

```
File - main
1 C:\Users\slab\anaconda3\envs\pytorch1\python.exe D:\UUU\test_code\k_arm_test\main.py
2 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000445-----
3 ***Pre-Screening開始***
4 ***Pre-Screening結束***
5 可能的攻擊方式: Universal Backdoor Attack
6 可能的 target class: 10
7 可能的 victim classes: ALL
8 ***Trigger Reverse Engineering開始***
9 Target: 10, victim: 22, Loss: 0.6154, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:4670.46, Cost:0.00 best_reg:4642.89 avg_loss_reg:4621.30: 23%| 234/1000 [-----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000446-----
10 early stop 所有
11 ***Trigger Reverse Engineering結束***
12 Target Class: 10 Victim Class: all Trigger Size: 4642.88837890625 Optimization Steps: 235
13 *****檢測結束***** 
14 檢測結果: Model是安全的(Benign)
15 整體耗時: 508.9595293998718
16 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000446-----
17 ***Pre-Screening開始***
18 ***Pre-Screening結束***
19 可能的攻擊方式: Universal Backdoor Attack
20 可能的 target class: 2
21 可能的 victim classes: ALL
22 ***Trigger Reverse Engineering開始***
23 Target: 2, victim: 16, Loss: 0.2676, Acc: 95.00%, CE_Loss: 0.06, Reg_Loss:91.43, Cost:0.00 best_reg:101.24 avg_loss_reg:91.47: 9%| | 87/1000 [35:04<6:00
24 early stop 所有
25 ***Trigger Reverse Engineering結束***
26 Target Class: 2 Victim Class: all Trigger Size: 101.24027252197266 Optimization Steps: 88
27 *****檢測結束***** 
28 檢測結果: Model含有後門(Abnormal)
29 整體耗時: 2115.3653445243835
30 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000447-----
31 ***Pre-Screening開始***
32 ***Pre-Screening結束***
33 可能的攻擊方式: Label Specific Backdoor Attack
34 可能的 target-victim 配對: ['2-1', '3-14', '8-1', '14-3', '14-12', '20-1', '22-1']
35 ***Trigger Reverse Engineering開始***
36 Target: 22, victim: 1, Loss: 7.8331, Acc: 0.00%, CE_Loss: 7.83, Reg_Loss:2549.89, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2537.14: 11%| | 106/1000 [-----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000448-----
37 ***Trigger Reverse Engineering結束***
38 Target Class: 2 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 21
39 *****檢測結束***** 
40 檢測結果: Model是安全的(Benign)
41 整體耗時: 40.285250663757324
42 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000448-----
43 ***Pre-Screening開始***
44 ***Pre-Screening結束***
45 ***檢測結束*** 
46 檢測結果: Model是安全的(Benign)
47 整體耗時: 13.6115047216415405
48 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000449-----
49 ***Pre-Screening開始***
50 ***Pre-Screening結束***
51 ***檢測結束*** 
52 檢測結果: Model是安全的(Benign)
53 整體耗時: 13.669980764389038
54 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000450-----
55 ***Pre-Screening開始***
56 ***Pre-Screening結束***
57 可能的攻擊方式: Universal Backdoor Attack
58 可能的 target class: 2
59 可能的 victim classes: ALL
60 ***Trigger Reverse Engineering開始***
61 Target: 2, victim: 19, Loss: 0.4472, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:3177.85, Cost:0.00 best_reg:3211.57 avg_loss_reg:3147.21: 13%| | 131/1000 [-----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000451-----
62 early stop 所有
63 ***Trigger Reverse Engineering結束***
64 Target Class: 2 Victim Class: all Trigger Size: 3211.5723702566966 Optimization Steps: 132
65 *****檢測結束***** 
66 檢測結果: Model是安全的(Benign)
67 整體耗時: 1916.7312288284302
68 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000451-----
69 ***Pre-Screening開始***
70 ***Pre-Screening結束***
```

```
72 檢測結果: Model是安全的(Benign)
73 整體耗時: 4.949232578277588 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000452
74 ***Pre-Screening開始***
75 ***Pre-Screening結束***
76 ***Pre-Screening結束***
77 ***檢測結束***
78 檢測結果: Model是安全的(Benign)
79 整體耗時: 16.315000295639038 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000453
80
81 ***Pre-Screening開始***
82 ***Pre-Screening結束***
83 ***檢測結束***
84 檢測結果: Model是安全的(Benign)
85 整體耗時: 13.186664342880249 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000454
86
87 ***Pre-Screening開始***
88 ***Pre-Screening結束***
89 可能的攻擊方式: Label Specific Backdoor Attack
90 可能的 target-victim 配對: ['6-7', '7-6']
91 ***Trigger Reverse Engineering 開始***
92 Target: 7, victim: 6, Loss: 4.9830, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:422.76, Cost:0.01 best_reg:429.16 avg_loss_reg:423.54: 14% | 144/1000 [10:12<1:00:40, 4.25s/it]
93 early stop 所有
94 ***Trigger Reverse Engineering 結束***
95 Target Class: 7 Victim Class: 6 Trigger Size: 422.7642822265625 Optimization Steps: 134
96 ***Symmetric Check開始***
97 Target: 6, victim: 7, Loss: 0.0565, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:14010.39, Cost:0.00 best_reg:13939.20 avg_loss_reg:13939.20: 100% | 134/134 [09:22<00:00, 4.20s/it]
98 ***Symmetric Check結束***
99 ***檢測結束*****
100 檢測結果: Model含有後門(Abnormal)
101 整體耗時: 1192.202980041504
102 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000455
103 ***Pre-Screening開始***
104 ***Pre-Screening結束***
105 ***檢測結束***
106 檢測結果: Model是安全的(Benign)
107 整體耗時: 8.389086246490479
108
109 ***Pre-Screening開始***
110 ***Pre-Screening結束***
111 可能的攻擊方式: Label Specific Backdoor Attack
112 可能的 target-victim 配對: ['1-13', '9-14', '11-13', '13-11', '14-13', '16-1']
113 ***Trigger Reverse Engineering 開始***
114 Target: 13, victim: 11, Loss: 2.6395, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.63, Cost:0.06 best_reg:48.31 avg_loss_reg:48.31: 23% | 120/1000 [15:39<52:25, 4.09s/it]
115 early stop 所有
116 ***Trigger Reverse Engineering 結束***
117 Target Class: 13 Victim Class: 11 Trigger Size: 45.63339614868164 Optimization Steps: 68
118 ***Symmetric Check開始***
119 Target: 11, victim: 13, Loss: 0.3959, Acc: 80.00%, CE_Loss: 0.40, Reg_Loss:8494.80, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:8416.27: 100% | 68/68 [04:00<00:00, 3.53s/it]
120 ***Symmetric Check結束***
121 ***檢測結束*****
122 檢測結果: Model含有後門(Abnormal)
123 整體耗時: 1201.0458145141602
124
125 ***Pre-Screening開始***
126 ***Pre-Screening結束***
127 可能的攻擊方式: Label Specific Backdoor Attack
128 可能的 target-victim 配對: ['1-7', '1-21', '2-1', '3-1', '4-3', '4-9', '5-9', '11-9', '15-7', '20-1', '20-19', '21-1', '21-19']
129 ***Trigger Reverse Engineering 開始***
130 Target: 1, victim: 21, Loss: 2.4678, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:470.00, Cost:0.01 best_reg:472.34 avg_loss_reg:472.34: 32% | 319/1000 [01:25<03:03, 3.71s/it]
131 early stop 所有
132 ***Trigger Reverse Engineering 結束***
133 Target Class: 1 Victim Class: 21 Trigger Size: 470.0036315917969 Optimization Steps: 119
134 ***Symmetric Check開始***
135 Target: 21, victim: 1, Loss: 1.2242, Acc: 90.00%, CE_Loss: 0.45, Reg_Loss:1165.80, Cost:0.00 best_reg:1297.40 avg_loss_reg:1183.93: 100% | 119/119 [00:30<00:00, 3.92s/it]
136 ***Symmetric Check結束***
137 ***檢測結束*****
138 檢測結果: Model是安全的(Benign)
139 整體耗時: 123.52171015739441
140 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000458
141 ***Pre-Screening開始***
142 ***Pre-Screening結束***
```

