

```

1 C:\Users\slab\anaconda3\envs\pytorch1\python.exe D:\UULi\test_code\k_arm_test\main.py
2 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-0000000000
3 ***Pre-Screening開始***
4 ***Pre-Screening結束***
5 可能的攻擊方式: Label Specific Backdoor Attack
6 可能的 target-victim 配對: ['0-4', '0-7']
7 ***Trigger Reverse Engineering開始***
8 Target: 0, victim: 7, Loss: 9.1085, Acc: 0.00%, CE_Loss: 9.11, Reg_Loss:2558.18, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2540.18: 3%| | 31/1000 [00:21<11:20, 1.42it/s]
9 ***Trigger Reverse Engineering結束***
10 Target Class: 0 Victim Class: 4 Trigger Size: 1000000000.0 Optimization Steps: 21
11 *****/*****檢測結束*****|
12 檢測結果: Model是安全的(Benign)
13 整體耗時: 32.627202983.6709
14 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-0000000001
15 ***Pre-Screening開始***
16 ***Pre-Screening結束***
17 可能的攻擊方式: Universal Backdoor Attack
18 可能的 target class: 0
19 可能的 victim classes: ALL
20 ***Trigger Reverse Engineering開始***
21 Target: 0, victim: 4, Loss: 2.8775, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:2877.28, Cost:0.00 best_reg:2917.16 avg_loss_reg:2906.83: 16%| | 160/1000 [27:10<2:22:42, 10.19s/it]
22 early stop 所有
23 ***Trigger Reverse Engineering結束***
24 Target Class: 0 Victim Class: all Trigger Size: 2885.2230224609375 Optimization Steps: 161
25 *****/*****檢測結束*****|
26 檢測結果: Model是安全的(Benign)
27 整體耗時: 1643.9113094806671
28 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-0000000002
29 ***Pre-Screening開始***
30 ***Pre-Screening結束***
31 ***檢測結束***|
32 檢測結果: Model是安全的(Benign)
33 整體耗時: 17.549953937530518
34 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-0000000003
35 ***Pre-Screening開始***
36 ***Pre-Screening結束***
37 可能的攻擊方式: Label Specific Backdoor Attack
38 可能的 target-victim 配對: ['0-5', '0-8', '1-6']
39 ***Trigger Reverse Engineering開始***
40 Target: 0, victim: 8, Loss: 2.1476, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:120.41, Cost:0.02 best_reg:121.92 avg_loss_reg:118.75: 13%| | 127/1000 [00:16<01:52, 7.77it/s]
41 early stop 所有
42 ***Trigger Reverse Engineering結束***
43 Target Class: 0 Victim Class: 8 Trigger Size: 120.41090393066406 Optimization Steps: 98
44 ***Symmetric Check開始***
45 Target: 8, victim: 0, Loss: 1.1514, Acc: 90.00%, CE_Loss: 0.51, Reg_Loss:3254.83, Cost:0.00 best_reg:6717.51 avg_loss_reg:3240.99: 100%| | 98/98 [00:12<00:00, 7.90it/s]
46 ***Symmetric Check結束***|
47 ***Pre-Screening開始***
48 檢測結果: Model含有後門(Abnormal)
49 整體耗時: 35.77088284492493
50 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-0000000004
51 ***Pre-Screening開始***
52 ***Pre-Screening結束***
53 可能的攻擊方式: Label Specific Backdoor Attack
54 可能的 target-victim 配對: ['12-14']
55 ***Trigger Reverse Engineering開始***
56 Target: 12, victim: 14, Loss: 8.0868, Acc: 0.00%, CE_Loss: 8.09, Reg_Loss:2543.81, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2532.46: 1%| | 10/1000 [00:01<01:51, 8.90it/s]
57 ***Trigger Reverse Engineering結束***
58 Target Class: 12 Victim Class: 14 Trigger Size: 1000000000.0 Optimization Steps: 11
59 *****/*****檢測結束*****|
60 檢測結果: Model是安全的(Benign)
61 整體耗時: 10.38974905014038
62 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-0000000005
63 ***Pre-Screening開始***
64 ***Pre-Screening結束***
65 可能的攻擊方式: Universal Backdoor Attack
66 可能的 target class: 0
67 可能的 victim classes: ALL
68 ***Trigger Reverse Engineering開始***
69 Target: 0, victim: 12, Loss: 1.7018, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:3809.92, Cost:0.00 best_reg:3799.33 avg_loss_reg:3818.20: 12%| | 115/1000 [13:56<1:47:19, 7.28s/it]
70 early stop 所有
71 ***Trigger Reverse Engineering結束***|

```

```
72 Target Class: 0 Victim Class: all Trigger Size: 3799.326904296875 Optimization Steps: 116
73 *****檢測結束*****
74 檢測結果: Model是安全的(Benign)
75 整體耗時: 848.5646343231201
76 *****Pre-Screening開始*****
77 *****Pre-Screening結束*****
78 可能的攻擊方式: Universal Backdoor Attack
79 可能的 target class: 10
80 可能的 victim classes: ALL
81
82 ***Trigger Reverse Engineering開始*****
83 Target: 10, victim: 12, Loss: 0.3737, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:830.03, Cost:0.00 best_reg:824.60 avg_loss_reg:830.00: 6%| | 65/1000 [02:28<35:35, 2.28s/it]
84 early stop 所有
85 ***Trigger Reverse Engineering結束*****
86 Target Class: all Victim Class: all Trigger Size: 824.5954318576389 Optimization Steps: 66
87 *****檢測結束*****
88 檢測結果: Model含有後門(Abnormal)
89 整體耗時: 157.88350629806519
90 *****掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000006
91 *****Pre-Screening開始*****
92 *****Pre-Screening結束*****
93 可能的攻擊方式: Label Specific Backdoor Attack
94 可能的 target-victim 配對: ['1-20', '9-20']
95 ***Trigger Reverse Engineering開始*****
96 Target: 9, victim: 20, Loss: 1.3081, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:514.91, Cost:0.00 best_reg:516.99 avg_loss_reg:517.99: 32%| | 320/1000 [00:44<01:34, 7.18it/s]
97 early stop 所有
98 ***Trigger Reverse Engineering結束*****
99 Target Class: 9 Victim Class: 20 Trigger Size: 514.91015625 Optimization Steps: 310
100 ***Symmetric Check開始*****
101 Target: 20, victim: 9, Loss: 1.8924, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:5364.59, Cost:0.00 best_reg:5274.17 avg_loss_reg:5359.79: 100%| | 310/310 [00:43<00:00, 7.15it/s]
102 ***Trigger Reverse Engineering結束*****
103 *****檢測結束*****
104 檢測結果: Model含有後門(Abnormal)
105 整體耗時: 99.69884490966797
106 *****掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000008
107 *****Pre-Screening開始*****
108 *****Pre-Screening結束*****
109 *****檢測結束*****
110 檢測結果: Model是安全的(Benign)
111 整體耗時: 20.20454919842871
112 *****檢測結束*****
113 *****Pre-Screening開始*****
114 *****Pre-Screening結束*****
115 可能的攻擊方式: Universal Backdoor Attack
116 可能的 target class: 4
117 可能的 victim classes: ALL
118 ***Trigger Reverse Engineering開始*****
119 Target: 4, victim: 19, Loss: 0.7130, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:93.90, Cost:0.01 best_reg:93.60 avg_loss_reg:93.72: 13%| | 126/1000 [52:39<6:05:16, 25.08s/it]
120 early stop 所有
121 ***Trigger Reverse Engineering結束*****
122 Target Class: 4 Victim Class: all Trigger Size: 93.59891401018415 Optimization Steps: 127
123 *****檢測結束*****
124 檢測結果: Model含有後門(Abnormal)
125 整體耗時: 3175.2218885421753
126 *****掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000010
127 *****Pre-Screening開始*****
128 *****Pre-Screening結束*****
129 *****檢測結束*****
130 檢測結果: Model是安全的(Benign)
131 整體耗時: 12.298462390899658
132 *****檢測結束*****
133 *****Pre-Screening開始*****
134 *****Pre-Screening結束*****
135 *****檢測結束*****
136 檢測結果: Model是安全的(Benign)
137 整體耗時: 11.59020876844604
138 *****檢測結束*****
139 *****Pre-Screening開始*****
140 *****Pre-Screening結束*****
141 *****檢測結束*****
142 檢測結果: Model是安全的(Benign)
```

```
143 整體耗時: 20.46985673904419 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000013-----
144 ***Pre-Screening開始***  
145 可能的攻擊方式: Label Specific Backdoor Attack  
146 可能的 target-victim 配對: [0-15, '2-1', '2-10', '3-4', '4-14', '5-10', '7-1', '7-9', '11-1', '11-10', '11-15', '12-4', '12-14', '15-14', '16-4]  
147 ***Trigger Reverse Engineering開始***  
148 Target: 11, victim: 15, Loss: 1.5402, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss: 124.50, Cost: 0.01 best_reg: 124.67 avg_loss_reg: 124.77: 43%|██████████| 427/1000 [03:05 <04:09, 2.30it/s]  
149 early stop 所有  
150 ***Trigger Reverse Engineering結束***  
151 Target Class: 11 Victim Class: 15 Trigger Size: 124.50299835205078 Optimization Steps: 127  
152 ***Symmetric Check開始***  
153 Target: 15, victim: 11 Loss: 7.2660, Acc: 80.00%, CE_Loss: 0.75, Reg_Loss: 9769.91, Cost: 0.00 best_reg: 15144.27 avg_loss_reg: 10184.31: 100%|██████████| 127/127 [00:46 <00:00, 2.71it/s]  
154 ***Symmetric Check結束***  
155 Target Class: 11 Victim Class: 15 Trigger Size: 124.50299835205078 Optimization Steps: 127  
156 ***Symmetric Check開始***  
157 ***Symmetric Check結束***  
158 檢測結果: Model含有後門(Abnormal)  
159 整體耗時: 241.6618514060974 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000014-----
160 ***Pre-Screening開始***  
161 整體耗時: 11.132597923278809 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000015-----
162 ***Pre-Screening結束***  
163 ***檢測結束***  
164 檢測結果: Model是安全的(Benign)  
165 整體耗時: 11.132597923278809 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000016-----
166 ***Pre-Screening開始***  
167 整體耗時: 8.272382497787476 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000016-----
168 ***Pre-Screening結束***  
169 ***檢測結束***  
170 檢測結果: Model是安全的(Benign)  
171 整體耗時: 8.272382497787476 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000017-----
172 ***Pre-Screening開始***  
173 整體耗時: 17.52834439277649 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000017-----
174 ***Pre-Screening結束***  
175 ***檢測結束***  
176 檢測結果: Model是安全的(Benign)  
177 整體耗時: 16.901154279708862 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000018-----
178 ***Pre-Screening開始***  
179 整體耗時: 8.8101508671740112 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000018-----
180 ***Pre-Screening結束***  
181 ***檢測結束***  
182 檢測結果: Model是安全的(Benign)  
183 整體耗時: 8.8101508671740112 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000019-----
184 ***Pre-Screening開始***  
185 整體耗時: 16.901154279708862 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000019-----
186 ***Pre-Screening結束***  
187 ***檢測結束***  
188 檢測結果: Model是安全的(Benign)  
189 整體耗時: 16.901154279708862 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000020-----
190 ***Pre-Screening開始***  
191 整體耗時: 3.6919925212860107 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000021-----
192 ***Pre-Screening結束***  
193 ***檢測結束***  
194 檢測結果: Model是安全的(Benign)  
195 整體耗時: 16.05219841003418 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000020-----
196 ***Pre-Screening開始***  
197 整體耗時: 3.6919925212860107 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000021-----
198 ***Pre-Screening結束***  
199 ***檢測結束***  
200 檢測結果: Model是安全的(Benign)  
201 整體耗時: 3.6919925212860107 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000021-----
202 ***Pre-Screening開始***  
203 整體耗時: 3.6919925212860107 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000021-----
204 ***Pre-Screening結束***  
205 ***檢測結束***  
206 檢測結果: Model是安全的(Benign)  
207 整體耗時: 12.595725774765015 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000022-----
208 ***Pre-Screening開始***  
209 ***Pre-Screening結束***  
210 可能的攻擊方式: Label Specific Backdoor Attack  
211 可能的 target-victim 配對: [0-11, '1-6', '1-7', '1-9, '2-0', '2-10', '3-11, '5-6', '5-8', '6-5', '7-1', '7-8', '9-3', '10-2]  
212 可能的 target-victim 配對: [0-11, '1-6', '1-7', '1-9, '2-0', '2-10', '3-11, '5-6', '5-8', '6-5', '7-1', '7-8', '9-3', '10-2]  
213 ***Trigger Reverse Engineering開始***
```

```

214 Target: 5, victim: 6, Loss: 2.3234, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:54.84, Cost:0.04 best_reg:54.97 avg_loss_reg:54.97: 27% | 266/1000 [00:19<00:54, 13.57it/s]
215 early stop 所有
216 ***Trigger Reverse Engineering結束***+
217 Target Class: 5 Victim Class: 6 Trigger Size: 54.83860778808594 Optimization Steps: 103
218 ***Symmetric Check開始***+
219 Target: 6, victim: 5, Loss: 1.6170, Acc: 90.00%, CE_Loss: 0.32, Reg_Loss:1945.85, Cost:0.00 best_reg:2060.69 avg_loss_reg:1978.39: 100% | 103/103 [00:07<00:00, 13.40it/s]
220 ***Symmetric Check結束***+
221 *****檢測結束*****+
222 檢測結果: Model含有後門(Abnormal)
223 整體耗時: 33.65658688545227
224 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000023-----
225 ***Pre-Screening開始***+
226 ***Pre-Screening結束***+
227 可能的攻擊方式: Label Specific Backdoor Attack
228 可能的 target-victim 配對: ['3-8', '9-6', '12-1', '12-8', '13-0']
229 ***Trigger Reverse Engineering開始***+
230 Target: 12, victim: 8, Loss: 1.3848, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:389.15, Cost:0.00 best_reg:390.60 avg_loss_reg:387.86: 34% | 340/1000 [01:19<02:34, 4.28it/s]
231 early stop 所有
232 ***Trigger Reverse Engineering結束***+
233 Target Class: 12 Victim Class: 8 Trigger Size: 389.1537170410156 Optimization Steps: 201
234 ***Symmetric Check開始***+
235 Target: 8, victim: 12, Loss: 1.8964, Acc: 95.00%, CE_Loss: 0.25, Reg_Loss:371.250, Cost:0.00 best_reg:4129.94 avg_loss_reg:3708.70: 100% | 201/201 [00:46<00:00, 4.30it/s]
236 ***Symmetric Check結束***+
237 *****檢測結束*****+
238 檢測結果: Model含有後門(Abnormal)
239 整體耗時: 136.11167430877686
240 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000024-----
241 ***Pre-Screening開始***+
242 ***Pre-Screening結束***+
243 可能的攻擊方式: Label Specific Backdoor Attack
244 可能的 target-victim 配對: ['8-5', '8-9']
245 ***Trigger Reverse Engineering開始***+
246 Target: 8, victim: 9, Loss: 13.2254, Acc: 0.00%, CE_Loss: 13.23, Reg_Loss:2587.64, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2561.44: 2% | 21/1000 [01:16<59:13, 3.63s/it]
247 ***Trigger Reverse Engineering結束***+
248 Target Class: 8 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
249 *****檢測結束*****+
250 檢測結果: Model是安全的(Benign)
251 整體耗時: 92.06118702888489
252 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000025-----
253 ***Pre-Screening開始***+
254 ***Pre-Screening結束***+
255 *****檢測結束*****+
256 檢測結果: Model是安全的(Benign)
257 整體耗時: 6.430930852890015
258 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000026-----
259 ***Pre-Screening開始***+
260 ***Pre-Screening結束***+
261 可能的攻擊方式: Label Specific Backdoor Attack
262 可能的 target-victim 配對: ['9-10', '9-16', '11-16']
263 ***Trigger Reverse Engineering開始***+
264 Target: 11, victim: 16, Loss: 6.6376, Acc: 0.00%, CE_Loss: 6.64, Reg_Loss:2525.99, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2518.81: 3% | 32/1000 [00:03<01:57, 8.21it/s]
265 ***Trigger Reverse Engineering結束***+
266 Target Class: 9 Victim Class: 10 Trigger Size: 10000000000.0 Optimization Steps: 11
267 *****檢測結束*****+
268 檢測結果: Model是安全的(Benign)
269 整體耗時: 11.79649543762207
270 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000027-----
271 ***Pre-Screening開始***+
272 ***Pre-Screening結束***+
273 可能的攻擊方式: Universal Backdoor Attack
274 可能的 target class: 6
275 可能的 victim classes: ALL
276 ***Trigger Reverse Engineering開始***+
277 Target: 6, victim: 19, Loss: 0.7005, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:1043.19, Cost:0.00 best_reg:1035.95 avg_loss_reg:1048.86: 6% | 61/1000 [32:39<8:22:36, 32.12s/it]
278 early stop 所有
279 ***Trigger Reverse Engineering結束***+
280 Target Class: all 1 Victim Class: 1035.9530290876116 Optimization Steps: 62
281 *****檢測結束*****+
282 檢測結果: Model含有後門(Abnormal)
283 整體耗時: 1979.93223785305023
284 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000028-----

```

```

285 ***Pre-Screening開始****
286 ***Pre-Screening結束****
287 可能的攻擊方式: Label Specific Backdoor Attack
288 可能的 target-victim 配對: [2-8]
289 ***Trigger Reverse Engineering 開始****
290 Target: 2, victim: 8, Loss: 4.8791, Acc: 0.00%, CE_Loss: 4.88, Reg_Loss:2577.06, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2559.87: 1%| | 10/1000 [00:30<50:21, 3.05s/it]
291 ***Trigger Reverse Engineering 結束****
292 Target Class: 2 Victim Class: 8 Trigger Size: 1000000000.0 Optimization Steps: 11
293 *****檢測結束*****檢測結束*****
294 檢測結果: Model是安全的(Benign)
295 整體耗時: 45.83541822433472
296 -----掃描檔案: D:\UU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000029-----
297 ***Pre-Screening開始****
298 ***Pre-Screening結束****
299 可能的攻擊方式: Label Specific Backdoor Attack
300 可能的 target-victim 配對: ['8-2', '8-6']
301 ***Trigger Reverse Engineering 開始****
302 Target: 8, victim: 6, Loss: 13.5948, Acc: 0.00%, CE_Loss: 13.59, Reg_Loss:2591.59, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2569.47: 3%| | 31/1000 [00:03<01:59, 8.11it/s]
303 ***Trigger Reverse Engineering 結束****
304 Target Class: 8 Victim Class: 2 Trigger Size: 1000000000.0 Optimization Steps: 21
305 *****檢測結束*****檢測結束*****
306 檢測結果: Model是安全的(Benign)
307 整體耗時: 10.320770502090454
308 -----掃描檔案: D:\UU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000030-----
309 ***Pre-Screening開始****
310 ***Pre-Screening結束****
311 可能的攻擊方式: Label Specific Backdoor Attack
312 可能的 target-victim 配對: ['1-3', '1-5', '4-1']
313 ***Trigger Reverse Engineering 開始****
314 Target: 4, victim: 1, Loss: 8.2156, Acc: 0.00%, CE_Loss: 8.22, Reg_Loss:2585.05, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2565.52: 3%| | 32/1000 [00:08<04:28, 3.60it/s]
315 ***Trigger Reverse Engineering 結束****
316 Target Class: 1 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 11
317 *****檢測結束*****檢測結束*****
318 檢測結果: Model是安全的(Benign)
319 整體耗時: 17.18355250358515
320 -----掃描檔案: D:\UU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000031-----
321 ***Pre-Screening開始****
322 ***Pre-Screening結束****
323 可能的攻擊方式: Label Specific Backdoor Attack
324 可能的 target-victim 配對: ['1-0', '3-4', '4-3']
325 ***Trigger Reverse Engineering 開始****
326 Target: 4, victim: 3, Loss: 0.4180, Acc: 95.00%, CE_Loss: 0.08, Reg_Loss:1734.67, Cost:0.00 best_reg:1736.45 avg_loss_reg:1733.61: 100%| | 1000/1000 [34:22<00:00, 2.06s/it]
327 ***Trigger Reverse Engineering 結束****
328 Target Class: 4 Victim Class: 3 Trigger Size: 1736.4454345703125 Optimization Steps: 978
329 *****檢測結束*****檢測結束*****
330 檢測結果: Model是安全的(Benign)
331 整體耗時: 2072.59046626091
332 -----掃描檔案: D:\UU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000032-----
333 ***Pre-Screening開始****
334 ***Pre-Screening結束****
335 可能的攻擊方式: Label Specific Backdoor Attack
336 可能的 target-victim 配對: ['2-4', '2-8', '8-4']
337 ***Trigger Reverse Engineering 開始****
338 Target: 2, victim: 4, Loss: 1.6283, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:91.62, Cost:0.02 best_reg:92.03 avg_loss_reg:92.03: 12%| | 122/1000 [02:00<14:30, 1.01it/s]
339 early stop 所有
340 ***Trigger Reverse Engineering 結束****
341 Target Class: 2 Victim Class: 4 Trigger Size: 91.61526489257812 Optimization Steps: 96
342 ***Symmetric Check開始****
343 Target: 4, victim: 2, Loss: 1.5548, Acc: 90.00%, CE_Loss: 0.49, Reg_Loss:1069.46, Cost:0.00 best_reg:1111.77 avg_loss_reg:1088.98: 100%| | 96/96 [01:33<00:00, 1.03it/s]
344 ***Symmetric Check結束****
345 *****檢測結束*****檢測結束*****
346 檢測結果: Model含有後門(Abnormal)
347 整體耗時: 227.4209806919098
348 -----掃描檔案: D:\UU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000033-----
349 ***Pre-Screening開始****
350 ***Pre-Screening結束****
351 ***檢測結束****
352 檢測結果: Model是安全的(Benign)
353 整體耗時: 12.049734830856323
354 -----掃描檔案: D:\UU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000034-----
355 ***Pre-Screening開始****

```

```
356 ***Pre-Screening結束***  
357 ***檢測結束***  
358 檢測結果: Model是安全的(Benign)  
359 整體耗時: 7.609855651855469  
360 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000035-----  
361 ***Pre-Screening開始***  
362 ***Pre-Screening結束***  
363 ***檢測結束***  
364 檢測結果: Model是安全的(Benign)  
365 整體耗時: 8.713872909545898  
366 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000036-----  
367 ***Pre-Screening開始***  
368 ***Pre-Screening結束***  
369 可能的攻擊方式: Label Specific Backdoor Attack  
370 可能的 target-victim 配對: ['1-8', '2-9', '3-4', '3-6', '4-7', '5-7', '6-7', '8-1', '8-10', '8-11', '9-2', '9-6', '10-1', '10-8', '10-14', '13-11', '14-0', '14-13', '15-14']  
371 ***Trigger Reverse Engineering開始***  
372 Target: 15, victim: 14, Loss: 14.4300, Acc: 0.00%, CE_Loss: 14.43, Reg_Loss:2586.78, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2565.79: 25% | 248/1000 [18:33<56:17, 4.49s/it]  
373 ***Trigger Reverse Engineering結束***  
374 Target Class: 1 Victim Class: 8 Trigger Size: 1000000000.0 Optimization Steps: 11  
375 *****檢測結束*****  
376 檢測結果: Model是安全的(Benign)  
377 整體耗時: 1140.3475620746613  
378 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000037-----  
379 ***Pre-Screening開始***  
380 ***Pre-Screening結束***  
381 可能的攻擊方式: Label Specific Backdoor Attack  
382 可能的 target-victim 配對: ['10-13', '14-4']  
383 ***Trigger Reverse Engineering開始***  
384 Target: 14, victim: 4, Loss: 3.1206, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:120.69, Cost:0.03 best_reg:122.70 avg_loss_reg:122.70: 10% | 104/1000 [00:33<04:44, 3.14it/s]  
385 early stop 所有  
386 ***Trigger Reverse Engineering結束***  
387 Target Class: 14 Victim Class: 4 Trigger Size: 120.689697265625 Optimization Steps: 84  
388 ***Symmetric Check開始***  
389 Target: 4, victim: 14, Loss: 1.8288, Acc: 0.00%, CE_Loss: 1.83, Reg_Loss:17365.15, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:17288.30: 100% | 84/84 [00:26<00:00, 3.21it/s]  
390 ***Symmetric Check結束***  
391 *****檢測結束*****  
392 檢測結果: Model含有後門(Abnormal)  
393 整體耗時: 69.78644633293152  
394 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000038-----  
395 ***Pre-Screening開始***  
396 ***Pre-Screening結束***  
397 ***檢測結束***  
398 檢測結果: Model是安全的(Benign)  
399 整體耗時: 16.580349445343018  
400 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000039-----  
401 ***Pre-Screening開始***  
402 ***Pre-Screening結束***  
403 可能的攻擊方式: Label Specific Backdoor Attack  
404 可能的 target-victim 配對: ['1-2', '1-5', '8-5', '12-5']  
405 ***Trigger Reverse Engineering開始***  
406 Target: 12, victim: 5, Loss: 10.9263, Acc: 0.00%, CE_Loss: 10.93, Reg_Loss:2546.80, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2534.95: 4% | 143/1000 [00:03<01:09, 13.70it/s]  
407 ***Trigger Reverse Engineering結束***  
408 Target Class: 1 Victim Class: 2 Trigger Size: 1000000000.0 Optimization Steps: 11  
409 *****檢測結束*****  
410 檢測結果: Model是安全的(Benign)  
411 整體耗時: 11.188262224197388  
412 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000040-----  
413 ***Pre-Screening開始***  
414 ***Pre-Screening結束***  
415 可能的攻擊方式: Universal Backdoor Attack  
416 可能的 target class: ALL  
417 可能的 victim classes: ALL  
418 ***Trigger Reverse Engineering開始***  
419 Target: 2, victim: 9, Loss: 0.2163, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:96.13, Cost:0.00 best_reg:116.95 avg_loss_reg:96.81: 10% | 104/1000 [09:36<1:22:45, 5.54s/it]  
420 early stop 所有  
421 ***Trigger Reverse Engineering結束***  
422 Target Class: 2 Victim Class: all 1 Trigger Size: 116.95089530944824 Optimization Steps: 105  
423 *****檢測結束*****  
424 檢測結果: Model含有後門(Abnormal)  
425 整體耗時: 586.144577980415  
426 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000041-----
```

```
427 ***Pre-Screening開始***  
428 ***Pre-Screening結束***  
429 可能的攻擊方式: Label Specific Backdoor Attack  
430 可能的 target-victim 配對: [0-20, '7-11', '8-1', '8-7', '8-11', '10-0', '10-9', '12-9', '13-1', '13-3', '13-19', '14-5', '14-9', '15-7', '17-19', '20-0]  
431 ***Trigger Reverse Engineering 開始***  
432 Target: 20, victim: 0, Loss: 1.2312, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss: 695.26, Cost: 0.00 best_Reg: 697.03 avg_Loss_Reg: 699.13: 60% | ██████████ | 599/1000 [02:26<01:37, 4.09it/s]  
433 early stop 所有  
434 ***Trigger Reverse Engineering 結束***  
435 Target Class: 20 Victim Class: 0 Trigger Size: 695.2594604492188 Optimization Steps: 279  
436 ***Symmetric Check開始***  
437 Target: 0, victim: 20, Loss: 0.6636, Acc: 95.00%, CE_Loss: 0.27, Reg_Loss: 1316.27, Cost: 0.00 best_Reg: 1335.39 avg_Loss_Reg: 1313.22: 100% | ██████████ | 279/279 [01:07<00:00, 4.13it/s]  
438 ***Symmetric Check結束***  
439 ***檢測結果: Model是安全的(Benign)  
440 整體耗時: 226.33615922972856  
441  
442 -----掃描檔案: D:\UUULi\Datasets\TroiAI\Round3\TrainData\models\unzip\id-00000042-----  
443 ***Pre-Screening 開始***  
444 ***Pre-Screening 結束***  
445 可能的攻擊方式: Label Specific Backdoor Attack  
446 可能的 target-victim 配對: ['4-9', '4-10', '11-10']  
447 ***Trigger Reverse Engineering 開始***  
448 Target: 4, victim: 10, Loss: 1.9583, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss: 33.41, Cost: 0.06 best_Reg: 34.13 avg_Loss_Reg: 34.13: 11% | █████ | 110/1000 [06:21<51:27, 3.47s/it]  
449 early stop 所有  
450 ***Trigger Reverse Engineering 結束***  
451 Target Class: 4 Victim Class: 10 Trigger Size: 33.41248321533203 Optimization Steps: 69  
452 ***Symmetric Check開始***  
453 Target: 10, victim: 4, Loss: 0.7188, Acc: 65.00%, CE_Loss: 0.72, Reg_Loss: 12533.46, Cost: 0.00 best_Reg: 10000000000.00 avg_Loss_Reg: 12407.27: 100% | ██████████ | 69/69 [03:53<00:00, 3.39s/it]  
454 ***Symmetric Check結束***  
455 ***檢測結果: Model含有後門(Abnormal)  
456 檢測結果: Model是安全的(Benign)  
457 整體耗時: 631.8594088554382  
458 -----掃描檔案: D:\UUULi\Datasets\TroiAI\Round3\TrainData\models\unzip\id-00000043-----  
459 ***Pre-Screening 結束***  
460 ***Pre-Screening 開始***  
461 ***檢測結果: Model是安全的(Benign)  
462 檢測結果: Model是安全的(Benign)  
463 整體耗時: 12.047940492630005  
464  
465 ***Pre-Screening 開始***  
466 ***Pre-Screening 結束***  
467 可能的攻擊方式: Label Specific Backdoor Attack  
468 可能的 target-victim 配對: ['0-6']  
469 ***Trigger Reverse Engineering 開始***  
470 Target: 0, victim: 6, Loss: 2.0927, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss: 895.77, Cost: 0.00 best_Reg: 898.52 avg_Loss_Reg: 898.52: 25% | █████ | 246/1000 [01:18<04:02, 3.11it/s]  
471 early stop 所有  
472 ***Trigger Reverse Engineering 結束***  
473 Target Class: 0 Victim Class: 6 Trigger Size: 895.7700805664062 Optimization Steps: 247  
474 ***Symmetric Check開始***  
475 Target: 6, victim: 0, Loss: 0.4522, Acc: 95.00%, CE_Loss: 0.08, Reg_Loss: 833.02, Cost: 0.00 best_Reg: 844.83 avg_Loss_Reg: 832.32: 100% | ██████████ | 247/247 [01:19<00:00, 3.10it/s]  
476 ***Symmetric Check結束***  
477 ***檢測結果: Model是安全的(Benign)  
478 檢測結果: Model是安全的(Benign)  
479 整體耗時: 165.35660219192505  
480 -----掃描檔案: D:\UUULi\Datasets\TroiAI\Round3\TrainData\models\unzip\id-00000045-----  
481 ***Pre-Screening 開始***  
482 ***Pre-Screening 結束***  
483 ***檢測結果: Model是安全的(Benign)  
484 檢測結果: Model是安全的(Benign)  
485 整體耗時: 17.712972164154053  
486  
487 ***Pre-Screening 開始***  
488 ***Pre-Screening 結束***  
489 ***檢測結果: Model是安全的(Benign)  
490 檢測結果: Model是安全的(Benign)  
491 整體耗時: 6.463090419769287  
492 -----掃描檔案: D:\UUULi\Datasets\TroiAI\Round3\TrainData\models\unzip\id-00000047-----  
493 ***Pre-Screening 開始***  
494 ***Pre-Screening 結束***  
495 ***檢測結果: Model是安全的(Benign)  
496 檢測結果: Model是安全的(Benign)  
497 整體耗時: 6.469682455062866
```

```

File - main
498 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000048
499 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000049
500 可能的攻擊方式: Label Specific Backdoor Attack
501 可能的 target-victim 配對: ['5-7']
502 ***Trigger Reverse Engineering 開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000050
503 Target: 5, victim: 7, Loss: 2.7606, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:101.61, Cost:0.03 best_reg:101.66 avg_loss_reg:101.66: 10% | 102/1000 [01:27<12:48, 1.17it/s]
504 Target Class: 5 Victim Class: 7 Trigger Size: 101.61225128173828 Optimization Steps: 103
505 early stop 所有
506 ***Trigger Reverse Engineering 結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000051
507 Target Class: 5 Victim Class: 7 Trigger Size: 101.61225128173828 Optimization Steps: 103
508 Target: 7, victim: 5, Loss: 2.2136, Acc: 80.00%, CE_Loss: 0.37, Reg_Loss:2766.08, Cost:0.00 best_reg:3081.28 avg_loss_reg:2768.00: 100% | 103/103 [01:27<00:00, 1.18it/s]
509 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000052
510 ***Symmetric Check結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000053
511 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000054
512 檢測結果: Model含有後門(Abnormal)
513 整體耗時: 186.492008388606567-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000049
514 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000055
515 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000056
516 可能的攻擊方式: Label Specific Backdoor Attack
517 可能的 target-victim 配對: ['3-2', '6-1']
518 ***Trigger Reverse Engineering 開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000057
519 Target: 6, victim: 1, Loss: 1.9192, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:106.27, Cost:0.02 best_reg:106.95 avg_loss_reg:106.95: 10% | 99/1000 [00:07<01:05, 13.74it/s]
520 Target Class: 6 Victim Class: 1 Trigger Size: 106.26641845703125 Optimization Steps: 79
521 early stop 所有
522 ***Trigger Reverse Engineering 結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000058
523 Target Class: 6 Victim Class: 1 Trigger Size: 106.26641845703125 Optimization Steps: 79
524 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000059
525 Target: 1, victim: 6, Loss: 1.6441, Acc: 40.00%, CE_Loss: 1.64, Reg_Loss:17481.23, Cost:0.00 best_reg:17302.98: 100% | 79/79 [00:05<00:00, 13.43it/s]
526 ***Symmetric Check結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000060
527 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000061
528 檢測結果: Model含有後門(Abnormal)
529 整體耗時: 19.07635188102722-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000050
530 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000062
531 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000063
532 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000064
533 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000065
534 檢測結果: Model是安全的(Benign)
535 整體耗時: 7.91306684013672-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000066
536 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000067
537 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000068
538 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000069
539 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000070
540 檢測結果: Model是安全的(Benign)
541 整體耗時: 9.256797313690186-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000071
542 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000072
543 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000073
544 可能的攻擊方式: Label Specific Backdoor Attack
545 可能的 target-victim 配對: ['2-4', '2-6']
546 可能的 target-victim 配對: ['2-4', '2-6']
547 ***Trigger Reverse Engineering 開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000074
548 Target: 2, victim: 6, Loss: 1.5610, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:26.97, Cost:0.06 best_reg:27.69 avg_loss_reg:27.69: 9% | 89/1000 [00:21<03:41, 4.12it/s]
549 early stop 所有
550 ***Trigger Reverse Engineering 結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000075
551 Target Class: 2 Victim Class: 6 Trigger Size: 26.973079681396484 Optimization Steps: 79
552 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000076
553 Target: 6, victim: 2, Loss: 1.1480, Acc: 50.00%, CE_Loss: 1.15, Reg_Loss:16848.31, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:16727.95: 100% | 79/79 [00:19<00:00, 4.15it/s]
554 ***Symmetric Check結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000077
555 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000078
556 檢測結果: Model含有後門(Abnormal)
557 整體耗時: 47.6233868598938-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000079
558 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000080
559 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000081
560 可能的攻擊方式: Universal Backdoor Attack
561 可能的 target class: 1
562 可能的 victim classes: ALL
563 可能的 victim classes: ALL
564 ***Trigger Reverse Engineering 開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000082
565 Target: 1, victim: 22, Loss: 1.4065, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:10502.64, Cost:0.00 best_reg:10413.47 avg_loss_reg:10432.45: 16% | 165/1000 [1:07:33<5:41:52, 24.57it/s]
566 early stop 所有
567 ***Trigger Reverse Engineering 結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000083
568 Target Class: 1 Victim Class: all Trigger Size: 10413.472778320312 Optimization Steps: 166

