```
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\Round2\TrainData\models\unzip\id-00000000----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-4']
***Trigger Reverse Engineering開始***
Target: 5, victim: 4, Loss: 1.4645, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:584.51, Cost:0.00 best_reg:585.27 avg_loss_reg:585.27:  14%|▉         | 135/1000 [13:47<1:28:20,  6.13s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 4 Trigger Size: 584.5062866210938 Optimization Steps: 136
***Symmetric Check開始***
Target: 4, victim: 5, Loss: 1.8918, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:527.20, Cost:0.00 best_reg:534.79 avg_loss_reg:534.79: 100%|██████████| 136/136 [13:45<00:00,  6.07s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1664.0562598705292
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000001----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-2', '2-0', '2-3', '3-2', '4-5', '5-4', '6-7', '6-9', '6-10', '7-3', '7-6', '7-8', '9-10', '10-9']
***Trigger Reverse Engineering開始***
Target: 10, victim: 9, Loss: 3.8212, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:140.21, Cost:0.03 best_reg:143.06 avg_loss_reg:137.11:  38%|███▊      | 385/1000 [05:36<08:57,  1.14it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 9 Trigger Size: 140.2120819091797 Optimization Steps: 116
***Symmetric Check開始***
Target: 9, victim: 10, Loss: 5.9592, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:147.86, Cost:0.04 best_reg:148.80 avg_loss_reg:148.80:  85%|████████▌ | 99/116 [01:30<00:15,  1.10it/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: 432.83162903785706
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000002----------------------------------------
***Pre-Screening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', '1-2', '1-12', '1-10', '2-3', '2-12', '2-17', '3-2', '5-13', '6-7', '7-8', '7-17', '9-3', '10-20', '12-2', '12-10', '12-11', '14-22', '14-11', '14-13', '15-13', '17-18', '18-12', '18-17', '19-21', '20-21', '21-17', '22-12', '22-13']
***Trigger Reverse Engineering開始***
Target: 7, victim: 8, Loss: 0.9186, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:108.16, Cost:0.01 best_reg:108.97 avg_loss_reg:108.97:  54%|█████▍    | 542/1000 [14:20<12:07,  1.59s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 8 Trigger Size: 108.15702819824219 Optimization Steps: 128
***Symmetric Check開始***
Target: 8, victim: 7, Loss: 4.2450, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:227.92, Cost:0.02 best_reg:229.15 avg_loss_reg:229.15:  93%|█████████▎| 119/128 [03:10<00:14,  1.60s/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: 1061.6695308685303
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000003----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-5', '3-2']
***Trigger Reverse Engineering開始***
Target: 3, victim: 2, Loss: 8.2946, Acc: 0.00%, CE_Loss: 8.29, Reg_Loss:2535.91, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2525.93:   2%|▏         | 21/1000 [00:14<11:27,  1.42it/s]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 16.350885152816772
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000004----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-2']
***Trigger Reverse Engineering開始***
Target: 3, victim: 2, Loss: 1.5550, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:87.41, Cost:0.02 best_reg:87.49 avg_loss_reg:87.08:  11%|▉         | 111/1000 [10:28<1:23:55,  5.66s/it]
  0%|          | 0/112 [00:00<?, ?it/s]early stop 所有
```

```
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 2 Trigger Size: 87.41078186035156 Optimization Steps: 112
***Symmetric Check開始***
Target: 2, victim: 3, Loss: 3.2985, Acc: 95.00%, CE_Loss: 0.27, Reg_Loss:598.89, Cost:0.01 best_reg:623.76 avg_loss_reg:607.06: 100%|[redacted]| 112/112 [10:08<00:00,  5.43s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1248.842206478119
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000005----------------------------------------
***Pre-Screening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']
***Trigger Reverse Engineering開始***
Target: 5, victim: 2, Loss: 1.9492, Acc: 100.00%, CE_Loss: 0.33, Reg_Loss:319.00, Cost:0.01 best_reg:319.39 avg_loss_reg:319.39:  18%|[redacted]        | 175/1000 [09:53<46:39,  3.39s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 2 Trigger Size: 319.00030517578125 Optimization Steps: 176
***Symmetric Check開始***
Target: 2, victim: 5, Loss: 1.1515, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:993.02, Cost:0.00 best_reg:980.25 avg_loss_reg:991.94: 100%|[redacted]| 176/176 [09:54<00:00,  3.38s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1193.2117941379547
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000006----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 19.261308908462524
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000007----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '4-7', '7-4']
***Trigger Reverse Engineering開始***
Target: 4, victim: 7, Loss: 1.1163, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:207.17, Cost:0.01 best_reg:207.29 avg_loss_reg:207.35:  17%|[redacted]        | 168/1000 [15:25<1:16:22,  5.51s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 7 Trigger Size: 207.17459106445312 Optimization Steps: 117
***Symmetric Check開始***
Target: 7, victim: 4, Loss: 1.0057, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:3167.37, Cost:0.00 best_reg:3286.24 avg_loss_reg:3286.24: 100%|[redacted]| 117/117 [10:34<00:00,  5.43s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1572.5823483467102
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000008----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.416816234588623
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000009----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-18', '0-19', '2-5', '2-12', '3-1', '5-6', '7-11', '8-7', '9-10', '10-7', '11-7', '12-5', '14-0', '14-13', '15-16', '16-15']
***Trigger Reverse Engineering開始***
Target: 11, victim: 7, Loss: 2.7093, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:498.94, Cost:0.01 best_reg:499.64 avg_loss_reg:499.64:  54%|[redacted]     | 543/1000 [31:33<26:33,  3.49s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 7 Trigger Size: 498.9437255859375 Optimization Steps: 205
***Symmetric Check開始***
Target: 7, victim: 11, Loss: 1.6747, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:295.83, Cost:0.01 best_reg:296.36 avg_loss_reg:296.63:  68%|[redacted]   | 139/205 [08:05<03:50,  3.50s/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: 2393.0403583049774
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000010----------------------------------------
***Pre-Screening開始***
```

```
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['12-11', '13-11', '13-12']
***Trigger Reverse Engineering開始***
Target: 13, victim: 11, Loss: 6.7275, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:373.24, Cost:0.02 best_reg:373.34 avg_loss_reg:373.34:  20%|██        | 201/1000 [06:28<25:44,  1.93s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 11 Trigger Size: 373.2357482910156 Optimization Steps: 138
***Symmetric Check開始***
Target: 11, victim: 13, Loss: 4.6726, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:260.59, Cost:0.02 best_reg:261.16 avg_loss_reg:261.16:  98%|██████████| 135/138 [04:18<00:05,  1.91s/it]
early stop 所有
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 654.291360616684
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000011----------
***Pre-Screening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', '3-5', '5-4', '6-7', '7-6', '8-0']
***Trigger Reverse Engineering開始***
Target: 5, victim: 4, Loss: 0.3666, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:123.57, Cost:0.00 best_reg:124.44 avg_loss_reg:124.44:  46%|████▋     | 463/1000 [07:53<09:09,  1.02s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 4 Trigger Size: 123.57212829589844 Optimization Steps: 223
***Symmetric Check開始***
Target: 4, victim: 5, Loss: 2.9841, Acc: 100.00%, CE_Loss: 0.65, Reg_Loss:461.88, Cost:0.01 best_reg:465.64 avg_loss_reg:468.02:  75%|███████▌  | 168/223 [02:52<00:56,  1.02s/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: 651.2950201034546
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000012----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['17-15']
***Trigger Reverse Engineering開始***
Target: 17, victim: 15, Loss: 1.6195, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:657.83, Cost:0.00 best_reg:659.15 avg_loss_reg:659.15:  14%|█         | 145/1000 [07:31<44:24,  3.12s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 17 Victim Class: 15 Trigger Size: 657.8291625976562 Optimization Steps: 146
***Symmetric Check開始***
Target: 15, victim: 17, Loss: 4.8683, Acc: 95.00%, CE_Loss: 0.28, Reg_Loss:1358.57, Cost:0.00 best_reg:1383.04 avg_loss_reg:1343.11: 100%|██████████| 146/146 [07:32<00:00,  3.10s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 917.2007367610931
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000013----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-8', '2-1', '2-6']
***Trigger Reverse Engineering開始***
Target: 2, victim: 6, Loss: 9.8620, Acc: 0.00%, CE_Loss: 9.86, Reg_Loss:2546.91, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2532.89:   3%|▎         | 32/1000 [00:20<10:09,  1.59it/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: 22.319307804107666
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000014----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.742951154708862
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000015----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '4-5', '5-0', '5-4']
```

```
***Trigger Reverse Engineering開始***
Target: 1, victim: 2, Loss: 0.5308, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:201.77, Cost:0.00 best_reg:219.76 avg_loss_reg:200.34:  22%|██▏         | 216/1000 [12:38<45:53,  3.51s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 2 Trigger Size: 201.76866149902344 Optimization Steps: 151
***Symmetric Check開始***
Target: 2, victim: 1, Loss: 1.7600, Acc: 90.00%, CE_Loss: 0.17, Reg_Loss:209.71, Cost:0.01 best_reg:214.07 avg_loss_reg:211.19: 100%|██████████| 151/151 [09:15<00:00,  3.68s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1321.1608629226685
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000016----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 14
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 14, victim: 12, Loss: 0.8590, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:169.67, Cost:0.01 best_reg:168.77 avg_loss_reg:169.71:  10%|▉         | 98/1000 [42:57<6:35:23, 26.30s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: all Trigger Size: 168.77167358398438 Optimization Steps: 99
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 2587.3155765533447
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000017----------
***Pre-Screening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', '7-4', '9-7', '9-10', '10-9', '10-14', '11-12', '13-2']
***Trigger Reverse Engineering開始***
Target: 10, victim: 9, Loss: 4.2454, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:348.40, Cost:0.01 best_reg:348.97 avg_loss_reg:348.97:  23%|██▎         | 228/1000 [03:03<10:20,  1.24it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 9 Trigger Size: 348.40411376953125 Optimization Steps: 119
***Symmetric Check開始***
Target: 9, victim: 10, Loss: 3.4414, Acc: 90.00%, CE_Loss: 0.27, Reg_Loss:278.01, Cost:0.01 best_reg:282.17 avg_loss_reg:282.17: 100%|██████████| 119/119 [01:35<00:00,  1.25it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 283.29552268981934
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000018----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-7', '3-6', '3-5']
***Trigger Reverse Engineering開始***
Target: 3, victim: 5, Loss: 1.4272, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:10.75, Cost:0.13 best_reg:11.96 avg_loss_reg:11.96:  10%|▉         | 100/1000 [00:31<04:42,  3.19it/s]
  0%|          | 0/65 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 5 Trigger Size: 10.745586395263672 Optimization Steps: 65
***Symmetric Check開始***
Target: 5, victim: 3, Loss: 18.6709, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:1613.43, Cost:0.01 best_reg:1688.66 avg_loss_reg:1688.66: 100%|██████████| 65/65 [00:20<00:00,  3.21it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 56.46527862548828
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000019----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-5', '6-0', '6-12', '8-0', '12-15', '14-0', '15-12']
***Trigger Reverse Engineering開始***
Target: 4, victim: 5, Loss: 3.1536, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:264.26, Cost:0.01 best_reg:265.94 avg_loss_reg:265.94:  25%|██▍         | 253/1000 [22:19<1:05:54,  5.29s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 5 Trigger Size: 264.2559509277344 Optimization Steps: 128
***Symmetric Check開始***
Target: 5, victim: 4, Loss: 3.0272, Acc: 95.00%, CE_Loss: 0.26, Reg_Loss:546.21, Cost:0.01 best_reg:558.34 avg_loss_reg:550.76: 100%|██████████| 128/128 [11:30<00:00,  5.39s/it]
***Symmetric Check結束***
**********檢測結束**********
```

```
檢測結果: Model是安全的(Benign)
整體耗時: 2044.8717439174652
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000020----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-5', '2-4']
***Trigger Reverse Engineering開始***
Target: 2, victim: 4, Loss: 3.4585, Acc: 0.00%, CE_Loss: 3.46, Reg_Loss:2497.30, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2498.32:   2%|          | 21/1000 [00:12<09:43,  1.68it/s]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 14.646475076675415
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000021----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 21
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 21, victim: 20, Loss: 0.4411, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:87.14, Cost:0.01 best_reg:84.86 avg_loss_reg:87.02:   8%|▊         | 76/1000 [2:11:48<26:42:25, 104.05s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 21 Victim Class: all Trigger Size: 84.85630852835519 Optimization Steps: 77
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 7934.120084285736
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000022----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-18', '3-2', '10-13', '12-13', '12-18', '19-21', '20-18']
