimization Steps: 211
***Symmetric Check開始***
Target: 0, victim: 12, Loss: 2.9927, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:815.62, Cost:0.00 best_reg:834.10 avg_loss_reg:825.07:  60%|██████▏   | 126/211 [01:13<00:49,  1.71it/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: 200.77342987060547
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000534----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-3', '3-0']
***Trigger Reverse Engineering開始***
Target: 3, victim: 0, Loss: 10.4018, Acc: 0.00%, CE_Loss: 10.40, Reg_Loss:2536.95, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2528.01:   2%|          | 21/1000 [00:01<01:31, 10.69it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 3 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 3.8334460258483887
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000535----------------------------------------
***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: 8, Loss: 1.9468, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:6567.68, Cost:0.00 best_reg:6586.20 avg_loss_reg:6572.04:  14%|▏         | 139/1000 [44:54<4:38:10, 19.39s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 6586.198079427083 Optimization Steps: 140
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 2708.246204137802
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000536----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.330997228622437
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000537----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.170516014099121
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000538----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.363024711608887
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000539----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.898921012878418
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000540----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
```

```
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-4']
***Trigger Reverse Engineering開始***
Target: 5, victim: 4, Loss: 11.2666, Acc: 0.00%, CE_Loss: 11.27, Reg_Loss:2544.13, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2529.88:   1%|          | 10/1000 [00:21<35:07,  2.13s/it]
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 28.147724866867065
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000541----------------------------------------
***Pre-Screening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', '19-11', '19-15']
***Trigger Reverse Engineering開始***
Target: 19, victim: 15, Loss: 3.2307, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:408.44, Cost:0.01 best_reg:408.81 avg_loss_reg:408.81:  22%|██▏         | 224/1000 [06:26<22:18,  1.73s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 19 Victim Class: 15 Trigger Size: 408.43609619140625 Optimization Steps: 131
***Symmetric Check開始***
Target: 15, victim: 19, Loss: 2.6477, Acc: 90.00%, CE_Loss: 0.48, Reg_Loss:4881.30, Cost:0.00 best_reg:5132.06 avg_loss_reg:4920.69: 100%|██████████| 131/131 [03:51<00:00,  1.76s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 635.1289131641388
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000542----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.723332643508911
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000543----------------------------------------
***Pre-Screening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', '13-1', '14-1']
***Trigger Reverse Engineering開始***
Target: 14, victim: 1, Loss: 6.0228, Acc: 0.00%, CE_Loss: 6.02, Reg_Loss:2560.02, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2538.76:   4%|▍         | 42/1000 [01:45<40:01,  2.51s/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: 124.54310584068298
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000544----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.861485242843628
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000545----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.604986190795898
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000546----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-0', '6-7']
***Trigger Reverse Engineering開始***
Target: 6, victim: 7, Loss: 4.3019, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:160.28, Cost:0.03 best_reg:160.54 avg_loss_reg:161.87:  16%|█▋          | 155/1000 [00:24<02:12,  6.38it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 7 Trigger Size: 160.28134155273438 Optimization Steps: 148
***Symmetric Check開始***
Target: 7, victim: 6, Loss: 0.7409, Acc: 100.00%, CE_Loss: 0.58, Reg_Loss:6210.67, Cost:0.00 best_reg:6099.01 avg_loss_reg:6156.56: 100%|██████████| 148/148 [00:22<00:00,  6.50it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 53.23779606819153
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000547----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.283130407333374
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000548----------------------------------------
***Pre-Screening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', '2-11', '3-4', '6-0', '6-4', '6-11', '7-11', '9-0', '10-0']
***Trigger Reverse Engineering開始***
Target: 10, victim: 0, Loss: 7.1067, Acc: 0.00%, CE_Loss: 7.11, Reg_Loss:2572.20, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2557.04:  12%|          | 118/1000 [00:10<01:19, 11.15it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 15.330056428909302
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000549----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 17
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 17, victim: 22, Loss: 0.4714, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:41.38, Cost:0.01 best_reg:41.25 avg_loss_reg:41.47:   7%|          | 68/1000 [08:23<1:55:01,  7.40s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 17 Victim Class: all Trigger Size: 41.25106334686279 Optimization Steps: 69
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 509.0661692619324
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000550----------------------------------------
***Pre-Screening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', '2-4', '3-0', '3-1', '4-2']
***Trigger Reverse Engineering開始***
Target: 4, victim: 2, Loss: 10.7499, Acc: 0.00%, CE_Loss: 10.75, Reg_Loss:2570.34, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2552.69:   6%|          | 64/1000 [01:09<17:02,  1.09s/it]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 3 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 73.91453909873962
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000551----------------------------------------
***Pre-Screening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', '13-2', '13-5', '15-3', '21-1']
***Trigger Reverse Engineering開始***
Target: 21, victim: 1, Loss: 4.2196, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:154.43, Cost:0.03 best_reg:155.00 avg_loss_reg:155.38:  21%|          | 208/1000 [02:10<08:18,  1.59it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 21 Victim Class: 1 Trigger Size: 154.434814453125 Optimization Steps: 155
***Symmetric Check開始***
Target: 1, victim: 21, Loss: 3.1639, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:384.59, Cost:0.01 best_reg:390.54 avg_loss_reg:384.37: 100%|          | 155/155 [01:31<00:00,  1.70it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 231.13523888587952
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000552----------------------------------------
***Pre-Screening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', '18-10']
***Trigger Reverse Engineering開始***
Target: 18, victim: 10, Loss: 7.7960, Acc: 10.00%, CE_Loss: 7.80, Reg_Loss:3467.33, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3251.88:   3%|          | 31/1000 [01:13<38:09,  2.36s/it]
***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: 85.15221929550171
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000553----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.172771692276001
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000554----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.78081727027893
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000555----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-2']
***Trigger Reverse Engineering開始***
Target: 4, victim: 2, Loss: 11.9984, Acc: 0.00%, CE_Loss: 12.00, Reg_Loss:2572.55, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2553.41:   1%|          | 10/1000 [00:42<1:10:35,  4.28s/it]
***Trigger Reverse Engineering結束***
Target Class: 4 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: 71.22577786445618
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000556----------
***Pre-Screening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', '0-5', '0-6', '1-0', '2-8', '6-3', '6-4', '8-2']
***Trigger Reverse Engineering開始***
Target: 8, victim: 2, Loss: 9.1414, Acc: 0.00%, CE_Loss: 9.14, Reg_Loss:2555.63, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2541.75:   9%|▉         | 87/1000 [00:07<01:19, 11.48it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 12.035704374313354
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000557----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.943172216415405
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000558----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.047840595245361
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000559----------
***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: 0.3756, Acc: 93.75%, CE_Loss: 0.15, Reg_Loss:508.26, Cost:0.00 best_reg:546.90 avg_loss_reg:509.27:   4%|▍         | 45/1000 [08:04<2:51:20, 10.77s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: all Trigger Size: 546.9043518066406 Optimization Steps: 46
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 491.95978236198425
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000560----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-6']
***Trigger Reverse Engineering開始***
Target: 2, victim: 6, Loss: 10.8139, Acc: 0.00%, CE_Loss: 10.81, Reg_Loss:2575.44, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2557.24:   1%|          | 10/1000 [00:01<02:19,  7.08it/s]
***Trigger Reverse Engineering結束***
```