```

```
569 *****檢測結束*****  
570 檢測結果: Model是安全的(Benign) | 100/1000 [00:02<02:06, 7.77it/s]  
571 整體耗時: 4068.8110830783844  
572 *****Pre-Screening開始*****  
573 *****Pre-Screening結束*****  
574 *****Pre-Screening結束*****  
575 *****檢測結束*****  
576 檢測結果: Model是安全的(Benign)  
577 整體耗時: 14.109715700149536  
578 *****Pre-Screening開始*****  
579 *****Pre-Screening結束*****  
580 可能的攻擊方式: Label Specific Backdoor Attack  
581 可能的 target-victim 配對: ['14-12']  
582 ***Trigger Reverse Engineering開始***  
583 Target: 14, victim: 12, Loss: 7.5283, Acc: 10.00%, CE_Loss: 7.53, Reg_Loss:2715.90, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2680.33: 2%| | 20/1000 [00:02<02:06, 7.77it/s]  
584 Target Class: 14 Victim Class: 12 Trigger Size: 1000000000.0 Optimization Steps: 21  
585 ***Trigger Reverse Engineering結束***  
586 Target Class: 14 Victim Class: 12 Trigger Size: 1000000000.0 Optimization Steps: 21  
587 *****檢測結束*****  
588 檢測結果: Model是安全的(Benign)  
589 整體耗時: 14.2777221441268921  
590 *****Pre-Screening開始*****  
591 *****Pre-Screening結束*****  
592 可能的攻擊方式: Label Specific Backdoor Attack  
593 可能的 target-victim 配對: ['1-7', '1-8', '1-16', '2-11', '6-10', '7-8', '16-7']  
594 ***Trigger Reverse Engineering開始***  
595 Target: 1, victim: 8, Loss: 2.2877, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:2028.92, Cost:0.00 best_reg:2031.48 avg_loss_reg:2031.48: 32%| | 325/1000 [00:39<01:22, 8.22it/s]  
596 Target stop 所有  
597 early stop 所有  
598 ***Trigger Reverse Engineering結束***  
599 Target Class: 8 Victim Class: 8 Trigger Size: 2028.91552734375 Optimization Steps: 239  
600 *****檢測結束*****  
601 檢測結果: Model是安全的(Benign)  
602 整體耗時: 47.49352955818176  
603 *****Pre-Screening開始*****  
604 *****Pre-Screening結束*****  
605 可能的攻擊方式: Label Specific Backdoor Attack  
606 可能的 target-victim 配對: ['10-1']  
607 ***Trigger Reverse Engineering開始***  
608 Target: 10, victim: 1, Loss: 13.6979, Acc: 0.00%, CE_Loss: 13.70, Reg_Loss:2543.86, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2533.13: 1%| | 10/1000 [00:01<02:33, 6.46it/s]  
609 Target Class: 10 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11  
610 ***Trigger Reverse Engineering結束***  
611 Target Class: 10 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11  
612 *****檢測結束*****  
613 檢測結果: Model是安全的(Benign)  
614 整體耗時: 11.388310194015503  
615 *****Pre-Screening開始*****  
616 *****Pre-Screening結束*****  
617 可能的攻擊方式: Label Specific Backdoor Attack  
618 可能的 target-victim 配對: ['8-1', '11-15', '17-4', '18-1']  
619 ***Trigger Reverse Engineering開始***  
620 Target: 18, victim: 1, Loss: 8.3917, Acc: 0.00%, CE_Loss: 8.39, Reg_Loss:2490.44, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2492.27: 6%| | 63/1000 [00:15<03:53, 4.02it/s]  
621 Target Class: 8 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 21  
622 ***Trigger Reverse Engineering結束***  
623 Target Class: 8 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 21  
624 *****檢測結束*****  
625 檢測結果: Model是安全的(Benign)  
626 整體耗時: 28.06581687927246  
627 *****Pre-Screening開始*****  
628 *****Pre-Screening結束*****  
629 *****Pre-Screening結束*****  
630 *****檢測結束*****  
631 檢測結果: Model是安全的(Benign)  
632 整體耗時: 14.115655389047852  
633 *****Pre-Screening開始*****  
634 *****Pre-Screening結束*****  
635 可能的攻擊方式: Label Specific Backdoor Attack  
636 可能的 target-victim 配對: ['2-9', '6-1', '6-2', '6-9', '9-2']  
637 ***Trigger Reverse Engineering開始***  
638 Target: 9, victim: 2, Loss: 9.5228, Acc: 10.00%, CE_Loss: 9.52, Reg_Loss:3092.37, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2998.41: 9%| | 94/1000 [05:06<49:15, 3.26s/it]  
639 Target Class: 9 Victim Class: 2 Trigger Size: 1000000000.0 Optimization Steps: 21  
*****檢測結束*****  
Page 9 of 67
```

```

640 ***Trigger Reverse Engineering 結束***  

641 Target Class: 2 Victim Class: 9 Trigger Size: 1000000000.0 Optimization Steps: 21  

642 *****檢測結束*****  

643 檢測結果: Model是安全的(Benign)  

644 整體耗時: 324.40434288978577  

645 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000061-----  

646 ***Pre-Screening開始***  

647 可能的攻擊方式: Label Specific Backdoor Attack  

648 可能的 target-victim 配對: [0-12, '2-6', '3-12', '12-0', '12-3']  

649 ***Trigger Reverse Engineering 開始***  

650 Target: 12, victim: 3, Loss: 1.2220, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:227.29, Cost:0.01 best_Reg:228.85 avg_Loss_Reg:230.24: 28%|████| 178/1000 [00:34<01:30, 8.01it/s]  

651 Target stop 所有  

652 early stop 所有  

653 ***Trigger Reverse Engineering 結束***  

654 Target Class: 12 Victim Class: 3 Trigger Size: 227.2919158935547 Optimization Steps: 178  

655 ***Symmetric Check開始***  

656 Target: 3, victim: 12, Loss: 1.5988, Acc: 95.00%, CE_Loss: 0.30, Reg_Loss:578.02, Cost:0.00 best_Reg:591.45 avg_Loss_Reg:574.87: 100%|████| 178/178 [00:22<00:00, 8.05it/s]  

657 ***Symmetric Check結束***  

658 *****檢測結束*****  

659 檢測結果: Model是安全的(Benign)  

660 整體耗時: 66.93280124664307  

661 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000062-----  

662 ***Pre-Screening開始***  

663 ***Pre-Screening 結束***  

664 可能的攻擊方式: Label Specific Backdoor Attack  

665 可能的 target-victim 配對: ['1-2', '1-22', '2-1', '2-23', '3-14', '3-15', '3-23', '4-8', '5-8', '6-8', '10-8', '14-2', '15-3', '15-14', '17-15', '18-12', '21-15', '21-19', '21-22', '22-1']  

666 ***Trigger Reverse Engineering 開始***  

667 Target: 22, victim: 1, Loss: 1.3573, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:334.49, Cost:0.00 best_Reg:334.99 avg_Loss_Reg:335.30: 46%|████| 459/1000 [00:43<00:51, 10.57it/s]  

668 early stop 所有  

669 ***Trigger Reverse Engineering 結束***  

670 Target Class: 22 Victim Class: 1 Trigger Size: 334.48626708984375 Optimization Steps: 163  

671 ***Symmetric Check開始***  

672 Target: 1, victim: 22, Loss: 1.9003, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:728.96, Cost:0.00 best_Reg:720.74 avg_Loss_Reg:726.78: 100%|████| 163/163 [00:15<00:00, 10.64it/s]  

673 ***Symmetric Check結束***  

674 *****檢測結束*****  

675 檢測結果: Model是安全的(Benign)  

676 整體耗時: 67.13302826881409  

677 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000063-----  

678 ***Pre-Screening開始***  

679 ***Pre-Screening 結束***  

680 可能的攻擊方式: Label Specific Backdoor Attack  

681 可能的 target-victim 配對: ['2-1', '5-3']  

682 ***Trigger Reverse Engineering 開始***  

683 Target: 5, victim: 3, Loss: 12.4081, Acc: 0.00%, CE_Loss: 12.41, Reg_Loss:2550.73, Cost:0.00 best_Reg:10000000000.00 avg_Loss_Reg:2538.93: 2%|████| 121/1000 [00:02<01:48, 9.06it/s]  

684 ***Trigger Reverse Engineering 結束***  

685 Target Class: 2 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11  

686 *****檢測結束*****  

687 檢測結果: Model是安全的(Benign)  

688 整體耗時: 8.242540121078491  

689 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000064-----  

690 ***Pre-Screening開始***  

691 ***Pre-Screening 結束***  

692 可能的攻擊方式: Universal Backdoor Attack  

693 可能的 target class: 1  

694 可能的 victim classes: ALL  

695 ***Trigger Reverse Engineering 開始***  

696 Target: 1, victim: 9, Loss: 0.3352, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:219.82, Cost:0.00 best_Reg:216.37 avg_Loss_Reg:218.93: 8%|████| 81/1000 [13:35<2:34:12, 10.07it/s]  

697 early stop 所有  

698 ***Trigger Reverse Engineering 結束***  

699 Target Class: 1 Victim Class: all Trigger Size: 216.37274932861328 Optimization Steps: 82  

700 *****檢測結束*****  

701 檢測結果: Model含有後門(Abnormal)  

702 整體耗時: 824.577677267456  

703 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000065-----  

704 ***Pre-Screening開始***  

705 ***Pre-Screening 結束***  

706 檢測結果: Model是安全的(Benign)  

707 整體耗時: 17.090968132019043  

708 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000066-----  

709 ***Pre-Screening 開始***  

710

```

```

711 ***Pre-Screening結束***  

712 可能的攻擊方式: Label Specific Backdoor Attack  

713 可能的 target-victim 配對: ['7-8']  

714 ***Trigger Reverse Engineering開始***  

715 Target: 7, victim: 8, Loss: 7.2764, Acc: 0.00%, CE_Loss: 7.28, Reg_Loss:2550.48, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2537.07: 1%| | 10/1000 [00:07<12:27, 1.33it/s]  

716 ***Trigger Reverse Engineering結束***  

717 Target Class: 7 Victim Class: 8 Trigger Size: 1000000000.0 Optimization Steps: 11  

718 *****檢測結果: Model是安全的(Benign)  

719 檢測結果: Model是安全的(Benign)  

720 整體耗時: 17.749913692474365  

721 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000067-----  

722 ***Pre-Screening開始***  

723 ***Pre-Screening結束***  

724 可能的攻擊方式: Universal Backdoor Attack  

725 可能的 target class: ALL  

726 可能的 victim classes: ALL  

727 ***Trigger Reverse Engineering開始***  

728 Target: 1, victim: 16, Loss: 0.0364, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:888.93, Cost:0.00 best_reg:862.01 avg_loss_reg:894.71: 7%| | 10/1000 [54:13<12:00:31, 46.49s/it]  

729 early stop 所有  

730 ***Trigger Reverse Engineering結束***  

731 Target Class: 1 Victim Class: all Trigger Size: 862.007246537642 Optimization Steps: 71  

732 *****檢測結果: Model含有後門(Abnormal)  

733 檢測結果: Model含有後門(Abnormal)  

734 整體耗時: 3281.0729250979  

735 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000068-----  

736 ***Pre-Screening開始***  

737 ***Pre-Screening結束***  

738 可能的攻擊方式: Universal Backdoor Attack  

739 可能的 target class: 0  

740 可能的 victim classes: ALL  

741 ***Trigger Reverse Engineering開始***  

742 Target: 0, victim: 3, Loss: 21.5826, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:561.41, Cost:0.04 best_reg:591.35 avg_loss_reg:591.35: 11%| | 114/1000 [11:06<1:26:21, 5.85s/it]  

743 early stop 所有  

744 ***Trigger Reverse Engineering結束***  

745 Target Class: 0 Victim Class: all Trigger Size: 567.5093383789062 Optimization Steps: 115  

746 *****檢測結果: Model含有後門(Abnormal)  

747 檢測結果: Model含有後門(Abnormal)  

748 整體耗時: 678.1912469863892  

749 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000069-----  

750 ***Pre-Screening開始***  

751 ***Pre-Screening結束***  

752 可能的攻擊方式: Label Specific Backdoor Attack  

753 可能的 target-victim 配對: ['3-15', '4-13', '15-3']  

754 ***Trigger Reverse Engineering開始***  

755 Target: 4, victim: 13, Loss: 6.9052, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:174.77, Cost:0.04 best_reg:175.98 avg_loss_reg:175.98: 13%| | 133/1000 [00:16<01:47, 8.05it/s]  

756 early stop 所有  

757 ***Trigger Reverse Engineering結束***  

758 Target Class: 4 Victim Class: 13 Trigger Size: 174.76739501953125 Optimization Steps: 101  

759 ***Symmetric Check開始***  

760 Target: 13, victim: 4, Loss: 3.3441, Acc: 60.00%, CE_Loss: 1.06, Reg_Loss:5132.66, Cost:0.00 best_reg:11446.18 avg_loss_reg:5152.19: 100%| | 101/101 [00:12<00:00, 8.18it/s]  

761 ***Symmetric Check結束***  

762 *****檢測結果: Model含有後門(Abnormal)  

763 檢測結果: Model含有後門(Abnormal)  

764 整體耗時: 37.879610776901245  

765 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000070-----  

766 ***Pre-Screening開始***  

767 ***Pre-Screening結束***  

768 ***檢測結束***  

769 檢測結果: Model是安全的(Benign)  

770 整體耗時: 14.030179500579834  

771 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000071-----  

772 ***Pre-Screening開始***  

773 ***Pre-Screening結束***  

774 ***檢測結束***  

775 檢測結果: Model是安全的(Benign)  

776 整體耗時: 12.382782459259033  

777 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000072-----  

778 ***Pre-Screening開始***  

779 ***Pre-Screening結束***  

780 可能的攻擊方式: Label Specific Backdoor Attack  

781 可能的 target-victim 配對: ['1-2']

```

```
782 ***Trigger Reverse Engineering 開始***  
783 Target: 1, victim: 2, Loss: 7.23, Acc: 10.00%, CE_Loss: 7.23, Reg_Loss:2849.44, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2790.99: 2%| | 20/1000 [00:02<02:07, 7.69it/s]  
784 ***Trigger Reverse Engineering 結束***  
785 Target Class: 1 Victim Class: 2 Trigger Size: 1000000000.0 Optimization Steps: 21  
786 *****檢測結束*****  
787 檢測結果: Model是安全的(Benign)  
788 整體耗時: 9.793334245681763  
789 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000073-----  
790 ***Pre-Screening 開始***  
791 ***Pre-Screening 結束***  
792 ***檢測結束***  
793 檢測結果: Model是安全的(Benign)  
794 耗時: 9.735391133998413  
795 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000074-----  
796 ***Pre-Screening 開始***  
797 ***Pre-Screening 結束***  
798 可能的攻擊方式: Universal Backdoor Attack  
799 可能的 target class: ALL  
800 可能的 victim classes: ALL  
801 ***Trigger Reverse Engineering 開始***  
802 Target: 2, victim: 12, Loss: 0.1760, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:78.20, Cost:0.00 best_reg:77.17 avg_loss_reg:77.29: 5%| | 50/1000 [01:47<34:09, 2.16s/it]  
803 early stop 所有  
804 ***Trigger Reverse Engineering 結束***  
805 Target Class: 2 Victim Class: all Trigger Size: 77.1730228000217 Optimization Steps: 51  
806 *****檢測結束*****  
807 檢測結果: Model含有後門(Abnormal)  
808 整體耗時: 116.48888731002808  
809 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000075-----  
810 ***Pre-Screening 開始***  
811 ***Pre-Screening 結束***  
812 可能的攻擊方式: Label Specific Backdoor Attack  
813 可能的 target-victim 配對: ['5-3', '5-7']  
814 ***Trigger Reverse Engineering 開始***  
815 Target: 5, victim: 7, Loss: 3.2535, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:52.87, Cost:0.06 best_reg:52.89 avg_loss_reg:52.93: 10%| | 95/1000 [00:09<01:26, 10.44it/s]  
816 early stop 所有  
817 ***Trigger Reverse Engineering 結束***  
818 Target Class: 5 Victim Class: 7 Trigger Size: 52.868919372558594 Optimization Steps: 87  
819 ***Symmetric Check開始***  
820 Target: 7, victim: 5, Loss: 10.0595, Acc: 70.00%, CE_Loss: 0.73, Reg_Loss:13994.41, Cost:0.00 best_reg:19791.03 avg_loss_reg:14401.38: 100%| | 87/87 [00:08<00:00, 10.49it/s]  
821 ***Symmetric Check 結束***  
822 *****檢測結束*****  
823 檢測結果: Model含有後門(Abnormal)  
824 耗時: 23.511597156524658  
825 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000076-----  
826 ***Pre-Screening 開始***  
827 ***Pre-Screening 結束***  
828 可能的攻擊方式: Label Specific Backdoor Attack  
829 可能的 target-victim 配對: ['8-9']  
830 ***Trigger Reverse Engineering 開始***  
831 Target: 8, victim: 9, Loss: 10.2534, Acc: 0.00%, CE_Loss: 10.25, Reg_Loss:2544.21, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2532.22: 1%| | 10/1000 [00:03<05:21, 3.08it/s]  
832 ***Trigger Reverse Engineering 結束***  
833 Target Class: 8 Victim Class: 9 Trigger Size: 1000000000.0 Optimization Steps: 11  
834 *****檢測結束*****  
835 檢測結果: Model是安全的(Benign)  
836 整體耗時: 11.7859981893539429  
837 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000077-----  
838 ***Pre-Screening 開始***  
839 ***Pre-Screening 結束***  
840 ***檢測結束***  
841 檢測結果: Model是安全的(Benign)  
842 整體耗時: 7.593531608581543  
843 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000078-----  
844 ***Pre-Screening 開始***  
845 ***Pre-Screening 結束***  
846 ***檢測結束***  
847 檢測結果: Model是安全的(Benign)  
848 整體耗時: 13.02119636356445  
849 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000079-----  
850 ***Pre-Screening 開始***  
851 ***Pre-Screening 結束***  
852 可能的攻擊方式: Label Specific Backdoor Attack
```

```

853 可能的 target-victim 配對: ['9-1', '21-1']
854 ***Trigger Reverse Engineering 開始***
855 Target: 21, victim: 1, Loss: 2.3981, Acc: 0.00%, CE_Loss: 2.40, Reg_Loss:3145.84, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2998.16: 3%| | 31/1000 [01:48<56:29, 3.50s/it]
856 ***Trigger Reverse Engineering 結束***
857 Target Class: 9 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11
858 *****檢測結果: Model是安全的(Benign)
859 檢測結果: Model是安全的(Benign)
860 整體耗時: 131.03706431388855
861 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000080-----
862 ***Pre-Screening 開始***
863 ***Pre-Screening 結束***
864 可能的攻擊方式: Label Specific Backdoor Attack
865 可能的 target-victim 配對: ['3-10', '13-10']
866 ***Trigger Reverse Engineering 開始***
867 Target: 13, victim: 10, Loss: 2.0125, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:114.49, Cost:0.02 best_reg:114.69 avg_loss_reg:114.69: 9%| | 92/1000 [04:16<42:14, 2.79s/it]
868 early stop 所有
869 ***Trigger Reverse Engineering 結束***
870 Target Class: 13 Victim Class: 10 Trigger Size: 114.49464416503906 Optimization Steps: 82
871 ***Symmetric Check 開始***
872 Target: 10, victim: 13, Loss: 2.9464, Acc: 90.00%, CE_Loss: 0.32, Reg_Loss:3940.23, Cost:0.00 best_reg:6668.54 avg_loss_reg:4001.40: 100%| | 82/82 [03:46<00:00, 2.76s/it]
873 ***Symmetric Check 結束***
874 *****檢測結果: Model含 有後門(Abnormal)
875 檢測結果: Model含 有後門(Abnormal)
876 整體耗時: 500.08529710769653
877 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000081-----
878 ***Pre-Screening 開始***
879 ***Pre-Screening 結束***
880 ***檢測結果: ***
881 檢測結果: Model是安全的(Benign)
882 整體耗時: 14.089277744293213
883 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000082-----
884 ***Pre-Screening 開始***
885 ***Pre-Screening 結束***
886 可能的攻擊方式: Universal Backdoor Attack
887 可能的 target class: 2
888 可能的 victim classes: ALL
889 ***Trigger Reverse Engineering 開始***
890 Target: 2, victim: 9, Loss: 0.1716, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:255.17, Cost:0.00 best_reg:5811.71 avg_loss_reg:318.77: 2%| | 17/1000 [00:27<26:31, 1.62s/it]
891 early stop 所有
892 ***Trigger Reverse Engineering 結束***
893 Target Class: 2 Victim Class: all Trigger Size: 5811.7144775390625 Optimization Steps: 18
894 *****檢測結果: Model是安全的(Benign)
895 檢測結果: Model是安全的(Benign)
896 整體耗時: 34.564368724823
897 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000083-----
898 ***Pre-Screening 開始***
899 ***Pre-Screening 結束***
900 可能的攻擊方式: Label Specific Backdoor Attack
901 可能的 target-victim 配對: ['2-7']
902 ***Trigger Reverse Engineering 開始***
903 Target: 2, victim: 7, Loss: 2.8437, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:48.77, Cost:0.06 best_reg:50.43 avg_loss_reg:50.43: 7%| | 72/1000 [00:07<01:39, 9.31it/s]
904 early stop 所有
905 ***Trigger Reverse Engineering 結束***
906 Target Class: 2 Victim Class: 7 Trigger Size: 48.77121353149414 Optimization Steps: 73
907 ***Symmetric Check 開始***
908 Target: 7, victim: 2, Loss: 3.3430, Acc: 95.00%, CE_Loss: 0.38, Reg_Loss:2963.41, Cost:0.00 best_reg:4572.58 avg_loss_reg:3095.16: 100%| | 73/73 [00:07<00:00, 9.71it/s]
909 ***Symmetric Check 結束***
910 *****檢測結果: Model含 有後門(Abnormal)
911 檢測結果: Model含 有後門(Abnormal)
912 整體耗時: 22.688708543777466
913 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000084-----
914 ***Pre-Screening 開始***
915 ***Pre-Screening 結束***
916 可能的攻擊方式: Universal Backdoor Attack
917 可能的 target class: 0
918 可能的 victim classes: ALL
919 ***Trigger Reverse Engineering 開始***
920 Target: 0, victim: 6, Loss: 0.6189, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:171.54, Cost:0.00 best_reg:171.89 avg_loss_reg:171.05: 11%| | 106/1000 [14:49<2:04:58, 8.39s/it]
921 early stop 所有
922 ***Trigger Reverse Engineering 結束***
923 Target Class: 0 Victim Class: all Trigger Size: 171.70403442382812 Optimization Steps: 107

```

File - main

```

924 *****檢測結束*****
925 檢測結果: Model含有後門(Abnormal)
926 整體耗時: 897.533429145813
927 *****Pre-Screening開始*****
928 *****Pre-Screening結束*****
929 可能的攻擊方式: Label Specific Backdoor Attack
930 可能的 target-victim 配對: [0-1', '0-18', '0-19', '8-7', '8-16', '12-17', '19-18']
931 ***Trigger Reverse Engineering開始***
932 Target: 8, victim: 16, Loss: 4.0465, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:346.96, Cost:0.01 best_reg:347.53 avg_loss_reg:347.53: 23% █ | 233/1000 [13:03 <42:57, 3.36s/it]
933 Target Class: 8 Victim Class: 16 Trigger Size: 346.96417236328125 Optimization Steps: 98
934 early stop 所有
935 ***Trigger Reverse Engineering結束***
936 Target Class: 8 Victim Class: 16 Trigger Size: 346.96417236328125 Optimization Steps: 98
937 ***Symmetric Check開始***
938 Target: 16, victim: 8, Loss: 1.5069, Acc: 25.00%, CE_Loss: 1.51, Reg_Loss:166.1627, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:16525.87: 100% █ | 98/98 [05:15 <00:00, 3.22s/it]
939 ***Symmetric Check結束***
940 *****檢測結束*****
941 檢測結果: Model含有後門(Abnormal)
942 整體耗時: 1123.600567182465
943 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000086-----
944 ***Pre-Screening開始***
945 ***Pre-Screening結束***
946 ***檢測結束***
947 檢測結果: Model是安全的(Benign)
948 整體耗時: 17.34115505218506
949 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000087-----
950 ***Pre-Screening開始***
951 ***Pre-Screening結束***
952 ***檢測結束***
953 檢測結果: Model是安全的(Benign)
954 整體耗時: 5.498942852020264
955 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000088-----
956 ***Pre-Screening開始***
957 ***Pre-Screening結束***
958 可能的攻擊方式: Label Specific Backdoor Attack
959 可能的 target-victim 配對: [0-1', '0-23', '3-4', '3-19', '9-4', '11-4', '11-19', '16-2', '17-3', '17-9', '18-4', '18-19', '19-4', '23-0']
960 ***Trigger Reverse Engineering開始***
961 Target: 18, victim: 19, Loss: 0.9857, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:384.85, Cost:0.00 best_reg:384.91 avg_loss_reg:385.41: 39% █ | 39/1000 [00:43 <01:08, 8.92it/s]
962 early stop 所有
963 ***Trigger Reverse Engineering結束***
964 Target Class: 18 Victim Class: 19 Trigger Size: 384.85443115234375 Optimization Steps: 151
965 ***Symmetric Check開始***
966 Target: 19, victim: 18, Loss: 2.8095, Acc: 90.00%, CE_Loss: 0.55, Reg_Loss:1003.34, Cost:0.00 best_reg:1152.97 avg_loss_reg:1009.49: 100% █ | 151/151 [00:16 <00:00, 9.08it/s]
967 ***Symmetric Check結束***
968 *****檢測結束*****
969 檢測結果: Model是安全的(Benign)
970 整體耗時: 73.36021900177002
971 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000089-----
972 ***Pre-Screening開始***
973 ***Pre-Screening結束***
974 可能的攻擊方式: Universal Backdoor Attack
975 可能的 target class: 9
976 可能的 victim classes: ALL
977 ***Trigger Reverse Engineering開始***
978 Target: 9, victim: 19, Loss: 0.1386, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:264.28, Cost:0.00 best_reg:339.97 avg_loss_reg:265.44: 3% █ | 27/1000 [02:13 < 1:20:04, 4.94s/it]
979 early stop 所有
980 ***Trigger Reverse Engineering結束***
981 Target Class: 9 Victim Class: all Trigger Size: 339.9654017857143 Optimization Steps: 28
982 *****檢測結束*****
983 檢測結果: Model含有後門(Abnormal)
984 整體耗時: 142.23385548591614
985 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000090-----
986 ***Pre-Screening開始***
987 ***Pre-Screening結束***
988 可能的攻擊方式: Label Specific Backdoor Attack
989 可能的 target-victim 配對: [1-0]
990 ***Trigger Reverse Engineering開始***
991 Target: 1, victim: 0, Loss: 9.1544, Acc: 0.00%, CE_Loss: 9.15, Reg_Loss:2586.48, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2565.96: 1% | 10/1000 [00:01 <02:12, 7.46it/s]
992 ***Trigger Reverse Engineering結束***
993 Target Class: 1 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 11
994 *****檢測結束*****

```

995 檢測結果: Model是安全的(Benign)  
996 整體耗時: 7.880602598190308 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000091-----  
997 \*\*\*Pre-Screening開始\*\*\*  
998 \*\*\*Pre-Screening結束\*\*\*  
999 \*\*\*Pre-Screening開始\*\*\*  
1000 \*\*\*檢測結束\*\*\*  
1001 檢測結果: Model是安全的(Benign)  
1002 整體耗時: 6.620845079421997 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000092-----  
1003 \*\*\*Pre-Screening開始\*\*\*  
1004 \*\*\*Pre-Screening結束\*\*\*  
1005 可能的攻擊方式: Label Specific Backdoor Attack  
1006 可能的target-victim 配對: [0-5]  
1007 可能的 target-victim 配對: [0-5]  
1008 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1009 Target: 0 victim: 5 Loss: 12.8185 Acc: 0.00% CE\_Loss: 12.82 Reg\_Loss:2546.30, Cost:0.00 best\_Reg:1000000000.00 avg\_loss\_Reg:2534.92: 1% | 10/1000 [00:05<09:20, 1.77it/s]  
1010 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1011 Target Class: 0 Victim Class: 5 Trigger Size: 1000000000.0 Optimization Steps: 11  
1012 \*\*\*\*\*檢測結束\*\*\*\*\*  
1013 檢測結果: Model是安全的(Benign)  
1014 整體耗時: 13.490098476409912 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000093-----  
1015 \*\*\*Pre-Screening開始\*\*\*  
1016 \*\*\*Pre-Screening結束\*\*\*  
1017 \*\*\*Pre-Screening開始\*\*\*  
1018 可能的攻擊方式: Label Specific Backdoor Attack  
1019 可能的 target-victim 配對: ['4-6', '10-6', '11-13']  
1020 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1021 Target: 11 victim: 13 Loss: 6.4381 Acc: 100.00% CE\_Loss: 0.12 Reg\_Loss:246.54, Cost:0.03 best\_Reg:250.94 avg\_loss\_Reg:243.85: 14% | 136/1000 [00:19<02:06, 6.83it/s]  
1022 0% | 0/77 [00:00< ?, ?it/s]early stop 所有  
1023 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1024 Target Class: 11 Victim Class: 13 Trigger Size: 246.5424041748047 Optimization Steps: 77  
1025 \*\*\*Symmetric Check開始\*\*\*  
1026 Target: 13 victim: 11 Loss: 9.5785 Acc: 70.00% CE\_Loss: 0.79 Reg\_Loss:8785.65, Cost:0.00 best\_Reg:12632.95 avg\_loss\_Reg:9457.98: 100% | 77/77 [00:11<00:00, 6.64it/s]  
1027 \*\*\*Symmetric Check結束\*\*\*  
1028 \*\*\*\*\*檢測結束\*\*\*\*\*  
1029 檢測結果: Model含有後門(Abnormal)  
1030 整體耗時: 38.07493352890015 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000094-----  
1031 \*\*\*Pre-Screening開始\*\*\*  
1032 \*\*\*Pre-Screening結束\*\*\*  
1033 可能的攻擊方式: Label Specific Backdoor Attack  
1034 可能的 target-victim 配對: ['1-2', '2-9', '2-22', '3-15', '4-20', '5-11', '5-20', '6-3', '7-3', '8-2', '8-22', '9-19', '11-20', '13-12', '13-20', '15-3', '15-11', '18-15', '18-5', '18-22', '20-5', '21-2', '21-8']  
1035 可能的 target-victim 配對: ['1-2', '2-9', '2-22', '3-15', '4-20', '5-11', '5-20', '6-3', '7-3', '8-2', '8-22', '9-19', '11-20', '13-12', '13-20', '15-3', '15-11', '18-15', '18-5', '18-22', '20-5', '21-2', '21-8']  
1036 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1037 Target: 3 victim: 15 Loss: 1.3984 Acc: 100.00% CE\_Loss: 0.11 Reg\_Loss:856.57, Cost:0.00 best\_Reg:862.66 avg\_loss\_Reg:862.66: 55% | 548/1000 [08:17<06:50, 1.10it/s]  
1038 early stop 所有  
1039 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1040 Target Class: 3 Victim Class: 15 Trigger Size: 856.5682373046875 Optimization Steps: 245  
1041 \*\*\*Symmetric Check開始\*\*\*  
1042 Target: 15 victim: 3 Loss: 1.0406 Acc: 100.00% CE\_Loss: 0.26 Reg\_Loss:3950.15, Cost:0.00 best\_Reg:3827.92 avg\_loss\_Reg:3965.08: 100% | 245/245 [04:21<00:00, 1.07it/s]  
1043 \*\*\*Symmetric Check結束\*\*\*  
1044 \*\*\*\*\*檢測結束\*\*\*\*\*  
1045 檢測結果: Model是安全的(Benign)  
1046 整體耗時: 772.6253283023834 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000095-----  
1047 \*\*\*Pre-Screening開始\*\*\*  
1048 \*\*\*Pre-Screening結束\*\*\*  
1049 可能的攻擊方式: Label Specific Backdoor Attack  
1050 可能的 target-victim 配對: ['2-3', '2-4', '2-5']  
1051 可能的 target-victim 配對: ['2-3', '2-4', '2-5']  
1052 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1053 Target: 2 victim: 5 Loss: 11.3240 Acc: 0.00% CE\_Loss: 11.32 Reg\_Loss:2581.18, Cost:0.00 best\_Reg:1000000000.00 avg\_loss\_Reg:2561.07: 4% | 42/1000 [00:18<06:50, 2.33it/s]  
1054 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1055 Target Class: 2 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 21  
1056 \*\*\*\*\*檢測結束\*\*\*\*\*  
1057 檢測結果: Model是安全的(Benign)  
1058 整體耗時: 22.240153551101685 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000096-----  
1059 \*\*\*Pre-Screening開始\*\*\*  
1060 \*\*\*Pre-Screening結束\*\*\*  
1061 可能的攻擊方式: Label Specific Backdoor Attack  
1062 可能的 target-victim 配對: ['2-3']  
1063 可能的 target-victim 配對: ['2-3']  
1064 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1065 Target: 2 victim: 3 Loss: 3.9951, Acc: 100.00%, CE\_Loss: 0.16 Reg\_Loss:149.94 avg\_loss\_Reg:149.94: 11% | 111/1000 [00:16<02:15, 6.55it/s]

```
1066 early stop 所有
1067 ***Trigger Reverse Engineering結束***
1068 Target Class: 2 Victim Class: 3 Trigger Size: 149.59913635253906 Optimization Steps: 112
1069 ***Symmetric Check開始***
1070 Target: 3, victim: 2, Loss: 1.3048, Acc: 70.00%, CE_Loss: 0.50, Reg_Loss:6105.99, Cost:0.00 best_reg:12299.64 avg_loss_reg:6139.63: 100%| [112/112 [00:17<00:00, 6.53it/s]
1071 ***Symmetric Check結束***
1072 ****Symmetric Check結束****
1073 檢測結果: Model含有後門(Abnormal)
1074 整體耗時: 37.55736589431763
1075 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000097-----
1076 ***Pre-Screening開始***
1077 ***Pre-Screening結束***
1078 ***檢測結束***
1079 檢測結果: Model是安全的(Benign)
1080 整體耗時: 17.50396156311035
1081 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000098-----
1082 ***Pre-Screening開始***
1083 ***Pre-Screening結束***
1084 可能的攻擊方式: Label Specific Backdoor Attack
1085 可能的 target-victim 配對: ['1-3', '1-7', '2-3', '2-6', '4-10', '7-1', '7-4', '7-12', '8-5', '8-6', '11-12']
1086 ***Trigger Reverse Engineering開始***
1087 Target: 1, victim: 7, Loss: 1.8698, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:520.50, Cost:0.00 best_reg:524.70 avg_loss_reg:524.70: 43%| [430/1000 [00:55<01:13, 7.77it/s]
1088 0%| [0/185 [00:00<?, ?it/s]early stop 所有
1089 ***Trigger Reverse Engineering結束***
1090 Target Class: 1 Victim Class: 7 Trigger Size: 520.50244140625 Optimization Steps: 185
1091 ***Symmetric Check開始***
1092 Target: 7, victim: 1, Loss: 2.4374, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:451.53, Cost:0.01 best_reg:456.84 avg_loss_reg:456.84: 74%| [137/185 [00:17<00:06, 7.76it/s]
1093 early stop 所有
1094 ****Symmetric Check結束****
1095 *****檢測結束*****
1096 檢測結果: Model是安全的(Benign)
1097 整體耗時: 79.86445927619934
1098 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000099-----
1099 ***Pre-Screening開始***
1100 ***Pre-Screening結束***
1101 可能的攻擊方式: Label Specific Backdoor Attack
1102 可能的 target-victim 配對: ['2-7', '3-1']
1103 ***Trigger Reverse Engineering開始***
1104 Target: 3, victim: 1, Loss: 8.7771, Acc: 5.00%, CE_Loss: 8.78, Reg_Loss:3219.60, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3078.77: 3%| [31/1000 [00:10<05:33, 2.91it/s]
1105 ***Trigger Reverse Engineering結束***
1106 Target Class: 2 Victim Class: 7 Trigger Size: 10000000000.0 Optimization Steps: 11
1107 *****檢測結束*****
1108 檢測結果: Model是安全的(Benign)
1109 整體耗時: 18.66694450378418
1110 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000100-----
1111 ***Pre-Screening開始***
1112 ***Pre-Screening結束***
1113 ***檢測結束***
1114 檢測結果: Model是安全的(Benign)
1115 整體耗時: 20.267292261123657
1116 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000101-----
1117 ***Pre-Screening開始***
1118 ***Pre-Screening結束***
1119 可能的攻擊方式: Universal Backdoor Attack
1120 可能的 target class: 4
1121 可能的 victim classes: ALL
1122 ***Trigger Reverse Engineering開始***
1123 Target: 4, victim: 17, Loss: 0.1802, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:270.06, Cost:0.00 best_reg:282.12 avg_loss_reg:277.22: 3%| [30/1000 [02:54<1:33:59, 5.81it/s]
1124 early stop 所有
1125 ***Trigger Reverse Engineering結束***
1126 Target Class: 4 Victim Class: all Trigger Size: 282.1248524983724 Optimization Steps: 31
1127 *****檢測結束*****
1128 檢測結果: Model含有後門(Abnormal)
1129 整體耗時: 185.93014001846313
1130 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000102-----
1131 ***Pre-Screening開始***
1132 ***Pre-Screening結束***
1133 可能的攻擊方式: Label Specific Backdoor Attack
1134 可能的 target-victim 配對: ['6-1', '6-2']
1135 ***Trigger Reverse Engineering開始***
1136 Target: 6, victim: 2, Loss: 2.0319, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:22.00, Cost:0.09 best_reg:23.01 avg_loss_reg:23.01: 8%| [76/1000 [00:38<07:48, 1.97it/s]
```

```
1137 early stop 所有
1138 ***Trigger Reverse Engineering結束***
1139 Target Class: 6 Victim Class: 2 Trigger Size: 22.000186920166016 Optimization Steps: 70
1140 ***Symmetric Check開始***
1141 Target: 2, victim: 6, Loss: 0.4768, Acc: 80.00%, CE_Loss: 0.48, Reg_Loss:14025.84, Cost:0.00 best_Reg:1000000000.00 avg_loss_Reg:13936.54: 100%|████| 70/70 [00:34<00:00, 2.01it/s]
1142 ***Symmetric Check結束***
1143 *****檢測結束*****  
1144 檢測結果: Model含有後門(Abnormal)
1145 整體耗時: 77.21825766563416  
1146 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000103-----  
1147 ***Pre-Screening開始***
1148 ***Pre-Screening結束***
1149 可能的攻擊方式: Universal Backdoor Attack
1150 可能的 target class: 7
1151 可能的 victim classes: ALL
1152 ***Trigger Reverse Engineering開始***
1153 Target: 7, victim: 19, Loss: 0.2759, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:77.38, Cost:0.00 best_Reg:83.56 avg_loss_Reg:77.14: 7%|█| 68/1000 [08:03<1:50:31, 7.11s/it]
1154 early stop 所有
1155 ***Trigger Reverse Engineering結束***
1156 Target Class: 7 Victim Class: all Trigger Size: 83.5587397984096 Optimization Steps: 69
1157 *****檢測結束*****  
1158 檢測結果: Model含有後門(Abnormal)
1159 整體耗時: 494.1946344314575  
1160 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000104-----  
1161 ***Pre-Screening開始***
1162 ***Pre-Screening結束***
1163 ***檢測結束***  
1164 檢測結果: Model是安全的(Benign)
1165 整體耗時: 13.409391403198242  
1166 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000105-----  
1167 ***Pre-Screening開始***
1168 ***Pre-Screening結束***
1169 ***檢測結束***  
1170 檢測結果: Model是安全的(Benign)
1171 整體耗時: 17.283063650131226  
1172 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000106-----  
1173 ***Pre-Screening開始***
1174 ***Pre-Screening結束***
1175 可能的攻擊方式: Label Specific Backdoor Attack
1176 可能的 target-victim 配對: ['1-2', '2-1', '2-17', '3-13', '4-9', '10-3', '12-3', '12-16', '13-3', '17-1', '17-2']
1177 ***Trigger Reverse Engineering開始***
1178 Target: 2, victim: 1, Loss: 0.7579, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:117.03, Cost:0.01 best_Reg:117.45 avg_loss_Reg:117.45: 51%|████| 508/1000 [00:39<00:37, 13.02it/s]
1179 early stop 所有
1180 ***Trigger Reverse Engineering結束***
1181 Target Class: 2 Victim Class: 1 Trigger Size: 117.02783203125 Optimization Steps: 187
1182 ***Symmetric Check開始***
1183 Target: 1, victim: 2, Loss: 0.9814, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:233.92, Cost:0.00 best_Reg:229.88 avg_loss_Reg:230.70: 100%|████| 187/187 [00:13<00:00, 14.05it/s]
1184 ***Symmetric Check結束***
1185 ***檢測結束*****  
1186 檢測結果: Model是安全的(Benign)
1187 整體耗時: 58.980252265930176  
1188 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000107-----  
1189 ***Pre-Screening開始***
1190 ***Pre-Screening結束***
1191 可能的攻擊方式: Label Specific Backdoor Attack
1192 可能的 target-victim 配對: ['0-12', '1-0', '9-2', '12-0', '13-0']
1193 ***Trigger Reverse Engineering開始***
1194 Target: 13, victim: 0, Loss: 0.8043, Acc: 100.00%, CE_Loss: 0.47, Reg_Loss:1137.55, Cost:0.00 best_Reg:1105.72 avg_loss_Reg:1135.88: 100%|████| 1000/1000 [03:40<00:00, 4.54it/s]
1195 ***Trigger Reverse Engineering結束***
1196 Target Class: 13 Victim Class: 0 Trigger Size: 1105.718505859375 Optimization Steps: 956
1197 ***檢測結束*****  
1198 檢測結果: Model是安全的(Benign)
1199 整體耗時: 229.24896478652954  
1200 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000108-----  
1201 ***Pre-Screening開始***
1202 ***Pre-Screening結束***
1203 可能的攻擊方式: Universal Backdoor Attack
1204 可能的 target class: 9
1205 可能的 victim classes: ALL
1206 ***Trigger Reverse Engineering開始***
1207 Target: 9, victim: 14, Loss: 0.2802, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:280.18, Cost:0.00 best_Reg:283.14 avg_loss_Reg:279.21: 8%|█| 82/1000 [07:25<1:23:02, 5.43s/it]
Page 17 of 67
```

```

1208 early stop 所有
1209 ***Trigger Reverse Engineering結束***
1210 Target Class: 9 Victim Class: all Trigger Size: 283.13702087402345 Optimization Steps: 83
1211 *****檢測結果*****檢測結束*****  

1212 檢測結果: Model含有後門(Abnormal)
1213 整體耗時: 455.85304403305054
1214 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000109-----
1215 ***Pre-Screening開始***
1216 ***Pre-Screening結束***
1217 可能的攻擊方式: Label Specific Backdoor Attack
1218 可能的 target-victim 配對: ['0-8', '0-10', '2-7']
1219 ***Trigger Reverse Engineering開始***
1220 Target: 0, victim: 8, Loss: 1.5482, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss: 0.11, Reg_Loss_reg:284.07: 18% █ | 183/1000 [00:38<02:53, 4.71it/s]
1221 early stop 所有
1222 ***Trigger Reverse Engineering結束***
1223 Target Class: 0 Victim Class: 8 Trigger Size: 283.7460021972656 Optimization Steps: 139
1224 ***Symmetric Check開始***
1225 Target: 8, victim: 0, Loss: 1.1270, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:1277.02, Cost:0.00 best_reg:1289.05 avg_loss_reg:1289.05: 100% █ | 139/139 [00:30<00:00, 4.63it/s]
1226 ***Symmetric Check結束***  

1227 *****檢測結果*****檢測結束*****  

1228 檢測結果: Model是安全的(Benign)
1229 整體耗時: 76.43703031539917 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000110-----
1230 ***Pre-Screening開始***
1231 ***Pre-Screening結束***
1232 ***Pre-Screening開始***
1233 可能的攻擊方式: Universal Backdoor Attack
1234 可能的 target class: 3
1235 可能的 victim classes: ALL
1236 ***Trigger Reverse Engineering開始***
1237 Target: 3, victim: 12, Loss: 0.2555, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:75.68, Cost:0.00 best_reg:73.78 avg_loss_reg:75.26: 8% █ | 82/1000 [33:08<6:11:01, 24.25s/it]
1238 early stop 所有
1239 ***Trigger Reverse Engineering結束***
1240 Target Class: 3 Victim Class: all Trigger Size: 73.77916717529297 Optimization Steps: 83
1241 *****檢測結果*****檢測結束*****  

1242 檢測結果: Model含有後門(Abnormal)
1243 整體耗時: 2003.1719031333923 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000111-----
1244 -----  

1245 ***Pre-Screening開始***
1246 ***Pre-Screening結束***
1247 ***檢測結果*****檢測結束***  

1248 檢測結果: Model是安全的(Benign)
1249 整體耗時: 10.94533109664917 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000112-----
1250 -----  

1251 ***Pre-Screening開始***
1252 ***Pre-Screening結束***
1253 可能的攻擊方式: Label Specific Backdoor Attack
1254 可能的 target-victim 配對: ['0-1', '16-11']
1255 ***Trigger Reverse Engineering開始***
1256 Target: 16, victim: 11, Loss: 5.8819, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:99.19, Cost:0.06 best_reg:99.62 avg_loss_reg:97.54: 13% █ | 126/1000 [02:59<20:42, 1.42s/it]
1257 early stop 所有
1258 ***Trigger Reverse Engineering結束***
1259 Target Class: 16 Victim Class: 11 Trigger Size: 99.1943359375 Optimization Steps: 116
1260 ***Symmetric Check開始***
1261 Target: 11, victim: 16, Loss: 1.2934, Acc: 90.00%, CE_Loss: 0.27, Reg_Loss:7774.00, Cost:0.00 best_reg:8254.67 avg_loss_reg:7815.20: 100% █ | 116/116 [02:42<00:00, 1.40s/it]
1262 ***Symmetric Check結束***  

1263 *****檢測結果*****檢測結束*****  

1264 檢測結果: Model含有後門(Abnormal)
1265 整體耗時: 358.08257007598877 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000113-----
1266 -----  

1267 ***Pre-Screening開始***
1268 ***Pre-Screening結束***
1269 ***檢測結果*****檢測結束***  

1270 檢測結果: Model是安全的(Benign)
1271 整體耗時: 18.308409214019775 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000114-----
1272 -----  

1273 ***Pre-Screening開始***
1274 ***Pre-Screening結束***
1275 可能的攻擊方式: Label Specific Backdoor Attack
1276 可能的 target-victim 配對: ['1-2', '2-1', '4-2', '4-16', '14-3']
1277 ***Trigger Reverse Engineering開始***
1278 Target: 1, victim: 2, Loss: 2.7199, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:75.11, Cost:0.00 best_reg:765.92 avg_loss_reg:765.92: 28% █ | 282/1000 [03:08<07:59, 1.50it/s]

