```
C:\Users\islab\anaconda3\envs\pytorch1_2_0\python.exe D:\UULi\test_code\k_arm_test\main.py
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000000----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 4, Loss: 0.2135, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:63.20, Cost:0.00 best_reg:63.08 avg_loss_reg:63.74:   7%|▌         | 66/1000 [13:44<3:14:24, 12.49s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 63.07805800437927 Optimization Steps: 67
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 828.2831335067749
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000001----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 4.70327615737915
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000002----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 3
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 3, victim: 4, Loss: 0.3418, Acc: 90.00%, CE_Loss: 0.18, Reg_Loss:70.53, Cost:0.00 best_reg:79.39 avg_loss_reg:76.94:   5%|▍         | 52/1000 [18:54<5:44:34, 21.81s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: all Trigger Size: 79.38817358016968 Optimization Steps: 53
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1137.9138464927673
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000003----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 3
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 3, victim: 4, Loss: 0.1769, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:229.93, Cost:0.00 best_reg:240.02 avg_loss_reg:229.81:   5%|▍         | 47/1000 [18:30<6:15:25, 23.64s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: all Trigger Size: 240.02048683166504 Optimization Steps: 48
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1116.0000867843628
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000004----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 3.824477434158325
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\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: ['0-1', '1-0']
***Trigger Reverse Engineering開始***
Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.40 avg_loss_reg:45.61:  20%|██        | 200/1000 [06:11<24:47,  1.86s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180
***Symmetric Check開始***
Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10:  68%|██████▊   | 676/1000 [20:52<10:00,  1.85s/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: 1627.9121837615967
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000006----------------------------------------
***Pre-Screening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: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.40 avg_loss_reg:45.61:  20%|██        | 200/1000 [06:49<27:18,  2.05s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180
***Symmetric Check開始***
Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10:  68%|███████    | 676/1000 [22:42<10:53,  2.02s/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: 1775.5744450092316
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000007----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-3', '1-4']
***Trigger Reverse Engineering開始***
Target: 1, victim: 3, Loss: 0.4389, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:85.39, Cost:0.01 best_reg:85.17 avg_loss_reg:84.85: 100%|██████████| 1000/1000 [54:42<00:00,  3.28s/it]
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 3 Trigger Size: 85.17329025268555 Optimization Steps: 982
***Symmetric Check開始***
Target: 3, victim: 1, Loss: 1.2631, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:71.62, Cost:0.02 best_reg:72.47 avg_loss_reg:71.65: 100%|██████████| 1000/1000 [54:41<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: 6572.109435558319
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000008----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['1-3', '3-1']
***Trigger Reverse Engineering開始***
Target: 1, victim: 3, Loss: 0.6401, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:125.66, Cost:0.01 best_reg:126.49 avg_loss_reg:126.49:  29%|███       | 286/1000 [10:57<27:22,  2.30s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: 3 Trigger Size: 125.77005767822266 Optimization Steps: 264
***Symmetric Check開始***
Target: 3, victim: 1, Loss: 0.1343, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:126.84, Cost:0.00 best_reg:127.01 avg_loss_reg:125.80:  27%|███       | 266/1000 [10:12<28:09,  2.30s/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: 1278.0683135986328
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000010----------------------------------------
***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: 0.3445, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:20.12, Cost:0.02 best_reg:20.07 avg_loss_reg:19.87:   8%|▊         | 80/1000 [29:11<5:35:38, 21.89s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 20.0680912733078 Optimization Steps: 81
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1758.829291343689
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000011----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.534503936767578
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\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: ['0-1', '1-0']
***Trigger Reverse Engineering開始***
Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.40 avg_loss_reg:45.61:  20%|██        | 200/1000 [08:02<32:08,  2.41s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180
***Symmetric Check開始***
Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10:  68%|██████████   | 676/1000 [27:01<12:57,  2.40s/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: 2111.062262058258
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000013----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 1
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 1, victim: 4, Loss: 0.4686, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:310.07, Cost:0.00 best_reg:306.49 avg_loss_reg:303.28:  12%|█         | 117/1000 [37:14<4:41:01, 19.10s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 306.49031257629395 Optimization Steps: 118
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 2241.4676427841187