## File - main

```

143 可能的攻擊方式: Universal Backdoor Attack
144 可能的 target class: 6
145 可能的 victim classes: ALL
146 ***Trigger Reverse Engineering開始***
147 Target: 6, victim: 19, Loss: 1.7720, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:3917.38, Cost:0.00 best_reg:3821.82 avg_loss_reg:3852.14: 8% █ | 77/1000 [03:06<37:11, 2.42s/it]
148 early stop 所有
149 ***Trigger Reverse Engineering結束***+
150 Target Class: 6 Victim Class: all Trigger Size: 3821.816336495536 Optimization Steps: 78
151 *****檢測結束*****+
152 檢測結果: Model是安全的(Benign)
153 整體耗時: 192.1087145805359
154 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000459-----
155 ***Pre-Screening開始***
156 ***Pre-Screening結束***
157 ***檢測結束***
158 檢測結果: Model是安全的(Benign)
159 整體耗時: 4.94709587097168
160 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000460-----
161 ***Pre-Screening開始***
162 ***Pre-Screening結束***
163 可能的攻擊方式: Label Specific Backdoor Attack
164 可能的 target-victim 配對: ['1-2', '2-1']
165 ***Trigger Reverse Engineering開始***
166 Target: 2, victim: 1, Loss: 8.2124, Acc: 0.00%, CE_Loss: 8.21, Reg_Loss:2557.19, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2542.86: 2% █ | 21/1000 [00:05<04:00, 4.07it/s]
167 ***Trigger Reverse Engineering結束***
168 Target Class: 1 Victim Class: 2 Trigger Size: 10000000000.0 Optimization Steps: 11
169 *****檢測結束*****+
170 檢測結果: Model是安全的(Benign)
171 整體耗時: 9.722591876983643
172 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000461-----
173 ***Pre-Screening開始***
174 ***Pre-Screening結束***
175 可能的攻擊方式: Label Specific Backdoor Attack
176 可能的 target-victim 配對: ['2-9', '8-3', '8-9', '8-13', '12-11', '12-13']
177 ***Trigger Reverse Engineering開始***
178 Target: 8, victim: 3, Loss: 2.3492, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:198.24, Cost:0.01 best_reg:207.35 avg_loss_reg:197.56: 21% █ | 210/1000 [08:29<31:56, 2.43s/it]
179 early stop 所有
180 ***Trigger Reverse Engineering結束***
181 Target Class: 8 Victim Class: 3 Trigger Size: 198.24041748046875 Optimization Steps: 95
182 ***Symmetric Check開始***
183 Target: 3, victim: 8, Loss: 0.6461, Acc: 90.00%, CE_Loss: 0.65, Reg_Loss:1914.280, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:19089.80: 100% █ | 95/95 [03:49<00:00, 2.42s/it]
184 ***Symmetric Check結束***
185 *****檢測結束*****+
186 檢測結果: Model含有後門(Abnormal)
187 整體耗時: 749.9109630584717
188 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000462-----
189 ***Pre-Screening開始***
190 ***Pre-Screening結束***
191 可能的攻擊方式: Label Specific Backdoor Attack
192 可能的 target-victim 配對: ['20-2', '20-7', '21-2']
193 ***Trigger Reverse Engineering開始***
194 Target: 20, victim: 7, Loss: 1.4165, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:48.38, Cost:0.03 best_reg:49.62 avg_loss_reg:47.49: 12% █ | 122/1000 [00:22<02:41, 5.43it/s]
195 early stop 所有
196 ***Trigger Reverse Engineering結束***
197 Target Class: 20 Victim Class: 7 Trigger Size: 48.37567901611328 Optimization Steps: 103
198 ***Symmetric Check開始***
199 Target: 7, victim: 20, Loss: 0.5173, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:3983.99, Cost:0.00 best_reg:11195.67 avg_loss_reg:3978.35: 100% █ | 103/103 [00:19<00:00, 5.36it/s]
200 ***Symmetric Check結束***
201 *****檢測結束*****+
202 檢測結果: Model含有後門(Abnormal)
203 整體耗時: 48.55360150337219
204 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000463-----
205 ***Pre-Screening開始***
206 ***Pre-Screening結束***
207 可能的攻擊方式: Universal Backdoor Attack
208 可能的 target class: 12
209 可能的 victim classes: ALL
210 ***Trigger Reverse Engineering開始***
211 Target: 12, victim: 12, Loss: 0.8067, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:806.73, Cost:0.00 best_reg:808.70 avg_loss_reg:795.52: 9% █ | 90/1000 [26:53<4:31:56, 17.93s/it]
212 early stop 所有
213 ***Trigger Reverse Engineering結束***+