```

```
1279 early stop 所有
1280 ***Trigger Reverse Engineering結束***
1281 Target Class: 1 Victim Class: 2 Trigger Size: 757.11474609375 Optimization Steps: 140
1282 ***Symmetric Check開始***
1283 Target: 2, victim: 1, Loss: 2.5011, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss: 1010.18, Cost:0.00 best_Reg:1012.91 avg_loss_Reg:1012.91: 100%|██████████| | 140/140 [01:41 <00:00, 1.38it/s]
1284 ***Symmetric Check結束***
1285 *****檢測結果: Model是安全的(Benign)
1286 整體耗時: 301.6820764541626
1288 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000115-----
1289 ***Pre-Screening開始***
1290 ***Pre-Screening結束***
1291 ***檢測結束*** 檢測結果: Model是安全的(Benign)
1292 整體耗時: 17.451646656639099
1293 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000116-----
1294 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000117-----
1295 ***Pre-Screening開始***
1296 ***Pre-Screening結束***
1297 可能的攻擊方式:Universal Backdoor Attack
1298 可能的 target class: 1
1299 可能的 victim classes: ALL
1300 ***Trigger Reverse Engineering開始***
1301 Target: 1, victim: 19, Loss: 1.6342, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss: 5515.40, Cost:0.00 best_Reg:5533.82 avg_loss_Reg:5706.35: 12%|████| | 115/1000 [53:53 <6:54:41, 28.11s/it]
1302 early stop 所有
1303 ***Trigger Reverse Engineering結束***
1304 Target Class: 1 Victim Class: all Trigger Size: 5533.819266183035 Optimization Steps: 116
1305 *****檢測結果: Model是安全的(Benign)
1306 檢測結果: Model是安全的(Benign)
1307 整體耗時: 3248.550849914551
1308 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000117-----
1309 ***Pre-Screening開始***
1310 ***Pre-Screening結束***
1311 可能的攻擊方式: Label Specific Backdoor Attack
1312 可能的 target-victim 配對: ['2-0', '2-3', '2-4']
1313 ***Trigger Reverse Engineering開始***
1314 Target: 2, victim: 4, Loss: 10.8851, Acc: 0.00%, CE_Loss: 10.89, Reg_Loss: 2546.01, Cost:0.00 best_Reg:10000000000.00 avg_loss_Reg:2534.08: 3%|████| | 32/1000 [00:03 <01:49, 8.81it/s]
1315 ***Trigger Reverse Engineering結束***
1316 Target Class: 2 Victim Class: 0 Trigger Size: 10000000000.00 Optimization Steps: 11
1317 *****檢測結果: Model是安全的(Benign)
1318 檢測結果: Model是安全的(Benign)
1319 整體耗時: 13.000511121749878
1320 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000118-----
1321 ***Pre-Screening開始***
1322 ***Pre-Screening結束***
1323 ***檢測結束*** 檢測結果: Model是安全的(Benign)
1324 檢測結果: Model是安全的(Benign)
1325 整體耗時: 25.40241551399231
1326 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000119-----
1327 ***Pre-Screening開始***
1328 ***Pre-Screening結束***
1329 ***檢測結束*** 檢測結果: Model是安全的(Benign)
1330 檢測結果: Model是安全的(Benign)
1331 整體耗時: 10.926257133483887
1332 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000120-----
1333 ***Pre-Screening開始***
1334 ***Pre-Screening結束***
1335 可能的攻擊方式: Label Specific Backdoor Attack
1336 可能的 target-victim 配對: ['0-8', '0-21', '1-7', '1-16', '2-11', '2-13', '2-16', '3-10', '6-19', '7-13', '7-16', '8-0', '8-19', '10-11', '10-16', '11-13', '11-10', '12-14', '15-14', '15-21', '15-5', '12-4', '16-10', '16-11', '17-5', '19-21', '21-0', '21-19']
1337 ***Trigger Reverse Engineering開始***
1338 Target: 16, victim: 11, Loss: 0.8928, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss: 1051.67, Cost:0.00 best_Reg:1069.50 avg_loss_Reg:1041.51: 61%|████| | 610/1000 [36:39 <23:26, 3.61s/it]
1339 early stop 所有
1340 ***Trigger Reverse Engineering結束***
1341 Target Class: 16 Victim Class: 11 Trigger Size: 1051.6719970703125 Optimization Steps: 219
1342 *****檢測結果: Model是安全的(Benign)
1343 檢測結果: Model是安全的(Benign)
1344 整體耗時: 2226.367737531662
1345 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000121-----
1346 ***Pre-Screening開始***
1347 ***Pre-Screening結束*** 檢測結果: Model是安全的(Benign)
1348 可能的攻擊方式: Label Specific Backdoor Attack
1349 可能的 target-victim 配對: ['1-14', '6-2', '14-1']
```

```

File - main
1350 ***Trigger Reverse Engineering開始****
1351 Target: 14, victim: 1, Loss: 5.3068, Acc: 10.00%, CE_Loss: 5.31, Reg_Loss: 3549.48, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:3309.52: 4% █ | 42/1000 [00:27<10:29, 1.52it/s]
1352 ***Trigger Reverse Engineering結束****
1353 Target Class: 1 Victim Class: 14 Trigger Size: 1000000000.0 Optimization Steps: 11
1354 ****檢測結果: Model是安全的(Benign)
1355 檢測結果: Model是安全的(Benign)
1356 整體耗時: 39.74085736274719
1357 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000122-----
1358 ***Pre-Screening開始****
1359 ***Pre-Screening結束****
1360 可能的攻擊方式: Universal Backdoor Attack
1361 可能的 target class: 2
1362 可能的 victim classes: ALL
1363 ***Trigger Reverse Engineering開始****
1364 Target: 2, victim: 14, Loss: 0.5384, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:97.46, Cost:0.01 best_reg:97.95 avg_loss_reg:95.25: 9% █ | 86/1000 [07:19<1:17:54, 5.11s/it]
1365 early stop 所有
1366 ***Trigger Reverse Engineering結束****
1367 Target Class: 2 Victim Class: all Trigger Size: 97.9474415283203 Optimization Steps: 87
1368 ****檢測結束*****檢測結果: Model含有後門(Abnormal)
1369 檢測結果: Model含有後門(Abnormal)
1370 整體耗時: 449.74557733535767
1371 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000123-----
1372 ***Pre-Screening開始****
1373 ***Pre-Screening結束****
1374 ***檢測結果: Model是安全的(Benign)
1375 檢測結果: Model是安全的(Benign)
1376 整體耗時: 11.765231847763062
1377 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000124-----
1378 ***Pre-Screening開始****
1379 ***Pre-Screening結束****
1380 ***檢測結果: Model是安全的(Benign)
1381 檢測結果: Model是安全的(Benign)
1382 整體耗時: 12.506844997406006
1383 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000125-----
1384 ***Pre-Screening開始****
1385 ***Pre-Screening結束****
1386 可能的攻擊方式: Label Specific Backdoor Attack
1387 可能的 target-victim 配對: ['4-3', '8-3']
1388 ***Trigger Reverse Engineering開始****
1389 Target: 4, victim: 3, Loss: 4.3082, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:813.26, Cost:0.01 best_reg:814.77 avg_loss_reg:814.77: 19% █ | 189/1000 [01:20<05:46, 2.34it/s]
1390 early stop 所有
1391 ***Trigger Reverse Engineering結束****
1392 Target Class: 4 Victim Class: 3 Trigger Size: 813.263427734375 Optimization Steps: 179
1393 ***Symmetric Check開始****
1394 Target: 3, victim: 4, Loss: 5.4069, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:2283.56, Cost:0.00 best_reg:2285.21 avg_loss_reg:2285.21: 94% █ | 168/179 [01:26<00:05, 1.95it/s]
1395 early stop 所有
1396 ***Symmetric Check結束****
1397 ***檢測結果: Model是安全的(Benign)
1398 檢測結果: Model是安全的(Benign)
1399 整體耗時: 175.42600464820862
1400 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000126-----
1401 ***Pre-Screening開始****
1402 ***Pre-Screening結束****
1403 可能的攻擊方式: Label Specific Backdoor Attack
1404 可能的 target-victim 配對: ['1-4', '2-4', '9-10', '10-0', '10-9']
1405 ***Trigger Reverse Engineering開始****
1406 Target: 10, victim: 0, Loss: 2.1735, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:266.33, Cost:0.01 best_reg:268.43 avg_loss_reg:268.43: 26% █ | 258/1000 [00:39<01:53, 6.56it/s]
1407 early stop 所有
1408 ***Trigger Reverse Engineering結束****
1409 Target Class: 10 Victim Class: 0 Trigger Size: 266.32720947265625 Optimization Steps: 214
1410 ***Symmetric Check開始****
1411 Target: 0, victim: 10, Loss: 1.4214, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:1727.01, Cost:0.00 best_reg:1700.06 avg_loss_reg:1723.15: 100% █ | 214/214 [00:30<00:00, 7.04it/s]
1412 ***Symmetric Check結束****
1413 ***檢測結果: Model是安全的(Benign)
1414 檢測結果: Model是安全的(Benign)
1415 整體耗時: 76.22197437286377
1416 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000127-----
1417 ***Pre-Screening開始****
1418 ***Pre-Screening結束****
1419 可能的攻擊方式: Label Specific Backdoor Attack
1420 可能的 target-victim 配對: ['2-1', '11-21', '14-21', '15-21', '22-21']

```

```

File - main
1421 ***Trigger Reverse Engineering開始****
1422 Target: 22, victim: 21, Loss: 10.5746, Acc: 0.00%, CE_Loss: 10.57, Reg_Loss:2523.19, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2517.02: 6% | 64/1000 [03:34<52:16, 3.35s/it]
1423 ***Trigger Reverse Engineering結束***
1424 Target Class: 2 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11
1425 ****檢測結果: Model是安全的(Benign)
1426 檢測結果: Model是安全的(Benign)
1427 整體耗時: 230.7379150390625
1428 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000128-----
1429 ***Pre-Screening開始****
1430 ***Pre-Screening結束***
1431 可能的攻擊方式: label Specific Backdoor Attack
1432 可能的 target-victim 配對: ['1-2', '4-1', '5-1', '8-2', '8-5', '8-7', '9-7']
1433 ***Trigger Reverse Engineering開始****
1434 Target: 8, victim: 2, Loss: 4.3483, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:244.42, Cost:0.02 best_reg:244.57 avg_loss_reg:245.15: 27% | 271/1000 [00:29<01:19, 9.12it/s]
1435 early stop 所有
1436 ***Trigger Reverse Engineering結束****
1437 Target Class: 8 Victim Class: 2 Trigger Size: 244.42417907714844 Optimization Steps: 121
1438 ***Symmetric Check開始****
1439 Target: 2, victim: 8, Loss: 1.0276, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:3700.98, Cost:0.00 best_reg:3777.15 avg_loss_reg:3777.15: 100% | 121/121 [00:13<00:00, 8.80it/s]
1440 ***Symmetric Check結束****
1441 ****檢測結果: Model含有後門(Abnormal)
1442 檢測結果: Model含有後門(Abnormal)
1443 整體耗時: 49.69510793685913
1444 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000129-----
1445 ***Pre-Screening開始****
1446 ***Pre-Screening結束***
1447 ***檢測結果: Model是安全的(Benign)
1448 檢測結果: Model是安全的(Benign)
1449 整體耗時: 17.729063034057617
1450 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000130-----
1451 ***Pre-Screening開始****
1452 ***Pre-Screening結束***
1453 ***檢測結果: Model是安全的(Benign)
1454 檢測結果: Model是安全的(Benign)
1455 整體耗時: 13.131453275680542
1456 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000131-----
1457 ***Pre-Screening開始****
1458 ***Pre-Screening結束***
1459 可能的攻擊方式: label Specific Backdoor Attack
1460 可能的 target-victim 配對: ['0-15', '1-15', '8-13', '10-16', '13-8', '17-0', '17-16']
1461 ***Trigger Reverse Engineering開始****
1462 Target: 1, victim: 15, Loss: 1.2195, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:1684.62, Cost:0.00 best_reg:1684.99 avg_loss_reg:1684.92: 50% | 501/1000 [21:41<21:36, 2.60s/it]
1463 early stop 所有
1464 ***Trigger Reverse Engineering結束****
1465 Target Class: 1 Victim Class: 15 Trigger Size: 1684.616455078125 Optimization Steps: 405
1466 ***檢測結果: Model是安全的(Benign)
1467 檢測結果: Model是安全的(Benign)
1468 整體耗時: 1317.3795902729034
1469 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000132-----
1470 ***Pre-Screening開始****
1471 ***Pre-Screening結束***
1472 可能的攻擊方式: Label Specific Backdoor Attack
1473 可能的 target-victim 配對: ['0-19', '8-4', '12-1', '18-19']
1474 ***Trigger Reverse Engineering開始****
1475 Target: 18, victim: 19, Loss: 11.2953, Acc: 0.00%, CE_Loss: 11.30, Reg_Loss:2563.41, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2548.16: 5% | 53/1000 [00:09<02:43, 5.77it/s]
1476 ***Trigger Reverse Engineering結束****
1477 Target Class: 0 Victim Class: 19 Trigger Size: 1000000000.0 Optimization Steps: 11
1478 ***檢測結果: Model是安全的(Benign)
1479 檢測結果: Model是安全的(Benign)
1480 整體耗時: 16.73827886581421
1481 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000133-----
1482 ***Pre-Screening開始****
1483 ***Pre-Screening結束***
1484 ***檢測結果: Model是安全的(Benign)
1485 檢測結果: Model是安全的(Benign)
1486 整體耗時: 10.23065193328857
1487 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000134-----
1488 ***Pre-Screening開始****
1489 ***檢測結果: Model是安全的(Benign)
1490 檢測結果: Model是安全的(Benign)
1491 檢測結果: Model是安全的(Benign)

```

1492 整體耗時: 11.668393850326538 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000135-----  
1493   \*\*\*Pre-Screening開始\*\*\*  
1494   可能的攻擊方式: Label Specific Backdoor Attack  
1495   可能的target-victim 配對: ['1-4', '5-1', '9-7']  
1496   \*\*\*Trigger Reverse Engineering開始\*\*\*  
1497 Target: 5, victim: 1, Loss: 1.6850, Acc: 100.00%, CE\_Loss: 0.18, Reg\_Loss:1508.55, Cost:0.00 best\_reg:1508.78 avg\_loss\_reg:1510.42: 29% | 290/1000 [00:33<01:21, 8.73it/s]  
1500 early stop 所有  
1501   \*\*\*Trigger Reverse Engineering結束\*\*\*  
1502 Target Class: 5 Victim Class: 1 Trigger Size: 1508.553955078125 Optimization Steps: 258  
1503 檢測結果: Model是安全的(Benign)  
1504   \*\*\*Pre-Screening開始\*\*\*  
1505   整體耗時: 40.61774826049805 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000136-----  
1506   \*\*\*Pre-Screening結束\*\*\*  
1507   \*\*\*Pre-Screening開始\*\*\*  
1508   \*\*\*Pre-Screening結束\*\*\*  
1509   \*\*\*檢測結果: Model是安全的(Benign)  
1510   整體耗時: 6.45193099755859 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000137-----  
1511   \*\*\*Pre-Screening開始\*\*\*  
1512   \*\*\*Pre-Screening結束\*\*\*  
1513   \*\*\*Pre-Screening開始\*\*\*  
1514   \*\*\*Pre-Screening結束\*\*\*  
1515   可能的攻擊方式: Label Specific Backdoor Attack  
1516   可能的target-victim 配對: ['2-13', '3-2', '3-13', '4-8', '5-4', '5-8', '5-13', '6-8', '10-4', '12-3']  
1517   \*\*\*Trigger Reverse Engineering開始\*\*\*  
1518 Target: 3, victim: 2, Loss: 1.8443, Acc: 100.00%, CE\_Loss: 0.15, Reg\_Loss:223.28, Cost:0.01 best\_reg:223.78 avg\_loss\_reg:223.60: 35% | 349/1000 [06:24<11:57, 1.10s/it]  
1519 early stop 所有  
1520   \*\*\*Trigger Reverse Engineering結束\*\*\*  
1521 Target Class: 3 Victim Class: 2 Trigger Size: 223.28207397460938 Optimization Steps: 177  
1522   \*\*\*Symmetric Check開始\*\*\*  
1523 Target: 2, victim: 3, Loss: 0.0896, Acc: 100.00%, CE\_Loss: 0.01, Reg\_Loss:4697.78, Cost:0.00 best\_reg:4744.28 avg\_loss\_reg:4761.69: 100% | 177/177 [03:16<00:00, 1.11s/it]  
1524   \*\*\*Symmetric Check結束\*\*\*  
1525   \*\*\*\*\*檢測結束\*\*\*\*\*  
1526 檢測結果: Model含有後門(Abnormal)  
1527 整體耗時: 589.9502079486847 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000138-----  
1528   \*\*\*\*\*檢測結束\*\*\*\*\*  
1529   \*\*\*Pre-Screening開始\*\*\*  
1530   \*\*\*Pre-Screening結束\*\*\*  
1531   可能的攻擊方式: Label Specific Backdoor Attack  
1532   可能的target-victim 配對: ['4-10']  
1533   \*\*\*Trigger Reverse Engineering開始\*\*\*  
1534 Target: 4, victim: 10, Loss: 2.6461, Acc: 100.00%, CE\_Loss: 0.22, Reg\_Loss:719.37, Cost:0.00 best\_reg:726.31 avg\_loss\_reg:719.76: 14% | 142/1000 [01:00<06:04, 2.35it/s]  
1535 early stop 所有  
1536   \*\*\*Trigger Reverse Engineering結束\*\*\*  
1537 Target Class: 4 Victim Class: 10 Trigger Size: 719.365234375 Optimization Steps: 143  
1538   \*\*\*Symmetric Check開始\*\*\*  
1539 Target: 10, victim: 4, Loss: 3.7186, Acc: 90.00%, CE\_Loss: 0.26, Reg\_Loss:5187.67, Cost:0.00 best\_reg:5232.50 avg\_loss\_reg:5232.50: 100% | 143/143 [01:02<00:00, 2.30it/s]  
1540   \*\*\*Symmetric Check結束\*\*\*  
1541   \*\*\*\*\*檢測結束\*\*\*\*\*  
1542 檢測結果: Model是安全的(Benign)  
1543 整體耗時: 130.94886660575867 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000139-----  
1544   \*\*\*\*\*檢測結束\*\*\*\*\*  
1545   \*\*\*Pre-Screening開始\*\*\*  
1546   \*\*\*Pre-Screening結束\*\*\*  
1547   \*\*\*檢測結束\*\*\*  
1548 檢測結果: Model是安全的(Benign)  
1549 整體耗時: 2.6243269443511963 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000140-----  
1550   \*\*\*\*\*檢測結束\*\*\*\*\*  
1551   \*\*\*Pre-Screening開始\*\*\*  
1552   \*\*\*Pre-Screening結束\*\*\*  
1553   可能的攻擊方式: Label Specific Backdoor Attack  
1554   可能的target-victim 配對: ['2-0', '10-0', '13-3', '16-0']  
1555   \*\*\*Trigger Reverse Engineering開始\*\*\*  
1556 Target: 16, victim: 0, Loss: 8.1876, Acc: 0.00%, CE\_Loss: 8.19, Reg\_Loss:3158.33, Cost:0.00 best\_reg:10000000000.00 avg\_loss\_reg:3017.95: 5% | 153/1000 [04:17<1:16:46, 4.86s/it]  
1557   \*\*\*Trigger Reverse Engineering結束\*\*\*  
1558 Target Class: 2 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11  
1559   \*\*\*\*\*檢測結束\*\*\*\*\*  
1560 檢測結果: Model是安全的(Benign)  
1561 整體耗時: 287.01466703414917 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000141-----  
1562   \*\*\*\*\*檢測結束\*\*\*\*\*

```

1563 ***Pre-Screening開始***
1564 ***Pre-Screening結束***
1565 可能的攻擊方式:Label Specific Backdoor Attack
1566 可能的 target-victim 配對: ['3-20', '4-17', '19-12']
1567 ***Trigger Reverse Engineering開始***
1568 Target: 19, victim: 12, Loss: 3.7116, Acc: 100.00%, CE_Loss: 0.40, Reg_Loss: 193.74, Cost:0.02 best_reg:194.30 avg_loss_reg:194.98: 19%|██████████| 194/1000 [13:04<54:17, 4.04s/it]
1569 early stop 所有
1570 ***Trigger Reverse Engineering結束***
1571 Target Class: 19 Victim Class: 12 Trigger Size: 193.73573303222656 Optimization Steps: 163
1572 ***Symmetric Check開始***
1573 Target: 12, victim: 19, Loss: 1.5044, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:6376.17, Cost:0.00 best_reg:6496.78 avg_loss_reg:6496.78: 100%|██████████| 163/163 [10:49<00:00, 3.99s/it]

1574 ***Symmetric Check結束***
1575 *****檢測結果: Model含有後門(Abnormal)
1576 整體耗時: 1456.4605922698975
1577 檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000142-----
1578 *****Pre-Screening開始***
1579 *****Pre-Screening結束***
1580 *****Pre-Screening開始***
1581 可能的攻擊方式:Label Specific Backdoor Attack
1582 可能的 target-victim 配對: ['0-3', '2-1', '2-4', '2-9', '3-0', '6-5', '6-16', '8-1', '8-5', '9-5', '10-5', '11-4', '17-0']
1583 ***Trigger Reverse Engineering開始***
1584 Target: 2, victim: 1, Loss: 2.1220, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:4378.35, Cost:0.00 best_reg:4382.39 avg_loss_reg:4424.00: 60%|████| 597/1000 [30:17<20:26, 3.04s/it]
1585 early stop 所有
1586 ***Trigger Reverse Engineering結束***
1587 Target Class: 2 Victim Class: 1 Trigger Size: 4378.3525390625 Optimization Steps: 425
1588 *****檢測結果: Model是安全的(Benign)
1589 檢測結果: Model是安全的(Benign)
1590 整體耗時: 1844.2108731269836
1591 檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000143-----
1592 *****Pre-Screening開始***
1593 *****Pre-Screening結束***
1594 可能的攻擊方式:Label Specific Backdoor Attack
1595 可能的 target-victim 配對: ['0-5', '1-3', '7-6']
1596 ***Trigger Reverse Engineering開始***
1597 Target: 1, victim: 3, Loss: 3.5995, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:1479.17, Cost:0.00 best_reg:1479.24 avg_loss_reg:1479.24: 24%|████| 237/1000 [01:29<04:49, 2.63it/s]
1598 early stop 所有
1599 ***Trigger Reverse Engineering結束***
1600 Target Class: 3 Victim Class: 3 Trigger Size: 1479.166748046875 Optimization Steps: 205
1601 *****檢測結果: Model是安全的(Benign)
1602 檢測結果: Model是安全的(Benign)
1603 整體耗時: 97.24881386756897
1604 檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000144-----
1605 *****Pre-Screening開始***
1606 *****Pre-Screening結束***
1607 *****檢測結果: Model是安全的(Benign)
1608 檢測結果: Model是安全的(Benign)
1609 整體耗時: 2.788980722427368
1610 檢測結果: Model是安全的(Benign)
1611 *****Pre-Screening開始***
1612 *****Pre-Screening結束***
1613 *****檢測結果: Model是安全的(Benign)
1614 檢測結果: Model是安全的(Benign)
1615 整體耗時: 9.539626121520996
1616 檢測結果: Model是安全的(Benign)
1617 *****Pre-Screening開始***
1618 *****Pre-Screening結束***
1619 *****檢測結果: Model是安全的(Benign)
1620 檢測結果: Model是安全的(Benign)
1621 整體耗時: 9.664697885513306
1622 檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000147-----
1623 *****Pre-Screening開始***
1624 *****Pre-Screening結束***
1625 *****檢測結果: Model是安全的(Benign)
1626 檢測結果: Model是安全的(Benign)
1627 整體耗時: 19.98484516143799
1628 檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000148-----
1629 *****Pre-Screening開始***
1630 *****Pre-Screening結束***
1631 可能的攻擊方式:Label Specific Backdoor Attack
1632 可能的 target-victim 配對: ['0-18', '7-10', '11-16', '15-16', '17-16']
1633 ***Trigger Reverse Engineering開始***

```

```

1634 Target: 17, victim: 16, Loss: 9.7743, Acc: 0.00%, CE_Loss: 9.77, Reg_Loss:2534.12, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2521.15: 7% | 74/1000 [05:44<1:151, 4.66s/it]

1635 ***Trigger Reverse Engineering結束***
1636 Target Class: 0 Victim Class: 18 Trigger Size: 1000000000.0 Optimization Steps: 21
1637 ***檢測結果: Model是安全的(Benign)
1638 檢測結果: Model是安全的(Benign)
1639 整體耗時: 373.0696756839752
1640 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000149
1641 ***Pre-Screening開始***
1642 ***Pre-Screening結束***
1643 ***檢測結果: Model是安全的(Benign)
1644 檢測結果: Model是安全的(Benign)
1645 整體耗時: 9.46427845954895
1646 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000150
1647 ***Pre-Screening開始***
1648 ***Pre-Screening結束***
1649 ***檢測結果: Model是安全的(Benign)
1650 檢測結果: Model是安全的(Benign)
1651 整體耗時: 6.986953973770142
1652 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000151
1653 ***Pre-Screening開始***
1654 ***Pre-Screening結束***
1655 ***檢測結果: Model是安全的(Benign)
1656 檢測結果: Model是安全的(Benign)
1657 整體耗時: 2.916640043258667
1658 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000152
1659 ***Pre-Screening開始***
1660 ***Pre-Screening結束***
1661 ***檢測結果: Model是安全的(Benign)
1662 檢測結果: Model是安全的(Benign)
1663 整體耗時: 7.358924388885498
1664 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000153
1665 ***Pre-Screening開始***
1666 ***Pre-Screening結束***
1667 可能的攻擊方式: Universal Backdoor Attack
1668 可能的 target class: 19
1669 可能的 victim classes: ALL
1670 ***Trigger Reverse Engineering開始***
1671 Target: 19, victim: 22, Loss: 0.4862, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:1641.07, Cost:0.00 best_reg:1636.47 avg_loss_reg:1614.44: 6% | 62/1000 [09:27<2:23:09, 9.16s/it]
1672 early stop 所有
1673 ***Trigger Reverse Engineering結束***
1674 Target Class: 19 Victim Class: all Trigger Size: 1636.4735026041667 Optimization Steps: 63
1675 -----檢測結果: Model含有後門(Abnormal)
1676 整體耗時: 580.8192658424377
1677 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000154
1678 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000155
1679 ***Pre-Screening開始***
1680 ***Pre-Screening結束***
1681 ***檢測結果: Model是安全的(Benign)
1682 檢測結果: Model是安全的(Benign)
1683 整體耗時: 3.025019407272339
1684 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000156
1685 ***Pre-Screening開始***
1686 ***Pre-Screening結束***
1687 ***檢測結果: Model是安全的(Benign)
1688 檢測結果: Model是安全的(Benign)
1689 整體耗時: 11.072980403900146
1690 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000157
1691 ***Pre-Screening開始***
1692 ***Pre-Screening結束***
1693 可能的攻擊方式: Label Specific Backdoor Attack
1694 可能的 target-victim 配對: ['0-12', '2-5', '4-8', '4-10', '6-10', '10-6']
1695 ***Trigger Reverse Engineering開始***
1696 Target: 10, victim: 6, Loss: 7.3118, Acc: 20.00%, CE_Loss: 7.31, Reg_Loss:2981.55, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2887.85: 10% | 95/1000 [00:10<01:38, 9.21s/it]
1697 ***Trigger Reverse Engineering結束***
1698 Target Class: 0 Victim Class: 12 Trigger Size: 1000000000.0 Optimization Steps: 21
1699 -----檢測結果: Model是安全的(Benign)
1700 整體耗時: 18.173159993042
1701 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000157
1702 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000158
1703 ***Pre-Screening開始***
1704 ***Pre-Screening結束***

```

```

1705 ***檢測結束***  

1706 檢測結果: Model是安全的(Benign)  

1707 整體耗時: 12.449477434158325  

1708 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000158-----  

1709 ***Pre-Screening開始***  

1710 ***Pre-Screening結束***  

1711 可能的攻擊方式: Label Specific Backdoor Attack  

1712 可能的 target-victim 配對: ['4-0']  

1713 ***Trigger Reverse Engineering開始***  

1714 Target: 4, victim: 0, Loss: 10.9118, Acc: 0.00%, CE_Loss: 10.91, Reg_Loss:2565.98, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2547.86: 1%| | 10/1000 [00:04<07:55, 2.08it/s]  

1715 ***Trigger Reverse Engineering結束***  

1716 Target Class: 4 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 11  

1717 *****檢測結束*****  

1718 檢測結果: Model是安全的(Benign)  

1719 整體耗時: 12.4471770286560059  

1720 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000159-----  

1721 ***Pre-Screening開始***  

1722 ***Pre-Screening結束***  

1723 可能的攻擊方式: Label Specific Backdoor Attack  

1724 可能的 target-victim 配對: ['8-5']  

1725 ***Trigger Reverse Engineering開始***  

1726 Target: 8, victim: 5, Loss: 1.4055, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:54.59, Cost:0.03 best_reg:56.84 avg_loss_reg:56.84: 10%| | 102/1000 [05:05<44:53, 3.00s/it]  

1727 early stop 所有  

1728 ***Trigger Reverse Engineering結束***  

1729 Target Class: 8 Victim Class: 5 Trigger Size: 54.58509826660156 Optimization Steps: 103  

1730 ***Symmetric Check開始***  

1731 Target: 5, victim: 8, Loss: 0.8852, Acc: 100.00%, CE_Loss: 0.75, Reg_Loss:3463.38, Cost:0.00 best_reg:3247.45 avg_loss_reg:3441.00: 100%| | 103/103 [05:12<00:00, 3.03s/it]  

1732 ***Symmetric Check結束***  

1733 *****檢測結束*****  

1734 檢測結果: Model含有後門 (Abnormal)  

1735 整體耗時: 635.8410024642944  

1736 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000160-----  

1737 ***Pre-Screening開始***  

1738 ***Pre-Screening結束***  

1739 可能的攻擊方式: Label Specific Backdoor Attack  

1740 可能的 target-victim 配對: ['2-12', '7-4']  

1741 ***Trigger Reverse Engineering開始***  

1742 Target: 7, victim: 4, Loss: 9.6687, Acc: 5.00%, CE_Loss: 9.67, Reg_Loss:4071.68, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:3698.69: 3%| | 31/1000 [00:09<04:56, 3.27it/s]  

1743 ***Trigger Reverse Engineering結束***  

1744 Target Class: 2 Victim Class: 12 Trigger Size: 1000000000.0 Optimization Steps: 11  

1745 *****檢測結束*****  

1746 檢測結果: Model是安全的(Benign)  

1747 整體耗時: 19.9996350288391113  

1748 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000161-----  

1749 ***Pre-Screening開始***  

1750 ***Pre-Screening結束***  

1751 ***檢測結束***  

1752 檢測結果: Model是安全的(Benign)  

1753 整體耗時: 6.556492328643799  

1754 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000162-----  

1755 ***Pre-Screening開始***  

1756 ***Pre-Screening結束***  

1757 ***檢測結束***  

1758 檢測結果: Model是安全的(Benign)  

1759 整體耗時: 11.457389116287231  

1760 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000163-----  

1761 ***Pre-Screening開始***  

1762 ***Pre-Screening結束***  

1763 可能的攻擊方式: Label Specific Backdoor Attack  

1764 可能的 target-victim 配對: ['0-10', '7-6', '10-2']  

1765 ***Trigger Reverse Engineering開始***  

1766 Target: 0, victim: 10, Loss: 4.4090, Acc: 100.00%, CE_Loss: 0.34, Reg_Loss:804.56, Cost:0.01 best_reg:806.51 avg_loss_reg:806.51: 17%| | 169/1000 [09:58<49:03, 3.54s/it]  

1767 0%| | 0/138 [00:00<?, ?it/s]early stop 所有  

1768 ***Trigger Reverse Engineering結束***  

1769 Target Class: 0 Victim Class: 10 Trigger Size: 804.5567626953125 Optimization Steps: 138  

1770 ***Symmetric Check開始***  

1771 Target: 10, victim: 0, Loss: 3.4626, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:655.82, Cost:0.01 best_reg:657.53 avg_loss_reg:657.53: 100%| | 138/138 [08:05<00:00, 3.52s/it]  

1772 ***Symmetric Check結束***  

1773 *****檢測結束*****  

1774 檢測結果: Model是安全的(Benign)  

1775 整體耗時: 1099.481012582779

```

File - main -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000164-----

1776     \*\*\*Pre-Screening開始\*\*\*  
 1777     \*\*\*Pre-Screening結束\*\*\*  
 1778     \*\*\*Pre-Screening結束\*\*\*  
 1779     可能的攻擊方式: Universal Backdoor Attack  
 1780     可能的 target class: 18  
 1781     可能的 victim classes: ALL  
 1782     \*\*\*Trigger Reverse Engineering開始\*\*\*  
 1783     Target: 18, victim: 22, Loss: 0.3491, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss: 784.08, Cost:0.00 best\_reg:777.31 avg\_loss\_reg:769.15: 16% █ | 160/1000 [42:20 <3:42:17, 15.88it/s]  
 1784     early stop 所有  
 1785     \*\*\*Trigger Reverse Engineering結束\*\*\*  
 1786     Target Class: 18 Victim Class: all Trigger Size: 777.3056869506836 Optimization Steps: 161  
 1787     \*\*\*\*\*檢測結果\*\*\*\*\*  
 1788     檢測結果: Model含有所謂後門(Abnormal)  
 1789     整體耗時: 2552.3722443580627  
 1790     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000165-----  
 1791     \*\*\*Pre-Screening開始\*\*\*  
 1792     \*\*\*Pre-Screening結束\*\*\*  
 1793     可能的攻擊方式: Label Specific Backdoor Attack  
 1794     可能的 target-victim 配對: ['9-4']  
 1795     \*\*\*Trigger Reverse Engineering開始\*\*\*  
 1796     Target: 9, victim: 4, Loss: 9.1343, Acc: 0.00%, CE\_Loss: 9.13, Reg\_Loss: 2595.83, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:2574.84: 1% | | 10/1000 [00:02 <04:25, 3.73it/s]  
 1797     \*\*\*Trigger Reverse Engineering結束\*\*\*  
 1798     Target Class: 9 Victim Class: 4 Trigger Size: 1000000000.0 Optimization Steps: 11  
 1799     \*\*\*\*\*檢測結果\*\*\*\*\*  
 1800     檢測結果: Model是安全的(Benign)  
 1801     整體耗時: 10.258039712905884  
 1802     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000166-----  
 1803     \*\*\*Pre-Screening開始\*\*\*  
 1804     \*\*\*Pre-Screening結束\*\*\*  
 1805     \*\*\*檢測結果\*\*\*  
 1806     檢測結果: Model是安全的(Benign)  
 1807     整體耗時: 11.502660512924194  
 1808     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000167-----  
 1809     \*\*\*Pre-Screening開始\*\*\*  
 1810     \*\*\*Pre-Screening結束\*\*\*  
 1811     \*\*\*檢測結果\*\*\*  
 1812     檢測結果: Model是安全的(Benign)  
 1813     整體耗時: 11.112302780151367  
 1814     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000168-----  
 1815     \*\*\*Pre-Screening開始\*\*\*  
 1816     \*\*\*Pre-Screening結束\*\*\*  
 1817     \*\*\*檢測結果\*\*\*  
 1818     檢測結果: Model是安全的(Benign)  
 1819     整體耗時: 10.316439151763916  
 1820     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000169-----  
 1821     \*\*\*Pre-Screening開始\*\*\*  
 1822     \*\*\*Pre-Screening結束\*\*\*  
 1823     \*\*\*檢測結果\*\*\*  
 1824     檢測結果: Model是安全的(Benign)  
 1825     整體耗時: 6.106948614120483  
 1826     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000170-----  
 1827     \*\*\*Pre-Screening開始\*\*\*  
 1828     \*\*\*Pre-Screening結束\*\*\*  
 1829     可能的攻擊方式: Label Specific Backdoor Attack  
 1830     可能的 target-victim 配對: ['2-0']  
 1831     \*\*\*Trigger Reverse Engineering開始\*\*\*  
 1832     Target: 2, victim: 0, Loss: 0.7838, Acc: 100.00%, CE\_Loss: 0.17, Reg\_Loss: 916.85, Cost:0.00 best\_reg:919.26 avg\_loss\_reg:920.08: 38% █ | | 377/1000 [03:58 <06:33, 1.58it/s]  
 1833     early stop 所有  
 1834     \*\*\*Trigger Reverse Engineering結束\*\*\*  
 1835     Target Class: 0 Victim Class: 0 Trigger Size: 916.8477783203125 Optimization Steps: 378  
 1836     \*\*\*Symmetric Check開始\*\*\*  
 1837     Target: 0, victim: 2, Loss: 1.5438, Acc: 100.00%, CE\_Loss: 0.22, Reg\_Loss: 6714.46, Cost:0.00 best\_reg:6733.06 avg\_loss\_reg:6702.65: 100% █ | | 378/378 [03:58 <00:00, 1.58it/s]  
 1838     \*\*\*Symmetric Check結束\*\*\*  
 1839     \*\*\*\*\*檢測結果\*\*\*\*\*  
 1840     檢測結果: Model是安全的(Benign)  
 1841     整體耗時: 484.760906457901  
 1842     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000171-----  
 1843     \*\*\*Pre-Screening開始\*\*\*  
 1844     \*\*\*Pre-Screening結束\*\*\*  
 1845     \*\*\*檢測結果\*\*\*  
 1846     檢測結果: Model是安全的(Benign)