***Trigger Reverse Engineering開始***
Target: 12, victim: 18, Loss: 2.6564, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:44.44, Cost:0.06 best_reg:46.24 avg_loss_reg:46.24:  27%|██▋       | 268/1000 [19:27<53:07,  4.35s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 18 Trigger Size: 44.44329833984375 Optimization Steps: 87
***Symmetric Check開始***
Target: 18, victim: 12, Loss: 1.2199, Acc: 55.00%, CE_Loss: 1.22, Reg_Loss:8156.61, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:8085.12: 100%|██████████| 87/87 [06:20<00:00,  4.37s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1570.797575712204
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000023----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-6', '3-2', '3-5']
***Trigger Reverse Engineering開始***
Target: 3, victim: 6, Loss: 0.7519, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:26.55, Cost:0.03 best_reg:26.63 avg_loss_reg:27.02:  14%|█▍        | 140/1000 [13:22<1:22:10,  5.73s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 6 Trigger Size: 26.55321502685547 Optimization Steps: 92
***Symmetric Check開始***
Target: 6, victim: 3, Loss: 1.9374, Acc: 95.00%, CE_Loss: 0.30, Reg_Loss:729.84, Cost:0.00 best_reg:818.32 avg_loss_reg:740.86: 100%|██████████| 92/92 [08:42<00:00,  5.67s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1338.4169886112213
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000024----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-3', '3-4', '4-2', '4-3', '4-11', '5-6', '5-12', '6-5', '6-12', '7-8', '8-7', '9-8', '10-11', '11-9']
***Trigger Reverse Engineering開始***
Target: 3, victim: 4, Loss: 4.2179, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:31.57, Cost:0.13 best_reg:33.03 avg_loss_reg:33.03:  44%|████▍     | 439/1000 [07:37<09:45,  1.04s/it]
  0%|          | 0/84 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 4 Trigger Size: 31.574466705322266 Optimization Steps: 84
***Symmetric Check開始***
```

```
Target: 4, victim: 3, Loss: 5.1056, Acc: 90.00%, CE_Loss: 0.37, Reg_Loss:184.75, Cost:0.03 best_reg:205.92 avg_loss_reg:193.42: 100%|| 84/84 [01:27<00:00,  1.04s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 550.8776593208313
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000025----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-8', '7-6']
***Trigger Reverse Engineering開始***
Target: 5, victim: 8, Loss: 2.1796, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:606.92, Cost:0.00 best_reg:607.36 avg_loss_reg:606.73:  22%|| 220/1000 [05:51<20:45,  1.60s/it]
  0%|          | 0/200 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 8 Trigger Size: 606.9244384765625 Optimization Steps: 200
***Symmetric Check開始***
Target: 8, victim: 5, Loss: 1.2477, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:347.26, Cost:0.00 best_reg:349.28 avg_loss_reg:349.28:  88%| | 177/200 [04:43<00:36,  1.60s/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: 641.4115657806396
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000026----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-16', '1-0', '1-3', '3-15', '5-16', '8-6', '8-7', '8-10', '9-10', '9-11', '11-10', '13-15', '13-17', '15-17', '17-6', '17-15', '19-12']
***Trigger Reverse Engineering開始***
Target: 13, victim: 15, Loss: 1.0026, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:89.82, Cost:0.01 best_reg:90.90 avg_loss_reg:88.78:  59%| | 590/1000 [41:26<28:47,  4.21s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 15 Trigger Size: 89.81779479980469 Optimization Steps: 260
***Symmetric Check開始***
Target: 15, victim: 13, Loss: 1.8935, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:519.75, Cost:0.00 best_reg:520.46 avg_loss_reg:520.46:  58%| | 152/260 [11:02<07:50,  4.36s/it]
early stop 所有
***Symmetric Check結束***
********************檢測結束********************
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 3163.896786212921
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000027----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 7.04800009727478
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000028----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-3', '3-4', '4-5']
***Trigger Reverse Engineering開始***
Target: 4, victim: 5, Loss: 12.9612, Acc: 0.00%, CE_Loss: 12.96, Reg_Loss:2564.29, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2547.72:   4%| | 42/1000 [03:45<1:25:37,  5.36s/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: 234.15252161026
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000029----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '0-20', '1-0', '1-12', '1-14', '3-4', '3-6', '4-6', '5-4', '6-3', '6-4', '7-8', '7-9', '7-10', '8-2', '8-3', '8-15', '9-2', '9-16', '9-8', '10-7', '10-9', '10-11', '11-8', '11-12', '11-13', '12-11', '13-11', '13-20', '13-4', '14-15', '15-16', '15-19', '16-19', '18-19', '18-17', '18-16', '19-15', '19-17']
***Trigger Reverse Engineering開始***
Target: 11, victim: 12, Loss: 15.9272, Acc: 95.00%, CE_Loss: 0.20, Reg_Loss:409.13, Cost:0.04 best_reg:466.65 avg_loss_reg:466.65: 100%|| 1000/1000 [17:02<00:00,  1.02s/it]
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 12 Trigger Size: 466.6546936035156 Optimization Steps: 68
***Symmetric Check開始***
Target: 12, victim: 11, Loss: 8.0876, Acc: 95.00%, CE_Loss: 0.30, Reg_Loss:1537.52, Cost:0.01 best_reg:1754.22 avg_loss_reg:1573.05: 100%|| 68/68 [01:07<00:00,  1.00it/s]
***Symmetric Check結束***
********************檢測結束********************
```

```
檢測結果: Model是安全的(Benign)
整體耗時: 1097.9811899662018
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000030----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['7-1', '7-6']
***Trigger Reverse Engineering開始***
Target: 7, victim: 6, Loss: 1.0043, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:42.75, Cost:0.02 best_reg:44.51 avg_loss_reg:42.55:  12%|          | 122/1000 [03:36<25:54,  1.77s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 6 Trigger Size: 42.750850677490234 Optimization Steps: 112
***Symmetric Check開始***
Target: 6, victim: 7, Loss: 0.5270, Acc: 90.00%, CE_Loss: 0.41, Reg_Loss:1323.80, Cost:0.00 best_reg:4083.97 avg_loss_reg:1314.18: 100%|| 112/112 [03:24<00:00,  1.83s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 424.00752115249634
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000031----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-6', '5-7', '6-5']
***Trigger Reverse Engineering開始***
Target: 6, victim: 5, Loss: 1.2770, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:227.56, Cost:0.01 best_reg:228.84 avg_loss_reg:228.84:  18%|          | 184/1000 [16:16<1:12:11,  5.31s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 5 Trigger Size: 227.56475830078125 Optimization Steps: 131
***Symmetric Check開始***
Target: 5, victim: 6, Loss: 1.0506, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:424.79, Cost:0.00 best_reg:420.95 avg_loss_reg:425.13: 100%|| 131/131 [11:33<00:00,  5.30s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1680.543764591217
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000032----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-5', '1-6', '1-8', '2-3', '3-2', '4-5', '6-15', '7-1', '7-11', '7-12', '8-10', '9-8', '9-11', '10-15', '11-7', '12-13', '12-14', '13-12', '13-14', '14-5', '14-12', '14-13', '15-0', '15-10']
***Trigger Reverse Engineering開始***
Target: 2, victim: 3, Loss: 3.2788, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:266.66, Cost:0.01 best_reg:267.09 avg_loss_reg:267.09:  52%|          | 523/1000 [27:40<25:14,  3.18s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 3 Trigger Size: 266.6648254394531 Optimization Steps: 116
***Symmetric Check開始***
Target: 3, victim: 2, Loss: 3.9591, Acc: 100.00%, CE_Loss: 0.34, Reg_Loss:476.82, Cost:0.01 best_reg:479.48 avg_loss_reg:479.52: 100%|| 116/116 [05:53<00:00,  3.05s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 2026.1261434555054
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000033----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-6', '6-5']
***Trigger Reverse Engineering開始***
Target: 5, victim: 6, Loss: 6.4207, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:240.92, Cost:0.03 best_reg:242.48 avg_loss_reg:242.48:  15%|          | 150/1000 [07:31<42:37,  3.01s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 6 Trigger Size: 240.91769409179688 Optimization Steps: 106
***Symmetric Check開始***
Target: 6, victim: 5, Loss: 4.2776, Acc: 90.00%, CE_Loss: 0.37, Reg_Loss:515.20, Cost:0.01 best_reg:523.25 avg_loss_reg:517.95: 100%|| 106/106 [05:30<00:00,  3.11s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 790.4845879077911
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000034----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-5', '4-6', '7-1', '7-4']
```

```
***Trigger Reverse Engineering開始***
Target: 7, victim: 4, Loss: 2.4180, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:61.43, Cost:0.04 best_reg:63.77 avg_loss_reg:62.13:  12%|          | 117/1000 [10:45<1:21:13,  5.52s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 4 Trigger Size: 61.42675018310547 Optimization Steps: 73
***Symmetric Check開始***
Target: 4, victim: 7, Loss: 0.1955, Acc: 95.00%, CE_Loss: 0.20, Reg_Loss:9030.64, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:8933.84: 100%|| 73/73 [06:37<00:00,  5.45s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1052.554583787918
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000035----------
***Pre-Screening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', '3-13', '4-5', '4-6', '5-4', '5-6', '9-10', '12-4', '12-13', '13-14', '14-13', '15-2', '15-8', '17-11']
***Trigger Reverse Engineering開始***
Target: 12, victim: 4, Loss: 1.5888, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:128.21, Cost:0.01 best_reg:128.68 avg_loss_reg:128.68:  39%|      | 386/1000 [05:08<08:10,  1.25it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 4 Trigger Size: 128.20550537109375 Optimization Steps: 89
***Symmetric Check開始***
Target: 4, victim: 12, Loss: 9.2024, Acc: 90.00%, CE_Loss: 0.45, Reg_Loss:5833.84, Cost:0.00 best_reg:6623.27 avg_loss_reg:6209.74: 100%|| 89/89 [01:11<00:00,  1.25it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 386.3221673965454
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000036----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-1', '3-13', '4-3', '10-12', '11-12', '11-15', '16-15']
***Trigger Reverse Engineering開始***
Target: 3, victim: 1, Loss: 1.4200, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:52.12, Cost:0.03 best_reg:52.92 avg_loss_reg:52.92:  30%|      | 301/1000 [26:02<1:00:29,  5.19s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 1 Trigger Size: 52.11592102050781 Optimization Steps: 77
***Symmetric Check開始***
Target: 1, victim: 3, Loss: 2.4761, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:2354.79, Cost:0.00 best_reg:2431.72 avg_loss_reg:2431.72: 100%|| 77/77 [06:47<00:00,  5.29s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1985.7354328632355
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000037----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 2.1266300678253174
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000038----------
***Pre-Screening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']
***Trigger Reverse Engineering開始***
Target: 3, victim: 2, Loss: 14.0997, Acc: 0.00%, CE_Loss: 14.10, Reg_Loss:2525.27, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2516.15:   1%|         | 10/1000 [00:34<56:42,  3.44s/it]
***Trigger Reverse Engineering結束***
Target Class: 3 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: 39.14864802360535
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000039----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-0', '6-1']
***Trigger Reverse Engineering開始***
Target: 1, victim: 0, Loss: 4.1925, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:234.74, Cost:0.02 best_reg:236.12 avg_loss_reg:236.12:  12%|          | 125/1000 [15:53<1:51:12,  7.63s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 0 Trigger Size: 234.73757934570312 Optimization Steps: 115
```

```
***Symmetric Check開始***
Target: 0, victim: 1, Loss: 2.3691, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:961.51, Cost:0.00 best_reg:963.48 avg_loss_reg:963.48: 100%|██████████| 115/115 [14:31<00:00,  7.58s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1859.352138519287
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000040----------------------------------------
***Pre-Screening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', '3-2', '6-7']
***Trigger Reverse Engineering開始***
Target: 3, victim: 2, Loss: 4.5895, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:77.42, Cost:0.06 best_reg:80.62 avg_loss_reg:80.62:  15%|█▌        | 146/1000 [01:46<10:23,  1.37it/s]
  0%|          | 0/95 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 2 Trigger Size: 77.41842651367188 Optimization Steps: 95
***Symmetric Check開始***
Target: 2, victim: 3, Loss: 8.6492, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:145.14, Cost:0.06 best_reg:147.24 avg_loss_reg:147.24:  97%|█████████▋| 92/95 [01:07<00:02,  1.36it/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: 178.9745192527771
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000041----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-3', '4-20', '6-5', '6-7', '8-9', '10-11', '11-5', '11-10', '11-19', '12-11', '12-7', '12-13', '13-12', '13-15', '13-20', '14-10', '14-12', '15-12', '15-13', '17-19']
***Trigger Reverse Engineering開始***
Target: 12, victim: 7, Loss: 1.0420, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:35.25, Cost:0.03 best_reg:42.20 avg_loss_reg:35.34:  52%|█████▏    | 520/1000 [45:44<42:13,  5.28s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 7 Trigger Size: 35.25355911254883 Optimization Steps: 99
***Symmetric Check開始***
Target: 7, victim: 12, Loss: 1.4433, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:2587.32, Cost:0.00 best_reg:2607.61 avg_loss_reg:2607.91: 100%|██████████| 99/99 [08:57<00:00,  5.43s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 3303.740555047989
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000042----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-5', '3-6']
***Trigger Reverse Engineering開始***
Target: 3, victim: 5, Loss: 5.2590, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:127.81, Cost:0.04 best_reg:130.82 avg_loss_reg:130.82:  11%|█         | 112/1000 [04:44<37:37,  2.54s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 5 Trigger Size: 127.80994415283203 Optimization Steps: 102