```
Target Class: 2 Victim Class: 6 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 3.5101823806762695
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000561----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 14.23822283744812
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000562----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.083018064498901
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000563----------
***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: 22, Loss: 2.5627, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:5760.08, Cost:0.00 best_reg:5601.66 avg_loss_reg:5669.43:  14%|▉         | 138/1000 [30:07<3:08:08, 13.10s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 5601.6558837890625 Optimization Steps: 139
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1819.8704240322113
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000564----------
***Pre-Screening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', '16-0', '19-0', '19-1']
***Trigger Reverse Engineering開始***
Target: 16, victim: 0, Loss: 2.0069, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:1802.23, Cost:0.00 best_reg:1802.64 avg_loss_reg:1794.10:  44%|████▍     | 435/1000 [02:20<03:03,  3.09it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 16 Victim Class: 0 Trigger Size: 1802.22705078125 Optimization Steps: 402
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 147.16095519065857
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000565----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 15.910375356674194
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000566----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-4', '6-12', '8-4', '8-7', '8-12', '10-1', '14-0', '15-3', '15-4', '15-10']
***Trigger Reverse Engineering開始***
Target: 15, victim: 3, Loss: 3.9901, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:340.05, Cost:0.01 best_reg:340.41 avg_loss_reg:340.41:  26%|██▋       | 263/1000 [06:29<18:10,  1.48s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 15 Victim Class: 3 Trigger Size: 340.0464782714844 Optimization Steps: 83
***Symmetric Check開始***
Target: 3, victim: 15, Loss: 1.3524, Acc: 100.00%, CE_Loss: 0.41, Reg_Loss:3196.65, Cost:0.00 best_reg:3224.75 avg_loss_reg:3224.75: 100%|██████████| 83/83 [02:02<00:00,  1.48s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 522.8435864448547
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000567----------
***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: 17, Loss: 0.4422, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:38.73, Cost:0.01 best_reg:38.48 avg_loss_reg:38.97:   8%|▉         | 79/1000 [22:26<4:21:32, 17.04s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 38.482114473978676 Optimization Steps: 80
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1355.764173746109
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000568----------------------------------------
***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: 3, Loss: 0.1663, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:1083.62, Cost:0.00 best_reg:1082.14 avg_loss_reg:1065.09:  18%|██        | 184/1000 [20:12<1:29:35,  6.59s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 1080.9166259765625 Optimization Steps: 185
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1220.8266117572784
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000569----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.250255346298218
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000570----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-19', '0-21', '0-22', '1-19', '11-21', '14-5', '15-17', '19-1', '20-19', '22-21', '23-1']
***Trigger Reverse Engineering開始***
Target: 14, victim: 5, Loss: 3.1244, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:1274.44, Cost:0.00 best_reg:1275.46 avg_loss_reg:1275.46:  30%|███       | 302/1000 [10:18<23:49,  2.05s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 5 Trigger Size: 1274.4359130859375 Optimization Steps: 192
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 629.776487827301
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000571----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.191042423248291
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000572----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-10', '1-13', '2-5', '10-7', '12-0', '13-0']
***Trigger Reverse Engineering開始***
Target: 10, victim: 7, Loss: 2.8645, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:105.16, Cost:0.03 best_reg:105.50 avg_loss_reg:106.69:  18%|█         | 179/1000 [01:16<05:52,  2.33it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 7 Trigger Size: 105.16439056396484 Optimization Steps: 114
***Symmetric Check開始***
Target: 7, victim: 10, Loss: 6.9945, Acc: 45.00%, CE_Loss: 1.03, Reg_Loss:13426.21, Cost:0.00 best_reg:23001.96 avg_loss_reg:13776.85: 100%|██████████| 114/114 [00:48<00:00,  2.34it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 133.4181671142578
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000573----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.728898763656616
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000574----------------------------------------
***Pre-Screening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', '7-1', '10-17']
***Trigger Reverse Engineering開始***
Target: 7, victim: 1, Loss: 1.1416, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:885.23, Cost:0.00 best_reg:887.64 avg_loss_reg:886.31:  62%|[redacted]| 623/1000 [05:44<03:28,  1.81it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 1 Trigger Size: 885.226806640625 Optimization Steps: 404
***Symmetric Check開始***
Target: 1, victim: 7, Loss: 2.5171, Acc: 15.00%, CE_Loss: 2.52, Reg_Loss:5782.18, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:5757.54:  50%|[redacted]| 200/404 [01:51<01:53,  1.80it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 462.5950481891632
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000575----------------------------------------
***Pre-Screening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: 4.0861, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:68.50, Cost:0.06 best_reg:69.83 avg_loss_reg:69.83:   6%|[redacted]| 62/1000 [00:10<02:33,  6.12it/s]
  0%|          | 0/63 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 7 Trigger Size: 68.50019836425781 Optimization Steps: 63
***Symmetric Check開始***
Target: 7, victim: 5, Loss: 1.7385, Acc: 0.00%, CE_Loss: 1.74, Reg_Loss:6983.76, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:6907.92: 100%|[redacted]| 63/63 [00:10<00:00,  6.15it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 23.665568113327026
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000576----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-1', '13-1', '15-1']
***Trigger Reverse Engineering開始***
Target: 15, victim: 1, Loss: 0.9409, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:553.89, Cost:0.00 best_reg:556.13 avg_loss_reg:556.13:  26%|[redacted]| 265/1000 [08:14<22:51,  1.87s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 15 Victim Class: 1 Trigger Size: 553.8919677734375 Optimization Steps: 224
***Symmetric Check開始***
Target: 1, victim: 15, Loss: 2.3771, Acc: 100.00%, CE_Loss: 0.37, Reg_Loss:3013.40, Cost:0.00 best_reg:3006.39 avg_loss_reg:3059.09: 100%|[redacted]| 224/224 [06:56<00:00,  1.86s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 925.6421337127686
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000577----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 3
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 3, victim: 3, Loss: 1.1826, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:525.45, Cost:0.00 best_reg:526.20 avg_loss_reg:526.20:  12%|[redacted]| 116/1000 [10:51<1:22:43,  5.61s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: all Trigger Size: 524.2131958007812 Optimization Steps: 117
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 657.6650137901306
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000578----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 3.8489797115325928
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000579----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
```

```
整體耗時: 2.0602707862854004
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000580----------
***Pre-Screening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', '4-2']
***Trigger Reverse Engineering開始***
Target: 4, victim: 2, Loss: 11.4366, Acc: 0.00%, CE_Loss: 11.44, Reg_Loss:2566.08, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2547.23:   2%|          | 21/1000 [00:37<29:25,  1.80s/it]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 45.692739725112915
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000581----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-22', '2-13', '3-5', '3-9', '3-19', '4-11', '4-19', '4-13', '6-22', '9-5', '10-11', '10-5', '10-3', '11-12', '11-19', '12-4', '12-11', '19-11', '19-12', '23-1', '23-22']
***Trigger Reverse Engineering開始***
Target: 19, victim: 12, Loss: 1.1265, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:433.39, Cost:0.00 best_reg:441.04 avg_loss_reg:441.04:  68%|[redacted]  | 676/1000 [08:07<03:53,  1.39it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 19 Victim Class: 12 Trigger Size: 433.3880310058594 Optimization Steps: 218
***Symmetric Check開始***
Target: 12, victim: 19, Loss: 3.7701, Acc: 90.00%, CE_Loss: 0.41, Reg_Loss:11348.51, Cost:0.00 best_reg:17046.46 avg_loss_reg:11788.08: 100%|[redacted]| 218/218 [02:51<00:00,  1.27it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 670.4567940235138
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000582----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-3', '0-15', '1-9', '4-7', '4-12', '5-7', '5-12', '6-4', '6-10', '8-9', '8-4', '8-1', '10-7', '14-2']
***Trigger Reverse Engineering開始***
Target: 8, victim: 1, Loss: 3.8778, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:145.44, Cost:0.03 best_reg:147.14 avg_loss_reg:144.11:  32%|[redacted]  | 317/1000 [09:29<20:27,  1.80s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 1 Trigger Size: 145.4407958984375 Optimization Steps: 95
***Symmetric Check開始***
Target: 1, victim: 8, Loss: 0.6991, Acc: 70.00%, CE_Loss: 0.70, Reg_Loss:16981.65, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:16894.49: 100%|[redacted]| 95/95 [02:47<00:00,  1.76s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 753.8526568412781
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000583----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-0']
***Trigger Reverse Engineering開始***
Target: 3, victim: 0, Loss: 6.4178, Acc: 10.00%, CE_Loss: 6.42, Reg_Loss:3052.59, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2927.46:   2%|          | 20/1000 [00:05<04:06,  3.97it/s]
***Trigger Reverse Engineering結束***
Target Class: 3 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: 10.48058295249939
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000584----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.08485221862793
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000585----------
***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: 11, Loss: 8.1480, Acc: 93.75%, CE_Loss: 0.08, Reg_Loss:5381.90, Cost:0.00 best_reg:5472.41 avg_loss_reg:5391.04:  11%|[redacted]  | 109/1000 [53:25<7:16:43, 29.41s/it]
```