1847 整體耗時: 9.399004220962524 執描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000172  
1848 \*\*\*Pre-Screening開始\*\*\*  
1849 \*\*\*Pre-Screening結束\*\*\*  
1850 \*\*\*Pre-Screening開始\*\*\*  
1851 \*\*\*檢測結束\*\*\*  
1852 檢測結果: Model是安全的(Benign)  
1853 整體耗時: 11.118836164474487 執描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000173  
1854 \*\*\*Pre-Screening開始\*\*\*  
1855 \*\*\*Pre-Screening結束\*\*\*  
1856 \*\*\*Pre-Screening開始\*\*\*  
1857 \*\*\*檢測結束\*\*\*  
1858 檢測結果: Model是安全的(Benign)  
1859 整體耗時: 3.993023157119751 執描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000174  
1860 \*\*\*Pre-Screening開始\*\*\*  
1861 \*\*\*Pre-Screening結束\*\*\*  
1862 \*\*\*Pre-Screening開始\*\*\*  
1863 \*\*\*檢測結束\*\*\*  
1864 檢測結果: Model是安全的(Benign)  
1865 整體耗時: 6.443248748779297 執描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000175  
1866 \*\*\*Pre-Screening開始\*\*\*  
1867 \*\*\*Pre-Screening結束\*\*\*  
1868 \*\*\*Pre-Screening開始\*\*\*  
1869 \*\*\*檢測結束\*\*\*  
1870 檢測結果: Model是安全的(Benign)  
1871 整體耗時: 9.17429494857788 執描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000176  
1872 \*\*\*Pre-Screening開始\*\*\*  
1873 \*\*\*Pre-Screening結束\*\*\*  
1874 \*\*\*Pre-Screening開始\*\*\*  
1875 \*\*\*檢測結束\*\*\*  
1876 檢測結果: Model是安全的(Benign)  
1877 整體耗時: 9.700076580047607 執描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000177  
1878 \*\*\*Pre-Screening開始\*\*\*  
1879 \*\*\*Pre-Screening結束\*\*\*  
1880 \*\*\*Pre-Screening開始\*\*\*  
1881 可能的攻擊方式: Universal Backdoor Attack  
1882 可能的 target class: 5  
1883 可能的 victim classes: ALL  
1884 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1885 Target: 5; victim: 6; Loss: 0.1988; Acc: 100.00%; CE\_Loss: 0.00; Reg\_Loss: 670.80; Cost: 0.00 best\_Reg: 664.12 avg\_Loss\_Reg: 669.98; 13% █ | 133/1000 [33:56<3:41:18, 15.3 s/it]  
1886 early stop 所有  
1887 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1888 Target Class: 5 Victim Class: all Trigger Size: 664.1233984375 Optimization Steps: 134  
1889 \*\*\*檢測結束\*\*\*  
1890 檢測結果: Model含有後門(ABnormal)  
1891 整體耗時: 2049.607510328293 執描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000178  
1892 \*\*\*Pre-Screening開始\*\*\*  
1893 \*\*\*Pre-Screening結束\*\*\*  
1894 \*\*\*Pre-Screening開始\*\*\*  
1895 \*\*\*檢測結束\*\*\*  
1896 檢測結果: Model是安全的(Benign)  
1897 整體耗時: 2.6641976833343506 執描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000179  
1898 \*\*\*Pre-Screening開始\*\*\*  
1899 \*\*\*Pre-Screening結束\*\*\*  
1900 \*\*\*Pre-Screening開始\*\*\*  
1901 \*\*\*檢測結束\*\*\*  
1902 檢測結果: Model是安全的(Benign)  
1903 整體耗時: 16.523897886276245 執描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000180  
1904 \*\*\*Pre-Screening開始\*\*\*  
1905 \*\*\*Pre-Screening開始\*\*\*  
1906 \*\*\*Pre-Screening結束\*\*\*  
1907 可能的攻擊方式: Label Specific Backdoor Attack  
1908 可能的 target-victim 配對: ['0-1', '0-2', '6-5']  
1909 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1910 Target: 0; victim: 2; Loss: 2.4812; Acc: 100.00%; CE\_Loss: 0.15; Reg\_Loss: 690.61; Cost: 0.00 best\_Reg: 695.37 avg\_Loss\_Reg: 695.37: 25% █ | 251/1000 [14:18<42:41, 3.42s/it]  
1911 0% | 0/178 [0:00<?, ?it/s]early stop 所有  
1912 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1913 Target Class: 0 Victim Class: 2 Trigger Size: 690.6088671875 Optimization Steps: 178  
1914 \*\*\*Symmetric Check開始\*\*\*  
1915 Target: 2; victim: 0; Loss: 0.8426; Acc: 60.00%; CE\_Loss: 0.84; Reg\_Loss: 14700.95; Cost: 0.00 best\_Reg: 1000000000.00 avg\_Loss\_Reg: 14688.43; 100% █ | 178/178 [10:06<00:00, 3.41s/t]  
1916 \*\*\*Symmetric Check結束\*\*\*  
1917 \*\*\*檢測結束\*\*\*

```

1918 檢測結果: Model含有後門(Abnormal)
1919 整體耗時: 1477.6634047031403
1920 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000181-----
1921 ***Pre-Screening開始***
1922 ***Pre-Screening結束***
1923 可能的攻擊方式: Label Specific Backdoor Attack
1924 可能的 target-victim 配對: ['2-5', '2-14', '4-7', '5-14', '10-7', '15-14']
1925 ***Trigger Reverse Engineering開始***
1926 Target: 2, victim: 14, Loss: 2.0464, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss: 33.64, Cost: 0.06 best_reg: 35.25 avg_loss_reg: 33.22: 15% █ | 148/1000 [04:46<27:28, 1.93s/it]
1927 early stop 所有
1928 ***Trigger Reverse Engineering結束***
1929 Target Class: 2 Victim Class: 14 Trigger Size: 33.63653564453125 Optimization Steps: 69
1930 ***Symmetric Check開始***
1931 Target: 14, victim: 2, Loss: 7.8493, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss: 7527.38, Cost: 0.00 best_reg: 8052.60 avg_loss_reg: 8144.33: 100% █ | 69/69 [02:12<00:00, 1.92s/it]
1932 ***Symmetric Check結束***
1933 *****檢測結束*****檢測結束*****
1934 檢測結果: Model含有後門(Abnormal)
1935 整體耗時: 434.2893204689026
1936 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000182-----
1937 ***Pre-Screening開始***
1938 ***Pre-Screening結束***
1939 ***檢測結果: Model是安全的(Benign)
1940 整體耗時: 18.2300083465576172
1941 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000183-----
1942 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000184-----
1943 ***Pre-Screening開始***
1944 ***Pre-Screening結束***
1945 可能的攻擊方式: Label Specific Backdoor Attack
1946 可能的 target-victim 配對: ['0-17', '1-12', '1-20', '1-21', '2-0', '2-11', '2-10', '3-2', '4-5', '4-9', '4-12', '5-12', '6-8', '6-11', '6-12', '7-18', '8-6', '8-9', '8-11', '9-8', '9-11', '11-8', '11-10', '11-19', '13-10', '17-0', '18-1', '18-7', '19-2', '20-21', '21-1', '21-12', '21-11']
1947 ***Trigger Reverse Engineering開始***
1948 Target: 21, victim: 11, Loss: 2.2823, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss: 425.56, Cost: 0.01 best_reg: 427.07 avg_loss_reg: 427.07: 68% █ | 156/1000 [36:52<17:35, 3.27s/it]
1949 early stop 所有
1950 ***Trigger Reverse Engineering結束***
1951 Target Class: 21 Victim Class: 11 Trigger Size: 425.5569763183594 Optimization Steps: 156
1952 ***Symmetric Check開始***
1953 Target: 11, victim: 21, Loss: 0.9748, Acc: 70.00%, CE_Loss: 0.97, Reg_Loss: 22108.08, Cost: 0.00 best_reg: 10000000000.00 avg_loss_reg: 22042.08: 100% █ | 156/156 [08:34<00:00, 3.30s/it]
1954 ***Symmetric Check結束***
1955 檢測結果: Model含有後門(Abnormal)
1956 整體耗時: 2747.7031893730164
1957 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000184-----
1958 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000185-----
1959 ***Pre-Screening開始***
1960 ***Pre-Screening結束***
1961 ***檢測結果: Model是安全的(Benign)
1962 整體耗時: 13.955691814422607
1963 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000186-----
1964 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000187-----
1965 ***Pre-Screening開始***
1966 ***Pre-Screening結束***
1967 ***檢測結果: Model是安全的(Benign)
1968 整體耗時: 7.551476240158081
1969 檢測結果: Model是安全的(Benign)
1970 整體耗時: 6.198354005813599
1971 ***Pre-Screening開始***
1972 ***Pre-Screening結束***
1973 ***檢測結果: Model是安全的(Benign)
1974 檢測結果: Model是安全的(Benign)
1975 整體耗時: 6.198354005813599
1976 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000187-----
1977 ***Pre-Screening開始***
1978 ***Pre-Screening結束***
1979 可能的攻擊方式: Label Specific Backdoor Attack
1980 可能的 target-victim 配對: ['1-20', '3-8', '3-6', '3-15', '4-13', '4-20', '6-3', '8-6', '9-3', '9-6', '9-11', '10-11', '10-12', '11-3', '11-8', '11-12', '13-1', '14-13', '15-3', '15-6', '16-13', '16-20', '20-11']
1981 ***Trigger Reverse Engineering開始***
1982 Target: 20, victim: 1, Loss: 1.0046, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss: 737.39, Cost: 0.00 best_reg: 740.88 avg_loss_reg: 740.88: 54% █ | 541/1000 [01:10<00:59, 7.70it/s]
1983 early stop 所有
1984 ***Trigger Reverse Engineering結束***
1985 Target Class: 20 Victim Class: 1 Trigger Size: 737.390625 Optimization Steps: 178
1986 ***Symmetric Check開始***
1987 Target: 1, victim: 20, Loss: 0.9989, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss: 317.94, Cost: 0.00 best_reg: 310.50 avg_loss_reg: 318.45: 100% █ | 178/178 [00:26<00:00, 6.74it/s]
1988 ***Symmetric Check結束***

```

1989 \*\*\*\*\*檢測結束\*\*\*\*\*  
1990 檢測結果: Model是安全的(Benign)  
1991 整體耗時: 104.3275701996643  
1992 \*\*\*\*\*Pre-Screening開始\*\*\*\*\*  
1993 \*\*\*Pre-Screening結束\*\*\*  
1994 可能的攻擊方式: Label Specific Backdoor Attack  
1995 可能的target-victim 配對: ['0-7', '1-3', '2-1', '2-9', '4-5', '4-12', '5-12', '7-0', '9-1', '9-3', '9-6', '13-14', '15-14']  
1996 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1997 Target: 13, victim: 14, Loss: 1.2788, Acc: 100.00%, CE\_Loss: 0.18, Reg\_Loss: 1096.02, Cost:0.00 best\_reg:1096.28 avg\_loss\_reg:1082.27: 72% █ | 723/1000 [23:35<09:02, 1.96s/it]  
1998 Target Class: 13 Victim Class: 14 Trigger Size: 1096.019775390625 Optimization Steps: 526  
1999 early stop 所有  
2000 \*\*\*Trigger Reverse Engineering結束\*\*\*  
2001 Target Class: 13 Victim Class: 14 Trigger Size: 1096.019775390625 Optimization Steps: 526  
2002 \*\*\*\*\*檢測結束\*\*\*\*\*  
2003 檢測結果: Model是安全的(Benign)  
2004 整體耗時: 1430.7862091064453  
2005 \*\*\*\*\*Pre-Screening開始\*\*\*\*\*  
2006 \*\*\*Pre-Screening結束\*\*\*  
2007 \*\*\*Pre-Screening結束\*\*\*  
2008 可能的攻擊方式: Label Specific Backdoor Attack  
2009 可能的 target-victim 配對: ['0-3', '0-18']  
2010 \*\*\*Trigger Reverse Engineering開始\*\*\*  
2011 Target: 0, victim: 18, Loss: 1.7949, Acc: 100.00%, CE\_Loss: 0.01, Reg\_Loss: 13.74, Cost:0.13 best\_Reg:15.65 avg\_loss\_Reg:15.65: 10% █ | 97/1000 [00:18<02:56, 5.12it/s]  
2012 early stop 所有  
2013 \*\*\*Trigger Reverse Engineering結束\*\*\*  
2014 Target Class: 0 Victim Class: 18 Trigger Size: 13.73945426940918 Optimization Steps: 77  
2015 \*\*\*Symmetric Check開始\*\*\*  
2016 Target: 18, victim: 0, Loss: 5.0626, Acc: 90.00%, CE\_Loss: 0.26, Reg\_Loss: 4806.15, Cost:0.00 best\_Reg:7334.80 avg\_loss\_Reg:5236.66: 100% █ | 77/77 [00:15<00:00, 5.04it/s]  
2017 \*\*\*Symmetric Check結束\*\*\*  
2018 \*\*\*\*\*檢測結束\*\*\*\*\*  
2019 檢測結果: Model含有後門(Abnormal)  
2020 整體耗時: 48.667075634002686  
2021 \*\*\*\*\*Pre-Screening結束\*\*\*\*\*  
2022 \*\*\*\*\*Pre-Screening開始\*\*\*\*\*  
2023 \*\*\*Pre-Screening結束\*\*\*  
2024 可能的攻擊方式: Label Specific Backdoor Attack  
2025 可能的 target-victim 配對: ['1-9', '7-8', '8-10', '10-8']  
2026 \*\*\*Trigger Reverse Engineering開始\*\*\*  
2027 Target: 10, victim: 8, Loss: 2.3022, Acc: 100.00%, CE\_Loss: 0.18, Reg\_Loss: 82.88, Cost:0.03 best\_Reg:83.56 avg\_loss\_Reg:82.70: 17% █ | 167/1000 [09:26<47:04, 3.39s/it]  
2028 early stop 所有  
2029 \*\*\*Trigger Reverse Engineering結束\*\*\*  
2030 Target Class: 10 Victim Class: 8 Trigger Size: 82.87805938720703 Optimization Steps: 125  
2031 \*\*\*Symmetric Check開始\*\*\*  
2032 Target: 8, victim: 10, Loss: 4.7076, Acc: 75.00%, CE\_Loss: 0.62, Reg\_Loss: 9203.32, Cost:0.00 best\_Reg:16200.26 avg\_loss\_Reg:9537.62: 100% █ | 125/125 [06:54<00:00, 3.31s/it]  
2033 \*\*\*Symmetric Check結束\*\*\*  
2034 \*\*\*\*\*檢測結束\*\*\*\*\*  
2035 檢測結果: Model含有後門(Abnormal)  
2036 整體耗時: 1000.4495198726654  
2037 \*\*\*\*\*Pre-Screening結束\*\*\*\*\*  
2038 \*\*\*Pre-Screening開始\*\*\*\*\*  
2039 \*\*\*Pre-Screening結束\*\*\*  
2040 可能的攻擊方式: Label Specific Backdoor Attack  
2041 可能的 target-victim 配對: ['0-1', '0-6', '0-15', '1-15', '2-17', '3-2', '3-5', '5-17', '6-1', '6-4', '6-19', '7-19', '8-6', '10-4', '10-13', '11-10', '11-15', '12-13', '12-17', '13-10', '16-9', '16-0', '16-10', '16-18', '17-12', '17-1', '17-2', '18-6', '19-4', '20-12', '20-13', '21-4', '22-1', '22-4', '22-6']  
2042 \*\*\*Trigger Reverse Engineering開始\*\*\*  
2043 Target: 7, victim: 14, Loss: 2.8302, Acc: 100.00%, CE\_Loss: 0.43, Reg\_Loss: 711.31, Cost:0.00 best\_Reg:711.46 avg\_loss\_Reg:708.78: 65% █ | 650/1000 [10:15<05:31, 1.06it/s]  
2044 early stop 所有  
2045 \*\*\*Trigger Reverse Engineering結束\*\*\*  
2046 Target Class: 7 Victim Class: 14 Trigger Size: 711.3124389648438 Optimization Steps: 235  
2047 \*\*\*Symmetric Check開始\*\*\*  
2048 Target: 14, victim: 7, Loss: 2.3942, Acc: 100.00%, CE\_Loss: 0.39, Reg\_Loss: 4502.24, Cost:0.00 best\_Reg:4448.60 avg\_loss\_Reg:4500.33: 100% █ | 235/235 [03:11<00:00, 1.23it/s]  
2049 \*\*\*Symmetric Check結束\*\*\*  
2050 \*\*\*\*\*檢測結束\*\*\*\*\*  
2051 檢測結果: Model是安全的(Benign)  
2052 整體耗時: 821.4709134101868  
2053 \*\*\*\*\*Pre-Screening開始\*\*\*\*\*  
2054 \*\*\*Pre-Screening結束\*\*\*  
2055 可能的攻擊方式: Label Specific Backdoor Attack  
2056 可能的 target-victim 配對: ['1-13', '2-1', '3-0', '3-2', '4-13', '5-0', '5-4', '5-10', '6-11', '6-12', '7-5', '7-10', '8-0', '8-10', '9-12', '9-13', '10-7', '11-6', '11-12', '12-6', '12-11', '13-1']  
2057 \*\*\*Trigger Reverse Engineering開始\*\*\*  
2058 Target: 13, victim: 1, Loss: 1.9356, Acc: 100.00%, CE\_Loss: 0.25, Reg\_Loss: 747.32, Cost:0.00 best\_Reg:747.93 avg\_loss\_Reg:747.93: 63% █ | 633/1000 [02:08<01:14, 4.94it/s]  
2059 Target Class: 13 Victim Class: 1 Trigger Size: 747.32 Optimization Steps: 526

```

2060 early stop 所有
2061 ***Trigger Reverse Engineering結束***
2062 Target Class: 13 Victim Class: 1 Trigger Size: 747.32067787109375 Optimization Steps: 383
2063 ***Symmetric Check開始***
2064 Target: 1, victim: 13, Loss: 2.0207, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:3836.43, Cost:0.00 best_reg:3832.30 avg_loss_reg:3865.17: 100%|██████████| 383/383 [01:16<00:00, 5.02it/s]
2065 ***Symmetric Check結束***
2066 *****檢測結果: Model是安全的(Benign)
2067 整體耗時: 212.6898331642151
2068 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000193-----
2069 *****Pre-Screening開始*****
2070 ***Pre-Screening結束***
2071 ***Pre-Screening結束***
2072 ***檢測結束***
2073 檢測結果: Model是安全的(Benign)
2074 整體耗時: 20.411783695220947
2075 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000194-----
2076 ***Pre-Screening開始***
2077 ***Pre-Screening結束***
2078 ***檢測結束***
2079 檢測結果: Model是安全的(Benign)
2080 整體耗時: 14.62452483177185
2081 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000195-----
2082 ***Pre-Screening開始***
2083 ***Pre-Screening結束***
2084 可能的攻擊方式: Universal Backdoor Attack
2085 可能的 target class: 7
2086 可能的 victim classes: ALL
2087 ***Trigger Reverse Engineering開始***
2088 Target: 7, victim: 6, Loss: 1.6562, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:3674.95, Cost:0.00 best_reg:3665.24 avg_loss_reg:3666.75: 16%|████| | 155/1000 [04:21<23:45, 1.69s/it]
2089 early stop 所有
2090 ***Trigger Reverse Engineering結束***
2091 Target Class: 7 Victim Class: all Trigger Size: 3664.0279134114585 Optimization Steps: 156
2092 *****檢測結束*****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000196-----
2093 檢測結果: Model是安全的(Benign)
2094 整體耗時: 265.77352237701416
2095 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000196-----
2096 ***Pre-Screening開始***
2097 ***Pre-Screening結束***
2098 可能的攻擊方式: Label Specific Backdoor Attack
2099 可能的 target-victim 配對: [0-11, '0-13', '11-0', '11-5', '11-13', '13-12']
2100 ***Trigger Reverse Engineering開始***
2101 Target: 13, victim: 12, Loss: 3.4855, Acc: 25.00%, CE_Loss: 3.49, Reg_Loss:3068.03, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2970.85: 8%|████| | 75/1000 [03:39<45:11, 2.93s/it]
2102 ***Trigger Reverse Engineering結束***
2103 Target Class: 0 Victim Class: 11 Trigger Size: 10000000000.0 Optimization Steps: 11
2104 *****檢測結束*****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000197-----
2105 檢測結果: Model是安全的(Benign)
2106 整體耗時: 240.7233336508484
2107 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000197-----
2108 ***Pre-Screening開始***
2109 ***Pre-Screening結束***
2110 ***檢測結束***
2111 檢測結果: Model是安全的(Benign)
2112 整體耗時: 10.923811912536621
2113 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000198-----
2114 ***Pre-Screening開始***
2115 ***Pre-Screening結束***
2116 可能的攻擊方式: Universal Backdoor Attack
2117 可能的 target class: 1
2118 可能的 victim classes: ALL
2119 ***Trigger Reverse Engineering開始***
2120 Target: 1, victim: 16, Loss: 4.2168, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:1249.43, Cost:0.00 best_reg:1249.23 avg_loss_reg:1249.23: 14%|████| | 135/1000 [1:16:19<8:09:05, 33.92s/it]
2121 early stop 所有
2122 ***Trigger Reverse Engineering結束***
2123 Target Class: 1 Victim Class: all Trigger Size: 1248.255042613637 Optimization Steps: 136
2124 *****檢測結束*****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000199-----
2125 檢測結果: Model含有後門(Abnormal)
2126 整體耗時: 4593.790768146515
2127 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000199-----
2128 ***Pre-Screening開始***
2129 ***Pre-Screening結束***
2130 可能的攻擊方式: Universal Backdoor Attack

```

```

2131 可能的 target class: 4
2132 可能的 victim classes: ALL
2133 ***Trigger Reverse Engineering開始***
2134 Target: 4, victim: 12, Loss: 0.6873, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:305.28, Cost:0.00 best_reg:306.10 avg_loss_reg:303.25: 14%| | 143/1000 [49.22<4:55:52, 20.71s/it]
2135 early stop 所有
2136 ***Trigger Reverse Engineering結束***
2137 Target Class: 4 Victim Class: all Trigger Size: 306.10232883029516 Optimization Steps: 144
2138 *****檢測結果: Model含有後門(Abnormal)
2139 檢測結果: Model耗時: 2974.5973365306854
2140 整體耗時: 2974.5973365306854
2141 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000200-----
2142 ***Pre-Screening開始***
2143 ***Pre-Screening結束***
2144 可能的攻擊方式: Label Specific Backdoor Attack
2145 可能的 target-victim 配對: ['19-0']
2146 ***Trigger Reverse Engineering開始***
2147 Target: 19, victim: 0, Loss: 0.4071, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:1174.83, Cost:0.00 best_reg:1175.85 avg_loss_reg:1177.57: 22%| | 215/1000 [13:28<49:13, 3.76s/it]
2148 early stop 所有
2149 ***Trigger Reverse Engineering結束***
2150 Target Class: 19 Victim Class: 0 Trigger Size: 1174.829833984375 Optimization Steps: 216
2151 *****檢測結果: Model是安全的(Benign)
2152 檢測結果: Model耗時: 835.370161533557
2153 整體耗時: 835.370161533557
2154 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000201-----
2155 ***Pre-Screening開始***
2156 ***Pre-Screening結束***
2157 ***檢測結果: Model是安全的(Benign)
2158 檢測結果: Model耗時: 19.8669332790374756
2159 整體耗時: 19.8669332790374756
2160 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000202-----
2161 ***Pre-Screening開始***
2162 ***Pre-Screening結束***
2163 可能的攻擊方式: Label Specific Backdoor Attack
2164 可能的 target-victim 配對: ['2-7', '2-9', '5-9']
2165 ***Trigger Reverse Engineering開始***
2166 Target: 2, victim: 7, Loss: 4.5071, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:828.98, Cost:0.01 best_reg:832.61 avg_loss_reg:833.69: 24%| | 241/1000 [04:38<14:36, 1.15s/it]
2167 early stop 所有
2168 ***Trigger Reverse Engineering結束***
2169 Target Class: 2 Victim Class: 7 Trigger Size: 828.98046875 Optimization Steps: 200
2170 ***Symmetric Check開始***
2171 Target: 7, victim: 2, Loss: 8.1691, Acc: 90.00%, CE_Loss: 0.64, Reg_Loss:2230.39, Cost:0.00 best_reg:2232.29: 100%| | 200/200 [03:35<00:00, 1.08s/it]
2172 ***Symmetric Check結束***
2173 ***檢測結果: Model是安全的(Benign)
2174 檢測結果: Model耗時: 504.65786504745483
2175 整體耗時: 504.65786504745483
2176 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000203-----
2177 ***Pre-Screening開始***
2178 ***Pre-Screening結束***
2179 ***檢測結果: Model是安全的(Benign)
2180 檢測結果: Model耗時: 17.48613667488098
2181 整體耗時: 17.48613667488098
2182 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000204-----
2183 ***Pre-Screening開始***
2184 ***Pre-Screening結束***
2185 可能的攻擊方式: Label Specific Backdoor Attack
2186 可能的 target-victim 配對: ['17-9']
2187 ***Trigger Reverse Engineering開始***
2188 Target: 17, victim: 9, Loss: 5.9559, Acc: 10.00%, CE_Loss: 5.96, Reg_Loss:3294.17, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:3048.43: 2%| | 20/1000 [01:06<54:08, 3.31s/it]
2189 ***Trigger Reverse Engineering結束***
2190 Target Class: 17 Victim Class: 9 Trigger Size: 1000000000.0 Optimization Steps: 21
2191 *****檢測結果: Model是安全的(Benign)
2192 檢測結果: Model耗時: 81.0947329133606
2193 整體耗時: 81.0947329133606
2194 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000205-----
2195 ***Pre-Screening開始***
2196 ***Pre-Screening結束***
2197 可能的攻擊方式: Universal Backdoor Attack
2198 可能的 target class: 9
2199 可能的 victim classes: ALL
2200 ***Trigger Reverse Engineering開始***
2201 Target: 9, victim: 9, Loss: 0.4088, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:35.54, Cost:0.01 best_reg:35.57 avg_loss_reg:35.10: 5%| | 53/1000 [01:21<24:23, 1.55s/it]
2202 -----
```

```

2202 early stop 所有
2203 ***Trigger Reverse Engineering結束***
2204 Target Class: 9 Victim Class: all Trigger Size: 35.573119163513184 Optimization Steps: 54
2205 *****檢測結果: Model含有後門(Abnormal)
2206 檢測結果: Model耗時: 88.10036444664001 整體耗時: 88.10036444664001 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000206-----
2207 ***Pre-Screening開始***
2208 ***Pre-Screening結束***
2209 可能的攻擊方式: Label Specific Backdoor Attack
2210 可能的 target-victim 配對: ['0-2', '0-15', '2-8', '2-12', '3-17', '4-14', '5-12', '6-12', '8-2', '9-2', '10-3', '11-0', '11-17', '13-3', '13-10', '13-17', '16-3']
2211 ***Trigger Reverse Engineering開始***
2212 Target: 4, victim: 14, Loss: 2.4853, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss: 1518.05, Cost:0.00 best_reg:1520.34 avg_loss_reg:1522.93: 52%|████| 519/1000 [04:49<04:27, 1.80it/s]
2213 ***Trigger Reverse Engineering結束***
2214 Target Class: 4 Victim Class: 14 Trigger Size: 1518.04931640625 Optimization Steps: 343
2215 early stop 所有
2216 ***Trigger Reverse Engineering結束***
2217 Target Class: 4 Victim Class: 14 Trigger Size: 1518.04931640625 Optimization Steps: 343
2218 *****檢測結果: Model是安全的(Benign) 整體耗時: 299.2864797115326 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000207-----
2219 *****檢測結果: Model是安全的(Benign) 整體耗時: 299.2864797115326 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000206-----
2220 ***Pre-Screening開始***
2221 ***Pre-Screening結束***
2222 可能的攻擊方式: Label Specific Backdoor Attack
2223 ***Pre-Screening開始***
2224 可能的 target-victim 配對: ['7-3'] 整體耗時: 79.0871148109436 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000208-----
2225 ***Pre-Screening結束***
2226 ***Trigger Reverse Engineering開始***
2227 Target: 7, victim: 3, Loss: 6.1714, Acc: 5.00%, CE_Loss: 6.17, Reg_Loss: 2977.46, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2889.50: 2%| 20/1000 [01:04<52:30, 3.21s/it]
2228 ***Trigger Reverse Engineering結束***
2229 Target Class: 7 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 21
2230 *****檢測結果: Model是安全的(Benign)
2231 檢測結果: Model是安全的(Benign) 整體耗時: 14.670723491859436 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000209-----
2232 ***Pre-Screening開始***
2233 ***Pre-Screening結束***
2234 ***Pre-Screening開始***
2235 ***Pre-Screening結束***
2236 ***檢測結果: Model是安全的(Benign) 整體耗時: 14.670723491859436 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000209-----
2237 檢測結果: Model是安全的(Benign) 整體耗時: 14.670723491859436 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000209-----
2238 ***Pre-Screening開始***
2239 ***檢測結果: Model是安全的(Benign) 整體耗時: 14.670723491859436 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000209-----
2240 ***Pre-Screening開始***
2241 ***Pre-Screening結束***
2242 ***檢測結果: Model是安全的(Benign) 整體耗時: 14.670723491859436 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000209-----
2243 檢測結果: Model是安全的(Benign) 整體耗時: 14.670723491859436 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000209-----
2244 檢測結果: Model是安全的(Benign) 整體耗時: 6.318421840667725 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000210-----
2245 ***Pre-Screening開始***
2246 ***Pre-Screening結束***
2247 ***Pre-Screening結束***
2248 ***檢測結果: Model是安全的(Benign) 整體耗時: 6.318421840667725 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000211-----
2249 檢測結果: Model是安全的(Benign) 整體耗時: 6.318421840667725 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000211-----
2250 檢測結果: Model是安全的(Benign) 整體耗時: 8.3533721618652344 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000212-----
2251 檢測結果: Model是安全的(Benign) 整體耗時: 8.184931755065918 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000212-----
2252 ***Pre-Screening開始***
2253 ***Pre-Screening結束***
2254 ***檢測結果: Model是安全的(Benign) 整體耗時: 8.184931755065918 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000212-----
2255 檢測結果: Model是安全的(Benign) 整體耗時: 8.184931755065918 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000212-----
2256 檢測結果: Model是安全的(Benign) 整體耗時: 8.184931755065918 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000212-----
2257 ***Pre-Screening開始***
2258 ***Pre-Screening結束***
2259 可能的攻擊方式: Label Specific Backdoor Attack
2260 可能的 target-victim 配對: ['1-3', '4-5'] 整體耗時: 8.184931755065918 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000212-----
2261 ***Trigger Reverse Engineering開始***
2262 Target: 1, victim: 3, Loss: 2.2081, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss: 899.46, Cost:0.00 best_reg:906.49 avg_loss_reg:906.49: 22%|████| 215/1000 [00:18<01:05, 11.90it/s]
2263 0%| 0/205 [00:00<?, ?it/s]early stop 所有
2264 ***Trigger Reverse Engineering結束***
2265 Target Class: 1 Victim Class: 3 Trigger Size: 899.4613037109375 Optimization Steps: 205
2266 ***Symmetric Check開始***
2267 Target: 3, victim: 1, Loss: 4.6158, Acc: 80.00%, CE_Loss: 0.49, Reg_Loss: 2788.24 avg_loss_reg:2755.98: 100%|████| 205/205 [00:16<00:00, 12.33it/s]
2268 Target: 3, victim: 1, Loss: 4.6158, Acc: 80.00%, CE_Loss: 0.49, Reg_Loss: 2753.29, Cost:0.00 best_reg:2788.24 avg_loss_reg:2755.98: 100%|████| 205/205 [00:16<00:00, 12.33it/s]
2269 ***Symmetric Check結束***
2270 檢測結果: Model是安全的(Benign) 整體耗時: 37.454235792160034
2271 檢測結果: Model是安全的(Benign) 整體耗時: 37.454235792160034

```

```

2273 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000213-----
2274 ***Pre-Screening開始****
2275 ***Pre-Screening結束****
2276 可能的攻擊方式: Label Specific Backdoor Attack
2277 可能的 target-victim 配對: ['9-4']
2278 ***Trigger Reverse Engineering開始****
2279 Target: 9, victim: 4, Loss: 4.763, Acc: 20.00%, CE_Loss: 4.76, Reg_Loss:3176.36, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2993.18: 2%| | 10/1000 [00:52<42:52, 2.62s/it]
2280 ***Trigger Reverse Engineering結束****
2281 Target Class: 9 Victim Class: 4 Trigger Size: 1000000000.0 Optimization Steps: 21
2282 *****檢測結果: Model是安全的(Benign)
2283 檢測結果: Model是安全的(Benign)
2284 整體耗時: 66.2883738081665
2285 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000214-----
2286 ***Pre-Screening開始****
2287 ***Pre-Screening結束****
2288 ***檢測結束****
2289 檢測結果: Model是安全的(Benign)
2290 整體耗時: 13.6220283589248657
2291 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000215-----
2292 ***Pre-Screening開始****
2293 ***Pre-Screening結束****
2294 ***檢測結束****
2295 檢測結果: Model是安全的(Benign)
2296 整體耗時: 16.186407804489136
2297 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000216-----
2298 ***Pre-Screening開始****
2299 ***Pre-Screening結束****
2300 ***檢測結束****
2301 檢測結果: Model是安全的(Benign)
2302 整體耗時: 6.229387998580933
2303 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000217-----
2304 ***Pre-Screening開始****
2305 ***Pre-Screening結束****
2306 ***檢測結束****
2307 檢測結果: Model是安全的(Benign)
2308 整體耗時: 6.2376015186309814
2309 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000218-----
2310 ***Pre-Screening開始****
2311 ***Pre-Screening結束****
2312 ***檢測結束****
2313 檢測結果: Model是安全的(Benign)
2314 整體耗時: 2.434854507446289
2315 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000219-----
2316 ***Pre-Screening開始****
2317 ***Pre-Screening結束****
2318 可能的攻擊方式: Label Specific Backdoor Attack
2319 可能的 target-victim 配對: ['6-0']
2320 ***Trigger Reverse Engineering開始****
2321 Target: 6, victim: 0, Loss: 6.9811, Acc: 0.00%, CE_Loss: 6.98, Reg_Loss:2589.08, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2567.88: 1%| | 10/1000 [00:35<59:10, 3.59s/it]
2322 ***Trigger Reverse Engineering結束****
2323 Target Class: 6 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 11
2324 *****檢測結果: Model是安全的(Benign)
2325 檢測結果: Model是安全的(Benign)
2326 整體耗時: 50.39560651779175
2327 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000220-----
2328 ***Pre-Screening開始****
2329 ***Pre-Screening結束****
2330 ***檢測結束****
2331 檢測結果: Model是安全的(Benign)
2332 整體耗時: 6.060251951217651
2333 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000221-----
2334 ***Pre-Screening開始****
2335 ***Pre-Screening結束****
2336 ***檢測結束****
2337 檢測結果: Model是安全的(Benign)
2338 整體耗時: 21.524623155593872
2339 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000222-----
2340 ***Pre-Screening開始****
2341 ***Pre-Screening結束****
2342 ***檢測結束****
2343 檢測結果: Model是安全的(Benign)

```

```

2344 整體耗時: 10.246219158172607 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000223-----
2345 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000223-----
2346 可能的攻擊方式: Label Specific Backdoor Attack
2347 可能的target-victim 配對: ['9-5', '13-6']
2348 可能的攻擊方式: Label Specific Backdoor Attack
2349 可能的 target-victim 配對: ['9-5', '13-6']
2350 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000224-----
2351 Target: 13, victim: 6, Loss: 9.3001, Acc: 0.00%, CE_Loss: 9.30, Reg_Loss:2572.66, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2558.02: 2%| | 21/1000 [00:23<18:09, 1.11s/it]
2352 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000224-----
2353 Target Class: 9 Victim Class: 5 Trigger Size: 1000000000.0 Optimization Steps: 11
2354 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000224-----
2355 檢測結果: Model是安全的(Benign)
2356 整體耗時: 32.411505937576294-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000224-----
2357 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000224-----
2358 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000224-----
2359 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000224-----
2360 可能的攻擊方式: Label Specific Backdoor Attack
2361 可能的 target-victim 配對: ['0-12', '11-12']
2362 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2363 Target: 11, victim: 12, Loss: 13.3322, Acc: 0.00%, CE_Loss: 13.33, Reg_Loss:2513.85, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2509.87: 2%| | 21/1000 [00:02<02:08, 7.64it/s]
2364 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2365 Target Class: 0 Victim Class: 12 Trigger Size: 1000000000.0 Optimization Steps: 11
2366 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2367 檢測結果: Model是安全的(Benign)
2368 整體耗時: 9.711946105896-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2369 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2370 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2371 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2372 ***檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2373 檢測結果: Model是安全的(Benign)
2374 整體耗時: 9.680684328079224-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2375 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2376 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2377 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2378 ***檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2379 檢測結果: Model是安全的(Benign)
2380 整體耗時: 8.77011227607727-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2381 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2382 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2383 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2384 ***檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2385 檢測結果: Model是安全的(Benign)
2386 整體耗時: 9.1478509029541-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2387 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2388 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2389 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000225-----
2390 可能的攻擊方式: Label Specific Backdoor Attack
2391 可能的 target-victim 配對: ['2-0']
2392 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000226-----
2393 Target: 2, victim: 0, Loss: 4.6806, Acc: 0.00%, CE_Loss: 4.68, Reg_Loss:2531.97, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2521.27: 1%| | 10/1000 [00:33<56:03, 3.40s/it]
2394 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000226-----
2395 Target Class: 2 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 11
2396 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000226-----
2397 檢測結果: Model是安全的(Benign)
2398 整體耗時: 42.158549308776855-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000226-----
2399 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000226-----
2400 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000226-----
2401 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000226-----
2402 ***檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000226-----
2403 檢測結果: Model是安全的(Benign)
2404 整體耗時: 16.701091766357422-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000226-----
2405 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000226-----
2406 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000226-----
2407 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000226-----
2408 可能的攻擊方式: Label Specific Backdoor Attack
2409 可能的 target-victim 配對: ['4-5']
2410 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000227-----
2411 Target: 4, victim: 5, Loss: 5.7675, Acc: 20.00%, CE_Loss: 5.77, Reg_Loss:3354.54, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:3172.22: 2%| | 120/1000 [00:02<01:48, 9.05it/s]
2412 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000227-----
2413 Target Class: 4 Victim Class: 5 Trigger Size: 1000000000.0 Optimization Steps: 21
2414 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000227-----