***Symmetric Check開始***
Target: 5, victim: 3, Loss: 3.7109, Acc: 80.00%, CE_Loss: 0.36, Reg_Loss:441.58, Cost:0.01 best_reg:467.91 avg_loss_reg:446.05: 100%|██████████| 102/102 [04:09<00:00,  2.45s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 540.8245801925659
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000043----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['7-4', '7-6']
***Trigger Reverse Engineering開始***
Target: 7, victim: 6, Loss: 1.3164, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:72.96, Cost:0.02 best_reg:72.99 avg_loss_reg:72.99:  10%|█         | 102/1000 [08:50<1:17:54,  5.21s/it]
  0%|          | 0/88 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 6 Trigger Size: 72.95845031738281 Optimization Steps: 88
***Symmetric Check開始***
Target: 6, victim: 7, Loss: 2.9850, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:1183.58, Cost:0.00 best_reg:1403.26 avg_loss_reg:1184.30: 100%|██████████| 88/88 [07:43<00:00,  5.27s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1028.6959199905396
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000044----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '1-0', '2-0', '3-2', '3-7', '4-5', '4-12', '4-3', '5-2', '5-3', '5-4', '6-7', '6-8', '7-3', '7-6', '8-6', '10-11', '10-12', '10-13', '11-10', '11-13', '12-4', '12-11', '12-13']
***Trigger Reverse Engineering開始***
Target: 6, victim: 7, Loss: 3.4545, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:56.33, Cost:0.06 best_reg:59.85 avg_loss_reg:59.85:  57%|[redacted]  | 566/1000 [03:26<02:38,  2.74it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 7 Trigger Size: 56.3314208984375 Optimization Steps: 92
***Symmetric Check開始***
Target: 7, victim: 6, Loss: 6.8110, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:75.28, Cost:0.09 best_reg:75.98 avg_loss_reg:75.98:  99%|[redacted]| 91/92 [00:32<00:00,  2.81it/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: 244.1977732181549
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000045----------------------------------------
***Pre-Screening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', '3-2', '5-1', '5-2', '5-8']
***Trigger Reverse Engineering開始***
Target: 3, victim: 0, Loss: 6.0237, Acc: 100.00%, CE_Loss: 0.34, Reg_Loss:221.67, Cost:0.03 best_reg:221.70 avg_loss_reg:221.98:  21%|[redacted]  | 209/1000 [11:28<43:25,  3.29s/it]
  0%|          | 0/116 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 0 Trigger Size: 221.67190551757812 Optimization Steps: 116
***Symmetric Check開始***
Target: 0, victim: 3, Loss: 9.5172, Acc: 100.00%, CE_Loss: 0.39, Reg_Loss:237.38, Cost:0.04 best_reg:240.17 avg_loss_reg:237.49:  96%|[redacted] | 111/116 [06:05<00:16,  3.29s/it]
early stop 所有
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1066.5303678512573
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000046----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.626201629638672
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000047----------------------------------------
***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: 20, Loss: 0.2860, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:56.49, Cost:0.01 best_reg:55.59 avg_loss_reg:55.59:  12%|[redacted]  | 118/1000 [1:40:52<12:33:58, 51.29s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 17 Victim Class: all Trigger Size: 55.58759716578892 Optimization Steps: 119
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 6069.085235834122
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000048----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 36.06670904159546
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000049----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '1-0', '2-1', '5-4', '7-4', '7-9', '7-10', '9-10', '10-9']
***Trigger Reverse Engineering開始***
Target: 0, victim: 1, Loss: 2.0766, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:109.79, Cost:0.02 best_reg:116.40 avg_loss_reg:107.46:  34%|[redacted]  | 339/1000 [05:12<10:09,  1.08it/s]
  0%|          | 0/125 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 109.7872314453125 Optimization Steps: 125
***Symmetric Check開始***
```

```
Target: 1, victim: 0, Loss: 2.6397, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:212.13, Cost:0.01 best_reg:215.11 avg_loss_reg:212.80:  98%|▉| 123/125 [01:48<00:01,  1.14it/s]
early stop 所有
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 427.27389335632324
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000050----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '0-18', '1-0', '1-5', '3-4', '4-11', '5-2', '5-6', '5-7', '7-17', '8-10', '8-11', '9-10', '9-8', '9-17', '10-7', '10-11', '11-10', '12-14', '12-18', '14-18', '15-8', '19-2', '19-5']
***Trigger Reverse Engineering開始***
Target: 11, victim: 10, Loss: 2.3545, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:179.97, Cost:0.01 best_reg:180.04 avg_loss_reg:180.04:  59%|▌    | 586/1000 [40:29<28:36,  4.15s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 10 Trigger Size: 179.97471618652344 Optimization Steps: 122
***Symmetric Check開始***
Target: 10, victim: 11, Loss: 1.5358, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:82.82, Cost:0.02 best_reg:83.63 avg_loss_reg:83.63: 100%|▉| 122/122 [08:47<00:00,  4.33s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 2974.149044275284
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000051----------------------------------------
***Pre-Screening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', '5-0']
***Trigger Reverse Engineering開始***
Target: 5, victim: 0, Loss: 16.5900, Acc: 0.00%, CE_Loss: 16.59, Reg_Loss:2546.57, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2532.36:   2%|▏         | 21/1000 [00:10<08:11,  1.99it/s]
***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: 20.717834949493408
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000052----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-5', '2-6', '7-6', '9-12', '12-9']
***Trigger Reverse Engineering開始***
Target: 12, victim: 9, Loss: 4.0734, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:224.93, Cost:0.02 best_reg:225.76 avg_loss_reg:225.76:  22%|▏        | 221/1000 [06:27<22:45,  1.75s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 9 Trigger Size: 224.92709350585938 Optimization Steps: 119
***Symmetric Check開始***
Target: 9, victim: 12, Loss: 2.6803, Acc: 90.00%, CE_Loss: 0.21, Reg_Loss:144.66, Cost:0.02 best_reg:151.57 avg_loss_reg:144.11: 100%|▉| 119/119 [03:27<00:00,  1.74s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 606.2266697883606
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000053----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-5', '6-3', '6-2']
***Trigger Reverse Engineering開始***
Target: 6, victim: 5, Loss: 1.0140, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:269.29, Cost:0.00 best_reg:270.34 avg_loss_reg:268.18:  21%|▏        | 206/1000 [02:35<09:58,  1.33it/s]
  0%|          | 0/175 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 5 Trigger Size: 269.29278564453125 Optimization Steps: 175
***Symmetric Check開始***
Target: 5, victim: 6, Loss: 2.3440, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:421.05, Cost:0.01 best_reg:421.41 avg_loss_reg:424.57:  97%|▉| 169/175 [02:08<00:04,  1.32it/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: 289.1358985900879
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000054----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
```

```
可能的 target-victim 配對: ['2-1', '5-0']
***Trigger Reverse Engineering開始***
Target: 2, victim: 1, Loss: 2.3741, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:134.80, Cost:0.02 best_reg:135.33 avg_loss_reg:135.33:  12%|          | 124/1000 [06:15<44:14,  3.03s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 134.7955322265625 Optimization Steps: 114
***Symmetric Check開始***
Target: 1, victim: 2, Loss: 2.9652, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:250.67, Cost:0.01 best_reg:258.61 avg_loss_reg:258.61: 100%|| 114/114 [05:43<00:00,  3.02s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 728.6107451915741
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000055----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '1-0', '2-3', '3-4']
***Trigger Reverse Engineering開始***
Target: 1, victim: 0, Loss: 1.3594, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:499.55, Cost:0.00 best_reg:501.87 avg_loss_reg:501.87:  19%|          | 187/1000 [13:13<57:27,  4.24s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 0 Trigger Size: 499.554443359375 Optimization Steps: 154
***Symmetric Check開始***
Target: 0, victim: 1, Loss: 1.0064, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:175.25, Cost:0.01 best_reg:176.15 avg_loss_reg:175.60:  91%|| 140/154 [09:58<00:59,  4.27s/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: 1399.4221584796906
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000056----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 7
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 7, victim: 12, Loss: 0.8452, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:367.35, Cost:0.00 best_reg:366.09 avg_loss_reg:367.18:   7%|          | 72/1000 [1:05:58<14:10:15, 54.97s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: all Trigger Size: 366.08656819661456 Optimization Steps: 73
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 3974.322370290756
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000057----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 26.39915418624878
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000058----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-20', '7-8', '18-15']
***Trigger Reverse Engineering開始***
Target: 18, victim: 15, Loss: 5.4842, Acc: 100.00%, CE_Loss: 0.46, Reg_Loss:294.10, Cost:0.02 best_reg:295.92 avg_loss_reg:295.92:  21%|          | 210/1000 [14:51<55:55,  4.25s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 18 Victim Class: 15 Trigger Size: 294.101806640625 Optimization Steps: 123
***Symmetric Check開始***
Target: 15, victim: 18, Loss: 2.0128, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:359.05, Cost:0.01 best_reg:359.15 avg_loss_reg:359.22: 100%|| 123/123 [08:40<00:00,  4.23s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1437.5482561588287
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000059----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-2', '2-0', '4-5', '9-11', '10-9']
***Trigger Reverse Engineering開始***
```

```
Target: 4, victim: 5, Loss: 0.7637, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:56.69, Cost:0.01 best_reg:60.94 avg_loss_reg:57.04:  26%|███       | 264/1000 [02:34<07:11,  1.71it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 5 Trigger Size: 56.691673278808594 Optimization Steps: 127
***Symmetric Check開始***
Target: 5, victim: 4, Loss: 1.8086, Acc: 95.00%, CE_Loss: 0.23, Reg_Loss:207.70, Cost:0.01 best_reg:218.47 avg_loss_reg:208.79: 100%|████████████| 127/127 [01:14<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: 235.19654655456543
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000060----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-5']
***Trigger Reverse Engineering開始***
Target: 0, victim: 5, Loss: 10.6913, Acc: 0.00%, CE_Loss: 10.69, Reg_Loss:2535.99, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2525.07:   1%|         | 10/1000 [00:36<59:37,  3.61s/it]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 44.413042306900024
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000061----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 16.79815983772278
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000062----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-1']
***Trigger Reverse Engineering開始***
Target: 3, victim: 1, Loss: 1.3765, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:555.07, Cost:0.00 best_reg:558.38 avg_loss_reg:561.20:  18%|██        | 175/1000 [17:58<1:24:44,  6.16s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 1 Trigger Size: 555.07470703125 Optimization Steps: 176
***Symmetric Check開始***
Target: 1, victim: 3, Loss: 1.2039, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:1028.47, Cost:0.00 best_reg:1017.77 avg_loss_reg:1017.77: 100%|████████████| 176/176 [17:58<00:00,  6.13s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 2169.288154602051
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000063----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.406555652618408
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000064----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 5
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 5, victim: 12, Loss: 0.5216, Acc: 86.36%, CE_Loss: 0.18, Reg_Loss:20.22, Cost:0.02 best_reg:21.56 avg_loss_reg:20.47:   5%|▌         | 53/1000 [19:00<5:39:33, 21.51s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: all Trigger Size: 21.56311798095703 Optimization Steps: 54
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1149.59379529953
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000065----------------------------------------
***Pre-Screening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', '2-0', '2-1', '3-5', '5-3', '5-8', '6-7', '9-14', '9-15', '11-10', '13-0', '13-7', '13-15', '14-12', '15-9']
***Trigger Reverse Engineering開始***
Target: 6, victim: 7, Loss: 1.6144, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:191.55, Cost:0.01 best_reg:191.71 avg_loss_reg:191.71:  50%|█████     | 504/1000 [53:59<53:07,  6.43s/it]
```

```
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 7 Trigger Size: 191.5477752685547 Optimization Steps: 146
***Symmetric Check開始***
Target: 7, victim: 6, Loss: 3.5974, Acc: 90.00%, CE_Loss: 0.41, Reg_Loss:629.94, Cost:0.01 best_reg:641.49 avg_loss_reg:631.31: 100%|[redacted]| 146/146 [15:38<00:00,  6.43s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 4199.947261571884
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000066----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-8', '1-2', '9-11', '11-9', '12-9', '12-11', '12-2']
***Trigger Reverse Engineering開始***
Target: 12, victim: 9, Loss: 1.7277, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:91.33, Cost:0.02 best_reg:92.16 avg_loss_reg:92.16:  28%|[redacted]| 276/1000 [14:06<37:01,  3.07s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 9 Trigger Size: 91.32717895507812 Optimization Steps: 118