```
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 5472.410705566406 Optimization Steps: 110
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 3221.573541164398
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000586----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-16', '20-21']
***Trigger Reverse Engineering開始***
Target: 20, victim: 21, Loss: 9.1024, Acc: 0.00%, CE_Loss: 9.10, Reg_Loss:2565.97, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2547.92:   2%|          | 21/1000 [00:02<01:35, 10.29it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 16 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 12.537878036499023
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000587----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.3591225147247314
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000588----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-11', '3-6', '3-13']
***Trigger Reverse Engineering開始***
Target: 3, victim: 13, Loss: 6.0264, Acc: 20.00%, CE_Loss: 6.03, Reg_Loss:3227.76, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3049.81:   5%|▌         | 52/1000 [00:11<03:33,  4.44it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 11 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 17.26356029510498
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000589----------------------------------------
***Pre-Screening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: 1, Loss: 1.8757, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:105.00, Cost:0.02 best_reg:105.08 avg_loss_reg:105.08:  16%|█▌        | 162/1000 [00:18<01:35,  8.81it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 1 Trigger Size: 105.00366973876953 Optimization Steps: 118
***Symmetric Check開始***
Target: 1, victim: 6, Loss: 7.5190, Acc: 30.00%, CE_Loss: 0.86, Reg_Loss:6657.34, Cost:0.00 best_reg:14625.24 avg_loss_reg:7214.89: 100%|██████████| 118/118 [00:13<00:00,  8.84it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 36.819767236709595
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000590----------------------------------------
***Pre-Screening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', '1-5', '1-0', '3-6']
***Trigger Reverse Engineering開始***
Target: 3, victim: 6, Loss: 7.6629, Acc: 10.00%, CE_Loss: 7.66, Reg_Loss:4138.95, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3696.73:   5%|▌         | 53/1000 [00:38<11:29,  1.37it/s]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 8 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 46.060728311538696
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000591----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['18-1']
***Trigger Reverse Engineering開始***
Target: 18, victim: 1, Loss: 5.1753, Acc: 20.00%, CE_Loss: 5.18, Reg_Loss:2927.72, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2819.88:   2%|          | 20/1000 [00:01<01:28, 11.11it/s]
```

```
***Trigger Reverse Engineering結束***
Target Class: 18 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: 6.83770489692688
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000592----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-15', '2-6', '2-9', '3-14', '3-16', '5-9', '6-7', '6-13', '7-13', '8-13', '9-5', '10-2', '11-2', '12-15', '13-7', '14-4', '15-1', '15-17', '16-15', '17-1']
***Trigger Reverse Engineering開始***
Target: 15, victim: 1, Loss: 0.6364, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:1793.33, Cost:0.00 best_reg:1796.31 avg_loss_reg:1830.53: 100%|██████████| 1000/1000 [43:36<00:00,  2.62s/it]
***Trigger Reverse Engineering結束***
Target Class: 15 Victim Class: 1 Trigger Size: 1793.328125 Optimization Steps: 637
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 2629.294574022293
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000593----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-12', '3-2', '4-1', '5-2', '5-6', '7-12', '8-2', '9-0', '9-1', '9-6', '10-4', '10-6', '11-0', '15-1']
***Trigger Reverse Engineering開始***
Target: 15, victim: 1, Loss: 8.1671, Acc: 0.00%, CE_Loss: 8.17, Reg_Loss:2548.50, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2537.87:  15%|█         | 153/1000 [00:13<01:16, 11.01it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 12 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 23.261059284210205
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000594----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-5', '1-4', '1-6', '2-4', '4-12', '5-14', '5-16', '6-12', '8-14', '11-4', '11-12', '14-3', '14-5', '16-5']
***Trigger Reverse Engineering開始***
Target: 5, victim: 14, Loss: 0.5870, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:2331.19, Cost:0.00 best_reg:2323.82 avg_loss_reg:2323.82: 100%|██████████| 1000/1000 [36:15<00:00,  2.18s/it]
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 14 Trigger Size: 2323.8232421875 Optimization Steps: 856
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 2190.445847272873
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000595----------------------------------------
***Pre-Screening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', '10-0', '14-4', '14-15', '17-15']
***Trigger Reverse Engineering開始***
Target: 14, victim: 4, Loss: 1.4724, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:182.89, Cost:0.01 best_reg:183.46 avg_loss_reg:183.46:  21%|██        | 207/1000 [08:18<31:51,  2.41s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 4 Trigger Size: 182.8880615234375 Optimization Steps: 133
***Symmetric Check開始***
Target: 4, victim: 14, Loss: 0.5284, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:3916.53, Cost:0.00 best_reg:12222.59 avg_loss_reg:3888.32: 100%|██████████| 133/133 [05:21<00:00,  2.42s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 833.0767560005188
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000596----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.070361614227295
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000597----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.730490922927856
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000598----------------------------------------
***Pre-Screening開始***
```

```
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.590410947799683
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000599----------
***Pre-Screening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']
***Trigger Reverse Engineering開始***
Target: 10, victim: 13, Loss: 2.7095, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:233.05, Cost:0.01 best_reg:233.12 avg_loss_reg:233.58:   9%|▉         | 93/1000 [06:11<1:00:19,  3.99s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 13 Trigger Size: 233.04537963867188 Optimization Steps: 94
***Symmetric Check開始***
Target: 13, victim: 10, Loss: 5.1421, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:11221.29, Cost:0.00 best_reg:11387.69 avg_loss_reg:11387.69: 100%|██████████| 94/94 [06:11<00:00,  3.95s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 761.2687764167786
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000600----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 23.153509616851807
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000601----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.348154067993164
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000602----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['7-9']
***Trigger Reverse Engineering開始***
Target: 7, victim: 9, Loss: 1.8292, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:220.44, Cost:0.01 best_reg:221.81 avg_loss_reg:222.50:  14%|▉         | 137/1000 [02:36<16:23,  1.14s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 9 Trigger Size: 220.4362030029297 Optimization Steps: 138
***Symmetric Check開始***
Target: 9, victim: 7, Loss: 1.7706, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:7196.47, Cost:0.00 best_reg:7225.23 avg_loss_reg:7225.23: 100%|██████████| 138/138 [02:35<00:00,  1.13s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 321.98487973213196
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000603----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.742900848388672
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000604----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 1.9415292739868164
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000605----------
***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: 1.1488, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:222.86, Cost:0.01 best_reg:217.52 avg_loss_reg:218.45:  11%|▉         | 106/1000 [02:47<23:35,  1.58s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: all Trigger Size: 217.52017822265626 Optimization Steps: 107
```