```

```
2415 檢測結果: Model是安全的(Benign)
2416 整體耗時: 10.612811803817749 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000231-----
2417
2418 ***Pre-Screening開始****
2419 ***Pre-Screening結束****
2420 ***檢測結束****
2421 檢測結果: Model是安全的(Benign)
2422 整體耗時: 2.4224973120269775 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000232-----
2423
2424 ***Pre-Screening開始****
2425 ***Pre-Screening結束****
2426 ***檢測結束****
2427 檢測結果: Model是安全的(Benign)
2428 整體耗時: 9.676013708114624 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000233-----
2429 ***Pre-Screening開始****
2430 ***Pre-Screening結束****
2431 ***Pre-Screening結束****
2432 ***檢測結束****
2433 檢測結果: Model是安全的(Benign)
2434 整體耗時: 7.888827085494995 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000234-----
2435
2436 ***Pre-Screening開始****
2437 ***Pre-Screening結束****
2438 可能的攻擊方式: Label Specific Backdoor Attack
2439 可能的 target-victim 配對: ['6-11']
2440 ***Trigger Reverse Engineering開始****
2441 Target: 6, victim: 11, Loss: 2.2984, Acc: 100.00%, CE_Loss: 0.33, Reg_Loss: 873.91, Cost: 0.00 best_Reg: 874.07 avg_Loss_Reg: 870.95: 29% | [REDACTED] | 294/1000 [10:34<25:22, 2.16s/it]
2442 early stop 所有
2443 ***Trigger Reverse Engineering結束****
2444 Target Class: 6 Victim Class: 11 Trigger Size: 873.9107666015625 Optimization Steps: 295
2445 ***Symmetric Check開始****
2446 Target: 11, victim: 6, Loss: 2.1714, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss: 6579.38, Cost: 0.00 best_Reg: 6557.29 avg_Loss_Reg: 6584.63: 100% | [REDACTED] | 295/295 [10:34<00:00, 2.15s/it]
2447 ***Symmetric Check結束****
2448 *****檢測結束*****
2449 檢測結果: Model是安全的(Benign)
2450 整體耗時: 1278.9124207496643 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000235-----
2451
2452 ***Pre-Screening開始****
2453 ***Pre-Screening結束****
2454 ***檢測結束****
2455 檢測結果: Model是安全的(Benign)
2456 整體耗時: 14.617265939712524 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000236-----
2457
2458 ***Pre-Screening開始****
2459 ***Pre-Screening結束****
2460 可能的攻擊方式: Label Specific Backdoor Attack
2461 可能的 target-victim 配對: ['1-5', '1-6', '6-1']
2462 ***Trigger Reverse Engineering開始****
2463 Target: 1, victim: 6, Loss: 4.2543, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss: 108.79, Cost: 0.04 best_Reg: 109.89 avg_Loss_Reg: 109.89: 13% | [REDACTED] | 132/1000 [06:39<43:47, 3.03s/it]
2464 early stop 所有
2465 ***Trigger Reverse Engineering結束****
2466 Target Class: 1 Victim Class: 6 Trigger Size: 108.79255676269531 Optimization Steps: 77
2467 ***Symmetric Check開始****
2468 Target: 6, victim: 1, Loss: 0.3218, Acc: 90.00%, CE_Loss: 0.32, Reg_Loss: 10620.24, Cost: 0.00 best_Reg: 1000000000.00 avg_Loss_Reg: 10516.87: 100% | [REDACTED] | 77/77 [03:51<00:00, 3.00s/it]
2469 ***Symmetric Check結束****
2470 *****檢測結束*****
2471 檢測結果: Model含有後門(Abnormal)
2472 整體耗時: 640.2766888141632 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000237-----
2473
2474 ***Pre-Screening開始****
2475 ***Pre-Screening結束****
2476 可能的攻擊方式: Label Specific Backdoor Attack
2477 可能的 target-victim 配對: ['3-13', '11-5', '13-3']
2478 ***Trigger Reverse Engineering開始****
2479 Target: 13, victim: 3, Loss: 7.8710, Acc: 15.00%, CE_Loss: 7.87, Reg_Loss: 3437.10, Cost: 0.00 best_Reg: 1000000000.00 avg_Loss_Reg: 3234.26: 6% | [REDACTED] | 62/1000 [00:39<09:51, 1.59it/s]
2480 ***Trigger Reverse Engineering結束****
2481 Target Class: 3 Victim Class: 13 Trigger Size: 1000000000.0 Optimization Steps: 21
2482 *****檢測結束*****
2483 檢測結果: Model是安全的(Benign)
2484 整體耗時: 49.253036975860596 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000238-----
```

```

2486 ***Pre-Screening開始***
2487 ***Pre-Screening結束***
2488 可能的攻擊方式: Label Specific Backdoor Attack
2489 可能的 target-victim 配對: ['1-6', '3-11', '6-20', '10-19', '10-21', '10-8', '17-16', '17-20', '19-20', '20-6', '20-19']
2490 ***Trigger Reverse Engineering開始***
2491 Target: 17, victim: 20, Loss: 1.5537, Acc: 100.00%, CE_Loss: 0.38, Reg_Loss: 1170.23, Cost:0.00 best_reg:1163.46 avg_loss_reg:1178.88: 100%|██████████| 1000/1000 [47.57<00:00, 2.88s/it]
2492 ***Trigger Reverse Engineering結束***
2493 Target Class: 17 Victim Class: 20 Trigger Size: 1163.456298828125 Optimization Steps: 661
2494 *****檢測結果: Model是安全的(Benign)
2495 檢測結果: Model是安全的(Benign)
2496 整體耗時: 2903.5240228176117 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000239-----
2497 *****檢測結果: Model是安全的(Benign)
2498 ***Pre-Screening開始***
2499 可能的攻擊方式: Label Specific Backdoor Attack
2500 可能的 target-victim 配對: ['1-2', '1-23', '5-23', '14-23', '22-23']
2501 可能的 target-victim 配對: ['1-2', '1-23', '5-23', '14-23', '22-23']
2502 ***Trigger Reverse Engineering開始***
2503 Target: 5, victim: 23, Loss: 2.0553, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss: 0.09, Reg_Loss:34.07, Cost:0.06 best_reg:35.86 avg_loss_reg:34.49: 19%|████| | 193/1000 [00:50<03:30, 3.83it/s]
2504 early stop 所有
2505 ***Trigger Reverse Engineering結束***
2506 Target Class: 5 Victim Class: 23 Trigger Size: 34.07093048095703 Optimization Steps: 80
2507 ***Symmetric Check開始***
2508 Target: 23, victim: 5, Loss: 0.8172, Acc: 40.00%, CE_Loss: 0.82, Reg_Loss:13663.40, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:13562.97: 100%|████| 80/80 [00:20<00:00, 3.86it/s]
2509 ***Symmetric Check結束***
2510 *****檢測結果: Model是安全的(Benign)
2511 檢測結果: Model含有後門(Abnormal)
2512 整體耗時: 82.85792303085327 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000240-----
2513 *****檢測結果: Model是安全的(Benign)
2514 ***Pre-Screening開始***
2515 ***Pre-Screening結束***
2516 *****檢測結果: Model是安全的(Benign)
2517 檢測結果: Model是安全的(Benign)
2518 整體耗時: 6.328764200210571 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000241-----
2519 *****檢測結果: Model是安全的(Benign)
2520 ***Pre-Screening開始***
2521 ***Pre-Screening結束***
2522 可能的攻擊方式: Label Specific Backdoor Attack
2523 可能的 target-victim 配對: ['0-9', '2-3', '2-9', '8-3', '8-9', '14-3', '15-9']
2524 ***Trigger Reverse Engineering開始***
2525 Target: 2, victim: 9, Loss: 0.9825, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:226.58, Cost:0.00 best_reg:226.96 avg_loss_reg:226.96: 24%|████| | 239/1000 [00:16<00:53, 14.12it/s]
2526 early stop 所有
2527 ***Trigger Reverse Engineering結束***
2528 Target Class: 2 Victim Class: 9 Trigger Size: 226.57591247558594 Optimization Steps: 153
2529 ***Symmetric Check開始***
2530 Target: 9, victim: 2, Loss: 2.3870, Acc: 100.00%, CE_Loss: 0.50, Reg_Loss:1886.10, Cost:0.00 best_reg:1894.00 avg_loss_reg:1894.00: 100%|████| 153/153 [00:10<00:00, 14.58it/s]
2531 ***Symmetric Check結束***
2532 *****檢測結果: Model是安全的(Benign)
2533 檢測結果: Model是安全的(Benign)
2534 檢測結果: Model是安全的(Benign)
2535 整體耗時: 34.32163858413696 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000242-----
2536 *****檢測結果: Model是安全的(Benign)
2537 ***Pre-Screening開始***
2538 ***Pre-Screening結束***
2539 檢測結果: Model是安全的(Benign)
2540 整體耗時: 3.92148494720459 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000243-----
2541 *****檢測結果: Model是安全的(Benign)
2542 ***Pre-Screening開始***
2543 ***Pre-Screening結束***
2544 *****檢測結果: Model是安全的(Benign)
2545 檢測結果: Model是安全的(Benign)
2546 整體耗時: 5.76967191696167 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000244-----
2547 *****檢測結果: Model是安全的(Benign)
2548 ***Pre-Screening開始***
2549 ***Pre-Screening結束***
2550 可能的攻擊方式: Label Specific Backdoor Attack
2551 可能的 target-victim 配對: ['7-0', '14-0', '16-0']
2552 ***Trigger Reverse Engineering開始***
2553 Target: 16, victim: 0, Loss: 12.3398, Acc: 0.00%, CE_Loss: 12.34, Reg_Loss:2546.67, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2533.22: 3%| | 32/10000 [00:37<18:48, 1.17s/it]
2554 ***Trigger Reverse Engineering結束***
2555 Target Class: 7 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 11
2556 *****檢測結果: Model是安全的(Benign)

```

2557 檢測結果: Model是安全的(Benign)  
2558 整體耗時: 50.18550157546997 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000245-----  
2559   \*\*\*Pre-Screening開始\*\*\*  
2560   \*\*\*Pre-Screening結束\*\*\*  
2561   可能的攻擊方式: Label Specific Backdoor Attack  
2562   可能的 target-victim 配對: ['0-8', '1-3', '1-4', '1-5', '5-3', '8-0', '10-4']  
2563   \*\*\*Trigger Reverse Engineering開始\*\*\*  
2564 Target: 10, victim: 4, Loss: 8.6155, Acc: 15.00%, CE\_Loss: 8.62, Reg\_Loss:3579.00, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:3339.31: 12% [■ | 116/1000 [00:16<02:05, 7.06it/s]  
2565 \*\*\*Trigger Reverse Engineering結束\*\*\*  
2566 Target Class: 0 Victim Class: 8 Trigger Size: 10000000000 Optimization Steps: 21  
2567 Target Class: 0 Victim Class: 8 Trigger Size: 10000000000 Optimization Steps: 21  
2568   \*\*\*\*\*檢測結果\*\*\*\*\*  
2569 檢測結果: Model是安全的(Benign)  
2570 整體耗時: 25.71719741821289 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000246-----  
2571   \*\*\*Pre-Screening開始\*\*\*  
2572   \*\*\*Pre-Screening結束\*\*\*  
2573   \*\*\*Pre-Screening開始\*\*\*  
2574   \*\*\*檢測結束\*\*\*  
2575 檢測結果: Model是安全的(Benign)  
2576 整體耗時: 13.339773138565063 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000247-----  
2577   \*\*\*Pre-Screening開始\*\*\*  
2578   \*\*\*Pre-Screening結束\*\*\*  
2579   \*\*\*Pre-Screening開始\*\*\*  
2580 可能的攻擊方式: Universal Backdoor Attack  
2581 可能的 target class: 7  
2582 可能的 victim classes: ALL  
2583   \*\*\*Trigger Reverse Engineering開始\*\*\*  
2584 Target: 7, victim: 12, Loss: 0.1830, Acc: 100.00%, CE\_Loss: 0.01, Reg\_Loss:76.55, Cost:0.00 best\_reg:80.21 avg\_loss\_reg:75.58: 6% [■ | 57/1000 [21:18<5:52:27, 22.43s/it]  
2585 early stop 所有  
2586   \*\*\*Trigger Reverse Engineering結束\*\*\*  
2587 Target Class: 7 Victim Class: all Trigger Size: 80.21017150878906 Optimization Steps: 58  
2588   \*\*\*\*\*檢測結果\*\*\*\*\*  
2589 檢測結果: Model含有後門(Abnormal)  
2590 整體耗時: 1289.224137544632 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000248-----  
2591   \*\*\*Pre-Screening開始\*\*\*  
2592   \*\*\*Pre-Screening結束\*\*\*  
2593   \*\*\*Pre-Screening開始\*\*\*  
2594   \*\*\*檢測結束\*\*\*  
2595 檢測結果: Model是安全的(Benign)  
2596 整體耗時: 6.279832363128662 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000249-----  
2597   \*\*\*Pre-Screening開始\*\*\*  
2598   \*\*\*Pre-Screening結束\*\*\*  
2599 可能的攻擊方式: Label Specific Backdoor Attack  
2600 可能的 target-victim 配對: ['1-0', '1-4', '1-22', '2-3', '4-15', '6-11', '10-0', '10-5', '13-4', '15-4', '17-15', '18-0', '21-1', '21-4', '22-1']  
2601   \*\*\*Trigger Reverse Engineering開始\*\*\*  
2602 Target: 13, victim: 4, Loss: 1.8781, Acc: 100.00%, CE\_Loss: 0.20, Reg\_Loss:1673.97, Cost:0.00 best\_reg:1684.14 avg\_loss\_reg:1684.14: 47% [■ | 467/1000 [21:42<24:46, 2.79s/it]  
2603 early stop 所有  
2604   \*\*\*Trigger Reverse Engineering結束\*\*\*  
2605 Target Class: 13 Victim Class: 4 Trigger Size: 1673.97412109375 Optimization Steps: 263  
2606 Target Class: 4 Trigger Size: 1673.97412109375 Optimization Steps: 263  
2607   \*\*\*\*\*檢測結果\*\*\*\*\*  
2608 檢測結果: Model是安全的(Benign)  
2609 整體耗時: 1329.244366186523 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000250-----  
2610   \*\*\*Pre-Screening開始\*\*\*  
2611   \*\*\*Pre-Screening結束\*\*\*  
2612   \*\*\*Pre-Screening開始\*\*\*  
2613   \*\*\*檢測結束\*\*\*  
2614 檢測結果: Model是安全的(Benign)  
2615 整體耗時: 6.342945098876953 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000251-----  
2616   \*\*\*\*\*檢測結果\*\*\*\*\*  
2617   \*\*\*Pre-Screening開始\*\*\*  
2618   \*\*\*Pre-Screening結束\*\*\*  
2619 可能的攻擊方式: Label Specific Backdoor Attack  
2620 可能的 target-victim 配對: ['2-10', '3-8', '12-2', '13-8', '15-8', '20-14', '21-18', '22-1']  
2621   \*\*\*Trigger Reverse Engineering開始\*\*\*  
2622 Target: 22, victim: 1, Loss: 8.5412, Acc: 0.00%, CE\_Loss: 8.54, Reg\_Loss:2566.56, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:2550.08: 14% [■ | 138/1000 [00:34<03:36, 3.97it/s]  
2623   \*\*\*Trigger Reverse Engineering結束\*\*\*  
2624 Target Class: 2 Victim Class: 10 Trigger Size: 1000000000.0 Optimization Steps: 21  
2625   \*\*\*\*\*檢測結果\*\*\*\*\*  
2626 檢測結果: Model是安全的(Benign)  
2627 整體耗時: 45.78194832801819

```

2628 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000252-----
2629 ***Pre-Screening開始***
2630 ***Pre-Screening結束***
2631 可能的攻擊方式: Label Specific Backdoor Attack
2632 可能的target-victim 配對: ['1-6', '1-20', '1-21', '3-14', '4-8', '5-15', '7-8', '8-15', '11-8', '11-10', '12-15', '13-19', '14-3', '14-19', '14-20', '15-5', '15-8', '16-19', '19-16', '21-1', '22-19']
2633 ***Trigger Reverse Engineering開始***
2634 Target: 21, victim: 1, Loss: 2.2654, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:620.62, Cost:0.00 best_reg:624.65 avg_loss_reg:631.27: 60% | 603/1000 [24:15<15:58, 2.41s/it]
2635 early stop 所有
2636 ***Trigger Reverse Engineering結束***
2637 Target Class: 21 Victim Class: 1 Trigger Size: 620.6196899414062 Optimization Steps: 246
2638 ***Symmetric Check開始***
2639 Target: 1, victim: 21, Loss: 2.1914, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:117.07, Cost:0.02 best_reg:119.15 avg_loss_reg:119.15: 54% | 134/246 [04:26<03:43, 1.99s/it]
2640 early stop 所有
2641 ***Symmetric Check結束***
2642 *****檢測結束*****檢測結束*****檢測結束*****
2643 檢測結果: Model是安全的(Benign)
2644 整體耗時: 1741.2192630767822
2645 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000253-----
2646 ***Pre-Screening開始***
2647 ***Pre-Screening結束***
2648 ***檢測結束***
2649 檢測結果: Model是安全的(Benign)
2650 整體耗時: 16.017282247543335
2651 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000254-----
2652 ***Pre-Screening開始***
2653 ***Pre-Screening結束***
2654 ***檢測結束***
2655 檢測結果: Model是安全的(Benign)
2656 整體耗時: 9.957149028778076
2657 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000255-----
2658 ***Pre-Screening開始***
2659 ***Pre-Screening結束***
2660 可能的攻擊方式: Universal Backdoor Attack
2661 可能的 target class: 2
2662 可能的 victim classes: ALL
2663 ***Trigger Reverse Engineering開始***
2664 Target: 2, victim: 6, Loss: 0.2611, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:559.69, Cost:0.00 best_reg:555.96 avg_loss_reg:557.36: 14% | 145/1000 [09:44<57:23, 4.03s/it]
2665 early stop 所有
2666 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000256-----
2667 Target Class: 2 Victim Class: all Trigger Size: 555.9589029947916 Optimization Steps: 146
2668 ***檢測結束***
2669 檢測結果: Model含有後門(Abnormal)
2670 整體耗時: 592.8882167339325
2671 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000257-----
2672 ***Pre-Screening開始***
2673 ***Pre-Screening結束***
2674 可能的攻擊方式: Label Specific Backdoor Attack
2675 可能的 target-victim 配對: ['2-10', '3-11', '4-10', '11-3']
2676 ***Trigger Reverse Engineering開始***
2677 Target: 2, victim: 10, Loss: 2.7357, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:102.52, Cost:0.03 best_reg:102.59 avg_loss_reg:102.59: 13% | 132/1000 [00:32<03:32, 4.08it/s]
2678 early stop 所有
2679 ***Trigger Reverse Engineering結束***
2680 Target Class: 2 Victim Class: 10 Trigger Size: 102.52171325683594 Optimization Steps: 90
2681 ***Symmetric Check開始***
2682 Target: 10, victim: 2, Loss: 2.2862, Acc: 90.00%, CE_Loss: 0.76, Reg_Loss:5142.69, Cost:0.00 best_reg:10939.42 avg_loss_reg:5261.17: 100% | 90/90 [00:21<00:00, 4.28it/s]
2683 ***Symmetric Check結束***
2684 ***檢測結束***檢測結束***檢測結束***
2685 檢測結果: Model含有後門(Abnormal)
2686 整體耗時: 61.55465626716614
2687 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000257-----
2688 ***Pre-Screening開始***
2689 ***Pre-Screening結束***
2690 可能的攻擊方式: Label Specific Backdoor Attack
2691 可能的 target-victim 配對: ['1-0', '3-15', '4-7', '4-8', '4-9', '5-7', '5-8', '5-10', '7-10', '8-7', '8-9', '11-9', '12-7', '12-8', '13-8', '15-10', '15-12', '17-14', '17-0', '17-2']
2692 ***Trigger Reverse Engineering開始***
2693 Target: 15, victim: 12, Loss: 0.6338, Acc: 100.00%, CE_Loss: 0.07 Reg_Loss:844.27 Cost:0.00 best_reg:844.85 avg_loss_reg:844.85: 55% | 550/1000 [03:08<02:34, 2.92it/s]
2694 early stop 所有
2695 ***Trigger Reverse Engineering結束***
2696 Target Class: 15 Victim Class: 12 Trigger Size: 844.2669677734375 Optimization Steps: 173
2697 ***Symmetric Check開始***
2698 Target: 12, victim: 15, Loss: 0.2086, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:9038.80, Cost:0.00 best_reg:8755.17 avg_loss_reg:9030.10: 100% | 173/173 [00:59<00:00, 2.91it/s]

```

```
2699 ***Symmetric Check結束***  
2700 *****檢測結果結束*****  
2701 檢測結果: Model含有後門(Abnormal)  
2702 整體耗時: 258.7712004184723  
2703 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000258-----  
2704 ***Pre-Screening開始***  
2705 ***Pre-Screening結束***  
2706 可能的攻擊方式: Label Specific Backdoor Attack  
2707 可能的 target-victim 配對: ['6-0']  
2708 ***Trigger Reverse Engineering開始***  
2709 Target: 6, victim: 0, Loss: 2.305, Acc: 100.00%, CE_Loss: 0.33, Reg_Loss:879.72, Cost:0.00 best_reg:880.66 avg_loss_reg:876.25: 19% █ | 194/1000 [00:26<01:51, 7.21it/s]  
2710 0% | 0/195 [00:00<?, ?it/s]early stop 所有  
2711 ***Trigger Reverse Engineering結束***  
2712 Target Class: 6 Victim Class: 0 Trigger Size: 879.718017578125 Optimization Steps: 195  
2713 ***Symmetric Check開始***  
2714 Target: 0, victim: 6 Loss: 1.3552, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:4031.27, Cost:0.00 best_reg:3960.17 avg_loss_reg:3996.11: 100% █ | 195/195 [00:28<00:00, 6.74it/s]  
2715 ***Symmetric Check結束***  
2716 *****檢測結果結束*****  
2717 檢測結果: Model是安全的(Benign)  
2718 整體耗時: 59.23349142074585  
2719 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000259-----  
2720 ***Pre-Screening開始***  
2721 ***Pre-Screening結束***  
2722 ***檢測結果: Model是安全的(Benign)  
2723 檢測結果: Model是安全的(Benign)  
2724 整體耗時: 14.57260537147522  
2725 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000260-----  
2726 ***Pre-Screening開始***  
2727 ***Pre-Screening結束***  
2728 可能的攻擊方式: Label Specific Backdoor Attack  
2729 可能的 target-victim 配對: ['3-5']  
2730 ***Trigger Reverse Engineering開始***  
2731 Target: 3, victim: 5, Loss: 8.5477, Acc: 20.00%, CE_Loss: 8.55, Reg_Loss:3872.52, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3559.12: 2% | | 20/1000 [00:53<43:31, 2.66s/it]  
2732 ***Trigger Reverse Engineering結束***  
2733 Target Class: 3 Victim Class: 5 Trigger Size: 10000000000.00 Optimization Steps: 21  
2734 *****檢測結果結束*****  
2735 檢測結果: Model是安全的(Benign)  
2736 整體耗時: 63.87156538036804  
2737 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000261-----  
2738 ***Pre-Screening開始***  
2739 ***Pre-Screening結束***  
2740 可能的攻擊方式: Label Specific Backdoor Attack  
2741 可能的 target-victim 配對: ['3-0', '4-0', '7-13', '10-1', '14-0']  
2742 ***Trigger Reverse Engineering開始***  
2743 Target: 7, victim: 13, Loss: 2.4544, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:294.99, Cost:0.01 best_reg:295.21 avg_loss_reg:295.36: 26% █ | 258/1000 [15:06<43:27, 3.51s/it]  
2744 early stop 所有  
2745 ***Trigger Reverse Engineering結束***  
2746 Target Class: 7 Victim Class: 13 Trigger Size: 294.993408203125 Optimization Steps: 157  
2747 ***Symmetric Check開始***  
2748 Target: 13, victim: 7, Loss: 0.6540, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:10113.93, Cost:0.00 best_reg:9741.82 avg_loss_reg:10099.10: 100% █ | 157/157 [08:54<00:00, 3.41s/it]  
2749 ***Symmetric Check結束***  
2750 *****檢測結果結束*****  
2751 檢測結果: Model含有後門(Abnormal)  
2752 整體耗時: 1461.9326655864716  
2753 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000262-----  
2754 ***Pre-Screening開始***  
2755 ***Pre-Screening結束***  
2756 可能的攻擊方式: Label Specific Backdoor Attack  
2757 可能的 target-victim 配對: ['0-18', '0-19', '1-18', '17-18', '18-0', '18-1', '19-0', '19-1']  
2758 ***Trigger Reverse Engineering開始***  
2759 Target: 19, victim: 0, Loss: 2.8555, Acc: 100.00%, CE_Loss: 0.43, Reg_Loss:213.08, Cost:0.01 best_reg:214.11 avg_loss_reg:214.11: 20% █ | 202/1000 [00:14<00:55, 14.37it/s]  
2760 0% | 0/125 [00:00<?, ?it/s]early stop 所有  
2761 ***Trigger Reverse Engineering結束***  
2762 Target Class: 19 Victim Class: 0 Trigger Size: 213.077880859375 Optimization Steps: 125  
2763 ***Symmetric Check開始***  
2764 Target: 0, victim: 19, Loss: 1.9032, Acc: 70.00%, CE_Loss: 0.46, Reg_Loss:427.91, Cost:0.00 best_reg:451.58 avg_loss_reg:426.96: 100% █ | 125/125 [00:08<00:00, 14.62it/s]  
2765 ***Symmetric Check結束***  
2766 *****檢測結果結束*****  
2767 檢測結果: Model是安全的(Benign)  
2768 整體耗時: 30.69347596168518  
2769 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000263-----
```

```
2770 ***Pre-Screening開始***  
2771 ***Pre-Screening結束***  
2772 ***檢測結束***  
2773 檢測結果: Model是安全的(Benign)  
2774 整體耗時: 22.036527395248413  
2775 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000264-----  
2776 ***Pre-Screening開始***  
2777 ***Pre-Screening結束***  
2778 ***檢測結束***  
2779 檢測結果: Model是安全的(Benign)  
2780 整體耗時: 7.798579454421997  
2781 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000265-----  
2782 ***Pre-Screening開始***  
2783 ***Pre-Screening結束***  
2784 可能的攻擊方式: Label Specific Backdoor Attack  
2785 可能的 target-victim 配對: ['2-9', '2-12', '7-9', '12-9']  
2786 ***Trigger Reverse Engineering開始***  
2787 Target: 2, victim: 12, Loss: 2.6690, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:68.85, Cost:0.04 best_reg:69.87 avg_loss_reg:69.87: 21% █ | 211/1000 [09:57<37:15, 2.83s/it]  
2788 early stop 所有  
2789 ***Trigger Reverse Engineering結束***  
2790 Target Class: 2 Victim Class: 12 Trigger Size: 68.85238647460938 Optimization Steps: 72  
2791 ***Symmetric Check開始***  
2792 Target: 12, victim: 2, Loss: 4.9122, Acc: 0.00%, CE_Loss: 4.91, Reg_Loss:14389.06, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:14262.21: 100% █ | 72/72 [03:23<00:00, 2.83s/it]  
2793 ***Symmetric Check結束***  
2794 ***檢測結束***  
2795 檢測結果: Model含有後門(Abnormal)  
2796 整體耗時: 831.797722101215  
2797 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000266-----  
2798 ***Pre-Screening開始***  
2799 ***Pre-Screening結束***  
2800 可能的攻擊方式: Universal Backdoor Attack  
2801 可能的 target class: 7  
2802 可能的 victim classes: ALL  
2803 ***Trigger Reverse Engineering開始***  
2804 Target: 7 victim: 6, Loss: 0.4118, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:255.91, Cost:0.00 best_reg:253.00 avg_loss_reg:254.95: 10% █ | 102/1000 [25:09<3:41:32, 14.80s/it]  
2805 early stop 所有  
2806 ***Trigger Reverse Engineering結束***  
2807 Target Class: all Trigger Size: 253.00390625 Optimization Steps: 103  
2808 ***檢測結束***  
2809 檢測結果: Model含有後門(Abnormal)  
2810 整體耗時: 1529.5436279773712  
2811 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000267-----  
2812 ***Pre-Screening開始***  
2813 ***Pre-Screening結束***  
2814 可能的攻擊方式: Label Specific Backdoor Attack  
2815 可能的 target-victim 配對: ['2-13', '3-13', '4-6', '8-7', '10-3', '11-6']  
2816 ***Trigger Reverse Engineering開始***  
2817 Target: 8, victim: 7, Loss: 0.9015, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:71.14, Cost:0.01 best_reg:71.90 avg_loss_reg:71.90: 45% █ | 452/1000 [00:51<01:02, 8.77it/s]  
2818 early stop 所有  
2819 ***Trigger Reverse Engineering結束***  
2820 Target Class: 8 Victim Class: 7 Trigger Size: 71.13677215576172 Optimization Steps: 127  
2821 ***Symmetric Check開始***  
2822 Target: 7, victim: 8, Loss: 8.2422, Acc: 80.00%, CE_Loss: 0.49, Reg_Loss:11632.27, Cost:0.00 best_reg:16824.35 avg_loss_reg:12409.88: 100% █ | 127/127 [00:14<00:00, 8.48it/s]  
2823 ***Symmetric Check結束***  
2824 ***檢測結束***  
2825 檢測結果: Model含有後門(Abnormal)  
2826 整體耗時: 75.29008531570435  
2827 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000268-----  
2828 ***Pre-Screening開始***  
2829 ***Pre-Screening結束***  
2830 可能的攻擊方式: Universal Backdoor Attack  
2831 可能的 target class: 0  
2832 可能的 victim classes: ALL  
2833 ***Trigger Reverse Engineering開始***  
2834 Target: 0, victim: 6, Loss: 1.4364, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:177.48, Cost:0.01 best_reg:179.58 avg_loss_reg:185.24: 14% █ | 144/1000 [15:17<1:30:52, 6.37s/it]  
2835 early stop 所有  
2836 ***Trigger Reverse Engineering結束***  
2837 Target Class: 0 Victim Class: all Trigger Size: 179.34065755208334 Optimization Steps: 145  
2838 ***檢測結束***  
2839 檢測結果: Model含有後門(Abnormal)  
2840 整體耗時: 924.2564198970795
```

```

2841     ***Pre-Screening開始*** 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000269
2842     ***Pre-Screening結束*** 
2843     ***Pre-Screening開始*** 
2844     可能的攻擊方式: Label Specific Backdoor Attack
2845     可能的 target-victim 配對: ['1-0', '2-4', '3-7', '7-3']
2846     ***Trigger Reverse Engineering開始*** 
2847     Target: 7, victim: 3, Loss: 9.2558, Acc: 0.00%, CE_Loss: 9.26, Reg_Loss:2598.33, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2571.89; 6%| | 63/1000 [02:46<41:09, 2.64s/it]
2848     ***Trigger Reverse Engineering結束*** 
2849     Target Class: 1 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 21
2850     *****檢測結果*****檢測結束***** 
2851     檢測結果: Model是安全的(Benign)
2852     整體耗時: 182.42415857315063
2853     插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000270
2854     ***Pre-Screening開始*** 
2855     ***Pre-Screening結束*** 
2856     ***檢測結果*****檢測結束***** 
2857     檢測結果: Model是安全的(Benign)
2858     整體耗時: 7.4649529457092285
2859     插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000271
2860     ***Pre-Screening開始*** 
2861     ***Pre-Screening結束*** 
2862     可能的攻擊方式: Label Specific Backdoor Attack
2863     可能的 target-victim 配對: ['0-12', '1-14', '2-7', '5-12']
2864     ***Trigger Reverse Engineering開始*** 
2865     Target: 5, victim: 12, Loss: 5.4542, Acc: 0.00%, CE_Loss: 5.45, Reg_Loss:2599.28, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2574.66; 5%| | 53/1000 [00:27<08:18, 1.90it/s]
2866     ***Trigger Reverse Engineering結束*** 
2867     Target Class: 0 Victim Class: 12 Trigger Size: 1000000000.0 Optimization Steps: 11
2868     *****檢測結果*****檢測結束***** 
2869     檢測結果: Model是安全的(Benign)
2870     整體耗時: 40.54869723320007
2871     插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000272
2872     ***Pre-Screening開始*** 
2873     ***Pre-Screening結束*** 
2874     可能的攻擊方式: Label Specific Backdoor Attack
2875     可能的 target-victim 配對: ['10-1']
2876     ***Trigger Reverse Engineering開始*** 
2877     Target: 10, victim: 1, Loss: 7.1734, Acc: 0.00%, CE_Loss: 7.17, Reg_Loss:2576.56, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2557.39; 1%| | 10/1000 [00:01<02:57, 5.57it/s]
2878     ***Trigger Reverse Engineering結束*** 
2879     Target Class: 10 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11
2880     *****檢測結果*****檢測結束***** 
2881     檢測結果: Model是安全的(Benign)
2882     整體耗時: 10.0901677760848999
2883     插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000273
2884     ***Pre-Screening開始*** 
2885     ***Pre-Screening結束*** 
2886     可能的攻擊方式: Label Specific Backdoor Attack
2887     可能的 target-victim 配對: ['3-13', '7-8', '8-7', '11-7', '13-2', '14-2']
2888     ***Trigger Reverse Engineering開始*** 
2889     Target: 11, victim: 7, Loss: 3.9573, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:216.81, Cost:0.02 best_reg:217.18 avg_loss_reg:217.14: 17%| | 169/1000 [00:24<02:00, 6.91it/s]
2890     early stop 所有
2891     ***Trigger Reverse Engineering結束*** 
2892     Target Class: 11 Victim Class: 7 Trigger Size: 216.811660766601156 Optimization Steps: 114
2893     ***Symmetric Check開始*** 
2894     Target: 7, victim: 11, Loss: 3.0480, Acc: 80.00%, CE_Loss: 0.89, Reg_Loss:4864.62, Cost:0.00 best_reg:10320.57 avg_loss_reg:4963.81: 100%| | 114/114 [00:19<00:00, 5.99it/s]
2895     ***Symmetric Check結束*** 
2896     *****檢測結果*****檢測結束***** 
2897     檢測結果: Model含有後門(Abnormal)
2898     整體耗時: 50.286834955215454
2899     插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000274
2900     ***Pre-Screening開始*** 
2901     ***Pre-Screening結束*** 
2902     ***檢測結果*****檢測結束***** 
2903     檢測結果: Model是安全的(Benign)
2904     整體耗時: 24.034883737564087
2905     插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000275
2906     ***Pre-Screening開始*** 
2907     ***Pre-Screening結束*** 
2908     ***檢測結果*****檢測結束***** 
2909     檢測結果: Model是安全的(Benign)
2910     整體耗時: 23.880672931671143
2911     插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000276