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000014----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 3
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 3, victim: 4, Loss: 1.0423, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:27.11, Cost:0.04 best_reg:27.05 avg_loss_reg:27.35:   7%|▋         | 70/1000 [26:37<5:53:43, 22.82s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: all Trigger Size: 27.04645323753357 Optimization Steps: 71
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1605.182599067688
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000015----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 4, Loss: 0.2567, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:170.54, Cost:0.00 best_reg:172.29 avg_loss_reg:168.89:  10%|▉         | 97/1000 [41:17<6:24:26, 25.54s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 172.29305267333984 Optimization Steps: 98
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 2486.9387426376343
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\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: 3
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 3, victim: 4, Loss: 0.4802, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:42.16, Cost:0.01 best_reg:42.68 avg_loss_reg:42.06:   6%|▌         | 60/1000 [21:19<5:34:11, 21.33s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: all Trigger Size: 42.67514705657959 Optimization Steps: 61
********************檢測結束**********************
檢測結果: Model含有後門(Abnormal)
```

```
整體耗時: 1287.5432851314545
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000017----------
***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: 0.5637, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:786.66, Cost:0.00 best_reg:789.96 avg_loss_reg:778.54:   8%|▊         | 81/1000 [32:06<6:04:13, 23.78s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 789.9558792114258 Optimization Steps: 82
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1934.4419870376587
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\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: ['0-1', '1-0']
***Trigger Reverse Engineering開始***
Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.40 avg_loss_reg:45.61:  20%|██        | 200/1000 [07:53<31:33,  2.37s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180
***Symmetric Check開始***
Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10:  68%|██████▊   | 676/1000 [26:23<12:38,  2.34s/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: 2064.5317862033844
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000020----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 4
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 4, victim: 4, Loss: 0.2084, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:312.59, Cost:0.00 best_reg:308.60 avg_loss_reg:305.98:   4%|▍         | 45/1000 [19:12<6:47:34, 25.61s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: all Trigger Size: 308.6006031036377 Optimization Steps: 46
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1165.4435005187988
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000021----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 8.925481796264648
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000022----------
***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: 0.3501, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:100.11, Cost:0.00 best_reg:102.53 avg_loss_reg:99.75:   4%|▍         | 39/1000 [15:11<6:14:31, 23.38s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 102.53005933761597 Optimization Steps: 40
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 920.4183917045593
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000023----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
```

```
整體耗時: 9.155029296875
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000025----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 4
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 4, victim: 4, Loss: 0.5656, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:1272.69, Cost:0.00 best_reg:1280.96 avg_loss_reg:1282.48:   8%|▉         | 80/1000 [24:13<4:38:32, 18.17s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: all Trigger Size: 1280.9589385986328 Optimization Steps: 81
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1461.3486971855164
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000027----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 4, Loss: 0.5350, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:237.79, Cost:0.00 best_reg:238.41 avg_loss_reg:236.35:  11%|▉         | 107/1000 [43:19<6:01:36, 24.30s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 238.41300296783447 Optimization Steps: 108
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 2614.057455778122
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\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: ['0-1', '1-0']
***Trigger Reverse Engineering開始***
Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.40 avg_loss_reg:45.61:  20%|██        | 200/1000 [07:21<29:26,  2.21s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180
***Symmetric Check開始***
Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10:  68%|██████▊   | 676/1000 [24:43<11:50,  2.19s/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: 1933.565217256546
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\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: ['0-3', '3-0']
***Trigger Reverse Engineering開始***
Target: 3, victim: 0, Loss: 0.6855, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:197.03, Cost:0.00 best_reg:199.56 avg_loss_reg:196.99: 100%|██████████| 1000/1000 [57:13<00:00,  3.43s/it]
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 3 Trigger Size: 173.3273048400879 Optimization Steps: 295
***Symmetric Check開始***
Target: 3, victim: 0, Loss: 1.0507, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:198.34, Cost:0.01 best_reg:198.27 avg_loss_reg:198.48:  18%|▉         | 182/1000 [10:32<47:20,  3.47s/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: 4075.524183988571