***Symmetric Check開始***
Target: 9, victim: 12, Loss: 2.0706, Acc: 70.00%, CE_Loss: 0.46, Reg_Loss:477.28, Cost:0.00 best_reg:538.66 avg_loss_reg:482.10: 100%|[redacted]| 118/118 [05:44<00:00,  2.92s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 1204.5142858028412
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000067----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['8-15', '9-8', '15-8']
***Trigger Reverse Engineering開始***
Target: 9, victim: 8, Loss: 2.5096, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:475.89, Cost:0.01 best_reg:476.18 avg_loss_reg:476.24:  16%|[redacted]| 161/1000 [06:52<35:48,  2.56s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 8 Trigger Size: 475.8892822265625 Optimization Steps: 139
***Symmetric Check開始***
Target: 8, victim: 9, Loss: 7.5727, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:422.87, Cost:0.02 best_reg:431.67 avg_loss_reg:425.38:  86%|[redacted]| 119/139 [05:06<00:51,  2.57s/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: 733.9020366668701
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000068----------------------------------------
***Pre-Screening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', '9-4']
***Trigger Reverse Engineering開始***
Target: 9, victim: 4, Loss: 3.5863, Acc: 20.00%, CE_Loss: 3.59, Reg_Loss:2665.24, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2599.76:   3%|[redacted]| 31/1000 [01:20<41:42,  2.58s/it]
***Trigger Reverse Engineering結束***
Target Class: 6 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: 89.92737865447998
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000069----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-7', '1-2', '1-9', '2-1', '2-16', '3-4', '4-3', '5-3', '5-4', '5-17', '6-5', '7-0', '8-10', '8-9', '8-15', '9-1', '9-8', '10-8', '10-16', '11-0', '11-1', '11-18', '12-11', '13-11', '13-17', '14-13', '14-15', '14-17', '15-8', '15-14', '16-10', '16-18', '17-4', '17-13', '17-15', '18-16', '18-14', '18-10']
***Trigger Reverse Engineering開始***
Target: 9, victim: 8, Loss: 4.8282, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:3174.23, Cost:0.00 best_reg:3391.67 avg_loss_reg:3391.67: 100%|[redacted]| 1000/1000 [1:26:30<00:00,  5.19s/it]
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 15 Trigger Size: 2181.711181640625 Optimization Steps: 35
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 5209.6555235385895
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000070----------------------------------------
***Pre-Screening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', '4-6', '5-6', '6-0', '6-5', '7-10', '8-9', '10-7', '11-0', '11-10']
***Trigger Reverse Engineering開始***
Target: 6, victim: 0, Loss: 3.3467, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:191.60, Cost:0.02 best_reg:192.42 avg_loss_reg:189.87:  39%|████      | 391/1000 [40:58<1:03:48,  6.29s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 0 Trigger Size: 191.60260009765625 Optimization Steps: 89
***Symmetric Check開始***
Target: 0, victim: 6, Loss: 1.8565, Acc: 95.00%, CE_Loss: 0.20, Reg_Loss:490.25, Cost:0.00 best_reg:590.02 avg_loss_reg:502.44: 100%|██████████| 89/89 [09:34<00:00,  6.46s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 3050.8941009044647
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000071----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-2', '1-2', '3-4', '5-0', '8-9', '9-18', '10-4', '16-2', '17-18']
***Trigger Reverse Engineering開始***
Target: 3, victim: 4, Loss: 1.8273, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:150.97, Cost:0.01 best_reg:151.15 avg_loss_reg:151.15:  26%|███       | 264/1000 [30:36<1:25:19,  6.96s/it]
  0%|          | 0/125 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 4 Trigger Size: 150.9722900390625 Optimization Steps: 125
***Symmetric Check開始***
Target: 4, victim: 3, Loss: 4.5776, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:384.24, Cost:0.01 best_reg:390.33 avg_loss_reg:390.33:  96%|██████████ | 120/125 [14:03<00:35,  7.03s/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: 2702.7054691314697
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000072----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.984390735626221
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000073----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-0', '2-1', '2-16', '3-10', '5-6', '6-5', '6-8', '14-9', '14-15', '15-9', '15-14', '15-16']
***Trigger Reverse Engineering開始***
Target: 2, victim: 0, Loss: 1.2036, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:214.32, Cost:0.01 best_reg:214.49 avg_loss_reg:214.69:  37%|████      | 369/1000 [05:09<08:50,  1.19it/s]
  0%|          | 0/141 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 0 Trigger Size: 214.32220458984375 Optimization Steps: 141
***Symmetric Check開始***
Target: 0, victim: 2, Loss: 2.5570, Acc: 95.00%, CE_Loss: 0.41, Reg_Loss:635.36, Cost:0.00 best_reg:647.61 avg_loss_reg:628.84: 100%|██████████| 141/141 [01:58<00:00,  1.19it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 435.88667249679565
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000074----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-6', '7-5', '8-4']
***Trigger Reverse Engineering開始***
Target: 5, victim: 6, Loss: 3.9303, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:63.92, Cost:0.06 best_reg:66.76 avg_loss_reg:66.76:  15%|██        | 148/1000 [01:33<08:55,  1.59it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 6 Trigger Size: 63.91997528076172 Optimization Steps: 104
***Symmetric Check開始***
Target: 6, victim: 5, Loss: 5.0198, Acc: 95.00%, CE_Loss: 0.21, Reg_Loss:187.55, Cost:0.03 best_reg:201.28 avg_loss_reg:190.53: 100%|██████████| 104/104 [01:04<00:00,  1.61it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 166.82569551467896
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000075----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
```

```
可能的 target-victim 配對: ['0-2', '1-2', '2-0', '3-21', '3-12', '3-7', '4-8', '6-5', '6-14', '9-7', '10-14', '10-20', '11-19', '11-2', '11-10', '14-10', '16-19', '17-19', '18-19', '20-10', '20-11', '21-4', '21-12']
***Trigger Reverse Engineering開始***
Target: 9, victim: 7, Loss: 1.1154, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:91.69, Cost:0.01 best_reg:95.35 avg_loss_reg:92.34:  62%|[redacted]| 618/1000 [16:19<10:05,  1.58s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 9 Victim Class: 7 Trigger Size: 91.69285583496094 Optimization Steps: 123
***Symmetric Check開始***
Target: 7, victim: 9, Loss: 2.3178, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:426.68, Cost:0.01 best_reg:435.33 avg_loss_reg:418.48: 100%|[redacted]| 123/123 [03:14<00:00,  1.58s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1185.3788526058197
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000076----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '1-0']
***Trigger Reverse Engineering開始***
Target: 1, victim: 0, Loss: 2.2630, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:36.09, Cost:0.06 best_reg:36.62 avg_loss_reg:36.62:  12%|[redacted]| 121/1000 [01:11<08:42,  1.68it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 0 Trigger Size: 36.0929069519043 Optimization Steps: 95
***Symmetric Check開始***
Target: 0, victim: 1, Loss: 2.6154, Acc: 90.00%, CE_Loss: 0.36, Reg_Loss:58.76, Cost:0.04 best_reg:59.97 avg_loss_reg:59.97: 100%|[redacted]| 95/95 [00:55<00:00,  1.71it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 129.46330070495605
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000077----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-2', '1-3', '1-4', '3-1', '7-5', '7-6']
***Trigger Reverse Engineering開始***
Target: 1, victim: 3, Loss: 1.1013, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:91.75, Cost:0.01 best_reg:92.28 avg_loss_reg:92.28:  28%|[redacted]| 284/1000 [03:26<08:39,  1.38it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 3 Trigger Size: 91.74713134765625 Optimization Steps: 113
***Symmetric Check開始***
Target: 3, victim: 1, Loss: 5.1711, Acc: 90.00%, CE_Loss: 0.34, Reg_Loss:282.77, Cost:0.02 best_reg:295.43 avg_loss_reg:284.99: 100%|[redacted]| 113/113 [01:22<00:00,  1.37it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 293.5281820297241
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000078----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-8']
***Trigger Reverse Engineering開始***
Target: 0, victim: 8, Loss: 2.0859, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:363.79, Cost:0.01 best_reg:364.24 avg_loss_reg:364.24:  16%|[redacted]| 156/1000 [16:28<1:29:07,  6.34s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 8 Trigger Size: 363.786865234375 Optimization Steps: 157
***Symmetric Check開始***
Target: 8, victim: 0, Loss: 2.4076, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:279.92, Cost:0.01 best_reg:280.71 avg_loss_reg:283.36:  94%|[redacted]| 147/157 [15:31<01:03,  6.34s/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: 1934.0635685920715
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000079----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-15', '2-0', '3-4', '5-6', '10-9', '10-20', '12-11', '13-5', '14-11', '15-20', '19-17']
***Trigger Reverse Engineering開始***
Target: 10, victim: 20, Loss: 1.5523, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:82.27, Cost:0.02 best_reg:82.37 avg_loss_reg:82.37:  33%|[redacted]| 331/1000 [11:43<23:41,  2.13s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 20 Trigger Size: 82.26667785644531 Optimization Steps: 106
```

```
***Symmetric Check開始***
Target: 20, victim: 10, Loss: 8.0781, Acc: 60.00%, CE_Loss: 0.98, Reg_Loss:2102.25, Cost:0.00 best_reg:2184.44 avg_loss_reg:2145.25: 100%|| 106/106 [03:49<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: 953.129403591156
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000080----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '1-6', '3-0', '3-4', '3-6', '5-9', '6-10', '7-0', '8-13', '9-10', '9-17', '9-14', '10-12', '10-16', '11-0', '11-2', '12-8', '12-10', '12-13', '14-16', '16-17', '16-18', '17-9', '18-15', '18-16', '18-17']
***Trigger Reverse Engineering開始***
Target: 3, victim: 4, Loss: 2.1437, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:264.71, Cost:0.01 best_reg:267.29 avg_loss_reg:267.29:  65%|     | 653/1000 [13:25<07:08,  1.23s/it]
  0%|          | 0/135 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 4 Trigger Size: 264.70855712890625 Optimization Steps: 135
***Symmetric Check開始***
Target: 4, victim: 3, Loss: 3.2015, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:389.21, Cost:0.01 best_reg:387.23 avg_loss_reg:389.44: 100%| 135/135 [02:45<00:00,  1.23s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 979.3001549243927
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000081----------------------------------------
***Pre-Screening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', '8-7', '9-7', '17-16']
***Trigger Reverse Engineering開始***
Target: 8, victim: 7, Loss: 3.0843, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:169.81, Cost:0.02 best_reg:173.74 avg_loss_reg:165.80:  15%|     | 153/1000 [04:50<26:50,  1.90s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 7 Trigger Size: 169.80502319335938 Optimization Steps: 120
***Symmetric Check開始***
Target: 7, victim: 8, Loss: 4.1089, Acc: 100.00%, CE_Loss: 0.49, Reg_Loss:1606.58, Cost:0.00 best_reg:1627.00 avg_loss_reg:1615.16: 100%| 120/120 [03:47<00:00,  1.89s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000082----------------------------------------
***Pre-Screening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', '2-4', '3-1', '4-0', '5-0', '6-7', '6-9', '6-13', '7-5', '8-9', '9-0', '10-11', '11-10', '11-12', '12-10', '12-11']
***Trigger Reverse Engineering開始***
Target: 6, victim: 7, Loss: 3.2495, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:183.69, Cost:0.02 best_reg:184.09 avg_loss_reg:184.36:  43%|     | 430/1000 [07:52<10:26,  1.10s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 7 Trigger Size: 183.6914825439453 Optimization Steps: 109
***Symmetric Check開始***
Target: 7, victim: 6, Loss: 7.1935, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:182.44, Cost:0.04 best_reg:183.62 avg_loss_reg:183.62:  92%|  | 100/109 [01:50<00:09,  1.11s/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: 589.9919376373291
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000083----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-2', '1-3', '1-12', '2-1', '2-3', '2-21', '3-9', '4-0', '4-5', '5-4', '6-0', '7-6', '7-20', '8-10', '8-11', '8-9', '9-12', '9-10', '9-8', '10-8', '10-12', '10-9', '11-8', '11-9', '11-12', '12-9', '12-11', '13-12', '13-21', '14-0', '14-16', '15-16', '16-15', '17-20', '18-8', '19-11', '19-18', '19-20', '20-17', '20-18', '20-19', '21-10']
***Trigger Reverse Engineering開始***
Target: 11, victim: 8, Loss: 1.9703, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:69.52, Cost:0.03 best_reg:69.80 avg_loss_reg:69.80:  79%|  | 786/1000 [06:50<01:51,  1.92it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 8 Trigger Size: 69.52107238769531 Optimization Steps: 101
***Symmetric Check開始***
Target: 8, victim: 11, Loss: 3.7878, Acc: 100.00%, CE_Loss: 0.44, Reg_Loss:440.74, Cost:0.01 best_reg:445.85 avg_loss_reg:445.85: 100%| 101/101 [00:52<00:00,  1.91it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
```

```
整體耗時: 469.1979444026947
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000084----------------------------------------
***Pre-Screening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', '3-1', '6-7', '7-6', '9-6', '9-12', '9-11', '10-9', '11-7', '11-10', '11-12', '12-6', '12-16', '12-5', '13-14', '14-13', '15-1', '15-3', '16-2', '16-17', '17-11', '17-12', '17-16']
***Trigger Reverse Engineering開始***
Target: 17, victim: 16, Loss: 4.8180, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:404.61, Cost:0.01 best_reg:411.78 avg_loss_reg:411.78:  62%|[redacted]    | 624/1000 [08:17<04:59,  1.26it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 17 Victim Class: 16 Trigger Size: 404.6092529296875 Optimization Steps: 117
***Symmetric Check開始***
Target: 16, victim: 17, Loss: 2.9520, Acc: 90.00%, CE_Loss: 0.23, Reg_Loss:807.11, Cost:0.00 best_reg:834.82 avg_loss_reg:816.42: 100%|[redacted]| 117/117 [01:31<00:00,  1.27it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 594.970291852951