```

```
214 Target Class: 12 Victim Class: all Trigger Size: 808.700341796875 Optimization Steps: 91
215 *****檢測結束*****
216 檢測結果: Model含有後門(Abnormal)
217 整體耗時: 1625.6330347061157 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000464-----
218 *****Pre-Screening開始****
219 *****Pre-Screening結束****
220 *****Pre-Screening結束****
221 ***檢測結束***
222 檢測結果: Model是安全的(Benign)
223 整體耗時: 9.479580402374268 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000465-----
224 *****Pre-Screening開始****
225 *****Pre-Screening結束****
226 *****Pre-Screening結束****
227 可能的攻擊方式: Universal Backdoor Attack
228 可能的 target class: ALL
229 可能的 victim classes: ALL
230 ***Trigger Reverse Engineering開始****
231 Target: 1, victim: 4, Loss: 1.0341, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:5157.92, Cost:0.00 best_reg:5401.73 avg_loss_reg:5101.63: 5%| | 48/1000 [07:17<2:24:46, 9.12s/it]
232 early stop 所有
233 ***Trigger Reverse Engineering結束****
234 Target Class: 1 Victim Class: all Trigger Size: 5401.7333984375 Optimization Steps: 49
235 *****檢測結束*****
236 檢測結果: Model是安全的(Benign)
237 整體耗時: 445.0679786205292 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000466-----
238 *****Pre-Screening開始****
239 *****Pre-Screening結束****
240 *****Pre-Screening結束****
241 ***檢測結束***
242 檢測結果: Model是安全的(Benign)
243 整體耗時: 4.631896257400513 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000467-----
244 *****Pre-Screening開始****
245 *****Pre-Screening結束****
246 *****Pre-Screening結束****
247 ***檢測結束***
248 檢測結果: Model是安全的(Benign)
249 整體耗時: 12.522701025009155 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000468-----
250 *****Pre-Screening開始****
251 *****Pre-Screening結束****
252 ***檢測結束***
253 ***檢測結束***
254 檢測結果: Model是安全的(Benign)
255 整體耗時: 12.749953746795654 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000469-----
256 *****Pre-Screening開始****
257 *****Pre-Screening結束****
258 *****Pre-Screening結束****
259 可能的攻擊方式: Label Specific Backdoor Attack
260 可能的 target-victim 配對: [6-11]
261 ***Trigger Reverse Engineering開始****
262 Target: 6, victim: 11, Loss: 11.1240, Acc: 0.00%, CE_Loss: 11.12, Reg_Loss:2582.18, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2562.63: 1%| | 10/1000 [00:27<44:37, 2.70s/it]
263 ***Trigger Reverse Engineering結束****
264 Target Class: 6 Victim Class: 11 Trigger Size: 1000000000.0 Optimization Steps: 11
265 *****檢測結束*****
266 檢測結果: Model是安全的(Benign)
267 整體耗時: 43.30045461654663 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000470-----
268 *****Pre-Screening開始****
269 *****Pre-Screening結束****
270 *****Pre-Screening結束****
271 ***檢測結束***
272 檢測結果: Model是安全的(Benign)
273 整體耗時: 6.345905065536499 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000471-----
274 *****Pre-Screening開始****
275 *****Pre-Screening結束****
276 *****Pre-Screening結束****
277 可能的攻擊方式: Universal Backdoor Attack
278 可能的 target class: 11
279 可能的 victim classes: ALL
280 ***Trigger Reverse Engineering開始****
281 Target: 11, victim: 16, Loss: 0.5763, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:1944.95, Cost:0.00 best_reg:1940.50 avg_loss_reg:1962.71: 8%| | 83/1000 [1:06:52<12:18:51, 48.34s/it]
282 early stop 所有
283 ***Trigger Reverse Engineering結束****
284 Target Class: 11 Victim Class: all Trigger Size: 1940.5022416548295 Optimization Steps: 84
```