```
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 172.85949182510376
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000606----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 28.435882329940796
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000607----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 19.791624784469604
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000608----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.467063188552856
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000609----------------------------------------
***Pre-Screening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', '11-3']
***Trigger Reverse Engineering開始***
Target: 11, victim: 3, Loss: 8.5467, Acc: 0.00%, CE_Loss: 8.55, Reg_Loss:2531.10, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2523.77:   2%|          | 21/1000 [00:01<01:30, 10.87it/s]
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 8 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 6.82317042350769
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000610----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 14.730799913406372
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000611----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 3.323225498199463
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000612----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-6', '1-19', '2-5', '10-7', '15-5', '18-6', '19-18']
***Trigger Reverse Engineering開始***
Target: 19, victim: 18, Loss: 5.6812, Acc: 0.00%, CE_Loss: 5.68, Reg_Loss:2556.37, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2541.53:   9%|▉         | 86/1000 [03:09<33:38,  2.21s/it]
***Trigger Reverse Engineering結束***
Target Class: 1 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: 209.46600341796875
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000613----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-0']
***Trigger Reverse Engineering開始***
Target: 4, victim: 0, Loss: 6.8558, Acc: 0.00%, CE_Loss: 6.86, Reg_Loss:2547.51, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2533.54:   1%|          | 10/1000 [00:08<13:23,  1.23it/s]
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 16.902014017105103
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000614----------------------------------------
***Pre-Screening開始***
```

```
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.804539203643799
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000615----------
***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: 1.0222, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:2299.88, Cost:0.00 best_reg:2290.21 avg_loss_reg:2331.96:  11%|▉         | 108/1000 [29:20<4:02:21, 16.30s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 2290.21376953125 Optimization Steps: 109
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1773.8662333488464
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000616----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-10', '3-10']
***Trigger Reverse Engineering開始***
Target: 3, victim: 10, Loss: 13.3420, Acc: 0.00%, CE_Loss: 13.34, Reg_Loss:2525.62, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2518.22:   2%|          | 21/1000 [00:01<01:25, 11.40it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 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: 6.882972478866577
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000617----------
***Pre-Screening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', '7-0', '11-6']
***Trigger Reverse Engineering開始***
Target: 11, victim: 6, Loss: 3.9676, Acc: 0.00%, CE_Loss: 3.97, Reg_Loss:2593.75, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2571.87:   3%|          | 32/1000 [00:55<27:53,  1.73s/it]
***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: 68.95675468444824
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000618----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.971666574478149
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000619----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.411704301834106
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000620----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['8-0']
***Trigger Reverse Engineering開始***
Target: 8, victim: 0, Loss: 3.0129, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:365.14, Cost:0.01 best_reg:370.49 avg_loss_reg:362.58:  14%|▍         | 145/1000 [03:06<18:17,  1.28s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 0 Trigger Size: 365.1361083984375 Optimization Steps: 146
***Symmetric Check開始***
Target: 0, victim: 8, Loss: 1.6848, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:1400.89, Cost:0.00 best_reg:1367.34 avg_loss_reg:1394.87: 100%|██████████| 146/146 [03:06<00:00,  1.28s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 383.1164741516113
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000621----------
```

```
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 0
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 0, victim: 9, Loss: 0.3661, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:505.61, Cost:0.00 best_reg:505.39 avg_loss_reg:501.41:   8%|▌         | 79/1000 [03:39<42:36,  2.78s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 505.3899884905134 Optimization Steps: 80
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 225.0068655014038
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000622----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.5148446559906
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000623----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.803854703903198
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000624----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.249783992767334
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000625----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.3142478466033936
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000626----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.930661678314209
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000627----------
***Pre-Screening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: 14.0721, Acc: 0.00%, CE_Loss: 14.07, Reg_Loss:2546.60, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2536.25:   1%|          | 10/1000 [00:28<46:50,  2.84s/it]
***Trigger Reverse Engineering結束***
Target Class: 15 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: 51.637799978256226
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000628----------
***Pre-Screening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: 3.3185, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:54.92, Cost:0.06 best_reg:63.08 avg_loss_reg:54.68:  11%|▉         | 106/1000 [00:08<01:14, 11.98it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 2 Trigger Size: 54.91869354248047 Optimization Steps: 107
***Symmetric Check開始***
Target: 2, victim: 14, Loss: 6.0680, Acc: 90.00%, CE_Loss: 0.33, Reg_Loss:335.71, Cost:0.02 best_reg:362.55 avg_loss_reg:348.53: 100%|██████████| 107/107 [00:08<00:00, 12.03it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 22.747052669525146
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000629----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.465019226074219
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000630----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 17.690117359161377
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000631----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.609151601791382
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000632----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.30630087852478
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000633----------------------------------------
***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: 4, Loss: 0.3813, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:20.07, Cost:0.02 best_reg:21.51 avg_loss_reg:19.74:   6%|▌         | 58/1000 [01:35<25:53,  1.65s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 21.50739049911499 Optimization Steps: 59
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 100.25975275039673
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000634----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-21', '1-0', '1-9', '1-20', '2-13', '2-17', '3-10', '3-13', '4-13', '4-18', '6-4', '6-5', '6-14', '8-19', '10-3', '10-18', '10-20', '11-20', '11-12', '11-18', '12-18', '13-4', '13-18', '14-17', '15-17', '16-3', '16-14', '16-21', '17-10', '17-14', '17-0', '18-10', '20-1', '20-22', '21-0', '21-22', '22-1', '22-9', '22-21']
***Trigger Reverse Engineering開始***
Target: 22, victim: 21, Loss: 2.5122, Acc: 100.00%, CE_Loss: 0.33, Reg_Loss:971.88, Cost:0.00 best_reg:983.72 avg_loss_reg:983.72:  84%|▊▊▊▊▊▊▊▊▍  | 841/1000 [32:16<06:06,  2.30s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 22 Victim Class: 21 Trigger Size: 971.8803100585938 Optimization Steps: 192
***Symmetric Check開始***
Target: 21, victim: 22, Loss: 1.0115, Acc: 95.00%, CE_Loss: 0.21, Reg_Loss:537.31, Cost:0.00 best_reg:556.47 avg_loss_reg:538.50: 100%|▉▉▉▉▉▉▉▉▉▉| 192/192 [07:04<00:00,  2.21s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 2380.1892080307007
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000635----------------------------------------
***Pre-Screening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', '8-2', '8-3', '18-4', '19-3', '22-3']
***Trigger Reverse Engineering開始***
Target: 8, victim: 2, Loss: 1.3425, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:49.22, Cost:0.03 best_reg:49.67 avg_loss_reg:49.27:  15%|▏         | 154/1000 [08:51<48:39,  3.45s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 2 Trigger Size: 49.220436096191406 Optimization Steps: 87
***Symmetric Check開始***
Target: 2, victim: 8, Loss: 2.2699, Acc: 35.00%, CE_Loss: 2.27, Reg_Loss:23774.01, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:23644.20: 100%|▉▉▉▉▉▉▉▉▉▉| 87/87 [04:58<00:00,  3.43s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 859.0679321289062
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000636----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.470768690109253
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000637----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 19.734752416610718
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000638----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['11-12']
***Trigger Reverse Engineering開始***
Target: 11, victim: 12, Loss: 7.0287, Acc: 0.00%, CE_Loss: 7.03, Reg_Loss:2536.67, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2526.50:   1%|          | 10/1000 [00:30<50:45,  3.08s/it]
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 12 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 45.817421197891235
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000639----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 3
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 3, victim: 22, Loss: 0.1504, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:761.22, Cost:0.00 best_reg:803.79 avg_loss_reg:755.62:   6%|▌          | 60/1000 [1:09:24<18:07:24, 69.41s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: all Trigger Size: 803.7866048177083 Optimization Steps: 61
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 4183.792681932449
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000640----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.523850917816162
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000641----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.645679712295532
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000642----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.1350061893463135
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000643----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-1', '4-11']
***Trigger Reverse Engineering開始***
Target: 4, victim: 11, Loss: 3.8687, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:97.13, Cost:0.04 best_reg:98.29 avg_loss_reg:98.29:  13%|▏          | 129/1000 [00:11<01:16, 11.38it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 11 Trigger Size: 97.13165283203125 Optimization Steps: 90
***Symmetric Check開始***
Target: 11, victim: 4, Loss: 4.7368, Acc: 90.00%, CE_Loss: 0.53, Reg_Loss:1871.25, Cost:0.00 best_reg:2087.29 avg_loss_reg:1909.97: 100%|██████████| 90/90 [00:07<00:00, 11.55it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
```