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000085----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['9-15', '11-12', '11-13', '13-11', '13-12', '14-5', '14-8', '14-15', '15-14']
***Trigger Reverse Engineering開始***
Target: 14, victim: 8, Loss: 4.2250, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:109.41, Cost:0.04 best_reg:115.74 avg_loss_reg:115.74:  30%|[redacted]       | 295/1000 [03:38<08:41,  1.35it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 8 Trigger Size: 109.40910339355469 Optimization Steps: 81
***Symmetric Check開始***
Target: 8, victim: 14, Loss: 5.3487, Acc: 95.00%, CE_Loss: 0.34, Reg_Loss:989.26, Cost:0.01 best_reg:1230.08 avg_loss_reg:1020.11: 100%|[redacted]| 81/81 [00:58<00:00,  1.37it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 282.9408583641052
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000086----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.433794736862183
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000087----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 23.823465585708618
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000088----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-13', '1-2', '1-10', '2-1', '3-4', '3-12', '4-3', '5-11', '5-4', '5-3', '6-8', '6-9', '6-10', '7-8', '7-5', '7-16', '8-6', '8-7', '8-9', '10-6', '10-16', '11-12', '11-5', '11-1', '12-0', '12-11', '13-0', '13-14', '13-15', '14-15', '15-14']
***Trigger Reverse Engineering開始***
Target: 14, victim: 15, Loss: 4.2759, Acc: 100.00%, CE_Loss: 0.45, Reg_Loss:149.43, Cost:0.03 best_reg:150.15 avg_loss_reg:150.15:  65%|[redacted]    | 648/1000 [25:51<14:02,  2.39s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 15 Trigger Size: 149.42855834960938 Optimization Steps: 106
***Symmetric Check開始***
Target: 15, victim: 14, Loss: 1.3779, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:545.95, Cost:0.00 best_reg:586.90 avg_loss_reg:533.63: 100%|[redacted]| 106/106 [04:19<00:00,  2.45s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1823.5465157032013
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000089----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-1', '3-4', '4-3']
***Trigger Reverse Engineering開始***
Target: 4, victim: 3, Loss: 1.4290, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:80.05, Cost:0.02 best_reg:80.35 avg_loss_reg:80.35:  17%|[redacted]        | 173/1000 [02:47<13:19,  1.03it/s]
  0%|          | 0/118 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 3 Trigger Size: 80.0498046875 Optimization Steps: 118
```

```
***Symmetric Check開始***
Target: 3, victim: 4, Loss: 1.3166, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:359.17, Cost:0.00 best_reg:360.57 avg_loss_reg:360.57: 100%|██████████| 118/118 [01:53<00:00,  1.04it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 286.28641152381897
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000090----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-8', '0-14', '2-1', '2-15', '2-16', '3-8', '3-14', '4-6', '5-6', '6-5', '6-21', '8-14', '9-10', '10-9', '10-11', '10-15', '11-13', '11-20', '12-9', '12-10', '12-14', '13-11', '13-23', '15-16', '15-17', '17-15', '17-16', '18-5', '18-21', '18-22', '19-22', '21-6', '21-22', '23-6', '23-9']
***Trigger Reverse Engineering開始***
Target: 12, victim: 10, Loss: 5.3765, Acc: 90.00%, CE_Loss: 0.34, Reg_Loss:294.86, Cost:0.02 best_reg:380.15 avg_loss_reg:319.31: 100%|██████████| 1000/1000 [09:07<00:00,  1.83it/s]
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 10 Trigger Size: 380.1536560058594 Optimization Steps: 60
***Symmetric Check開始***
Target: 10, victim: 12, Loss: 5.4382, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:1589.22, Cost:0.00 best_reg:1678.02 avg_loss_reg:1678.02: 100%|██████████| 60/60 [00:33<00:00,  1.77it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 589.2769432067871
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000091----------------------------------------
***Pre-Screening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', '3-4', '4-3', '7-6', '7-12', '8-6', '10-9', '11-12', '12-7', '12-8', '12-11']
***Trigger Reverse Engineering開始***
Target: 4, victim: 3, Loss: 3.5115, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:87.89, Cost:0.04 best_reg:87.95 avg_loss_reg:87.95:  31%|███       | 313/1000 [02:59<06:34,  1.74it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 3 Trigger Size: 87.88641357421875 Optimization Steps: 81
***Symmetric Check開始***
Target: 3, victim: 4, Loss: 3.9256, Acc: 90.00%, CE_Loss: 0.42, Reg_Loss:461.16, Cost:0.01 best_reg:471.63 avg_loss_reg:471.63: 100%|██████████| 81/81 [00:45<00:00,  1.79it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 231.07721042633057
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000092----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-2', '1-4', '2-3', '2-5', '4-5', '4-15', '5-4', '6-7', '6-8', '7-8', '8-6', '8-7', '8-14', '9-11', '10-0', '10-6', '10-9', '11-9', '11-10', '12-10', '12-13', '12-15', '13-5', '13-14', '15-16', '16-15']
***Trigger Reverse Engineering開始***
Target: 12, victim: 15, Loss: 1.9431, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:69.10, Cost:0.03 best_reg:69.87 avg_loss_reg:69.87:  71%|███████   | 708/1000 [08:26<03:28,  1.40it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 15 Trigger Size: 69.1041259765625 Optimization Steps: 104
***Symmetric Check開始***
Target: 15, victim: 12, Loss: 6.2717, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:794.78, Cost:0.01 best_reg:822.21 avg_loss_reg:822.21: 100%|██████████| 104/104 [01:12<00:00,  1.44it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 584.6442468166351
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000093----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-6', '3-7']
***Trigger Reverse Engineering開始***
Target: 3, victim: 7, Loss: 3.6395, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:27.70, Cost:0.13 best_reg:30.00 avg_loss_reg:30.00:  10%|█         | 103/1000 [03:21<29:18,  1.96s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 7 Trigger Size: 27.704566955566406 Optimization Steps: 80
***Symmetric Check開始***
Target: 7, victim: 3, Loss: 5.1191, Acc: 100.00%, CE_Loss: 0.40, Reg_Loss:621.52, Cost:0.01 best_reg:633.30 avg_loss_reg:633.30: 100%|██████████| 80/80 [02:34<00:00,  1.94s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 362.07052397727966
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000094----------------------------------------
***Pre-Screening開始***
```

```
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '0-2', '2-11', '5-9', '11-2', '11-4', '11-10']
***Trigger Reverse Engineering開始***
Target: 0, victim: 2, Loss: 1.5848, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:953.10, Cost:0.00 best_reg:965.52 avg_loss_reg:969.45:  28%|███       | 276/1000 [07:13<18:56,  1.57s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 2 Trigger Size: 953.09765625 Optimization Steps: 162
***Symmetric Check開始***
Target: 2, victim: 0, Loss: 2.1655, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:400.73, Cost:0.01 best_reg:402.84 avg_loss_reg:402.84:  90%|██████████ | 146/162 [03:49<00:25,  1.57s/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: 670.9291820526123
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000095----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '0-13', '4-5', '7-14', '8-9', '8-14', '10-9', '10-12', '12-13', '13-3', '13-5', '13-12', '14-5']
***Trigger Reverse Engineering開始***
Target: 4, victim: 5, Loss: 2.1643, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:263.96, Cost:0.01 best_reg:265.68 avg_loss_reg:264.85:  34%|████      | 342/1000 [06:57<13:23,  1.22s/it]
  0%|          | 0/129 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 5 Trigger Size: 263.95562744140625 Optimization Steps: 129
***Symmetric Check開始***
Target: 5, victim: 4, Loss: 3.7029, Acc: 100.00%, CE_Loss: 0.34, Reg_Loss:295.58, Cost:0.01 best_reg:295.40 avg_loss_reg:297.05: 100%|██████████| 129/129 [02:36<00:00,  1.21s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 581.4466481208801
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000096----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-4']
***Trigger Reverse Engineering開始***
Target: 5, victim: 4, Loss: 1.5058, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:406.49, Cost:0.00 best_reg:409.87 avg_loss_reg:402.75:  17%|██        | 168/1000 [04:28<22:08,  1.60s/it]
  0%|          | 0/169 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 4 Trigger Size: 406.49334716796875 Optimization Steps: 169
***Symmetric Check開始***
Target: 4, victim: 5, Loss: 5.2443, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:195.35, Cost:0.03 best_reg:198.74 avg_loss_reg:193.10:  69%|███████▊  | 117/169 [03:06<01:22,  1.60s/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: 461.97503328323364
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000097----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['14-15', '14-21', '15-14', '19-18']
***Trigger Reverse Engineering開始***
Target: 19, victim: 18, Loss: 4.2652, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:522.81, Cost:0.01 best_reg:526.78 avg_loss_reg:513.96:  24%|██        | 235/1000 [06:52<22:22,  1.75s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 19 Victim Class: 18 Trigger Size: 522.811767578125 Optimization Steps: 132
***Symmetric Check開始***
Target: 18, victim: 19, Loss: 3.5714, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:652.05, Cost:0.01 best_reg:652.60 avg_loss_reg:653.71: 100%|██████████| 132/132 [03:47<00:00,  1.72s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 650.4799921512604
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000098----------------------------------------
***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: 14, Loss: 1.7963, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:105.01, Cost:0.02 best_reg:104.48 avg_loss_reg:106.90:  12%|▉          | 118/1000 [1:55:40<14:24:37, 58.82s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: all Trigger Size: 104.47900009155273 Optimization Steps: 119
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 6960.125637292862
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000099----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-2', '0-12', '1-2', '7-9', '13-12']
***Trigger Reverse Engineering開始***
Target: 7, victim: 9, Loss: 1.9461, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:234.06, Cost:0.01 best_reg:234.54 avg_loss_reg:236.64:  18%|▉          | 183/1000 [04:58<22:14,  1.63s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 9 Trigger Size: 234.05921936035156 Optimization Steps: 139
***Symmetric Check開始***
Target: 9, victim: 7, Loss: 2.2361, Acc: 95.00%, CE_Loss: 0.20, Reg_Loss:602.12, Cost:0.00 best_reg:612.81 avg_loss_reg:603.72: 100%|██████████| 139/139 [03:45<00:00,  1.62s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 534.2451767921448
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000100----------
***Pre-Screening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']
***Trigger Reverse Engineering開始***
Target: 4, victim: 1, Loss: 2.2783, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:86.41, Cost:0.03 best_reg:86.99 avg_loss_reg:86.99:  11%|▉          | 111/1000 [06:30<52:04,  3.51s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 1 Trigger Size: 86.41303253173828 Optimization Steps: 112
***Symmetric Check開始***
Target: 1, victim: 4, Loss: 2.6272, Acc: 95.00%, CE_Loss: 0.43, Reg_Loss:2201.43, Cost:0.00 best_reg:2331.92 avg_loss_reg:2230.76: 100%|██████████| 112/112 [06:29<00:00,  3.48s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 788.6487164497375
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000101----------
***Pre-Screening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', '3-4', '6-5', '9-7', '10-17', '15-17', '16-0', '16-4', '16-17', '17-15', '17-16']
***Trigger Reverse Engineering開始***
Target: 16, victim: 4, Loss: 3.8713, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:66.21, Cost:0.06 best_reg:66.45 avg_loss_reg:66.45:  36%|███▋       | 355/1000 [09:27<17:11,  1.60s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 16 Victim Class: 4 Trigger Size: 66.21123504638672 Optimization Steps: 76
***Symmetric Check開始***
Target: 4, victim: 16, Loss: 5.3340, Acc: 85.00%, CE_Loss: 0.60, Reg_Loss:3158.64, Cost:0.00 best_reg:4286.39 avg_loss_reg:3219.71: 100%|██████████| 76/76 [02:00<00:00,  1.59s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 699.1269299983978
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000102----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.2286293506622314
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000103----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-6']
***Trigger Reverse Engineering開始***
Target: 5, victim: 6, Loss: 1.3246, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:361.22, Cost:0.00 best_reg:361.93 avg_loss_reg:361.79:  14%|▉          | 144/1000 [07:27<44:19,  3.11s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 6 Trigger Size: 361.216064453125 Optimization Steps: 145
```

```
***Symmetric Check開始***
Target: 6, victim: 5, Loss: 1.0979, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:272.24, Cost:0.00 best_reg:272.56 avg_loss_reg:272.56:  92%|[redacted]| 133/145 [06:54<00:37,  3.12s/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: 871.0345122814178
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000104----------
***Pre-Screening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', '4-5', '6-7', '6-8', '8-6', '8-7', '10-9', '10-11', '11-10']
***Trigger Reverse Engineering開始***
Target: 11, victim: 10, Loss: 1.9514, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:63.94, Cost:0.03 best_reg:68.60 avg_loss_reg:63.51:  37%|[redacted]| 369/1000 [04:33<07:47,  1.35it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 10 Trigger Size: 63.94379425048828 Optimization Steps: 123
***Symmetric Check開始***
Target: 10, victim: 11, Loss: 1.9296, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:96.64, Cost:0.02 best_reg:97.33 avg_loss_reg:97.33:  89%|[redacted]| 110/123 [01:23<00:09,  1.31it/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: 363.1817283630371