```

```
2912 ***Pre-Screening開始***  
2913 ***Pre-Screening結束***  
2914 ***檢測結束***  
2915 檢測結果: Model是安全的(Benign)  
2916 整體耗時: 11.835036754608154  
2917 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000277-----  
2918 ***Pre-Screening開始***  
2919 ***Pre-Screening結束***  
2920 可能的攻擊方式: Label Specific Backdoor Attack  
2921 可能的 target-victim 配對: ['7-8']  
2922 ***Trigger Reverse Engineering開始***  
2923 Target: 7, victim: 8, Loss: 9.1221, Acc: 0.00%, CE_Loss: 9.12, Reg_Loss:2574.99, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2555.77: 1%| | 10/1000 [00:04<07:54, 2.08it/s]  
2924 ***Trigger Reverse Engineering結束***  
2925 Target Class: 7 Victim Class: 8 Trigger Size: 1000000000.0 Optimization Steps: 11  
2926 *****檢測結束*****  
2927 檢測結果: Model是安全的(Benign)  
2928 整體耗時: 15.46074914932251  
2929 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000278-----  
2930 ***Pre-Screening開始***  
2931 ***Pre-Screening結束***  
2932 ***檢測結束***  
2933 檢測結果: Model是安全的(Benign)  
2934 整體耗時: 28.607166528701782  
2935 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000279-----  
2936 ***Pre-Screening開始***  
2937 ***Pre-Screening結束***  
2938 檢測結果: Model是安全的(Benign)  
2939 整體耗時: 9.633477449417114  
2940 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000280-----  
2941 ***Pre-Screening開始***  
2942 ***Pre-Screening結束***  
2943 ***Pre-Screening開始***  
2944 可能的攻擊方式: Label Specific Backdoor Attack  
2945 可能的 target-victim 配對: ['4-12']  
2946 ***Trigger Reverse Engineering開始***  
2947 Target: 4, victim: 12, Loss: 10.8191, Acc: 0.00%, CE_Loss: 10.82, Reg_Loss:2537.32, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2526.63: 1%| | 10/1000 [00:03<06:22, 2.59it/s]  
2948 ***Trigger Reverse Engineering結束***  
2949 Target Class: 4 Victim Class: 12 Trigger Size: 1000000000.0 Optimization Steps: 11  
2950 *****檢測結束*****  
2951 檢測結果: Model是安全的(Benign)  
2952 整體耗時: 13.260554552078247  
2953 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000281-----  
2954 ***Pre-Screening開始***  
2955 ***Pre-Screening結束***  
2956 ***檢測結束***  
2957 檢測結果: Model是安全的(Benign)  
2958 整體耗時: 14.600783354873657  
2959 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000282-----  
2960 ***Pre-Screening開始***  
2961 ***Pre-Screening結束***  
2962 ***檢測結束***  
2963 檢測結果: Model是安全的(Benign)  
2964 整體耗時: 36.816036224365234  
2965 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000283-----  
2966 ***Pre-Screening開始***  
2967 ***Pre-Screening結束***  
2968 ***檢測結束***  
2969 檢測結果: Model是安全的(Benign)  
2970 整體耗時: 5.61470937728818  
2971 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000284-----  
2972 ***Pre-Screening開始***  
2973 ***Pre-Screening結束***  
2974 可能的攻擊方式: Label Specific Backdoor Attack  
2975 可能的 target-victim 配對: ['1-2', '2-1', '4-3', '4-11', '9-3', '14-11', '19-2', '22-1', '22-2']  
2976 ***Trigger Reverse Engineering開始***  
2977 Target: 4, victim: 11, Loss: 2.5807, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:43.90, Cost:0.06 best_reg:44.19 avg_loss_reg:43.36: 22%| | 122/1000 [03:38<12:46, 1.02it/s]  
2978 early stop 所有  
2979 ***Trigger Reverse Engineering結束***  
2980 Target Class: 4 Victim Class: 11 Trigger Size: 43.900657653808594 Optimization Steps: 91  
2981 ***Symmetric Check開始***  
2982 Target: 11, victim: 4, Loss: 0.4296, Acc: 85.00%, CE_Loss: 0.43, Reg_Loss:19473.90, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:19374.88: 100%| | 91/91 [01:21<00:00, 1.12it/s] 91/91 [01:21<00:00, 1.12it/s]
```

```

2983 ***Symmetric Check結束***  

2984 *****檢測結束*****  

2985 檢測結果: Model含有後門(Abnormal)  

2986 整體耗時: 311.3421742916107  

2987 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000285-----  

2988 ***Pre-Screening開始***  

2989 ***Pre-Screening結束***  

2990 可能的攻擊方式: Label Specific Backdoor Attack  

2991 可能的 target-victim 配對: ['4-18', '13-3', '14-18', '16-3']  

2992 ***Trigger Reverse Engineering開始***  

2993 Target: 14, victim: 18, Loss: 2.5877, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:94.10, Cost:0.03 best_reg:95.52 avg_loss_reg:95.52: 14% █ | 145/1000 [00:16<01:39, 8.59it/s]  

2994 early stop 所有  

2995 ***Trigger Reverse Engineering結束***  

2996 Target Class: 14 Victim Class: 18 Trigger Size: 94.09506225585938 Optimization Steps: 112  

2997 ***Symmetric Check開始***  

2998 Target: 18, victim: 14, Loss: 5.2238, Acc: 90.00%, CE_Loss: 0.67, Reg_Loss:3033.36, Cost:0.00 best_reg:3112.93 avg_loss_reg:3070.61: 100% █ | 112/112 [00:13<00:00, 8.46it/s]  

2999 ***Symmetric Check結束***  

3000 檢測結果: Model含有後門(Abnormal)  

3001 整體耗時: 35.91523265838623  

3002 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000286-----  

3003 -----檢測結束*****  

3004 ***Pre-Screening開始***  

3005 ***Pre-Screening結束***  

3006 可能的攻擊方式: Label Specific Backdoor Attack  

3007 可能的 target-victim 配對: ['10-12', '10-13']  

3008 ***Trigger Reverse Engineering開始***  

3009 Target: 10, victim: 13, Loss: 8.9809, Acc: 0.00%, CE_Loss: 8.98, Reg_Loss:2543.81, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2530.32: 2% | | 21/1000 [00:03<02:57, 5.50it/s]  

3010 ***Trigger Reverse Engineering結束***  

3011 Target Class: 10 Victim Class: 12 Trigger Size: 1000000000.00 Optimization Steps: 11  

3012 ***檢測結束*****  

3013 檢測結果: Model是安全的(Benign)  

3014 整體耗時: 9.533351182937622  

3015 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000287-----  

3016 ***Pre-Screening開始***  

3017 ***Pre-Screening結束***  

3018 可能的攻擊方式: Label Specific Backdoor Attack  

3019 可能的 target-victim 配對: ['0-10', '6-3', '10-0']  

3020 ***Trigger Reverse Engineering開始***  

3021 Target: 0, victim: 10, Loss: 1.4801, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:575.54, Cost:0.00 best_reg:576.44 avg_loss_reg:575.33: 24% █ | | 235/1000 [12:05<39:22, 3.09s/it]  

3022 early stop 所有  

3023 ***Trigger Reverse Engineering結束***  

3024 Target Class: 0 Victim Class: 10 Trigger Size: 575.5419921875 Optimization Steps: 194  

3025 ***Symmetric Check開始***  

3026 Target: 10, victim: 0, Loss: 0.9422, Acc: 95.00%, CE_Loss: 0.26, Reg_Loss:1027.04, Cost:0.00 best_reg:1060.54 avg_loss_reg:1020.31: 100% █ | | 194/194 [09:56<00:00, 3.07s/it]  

3027 ***Symmetric Check結束***  

3028 檢測結果: Model是安全的(Benign)  

3029 整體耗時: 1332.5574412345886  

3030 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000288-----  

3031 -----檢測結束*****  

3032 ***Pre-Screening開始***  

3033 ***Pre-Screening結束***  

3034 可能的攻擊方式: Universal Backdoor Attack  

3035 可能的 target class: 8  

3036 可能的 victim classes: ALL  

3037 ***Trigger Reverse Engineering開始***  

3038 Target: 8, victim: 16, Loss: 0.3565, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:70.43, Cost:0.01 best_reg:81.13 avg_loss_reg:70.85: 7% █ | | 66/1000 [04:06<58:12, 3.74s/it]  

3039 early stop 所有  

3040 ***Trigger Reverse Engineering結束***  

3041 Target Class: 8 Victim Class: all Trigger Size: 81.12675603230794 Optimization Steps: 67  

3042 ***檢測結束*****  

3043 檢測結果: Model含有後門(Abnormal)  

3044 整體耗時: 253.48026180267334  

3045 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000289-----  

3046 ***Pre-Screening開始***  

3047 ***Pre-Screening結束***  

3048 可能的攻擊方式: Label Specific Backdoor Attack  

3049 可能的 target-victim 配對: ['13-0']  

3050 ***Trigger Reverse Engineering開始***  

3051 Target: 13, victim: 0, Loss: 7.3209, Acc: 0.00%, CE_Loss: 7.32, Reg_Loss:2553.39, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2540.90: 1% | | 10/1000 [00:22<36:33, 2.22s/it]  

3052 ***Trigger Reverse Engineering結束***  

3053 Target Class: 13 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 11

```

```
3054 ****Pre-Screening結束**** 檢測結果: Model是安全的(Benign)
3055 整體耗時: 35.53170442581177 報錯檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000290-
3056 ****Pre-Screening開始**** 檢測結果: Model是安全的(Benign)
3057 可能的攻擊方式: Label Specific Backdoor Attack
3058 可能的 target-victim 配對: [r0-8]
3059 ***Trigger Reverse Engineering開始****
3060 Target: 0, victim: 8, Loss: 3.3472, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:1408.71, Cost:0.00 best_reg:1414.26 avg_loss_reg:1405.70: 15%|█ | 149/1000 [11:52<1:07:49, 4.78s/it]
3061 early stop 所有
3062 ***Trigger Reverse Engineering結束****
3063 Target Class: 0 Victim Class: 8 Trigger Size: 1408.7076416015625 Optimization Steps: 150
3064 ****Pre-Screening開始****
3065 Target Class: 0 Victim Class: 8 Trigger Size: 1408.71, Cost:0.00 best_reg:1408.71, Cost:0.00 best_reg:1414.26 avg_loss_reg:1405.70: 15%|█ | 149/1000 [11:52<1:07:49, 4.78s/it]
3066 Target Class: 0 Victim Class: 8 Trigger Size: 1408.7076416015625 Optimization Steps: 150
3067 ****Pre-Screening結束****
3068 檢測結果: Model是安全的(Benign)
3069 整體耗時: 735.323009967804 報錯檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000291-
3070 ****Pre-Screening開始****
3071 ****Pre-Screening結束****
3072 可能的攻擊方式: Universal Backdoor Attack
3073 可能的 target class: 0
3074 可能的 victim classes: ALL
3075 可能的 target class: 0
3076 ***Trigger Reverse Engineering開始****
3077 Target: 0, victim: 9, Loss: 0.2001, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:58.89, Cost:0.00 best_reg:57.97 avg_loss_reg:58.59: 8%|█ | 77/1000 [16:59<3:23:36, 13.24s/it]
3078 early stop 所有
3079 ***Trigger Reverse Engineering結束****
3080 Target Class: 0 Victim Class: all Trigger Size: 57.970904214041575 Optimization Steps: 78
3081 ****Pre-Screening結束****
3082 檢測結果: Model含有後門(Abnormal)
3083 整體耗時: 1030.4302251338959 報錯檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000292-
3084 ****Pre-Screening開始****
3085 ****Pre-Screening結束****
3086 ****Pre-Screening結束****
3087 ****檢測結束****
3088 檢測結果: Model是安全的(Benign)
3089 整體耗時: 8.500859260559082 報錯檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000293-
3090 ****Pre-Screening結束****
3091 ****Pre-Screening開始****
3092 ****Pre-Screening結束****
3093 ****檢測結束****
3094 檢測結果: Model是安全的(Benign)
3095 整體耗時: 1.9401400089263916 報錯檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000294-
3096 ****Pre-Screening結束****
3097 ****Pre-Screening開始****
3098 ****Pre-Screening結束****
3099 可能的攻擊方式: Universal Backdoor Attack
3100 可能的 target class: 0
3101 可能的 victim classes: ALL
3102 ***Trigger Reverse Engineering開始****
3103 Target: 0, victim: 9, Loss: 0.2176, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:319.79, Cost:0.00 best_reg:316.05 avg_loss_reg:318.34: 9%|█ | 90/1000 [01:01<10:19, 1.47it/s]
3104 early stop 所有
3105 ***Trigger Reverse Engineering結束****
3106 Target Class: 0 Victim Class: all Trigger Size: 316.0466766357422 Optimization Steps: 91
3107 ****Pre-Screening結束****
3108 檢測結果: Model含有後門(Abnormal)
3109 整體耗時: 66.52274012565613 報錯檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000295-
3110 ****Pre-Screening開始****
3111 ****Pre-Screening結束****
3112 ****Pre-Screening結束****
3113 ****檢測結束****
3114 檢測結果: Model是安全的(Benign)
3115 整體耗時: 5.0246827602386475 報錯檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000296-
3116 ****Pre-Screening開始****
3117 ****Pre-Screening結束****
3118 ****Pre-Screening結束****
3119 ****檢測結束****
3120 檢測結果: Model是安全的(Benign)
3121 整體耗時: 13.946580410003662 報錯檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000297-
3122 ****Pre-Screening開始****
3123 ****Pre-Screening結束****
3124 ****Pre-Screening結束****
```

```

3125 可能的攻擊方式: Label Specific Backdoor Attack
3126 可能的 target-victim 配對: ['7-0', '7-5']
3127 ***Trigger Reverse Engineering開始***
3128 Target: 7, victim: 0, Loss: 1.5542, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:284.63, Cost:0.01 best_reg:285.20 avg_loss_reg:285.53: 17% █ | 172/1000 [03:39<17:35, 1.27s/it]
3129 early stop 所有
3130 ***Trigger Reverse Engineering結束***
3131 Target Class: 7 Victim Class: 0 Trigger Size: 284.62506103515625 Optimization Steps: 155
3132 ***Symmetric Check開始***
3133 Target: 0, victim: 7, Loss: 8.3136, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:476.59, Cost:0.02 best_reg:483.70 avg_loss_reg:483.70: 100% █ | 155/155 [03:21<00:00, 1.30s/it]
3134 ***Symmetric Check結束***
3135 *****檢測結束*****
3136 檢測結果: Model是安全的(Benign)
3137 整體耗時: 427.1314253807068
3138 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000298-----
3139 ***Pre-Screening開始***
3140 ***Pre-Screening結束***
3141 可能的攻擊方式: Label Specific Backdoor Attack
3142 可能的 target-victim 配對: ['0-20', '1-8', '4-8', '5-7', '7-11', '9-14', '9-12', '9-15', '10-18', '10-4', '10-9', '12-6', '12-8', '13-6', '15-12', '16-5', '16-6', '16-12', '17-11', '18-2', '18-19', '19-14', '19-20', '20-0']
3143 ***Trigger Reverse Engineering開始***
3144 Target: 0, victim: 20, Loss: 4.0837, Acc: 100.00%, CE_Loss: 0.34, Reg_Loss:218.92, Cost:0.02 best_reg:219.43 avg_loss_reg:219.43: 41% █ | 412/1000 [16:21<23:20, 2.38s/it]
3145 early stop 所有
3146 ***Trigger Reverse Engineering結束***
3147 Target Class: 0 Victim Class: 20 Trigger Size: 218.91944885253906 Optimization Steps: 119
3148 ***Symmetric Check開始***
3149 Target: 20, victim: 0, Loss: 6.4806, Acc: 90.00%, CE_Loss: 0.34, Reg_Loss:1819.57, Cost:0.00 best_reg:2016.21 avg_loss_reg:1850.03: 100% █ | 119/119 [04:11<00:00, 2.11s/it]
3150 ***Symmetric Check結束***
3151 *****檢測結束*****
3152 檢測結果: Model是安全的(Benign)
3153 整體耗時: 1249.1257319450378
3154 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000299-----
3155 ***Pre-Screening開始***
3156 ***Pre-Screening結束***
3157 ***檢測結束***
3158 檢測結果: Model是安全的(Benign)
3159 整體耗時: 2.0644288063049316
3160 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000300-----
3161 ***Pre-Screening開始***
3162 ***Pre-Screening結束***
3163 可能的攻擊方式: Label Specific Backdoor Attack
3164 可能的 target-victim 配對: ['0-9', '4-5', '4-8', '7-0', '7-6', '8-3', '8-4']
3165 ***Trigger Reverse Engineering開始***
3166 Target: 7, victim: 0, Loss: 1.1127, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:1432.11, Cost:0.00 best_reg:1436.21 avg_loss_reg:1433.47: 42% █ | 419/1000 [22:46<31:34, 3.26s/it]
3167 early stop 所有
3168 ***Trigger Reverse Engineering結束***
3169 Target Class: 7 Victim Class: 0 Trigger Size: 1432.1094970703125 Optimization Steps: 343
3170 ***檢測結束*****
3171 檢測結果: Model是安全的(Benign)
3172 整體耗時: 1377.9544868469238
3173 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000301-----
3174 ***Pre-Screening開始***
3175 ***Pre-Screening結束***
3176 ***檢測結束***
3177 檢測結果: Model是安全的(Benign)
3178 整體耗時: 1.92500758171108154
3179 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000302-----
3180 ***Pre-Screening開始***
3181 ***Pre-Screening結束***
3182 ***檢測結束***
3183 檢測結果: Model是安全的(Benign)
3184 整體耗時: 4.96380667599487
3185 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000303-----
3186 ***Pre-Screening開始***
3187 ***Pre-Screening結束***
3188 ***檢測結束***
3189 檢測結果: Model是安全的(Benign)
3190 整體耗時: 6.6166260246216
3191 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000304-----
3192 ***Pre-Screening開始***
3193 ***檢測結束***
3194 ***檢測結束***
3195 檢測結果: Model是安全的(Benign)

```

3196 整體耗時: 6.236108303070068 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000305-----  
3197   \*\*\*Pre-Screening開始\*\*\*\*\*  
3198   \*\*\*Pre-Screening結束\*\*\*\*\*  
3199 可能的攻擊方式: Universal Backdoor Attack  
3200 可能的 victim classes: ALL  
3201 可能的 target class: 6  
3202 可能的 victim classes: ALL  
3203 \*\*\*Trigger Reverse Engineering開始\*\*\*\*\*  
3204 Target: 6, victim: 6, Loss: 0.2643, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss: 6.85, Cost:0.04 best\_reg:6.75 avg\_loss\_reg:6.82: 9% | | 93/1000 [02:29<24:18, 1.61s/t]  
3205 early stop 所有  
3206 \*\*\*Trigger Reverse Engineering結束\*\*\*\*\*  
3207 Target Class: 6 Victim Class: all Trigger Size: 6.747086906433106 Optimization Steps: 94  
3208 檢測結果: Model含 有後門(Abnormal)  
3209 整體耗時: 154.31021928787231 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000306-----  
3210   \*\*\*Pre-Screening開始\*\*\*\*\*  
3211   \*\*\*Pre-Screening結束\*\*\*\*\*  
3212 可能的攻擊方式: Label Specific Backdoor Attack  
3213   \*\*\*Pre-Screening結束\*\*\*\*\*  
3214 可能的 victim 配對: ['9', '12']  
3215 可能的 target-victim 配對: ['9', '12']  
3216 \*\*\*Trigger Reverse Engineering開始\*\*\*\*\*  
3217 Target: 9, victim: 12, Loss: 12.5037, Acc: 0.00%, CE\_Loss: 12.50, Reg\_Loss: 2532.20, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:2524.50: 1% | | 10/1000 [00:01<02:50, 5.81it/s]  
3218 \*\*\*Trigger Reverse Engineering結束\*\*\*\*\*  
3219 Target Class: 9 Victim Class: 12 Trigger Size: 1000000000.0 Optimization Steps: 11  
3220   \*\*\*Pre-Screening結束\*\*\*\*\*  
3221 檢測結果: Model是安全的(Benign)  
3222 整體耗時: 7.7492430210113525 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000307-----  
3223   \*\*\*Pre-Screening開始\*\*\*\*\*  
3224   \*\*\*Pre-Screening結束\*\*\*\*\*  
3225 可能的攻擊方式: Label Specific Backdoor Attack  
3226 可能的 target-victim 配對: ['2', '21', '23-1']  
3227 可能的 target-victim 配對: ['2-21', '23-1']  
3228 \*\*\*Trigger Reverse Engineering開始\*\*\*\*\*  
3229 Target: 23, victim: 1, Loss: 5.7499, Acc: 0.00%, CE\_Loss: 5.75, Reg\_Loss: 2592.91, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:2568.80: 2% | | 121/1000 [00:07<06:02, 2.70it/s]  
3230 \*\*\*Trigger Reverse Engineering結束\*\*\*\*\*  
3231 Target Class: 21 Victim Class: 21 Trigger Size: 1000000000.0 Optimization Steps: 11  
3232   \*\*\*Pre-Screening結束\*\*\*\*\*  
3233 檢測結果: Model是安全的(Benign)  
3234 整體耗時: 14.389706893005188 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000308-----  
3235   \*\*\*Pre-Screening開始\*\*\*\*\*  
3236   \*\*\*Pre-Screening結束\*\*\*\*\*  
3237   \*\*\*Pre-Screening結束\*\*\*\*\*  
3238   \*\*\*Pre-Screening結束\*\*\*\*\*  
3239 檢測結果: Model是安全的(Benign)  
3240 整體耗時: 9.02915334701538 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000309-----  
3241   \*\*\*Pre-Screening開始\*\*\*\*\*  
3242   \*\*\*Pre-Screening結束\*\*\*\*\*  
3243   \*\*\*Pre-Screening結束\*\*\*\*\*  
3244   \*\*\*Pre-Screening結束\*\*\*\*\*  
3245 檢測結果: Model是安全的(Benign)  
3246 整體耗時: 12.687676668167114 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000310-----  
3247   \*\*\*Pre-Screening開始\*\*\*\*\*  
3248   \*\*\*Pre-Screening結束\*\*\*\*\*  
3249   \*\*\*Pre-Screening結束\*\*\*\*\*  
3250 可能的攻擊方式: Universal Backdoor Attack  
3251 可能的 target class: 6  
3252 可能的 victim classes: ALL  
3253 \*\*\*Trigger Reverse Engineering開始\*\*\*\*\*  
3254 Target: 6, victim: 14, Loss: 0.3528, Acc: 90.62%, CE\_Loss: 0.13, Reg\_Loss: 151.66, Cost:0.00 best\_reg:152.74 avg\_loss\_reg:149.77: 8% | | 80/1000 [13:40<2:37:16, 10.26s/t]  
3255 early stop 所有  
3256   \*\*\*Pre-Screening結束\*\*\*\*\*  
3257 Target Class: 6 Victim Class: all Trigger Size: 152.74190826416014 Optimization Steps: 81  
3258   \*\*\*Pre-Screening結束\*\*\*\*\*  
3259 檢測結果: Model含 有後門(Abnormal)  
3260 整體耗時: 829.546571969986 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000311-----  
3261   \*\*\*Pre-Screening開始\*\*\*\*\*  
3262   \*\*\*Pre-Screening結束\*\*\*\*\*  
3263   \*\*\*Pre-Screening結束\*\*\*\*\*  
3264   \*\*\*Pre-Screening結束\*\*\*\*\*  
3265 檢測結果: Model是安全的(Benign)  
3266 整體耗時: 5.035828590393066

## File - main

-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000312-----

3267   \*\*\*Pre-Screening開始  
3268   \*\*\*Pre-Screening結束\*\*\*  
3269   \*\*\*Pre-Screening結束\*\*\*

3270 可能的攻擊方式: Universal Backdoor Attack  
3271 可能的 target class: 0  
3272 可能的 victim classes: ALL  
3273   \*\*\*Trigger Reverse Engineering開始\*\*\*  
3274 Target: 0, victim: 6, Loss: 2.5409, Acc: 100.00%, CE\_Loss: 0.01, Reg\_Loss:5694.87, Cost:0.00 best\_reg:5736.33 avg\_loss\_reg:5723.15: 13%| | 130/1000 [31:42 <3:32:15, 14.64s/it]  
3275 early stop 所有  
3276   \*\*\*Trigger Reverse Engineering結束\*\*\*  
3277 Target Class: 0 Victim Class: all Trigger Size: 5736.3283203125 Optimization Steps: 131  
3278   \*\*\*\*\*檢測結果: Model是安全的(Benign)  
3279 檢測結果: Model是安全的(Benign)  
3280 整體耗時: 1913.6277701854706  
3281-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000313-----

3282   \*\*\*Pre-Screening開始\*\*\*  
3283   \*\*\*Pre-Screening結束\*\*\*  
3284 可能的攻擊方式: Label Specific Backdoor Attack  
3285 可能的 target-victim 配對: ['1-16', '2-1', '2-16', '4-6', '7-4', '7-6', '7-10', '8-4', '9-3', '9-12', '10-4', '10-6', '10-8', '14-5', '14-9', '14-3']  
3286   \*\*\*Trigger Reverse Engineering開始\*\*\*  
3287 Target: 1, victim: 1, Loss: 0.4673, Acc: 100.00%, CE\_Loss: 0.14, Reg\_Loss:326.49, Cost:0.00 best\_reg:326.97 avg\_loss\_reg:329.15: 63%| | 634/1000 [14:25 <08:19, 1.37s/it]  
3288 early stop 所有  
3289   \*\*\*Trigger Reverse Engineering結束\*\*\*  
3290 Target Class: 2 Victim Class: 1 Trigger Size: 326.4883728027344 Optimization Steps: 426  
3291   \*\*\*Symmetric Check開始\*\*\*  
3292 Target: 1, victim: 2, Loss: 1.3830, Acc: 100.00%, CE\_Loss: 0.16, Reg\_Loss:1838.50, Cost:0.00 best\_reg:1843.37 avg\_loss\_reg:1843.37: 72%| | 305/426 [06:33 <02:36, 1.29s/it]  
3293 early stop 所有  
3294   \*\*\*Symmetric Check結束\*\*\*  
3295   \*\*\*\*\*檢測結果: Model是安全的(Benign)  
3296 檢測結果: Model是安全的(Benign)  
3297 整體耗時: 1274.3152511119843  
3298-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000314-----

3299   \*\*\*Pre-Screening開始\*\*\*  
3300   \*\*\*Pre-Screening結束\*\*\*

3301 可能的攻擊方式: Label Specific Backdoor Attack  
3302 可能的 target-victim 配對: ['0-4', '1-3', '1-5', '4-0', '5-1']  
3303   \*\*\*Trigger Reverse Engineering開始\*\*\*  
3304 Target: 5, victim: 1, Loss: 6.8003, Acc: 15.00%, CE\_Loss: 6.80, Reg\_Loss:3458.16, Cost:0.00 best\_reg:10000000000.00 avg\_loss\_reg:3256.90: 6%| | 64/1000 [03:12 <47:01, 3.01s/it]  
3305   \*\*\*Trigger Reverse Engineering結束\*\*\*  
3306 Target Class: 0 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 11  
3307   \*\*\*\*\*檢測結果: Model是安全的(Benign)  
3308 檢測結果: Model是安全的(Benign)  
3309 整體耗時: 206.882228225708008  
3310-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000315-----

3311   \*\*\*Pre-Screening開始\*\*\*  
3312   \*\*\*Pre-Screening結束\*\*\*

3313 可能的攻擊方式: Label Specific Backdoor Attack  
3314 可能的 target-victim 配對: ['2-21']  
3315   \*\*\*Trigger Reverse Engineering開始\*\*\*  
3316 Target: 2, victim: 21, Loss: 7.8032, Acc: 0.00%, CE\_Loss: 7.80, Reg\_Loss:2552.49, Cost:0.00 best\_reg:10000000000.00 avg\_loss\_reg:2539.31: 1%| | 10/1000 [00:02 <03:30, 4.69it/s]  
3317   \*\*\*Trigger Reverse Engineering結束\*\*\*  
3318 Target Class: 2 Victim Class: 21 Trigger Size: 1000000000.0 Optimization Steps: 11  
3319   \*\*\*\*\*檢測結果: Model是安全的(Benign)  
3320 檢測結果: Model是安全的(Benign)  
3321 整體耗時: 8.86907434463501  
3322-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000316-----

3323   \*\*\*Pre-Screening開始\*\*\*  
3324   \*\*\*Pre-Screening結束\*\*\*

3325 可能的攻擊方式: Label Specific Backdoor Attack  
3326 可能的 target-victim 配對: ['6-0', '11-0']  
3327   \*\*\*Trigger Reverse Engineering開始\*\*\*  
3328 Target: 11, victim: 0, Loss: 6.7771, Acc: 0.00%, CE\_Loss: 6.78, Reg\_Loss:2515.07, Cost:0.00 best\_reg:10000000000.00 avg\_loss\_reg:2512.11: 2%| | 21/1000 [00:31 <24:07, 1.48s/it]  
3329   \*\*\*Trigger Reverse Engineering結束\*\*\*  
3330 Target Class: 6 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11  
3331   \*\*\*\*\*檢測結果: Model是安全的(Benign)  
3332 檢測結果: Model是安全的(Benign)  
3333 整體耗時: 40.993611335754395  
3334   \*\*\*Pre-Screening開始\*\*\*  
3335   \*\*\*Pre-Screening結束\*\*\*  
3336   \*\*\*Pre-Screening結束\*\*\*  
3337   \*\*\*檢測結果: Model是安全的(Benign)

-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000317-----

```
3338 檢測結果: Model是安全的(Benign)
3339 整體耗時: 6.335360288619995 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000318
3340
3341 ***Pre-Screening開始***
3342 ***Pre-Screening結束***
3343 ***檢測結束***
3344 檢測結果: Model是安全的(Benign)
3345 整體耗時: 12.53815484046936 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000319
3346
3347 ***Pre-Screening開始***
3348 ***Pre-Screening結束***
3349 可能的攻擊方式: Label Specific Backdoor Attack
3350 可能的 target-victim 配對: [7-9]
3351 ***Trigger Reverse Engineering開始***
3352 Target: 7, victim: 9, Loss: 9.3304, Acc: 10.00%, CE_Loss: 9.33, Reg_Loss:2970.36, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2847.66: 2%| | 20/1000 [0:30<24:38, 1.51it/s]
3353 ***Trigger Reverse Engineering結束***
3354 Target Class: 9 Victim Class: 9 Trigger Size: 1000000000.0 Optimization Steps: 21
3355 *****檢測結束*****
3356 檢測結果: Model是安全的(Benign)
3357 整體耗時: 43.0543429851532 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000320
3358
3359 ***Pre-Screening開始***
3360 ***Pre-Screening結束***
3361 ***檢測結束***
3362 檢測結果: Model是安全的(Benign)
3363 整體耗時: 4.648034334182739 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000321
3364
3365 ***Pre-Screening開始***
3366 ***Pre-Screening結束***
3367 可能的攻擊方式: Universal Backdoor Attack
3368 可能的 target class: 4
3369 可能的 victim classes: ALL
3370 ***Trigger Reverse Engineering開始***
3371 Target: 4, victim: 9, Loss: 0.2310, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:230.64, Cost:0.00 best_reg:237.42 avg_loss_reg:228.67: 9%| | 93/1000 [01:14<12:06, 1.25it/s]
3372 early stop 所有
3373 ***Trigger Reverse Engineering結束***
3374 Target Class: 4 Victim Class: all Trigger Size: 237.4216423034668 Optimization Steps: 94
3375 *****檢測結束*****
3376 檢測結果: Model含有後門(Abnormal)
3377 整體耗時: 79.00211191177368 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000322
3378
3379 ***Pre-Screening開始***
3380 ***Pre-Screening結束***
3381 可能的攻擊方式: Label Specific Backdoor Attack
3382 可能的 target-victim 配對: [0-8, '1-3', '2-1', '2-5', '2-6', '3-6', '5-2', '5-6', '6-2', '6-5', '9-3', '10-3', '12-18', '17-8]
3383 ***Trigger Reverse Engineering開始***
3384 Target: 2, victim: 5, Loss: 2.9384, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:110.89, Cost:0.03 best_reg:113.64 avg_loss_reg:109.01: 69%| | 688/1000 [08:05<03:40, 1.42it/s]
3385 early stop 所有
3386 ***Trigger Reverse Engineering結束***
3387 Target Class: 2 Victim Class: 5 Trigger Size: 110.89006042480469 Optimization Steps: 75
3388 ***Symmetric Check開始***
3389 Target: 5, victim: 2, Loss: 1.9302, Acc: 35.00%, CE_Loss: 1.93, Reg_Loss:10730.96, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:10618.96: 100%| | 75/75 [0:51<00:00, 1.44it/s]
3390 ***Symmetric Check結束***
3391 *****檢測結束*****
3392 檢測結果: Model含有後門(Abnormal)
3393 整體耗時: 545.1646373271942 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000323
3394
3395 ***Pre-Screening開始***
3396 ***Pre-Screening結束***
3397 可能的攻擊方式: Label Specific Backdoor Attack
3398 可能的 target-victim 配對: ['9-0']
3399 ***Trigger Reverse Engineering開始***
3400 Target: 9, victim: 0, Loss: 4.0282, Acc: 15.00%, CE_Loss: 4.03, Reg_Loss:3579.64, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:3358.63: 2%| | 20/1000 [00:06<05:40, 2.88it/s]
3401 ***Trigger Reverse Engineering結束***
3402 Target Class: 9 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 21
3403 *****檢測結束*****
3404 檢測結果: Model是安全的(Benign)
3405 整體耗時: 12.6623215675354 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000324
3406
3407 ***Pre-Screening開始***
3408 ***Pre-Screening結束***
```

file - main

```
3409 可能的攻擊方式: Label Specific Backdoor Attack
3410 可能的 target-victim 配對: ['17-0']
3411 ***Trigger Reverse Engineering 開始***
3412 Target: 17, victim: 0, Loss: 9.3512, Acc: 0.00%, CE_Loss: 9.35, Reg_Loss: 9.35, Reg_Loss_reg:2514.84, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2508.08: 1%
3413 ***Trigger Reverse Engineering 結束***
3414 Trigger Reverse Engineering 完成: 10000000000.00
3415 Total Cost: 17. Victim: 0. Total Loss: 9.3512. Success Rate: 1.0
```

### Optimization steps:

卷之三

-拖拉檔案至 D:\Datasets\TroiA\Round3\TrainData\models\unzip\id-0000032

卷之三

Screening 結束 \*\*\* 政擊方式: Universal Backdoor Attack

target class: 6  
victim classes: ALL

ger Reverse Enginee  
6, victim: 12, Loss:

Crop Reverse Engineering

Class: 6 Victim Class  
\*\*\*\*\* 檢測結果 \*\*\*\*\*  
羣：Mode | 有後門

時：1809.00797224

-Screening開始\*\*\*  
-Screening結束\*\*\*

攻擊方式: Label Spec target-victim 配對

ger Reverse Enginee  
; 8, victim: 7, Loss: 8  
acc Days Error Main

ger Reverse English  
Class: 8 Victim Class  
\*\*\*\*\*  
\*\*\*\*\*

果: Model是安全的  
时: 6.76436376571

Screening開始\*\*\*

Screening 結束\*\*\*

果：Model是安全的  
時：18.1855528354

-Screening 開始\*\*\*  
-Screening 終了\*\*\*

攻擊方式: Label Spec target-victim 配對

ger Reverse Enginee  
r: 11, victim: 5, Loss:

Copyright © 2011 by Pearson Education, Inc.

Class: I Victim Classification  
Biometric Check\*  
Victim: 11 Losses

\*\*\*\*\* 檢測結果 \*\*\*\*\*

果：Model含有後門  
時：1071.24110341

-Screening開始\*\*\*

结束\*\*\*

時：15.6225063800

-Screening開始\*\*\*  
-Screening結束\*\*\*

攻擊方式: Universal  
target class: 5

victim classes: All  
ger Reverse Engine

```
3480 early stop 所有
3481 ***Trigger Reverse Engineering結束***
3482 Target Class: 5 Victim Class: all Trigger Size: 265.90570678710935 Optimization Steps: 86
3483 *****檢測結果*****檢測結束*****
3484 檢測結果: Model含有後門(Abnormal)
3485 整體耗時: 700.4093108177185
3486 -----掃描檔案: D:\UU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000331-----
3487 ***Pre-Screening開始***
3488 ***Pre-Screening結束***
3489 可能的攻擊方式: Label Specific Backdoor Attack
3490 可能的 target-victim 配對: ['4-6', '6-4', '14-5']
3491 ***Trigger Reverse Engineering開始***
3492 Target: 14, victim: 5, Loss: 12.6698, Acc: 0.00%, CE_Loss: 12.67, Reg_Loss:2538.88, Cost:0.00 best_Reg:1000000000.00 avg_Loss_Reg:2529.34: 3% | 32/1000 [00:13<06:55, 2.33it/s]
3493 ***Trigger Reverse Engineering結束***
3494 Target Class: 4 Victim Class: 6 Trigger Size: 1000000000.0 Optimization Steps: 11
3495 *****檢測結果*****檢測結束*****
3496 檢測結果: Model是安全的(Benign)
3497 整體耗時: 19.45664691925049
3498 -----掃描檔案: D:\UU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000332-----
3499 ***Pre-Screening開始***
3500 ***Pre-Screening結束***
3501 可能的攻擊方式: Universal Backdoor Attack
3502 可能的 target class: 16
3503 可能的 victim classes: ALL
3504 ***Trigger Reverse Engineering開始***
3505 Target: 16, victim: 17, Loss: 0.3459, Acc: 96.43%, CE_Loss: 0.09, Reg_Loss:874.24, Cost:0.00 best_Reg:886.97 avg_Loss_Reg:887.27: 12% | 120/1000 [51:10<6:15:16, 25.59s/it]
3506 early stop 所有
3507 ***Trigger Reverse Engineering結束***
3508 Target Class: 16 Victim Class: all Trigger Size: 886.9656219482422 Optimization Steps: 121
3509 *****檢測結果*****檢測結束*****
3510 檢測結果: Model含有後門(Abnormal)
3511 整體耗時: 3083.6483561992645
3512 -----掃描檔案: D:\UU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000333-----
3513 ***Pre-Screening開始***
3514 ***Pre-Screening結束***
3515 可能的攻擊方式: Label Specific Backdoor Attack
3516 可能的 target-victim 配對: ['3-5', '15-2', '22-0', '23-1']
3517 ***Trigger Reverse Engineering開始***
3518 Target: 22, victim: 0, Loss: 0.9291, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:48.74, Cost:0.02 best_Reg:52.24 avg_Loss_Reg:48.55: 22% | 219/1000 [00:21<01:15, 10.30it/s]
3519 early stop 所有
3520 ***Trigger Reverse Engineering結束***
3521 Target Class: 22 Victim Class: 0 Trigger Size: 48.737030029296875 Optimization Steps: 114
3522 ***Symmetric Check開始***
3523 Target: 0, victim: 22, Loss: 1.5909, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:258.60, Cost:0.01 best_Reg:259.68 avg_Loss_Reg:259.68: 100% | 114/114 [00:11<00:00, 10.04it/s]
3524 ***Symmetric Check結束*****
3525 檢測結果: Model是安全的(Benign)
3526 整體耗時: 42.551265716552734
3527 -----掃描檔案: D:\UU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000334-----
3528 -----檢測結果: Model是安全的(Benign)
3529 ***Pre-Screening開始***
3530 ***Pre-Screening結束***
3531 檢測結果: Model是安全的(Benign)
3532 整體耗時: 4.497998476028442
3533 檢測結果: Model是安全的(Benign)
3534 -----掃描檔案: D:\UU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000335-----
3535 ***Pre-Screening開始***
3536 ***Pre-Screening結束***
3537 ***檢測結束***
3538 檢測結果: Model是安全的(Benign)
3539 整體耗時: 4.792309522628784
3540 -----掃描檔案: D:\UU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000336-----
3541 ***Pre-Screening開始***
3542 ***Pre-Screening結束***
3543 可能的攻擊方式: Label Specific Backdoor Attack
3544 可能的 target-victim 配對: ['3-5', '3-7', '9-10', '12-1', '12-0', '12-8']
3545 ***Trigger Reverse Engineering開始***
3546 Target: 12, victim: 8, Loss: 12.5223, Acc: 0.00%, CE_Loss: 12.52, Reg_Loss:2484.50, Cost:0.00 best_Reg:1000000000.00 avg_Loss_Reg:2479.38: 6% | 65/1000 [01:01<14:48, 1.05it/s]
3547 ***Trigger Reverse Engineering結束***
3548 Target Class: 3 Victim Class: 5 Trigger Size: 1000000000.0 Optimization Steps: 11
3549 *****檢測結果*****檢測結束*****
3550 檢測結果: Model是安全的(Benign)
```

```

3551 整體耗時: 68.87157225608826 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000337-----
3552 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000337-----
3553 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000337-----
3554 可能的攻擊方式: Label Specific Backdoor Attack
3555 可能的 target-victim 配對: ['6-7', '7-9']
3556 可能的 target-victim 配對: ['6-7', '7-9']
3557 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000338-----
3558 Target: 7 victim: 9, Loss: 12.4700, Acc: 0.00%, CE_Loss: 12.47, Reg_Loss:2593.65, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2570.58: 2%| | 21/1000 [00:17<13:34, 1.20it/s]
3559 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000338-----
3560 Target Class: 6 Victim Class: 7 Trigger Size: 1000000000.00 Optimization Steps: 11
3561 *****檢測結果: Model是安全的(Benign)-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000338-----
3562 檢測結果: Model是安全的(Benign)
3563 整體耗時: 26.603146076202393-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000338-----
3564 *****檢測結果: Model是安全的(Benign)-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000338-----
3565 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000338-----
3566 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000338-----
3567 ***檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000338-----
3568 檢測結果: Model是安全的(Benign)
3569 整體耗時: 7.014855623245239-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000339-----
3570 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000339-----
3571 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000339-----
3572 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000339-----
3573 可能的攻擊方式: Label Specific Backdoor Attack
3574 可能的 target-victim 配對: ['16-10']
3575 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000340-----
3576 Target: 16, victim: 10, Loss: 3.5172, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:299.20, Cost:0.01 best_reg:299.87 avg_loss_reg:299.87: 16%| | 160/1000 [08:32<44:53, 3.21s/it]
3577 0%| | 0/161 [00.00< ?, ?it/s]early stop 所有
3578 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000340-----
3579 Target Class: 16 Victim Class: 10 Trigger Size: 299.2015380859375 Optimization Steps: 161
3580 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000340-----
3581 Target: 10, victim: 16, Loss: 2.3431, Acc: 95.00%, CE_Loss: 0.25, Reg_Loss:3140.07, Cost:0.00 best_reg:3183.31 avg_loss_reg:3055.32: 100%| | 161/161 [09:44<00:00, 3.63s/it]
3582 ***Symmetric Check結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000340-----
3583 *****檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000340-----
3584 檢測結果: Model含有後門(Abnormal)
3585 整體耗時: 1113.822380680084-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000340-----
3586 *****檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000340-----
3587 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000340-----
3588 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000340-----
3589 可能的攻擊方式: Label Specific Backdoor Attack
3590 可能的 target-victim 配對: ['2-7', '3-1', '6-7', '9-3', '10-3', '10-6', '10-15', '11-1', '11-17', '11-18', '14-16', '18-19', '19-1']
3591 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000341-----
3592 Target: 10, victim: 3, Loss: 1.8873, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:1142.91 avg_loss_reg:1151.57: 46%| | 463/1000 [00:49<00:56, 9.43it/s]
3593 early stop 所有
3594 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000341-----
3595 Target Class: 10 Victim Class: 3 Trigger Size: 1140.197021484375 Optimization Steps: 201
3596 *****檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000341-----
3597 檢測結果: Model是安全的(Benign)
3598 整體耗時: 54.143009185791016-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000341-----
3599 *****檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000341-----
3600 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000341-----
3601 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000341-----
3602 ***檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000341-----
3603 檢測結果: Model是安全的(Benign)
3604 整體耗時: 5.157269477844238-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000341-----
3605 *****檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000341-----
3606 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000342-----
3607 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000342-----
3608 ***檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000342-----
3609 檢測結果: Model是安全的(Benign)
3610 整體耗時: 10.143176794052124-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000342-----
3611 *****檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000342-----
3612 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000342-----
3613 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000342-----
3614 ***檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000342-----
3615 檢測結果: Model是安全的(Benign)
3616 整體耗時: 11.981877565383911-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000342-----
3617 *****檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000342-----
3618 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000342-----
3619 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000342-----
3620 可能的攻擊方式: Label Specific Backdoor Attack
3621 可能的 target-victim 配對: ['17-5', '19-5', '22-5']-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000342-----