```
整體耗時: 23.772928714752197
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000644----------
***Pre-Screening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', '5-13', '18-1', '19-1']
***Trigger Reverse Engineering開始***
Target: 19, victim: 1, Loss: 11.0630, Acc: 0.00%, CE_Loss: 11.06, Reg_Loss:2538.95, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2530.16:   5%|▌         | 53/1000 [01:30<26:49,  1.70s/it]
***Trigger Reverse Engineering結束***
Target Class: 0 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: 106.82014775276184
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000645----------
***Pre-Screening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']
***Trigger Reverse Engineering開始***
Target: 8, victim: 1, Loss: 7.1400, Acc: 0.00%, CE_Loss: 7.14, Reg_Loss:2558.43, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2546.68:   1%|         | 10/1000 [00:07<11:34,  1.43it/s]
***Trigger Reverse Engineering結束***
Target Class: 8 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: 14.016075611114502
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000646----------
***Pre-Screening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', '0-15', '2-10', '3-5', '4-8', '5-10', '5-8', '5-3', '6-0', '6-12', '6-13', '7-8', '8-5', '8-3', '8-14', '10-2', '10-4', '10-5', '11-1', '13-12', '15-14', '15-1', '15-11']
***Trigger Reverse Engineering開始***
Target: 8, victim: 3, Loss: 3.6248, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:94.26, Cost:0.04 best_reg:95.69 avg_loss_reg:95.69:  37%|███▋      | 370/1000 [08:23<14:17,  1.36s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 3 Trigger Size: 94.2636489868164 Optimization Steps: 72
***Symmetric Check開始***
Target: 3, victim: 8, Loss: 1.0692, Acc: 70.00%, CE_Loss: 1.07, Reg_Loss:12001.84, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:11945.58: 100%|██████████| 72/72 [01:30<00:00,  1.26s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 605.6252410411835
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000647----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-13', '2-14', '3-13', '9-1', '9-14', '11-5', '12-5', '12-16', '15-6', '17-16']
***Trigger Reverse Engineering開始***
Target: 9, victim: 1, Loss: 1.3749, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:1281.17, Cost:0.00 best_reg:1281.72 avg_loss_reg:1281.72:  35%|███▌      | 352/1000 [21:29<39:33,  3.66s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 1 Trigger Size: 1281.17138671875 Optimization Steps: 176
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1314.2148549556732
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000648----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 20.29254722595215
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000649----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.354369401931763
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000650----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-11', '8-11', '10-11']
```

```
***Trigger Reverse Engineering開始***
Target: 10, victim: 11, Loss: 7.4590, Acc: 0.00%, CE_Loss: 7.46, Reg_Loss:2497.12, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2497.88:   3%|▍         | 32/1000 [00:18<09:17,  1.74it/s]
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 11 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 27.135023832321167
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000651----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 22, Loss: 2.8162, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:4224.23, Cost:0.00 best_reg:4220.36 avg_loss_reg:4223.00:  20%|██        | 203/1000 [2:03:18<8:04:05, 36.44s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 4220.36181640625 Optimization Steps: 204
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 7416.994409561157
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000652----------------------------------------
***Pre-Screening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', '3-10']
***Trigger Reverse Engineering開始***
Target: 3, victim: 10, Loss: 3.1053, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:118.10, Cost:0.03 best_reg:119.13 avg_loss_reg:112.37:  13%|█▎        | 128/1000 [04:38<31:36,  2.18s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 10 Trigger Size: 118.10035705566406 Optimization Steps: 91
***Symmetric Check開始***
Target: 10, victim: 3, Loss: 1.0420, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:4297.76, Cost:0.00 best_reg:4374.31 avg_loss_reg:4374.31: 100%|██████████| 91/91 [03:16<00:00,  2.16s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 483.4890127182007
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000653----------------------------------------
***Pre-Screening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', '2-3', '3-2', '3-4', '3-8', '6-10', '6-7', '6-5', '7-5', '7-6', '8-2']
***Trigger Reverse Engineering開始***
Target: 6, victim: 5, Loss: 1.7442, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:1020.60, Cost:0.00 best_reg:1021.02 avg_loss_reg:1020.48:  60%|██████    | 603/1000 [13:33<08:55,  1.35s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 5 Trigger Size: 1020.60205078125 Optimization Steps: 416
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 823.4601445198059
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000654----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['13-6']
***Trigger Reverse Engineering開始***
Target: 13, victim: 6, Loss: 1.8131, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:1048.42, Cost:0.00 best_reg:1050.15 avg_loss_reg:1052.32:  94%|█████████▍| 940/1000 [23:59<01:31,  1.53s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 6 Trigger Size: 1048.416015625 Optimization Steps: 941
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1451.3768966197968
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000655----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-2', '5-6']
***Trigger Reverse Engineering開始***
Target: 5, victim: 6, Loss: 3.2949, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:36.93, Cost:0.09 best_reg:39.55 avg_loss_reg:39.55:   8%|▊         | 81/1000 [00:35<06:47,  2.26it/s]
early stop 所有
```

```
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 6 Trigger Size: 36.931026458740234 Optimization Steps: 70
***Symmetric Check開始***
Target: 6, victim: 5, Loss: 1.9218, Acc: 10.00%, CE_Loss: 1.92, Reg_Loss:6522.63, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:6451.48: 100%|[redacted]| 70/70 [00:30<00:00,  2.28it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 71.0315477848053
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000656----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 23
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 23, victim: 22, Loss: 0.2336, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:46.10, Cost:0.01 best_reg:44.92 avg_loss_reg:45.48:  10%|[redacted]         | 96/1000 [13:50<2:10:23,  8.65s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 23 Victim Class: all Trigger Size: 44.92218526204427 Optimization Steps: 97
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 837.3877494335175
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000657----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 11.432076692581177
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000658----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 16.57835030555725
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000659----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-0', '4-2']
***Trigger Reverse Engineering開始***
Target: 4, victim: 2, Loss: 5.4997, Acc: 0.00%, CE_Loss: 5.50, Reg_Loss:2578.87, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2558.30:   2%|[redacted]          | 21/1000 [00:05<04:00,  4.08it/s]
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 8.324453830718994
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000660----------------------------------------
***Pre-Screening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: 12.4748, Acc: 0.00%, CE_Loss: 12.47, Reg_Loss:2558.86, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2545.27:   1%|[redacted]          | 10/1000 [00:02<04:43,  3.49it/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: 9.11338496208191
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000661----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-13']
***Trigger Reverse Engineering開始***
Target: 2, victim: 13, Loss: 13.1293, Acc: 0.00%, CE_Loss: 13.13, Reg_Loss:2546.42, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2535.49:   1%|[redacted]          | 10/1000 [00:01<02:10,  7.56it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 13 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 6.998090028762817
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000662----------------------------------------
```

```
***Pre-Screening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', '5-1', '9-6', '9-11']
***Trigger Reverse Engineering開始***
Target: 9, victim: 6, Loss: 6.0371, Acc: 100.00%, CE_Loss: 0.38, Reg_Loss:3768.44, Cost:0.00 best_reg:3772.02 avg_loss_reg:3772.02:  31%|███       | 309/1000 [09:53<22:07,  1.92s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 6 Trigger Size: 3768.43701171875 Optimization Steps: 276
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 603.9759449958801
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000663----------------------------------------
***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: 4, Loss: 0.5035, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:2548.90, Cost:0.00 best_reg:2543.55 avg_loss_reg:2514.48:  23%|██        | 230/1000 [31:36<1:45:48,  8.24s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: all Trigger Size: 2543.5538940429688 Optimization Steps: 231
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1902.447039604187
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000664----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-3', '2-5', '7-1']
***Trigger Reverse Engineering開始***
Target: 2, victim: 5, Loss: 0.1659, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:2118.79, Cost:0.00 best_reg:2088.90 avg_loss_reg:2115.60: 100%|██████████| 1000/1000 [45:13<00:00,  2.71s/it]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 5 Trigger Size: 2088.895751953125 Optimization Steps: 977
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 2730.6394517421722
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000665----------------------------------------
***Pre-Screening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: 7.2909, Acc: 0.00%, CE_Loss: 7.29, Reg_Loss:2537.58, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2526.24:   1%|         | 10/1000 [00:15<26:13,  1.59s/it]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 34.70030760765076
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000666----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.526058912277222
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000667----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 15.331050634384155
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000668----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.466902017593384
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000669----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
```