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000105----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '0-2', '1-0', '1-2', '2-0', '4-9', '4-13', '5-6', '6-5', '8-9', '11-12', '12-11', '12-13', '13-12', '17-13']
***Trigger Reverse Engineering開始***
Target: 11, victim: 12, Loss: 2.4650, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:451.61, Cost:0.01 best_reg:452.81 avg_loss_reg:452.81:  47%|[redacted]| 473/1000 [27:58<31:10,  3.55s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 12 Trigger Size: 451.6145324707031 Optimization Steps: 121
***Symmetric Check開始***
Target: 12, victim: 11, Loss: 5.2288, Acc: 80.00%, CE_Loss: 0.43, Reg_Loss:421.59, Cost:0.01 best_reg:439.97 avg_loss_reg:439.97: 100%|[redacted]| 121/121 [07:04<00:00,  3.51s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 2117.608879804611
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000106----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 12, Loss: 0.7036, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:363.11, Cost:0.00 best_reg:367.69 avg_loss_reg:358.63:   6%|[redacted]| 64/1000 [48:36<11:50:53, 45.57s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 367.68621215820315 Optimization Steps: 65
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 2938.888060569763
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000107----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['4-3', '20-16']
***Trigger Reverse Engineering開始***
Target: 4, victim: 3, Loss: 3.0681, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:165.09, Cost:0.02 best_reg:169.81 avg_loss_reg:169.81:  12%|[redacted]| 121/1000 [00:55<06:42,  2.19it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 3 Trigger Size: 165.09390258789062 Optimization Steps: 111
***Symmetric Check開始***
Target: 3, victim: 4, Loss: 3.8735, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:727.29, Cost:0.01 best_reg:736.65 avg_loss_reg:736.65: 100%|[redacted]| 111/111 [00:51<00:00,  2.16it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 117.91414546966553
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000108----------
```

```
***Pre-Screening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: 4.5439, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:256.25, Cost:0.02 best_reg:259.15 avg_loss_reg:259.15:  12%|          | 117/1000 [04:22<32:57,  2.24s/it]
  0%|          | 0/118 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 4 Trigger Size: 256.2516174316406 Optimization Steps: 118
***Symmetric Check開始***
Target: 4, victim: 5, Loss: 5.1796, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:193.12, Cost:0.03 best_reg:194.85 avg_loss_reg:194.85:  90%|          | 106/118 [03:57<00:26,  2.24s/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: 510.287034034729
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000109----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-0']
***Trigger Reverse Engineering開始***
Target: 6, victim: 0, Loss: 2.4947, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:28.04, Cost:0.09 best_reg:28.99 avg_loss_reg:28.99:   6%|          | 65/1000 [02:50<40:46,  2.62s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 0 Trigger Size: 28.038414001464844 Optimization Steps: 66
***Symmetric Check開始***
Target: 0, victim: 6, Loss: 0.2435, Acc: 90.00%, CE_Loss: 0.24, Reg_Loss:11105.07, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:11071.01: 100%|          | 66/66 [02:49<00:00,  2.57s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 346.94814705848694
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000110----------------------------------------
***Pre-Screening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', '3-0', '3-1']
***Trigger Reverse Engineering開始***
Target: 3, victim: 0, Loss: 0.8395, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:65.39, Cost:0.01 best_reg:65.61 avg_loss_reg:65.89:  15%|          | 151/1000 [03:56<22:11,  1.57s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 0 Trigger Size: 65.3886947631836 Optimization Steps: 109
***Symmetric Check開始***
Target: 0, victim: 3, Loss: 4.3591, Acc: 80.00%, CE_Loss: 0.67, Reg_Loss:1638.11, Cost:0.00 best_reg:1731.56 avg_loss_reg:1605.43: 100%|          | 109/109 [02:50<00:00,  1.57s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 411.64203238487244
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000111----------------------------------------
***Pre-Screening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', '3-1']
***Trigger Reverse Engineering開始***
Target: 3, victim: 1, Loss: 2.5371, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:62.36, Cost:0.04 best_reg:62.73 avg_loss_reg:62.73:  13%|          | 127/1000 [07:01<48:14,  3.32s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 1 Trigger Size: 62.36111068725586 Optimization Steps: 96
***Symmetric Check開始***
Target: 1, victim: 3, Loss: 12.7388, Acc: 90.00%, CE_Loss: 0.46, Reg_Loss:478.94, Cost:0.03 best_reg:509.06 avg_loss_reg:485.13: 100%|          | 96/96 [05:15<00:00,  3.29s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 751.0286712646484
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000112----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '1-2', '2-18', '3-18', '6-10', '8-10', '8-15', '8-11', '9-11', '10-4', '10-11', '10-15', '12-11', '13-18', '14-15', '15-0', '15-10', '15-14', '17-14', '18-2']
***Trigger Reverse Engineering開始***
Target: 0, victim: 1, Loss: 1.9968, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:162.47, Cost:0.01 best_reg:162.94 avg_loss_reg:162.94:  47%|          | 469/1000 [14:06<15:58,  1.80s/it]
```

early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 162.4669189453125 Optimization Steps: 125
***Symmetric Check開始***
Target: 1, victim: 0, Loss: 2.8401, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:347.15, Cost:0.01 best_reg:347.16 avg_loss_reg:347.16:  97%|[redacted]| 121/125 [03:47<00:07,  1.88s/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: 1085.906078338623
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000113----------
***Pre-Screening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', '1-6', '1-9', '1-10', '2-5', '2-13', '3-2', '3-14', '3-16', '4-5', '4-15', '5-4', '5-15', '5-13', '6-8', '6-1', '6-10', '7-6', '7-11', '7-17', '8-1', '8-10', '8-15', '9-8', '10-1', '10-7', '10-8', '11-4', '11-7', '11-8', '12-2', '13-5', '13-17', '13-18', '14-3', '14-5', '15-4', '15-18', '16-3', '16-17', '16-18', '17-4', '17-18', '18-13', '18-15', '18-17']
***Trigger Reverse Engineering開始***
Target: 6, victim: 8, Loss: 1.8318, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:20.70, Cost:0.09 best_reg:22.32 avg_loss_reg:22.32:  89%|[redacted]| 886/1000 [08:41<01:07,  1.70it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 8 Trigger Size: 20.697288513183594 Optimization Steps: 68
***Symmetric Check開始***
Target: 8, victim: 6, Loss: 6.0641, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:510.32, Cost:0.01 best_reg:539.62 avg_loss_reg:539.62: 100%|[redacted]| 68/68 [00:39<00:00,  1.73it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 567.4964280128479
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000114----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-0', '4-5', '5-4', '6-7']
***Trigger Reverse Engineering開始***
Target: 4, victim: 5, Loss: 2.1294, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:117.06, Cost:0.02 best_reg:117.27 avg_loss_reg:117.27:  21%|[redacted]| 209/1000 [00:49<03:05,  4.26it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 5 Trigger Size: 117.05807495117188 Optimization Steps: 107
***Symmetric Check開始***
Target: 5, victim: 4, Loss: 7.3185, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:620.32, Cost:0.01 best_reg:635.57 avg_loss_reg:635.57: 100%|[redacted]| 107/107 [00:24<00:00,  4.29it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 75.74338817596436
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000115----------
***Pre-Screening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']
***Trigger Reverse Engineering開始***
Target: 7, victim: 0, Loss: 1.4147, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:382.63, Cost:0.00 best_reg:385.27 avg_loss_reg:385.27:  16%|[redacted]| 163/1000 [08:05<41:32,  2.98s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 0 Trigger Size: 382.6292419433594 Optimization Steps: 164
***Symmetric Check開始***
Target: 0, victim: 7, Loss: 5.9056, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:223.56, Cost:0.03 best_reg:226.47 avg_loss_reg:226.47:  68%|[redacted]| 111/164 [05:33<02:39,  3.00s/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: 826.9991669654846
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000116----------
***Pre-Screening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', '3-8']
***Trigger Reverse Engineering開始***
Target: 3, victim: 8, Loss: 1.2394, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:717.09, Cost:0.00 best_reg:717.47 avg_loss_reg:717.47:  32%|[redacted]| 322/1000 [05:24<11:23,  1.01s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 8 Trigger Size: 717.0944213867188 Optimization Steps: 180
***Symmetric Check開始***

```
Target: 8, victim: 3, Loss: 3.2231, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:586.81, Cost:0.01 best_reg:585.57 avg_loss_reg:585.71: 100%|██████████| 180/180 [03:01<00:00,  1.01s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 512.6645107269287
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000117----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-0', '1-20', '2-3', '4-8', '5-4', '6-0', '6-4', '6-20', '10-15', '11-17', '11-20', '12-16', '13-9', '14-15', '14-10', '14-13', '15-10', '15-13', '15-14', '18-19', '19-16', '20-1']
***Trigger Reverse Engineering開始***
Target: 15, victim: 10, Loss: 1.6581, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:126.23, Cost:0.01 best_reg:128.95 avg_loss_reg:128.95:  54%|█████▍    | 544/1000 [05:23<04:30,  1.68it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 15 Victim Class: 10 Trigger Size: 126.22673034667969 Optimization Steps: 124
***Symmetric Check開始***
Target: 10, victim: 15, Loss: 0.7991, Acc: 90.00%, CE_Loss: 0.20, Reg_Loss:397.88, Cost:0.00 best_reg:408.56 avg_loss_reg:399.83: 100%|██████████| 124/124 [01:13<00:00,  1.68it/s]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 404.27442693710327
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000118----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-18', '0-21', '1-2', '3-2', '4-2', '5-6', '7-9', '7-10', '8-9', '8-10', '8-12', '9-10', '11-9', '11-10', '11-21', '12-6', '13-16', '14-15', '15-14', '15-22', '18-0', '18-21', '18-22', '20-21', '21-22', '22-15']
***Trigger Reverse Engineering開始***
Target: 11, victim: 10, Loss: 2.7937, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:67.31, Cost:0.04 best_reg:67.33 avg_loss_reg:67.33:  60%|██████    | 596/1000 [10:59<07:27,  1.11s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 10 Trigger Size: 67.31299591064453 Optimization Steps: 112
***Symmetric Check開始***
Target: 10, victim: 11, Loss: 4.5236, Acc: 100.00%, CE_Loss: 0.43, Reg_Loss:359.53, Cost:0.01 best_reg:358.30 avg_loss_reg:358.90: 100%|██████████| 112/112 [02:00<00:00,  1.08s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 788.7021725177765
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000119----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-0', '6-5', '10-9', '11-10', '12-0', '12-9', '12-10']
***Trigger Reverse Engineering開始***
Target: 12, victim: 9, Loss: 2.2421, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:115.66, Cost:0.02 best_reg:120.01 avg_loss_reg:120.01:  22%|██        | 217/1000 [10:46<38:54,  2.98s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 9 Trigger Size: 115.65518188476562 Optimization Steps: 121
***Symmetric Check開始***
Target: 9, victim: 12, Loss: 2.6178, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:317.41, Cost:0.01 best_reg:330.95 avg_loss_reg:315.39: 100%|██████████| 121/121 [06:21<00:00,  3.15s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1043.3193871974945
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000120----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-2', '5-4']
***Trigger Reverse Engineering開始***
Target: 5, victim: 4, Loss: 1.0518, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:198.28, Cost:0.01 best_reg:203.17 avg_loss_reg:203.17:  15%|█         | 153/1000 [02:37<14:31,  1.03s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 4 Trigger Size: 198.27621459960938 Optimization Steps: 133
***Symmetric Check開始***
Target: 4, victim: 5, Loss: 3.5324, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:988.49, Cost:0.00 best_reg:1005.01 avg_loss_reg:1005.01: 100%|██████████| 133/133 [02:16<00:00,  1.02s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 299.5324423313141
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000121----------------------------------------
***Pre-Screening開始***
```

```
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-4']
***Trigger Reverse Engineering開始***
Target: 3, victim: 4, Loss: 6.9917, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:590.24, Cost:0.01 best_reg:595.65 avg_loss_reg:595.65:  13%|          | 130/1000 [05:43<38:15,  2.64s/it]
  0%|          | 0/131 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 4 Trigger Size: 590.2437744140625 Optimization Steps: 131
***Symmetric Check開始***
Target: 4, victim: 3, Loss: 3.5460, Acc: 95.00%, CE_Loss: 0.35, Reg_Loss:630.44, Cost:0.01 best_reg:636.02 avg_loss_reg:636.02: 100%|| 131/131 [05:43<00:00,  2.62s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 695.6213431358337
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000122----------
***Pre-Screening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', '1-2', '1-3', '2-1', '2-3', '2-12', '3-1', '3-2', '6-1', '6-12', '6-14', '8-7', '12-14', '13-12']
***Trigger Reverse Engineering開始***
Target: 12, victim: 14, Loss: 4.3537, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:156.31, Cost:0.03 best_reg:157.77 avg_loss_reg:157.77:  40%|      | 403/1000 [03:54<05:47,  1.72it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 12 Victim Class: 14 Trigger Size: 156.30853271484375 Optimization Steps: 111
***Symmetric Check開始***
Target: 14, victim: 12, Loss: 3.8831, Acc: 90.00%, CE_Loss: 0.57, Reg_Loss:193.66, Cost:0.02 best_reg:204.40 avg_loss_reg:204.40: 100%|| 111/111 [01:04<00:00,  1.71it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 305.4937949180603