File - main

```

285 *****檢測結束*****
286 檢測結果: Model是安全的(Benign)
287 整體耗時: 4027.8936009407043 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000472-----
288 ***Pre-Screening開始***
289 ***Pre-Screening結束***
290 可能的攻擊方式: Label Specific Backdoor Attack
291 可能的 target-victim 配對: ['1-10', '2-3', '3-2', '3-10', '4-14', '5-11', '5-13', '6-13', '7-9', '8-18', '9-11', '10-3', '12-5', '14-4', '16-9', '16-11', '16-13', '19-3', '19-10', '20-1', '20-2']
292 ***Trigger Reverse Engineering開始***
293 Target: 2, victim: 3, Loss: 4.2976, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:796.70, Cost:0.01 best_reg:797.06 avg_loss_reg:797.34: 60% | 602/1000 [19:07<12:38, 1.91s/it]
294 Target: 3, victim: 2, Loss: 3.5176, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:968.04, Cost:0.00 best_reg:981.31 avg_loss_reg:981.31: 73% | 142/195 [03:36<01:20, 1.52s/it]
295 early stop 所有
296 ***Trigger Reverse Engineering結束***
297 Target Class: 2 Victim Class: 3 Trigger Size:796.70166015625 Optimization Steps: 195
298 ***Symmetric Check開始***
299 Target: 3, victim: 2, Loss: 3.5176, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:968.04, Cost:0.00 best_reg:981.31 avg_loss_reg:981.31: 73% | 142/195 [03:36<01:20, 1.52s/it]
300 early stop 所有
301 ***Symmetric Check結束***
302 ***Pre-Screening結束***
303 檢測結果: Model是安全的(Benign)
304 整體耗時: 1379.2330272197723 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000473-----
305 ***Pre-Screening結束***
306 ***Pre-Screening開始***
307 ***Pre-Screening結束***
308 ***檢測結束***
309 檢測結果: Model是安全的(Benign)
310 整體耗時: 6.054565191268921 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000474-----
311 ***Pre-Screening開始***
312 ***Pre-Screening結束***
313 ***Pre-Screening結束***
314 可能的攻擊方式: Label Specific Backdoor Attack
315 可能的 target-victim 配對: ['4-18', '5-18', '8-9', '22-21']
316 ***Trigger Reverse Engineering開始***
317 Target: 22, victim: 21, Loss: 7.7380, Acc: 0.00%, CE_Loss: 7.74, Reg_Loss:2525.05, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2516.91: 5% | 53/1000 [01:30<26:57, 1.71s/it]
318 ***Trigger Reverse Engineering結束***
319 Target Class: 4 Victim Class: 18 Trigger Size: 10000000000.0 Optimization Steps: 21
320 ***檢測結束***
321 檢測結果: Model是安全的(Benign)
322 整體耗時: 107.49298167228699 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000475-----
323 ***Pre-Screening開始***
324 ***Pre-Screening結束***
325 可能的攻擊方式: Label Specific Backdoor Attack
326 可能的 target-victim 配對: ['16-0']
327 可能的 target-victim 配對: ['16-0']
328 ***Trigger Reverse Engineering開始***
329 Target: 16, victim: 0, Loss: 4.3915, Acc: 20.00%, CE_Loss: 4.39, Reg_Loss:2943.35, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2877.14: 2% | 20/1000 [01:13<1:00:04, 3.68s/it]
330 ***Trigger Reverse Engineering結束***
331 Target Class: 16 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 21
332 ***檢測結束***
333 檢測結果: Model是安全的(Benign)
334 整體耗時: 100.53090262413025 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000476-----
335 ***Pre-Screening開始***
336 ***Pre-Screening結束***
337 ***Pre-Screening結束***
338 可能的攻擊方式: Label Specific Backdoor Attack
339 可能的 target-victim 配對: ['0-13', '1-0', '1-2', '1-22', '2-1', '2-3', '2-6', '3-1', '3-16', '4-2', '4-5', '5-6', '5-11', '6-5', '6-13', '7-22', '7-5', '7-21', '8-13', '8-9', '8-18', '9-16', '10-3', '10-16', '11-5', '11-13', '11-18', '12-7', '12-20', '13-0', '13-19', '14-19', '14-18', '12-18', '12-21', '17-22', '18-11', '18-20', '19-13', '19-15', '19-20', '20-1', '20-21', '21-7', '21-20', '21-22', '22-1']
340 ***Trigger Reverse Engineering開始***
341 Target: 1, victim: 22, Loss: 2.2814, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:1329.19, Cost:0.00 best_reg:1343.86 avg_loss_reg:1343.86: 91% | 911/1000 [39:39<03:52, 2.61s/it]
342 early stop 所有
343 ***Trigger Reverse Engineering結束***
344 Target Class: 1 Victim Class: 22 Trigger Size: 1329.1861572265625 Optimization Steps: 203
345 ***檢測結束***
346 檢測結果: Model是安全的(Benign)
347 整體耗時: 2393.9243268966675 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000477-----
348 ***Pre-Screening開始***
349 ***Pre-Screening結束***
350 ***檢測結束***
351 檢測結果: Model是安全的(Benign)
352 整體耗時: 32.64503526687622 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000478-----
353
354