```
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.110928773880005
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000670----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.919736623764038
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000671----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.17254114151001
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000672----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-16', '3-11', '10-3', '10-4', '11-3', '12-4']
***Trigger Reverse Engineering開始***
Target: 2, victim: 16, Loss: 1.1595, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:690.64, Cost:0.00 best_reg:703.23 avg_loss_reg:694.91:  30%|███       | 302/1000 [01:05<02:30,  4.64it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 16 Trigger Size: 690.636962890625 Optimization Steps: 218
***Symmetric Check開始***
Target: 16, victim: 2, Loss: 1.9598, Acc: 95.00%, CE_Loss: 0.36, Reg_Loss:1602.38, Cost:0.00 best_reg:1649.82 avg_loss_reg:1608.71: 100%|██████████| 218/218 [00:46<00:00,  4.65it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 118.14670515060425
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000673----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 16.57869577407837
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000674----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['9-14']
***Trigger Reverse Engineering開始***
Target: 9, victim: 14, Loss: 4.3517, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:32.76, Cost:0.13 best_reg:34.57 avg_loss_reg:34.57:   6%|▌         | 64/1000 [01:22<20:01,  1.28s/it]
  0%|          | 0/65 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 14 Trigger Size: 32.75567626953125 Optimization Steps: 65
***Symmetric Check開始***
Target: 14, victim: 9, Loss: 2.4571, Acc: 20.00%, CE_Loss: 2.46, Reg_Loss:14820.69, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:14760.00: 100%|██████████| 65/65 [01:22<00:00,  1.26s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 179.68475675582886
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000675----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 2.130906820297241
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000676----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.780931234359741
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000677----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.777793407440186
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000678----------------------------------------
***Pre-Screening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']
***Trigger Reverse Engineering開始***
Target: 1, victim: 20, Loss: 1.0873, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:411.37, Cost:0.00 best_reg:415.51 avg_loss_reg:415.51:  18%|██        | 184/1000 [14:08<1:02:43,  4.61s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 20 Trigger Size: 411.36968994140625 Optimization Steps: 185
***Symmetric Check開始***
Target: 20, victim: 1, Loss: 1.7781, Acc: 95.00%, CE_Loss: 0.35, Reg_Loss:952.76, Cost:0.00 best_reg:999.21 avg_loss_reg:950.30: 100%|██████████| 185/185 [14:09<00:00,  4.59s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1727.3869981765747
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000679----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-0']
***Trigger Reverse Engineering開始***
Target: 4, victim: 0, Loss: 2.0641, Acc: 25.00%, CE_Loss: 2.06, Reg_Loss:3002.70, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2882.85:   2%|▏         | 20/1000 [01:30<1:13:45,  4.52s/it]
***Trigger Reverse Engineering結束***
Target Class: 4 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: 112.15475869178772
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000680----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 1.5067570209503174
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000681----------------------------------------
***Pre-Screening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']
***Trigger Reverse Engineering開始***
Target: 0, victim: 15, Loss: 1.2714, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:512.88, Cost:0.00 best_reg:514.32 avg_loss_reg:514.32:  20%|██        | 198/1000 [07:12<29:11,  2.18s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 15 Trigger Size: 512.8826904296875 Optimization Steps: 199
***Symmetric Check開始***
Target: 15, victim: 0, Loss: 4.0109, Acc: 100.00%, CE_Loss: 0.45, Reg_Loss:1054.06, Cost:0.00 best_reg:1047.92 avg_loss_reg:1043.06: 100%|██████████| 199/199 [07:12<00:00,  2.17s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 881.8849618434906
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000682----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '1-0', '3-6', '3-8', '7-8', '10-2', '11-6']
***Trigger Reverse Engineering開始***
Target: 11, victim: 6, Loss: 13.7306, Acc: 0.00%, CE_Loss: 13.73, Reg_Loss:2560.59, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2544.49:  10%|▉         | 96/1000 [00:43<06:46,  2.22it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 49.22421908378601
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000683----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 18.853120803833008
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000684----------------------------------------
***Pre-Screening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']
***Trigger Reverse Engineering開始***
Target: 3, victim: 8, Loss: 0.6416, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:235.20, Cost:0.00 best_reg:223.51 avg_loss_reg:231.05: 100%|██████████| 1000/1000 [09:39<00:00,  1.73it/s]
  0%|          | 0/1000 [00:00<?, ?it/s]***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 8 Trigger Size: 223.5057373046875 Optimization Steps: 1000
***Symmetric Check開始***
Target: 8, victim: 3, Loss: 4.1772, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:2578.38, Cost:0.00 best_reg:2579.81 avg_loss_reg:2594.51:  34%|███▍      | 343/1000 [03:19<06:22,  1.72it/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: 787.1261568069458
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000685----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 11
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 11, victim: 16, Loss: 0.1108, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:166.26, Cost:0.00 best_reg:168.92 avg_loss_reg:165.75:  10%|▉         | 95/1000 [09:29<1:30:21,  5.99s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: all Trigger Size: 168.91581217447916 Optimization Steps: 96
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 576.4152617454529
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000686----------------------------------------
***Pre-Screening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: 1.2857, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:237.73, Cost:0.01 best_reg:238.45 avg_loss_reg:238.45:  15%|▏         | 146/1000 [00:23<02:14,  6.34it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 237.72679138183594 Optimization Steps: 147
***Symmetric Check開始***
Target: 1, victim: 2, Loss: 1.1302, Acc: 95.00%, CE_Loss: 0.12, Reg_Loss:1519.89, Cost:0.00 best_reg:1569.70 avg_loss_reg:1520.63: 100%|██████████| 147/147 [00:23<00:00,  6.34it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 52.078930139541626
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000687----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-3']
***Trigger Reverse Engineering開始***
Target: 0, victim: 3, Loss: 4.4993, Acc: 20.00%, CE_Loss: 4.50, Reg_Loss:3479.14, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3234.86:   2%|▏         | 20/1000 [00:40<33:13,  2.03s/it]
***Trigger Reverse Engineering結束***
Target Class: 0 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: 47.284698724746704
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000688----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['12-0']
***Trigger Reverse Engineering開始***
Target: 12, victim: 0, Loss: 7.3933, Acc: 0.00%, CE_Loss: 7.39, Reg_Loss:2550.46, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2539.51:   1%|▏         | 10/1000 [00:12<20:56,  1.27s/it]
***Trigger Reverse Engineering結束***
Target Class: 12 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: 23.71685028076172
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000689----------------------------------------
***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: 12, Loss: 2.9553, Acc: 91.67%, CE_Loss: 0.46, Reg_Loss:12.81, Cost:0.19 best_reg:12.83 avg_loss_reg:12.78: 10%|▉ | 103/1000 [1:04:17<9:19:53, 37.45s/it]
early stop 所有
Trigger Reverse Engineering結束
Target Class: 8 Victim Class: all Trigger Size: 12.82270728217231 Optimization Steps: 104
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 3876.8685262203217
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000690----------
Pre-Screening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']
Trigger Reverse Engineering開始
Target: 2, victim: 9, Loss: 11.7419, Acc: 0.00%, CE_Loss: 11.74, Reg_Loss:2531.56, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2526.17:   1%| | 10/1000 [00:11<19:15, 1.17s/it]
Trigger Reverse Engineering結束
Target Class: 2 Victim Class: 9 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 19.89568018913269
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000691----------
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: 4, Loss: 0.3427, Acc: 95.83%, CE_Loss: 0.03, Reg_Loss:92.49, Cost:0.00 best_reg:93.21 avg_loss_reg:91.92:   6%|▋ | 65/1000 [01:23<20:06, 1.29s/it]
early stop 所有
Trigger Reverse Engineering結束
Target Class: 2 Victim Class: all Trigger Size: 93.21238708496094 Optimization Steps: 66
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 89.10876369476318
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000692----------
Pre-Screening開始
Pre-Screening結束
檢測結束
檢測結果: Model是安全的(Benign)
整體耗時: 20.58068609237671
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000693----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-19', '5-6', '5-21', '9-10', '10-9', '12-11', '13-3', '13-21', '14-21', '15-6', '16-9', '16-10', '17-6', '18-21', '20-6']
Trigger Reverse Engineering開始
Target: 16, victim: 9, Loss: 1.4494, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:549.04, Cost:0.00 best_reg:558.36 avg_loss_reg:558.36: 36%|▍▍▍▍ | 365/1000 [13:08<22:52, 2.16s/it]
early stop 所有
Trigger Reverse Engineering結束
Target Class: 16 Victim Class: 9 Trigger Size: 549.0377807617188 Optimization Steps: 174
Symmetric Check開始
Target: 9, victim: 16, Loss: 2.6490, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:3645.03, Cost:0.00 best_reg:3634.60 avg_loss_reg:3652.31: 100%|▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉| 174/174 [06:15<00:00, 2.16s/it]
Symmetric Check結束
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1184.7377574443817
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000694----------
Pre-Screening開始
Pre-Screening結束
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['8-4']
Trigger Reverse Engineering開始
Target: 8, victim: 4, Loss: 3.4796, Acc: 90.00%, CE_Loss: 0.28, Reg_Loss:947.28, Cost:0.00 best_reg:946.05 avg_loss_reg:946.09: 100%|▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉| 1000/1000 [11:14<00:00, 1.48it/s]
Trigger Reverse Engineering結束
Target Class: 8 Victim Class: 4 Trigger Size: 946.0474853515625 Optimization Steps: 1000
Symmetric Check開始
Target: 4, victim: 8, Loss: 2.6015, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:3454.75, Cost:0.00 best_reg:3457.81 avg_loss_reg:3474.77: 51%|▌▌▌▌▌ | 513/1000 [05:46<05:28, 1.48it/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: 1027.8068509101868
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000695----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.718286037445068
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000696----------
***Pre-Screening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', '3-2', '21-2']
***Trigger Reverse Engineering開始***
Target: 21, victim: 2, Loss: 10.3151, Acc: 0.00%, CE_Loss: 10.32, Reg_Loss:2521.05, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2514.59:   3%|▌          | 32/1000 [01:12<36:26,  2.26s/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: 94.64382028579712
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000697----------
***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: 0.4455, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:23.58, Cost:0.02 best_reg:25.39 avg_loss_reg:23.52:   6%|▉          | 64/1000 [00:31<07:41,  2.03it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 25.389612197875977 Optimization Steps: 65
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 33.49763107299805
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000698----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-16', '2-3', '3-2', '4-11', '16-1', '17-2']
***Trigger Reverse Engineering開始***
Target: 3, victim: 2, Loss: 1.6123, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:640.10, Cost:0.00 best_reg:640.45 avg_loss_reg:644.78:  91%|[redacted]  | 914/1000 [27:16<02:34,  1.79s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 2 Trigger Size: 640.1043701171875 Optimization Steps: 726
***Symmetric Check開始***
Target: 2, victim: 3, Loss: 3.5070, Acc: 90.00%, CE_Loss: 0.32, Reg_Loss:3188.06, Cost:0.00 best_reg:3234.84 avg_loss_reg:3187.92: 100%|[redacted]| 726/726 [19:50<00:00,  1.64s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 2841.84259724617
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000699----------
***Pre-Screening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']
***Trigger Reverse Engineering開始***
Target: 11, victim: 1, Loss: 9.4002, Acc: 5.00%, CE_Loss: 9.40, Reg_Loss:2858.24, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2771.65:   2%|▏          | 20/1000 [00:09<07:59,  2.04it/s]
***Trigger Reverse Engineering結束***
Target Class: 11 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: 20.151041984558105
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000700----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['7-0', '7-11']
***Trigger Reverse Engineering開始***
Target: 7, victim: 11, Loss: 2.8605, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:48.64, Cost:0.06 best_reg:48.89 avg_loss_reg:48.98:  10%|▊         | 104/1000 [03:30<30:11,  2.02s/it]
early stop 所有
```