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000123----------
***Pre-Screening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', '6-3', '18-15']
***Trigger Reverse Engineering開始***
Target: 6, victim: 3, Loss: 4.5250, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:550.12, Cost:0.01 best_reg:551.83 avg_loss_reg:563.55:  32%|      | 324/1000 [16:38<34:42,  3.08s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 3 Trigger Size: 550.119140625 Optimization Steps: 200
***Symmetric Check開始***
Target: 3, victim: 6, Loss: 1.3999, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:234.26, Cost:0.01 best_reg:235.69 avg_loss_reg:233.82:  84%|  | 168/200 [08:38<01:38,  3.09s/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: 1532.343828201294
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000124----------
***Pre-Screening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', '4-2', '9-10', '9-11', '10-9', '10-11', '11-5', '11-9', '12-9', '17-18', '18-16']
***Trigger Reverse Engineering開始***
Target: 11, victim: 9, Loss: 2.3399, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:124.16, Cost:0.02 best_reg:126.68 avg_loss_reg:126.68:  36%|      | 359/1000 [11:38<20:46,  1.94s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 11 Victim Class: 9 Trigger Size: 124.16310119628906 Optimization Steps: 120
***Symmetric Check開始***
Target: 9, victim: 11, Loss: 2.9803, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:241.18, Cost:0.01 best_reg:241.99 avg_loss_reg:241.99:  98%|  | 118/120 [03:57<00:04,  2.01s/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: 947.5777244567871
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000125----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.717326879501343
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000126----------
```

```
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-11', '7-8', '8-7', '13-12']
***Trigger Reverse Engineering開始***
Target: 6, victim: 11, Loss: 2.1514, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:79.97, Cost:0.03 best_reg:80.32 avg_loss_reg:78.82:  20%|██        | 200/1000 [06:28<25:55,  1.94s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 11 Trigger Size: 79.96708679199219 Optimization Steps: 96
***Symmetric Check開始***
Target: 11, victim: 6, Loss: 9.3264, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:1185.39, Cost:0.01 best_reg:1198.95 avg_loss_reg:1198.95: 100%|██████████| 96/96 [03:12<00:00,  2.00s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 591.0879402160645
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000127----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-4', '4-3']
***Trigger Reverse Engineering開始***
Target: 4, victim: 3, Loss: 1.4260, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:117.19, Cost:0.01 best_reg:117.56 avg_loss_reg:117.56:  18%|█▊        | 177/1000 [02:10<10:07,  1.35it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 3 Trigger Size: 117.18589782714844 Optimization Steps: 140
***Symmetric Check開始***
Target: 3, victim: 4, Loss: 5.0992, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:190.44, Cost:0.03 best_reg:191.31 avg_loss_reg:191.31:  71%|███████▏   | 100/140 [01:14<00:29,  1.35it/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: 209.61444425582886
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000128----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-3']
***Trigger Reverse Engineering開始***
Target: 5, victim: 3, Loss: 0.5259, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:18.71, Cost:0.03 best_reg:18.74 avg_loss_reg:18.74:  10%|█         | 105/1000 [04:42<40:10,  2.69s/it]
  0%|          | 0/106 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 3 Trigger Size: 18.708370208740234 Optimization Steps: 106
***Symmetric Check開始***
Target: 3, victim: 5, Loss: 0.8196, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:734.69, Cost:0.00 best_reg:753.17 avg_loss_reg:753.17: 100%|██████████| 106/106 [04:43<00:00,  2.67s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 576.2841520309448
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000129----------------------------------------
***Pre-Screening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', '7-0']
***Trigger Reverse Engineering開始***
Target: 4, victim: 3, Loss: 0.8140, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:42.84, Cost:0.02 best_reg:43.23 avg_loss_reg:43.23:  12%|█▏        | 120/1000 [03:26<25:17,  1.72s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 3 Trigger Size: 42.83763885498047 Optimization Steps: 110
***Symmetric Check開始***
Target: 3, victim: 4, Loss: 1.0948, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:377.54, Cost:0.00 best_reg:432.35 avg_loss_reg:377.84: 100%|██████████| 110/110 [03:08<00:00,  1.71s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 400.0369601249695
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000130----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['6-5', '6-7', '7-5', '9-5', '13-8', '15-16']
***Trigger Reverse Engineering開始***
Target: 15, victim: 16, Loss: 3.1505, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:394.42, Cost:0.01 best_reg:395.10 avg_loss_reg:395.10:  30%|███       | 305/1000 [04:18<09:47,  1.18it/s]
```

early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 15 Victim Class: 16 Trigger Size: 394.4214782714844 Optimization Steps: 130
***Symmetric Check開始***
Target: 16, victim: 15, Loss: 2.4904, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:299.35, Cost:0.01 best_reg:300.02 avg_loss_reg:300.02:  98%|[redacted]| 128/130 [01:49<00:01,  1.17it/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: 375.6776239871979
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000131----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-4', '3-4', '4-0', '5-4', '6-4', '7-0', '9-7', '10-7', '15-0', '20-16', '20-19', '21-0']
***Trigger Reverse Engineering開始***
Target: 2, victim: 4, Loss: 3.2724, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:274.49, Cost:0.01 best_reg:277.77 avg_loss_reg:277.77:  43%|[redacted]| 432/1000 [16:15<21:22,  2.26s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 4 Trigger Size: 274.4857482910156 Optimization Steps: 111
***Symmetric Check開始***
Target: 4, victim: 2, Loss: 5.4364, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:306.08, Cost:0.02 best_reg:307.11 avg_loss_reg:307.11: 100%|[redacted]| 111/111 [04:14<00:00,  2.30s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1245.7302441596985
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000132----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-4', '4-3', '5-2']
***Trigger Reverse Engineering開始***
Target: 5, victim: 2, Loss: 2.7454, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:31.02, Cost:0.09 best_reg:34.79 avg_loss_reg:34.79:  11%|[redacted]| 111/1000 [01:05<08:42,  1.70it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 5 Victim Class: 2 Trigger Size: 31.02216339111328 Optimization Steps: 67
***Symmetric Check開始***
Target: 2, victim: 5, Loss: 4.5762, Acc: 100.00%, CE_Loss: 0.60, Reg_Loss:1178.76, Cost:0.00 best_reg:1240.46 avg_loss_reg:1240.46: 100%|[redacted]| 67/67 [00:39<00:00,  1.71it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 106.6081268787384
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000133----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 16.397372245788574
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000134----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-2', '1-0', '1-2', '4-13', '12-14', '14-12']
***Trigger Reverse Engineering開始***
Target: 1, victim: 2, Loss: 2.9708, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:553.83, Cost:0.01 best_reg:554.73 avg_loss_reg:556.53:  26%|[redacted]| 265/1000 [13:35<37:43,  3.08s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 2 Trigger Size: 553.8289184570312 Optimization Steps: 142
***Symmetric Check開始***
Target: 2, victim: 1, Loss: 2.9939, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:832.98, Cost:0.00 best_reg:819.21 avg_loss_reg:819.21: 100%|[redacted]| 142/142 [07:15<00:00,  3.07s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1265.0010001659393
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000135----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-4', '6-3']
***Trigger Reverse Engineering開始***
Target: 2, victim: 4, Loss: 4.0457, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:29.44, Cost:0.13 best_reg:31.55 avg_loss_reg:31.55:   9%|[redacted]| 91/1000 [02:50<28:26,  1.88s/it]

early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 4 Trigger Size: 29.444793701171875 Optimization Steps: 81
***Symmetric Check開始***
Target: 4, victim: 2, Loss: 6.8036, Acc: 90.00%, CE_Loss: 0.34, Reg_Loss:1914.46, Cost:0.00 best_reg:1948.31 avg_loss_reg:1948.31: 100%| 81/81 [02:30<00:00, 1.86s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 326.468638420105
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000136----------
***Pre-Screening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', '8-6', '8-7']
***Trigger Reverse Engineering開始***
Target: 8, victim: 7, Loss: 3.6840, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:60.22, Cost:0.06 best_reg:61.64 avg_loss_reg:61.64: 17%| | 174/1000 [02:29<11:48, 1.17it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 7 Trigger Size: 60.22124481201172 Optimization Steps: 100
***Symmetric Check開始***
Target: 7, victim: 8, Loss: 3.5618, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:296.82, Cost:0.01 best_reg:303.47 avg_loss_reg:303.47: 100%| 100/100 [01:25<00:00, 1.16it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 241.4755573272705
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000137----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '1-0', '1-7', '2-9', '2-4', '2-3', '3-2', '4-2', '5-4', '5-6', '6-0', '6-10', '6-12', '7-11', '7-9', '7-13', '8-3', '9-8', '9-11', '10-0', '10-5', '11-7', '11-12', '11-13', '12-6', '12-10', '13-3', '13-12']
***Trigger Reverse Engineering開始***
Target: 0, victim: 1, Loss: 7.4824, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:187.92, Cost:0.04 best_reg:189.61 avg_loss_reg:189.96: 57%| | 566/1000 [05:42<04:22, 1.65it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 187.91848754882812 Optimization Steps: 109
***Symmetric Check開始***
Target: 1, victim: 0, Loss: 1.6454, Acc: 90.00%, CE_Loss: 0.15, Reg_Loss:295.09, Cost:0.01 best_reg:321.30 avg_loss_reg:297.06: 100%| 109/109 [01:04<00:00, 1.69it/s]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 412.7281537055969
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000138----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-8', '0-13', '1-2', '2-1', '3-5', '3-6', '4-3', '4-6', '4-5', '5-3', '5-6', '5-16', '6-3', '7-8', '7-9', '7-14', '8-9', '8-0', '8-10', '9-1', '9-8', '10-2', '10-8', '10-16', '11-1', '11-12', '11-13', '12-0', '12-7', '13-9', '14-7', '14-15', '14-22', '15-21', '16-14', '16-15', '16-6', '18-23', '19-15', '19-18', '19-17', '20-21', '20-18', '20-8', '21-9', '21-15', '21-17', '22-14', '22-19', '22-18', '23-22', '23-18', '23-21']
***Trigger Reverse Engineering開始***
Target: 20, victim: 21, Loss: 1.7341, Acc: 95.00%, CE_Loss: 0.29, Reg_Loss:285.03, Cost:0.01 best_reg:291.77 avg_loss_reg:292.55: 100%| 1000/1000 [55:24<00:00, 3.32s/it]
***Trigger Reverse Engineering結束***
Target Class: 20 Victim Class: 21 Trigger Size: 291.7674560546875 Optimization Steps: 214
***Symmetric Check開始***
Target: 21, victim: 20, Loss: 1.6959, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:687.32, Cost:0.00 best_reg:688.03 avg_loss_reg:688.32: 77%| | 164/214 [09:23<02:51, 3.44s/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: 3905.1686387062073
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000139----------
***Pre-Screening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', '6-3', '6-2']
***Trigger Reverse Engineering開始***
Target: 6, victim: 2, Loss: 6.9645, Acc: 0.00%, CE_Loss: 6.96, Reg_Loss:2537.13, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2524.44: 3%| | 32/1000 [01:50<55:42, 3.45s/it]
***Trigger Reverse Engineering結束***
Target Class: 6 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 120.29187750816345
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000140----------

```
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 23.776296138763428
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000141----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-19', '4-13', '5-2', '7-6', '8-9', '9-14', '10-9', '12-9', '14-17', '15-13', '17-14', '18-13', '19-6']
***Trigger Reverse Engineering開始***
Target: 7, victim: 6, Loss: 2.7522, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:495.87, Cost:0.01 best_reg:503.39 avg_loss_reg:497.48:  44%|[redacted]      | 442/1000 [07:23<09:20,  1.00s/it]
  0%|          | 0/130 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 6 Trigger Size: 495.8712158203125 Optimization Steps: 130
***Symmetric Check開始***
Target: 6, victim: 7, Loss: 2.3971, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:183.48, Cost:0.01 best_reg:186.70 avg_loss_reg:186.70:  95%|[redacted] | 123/130 [02:04<00:07,  1.01s/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: 576.9855492115021
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000142----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['8-6', '10-6', '13-14', '17-18']
***Trigger Reverse Engineering開始***
Target: 13, victim: 14, Loss: 7.5496, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:125.70, Cost:0.06 best_reg:130.17 avg_loss_reg:130.17:  20%|[redacted]       | 200/1000 [00:50<03:22,  3.95it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 14 Trigger Size: 125.70492553710938 Optimization Steps: 96
***Symmetric Check開始***
Target: 14, victim: 13, Loss: 7.0482, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:117.31, Cost:0.06 best_reg:120.87 avg_loss_reg:120.87:  99%|[redacted]| 95/96 [00:24<00:00,  3.94it/s]
early stop 所有
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 79.98512291908264
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000143----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-4']
***Trigger Reverse Engineering開始***
Target: 3, victim: 4, Loss: 2.9690, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:50.90, Cost:0.06 best_reg:51.46 avg_loss_reg:51.46:   6%|[redacted]         | 65/1000 [03:05<44:28,  2.85s/it]