```

```
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: 6.31959342956543  
360 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000479-----  
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: 7.60225772857666  
366 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000480-----  
367 ***Pre-Screening開始***  
368 ***Pre-Screening結束***  
369 ***檢測結束***  
370 檢測結果: Model是安全的(Benign)  
371 整體耗時: 5.6397130489349365  
372 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000481-----  
373 ***Pre-Screening開始***  
374 ***Pre-Screening結束***  
375 可能的攻擊方式: Label Specific Backdoor Attack  
376 可能的 target-victim 配對: ['1-9', '5-16', '11-0', '13-5', '15-16']  
377 ***Trigger Reverse Engineering 開始***  
378 Target: 1, victim: 9, Loss: 1.6601, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:1024.46, Cost:0.00 best_reg:1029.03 avg_loss_reg:1029.03: 23% [■] | 233/1000 [18:54<1:02:13, 4.87s/it]  
379 early stop 所有  
380 ***Trigger Reverse Engineering 結束***  
381 Target Class: 1 Victim Class: 9 Trigger Size: 1024.4587/40234375 Optimization Steps: 190  
382 *****檢測結束*****  
383 檢測結果: Model是安全的(Benign)  
384 整體耗時: 1158.3292882442474  
385 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000482-----  
386 ***Pre-Screening開始***  
387 ***Pre-Screening結束***  
388 ***檢測結束***  
389 檢測結果: Model是安全的(Benign)  
390 整體耗時: 18.340771436691284  
391 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000483-----  
392 ***Pre-Screening開始***  
393 ***Pre-Screening結束***  
394 可能的攻擊方式: Universal Backdoor Attack  
395 可能的 target class: 18  
396 可能的 victim classes: ALL  
397 ***Trigger Reverse Engineering 開始***  
398 Target: 18, victim: 19, Loss: 0.2427, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:363.81, Cost:0.00 best_reg:357.10 avg_loss_reg:361.13: 10% [■] | 99/1000 [38:49<5:53:17, 23.53s/it]  
399 early stop 所有  
400 ***Trigger Reverse Engineering 結束***  
401 Target Class: 18 Victim Class: all Trigger Size: 357.10140119280135 Optimization Steps: 100  
402 *****檢測結束*****  
403 檢測結果: Model含有後門(Abnormal)  
404 整體耗時: 2341.3998906612396  
405 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000484-----  
406 ***Pre-Screening開始***  
407 ***Pre-Screening結束***  
408 可能的攻擊方式: Label Specific Backdoor Attack  
409 可能的 target-victim 配對: ['3-6']  
410 ***Trigger Reverse Engineering 開始***  
411 Target: 3, victim: 6, Loss: 2.6270, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:19.56, Cost:0.13 best_reg:20.36 avg_loss_reg:20.36: 6% [■] | 65/1000 [00:07<01:52, 8.28it/s]  
412 early stop 所有  
413 ***Trigger Reverse Engineering 結束***  
414 Target Class: 3 Victim Class: 6 Trigger Size: 19.558185577392578 Optimization Steps: 66  
415 ***Symmetric Check開始***  
416 Target: 6, victim: 3, Loss: 3.9893, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:2520.09, Cost:0.00 best_reg:2581.22 avg_loss_reg:2581.22: 100% [■] | 66/66 [00:07<00:00, 8.54it/s]  
417 ***Symmetric Check結束***  
418 *****檢測結束*****  
419 檢測結果: Model含有後門(Abnormal)  
420 整體耗時: 17.868822813034058  
421 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000485-----  
422 ***Pre-Screening開始***  
423 ***Pre-Screening結束***  
424 可能的攻擊方式: Label Specific Backdoor Attack  
425 可能的 target-victim 配對: ['1-11']
```

```

426 ***Trigger Reverse Engineering開始***  

427 Target: 10, victim: 11, Loss: 9.1305, Acc: 0.00%, CE_Loss: 9.13, Reg_Loss:2543.78, Cost:0.00 best_Reg:1000000000.00 avg_loss_Reg:2532.51: 1%| | 10/1000 [00:03<06:22, 2.59it/s]  

428 ***Trigger Reverse Engineering結束***  

429 Target Class: 10 Victim Class: 11 Trigger Size: 1000000000.0 Optimization Steps: 11  

430 *****檢測結束*****  

431 檢測結果: Model是安全的(Benign)  

432 整體耗時: 9.986019611358643  

433 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000486-----  

434 ***Pre-Screening開始***  

435 ***Pre-Screening結束***  

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

437 可能的 target-victim 配對: [4-3]  

438 ***Trigger Reverse Engineering開始***  

439 Target: 4, victim: 3, Loss: 11.2577, Acc: 0.00%, CE_Loss: 11.26, Reg_Loss:2591.12, Cost:0.00 best_Reg:1000000000.00 avg_loss_Reg:2570.44: 1%| | 10/1000 [00:01<03:01, 5.47it/s]  

440 ***Trigger Reverse Engineering結束***  

441 Target Class: 4 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 11  

442 *****檢測結束*****  

443 檢測結果: Model是安全的(Benign)  

444 整體耗時: 4.39846396446228  

445 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000487-----  

446 ***Pre-Screening開始***  

447 ***Pre-Screening結束***  

448 ***檢測結束***  

449 檢測結果: Model是安全的(Benign)  

450 整體耗時: 16.589495182037354  

451 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000488-----  

452 ***Pre-Screening開始***  

453 ***Pre-Screening結束***  

454 ***檢測結束***  

455 檢測結果: Model是安全的(Benign)  

456 整體耗時: 13.58474135988647  

457 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000489-----  

458 ***Pre-Screening開始***  

459 ***Pre-Screening結束***  

460 檢測結果: Model是安全的(Benign)  

461 檢測結果: Model是安全的(Benign)  

462 整體耗時: 11.06437373161316  

463 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000490-----  

464 ***Pre-Screening開始***  

465 ***Pre-Screening結束***  

466 ***檢測結束***  

467 檢測結果: Model是安全的(Benign)  

468 整體耗時: 8.690270183470581  

469 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000491-----  

470 ***Pre-Screening開始***  

471 ***Pre-Screening結束***  

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

473 可能的 target-victim 配對: [4-10, '5-12', '5-14', '9-14', '11-14', '13-3', '13-12', '14-8', '14-9', '17-0']  

474 ***Trigger Reverse Engineering開始***  

475 Target: 14, victim: 8, Loss: 2.3006, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:2136.66, Cost:0.00 best_Reg:2160.59 avg_loss_Reg:2187.44: 36%| | 362/1000 [17:45<31:17, 2.94s/it]  

476 early stop 所有  

477 ***Trigger Reverse Engineering結束***  

478 Target Class: 14 Victim Class: 8 Trigger Size: 2136.660888671875 Optimization Steps: 243  

479 *****檢測結束*****  

480 檢測結果: Model是安全的(Benign)  

481 整體耗時: 1086.8663012981415  

482 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000492-----  

483 ***Pre-Screening開始***  

484 ***Pre-Screening結束***  

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

486 可能的 target-victim 配對: ['1-19', '2-11', '13-0', '13-4', '14-4', '16-9', '19-1', '20-1', '20-22', '22-0']  

487 ***Trigger Reverse Engineering開始***  

488 Target: 13, victim: 4, Loss: 1.2602, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:157.08, Cost:0.01 best_Reg:157.26 avg_loss_Reg:157.16: 31%| | 308/1000 [02:19<05:13, 2.20it/s]  

489 early stop 所有  

490 ***Trigger Reverse Engineering結束***  

491 Target Class: 13 Victim Class: 4 Trigger Size: 157.07608032226562 Optimization Steps: 179  

492 ***Symmetric Check開始***  

493 Target: 4, victim: 13, Loss: 2.6631, Acc: 95.00%, CE_Loss: 0.37, Reg_Loss:2289.50, Cost:0.00 best_Reg:2335.35 avg_loss_Reg:2304.50: 100%| | 179/179 [01:21<00:00, 2.20it/s]  

494 ***Symmetric Check結束***  

495 *****檢測結束*****  

496 檢測結果: Model含有後門(Abnormal)