```
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 11 Trigger Size: 48.642311096191406 Optimization Steps: 70
***Symmetric Check開始***
Target: 11, victim: 7, Loss: 0.9386, Acc: 80.00%, CE_Loss: 0.94, Reg_Loss:14407.58, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:14319.05: 100%|██████████| 70/70 [02:20<00:00,  2.01s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 363.8659689426422
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000701----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.618107080459595
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000702----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.191958427429199
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000703----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 23.481870651245117
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000704----------------------------------------
***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: 10.8198, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:4788.56, Cost:0.00 best_reg:4779.12 avg_loss_reg:4787.68:  19%|██        | 193/1000 [47:26<3:18:20, 14.75s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 4778.8970947265625 Optimization Steps: 194
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 2859.2218952178955
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000705----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.072410106658936
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000706----------------------------------------
***Pre-Screening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']
***Trigger Reverse Engineering開始***
Target: 0, victim: 1, Loss: 10.3407, Acc: 0.00%, CE_Loss: 10.34, Reg_Loss:2559.91, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2544.72:   1%|         | 10/1000 [00:01<02:04,  7.98it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 6.113981008529663
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000707----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['9-1']
***Trigger Reverse Engineering開始***
Target: 9, victim: 1, Loss: 12.2789, Acc: 0.00%, CE_Loss: 12.28, Reg_Loss:2579.03, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2560.01:   1%|         | 10/1000 [00:01<02:35,  6.36it/s]
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 6.911442756652832
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000708----------------------------------------
```

```
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.035977840423584
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000709----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-12', '7-2', '7-12', '14-12']
***Trigger Reverse Engineering開始***
Target: 14, victim: 12, Loss: 10.3063, Acc: 0.00%, CE_Loss: 10.31, Reg_Loss:2579.40, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2559.17:   4%|▌         | 43/1000 [00:04<01:47,  8.92it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 12 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 9.917515277862549
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000710----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 17.292698860168457
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000711----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.897483825683594
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000712----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-6', '8-6', '15-6', '15-10', '17-18', '21-6']
***Trigger Reverse Engineering開始***
Target: 21, victim: 6, Loss: 12.1124, Acc: 0.00%, CE_Loss: 12.11, Reg_Loss:2549.18, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2536.79:   6%|▌         | 65/1000 [00:20<04:57,  3.14it/s]
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 6 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 27.61710786819458
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000713----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.882686614990234
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000714----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 13
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 13, victim: 12, Loss: 0.3804, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:570.40, Cost:0.00 best_reg:562.74 avg_loss_reg:565.14:  10%|▉         | 99/1000 [49:27<7:30:09, 29.98s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: all Trigger Size: 562.7442355685764 Optimization Steps: 100
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 2984.7816500663757
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000715----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 14, Loss: 0.4672, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:202.01, Cost:0.00 best_reg:203.81 avg_loss_reg:201.60:   6%|▌         | 65/1000 [38:15<9:10:23, 35.32s/it]
early stop 所有
***Trigger Reverse Engineering結束***
```