```

```
e - main
6222 ***Trigger Reverse Engineering開始****
6223 Target: 22, victim: 5, Loss: 10.0402, Acc: 0.00%, CE_Loss: 10.04, Reg_Loss:2555.11, Cost:0.00 best_reg:2542.00: 3%|| | 32/1000 [00:30<15:09, 1.06it/s]
6224 ***Trigger Reverse Engineering結束****
6225 Target Class: 17 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
6226 *****檢測結束*****
6227 檢測結果: Model是安全的(Benign)
6228 整體耗時: 38.2461199760437 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000345-----
6229 ***Pre-Screening開始****
630 ***Pre-Screening結束*****
631 可能的攻擊方式: Label Specific Backdoor Attack
632 可能的 target-victim 配對: ['0-2', '0-6']
633 可能的 target-victim 配對: ['0-5', '3-4', '4-1', '4-3']
634 ***Trigger Reverse Engineering開始****
635 Target: 0, victim: 6, Loss: 1.5478, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:180.21, Cost:0.01 best_reg:181.40 avg_loss_reg:181.40: 16%|| | 164/1000 [08:01<40:55, 2.94s/it]
636 early stop 所有
637 ***Trigger Reverse Engineering結束****
638 Target Class: 0 Victim Class: 6 Trigger Size: 180.20608520507812 Optimization Steps: 121
639 ***Symmetric Check開始****
640 Target: 6, victim: 0, Loss: 0.5100, Acc: 90.00%, CE_Loss: 0.51, Reg_Loss:8921.35, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:8947.13: 100%|| | 121/121 [05:56<00:00, 2
641 ***Symmetric Check結束*****
642 *****檢測結束*****
643 檢測結果: Model含有後門(Abnormal)
644 整體耗時: 846.6174244880676 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000346-----
645 ***Pre-Screening開始****
646 ***Pre-Screening結束*****
647 可能的攻擊方式: Label Specific Backdoor Attack
648 可能的 target-victim 配對: ['0-5', '3-4', '4-1', '4-3']
649 可能的 target-victim 配對: ['0-5', '3-4', '4-1', '4-3']
650 ***Trigger Reverse Engineering開始****
651 Target: 4, victim: 3, Loss: 6.9602, Acc: 15.00%, CE_Loss: 6.96, Reg_Loss:2812.63, Cost:0.00 best_reg:2795.34: 6%|| | 63/1000 [02:22<35:19, 2.26s/it]
652 ***Trigger Reverse Engineering結束****
653 Target Class: 0 Victim Class: 5 Trigger Size: 1000000000.0 Optimization Steps: 11
654 *****檢測結束*****
655 檢測結果: Model是安全的(Benign)
656 整體耗時: 149.1050362586975 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000347-----
657 ***Pre-Screening開始****
658 ***Pre-Screening結束*****
659 ***Pre-Screening結束*****
660 ***檢測結束*****
661 檢測結果: Model是安全的(Benign)
662 整體耗時: 5.385232925415039 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000348-----
663 ***Pre-Screening結束*****
664 ***Pre-Screening開始****
665 ***Pre-Screening結束*****
666 可能的攻擊方式: Universal Backdoor Attack
667 可能的 target class: 0
668 可能的 victim classes: ALL
669 ***Trigger Reverse Engineering開始****
670 Target: 0, victim: 6, Loss: 3.3575, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:3290.78, Cost:0.00 best_reg:3272.15 avg_loss_reg:3345.69: 28%|| | 278/1000 [46:42<2:01:18, 10.08s/it]
671 early stop 所有
672 ***Trigger Reverse Engineering結束*****
673 Target Class: 0 Victim Class: all Trigger Size: 3272.1532389322915 Optimization Steps: 279
674 *****檢測結束*****
675 檢測結果: Model是安全的(Benign)
676 整體耗時: 2809.8104202747345 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000349-----
677 ***Pre-Screening開始****
678 ***Pre-Screening結束*****
679 ***Pre-Screening結束*****
680 可能的攻擊方式: Universal Backdoor Attack
681 可能的 target class: 2
682 可能的 victim classes: ALL
683 ***Trigger Reverse Engineering開始****
684 Target: 2, victim: 20, Loss: 2.1570, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:4845.65, Cost:0.00 best_reg:4851.19 avg_loss_reg:4861.34: 17%|| | 166/1000 [1:03:27<5:18:51, 22.94s/it]
685 early stop 所有
686 ***Trigger Reverse Engineering結束*****
687 Target Class: 2 Victim Class: all Trigger Size: 4841.870989118303 Optimization Steps: 167
688 *****檢測結束*****
689 檢測結果: Model是安全的(Benign)
690 整體耗時: 3821.095847129822 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000350-----
691 ***Pre-Screening開始****
```

```
3693 ***Pre-Screening結束***  
3694 可能的攻擊方式: Label Specific Backdoor Attack  
3695 可能的 target-victim 配對: ['1-7', '1-10']  
3696 ***Trigger Reverse Engineering開始***  
3697 Target: 1, victim: 7, Loss: 3.2053, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:54.42, Cost:0.06 best_reg:54.83 avg_loss_reg:54.83: 10%| | 104/1000 [00:15<02:13, 6.72it/s]  
3698 0%| | 0/83 [00:00 < ?, ?]early stop 所有  
3699 ***Trigger Reverse Engineering結束***  
3700 Target Class: 1 Victim Class: 7 Trigger Size: 54.419059387207 Optimization Steps: 83  
3701 ***Symmetric Check開始***  
3702 Target: 7, victim: 1, Loss: 1.3867, Acc: 35.00%, CE_Loss: 1.39, Reg_Loss:15893.03, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:15759.57: 100%| | 83/83 [00:12<00:00, 6.56it/s]  
3703 ***Symmetric Check結束***  
3704 ***Symmetric Check結束***  
3705 檢測結果: Model含 有後門(Abnormal)  
3706 整體耗時: 33.74845600128174  
3707 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000351-----  
3708 ***Pre-Screening開始***  
3709 ***Pre-Screening結束***  
3710 ***檢測結果: Model是安全的(Benign)  
3711 整體耗時: 6.53731791256714  
3712 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000352-----  
3713 -----  
3714 ***Pre-Screening開始***  
3715 ***Pre-Screening結束***  
3716 可能的攻擊方式: Label Specific Backdoor Attack  
3717 可能的 target-victim 配對: ['0-10', '1-0', '1-7', '1-10', '5-0', '7-1', '8-1', '10-0', '12-10']  
3718 ***Trigger Reverse Engineering開始***  
3719 Target: 1, victim: 0, Loss: 4.7732, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:54.51, Cost:0.09 best_reg:56.07 avg_loss_reg:56.07: 17%| | 167/1000 [00:16<01:20, 10.35it/s]  
3720 early stop 所有  
3721 ***Trigger Reverse Engineering結束***  
3722 Target Class: 1 Victim Class: 0 Trigger Size: 54.510581970214844 Optimization Steps: 68  
3723 ***Symmetric Check開始***  
3724 Target: 0, victim: 1, Loss: 0.4796, Acc: 80.00%, CE_Loss: 0.48, Reg_Loss:17405.35, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:17260.42: 100%| | 68/68 [00:06<00:00, 10.26it/s]  
3725 ***Symmetric Check結束***  
3726 -----  
3727 檢測結果: Model含 有後門(Abnormal)  
3728 整體耗時: 27.5586318171692  
3729 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000353-----  
3730 ***Pre-Screening開始***  
3731 ***Pre-Screening結束***  
3732 ***檢測結果: Model是安全的(Benign)  
3733 整體耗時: 5.758951663970947  
3734 -----  
3735 -----  
3736 ***Pre-Screening開始***  
3737 ***Pre-Screening結束***  
3738 ***檢測結果: Model是安全的(Benign)  
3739 整體耗時: 6.725831031799316  
3740 -----  
3741 -----  
3742 ***Pre-Screening開始***  
3743 ***Pre-Screening結束***  
3744 可能的攻擊方式: Label Specific Backdoor Attack  
3745 可能的 target-victim 配對: ['3-5', '6-8']  
3746 ***Trigger Reverse Engineering開始***  
3747 Target: 6, victim: 8, Loss: 10.2825, Acc: 0.00%, CE_Loss: 10.28, Reg_Loss:2576.66, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2556.35: 2%| | 21/1000 [00:02<02:01, 8.04it/s]  
3748 ***Trigger Reverse Engineering結束***  
3749 Target Class: 3 Victim Class: 5 Trigger Size: 1000000000.0 Optimization Steps: 11  
3750 -----  
3751 檢測結果: Model是安全的(Benign)  
3752 整體耗時: 7.385179042816162  
3753 -----  
3754 ***Pre-Screening開始***  
3755 ***Pre-Screening結束***  
3756 ***檢測結果: Model是安全的(Benign)  
3757 檢測結果: Model是安全的(Benign)  
3758 整體耗時: 5.305670499801636  
3759 -----  
3760 ***Pre-Screening開始***  
3761 ***Pre-Screening結束***  
3762 ***檢測結果: Model是安全的(Benign)  
3763 檢測結果: Model是安全的(Benign)
```

```

3764 整體耗時: 7.878838062286377 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000358-----
3765 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000358-----
3766 可能的攻擊方式: Label Specific Backdoor Attack
3767 可能的target-victim 配對: ['2-1', '3-4', '7-10', '7-12', '10-12', '17-1']
3768 可能的攻擊方式: Label Specific Backdoor Attack
3769 可能的target-victim 配對: ['2-1', '3-4', '7-10', '7-12', '10-12', '17-1']
3770 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000358-----
3771 Target: 7, victim: 12, Loss: 1.6455, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:975.52, Cost:0.00 best_reg:980.22 avg_loss_reg:980.22: 36%|████| | 356/1000 [11:24<20:38, 1.92s/it]
3772 0%| | 0/251 [0:00 < ?, ?it/s]early stop 所有
3773 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000358-----
3774 Target Class: 7 Victim Class: 12 Trigger Size: 975.5238037109375 Optimization Steps: 251
3775 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000358-----
3776 Target: 12, victim: 7, Loss: 2.9300, Acc: 90.00%, CE_Loss: 0.64, Reg_Loss:5160.49, Cost:0.00 best_reg:5196.58 avg_loss_reg:5166.26: 100%|████| | 251/251 [07:53<00:00, 1.89s/it]
3777 ***Symmetric Check結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000358-----
3778 *****檢測結果: Model是安全的(Benign)*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000358-----
3779 檢測結果: Model是安全的(Benign)-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000358-----
3780 整體耗時: 1167.7012283802032 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000358-----
3781 *****檢測結果: Model含有後門(Abnormal)*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000358-----
3782 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000358-----
3783 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000358-----
3784 可能的攻擊方式: Universal Backdoor Attack
3785 可能的 target class: 8
3786 可能的 victim classes: ALL
3787 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000358-----
3788 Target: 8, victim: 22, Loss: 0.2151, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:483.02, Cost:0.00 best_reg:486.89 avg_loss_reg:480.74: 8%|████| | 82/1000 [30:57 < 5:46:38, 22.66s/it]
3789 early stop 所有
3790 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000360-----
3791 Target Class: 8 Victim Class: all Trigger Size: 486.88933715820315 Optimization Steps: 83
3792 *****檢測結果: Model含有後門(Abnormal)*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000360-----
3793 檢測結果: Model含有後門(Abnormal)
3794 整體耗時: 1873.4004418849945 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000360-----
3795 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000360-----
3796 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000360-----
3797 可能的攻擊方式: Label Specific Backdoor Attack
3798 可能的target-victim 配對: ['2-1', '3-13', '13-3', '18-0']
3799 可能的攻擊方式: Label Specific Backdoor Attack
3800 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000360-----
3801 Target: 18, victim: 0, Loss: 0.0839, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:118.10, Cost:0.00 best_reg:486.89 avg_loss_reg:480.74: 8%|████| | 317/1000 [00:22<00:48, 13.94it/s]
3802 early stop 所有
3803 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000360-----
3804 Target Class: 18 Victim Class: 0 Trigger Size: 118.10191345214844 Optimization Steps: 237
3805 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000360-----
3806 Target: 0, victim: 18, Loss: 2.5557, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:435.88, Cost:0.01 best_reg:440.90 avg_loss_reg:440.90: 61%|████| | 144/237 [00:09<00:06, 15.14it/s]
3807 early stop 所有
3808 *****檢測結果: Model是安全的(Benign)*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000361-----
3809 ***Symmetric Check結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000361-----
3810 檢測結果: Model是安全的(Benign)
3811 整體耗時: 41.28732872009277 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000361-----
3812 *****檢測結果: Model含有後門(Abnormal)*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000361-----
3813 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000361-----
3814 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000361-----
3815 可能的攻擊方式: Universal Backdoor Attack
3816 可能的 target class: 15
3817 可能的 victim classes: ALL
3818 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000361-----
3819 Target: 15, victim: 17, Loss: 0.3861, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:571.10, Cost:0.00 best_reg:567.83 avg_loss_reg:571.29: 9%|████| | 91/1000 [04:57 < 49:27, 3.26s/it]
3820 early stop 所有
3821 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000361-----
3822 Target Class: 15 Victim Class: all Trigger Size: 567.8334452311198 Optimization Steps: 92
3823 *****檢測結果: Model含有後門(Abnormal)*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000361-----
3824 檢測結果: Model含有後門(Abnormal)
3825 整體耗時: 302.498186114502 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000361-----
3826 *****檢測結果: Model是安全的(Benign)*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000362-----
3827 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000362-----
3828 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000362-----
3829 可能的攻擊方式: Label Specific Backdoor Attack
3830 可能的target-victim 配對: ['0-16', '8-1', '11-1']
3831 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000362-----
3832 Target: 0, victim: 16, Loss: 2.5543, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:697.10, Cost:0.00 best_reg:715.03 avg_loss_reg:704.37: 21%|████| | 213/1000 [02:11 < 08:05, 1.62it/s]
3833 0%| | 0/172 [00:00 < ?, ?it/s]early stop 所有
3834 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000362-----

```

3835 Target Class: 0 Victim Class: 16 Trigger Size: 697.10009765625 Optimization Steps: 172

3836 \*\*\*Symmetric Check開始\*\*\*

3837 Target: 16, victim: 0, Loss: 1.1219, Acc: 100.00%, CE\_Loss: 0.20, Reg\_Loss:921.77, Cost:0.00 best\_reg:917.25 avg\_loss\_reg:921.78: 100%|██████████| 172/172 [01:45<00:00, 1.63it/s]

3838 \*\*\*Symmetric Check結束\*\*\*

3839 \*\*\*Symmetric Check開始\*\*\*

3840 檢測結果: Model是安全的(Benign)

3841 整體耗時: 243.44098162651062

3842 \*\*\*Pre-Screening開始\*\*\*

3843 \*\*\*Pre-Screening結束\*\*\*

3844 \*\*\*Pre-Screening結束\*\*\*

3845 \*\*\*檢測結束\*\*\*

3846 檢測結果: Model是安全的(Benign)

3847 整體耗時: 10.66360710144043

3848 \*\*\*Pre-Screening開始\*\*\*

3849 \*\*\*Pre-Screening結束\*\*\*

3850 \*\*\*Pre-Screening開始\*\*\*

3851 可能的攻擊方式: Label Specific Backdoor Attack

3852 可能的 target-victim 配對: ['1-3', '1-4', '1-13', '3-0', '7-3', '9-12', '11-0', '14-9']

3853 \*\*\*Trigger Reverse Engineering開始\*\*\*

3854 Target: 7, victim: 13, Loss: 1.0191, Acc: 100.00%, CE\_Loss: 0.12, Reg\_Loss:177.72, Cost:0.01 best\_reg:180.13 avg\_loss\_reg:173.70: 32%|████| 317/1000 [03:15<07:01, 1.62it/s]

3855 early stop 所有

3856 \*\*\*Trigger Reverse Engineering結束\*\*\*

3857 Target Class: 7 Victim Class: 13 Trigger Size: 177.72308349609375 Optimization Steps: 148

3858 \*\*\*Symmetric Check開始\*\*\*

3859 Target: 13, victim: 7, Loss: 5.3910, Acc: 95.00%, CE\_Loss: 0.33, Reg\_Loss:1499.19, Cost:0.00 best\_reg:1537.90 avg\_loss\_reg:1501.97: 100%|████████| 148/148 [01:30<00:00, 1.63it/s]

3860 \*\*\*Symmetric Check結束\*\*\*

3861 \*\*\*Pre-Screening結束\*\*\*

3862 檢測結果: Model是安全的(Benign)

3863 整體耗時: 292.8055000305176

3864 \*\*\*Pre-Screening開始\*\*\*

3865 \*\*\*Pre-Screening結束\*\*\*

3866 可能的攻擊方式: Universal Backdoor Attack

3867 可能的 target class: 0

3868 可能的 victim classes: ALL

3869 \*\*\*Trigger Reverse Engineering開始\*\*\*

3870 Target: 0, victim: 12, Loss: 0.4519, Acc: 100.00%, CE\_Loss: 0.01, Reg\_Loss:3354.73, Cost:0.00 best\_reg:3307.56 avg\_loss\_reg:3286.58: 8%|████| 85/1000 [05:39<1:00:55, 3.99s/it]

3871 early stop 所有

3872 \*\*\*Trigger Reverse Engineering結束\*\*\*

3873 \*\*\*Pre-Screening開始\*\*\*

3874 Target Class: 0 Victim Class: all Trigger Size: 3307.563818359375 Optimization Steps: 86

3875 \*\*\*Pre-Screening結束\*\*\*

3876 檢測結果: Model是安全的(Benign)

3877 整體耗時: 346.6965730190277

3878 \*\*\*Pre-Screening開始\*\*\*

3879 \*\*\*Pre-Screening結束\*\*\*

3880 檢測結果: Model是安全的(Benign)

3881 \*\*\*Pre-Screening結束\*\*\*

3882 檢測結果: Model是安全的(Benign)

3883 整體耗時: 6.257125616073608

3884 \*\*\*Pre-Screening開始\*\*\*

3885 \*\*\*Pre-Screening結束\*\*\*

3886 \*\*\*Pre-Screening結束\*\*\*

3887 可能的攻擊方式: Universal Backdoor Attack

3888 可能的 target class: 11

3889 可能的 victim classes: ALL

3890 \*\*\*Trigger Reverse Engineering開始\*\*\*

3891 Target: 11, victim: 12, Loss: 0.2309, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss:346.29, Cost:0.00 best\_reg:348.40 avg\_loss\_reg:342.99: 7%|████| 170/1000 [45:00<9:57:51, 38.57s/it]

3892 early stop 所有

3893 \*\*\*Trigger Reverse Engineering結束\*\*\*

3894 Target Class: 11 Victim Class: all Trigger Size: 348.4009704589844 Optimization Steps: 71

3895 \*\*\*Pre-Screening結束\*\*\*

3896 檢測結果: Model含有所後門(Abnormal)

3897 整體耗時: 2713.2469820976257

3898 \*\*\*Pre-Screening開始\*\*\*

3899 \*\*\*Pre-Screening結束\*\*\*

3900 \*\*\*Pre-Screening結束\*\*\*

3901 \*\*\*檢測結束\*\*\*

3902 檢測結果: Model是安全的(Benign)

3903 整體耗時: 10.642746210098267

3904 \*\*\*Pre-Screening開始\*\*\*

3905 \*\*\*Pre-Screening結束\*\*\*

```
3906 ***Pre-Screening結束***  
3907 可能的攻擊方式: Label Specific Backdoor Attack  
3908 可能的 target-victim 配對: ['6-1', '6-4']  
3909 ***Trigger Reverse Engineering開始***  
3910 Target: 6, victim: 4, Loss: 4.8886, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:179.35, Cost:0.03 best_reg:179.76 avg_loss_reg:178.64: 15%| | 150/1000 [01:08<06:25, 2.20it/s]  
3911 early stop 所有  
3912 ***Trigger Reverse Engineering結束***  
3913 Target Class: 6 Victim Class: 4 Trigger Size: 179.3450927734375 Optimization Steps: 121  
3914 ***Symmetric Check開始***  
3915 Target: 4, victim: 6, Loss: 0.7534, Acc: 90.00%, CE_Loss: 0.46, Reg_Loss:498.247, Cost:0.00 best_reg:9232.01 avg_loss_reg:4939.88: 100%| | 121/121 [00:51<00:00, 2.35it/s]  
3916 ***Symmetric Check結束***  
3917 ********檢測結果*****  
3918 檢測結果: Model倉有後門(Abnormal)  
3919 整體耗時: 123.55148339271545  
3920 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000370-----  
3921 ***Pre-Screening開始***  
3922 ***Pre-Screening結束***  
3923 ***檢測結果: Model是安全的(Benign)  
3924 整體耗時: 5.930258512496948  
3925 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000371-----  
3926 -----  
3927 ***Pre-Screening開始***  
3928 ***Pre-Screening結束***  
3929 可能的攻擊方式: Label Specific Backdoor Attack  
3930 可能的 target-victim 配對: ['1-7', '1-10', '4-7', '6-5']  
3931 ***Trigger Reverse Engineering開始***  
3932 Target: 1, victim: 7, Loss: 1.8228, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:1113.65, Cost:0.00 best_reg:1116.76 avg_loss_reg:1116.76: 31%| | 313/1000 [02:09<04:43, 2.43it/s]  
3933 early stop 所有  
3934 ***Trigger Reverse Engineering結束***  
3935 Target Class: 1 Victim Class: 7 Trigger Size: 1113.651123046875 Optimization Steps: 239  
3936 -----  
3937 檢測結果: Model是安全的(Benign)  
3938 整體耗時: 135.523259363974  
3939 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000372-----  
3940 -----  
3941 ***Pre-Screening開始***  
3942 可能的攻擊方式: Label Specific Backdoor Attack  
3943 可能的 target-victim 配對: ['0-10', '3-13', '4-13', '7-13']  
3944 ***Trigger Reverse Engineering開始***  
3945 Target: 7, victim: 13, Loss: 3.0903, Acc: 20.00%, CE_Loss: 3.09, Reg_Loss:3235.27, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3052.37: 5%| | 53/1000 [00:49<14:41, 1.07it/s]  
3946 ***Trigger Reverse Engineering結束***  
3947 Target Class: 0 Victim Class: 10 Trigger Size: 10000000000.0 Optimization Steps: 11  
3948 -----  
3949 檢測結果: Model是安全的(Benign)  
3950 整體耗時: 56.9391188621521  
3951 -----  
3952 ***Pre-Screening開始***  
3953 ***Pre-Screening結束***  
3954 可能的攻擊方式: Label Specific Backdoor Attack  
3955 可能的 target-victim 配對: ['2-6']  
3956 ***Trigger Reverse Engineering開始***  
3957 Target: 2, victim: 6, Loss: 9.9193, Acc: 0.00%, CE_Loss: 9.92, Reg_Loss:2606.60, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2578.62: 1%| | 10/1000 [00:09<14:53, 1.11it/s]  
3958 ***Trigger Reverse Engineering結束***  
3959 Target Class: 2 Victim Class: 6 Trigger Size: 10000000000.0 Optimization Steps: 11  
3960 -----  
3961 檢測結果: Model是安全的(Benign)  
3962 整體耗時: 17.979365587234497  
3963 -----  
3964 ***Pre-Screening開始***  
3965 ***Pre-Screening結束***  
3966 ***檢測結果*****  
3967 檢測結果: Model是安全的(Benign)  
3968 整體耗時: 15.113564491271973  
3969 -----  
3970 ***Pre-Screening開始***  
3971 ***Pre-Screening結束***  
3972 可能的攻擊方式: Label Specific Backdoor Attack  
3973 可能的 target-victim 配對: ['1-10', '2-16', '2-12', '3-17', '3-1', '4-7', '5-17', '6-20', '7-5', '7-12', '7-17', '8-0', '8-20', '9-3', '9-7', '10-1', '10-9', '11-4', '11-5', '11-12', '13-2', '14-1', '16-2', '17-5', '17-7', '17-12', '18-1', '18-9', '18-20', '19-6', '20-6', '21-15', '21-20', '21-19']  
3974 ***Trigger Reverse Engineering開始***  
3975 Target: 11, victim: 12, Loss: 2.0982, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:1215.98, Cost:0.00 best_reg:1217.94 avg_loss_reg:1227.84: 83%| | 830/1000 [01:43<00:21, 8.00it/s]  
3976 early stop 所有
```

```
3977 ***Trigger Reverse Engineering結束***  
3978 Target Class: 11 Victim Class: 12 Trigger Size: 1215.9766845703125 Optimization Steps: 405  
3979 ****檢測結束*****  
3980 檢測結果: Model是安全的(Benign)  
3981 整體耗時: 109,23744702339172  
3982 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000376-----  
3983 ***Pre-Screening開始***  
3984 ***Pre-Screening結束***  
3985 ***檢測結束***  
3986 檢測結果: Model是安全的(Benign)  
3987 整體耗時: 6.0404393672943115  
3988 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000377-----  
3989 ***Pre-Screening開始***  
3990 ***Pre-Screening結束***  
3991 可能的攻擊方式: Label Specific Backdoor Attack  
3992 可能的 target-victim 配對: ['0-2', '1-0', '1-4', '2-1', '3-5']  
3993 ***Trigger Reverse Engineering開始***  
3994 Target: 3, victim: 5 Loss: 4.6918, Acc: 0.00%, CE_Loss: 4.69, Reg_Loss: 2557.34, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2542.31: 6% █ | 64/1000 [00:29<07:10, 2.17it/s]  
3995 ***Trigger Reverse Engineering結束***  
3996 Target Class: 0 Victim Class: 2 Trigger Size: 10000000000.0 Optimization Steps: 11  
3997 *****檢測結束*****  
3998 檢測結果: Model是安全的(Benign)  
3999 整體耗時: 33.2822949886322  
4000 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000378-----  
4001 ***Pre-Screening開始***  
4002 ***Pre-Screening結束***  
4003 ***檢測結束***  
4004 檢測結果: Model是安全的(Benign)  
4005 整體耗時: 6.759771108627319  
4006 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000379-----  
4007 ***Pre-Screening開始***  
4008 ***Pre-Screening結束***  
4009 可能的攻擊方式: Label Specific Backdoor Attack  
4010 可能的 target-victim 配對: ['1-2', '8-2']  
4011 ***Trigger Reverse Engineering開始***  
4012 Target: 1, victim: 2, Loss: 1.1429, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:454.84, Cost:0.00 best_reg:458.83 avg_loss_reg:449.87: 25% █ | 248/1000 [02:45<08:22, 1.50it/s]  
4013 early stop 所有  
4014 ***Trigger Reverse Engineering結束***  
4015 Target Class: 1 Victim Class: 2 Trigger Size: 454.83990478515625 Optimization Steps: 238  
4016 ***Symmetric Check開始***  
4017 Target: 2, victim: 1 Loss: 1.6893, Acc: 100.00%, CE_Loss: 0.55, Reg_Loss:508.24, Cost:0.00 best_reg:485.99 avg_loss_reg:508.10: 100% █ | 238/238 [02:42<00:00, 1.46it/s]  
4018 ***Symmetric Check結束***  
4019 *****檢測結束*****  
4020 檢測結果: Model是安全的(Benign)  
4021 整體耗時: 334.1624011993408  
4022 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000380-----  
4023 ***Pre-Screening開始***  
4024 ***Pre-Screening結束***  
4025 可能的攻擊方式: Label Specific Backdoor Attack  
4026 可能的 target-victim 配對: ['15-1', '15-7']  
4027 ***Trigger Reverse Engineering開始***  
4028 Target: 15, victim: 1, Loss: 3.0122, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:810.54, Cost:0.00 best_reg:811.22 avg_loss_reg:804.46: 19% █ | 193/1000 [00:27<01:54, 7.05it/s]  
4029 early stop 所有  
4030 ***Trigger Reverse Engineering結束***  
4031 Target Class: 15 Victim Class: 1 Trigger Size: 810.542724609375 Optimization Steps: 183  
4032 ***Symmetric Check開始***  
4033 Target: 1, victim: 15, Loss: 1.6863, Acc: 70.00%, CE_Loss: 0.79, Reg_Loss:4562.24, Cost:0.00 best_reg:10118.81 avg_loss_reg:4587.21: 100% █ | 183/183 [00:26<00:00, 6.97it/s]  
4034 ***Symmetric Check結束***  
4035 *****檢測結束*****  
4036 檢測結果: Model含有後門(Abnormal)  
4037 整體耗時: 58.86849761009216  
4038 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000381-----  
4039 ***Pre-Screening開始***  
4040 ***Pre-Screening結束***  
4041 ***檢測結束***  
4042 檢測結果: Model是安全的(Benign)  
4043 整體耗時: 3.062547206878662  
4044 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000382-----  
4045 ***Pre-Screening開始***  
4046 ***Pre-Screening結束***  
4047 可能的攻擊方式: Universal Backdoor Attack
```

```
4048 可能的 target class: 7  
4049 可能的 victim classes: ALL  
4050 ***Trigger Reverse Engineering開始***  
4051 Target: 7, victim: 16, Loss: 0.3407, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:511.07, Cost:0.00 best_reg:505.86 avg_loss_reg:507.27: 16%|████| | 163/1000 [1:00:26<5:10:19, 22.25s/it]  
4052 early stop 所有  
4053 ***Trigger Reverse Engineering結束***  
4054 Target Class: 7 Victim Class: all Trigger Size: 505.8648274739583 Optimization Steps: 164  
4055 *****檢測結果: Model含有後門(Abnormal)  
4056 檢測結果: Model含有後門(Abnormal)  
4057 整體耗時: 3638.8696593966675  
4058 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000383-----  
4059 ***Pre-Screening開始***  
4060 ***Pre-Screening結束***  
4061 可能的攻擊方式: Label Specific Backdoor Attack  
4062 可能的 target-victim 配對: ['3-14', '10-5', '10-18', '21-1']  
4063 ***Trigger Reverse Engineering開始***  
4064 Target: 10, victim: 18, Loss: 2.5464, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:315.79, Cost:0.01 best_reg:316.40 avg_loss_reg:316.40: 19%|████| | 191/1000 [00:24<01:43, 7.84it/s]  
4065 early stop 所有  
4066 ***Trigger Reverse Engineering結束***  
4067 Target Class: 10 Victim Class: 18 Trigger Size: 315.7879943847656 Optimization Steps: 128  
4068 ***Symmetric Check開始***  
4069 Target: 18, victim: 10, Loss: 3.1301, Acc: 70.00%, CE_Loss: 0.94, Reg_Loss:7379.08, Cost:0.00 best_reg:14340.97 avg_loss_reg:7468.34: 100%|████| | 128/128 [00:16<00:00, 7.70it/s]  
4070 ***Symmetric Check結束***  
4071 *****檢測結果: Model含有後門(Abnormal)  
4072 檢測結果: Model含有後門(Abnormal)  
4073 整體耗時: 46.7012241973877  
4074 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000384-----  
4075 ***Pre-Screening開始***  
4076 ***Pre-Screening結束***  
4077 可能的攻擊方式: Label Specific Backdoor Attack  
4078 可能的 target-victim 配對: ['0-1', '0-16', '1-16', '2-12', '7-8', '10-12', '12-2', '14-15', '15-16', '16-1', '16-15']  
4079 ***Trigger Reverse Engineering開始***  
4080 Target: 16, victim: 1, Loss: 2.0948, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:824.44, Cost:0.00 best_reg:825.00 avg_loss_reg:827.18: 71%|████| | 714/1000 [01:12<00:28, 9.88it/s]  
4081 early stop 所有  
4082 ***Trigger Reverse Engineering結束***  
4083 Target Class: 16 Victim Class: 1 Trigger Size: 824.4365234375 Optimization Steps: 574  
4084 ***Symmetric Check開始***  
4085 Target: 1, victim: 16, Loss: 6.3692, Acc: 100.00%, CE_Loss: 0.33, Reg_Loss:1789.55, Cost:0.00 best_reg:1790.88 avg_loss_reg:1798.32: 95%|████| | 544/574 [00:55<00:03, 9.80it/s]  
4086 early stop 所有  
4087 ***Symmetric Check結束***  
4088 *****檢測結果: Model是安全的(Benign)  
4089 檢測結果: Model是安全的(Benign)  
4090 整體耗時: 132.8791128997803  
4091 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000385-----  
4092 ***Pre-Screening開始***  
4093 ***Pre-Screening結束***  
4094 ***檢測結果: Model是安全的(Benign)  
4095 檢測結果: Model是安全的(Benign)  
4096 整體耗時: 13.34387731552124  
4097 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000386-----  
4098 ***Pre-Screening開始***  
4099 ***Pre-Screening結束***  
4100 可能的攻擊方式: Universal Backdoor Attack  
4101 可能的 target class: 1  
4102 可能的 victim classes: ALL  
4103 ***Trigger Reverse Engineering開始***  
4104 Target: 1, victim: 12, Loss: 5.2271, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:3484.75, Cost:0.00 best_reg:3487.93 avg_loss_reg:3488.08: 21%|████| | 208/1000 [52:49<3:21:08, 15.24s/it]  
4105 early stop 所有  
4106 ***Trigger Reverse Engineering結束***  
4107 Target Class: 1 Victim Class: all Trigger Size: 3484.59853515625 Optimization Steps: 209  
4108 *****檢測結果: Model是安全的(Benign)  
4109 檢測結果: Model是安全的(Benign)  
4110 整體耗時: 3180.5453498363495  
4111 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000387-----  
4112 ***Pre-Screening開始***  
4113 ***Pre-Screening結束***  
4114 ***檢測結果: Model是安全的(Benign)  
4115 檢測結果: Model是安全的(Benign)  
4116 整體耗時: 17.066123485565186  
4117 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000388-----  
4118 ***Pre-Screening開始***
```

```
4119 ***Pre-Screening結束***  
4120 可能的攻擊方式: Universal Backdoor Attack  
4121 可能的 target class: 11  
4122 可能的 victim classes: ALL  
4123 ***Trigger Reverse Engineering開始***  
4124 Target: 11, victim: 16, Loss: 0.6910, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:460.67, Cost:0.00 best_reg:465.29 avg_loss_reg:470.59: 15%| | 152/1000 [1:38:16<9:08:15, 38.79s/it]  
4125 early stop 所有  
4126 ***Trigger Reverse Engineering結束***  
4127 Target Class: 11 Victim Class: all Trigger Size: 465.29006125710225 Optimization Steps: 153  
4128 ****檢測結果: Model倉有後門(Abnormal)  
4129 檢測結果: Model倉有後門(Abnormal)  
4130 整體耗時: 5912.958165884018  
4131 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000389-----  
4132 ***Pre-Screening開始***  
4133 ***Pre-Screening結束***  
4134 可能的攻擊方式: Universal Backdoor Attack  
4135 可能的 target class: 4  
4136 可能的 victim classes: ALL  
4137 ***Trigger Reverse Engineering開始***  
4138 Target: 4, victim: 14, Loss: 0.1276, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:25.19, Cost:0.01 best_reg:25.11 avg_loss_reg:24.55: 6%| | 57/1000 [33:18<9:11:07, 35.07s/it]  
4139 early stop 所有  
4140 ***Trigger Reverse Engineering結束***  
4141 Target Class: 4 Victim Class: all Trigger Size: 25.106945419311522 Optimization Steps: 58  
4142 ****檢測結果: Model倉有後門(Abnormal)  
4143 檢測結果: Model倉有後門(Abnormal)  
4144 整體耗時: 2013.7501435279846  
4145 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000390-----  
4146 ***Pre-Screening開始***  
4147 ***Pre-Screening結束***  
4148 ****檢測結果: Model是安全的(Benign)  
4149 檢測結果: Model是安全的(Benign)  
4150 整體耗時: 10.823410749435425  
4151 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000391-----  
4152 ***Pre-Screening開始***  
4153 ***Pre-Screening結束***  
4154 可能的攻擊方式: Label Specific Backdoor Attack  
4155 可能的 target-victim 配對: ['1-0', '1-2', '1-4']  
4156 ***Trigger Reverse Engineering開始***  
4157 Target: 1, victim: 4, Loss: 9.4199, Acc: 0.00%, CE_Loss: 9.42, Reg_Loss:2574.83, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2558.21: 4%| | 42/1000 [02:17<52:13, 3.27s/it]  
4158 ***Trigger Reverse Engineering結束***  
4159 Target Class: 1 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 21  
4160 ****檢測結果: Model是安全的(Benign)  
4161 整體耗時: 146.41415405273438  
4162 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000392-----  
4163 ***Pre-Screening開始***  
4164 ***Pre-Screening結束***  
4165 ***Pre-Screening開始***  
4166 ***Pre-Screening結束***  
4167 檢測結果: Model是安全的(Benign)  
4168 整體耗時: 5.1223389316558838  
4169 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000393-----  
4170 ***Pre-Screening開始***  
4171 ***Pre-Screening結束***  
4172 可能的攻擊方式: Label Specific Backdoor Attack  
4173 可能的 target-victim 配對: ['1-5']  
4174 ***Trigger Reverse Engineering開始***  
4175 Target: 1, victim: 5, Loss: 10.9795, Acc: 0.00%, CE_Loss: 10.98, Reg_Loss:2566.29, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2549.80: 1%| | 10/1000 [00:01<02:20, 7.03it/s]  
4176 ***Trigger Reverse Engineering結束***  
4177 Target Class: 1 Victim Class: 5 Trigger Size: 1000000000.0 Optimization Steps: 11  
4178 ****檢測結果: Model是安全的(Benign)  
4179 檢測結果: Model是安全的(Benign)  
4180 整體耗時: 6.40530800819397  
4181 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000394-----  
4182 ***Pre-Screening開始***  
4183 ***Pre-Screening結束***  
4184 ***檢測結果: Model是安全的(Benign)  
4185 檢測結果: Model是安全的(Benign)  
4186 整體耗時: 10.0305625505066  
4187 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000395-----  
4188 ***Pre-Screening開始***  
4189 ***Pre-Screening結束***
```