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000030----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 1
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 1, victim: 4, Loss: 0.6242, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:120.28, Cost:0.01 best_reg:120.76 avg_loss_reg:120.06:  16%|▊         | 160/1000 [58:28<5:06:58, 21.93s/it]
early stop 所有
```

```
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 120.75566482543945 Optimization Steps: 161
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 3516.8754754066467
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000031----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 1
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 1, victim: 4, Loss: 0.7070, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:1534.29, Cost:0.00 best_reg:1533.19 avg_loss_reg:1514.91:   7%|▋         | 68/1000 [25:50<5:54:06, 22.80s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 1533.194465637207 Optimization Steps: 69
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1558.9308531284332
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000032----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 12.955620527267456
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000033----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 3
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 3, victim: 4, Loss: 0.3419, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:67.53, Cost:0.01 best_reg:69.34 avg_loss_reg:67.33:   6%|▌         | 55/1000 [20:48<5:57:23, 22.69s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: all Trigger Size: 69.34024429321289 Optimization Steps: 56
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1257.139442205429
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000034----------------------------------------
***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: 0.5652, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:33.08, Cost:0.02 best_reg:33.61 avg_loss_reg:33.07:   6%|▌         | 61/1000 [25:55<6:39:08, 25.50s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 33.6125853061676 Optimization Steps: 62
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1565.9251728057861
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\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', '1-0']
***Trigger Reverse Engineering開始***
Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.40 avg_loss_reg:45.61:  20%|██        | 200/1000 [07:59<31:58,  2.40s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180
***Symmetric Check開始***
Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10:  68%|██████▊   | 676/1000 [26:38<12:46,  2.36s/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: 2087.5848660469055
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000036----------------------------------------
```

```
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 4, Loss: 0.4660, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:299.91, Cost:0.00 best_reg:300.23 avg_loss_reg:296.85:  15%|          | 154/1000 [58:06<5:19:10, 22.64s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 300.23338317871094 Optimization Steps: 155
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 3494.8505856990814
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000037----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['0-1', '1-0']
***Trigger Reverse Engineering開始***
Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.40 avg_loss_reg:45.61:  20%|          | 200/1000 [06:12<24:50,  1.86s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180
***Symmetric Check開始***
Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10:  68%|          | 676/1000 [20:56<10:02,  1.86s/it]
early stop 所有
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 1636.7973186969757
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000038----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 13.209598541259766
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\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: ['3-2']
***Trigger Reverse Engineering開始***
Target: 3, victim: 2, Loss: 0.5535, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:368.97, Cost:0.00 best_reg:374.09 avg_loss_reg:374.09:  16%|          | 160/1000 [09:03<47:31,  3.39s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 2 Trigger Size: 370.69390869140625 Optimization Steps: 161
***Symmetric Check開始***
Target: 2, victim: 3, Loss: 0.6408, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:425.79, Cost:0.00 best_reg:425.93 avg_loss_reg:426.09:  20%|          | 203/1000 [11:33<45:23,  3.42s/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: 1246.8177254199982
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\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: ['2-3', '2-4']
***Trigger Reverse Engineering開始***
Target: 2, victim: 3, Loss: 0.1273, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:84.49, Cost:0.00 best_reg:84.10 avg_loss_reg:84.31:  46%|          | 465/1000 [21:30<24:44,  2.78s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 3 Trigger Size: 84.08224678039551 Optimization Steps: 401
***Symmetric Check開始***
Target: 3, victim: 2, Loss: 1.1884, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:155.77, Cost:0.01 best_reg:154.53 avg_loss_reg:156.60: 100%|          | 1000/1000 [46:38<00:00,  2.80s/it]
***Symmetric Check結束***
**********檢測結束**********
檢測結果: Model是安全的(Benign)
整體耗時: 4097.412398338318
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000041----------
***Pre-Screening開始***
```

```
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 2
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 2, victim: 4, Loss: 0.2925, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:278.10, Cost:0.00 best_reg:273.68 avg_loss_reg:272.26:   6%|▌         | 61/1000 [24:23<6:15:33, 24.00s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: all Trigger Size: 273.6800365447998 Optimization Steps: 62
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1473.4870507717133
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000042----------