```
Target Class: 2 Victim Class: all Trigger Size: 203.8075393676758 Optimization Steps: 66
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 2314.777684688568
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000716----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-6']
***Trigger Reverse Engineering開始***
Target: 0, victim: 6, Loss: 2.8356, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:801.25, Cost:0.00 best_reg:803.33 avg_loss_reg:796.24:  12%|          | 121/1000 [00:37<04:35,  3.19it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 6 Trigger Size: 801.2451171875 Optimization Steps: 122
***Symmetric Check開始***
Target: 6, victim: 0, Loss: 2.2999, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:4779.47, Cost:0.00 best_reg:4780.58 avg_loss_reg:4795.71: 100%|| 122/122 [00:38<00:00,  3.15it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 82.74287629127502
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000717----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-12', '9-12']
***Trigger Reverse Engineering開始***
Target: 9, victim: 12, Loss: 1.0474, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:612.21, Cost:0.00 best_reg:613.10 avg_loss_reg:613.10:  19%|          | 187/1000 [16:43<1:12:42,  5.37s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 12 Trigger Size: 612.2073974609375 Optimization Steps: 177
***Symmetric Check開始***
Target: 12, victim: 9, Loss: 2.4012, Acc: 95.00%, CE_Loss: 0.43, Reg_Loss:2954.34, Cost:0.00 best_reg:3074.04 avg_loss_reg:2968.75: 100%|| 177/177 [15:44<00:00,  5.34s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1971.8763029575348
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000718----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 25.312814235687256
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000719----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['10-0']
***Trigger Reverse Engineering開始***
Target: 10, victim: 0, Loss: 10.1701, Acc: 0.00%, CE_Loss: 10.17, Reg_Loss:2541.75, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2531.86:   1%|          | 10/1000 [00:03<06:07,  2.69it/s]
***Trigger Reverse Engineering結束***
Target Class: 10 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: 9.31330132484436
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000720----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.403835773468018
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000721----------------------------------------
***Pre-Screening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', '11-12', '11-16', '12-16']
***Trigger Reverse Engineering開始***
Target: 11, victim: 16, Loss: 1.9336, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:21.83, Cost:0.09 best_reg:22.51 avg_loss_reg:22.51:  18%|          | 175/1000 [01:15<05:54,  2.32it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 16 Trigger Size: 21.83353042602539 Optimization Steps: 80
***Symmetric Check開始***
```

```
Target: 16, victim: 11, Loss: 4.5419, Acc: 20.00%, CE_Loss: 4.54, Reg_Loss:12701.46, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:12545.80: 100%|[redacted]| 80/80 [00:34<00:00,  2.33it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 116.69450879096985
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000722----------------------------------------
***Pre-Screening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']
***Trigger Reverse Engineering開始***
Target: 11, victim: 1, Loss: 6.0542, Acc: 0.00%, CE_Loss: 6.05, Reg_Loss:2546.54, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2534.49:   1%|         | 10/1000 [00:01<02:56,  5.59it/s]
***Trigger Reverse Engineering結束***
Target Class: 11 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: 9.031298398971558
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000723----------------------------------------
***Pre-Screening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', '3-2', '3-8', '4-0', '4-3', '4-7', '5-6', '5-8', '6-12', '6-3', '6-0', '8-2', '8-6', '8-7']
***Trigger Reverse Engineering開始***
Target: 0, victim: 12, Loss: 1.3666, Acc: 100.00%, CE_Loss: 0.33, Reg_Loss:693.76, Cost:0.00 best_reg:672.58 avg_loss_reg:692.79: 100%|[redacted]| 1000/1000 [03:25<00:00,  4.86it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 12 Trigger Size: 672.581787109375 Optimization Steps: 857
***Symmetric Check開始***
Target: 12, victim: 0, Loss: 2.0937, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:1838.54, Cost:0.00 best_reg:1840.42 avg_loss_reg:1809.74:  47%|[redacted]     | 407/857 [01:24<01:33,  4.83it/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: 295.20368337631226
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000724----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.10049033164978
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000725----------------------------------------
***Pre-Screening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', '9-11', '15-3']
***Trigger Reverse Engineering開始***
Target: 15, victim: 3, Loss: 11.6112, Acc: 5.00%, CE_Loss: 11.61, Reg_Loss:3915.67, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3549.89:   6%|▌         | 62/1000 [00:23<05:50,  2.68it/s]
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 15 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: 31.230525732040405
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000726----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.968591213226318
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000727----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.286365747451782
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000728----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['13-0']
***Trigger Reverse Engineering開始***
Target: 13, victim: 0, Loss: 13.6380, Acc: 0.00%, CE_Loss: 13.64, Reg_Loss:2548.91, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2536.98:   1%|         | 10/1000 [00:11<18:32,  1.12s/it]
***Trigger Reverse Engineering結束***
```

```
Target Class: 13 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 20.9816153049469
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000729----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.113463640213013
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000730----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-4', '1-9', '4-0', '8-9', '8-10', '9-10']
***Trigger Reverse Engineering開始***
Target: 8, victim: 9, Loss: 0.9708, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:1023.28, Cost:0.00 best_reg:1025.14 avg_loss_reg:1019.70:  60%|[redacted]  | 595/1000 [07:32<05:08,  1.31it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 9 Trigger Size: 1023.2766723632812 Optimization Steps: 540
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 460.4918522834778
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000731----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-21', '0-22', '1-9', '1-10', '1-18', '2-7', '2-16', '3-2', '3-13', '4-17', '4-18', '5-6', '5-13', '5-16', '6-16', '6-13', '6-5', '8-2', '8-16', '9-16', '9-5', '9-2', '10-1', '10-18', '11-15', '11-18', '11-21', '12-19', '13-6', '13-5', '13-8', '14-1', '15-17', '16-2', '16-6', '16-7', '17-11', '17-15', '18-15', '18-21', '19-12', '19-15', '19-17', '20-0', '20-4', '20-21', '21-0', '21-20', '22-0', '22-20']
***Trigger Reverse Engineering開始***
Target: 0, victim: 22, Loss: 1.0856, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:1439.53, Cost:0.00 best_reg:1442.64 avg_loss_reg:1444.89: 100%|[redacted]| 997/1000 [09:25<00:01,  1.76it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 22 Trigger Size: 1439.5318603515625 Optimization Steps: 256
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 572.6002960205078
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000732----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.149557113647461
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000733----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-2', '4-9', '5-2']
***Trigger Reverse Engineering開始***
Target: 4, victim: 9, Loss: 2.5614, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:44.31, Cost:0.06 best_reg:45.91 avg_loss_reg:44.52:  12%|[redacted]  | 123/1000 [05:22<38:20,  2.62s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 9 Trigger Size: 44.307952880859375 Optimization Steps: 71
***Symmetric Check開始***
Target: 9, victim: 4, Loss: 1.5890, Acc: 30.00%, CE_Loss: 1.59, Reg_Loss:22831.02, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:22714.28: 100%|[redacted]| 71/71 [03:03<00:00,  2.59s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 523.4543125629425
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000734----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-4']
***Trigger Reverse Engineering開始***
Target: 6, victim: 4, Loss: 5.3666, Acc: 10.00%, CE_Loss: 5.37, Reg_Loss:3301.15, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3139.69:   2%|[redacted]  | 20/1000 [00:03<02:43,  6.01it/s]
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 21
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 8.137158155441284
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000735----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 14.69479250907898
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000736----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.977197885513306
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000737----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-6', '2-9', '2-11', '5-6', '8-6', '9-2', '11-2']
***Trigger Reverse Engineering開始***
Target: 5, victim: 6, Loss: 2.1440, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:264.51, Cost:0.01 best_reg:267.42 avg_loss_reg:267.42:  31%|███       | 307/1000 [00:35<01:19,  8.71it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 6 Trigger Size: 264.51239013671875 Optimization Steps: 156
***Symmetric Check開始***
Target: 6, victim: 5, Loss: 4.8885, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:1366.86, Cost:0.00 best_reg:1375.47 avg_loss_reg:1375.47: 100%|████████████| 156/156 [00:18<00:00,  8.44it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 59.214218854904175
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round3\TrainData\models\unzip\id-00000738----------------------------------------
***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***

```