4190 \*\*\*檢測結束\*\*\*  
4191 檢測結果: Model是安全的(Benign)  
4192 整體耗時: 5.8176820278167725  
4193 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000396-----  
4194 \*\*\*Pre-Screening開始\*\*\*  
4195 \*\*\*Pre-Screening結束\*\*\*  
4196 可能的攻擊方式: Universal Backdoor Attack  
4197 可能的 target class: 2  
4198 可能的 victim classes: ALL  
4199 \*\*\*Trigger Reverse Engineering開始\*\*\*  
4200 Target: 2, victim: 22, Loss: 0.1062, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss:354.49, Cost:0.00 best\_reg:348.38 avg\_loss\_reg:346.73: 8% █ | 78/1000 [48:01 <9:27:41, 36.94s/it]  
4201 early stop 所有  
4202 \*\*\*Trigger Reverse Engineering結束\*\*\*  
4203 Target Class: 2 Victim Class: all Trigger Size: 348.3751907348633 Optimization Steps: 79  
4204 \*\*\*\*\*檢測結束\*\*\*\*\*  
4205 檢測結果: Model含有後門(Abnormal)  
4206 整體耗時: 2900.60420655899  
4207 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000397-----  
4208 \*\*\*Pre-Screening開始\*\*\*  
4209 \*\*\*Pre-Screening結束\*\*\*  
4210 可能的攻擊方式: Universal Backdoor Attack  
4211 可能的 target class: 1  
4212 可能的 victim classes: ALL  
4213 \*\*\*Trigger Reverse Engineering開始\*\*\*  
4214 Target: 1, victim: 9, Loss: 1.2414, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss:163.45, Cost:0.01 best\_reg:163.82 avg\_loss\_reg:162.64: 9% █ | 87/1000 [01:49 < 19:04, 1.25s/it]  
4215 early stop 所有  
4216 \*\*\*Trigger Reverse Engineering結束\*\*\*  
4217 Target Class: 1 Victim Class: all Trigger Size: 163.8156509399414 Optimization Steps: 88  
4218 \*\*\*\*\*檢測結束\*\*\*\*\*  
4219 檢測結果: Model含有後門(Abnormal)  
4220 整體耗時: 117.99328184127808  
4221 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000398-----  
4222 \*\*\*Pre-Screening開始\*\*\*  
4223 \*\*\*Pre-Screening結束\*\*\*  
4224 可能的攻擊方式: Label Specific Backdoor Attack  
4225 可能的 target-victim 配對: ['9-1']  
4226 \*\*\*Trigger Reverse Engineering開始\*\*\*  
4227 Target: 9, victim: 1, Loss: 8.7729, Acc: 0.00%, CE\_Loss: 8.77, Reg\_Loss:2574.31, Cost:0.00 best\_reg:10000000000.00 avg\_loss\_reg:2557.49: 1% | 10/1000 [00:05 < 09:46, 1.69it/s]  
4228 \*\*\*Trigger Reverse Engineering結束\*\*\*  
4229 Target Class: 9 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11  
4230 \*\*\*\*\*檢測結束\*\*\*\*\*  
4231 檢測結果: Model是安全的(Benign)  
4232 整體耗時: 11.585622310638428  
4233 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000399-----  
4234 \*\*\*Pre-Screening開始\*\*\*  
4235 \*\*\*Pre-Screening結束\*\*\*  
4236 \*\*\*\*\*檢測結束\*\*\*\*\*  
4237 檢測結果: Model是安全的(Benign)  
4238 整體耗時: 14.854406595230103  
4239 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000400-----  
4240 \*\*\*Pre-Screening開始\*\*\*  
4241 \*\*\*Pre-Screening結束\*\*\*  
4242 可能的攻擊方式: Label Specific Backdoor Attack  
4243 可能的 target-victim 配對: ['2-23', '16-4', '20-18']  
4244 \*\*\*Trigger Reverse Engineering開始\*\*\*  
4245 Target: 2, victim: 23, Loss: 1.0036, Acc: 100.00%, CE\_Loss: 0.22, Reg\_Loss:780.74, Cost:0.00 best\_reg:784.12 avg\_loss\_reg:784.12: 23% █ | 231/1000 [00:34 < 01:56, 6.61it/s]  
4246 0% | 0/210 [00:00 < ?, ?it/s] early stop 所有  
4247 \*\*\*Trigger Reverse Engineering結束\*\*\*  
4248 Target Class: 2 Victim Class: 23 Trigger Size: 780.7389526367188 Optimization Steps: 210  
4249 \*\*\*Symmetric Check開始\*\*\*  
4250 Target: 23, victim: 2, Loss: 3.1949, Acc: 100.00%, CE\_Loss: 0.33, Reg\_Loss:376.78, Cost:0.01 best\_reg:379.88 avg\_loss\_reg:379.88: 88% █ | 185/210 [00:29 < 00:04, 6.20it/s]  
4251 early stop 所有  
4252 \*\*\*Symmetric Check結束\*\*\*  
4253 \*\*\*\*\*檢測結束\*\*\*\*\*  
4254 檢測結果: Model是安全的(Benign)  
4255 整體耗時: 70.99684596061707  
4256 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000401-----  
4257 \*\*\*Pre-Screening開始\*\*\*  
4258 \*\*\*Pre-Screening結束\*\*\*  
4259 \*\*\*檢測結束\*\*\*  
4260 檢測結果: Model是安全的(Benign)

4261 整體耗時: 5.263123512268066 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000402  
4262 \*\*\*Pre-Screening開始\*\*\*  
4263 \*\*\*Pre-Screening結束\*\*\*  
4264 \*\*\*Pre-Screening開始\*\*\*  
4265 \*\*\*檢測結束\*\*\*  
4266 檢測結果: Model是安全的(Benign)  
4267 整體耗時: 3.311382532119751  
4268 \*\*\*Pre-Screening開始\*\*\* | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000403  
4269 \*\*\*Pre-Screening結束\*\*\*  
4270 \*\*\*Pre-Screening開始\*\*\* | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000403  
4271 可能的攻擊方式: Universal Backdoor Attack  
4272 可能的 target class: 11  
4273 可能的 victim classes: ALL  
4274 \*\*\*Trigger Reverse Engineering開始\*\*\*  
4275 Target: 11, victim: 12, Loss: 0.3512, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss: 156.09, Cost:0.00 best\_reg:165.57 avg\_loss\_reg:154.15: 5% | | 48/1000 [07:16<2:24:17, 9.09s/it]  
4276 early stop 所有  
4277 \*\*\*Trigger Reverse Engineering結束\*\*\*  
4278 Target Class: 11 Victim Class: all Trigger Size: 165.57279052734376 Optimization Steps: 49  
4279 \*\*\*\*\*檢測結束\*\*\*\*\*  
4280 檢測結果: Model含有後門(Abnormal)  
4281 整體耗時: 442.98185500827026 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000404  
4282 \*\*\*Pre-Screening開始\*\*\*  
4283 \*\*\*Pre-Screening結束\*\*\*  
4284 \*\*\*Pre-Screening開始\*\*\*  
4285 可能的攻擊方式: Label Specific Backdoor Attack  
4286 可能的 target-victim 配對: ['7-0', '7-2']  
4287 \*\*\*Trigger Reverse Engineering開始\*\*\*  
4288 Target: 7, victim: 2, Loss: 2.3866, Acc: 100.00%, CE\_Loss: 0.01, Reg\_Loss:41.25, Cost:0.06 best\_reg:42.38 avg\_loss\_reg:42.38: 8% | | 79/1000 [02:57<34:24, 2.24s/it]  
4289 early stop 所有  
4290 \*\*\*Trigger Reverse Engineering結束\*\*\*  
4291 Target Class: 7 Victim Class: 2 Trigger Size: 41.25117874145508 Optimization Steps: 69  
4292 \*\*\*Symmetric Check開始\*\*\*  
4293 Target: 2, victim: 7, Loss: 1.2989, Acc: 95.00%, CE\_Loss: 0.46, Reg\_Loss:2846.08, Cost:0.00 best\_reg:6141.67 avg\_loss\_reg:2873.37: 100% | | 69/69 [02:32<00:00, 2.21s/it]  
4294 \*\*\*Symmetric Check結束\*\*\*  
4295 \*\*\*\*\*檢測結束\*\*\*\*\*  
4296 檢測結果: Model含有後門(Abnormal)  
4297 整體耗時: 336.5531601905823 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000405  
4298 \*\*\*Pre-Screening開始\*\*\* | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000405  
4299 \*\*\*Pre-Screening結束\*\*\*  
4300 \*\*\*Pre-Screening開始\*\*\*  
4301 \*\*\*檢測結束\*\*\*  
4302 檢測結果: Model是安全的(Benign)  
4303 整體耗時: 11.637441873550415 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000406  
4304 \*\*\*Pre-Screening開始\*\*\*  
4306 \*\*\*Pre-Screening結束\*\*\*  
4307 可能的攻擊方式: Label Specific Backdoor Attack  
4308 可能的 target-victim 配對: ['4-3']  
4309 \*\*\*Trigger Reverse Engineering開始\*\*\*  
4310 Target: 4, victim: 3, Loss: 7.1372, Acc: 10.00%, CE\_Loss: 7.14, Reg\_Loss:3155.50, Cost:0.00 best\_reg:10000000000.00 avg\_loss\_reg:2996.66: 2% | | 20/1000 [00:06<05:36, 2.91it/s]  
4311 \*\*\*Trigger Reverse Engineering結束\*\*\*  
4312 Target Class: 4 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 21  
4313 \*\*\*\*\*檢測結束\*\*\*\*\*  
4314 檢測結果: Model是安全的(Benign)  
4315 整體耗時: 12.280215501785278 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000407  
4316 \*\*\*Pre-Screening開始\*\*\*  
4317 \*\*\*Pre-Screening結束\*\*\*  
4318 \*\*\*Pre-Screening結束\*\*\*  
4319 可能的攻擊方式: Label Specific Backdoor Attack  
4320 可能的 target-victim 配對: ['0-3', '0-5', '0-9', '9-0', '9-3']  
4321 \*\*\*Trigger Reverse Engineering開始\*\*\*  
4322 Target: 9, victim: 3, Loss: 8.93, Acc: 0.00%, CE\_Loss: 8.93, Reg\_Loss:2566.66, Cost:0.00 best\_reg:2551.13: 5% | | 54/1000 [00:25<07:24, 2.13it/s]  
4323 \*\*\*Trigger Reverse Engineering結束\*\*\*  
4324 Target Class: 0 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 11  
4325 \*\*\*\*\*檢測結束\*\*\*\*\*  
4326 檢測結果: Model是安全的(Benign)  
4327 整體耗時: 31.771421909332275 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000408  
4328 \*\*\*Pre-Screening開始\*\*\*  
4329 \*\*\*Pre-Screening結束\*\*\*  
4330 \*\*\*Pre-Screening結束\*\*\*  
4331 \*\*\*檢測結束\*\*\*

```

4332 檢測結果: Model是安全的(Benign)
4333 整體耗時: 12.038453817367554 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000409
4334 ***Pre-Screening開始***
4335 ***Pre-Screening結束***
4336 ***Pre-Screening結束***
4337 ***檢測結束*** 檢測結果: Model是安全的(Benign)
4338 整體耗時: 5.76853728943726 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000410
4340 -----



4341 ***Pre-Screening開始***
4342 ***Pre-Screening結束*** 可能的攻擊方式: Label Specific Backdoor Attack
4343 可能的target-victim 配對: ['3-4', '3-5', '4-3']
4344 可能的Trigger Reverse Engineering開始***
4345 Target: 3; victim: 5; Loss: 1.4301; Acc: 100.00%; CE_Loss: 0.12; Reg_Loss:171.93, Cost:0.01 best_reg:172.52 avg_loss_reg:172.18: 12% █ | 117/1000 [00:14<01:47, 8.19it/s]
4346 early stop 所有
4347 ***Trigger Reverse Engineering結束*** Target Class: 3; Victim Class: 5; Trigger Size: 171.92515563964844 Optimization Steps: 100
4348 ***Symmetric Check開始*** Target: 5; victim: 3; Loss: 1.8552; Acc: 50.00%; CE_Loss: 1.86; Reg_Loss:9442.78, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:9370.38: 100% █ | 100/100 [00:12<00:00, 8.28it/s]
4349 Target Class: 3; Victim Class: 5; Trigger Size: 171.92515563964844 Optimization Steps: 100
4350 ***Symmetric Check結束*** 檢測結果: Model含有後門(Abnormal)
4351 整體耗時: 28.2333701467514038 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000411
4352 ***Symmetric Check結束*** 檢測結果: Model含有後門(Abnormal)
4353 *****檢測結束***** 檢測結果: Model含有後門(Abnormal)
4354 檢測結果: Model含有後門(Abnormal)
4355 整體耗時: 4.866551876068115 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000412
4356 ***Pre-Screening開始***
4357 ***Pre-Screening結束*** 可能的攻擊方式: Universal Backdoor Attack
4358 檢測結果: Model是安全的(Benign)
4359 ***檢測結束*** 檢測結果: Model是安全的(Benign)
4360 檢測結果: Model是安全的(Benign)
4361 整體耗時: 4.95885968208313 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000413
4362 ***Pre-Screening開始***
4363 ***Pre-Screening結束*** 可能的 target class: 2
4364 ***Pre-Screening結束*** 可能的 victim classes: ALL
4365 可能的攻擊方式: Universal Backdoor Attack
4366 可能的 target class: 2
4367 可能的 victim classes: ALL
4368 ***Trigger Reverse Engineering開始*** Target: 2; victim: 9; Loss: 0.1640; Acc: 100.00%; CE_Loss: 0.00; Reg_Loss:109.36, Cost:0.00 best_reg:119.03 avg_loss_reg:108.64: 5% █ | 54/1000 [00:42<12:26, 1.27it/s]
4369 Target Class: 2; Victim Class: all; Trigger Size: 119.02754974365234 Optimization Steps: 55
4370 early stop 所有
4371 ***Trigger Reverse Engineering結束*** Target Class: 7; Victim Class: 9; Trigger Size: 119.02754974365234 Optimization Steps: 55
4372 Target Class: 2; Victim Class: all; Trigger Size: 119.02754974365234 Optimization Steps: 55
4373 *****檢測結束***** 檢測結果: Model含有後門(Abnormal)
4374 檢測結果: Model含有後門(Abnormal)
4375 整體耗時: 46.95885968208313 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000414
4376 ***Pre-Screening開始***
4377 ***Pre-Screening結束*** 可能的攻擊方式: Label Specific Backdoor Attack
4378 可能的 target-victim 配對: ['2-5', '3-0', '3-5', '4-8', '5-2', '5-3', '7-8', '7-9', '10-0']
4379 可能的攻擊方式: Label Specific Backdoor Attack
4380 可能的 target-victim 配對: ['2-5', '3-0', '3-5', '4-8', '5-2', '5-3', '7-8', '7-9', '10-0']
4381 ***Trigger Reverse Engineering開始*** Target: 7; victim: 9; Loss: 3.1831; Acc: 100.00%; CE_Loss: 0.13; Reg_Loss:267.62, Cost:0.01 best_reg:270.47 avg_loss_reg:266.60: 30% █ | 299/1000 [00:36<01:24, 8.26it/s]
4382 Target: 7; victim: 9; Loss: 3.1831; Acc: 100.00%; CE_Loss: 0.13; Reg_Loss:267.62, Cost:0.01 best_reg:270.47 avg_loss_reg:266.60: 30% █ | 299/1000 [00:36<01:24, 8.26it/s]
4383 early stop 所有
4384 ***Trigger Reverse Engineering結束*** Target Class: 7; Victim Class: 9; Trigger Size: 267.62371826171875 Optimization Steps: 144
4385 Target Class: 7; Victim Class: 9; Trigger Size: 267.62371826171875 Optimization Steps: 144
4386 ***Symmetric Check開始*** Target: 9; victim: 7; Loss: 3.6260; Acc: 20.00%; CE_Loss: 1.38; Reg_Loss:7591.18, Cost:0.00 best_reg:14895.91 avg_loss_reg:7643.52: 100% █ | 144/144 [00:17<00:00, 8.25it/s]
4387 Target: 9; victim: 7; Loss: 3.6260; Acc: 20.00%; CE_Loss: 1.38; Reg_Loss:7591.18, Cost:0.00 best_reg:14895.91 avg_loss_reg:7643.52: 100% █ | 144/144 [00:17<00:00, 8.25it/s]
4388 ***Symmetric Check結束*** 檢測結果: Model含有後門(Abnormal)
4389 *****檢測結束***** 檢測結果: Model含有後門(Abnormal)
4390 檢測結果: Model含有後門(Abnormal)
4391 整體耗時: 58.883779527576836 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000414
4392 -----



4393 ***Pre-Screening開始***
4394 ***Pre-Screening結束*** 檢測結果: Model是安全的(Benign)
4395 ***檢測結束*** 檢測結果: Model是安全的(Benign)
4396 檢測結果: Model是安全的(Benign)
4397 整體耗時: 14.39618968963623 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000415
4398 ***Pre-Screening開始***
4399 ***檢測結束*** 檢測結果: Model是安全的(Benign)
4400 ***Pre-Screening結束*** 檢測結果: Model是安全的(Benign)
4401 ***檢測結束*** 檢測結果: Model是安全的(Benign)
4402 檢測結果: Model是安全的(Benign)

```

```
4403 整體耗時: 13.509204149246216 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000416-----  
4404 ***Pre-Screening開始***  
4405 ***Pre-Screening結束***  
4406 ***Pre-Screening開始***  
4407 ***檢測結束***  
4408 檢測結果: Model是安全的(Benign)  
4409 整體耗時: 5.237755298614502  
4410 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000417-----  
4411 ***Pre-Screening開始***  
4412 ***Pre-Screening結束***  
4413 可能的攻擊方式: Label Specific Backdoor Attack  
4414 可能的 target-victim 配對: ['0-1', '2-3', '4-1', '10-3', '12-1', '12-5', '12-16', '17-16']  
4415 ***Trigger Reverse Engineering開始***  
4416 Target: 17, victim: 16 Loss: 10.2244, Acc: 0.00%, CE_Loss: 10.22, Reg_Loss: 2563.50, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2548.03: 10% █ | 97/1000 [00:11<01:51, 8.11it/s]  
4417 ***Trigger Reverse Engineering結束***  
4418 Target Class: 0 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11  
4419 *****檢測結束*****  
4420 檢測結果: Model是安全的(Benign)  
4421 整體耗時: 17.779464721679688 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000418-----  
4422 ***Pre-Screening開始***  
4423 ***Pre-Screening結束***  
4424 可能的攻擊方式: Label Specific Backdoor Attack  
4425 可能的 target-victim 配對: ['1-18', '2-16', '18-1']  
4426 可能的 target-victim 配對: ['1-18', '2-16', '18-1']  
4427 ***Trigger Reverse Engineering開始***  
4428 Target: 18, victim: 1, Loss: 8.7006, Acc: 0.00%, CE_Loss: 8.70, Reg_Loss: 2539.63, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2529.47: 4% █ | 42/1000 [00:13<05:11, 3.08it/s]  
4429 ***Trigger Reverse Engineering結束***  
4430 Target Class: 1 Victim Class: 18 Trigger Size: 1000000000.0 Optimization Steps: 21  
4431 *****檢測結束*****  
4432 檢測結果: Model是安全的(Benign)  
4433 整體耗時: 20.849449596133423 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000419-----  
4434 ***Pre-Screening開始***  
4435 ***Pre-Screening結束***  
4436 ***Pre-Screening開始***  
4437 ***檢測結束***  
4438 檢測結果: Model是安全的(Benign)  
4439 整體耗時: 10.909383773803711 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000420-----  
4440 ***Pre-Screening開始***  
4441 ***Pre-Screening結束***  
4442 可能的攻擊方式: Universal Backdoor Attack  
4443 可能的 target class: 1  
4444 可能的 victim classes: ALL  
4445 可能的 victim classes: ALL  
4446 ***Trigger Reverse Engineering開始***  
4447 Target: 1, victim: 12, Loss: 0.4286, Acc: 96.88%, CE_Loss: 0.13, Reg_Loss: 5022.23, Cost:0.00 best_reg:4718.50 avg_loss_reg:5132.37: 9% █ | 89/1000 [12:42<2:10:04, 8.57s/it]  
4448 early stop 所有  
4449 ***Trigger Reverse Engineering結束***  
4450 Target Class: 1 Victim Class: all Trigger Size: 4718.504296875 Optimization Steps: 90  
4451 *****檢測結束*****  
4452 檢測結果: Model是安全的(Benign)  
4453 整體耗時: 772.5430574417114 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000421-----  
4454 ***Pre-Screening開始***  
4455 ***Pre-Screening結束***  
4456 ***Pre-Screening結束***  
4457 ***檢測結束***  
4458 檢測結果: Model是安全的(Benign)  
4459 整體耗時: 6.237573146820068 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000422-----  
4460 ***Pre-Screening開始***  
4461 ***Pre-Screening結束***  
4462 ***Pre-Screening結束***  
4463 可能的攻擊方式: Label Specific Backdoor Attack  
4464 可能的 target-victim 配對: ['0-1', '1-0', '3-0', '3-8', '5-21', '10-1', '10-14', '17-8', '20-0', '22-0', '23-0', '23-1']  
4465 ***Trigger Reverse Engineering開始***  
4466 Target: 0, victim: 1, Loss: 1.0628, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss: 255.68 avg_loss_reg:256.08: 41% █ | 408/1000 [00:34<00:50, 11.70it/s]  
4467 early stop 所有  
4468 ***Trigger Reverse Engineering結束***  
4469 Target Class: 0 Victim Class: 1 Trigger Size: 255.48068237304688 Optimization Steps: 196  
4470 ***Symmetric Check開始***  
4471 Target: 1, victim: 0 Loss: 1.7400, Acc: 90.00%, CE_Loss: 0.33, Reg_Loss: 278.34, Cost:0.01 best_reg:284.07 avg_loss_reg:279.10: 100% █ | 196/196 [00:16<00:00, 11.88it/s]  
4472 ***Symmetric Check結束***  
4473 *****檢測結束*****
```

```

File - main
4474 檢測結果: Model是安全的(Benign)
4475 整體耗時: 57.083882093429565 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4476 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4477 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4478 可能的攻擊方式: Universal Backdoor Attack
4479 可能的 target class: 3
4480 可能的 victim classes: ALL
4481 可能的 victim classes: ALL
4482 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4483 Target: 3, victim: 16, Loss: 0.9905, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:57.97, Cost:0.02 best_reg:58.31 avg_loss_reg:58.15: 10%■ | 100/1000 [31:29 <4:43:29, 18.90s/it]
4484 early stop 所有
4485 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4486 Target Class: 3 Victim Class: all Trigger Size: 58.17532857259115 Optimization Steps: 101
4487 *****檢測結果: Model含有後門(Abnormal)-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4488 檢測結果: Model含有後門(Abnormal)
4489 耗時: 1905.0320341587067 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4490 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4491 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4492 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4493 可能的攻擊方式: Universal Backdoor Attack
4494 可能的 target class: 9
4495 可能的 victim classes: ALL
4496 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4497 Target: 9, victim: 9, Loss: 0.1102, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:246.55, Cost:0.00 best_reg:254.01 avg_loss_reg:244.57: 5%■ | 153/1000 [05:41 < 1:41:40, 6.44s/it]
4498 early stop 所有
4499 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4500 Target Class: 9 Victim Class: all Trigger Size: 254.0085950578962 Optimization Steps: 54
4501 *****檢測結果: Model含有後門(Abnormal)-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4502 檢測結果: Model含有後門(Abnormal)
4503 耗時: 353.878351688385 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4504 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4505 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4506 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4507 *****檢測結果: Model是安全的(Benign)-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4508 檢測結果: Model是安全的(Benign)
4509 耗時: 17.767489671707153 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4510 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4511 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4512 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4513 可能的攻擊方式: Label Specific Backdoor Attack
4514 可能的 target-victim 配對: ['1-7', '7-1']
4515 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4516 Target: 7, victim: 1, Loss: 9.5066, Acc: 0.00%, CE_Loss: 9.51, Reg_Loss:2551.13, Cost:0.00 best_reg:100000000000.00 avg_loss_reg:2558.44: 3%■ | 31/1000 [00:02 < 01:11, 13.64it/s]
4517 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4518 Target Class: 1 Victim Class: 7 Trigger Size: 10000000000.00 Optimization Steps: 21
4519 *****檢測結果: Model是安全的(Benign)-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4520 檢測結果: Model是安全的(Benign)
4521 耗時: 6.997875928878784 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4522 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4523 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4524 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4525 *****檢測結果: Model是安全的(Benign)-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4526 檢測結果: Model是安全的(Benign)
4527 耗時: 9.52353811264038 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4528 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4529 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4530 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4531 *****檢測結果: Model是安全的(Benign)-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4532 檢測結果: Model是安全的(Benign)
4533 耗時: 5.410531759262085 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4534 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4535 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4536 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4537 可能的攻擊方式: Label Specific Backdoor Attack
4538 可能的 target-victim 配對: ['0-1', '1-2', '2-1', '5-7']
4539 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4540 Target: 2, victim: 1, Loss: 2.8085, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:20.10, Cost:0.13 best_reg:20.13 avg_loss_reg:20.49: 15%■ | 149/1000 [07:27 < 42:34, 3.00s/it]
4541 early stop 所有
4542 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423
4543 Target Class: 2 Victim Class: 1 Trigger Size: 20.09794044494629 Optimization Steps: 96
4544 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000423

```

```

4545 Target: 1, victim: 2, Loss: 0.1070, Acc: 95.00%, CE_Loss: 0.11, Reg_Loss:11699.47, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:11596.09: 100% █ 96/96 [04:46<00:00, 2.99s/it]
4546 ***Symmetric Check結束*** 
4547 *****檢測結果: Model含有後門(Abnormal)
4548 檢測結果: Model含有後門(Abnormal)
4549 整體耗時: 752.6907222270966
4550 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000430-----
4551 ***Pre-Screening開始*** 
4552 ***Pre-Screening結束*** 
4553 ***檢測結束*** 
4554 檢測結果: Model是安全的(Benign)
4555 整體耗時: 15.926489114761353
4556 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000431-----
4557 ***Pre-Screening開始*** 
4558 ***Pre-Screening結束*** 
4559 ***檢測結束*** 
4560 檢測結果: Model是安全的(Benign)
4561 整體耗時: 5.127343416213989
4562 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000432-----
4563 ***Pre-Screening開始*** 
4564 ***Pre-Screening結束*** 
4565 可能的攻擊方式: Universal Backdoor Attack
4566 可能的 target class: 0
4567 可能的 victim classes: ALL
4568 ***Trigger Reverse Engineering開始*** 
4569 Target: 0, victim: 12, Loss: 2.3083, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:5166.56, Cost:0.00 best_reg:5139.15 avg_loss_reg:5144.94: 10% █ | 96/1000 [27:08<4:15:33, 16.96s/it]
4570 early stop 所有
4571 ***Trigger Reverse Engineering結束*** 
4572 Target Class: all Victim Class: all Trigger Size: 5139.151953125 Optimization Steps: 97
4573 *****檢測結果: Model是安全的(Benign)
4574 檢測結果: Model是安全的(Benign)
4575 整體耗時: 1640.0265655517578
4576 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000433-----
4577 ***Pre-Screening開始*** 
4578 ***Pre-Screening結束*** 
4579 可能的攻擊方式: Label Specific Backdoor Attack
4580 可能的 target-victim 配對: ['6-7', '12-2', '12-6', '12-7']
4581 ***Trigger Reverse Engineering開始*** 
4582 Target: 12, victim: 7, Loss: 0.9666, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:11.17, Cost:0.09 best_reg:11.92 avg_loss_reg:11.92: 10% █ | 104/1000 [00:07<01:02, 14.45it/s]
4583 early stop 所有
4584 ***Trigger Reverse Engineering結束*** 
4585 Target Class: 12 Victim Class: 7 Trigger Size: 11.17060661315918 Optimization Steps: 72
4586 ***Symmetric Check開始*** 
4587 Target: 7, victim: 12, Loss: 2.5084, Acc: 100.00%, CE_Loss: 0.40, Reg_Loss:4742.68, Cost:0.00 best_reg:7876.27 avg_loss_reg:4828.02: 100% █ | 72/72 [00:04<00:00, 15.11it/s]
4588 ***Symmetric Check結束*** 
4589 檢測結果: Model含有後門(Abnormal)
4590 整體耗時: 16.65692923453186
4591 ***Pre-Screening開始*** 
4592 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000434-----
4593 ***Pre-Screening結束*** 
4594 ***Pre-Screening開始*** 
4595 可能的攻擊方式: Label Specific Backdoor Attack
4596 可能的 target-victim 配對: ['2-1']
4597 ***Trigger Reverse Engineering開始*** 
4598 Target: 2, victim: 1, Loss: 6.9982, Acc: 10.00%, CE_Loss: 7.00, Reg_Loss:4033.58, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:3634.46: 2% | | 20/1000 [01:23<1:08:26, 4.19s/it]
4599 ***Trigger Reverse Engineering結束*** 
4600 Target Class: 2 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 21
4601 *****檢測結果: Model是安全的(Benign)
4602 檢測結果: Model是安全的(Benign)
4603 整體耗時: 92.40736222267151
4604 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000435-----
4605 ***Pre-Screening開始*** 
4606 ***Pre-Screening結束*** 
4607 ***檢測結束*** 
4608 檢測結果: Model是安全的(Benign)
4609 整體耗時: 4.887247800827026
4610 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000436-----
4611 ***Pre-Screening開始*** 
4612 ***Pre-Screening結束*** 
4613 可能的攻擊方式: Label Specific Backdoor Attack
4614 可能的 target-victim 配對: ['1-6', '1-7', '1-8', '3-5', '6-5', '8-7', '10-0']
4615 ***Trigger Reverse Engineering開始*** 

```

```

4616 Target: 1, victim: 6, Loss: 2.0491, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:252.65, Cost:0.01 best_reg:253.94 avg_loss_reg:249.45: 24%|████| | 240/1000 [00:29<01:32, 8.23it/s]
4617 early stop 所有
4618 ***Trigger Reverse Engineering結束***
4619 Target Class: 1 Victim Class: 6 Trigger Size: 252.6473388671875 Optimization Steps: 120
4620 ***Symmetric Check開始***
4621 Target: 6, victim: 1, Loss: 2.2023, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:1898.09, Cost:0.00 best_reg:1950.49 avg_loss_reg:1950.49: 100%|████| | 120/120 [00:14<00:00, 8.33it/s]
4622 ***Symmetric Check結束***
4623 整體耗時: 48.54423785209656
4624 檢測結果: Model是安全的(Benign)
4625 整體耗時: 48.54423785209656
4626 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000437-----
4627 ***Pre-Screening開始***
4628 ***Pre-Screening結束***
4629 ***檢測結果: Model是安全的(Benign)
4630 整體耗時: 5.665287733078003
4631 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000438-----
4632 ***Pre-Screening開始***
4633 ***Pre-Screening結束***
4634 可能的攻擊方式: Label Specific Backdoor Attack
4635 可能的 target-victim 配對: ['1-18', '18-1']
4636 可能的 target-victim 配對: Label Specific Backdoor Attack
4637 ***Trigger Reverse Engineering開始***
4638 Target: 18, victim: 1, Loss: 4.1972, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:775.25, Cost:0.01 best_reg:784.13 avg_loss_reg:786.13: 28%|████| | 280/1000 [02:54<07:27, 1.61it/s]
4639 early stop 所有
4640 ***Trigger Reverse Engineering結束***
4641 Target Class: 18 Victim Class: 1 Trigger Size: 775.2532958984375 Optimization Steps: 202
4642 ***Symmetric Check開始***
4643 Target: 1, victim: 18, Loss: 0.5824, Acc: 95.00%, CE_Loss: 0.14, Reg_Loss:669.40, Cost:0.00 best_reg:676.06 avg_loss_reg:668.62: 100%|████| | 202/202 [02:05<00:00, 1.61it/s]
4644 ***Symmetric Check結束***
4645 *****檢測結果: Model是安全的(Benign)
4646 檢測結果: Model是安全的(Benign)
4647 整體耗時: 306.310610774994
4648 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000439-----
4649 ***Pre-Screening開始***
4650 ***Pre-Screening結束***
4651 可能的攻擊方式: Label Specific Backdoor Attack
4652 可能的 target-victim 配對: ['13-1']
4653 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000440-----
4654 Target: 13, victim: 1, Loss: 5.6023, Acc: 0.00%, CE_Loss: 5.60, Reg_Loss:253.624, Cost:0.00 best_reg:100000000000.00 avg_loss_reg:2527.87: 1%|████| | 10/1000 [00:01<02:46, 5.94it/s]
4655 ***Trigger Reverse Engineering結束***
4656 Target Class: 13 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 11
4657 *****檢測結果: Model是安全的(Benign)
4658 檢測結果: Model是安全的(Benign)
4659 整體耗時: 6.431513071060181
4660 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000441-----
4661 ***Pre-Screening開始***
4662 ***Pre-Screening結束***
4663 可能的攻擊方式: Label Specific Backdoor Attack
4664 可能的 target-victim 配對: ['2-1', '15-18', '19-10', '20-0']
4665 ***Trigger Reverse Engineering開始***
4666 Target: 20, victim: 0, Loss: 7.6356, Acc: 5.00%, CE_Loss: 7.64, Reg_Loss:3740.49, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3413.21: 6%|████| | 63/1000 [00:20<05:01, 3.11it/s]
4667 ***Trigger Reverse Engineering結束***
4668 Target Class: 2 Victim Class: 1 Trigger Size: 10000000000.0 Optimization Steps: 21
4669 *****檢測結果: Model是安全的(Benign)
4670 檢測結果: Model是安全的(Benign)
4671 整體耗時: 26.2703724497986
4672 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000442-----
4673 ***Pre-Screening開始***
4674 ***Pre-Screening結束***
4675 ***檢測結果: Model是安全的(Benign)
4676 檢測結果: Model是安全的(Benign)
4677 整體耗時: 5.197281837463379
4678 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000443-----
4679 ***Pre-Screening開始***
4680 ***Pre-Screening結束***
4681 可能的攻擊方式: Label Specific Backdoor Attack
4682 可能的 target-victim 配對: ['1-2', '2-1', '2-3']
4683 ***Trigger Reverse Engineering開始***
4684 Target: 2, victim: 3, Loss: 1.6487, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:457.70, Cost:0.00 best_reg:459.04 avg_loss_reg:463.26: 41%|████| | 410/1000 [21:54<31:31, 3.21s/t]
4685 early stop 所有
4686 ***Trigger Reverse Engineering結束***

```

```
file - main
4687 Target Class: 2 Victim Class: 3 Trigger Size: 457.69580078125 Optimization Steps: 337
4688 ***Symmetric Check開始***
4689 Target: 3; victim: 2; Loss: 1.4711, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss: 6887.11, Cost:0.00 best_reg:6785.85 avg_loss_reg:6881.59: 100%|██████████| 337/337 [18:38<0:00, 3.32s/it]
4690 ***Symmetric Check結束*** 
4691 檢測結果: Model含有後門(Abnormal)
4692 整體耗時: 2443.038028717041
4693 -----掃描檔案:D:\UUUI\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000443-----
4694 -----Pre-Screening開始*** 
4695 ***Pre-Screening結束*** 
4696 可能的攻擊方式: Label Specific Backdoor Attack
4697 可能的 target-victim 配對: ['2-0', '9-8']
4698 可能的 target-victim 配對: ['2-0', '9-8']
4699 ***Trigger Reverse Engineering 開始*** 
4700 Target: 9; victim: 8; Loss: 6.6005, Acc: 0.00%, CE_Loss: 6.60, Reg_Loss:2557.31, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2543.30: 2%|████| 21/1000 [00:02<02:06, 7.74it/s]
4701 ***Trigger Reverse Engineering 結束*** 
4702 Target Class: 2 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 11
4703 檢測結果: Model是安全的(Benign)
4704 整體耗時: 7.605119943618774
4705 -----掃描檔案:D:\UUUI\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000444-----
4706 -----Pre-Screening結束*** 
4707 ***Pre-Screening開始*** 
4708 可能的攻擊方式: Label Specific Backdoor Attack
4709 可能的 target-victim 配對: ['2-10', '3-12', '7-3', '8-3', '10-14', '11-11', '14-15', '16-12', '16-6', '16-11', '17-1']
4710 可能的 target-victim 配對: ['2-10', '3-12', '7-3', '8-3', '10-14', '11-11', '14-15', '16-12', '16-6', '16-11', '17-1']
4711 ***Trigger Reverse Engineering 開始*** 
4712 Target: 16; victim: 12; Loss: 0.4516, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:182.44, Cost:0.00 best_reg:183.94 avg_loss_reg:183.94: 28%|████| 279/1000 [05:36<14:29, 1.21s/it]
4713 early stop 所有
4714 ***Trigger Reverse Engineering 結束*** 
4715 Target Class: 16 Victim Class: 12 Trigger Size: 182.4385986328125 Optimization Steps: 144
4716 ***Symmetric Check開始*** 
4717 Target: 12; victim: 16; Loss: 0.7762, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:1603.96, Cost:0.00 best_reg:1609.60 avg_loss_reg:1625.29: 100%|████| 144/144 [03:00<00:00, 1.25s/it]
4718 ***Symmetric Check結束*** 
4719 -----Pre-Screening結束*** 
4720 檢測結果: Model是安全的(Benign)
4721 整體耗時: 523.8364114761353
4722 -----掃描檔案:D:\UUUI\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000445-----
4723 -----Pre-Screening開始*** 
4724 -----Pre-Screening結束*** 
4725 可能的攻擊方式: Universal Backdoor Attack
4726 可能的 target class: 10
4727 可能的 victim classes: ALL
4728 ***Trigger Reverse Engineering 開始*** 
4729 Target: 10; victim: 19; Loss: 0.4989, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:5138.34, Cost:0.00 best_reg:33452.80 avg_loss_reg:5059.68: 3%|████| 34/1000 [10:51<5:08:40, 19.17s/it]
4730 Traceback (most recent call last):
4731 File "D:\UUUI\test_code\k_arm\test\main.py", line 158, in <module>
4732     trigger_reverse_engineering(target_classes, victim_classes, backdoor_type, model, DATA_PATH,
4733     File "D:\UUUI\test_code\k_arm\test\k_armreverse.py", line 54, in trigger_reverse_engineering
4734     pattern, mask, l1_norm, time_cost = scanner.scanning(
4735     File "D:\UUUI\test_code\k_arm\test\k_arm\scanner.py", line 123, in scanning
4736     for images, labels in data_loaders[target_index]:
4737     File "C:\Users\slab\anaconda3\envs\pytorch1\lib\site-packages\torch\utils\data\loader.py", line 435, in __next__
4738     data = self._next_data()
4739     File "C:\Users\slab\anaconda3\envs\pytorch1\lib\site-packages\torch\utils\data\loader.py", line 475, in __next_data
4740     data = self._dataset_fetcher.fetch(index) # may raise StopIteration
4741     File "C:\Users\slab\anaconda3\envs\pytorch1\lib\site-packages\torch\utils\data\util\fetch.py", line 44, in fetch
4742     data = [self._dataset[index] for index in possibly_batched_index]
4743     File "C:\Users\slab\anaconda3\envs\pytorch1\lib\site-packages\torch\utils\data\util\fetch.py", line 937, in convert
4744     data = [self._dataset[index] for index in possibly_batched_index]
4745     File "D:\UUUI\test_code\k_arm\dataset.py", line 35, in __getitem__
4746     image = Image.open(img_path).convert('RGB')
4747     File "C:\Users\slab\anaconda3\envs\pytorch1\lib\site-packages\PIL\Image.py", line 269, in load
4748     self.load()
4749     File "C:\Users\slab\anaconda3\envs\pytorch1\lib\site-packages\PIL\ImageFile.py", line 1073741510 (0xC0000013A: interrupted by Ctrl+C)
4750     n, err_code = decoder.decode(b)
4751 KeyboardInterrupt
4752 Process finished with exit code -1073741510 (0xC0000013A: interrupted by Ctrl+C)
4753
```