***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: 0.7136, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:37.36, Cost:0.02 best_reg:37.10 avg_loss_reg:37.26:   9%|▉         | 93/1000 [40:41<6:36:48, 26.25s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: all Trigger Size: 37.10411858558655 Optimization Steps: 94
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 2451.3769154548645
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000043----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 4
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 4, victim: 4, Loss: 0.2573, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:868.37, Cost:0.00 best_reg:865.35 avg_loss_reg:863.21:  13%|█▎        | 127/1000 [54:26<6:14:12, 25.72s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: all Trigger Size: 865.3509826660156 Optimization Steps: 128
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 3276.633634328842
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\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: ['0-2']
***Trigger Reverse Engineering開始***
Target: 0, victim: 2, Loss: 0.8247, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:13.60, Cost:0.06 best_reg:13.47 avg_loss_reg:13.31:  10%|▉         | 102/1000 [05:22<47:17,  3.16s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 2 Trigger Size: 13.468923568725586 Optimization Steps: 103
***Symmetric Check開始***
Target: 2, victim: 0, Loss: 0.6550, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:86.24, Cost:0.01 best_reg:85.58 avg_loss_reg:85.59:  12%|▉         | 118/1000 [06:13<46:32,  3.17s/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: 705.1485214233398
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000045----------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 1
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 1, victim: 4, Loss: 0.2210, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:219.45, Cost:0.00 best_reg:225.20 avg_loss_reg:217.69:   6%|▌         | 64/1000 [25:27<6:12:20, 23.87s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 225.19631671905518 Optimization Steps: 65
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 1537.2975137233734
```

```
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000046----------------------------------------
***Pre-Screening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: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.40 avg_loss_reg:45.61:  20%|██        | 200/1000 [07:09<28:39,  2.15s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180
***Symmetric Check開始***
Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10:  68%|███████   | 676/1000 [24:34<11:46,  2.18s/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: 1913.3076639175415
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\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: 1
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 1, victim: 4, Loss: 0.1751, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:886.30, Cost:0.00 best_reg:872.85 avg_loss_reg:868.04:   5%|▌         | 46/1000 [19:12<6:38:22, 25.05s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 1 Victim Class: all Trigger Size: 872.8489189147949 Optimization Steps: 47
********************檢測結束********************
檢測結果: Model含有後門(Abnormal)
整體耗時: 1162.6434829235077
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000048----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
可能的攻擊方式: Label Specific Backdoor Attack
可能的 target-victim 配對: ['3-2']
***Trigger Reverse Engineering開始***
Target: 3, victim: 2, Loss: 1.2051, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:40.88, Cost:0.03 best_reg:41.30 avg_loss_reg:41.86: 100%|██████████| 1000/1000 [57:06<00:00,  3.43s/it]
***Trigger Reverse Engineering結束***
Target Class: 3 Victim Class: 2 Trigger Size: 41.30317497253418 Optimization Steps: 1000
***Symmetric Check開始***
Target: 2, victim: 3, Loss: 1.1839, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:148.40, Cost:0.01 best_reg:147.60 avg_loss_reg:147.60:  12%|▏         | 115/1000 [06:38<51:03,  3.46s/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: 3834.3740067481995
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\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: ['2-1']
***Trigger Reverse Engineering開始***
Target: 2, victim: 1, Loss: 0.0947, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:199.85, Cost:0.00 best_reg:200.30 avg_loss_reg:198.73:  65%|██████▍   | 648/1000 [26:12<14:14,  2.43s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 2 Victim Class: 1 Trigger Size: 199.5136947631836 Optimization Steps: 649
***Symmetric Check開始***
Target: 1, victim: 2, Loss: 0.2323, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:141.12, Cost:0.00 best_reg:139.82 avg_loss_reg:146.88: 100%|██████████| 1000/1000 [41:15<00:00,  2.48s/it]
***Symmetric Check結束***
********************檢測結束********************
檢測結果: Model是安全的(Benign)
整體耗時: 4058.6572165489197
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000051----------------------------------------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 10.353127717971802
----------------------------------------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000052----------------------------------------
***Pre-Screening開始***
```

```
***Pre-Screening結束***
可能的攻擊方式: Universal Backdoor Attack
可能的 target class: 4
可能的 victim classes: ALL
***Trigger Reverse Engineering開始***
Target: 4, victim: 4, Loss: 0.3230, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:483.68, Cost:0.00 best_reg:484.19 avg_loss_reg:476.90:  12%|▉          | 116/1000 [43:22<5:30:31, 22.43s/it]
early stop 所有
***Trigger Reverse Engineering結束***
Target Class: 4 Victim Class: all Trigger Size: 484.1893997192383 Optimization Steps: 117
**********檢測結束**********
檢測結果: Model含有後門(Abnormal)
整體耗時: 2611.512620449066
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000053----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.647079229354858
----------掃描檔案: D:\UULi\Datasets\TrojAi\Round1\TrainData\models\unzip\id-00000054----------
***Pre-Screening開始***
***Pre-Screening結束***
***檢測結束***
檢測結果: Model是安全的(Benign)
整體耗時: 9.317601680755615

Process finished with exit code 0
```