  0%|          | 0/66 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 4 Trigger Size: 50.90488052368164 Optimization Steps: 66
***Symmetric Check開始***
Target: 4, victim: 3, Loss: 3.2524, Acc: 5.00%, CE_Loss: 3.25, Reg_Loss:11543.80, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:11396.26: 100%|[redacted]| 66/66 [03:05<00:00,  2.81s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 383.44606041908264
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000144----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 5.665728807449341
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000145----------
***Pre-Screening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', '0-11', '1-0', '2-1', '2-11', '2-14', '4-3', '4-8', '4-14', '6-9', '7-14', '8-9', '8-11', '9-8', '9-12', '10-3', '10-4', '12-9', '12-13', '13-12', '14-5', '15-16', '15-17', '16-15', '18-7', '18-16', '18-17', '19-10', '19-17']
***Trigger Reverse Engineering開始***
Target: 4, victim: 14, Loss: 4.0328, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:148.64, Cost:0.03 best_reg:151.11 avg_loss_reg:151.11:  60%|[redacted]    | 604/1000 [07:52<05:09,  1.28it/s]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: 14 Trigger Size: 148.6416015625 Optimization Steps: 105
```

```
***Symmetric Check開始***
Target: 14, victim: 4, Loss: 6.0884, Acc: 90.00%, CE_Loss: 0.33, Reg_Loss:505.73, Cost:0.01 best_reg:517.89 avg_loss_reg:517.89: 100%|██████████| 105/105 [01:22<00:00,  1.28it/s]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 560.7199630737305
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000146----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-12', '2-14', '7-10', '13-14']
***Trigger Reverse Engineering開始***
Target: 7, victim: 10, Loss: 2.6537, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:309.14, Cost:0.01 best_reg:309.79 avg_loss_reg:312.27:  17%|█▋        | 166/1000 [06:43<33:48,  2.43s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 10 Trigger Size: 309.1419982910156 Optimization Steps: 123
***Symmetric Check開始***
Target: 10, victim: 7, Loss: 7.1232, Acc: 90.00%, CE_Loss: 0.50, Reg_Loss:872.46, Cost:0.01 best_reg:902.85 avg_loss_reg:878.10: 100%|██████████| 123/123 [05:03<00:00,  2.46s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 719.8309864997864
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000147----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 6.653322458267212
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000148----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-1']
***Trigger Reverse Engineering開始***
Target: 5, victim: 1, Loss: 9.1225, Acc: 0.00%, CE_Loss: 9.12, Reg_Loss:2552.96, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2536.77:   1%|          | 10/1000 [00:58<1:37:04,  5.88s/it]
***Trigger Reverse Engineering結束***
Target Class: 5 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: 71.76907205581665
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000149----------------------------------------
***Pre-Screening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', '2-0', '5-6', '6-5', '8-10', '9-13', '10-8', '13-1', '13-6', '13-9']
***Trigger Reverse Engineering開始***
Target: 10, victim: 8, Loss: 1.5686, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:126.23, Cost:0.01 best_reg:126.26 avg_loss_reg:126.26:  37%|████▏     | 373/1000 [06:16<10:32,  1.01s/it]
  0%|          | 0/117 [00:00<?, ?it/s]early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 8 Trigger Size: 126.23197174072266 Optimization Steps: 117
***Symmetric Check開始***
Target: 8, victim: 10, Loss: 1.4395, Acc: 95.00%, CE_Loss: 0.18, Reg_Loss:166.03, Cost:0.01 best_reg:167.99 avg_loss_reg:167.43: 100%|██████████| 117/117 [02:03<00:00,  1.06s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 507.0618498325348
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000150----------------------------------------
***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: 5.0200, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:2231.11, Cost:0.00 best_reg:2213.04 avg_loss_reg:2234.28:  13%|█▎        | 131/1000 [43:41<4:49:46, 20.01s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 2209.4636840820312 Optimization Steps: 132
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 2632.6103870868683
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000151----------------------------------------
```

```
***Pre-Screening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: 11.6228, Acc: 0.00%, CE_Loss: 11.62, Reg_Loss:2554.15, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2539.58:   1%|          | 10/1000 [00:46<1:16:27,  4.63s/it]
***Trigger Reverse Engineering結束***
Target Class: 3 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: 59.49239540100098
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000152----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 0
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 0, victim: 12, Loss: 0.7194, Acc: 93.75%, CE_Loss: 0.14, Reg_Loss:33.83, Cost:0.02 best_reg:35.39 avg_loss_reg:35.93:  12%|▉          | 124/1000 [32:02<3:46:21, 15.50s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 35.39406051635742 Optimization Steps: 125
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1928.2809221744537
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000153----------
***Pre-Screening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', '1-2', '2-0', '2-1', '2-3', '3-1', '3-13', '4-5', '5-14', '6-7', '6-14', '6-15', '7-14', '7-15', '8-9', '9-8', '9-12', '11-13', '12-13', '13-11', '13-12', '14-15']
***Trigger Reverse Engineering開始***
Target: 13, victim: 12, Loss: 1.7617, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:316.87, Cost:0.01 best_reg:317.82 avg_loss_reg:316.86:  52%|▌████▏     | 523/1000 [20:32<18:44,  2.36s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 13 Victim Class: 12 Trigger Size: 316.87066650390625 Optimization Steps: 139
***Symmetric Check開始***
Target: 12, victim: 13, Loss: 3.2861, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:262.59, Cost:0.01 best_reg:266.82 avg_loss_reg:254.87:  86%|████████▋ | 119/139 [04:52<00:49,  2.46s/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: 1536.9603927135468
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000154----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-0', '2-3', '3-2', '4-5']
***Trigger Reverse Engineering開始***
Target: 3, victim: 2, Loss: 1.1236, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:136.58, Cost:0.01 best_reg:136.80 avg_loss_reg:136.80:  17%|▏          | 173/1000 [04:16<20:27,  1.48s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 2 Trigger Size: 136.57879638671875 Optimization Steps: 140
***Symmetric Check開始***
Target: 2, victim: 3, Loss: 4.0775, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:333.89, Cost:0.01 best_reg:335.88 avg_loss_reg:335.88:  94%|█████████▍| 132/140 [03:22<00:12,  1.53s/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: 462.49137473106384
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000155----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-4', '2-7', '3-2', '7-9', '8-7', '8-9', '9-7', '10-11', '11-10', '11-14', '11-19', '17-19', '18-19']
***Trigger Reverse Engineering開始***
Target: 17, victim: 19, Loss: 1.3248, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:142.96, Cost:0.01 best_reg:143.00 avg_loss_reg:143.00:  40%|████      | 399/1000 [09:51<14:50,  1.48s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 17 Victim Class: 19 Trigger Size: 142.96051025390625 Optimization Steps: 130
***Symmetric Check開始***
Target: 19, victim: 17, Loss: 1.4546, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:172.75, Cost:0.01 best_reg:171.77 avg_loss_reg:171.77: 100%|██████████| 130/130 [03:19<00:00,  1.53s/it]
```

```
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 799.8822538852692
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000156----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['8-5']
***Trigger Reverse Engineering開始***
Target: 8, victim: 5, Loss: 6.5113, Acc: 0.00%, CE_Loss: 6.51, Reg_Loss:2598.83, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2572.49:   1%|          | 10/1000 [00:36<59:43,  3.62s/it]
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 45.05442976951599
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000157----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['7-6']
***Trigger Reverse Engineering開始***
Target: 7, victim: 6, Loss: 5.9989, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:224.28, Cost:0.03 best_reg:226.74 avg_loss_reg:226.74:  10%|▉         | 96/1000 [01:51<17:33,  1.16s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 7 Victim Class: 6 Trigger Size: 224.2831268310547 Optimization Steps: 97
***Symmetric Check開始***
Target: 6, victim: 7, Loss: 2.2574, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:605.85, Cost:0.00 best_reg:626.93 avg_loss_reg:626.93: 100%|██████████| 97/97 [01:51<00:00,  1.15s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 226.7733347415924
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000158----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-15', '9-8', '17-10', '17-11']
***Trigger Reverse Engineering開始***
Target: 17, victim: 11, Loss: 2.2357, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:611.21, Cost:0.00 best_reg:617.98 avg_loss_reg:624.30:  27%|██▋       | 274/1000 [24:45<1:05:37,  5.42s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 17 Victim Class: 11 Trigger Size: 611.21484375 Optimization Steps: 164
***Symmetric Check開始***
Target: 11, victim: 17, Loss: 1.5146, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:391.45, Cost:0.00 best_reg:401.44 avg_loss_reg:399.60: 100%|██████████| 164/164 [14:45<00:00,  5.40s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 2401.6984424591064
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000159----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-2', '6-8', '6-13', '7-6', '7-8', '8-6', '8-10', '10-6', '10-8', '11-15', '15-11', '16-15']
***Trigger Reverse Engineering開始***
Target: 16, victim: 15, Loss: 1.8926, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:148.10, Cost:0.01 best_reg:148.99 avg_loss_reg:148.99:  36%|███▋      | 364/1000 [20:11<35:17,  3.33s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 16 Victim Class: 15 Trigger Size: 148.09637451171875 Optimization Steps: 127
***Symmetric Check開始***
Target: 15, victim: 16, Loss: 1.0746, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:409.12, Cost:0.00 best_reg:425.95 avg_loss_reg:405.20: 100%|██████████| 127/127 [06:56<00:00,  3.28s/it]
***Symmetric Check結束***
********************檢測結束**********************
檢測結果: Model是安全的(Benign)
整體耗時: 1645.4403192996979
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000160----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['10-11', '14-13']
***Trigger Reverse Engineering開始***
Target: 14, victim: 13, Loss: 7.6136, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:286.37, Cost:0.03 best_reg:287.72 avg_loss_reg:287.72:  11%|▉         | 109/1000 [03:40<30:03,  2.02s/it]
```

```
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 14 Victim Class: 13 Trigger Size: 286.3678894042969 Optimization Steps: 99
***Symmetric Check開始***
Target: 13, victim: 14, Loss: 11.4595, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:129.27, Cost:0.09 best_reg:130.57 avg_loss_reg:130.57:  91%|[redacted] | 90/99 [03:02<00:18,  2.03s/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: 414.28334045410156
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000161----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['5-3', '8-6']
***Trigger Reverse Engineering開始***
Target: 8, victim: 6, Loss: 2.2239, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:179.08, Cost:0.01 best_reg:182.72 avg_loss_reg:182.72:  13%|[redacted] | 128/1000 [05:27<37:12,  2.56s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 8 Victim Class: 6 Trigger Size: 179.07894897460938 Optimization Steps: 118
***Symmetric Check開始***
Target: 6, victim: 8, Loss: 3.5912, Acc: 95.00%, CE_Loss: 0.27, Reg_Loss:291.73, Cost:0.01 best_reg:304.98 avg_loss_reg:294.33: 100%|[redacted]| 118/118 [04:55<00:00,  2.51s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 634.2849185466766
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000162----------------------------------------
***Pre-Screening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', '4-8', '5-6', '5-8', '6-5', '6-8', '6-11', '8-7', '8-12', '10-11', '10-12', '11-6', '11-10', '11-12', '13-14', '14-12', '15-17', '19-17']
***Trigger Reverse Engineering開始***
Target: 10, victim: 12, Loss: 3.2137, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:261.40, Cost:0.01 best_reg:262.83 avg_loss_reg:262.83:  45%|[redacted] | 447/1000 [25:54<32:03,  3.48s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 10 Victim Class: 12 Trigger Size: 261.40325927734375 Optimization Steps: 142
***Symmetric Check開始***
Target: 12, victim: 10, Loss: 7.5724, Acc: 100.00%, CE_Loss: 0.49, Reg_Loss:276.46, Cost:0.03 best_reg:277.01 avg_loss_reg:277.01:  79%|[redacted] | 112/142 [07:34<02:01,  4.05s/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: 2029.6381077766418
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round2\TrainData\models\unzip\id-00000163----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['2-1', '5-3', '6-1', '6-4', '8-13', '9-10', '9-13', '10-9', '10-13', '11-12', '12-11']
***Trigger Reverse Engineering開始***
Target: 12, victim: 11, Loss: 2.8161, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:2767.58, Cost:0.00 best_reg:2769.93 avg_loss_reg:2819.71:  24%|[redacted] | 235/1000 [02:33<08:20,  1.53it/s]
Traceback (most recent call last):
  File "D:\UULi\test_code\k_arm_test\main.py", line 158, in <module>
    trigger_reverse_engineering(target_classes, victim_classes, backdoor_type, model, DATA_PATH,
  File "D:\UULi\test_code\k_arm_test\k_arm\reverse.py", line 54, in trigger_reverse_engineering
    pattern, mask, l1_norm, time_cost = scanner.scanning(
  File "D:\UULi\test_code\k_arm_test\k_arm\scanner.py", line 149, in scanning
    f'Target: {target_classes[target_index]}, victim: {labels[0]}, Loss: {loss:.4f},'
  File "C:\Users\islab\anaconda3\envs\pytorch1\lib\site-packages\torch\tensor.py", line 534, in __format__
    return self.item().__format__(format_spec)
KeyboardInterrupt

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