```

整體耗時: 228.1006999015808

\*\*\*Pre-Screening開始\*\*\*

\*\*\*Pre-Screening結束\*\*\*

500 檢測結果: Model是安全的(Benign)

501 整體耗時: 6.041424751281738

504 \*\*\*Pre-Screening開始\*\*\*

505 \*\*\*Pre-Screening結束\*\*\*

506 \*\*\*檢測結果: Model是安全的(Benign)

507 整體耗時: 32.34579849243164

508 檢測結果: Model是安全的(Benign)

509 整體耗時: 132.34579849243164

510 \*\*\*Pre-Screening開始\*\*\*

511 \*\*\*Pre-Screening結束\*\*\*

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

513 可能的 target-victim 配對: ['0-17', '7-8', '13-18', '18-19']

514 可能的 target-victim 配對: ['0-17', '7-8', '13-18', '18-19']

515 \*\*\*Trigger Reverse Engineering開始\*\*\*

516 Target: 0, victim: 17, Loss: 2.6233, Acc: 100.00%, CE\_Loss: 0.07, Reg\_Loss:44.27, Cost:0.06 best\_reg:45.01 avg\_loss\_reg:45.01: 13% [■]

517 early\_stop 所有

518 \*\*\*Trigger Reverse Engineering結束\*\*\*

519 Target Class: 0 Victim Class: 17 Trigger Size: 44.26556396484375 Optimization Steps: 91

520 \*\*\*Symmetric Check開始\*\*\*

521 Target: 17, victim: 0, Loss: 2.0320, Acc: 5.00%, CE\_Loss: 2.03, Reg\_Loss:14961.56, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:14797.46: 100% [■]

522 \*\*\*Symmetric Check結束\*\*\*

523 \*\*\*檢測結果: Model含有後門(Abnormal)

524 檢測結果: Model含有後門(Abnormal)

525 整體耗時: 480.39882802963257

526 \*\*\*Pre-Screening開始\*\*\*

527 \*\*\*Pre-Screening結束\*\*\*

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

529 可能的 target-victim 配對: ['3-4', '4-2']

530 可能的 target-victim 配對: ['3-4', '4-2']

531 \*\*\*Trigger Reverse Engineering開始\*\*\*

532 Target: 4, victim: 2, Loss: 7.6594, Acc: 0.00%, CE\_Loss: 7.66, Reg\_Loss:2536.81, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:2528.22: 2% [■]

533 \*\*\*Trigger Reverse Engineering結束\*\*\*

534 Target Class: 3 Victim Class: 4 Trigger Size: 1000000000.0 Optimization Steps: 11

535 \*\*\*檢測結果: Model是安全的(Benign)

536 檢測結果: Model是安全的(Benign)

537 整體耗時: 7.097445964813232

538 \*\*\*Pre-Screening開始\*\*\*

539 \*\*\*Pre-Screening結束\*\*\*

540 可能的攻擊方式: Universal Backdoor Attack

541 可能的 victim classes: ALL

542 可能的 target class: 10

543 可能的 victim classes: ALL

544 \*\*\*Trigger Reverse Engineering開始\*\*\*

545 Target: 10, victim: 9, Loss: 0.2679, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss:79.35, Cost:0.00 best\_reg:85.46 avg\_loss\_reg:78.87: 5% [■]

546 early\_stop 所有

547 \*\*\*Trigger Reverse Engineering結束\*\*\*

548 Target Class: 10 Victim Class: all Trigger Size: 85.46172768729073 Optimization Steps: 50

549 \*\*\*檢測結果: Model含有後門(Abnormal)

550 檢測結果: Model含有後門(Abnormal)

551 整體耗時: 345.83332085609436

552 \*\*\*Pre-Screening開始\*\*\*

553 \*\*\*Pre-Screening結束\*\*\*

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

555 可能的 target-victim 配對: ['0-17', '7-8', '13-18', '18-19']

556 檢測結果: Model是安全的(Benign)

557 整體耗時: 17.476946115493774

558 \*\*\*Pre-Screening開始\*\*\*

559 \*\*\*Pre-Screening結束\*\*\*

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

561 可能的 target-victim 配對: ['0-17', '7-8', '13-18', '18-19']

562 檢測結果: Model是安全的(Benign)

563 整體耗時: 9.31407737319336

564 \*\*\*Pre-Screening開始\*\*\*

565 \*\*\*Pre-Screening結束\*\*\*

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

567 檢測結果: Model是安全的(Benign)

```

568 檢測結果: Model是安全的(Benign)
569 整體耗時: 6.391058921813965                                         | 握描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000501
570                                         | 119/1000 [2:51:48<21:12:01, 86.63s/it]
571 ***Pre-Screening開始***                                           |
572 ***Pre-Screening結束***                                           |
573 可能的攻擊方式: Universal Backdoor Attack
574 可能的 target class: 18
575 可能的 victim classes: ALL
576 ***Trigger Reverse Engineering開始***                           |
577 Target: 18, victim: 20, Loss: 0.2463, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:554.00, Cost:0.00 best_reg:557.91 avg_loss_reg:551.87: 12%| █ | 119/1000 [2:51:48<21:12:01, 86.63s/it]
578 early stop 所有
579 ***Trigger Reverse Engineering結束***                           |
580 Target Class: 18 Victim Class: all Trigger Size: 557.9116908482143 Optimization Steps: 120
581 *****檢測結束*****                                           |
582 檢測結果: Model含有後門(Abnormal)
583 整體耗時: 10335.603230714798                                         | 握描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000502
584 *****Pre-Screening開始***                                         |
585 *****Pre-Screening結束***                                         |
586 *****Pre-Screening結束***                                         |
587 可能的攻擊方式: Label Specific Backdoor Attack
588 可能的 target-victim 配對: ['3-4', '4-3', '5-0']
589 ***Trigger Reverse Engineering開始***                           |
590 Target: 5, victim: 0, Loss: 0.9095, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:528.48, Cost:0.00 best_reg:533.69 avg_loss_reg:526.46: 38%| █ | 384/1000 [00:56<01:30, 6.82it/s]
591 early stop 所有
592 ***Trigger Reverse Engineering結束***                           |
593 Target Class: 5 Victim Class: 0 Trigger Size: 528.4754028320312 Optimization Steps: 353
594 ***Symmetric Check開始***                                         |
595 Target: 0, victim: 5, Loss: 1.1086, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:2260.90, Cost:0.00 best_reg:2263.79 avg_loss_reg:2260.75: 57%| █ | 200/353 [00:29<00:22, 6.82it/s]
596 early stop 所有
597 ***Symmetric Check結束***                                         |
598 *****檢測結束*****                                           |
599 檢測結果: Model是安全的(Benign)
600 整體耗時: 94.84227633476257                                         | 握描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000503
601 *****Pre-Screening結束*****                                         |
602 *****Pre-Screening開始***                                         |
603 *****Pre-Screening結束***                                         |
604 *****檢測結束***                                           |
605 檢測結果: Model是安全的(Benign)
606 整體耗時: 11.296743392944336                                         | 握描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000504
607 *****Pre-Screening結束*****                                         |
608 *****Pre-Screening開始***                                         |
609 *****Pre-Screening結束***                                         |
610 可能的攻擊方式: Label Specific Backdoor Attack
611 可能的 target-victim 配對: ['3-4', '20-4']
612 ***Trigger Reverse Engineering開始***                           |
613 Target: 20, victim: 4, Loss: 10.2242, Acc: 0.00%, CE_Loss: 10.22, Reg_Loss:2563.23, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2546.65: 2%| | 21/1000 [00:10<08:05, 2.02it/s]
614 ***Trigger Reverse Engineering結束***                           |
615 Target Class: 3 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 11
616 *****檢測結束*****                                           |
617 檢測結果: Model是安全的(Benign)
618 整體耗時: 18.445801734924316                                         | 握描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000505
619 *****Pre-Screening結束*****                                         |
620 *****Pre-Screening開始***                                         |
621 *****Pre-Screening結束***                                         |
622 可能的攻擊方式: Label Specific Backdoor Attack
623 可能的 target-victim 配對: ['1-4']
624 ***Trigger Reverse Engineering開始***                           |
625 Target: 1, victim: 4, Loss: 5.8203, Acc: 5.00%, CE_Loss: 5.82, Reg_Loss:4032.35, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3714.88: 2%| | 20/1000 [00:43<35:19, 2.16s/it]
626 ***Trigger Reverse Engineering結束***                           |
627 Target Class: 1 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 21
628 *****檢測結束*****                                           |
629 檢測結果: Model是安全的(Benign)
630 整體耗時: 51.48796224594116                                         | 握描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000506
631 *****Pre-Screening開始***                                         |
632 *****Pre-Screening結束***                                         |
633 *****Pre-Screening結束***                                         |
634 可能的攻擊方式: Label Specific Backdoor Attack
635 可能的 target-victim 配對: ['0-7', '0-19', '2-12', '3-4', '3-9', '4-3', '5-6', '5-11', '6-3', '6-5', '8-11', '9-3', '12-2', '15-2', '15-18', '16-0', '16-1', '16-7', '17-14', '18-16', '18-19', '18-20', '19-18', '20-1', '20-16']
636 ***Trigger Reverse Engineering開始***                           |
637 Target: 19, victim: 18, Loss: 1.5233, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:1797.57, Cost:0.00 best_reg:1800.22 avg_loss_reg:1800.22: 64%| █ | 644/1000 [07:06<03:55, 1.51it/s]
638 early stop 所有

```

```

639 ***Trigger Reverse Engineering結束***  

640 Target Class: 19 Victim Class: 18 Trigger Size: 1797.567626953125 Optimization Steps: 319  

641 *****檢測結束*****  

642 檢測結果: Model是安全的(Benign)  

643 整體耗時: 434.56749844551086  

644 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000507-----  

645 ***Pre-Screening開始***  

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

647 可能的 target-victim 配對: [6-3]  

648 ***Trigger Reverse Engineering開始***  

649 Target: 6, victim: 3, Loss: 13.0298, Acc: 0.00%, CE_Loss: 13.03, Reg_Loss:2567.32, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2550.86: 1%| | 10/1000 [0:01<01:40, 9.80it/s]  

650 Target Class: 6 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 11  

651 *****檢測結束*****  

652 Target Class: 6 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 11  

653 *****檢測結束*****  

654 檢測結果: Model是安全的(Benign)  

655 整體耗時: 6.01404333114624  

656 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000508-----  

657 ***Pre-Screening開始***  

658 ***Pre-Screening結束***  

659 ***檢測結束***  

660 檢測結果: Model是安全的(Benign)  

661 整體耗時: 11.146109104156494  

662 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000509-----  

663 ***Pre-Screening開始***  

664 ***Pre-Screening結束***  

665 ***檢測結束***  

666 檢測結果: Model是安全的(Benign)  

667 整體耗時: 23.142169952392578  

668 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000510-----  

669 ***Pre-Screening開始***  

670 ***Pre-Screening結束***  

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

672 可能的 target-victim 配對: [0-15, '3-20', '10-15', '15-20', '17-20', '20-15', '21-20]  

673 ***Trigger Reverse Engineering開始***  

674 Target: 21, victim: 20, Loss: 15.1456, Acc: 0.00%, CE_Loss: 15.15, Reg_Loss:2496.88, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2491.75: 9%| | 18/1000 [03:49<40:42, 2.67s/it]  

675 ***Trigger Reverse Engineering結束***  

676 Target Class: 0 Victim Class: 15 Trigger Size: 1000000000.0 Optimization Steps: 11  

677 *****檢測結束*****  

678 檢測結果: Model是安全的(Benign)  

679 整體耗時: 251.00414991378784  

680 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000511-----  

681 ***Pre-Screening開始***  

682 ***Pre-Screening結束***  

683 ***檢測結束***  

684 檢測結果: Model是安全的(Benign)  

685 整體耗時: 11.085107803344727  

686 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000512-----  

687 ***Pre-Screening開始***  

688 ***Pre-Screening結束***  

689 ***檢測結束***  

690 檢測結果: Model是安全的(Benign)  

691 整體耗時: 5.267090797424316  

692 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000513-----  

693 ***Pre-Screening開始***  

694 ***Pre-Screening結束***  

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

696 可能的 target-victim 配對: ['13-8', '14-1']  

697 ***Trigger Reverse Engineering開始***  

698 Target: 13, victim: 8, Loss: 1.4495, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:179.81, Cost:0.01 best_reg:180.59 avg_loss_reg:15347.84: 16%| | 155/1000 [06:22<34:45, 2.47s/it]  

699 early stop 所有  

700 ***Trigger Reverse Engineering結束***  

701 Target Class: 13 Victim Class: 8 Trigger Size: 179.80850219726562 Optimization Steps: 145  

702 ***Symmetric Check開始***  

703 Target: 8, victim: 13, Loss: 0.4692, Acc: 85.00%, CE_Loss: 0.47, Reg_Loss:15403.12, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:15347.84: 100%| | 145/145 [05:57<00:00, 2.47s/it]  

704 ***Symmetric Check結束***  

705 *****檢測結束*****  

706 檢測結果: Model含有後門(Abnormal)  

707 整體耗時: 751.1787374019623  

708 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000514-----  

709 ***Pre-Screening開始***
```

```

710 ***Pre-Screening結束***  

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

712 可能的 target-victim 配對: ['2-3', '2-6']  

713 ***Trigger Reverse Engineering 開始***  

714 Target: 2, victim: 3, Loss: 1.7907, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:67.55, Cost:0.03 best_reg:67.63 avg_loss_reg:67.63: 10% █ | 102/1000 [00:36<05:17, 2.83it/s]  

715 early stop 所有  

716 ***Trigger Reverse Engineering 結束***  

717 Target Class: 2 Victim Class: 3 Trigger Size: 67.55 [597759521484 Optimization Steps: 93  

718 ***Symmetric Check開始***  

719 Target: 3, victim: 2, Loss: 1.8897, Acc: 95.00%, CE_Loss: 0.28, Reg_Loss:5423.27, Cost:0.00 best_reg:12199.41 avg_loss_reg:5503.18: 100% █ | 93/93 [00:32<00:00, 2.87it/s]  

720 ***Symmetric Check結束***  

721 檢測結果: Model含有後門(Abnormal)  

722 整體耗時: 73.57213521003723  

723  

724 -----掃描檔案: D:\UUUI\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000515-----  

725 ***Pre-Screening 開始***  

726 ***Pre-Screening 結束***  

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

728 可能的 target-victim 配對: ['4-1', '4-2', '4-5', '5-0']  

729 ***Trigger Reverse Engineering 開始***  

730 Target: 5, victim: 0, Loss: 3.3136, Acc: 20.00%, CE_Loss: 3.31, Reg_Loss:3948.22, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:3649.38: 5% █ | 53/1000 [01:02<18:30, 1.17s/it]  

731 ***Trigger Reverse Engineering 結束***  

732 Target Class: 4 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11  

733 ***Pre-Screening 結束***  

734 檢測結果: Model是安全的(Benign)  

735 整體耗時: 67.69993734359741  

736 -----掃描檔案: D:\UUUI\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000516-----  

737 ***Pre-Screening 開始***  

738 ***Pre-Screening 結束***  

739 ***檢測結束***  

740 檢測結果: Model是安全的(Benign)  

741 整體耗時: 10.565248250961304  

742 -----掃描檔案: D:\UUUI\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000517-----  

743 ***Pre-Screening 開始***  

744 ***Pre-Screening 結束***  

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

746 可能的 target-victim 配對: ['3-4', '4-3', '5-2']  

747 ***Trigger Reverse Engineering 開始***  

748 Target: 4, victim: 3, Loss: 4.3456, Acc: 100.00%, CE_Loss: 0.39, Reg_Loss:781.24, Cost:0.01 best_reg:782.48 avg_loss_reg:782.48: 27% █ | 271/1000 [10:06<27:11, 2.24s/it]  

749 early stop 所有  

750 ***Trigger Reverse Engineering 結束***  

751 Target Class: 3 Victim Class: 3 Trigger Size: 781.236811640625 Optimization Steps: 249  

752 ***Symmetric Check開始***  

753 Target: 3, victim: 4, Loss: 2.5840, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:1057.22, Cost:0.00 best_reg:1031.29 avg_loss_reg:1057.62: 100% █ | 249/249 [09:07<00:00, 2.20s/it]  

754 ***Symmetric Check結束***  

755 ***Pre-Screening 開始***  

756 檢測結果: Model是安全的(Benign)  

757 整體耗時: 1164.1218991279602  

758 -----掃描檔案: D:\UUUI\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000518-----  

759 ***Pre-Screening 結束***  

760 ***Pre-Screening 結束***  

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

762 可能的 target-victim 配對: ['1-4', '8-10', '10-8']  

763 ***Trigger Reverse Engineering 開始***  

764 Target: 10, victim: 8, Loss: 5.2189, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:649.29, Cost:0.01 best_reg:650.68 avg_loss_reg:650.68: 19% █ | 191/1000 [00:20<01:27, 9.25it/s]  

765 early stop 所有  

766 ***Trigger Reverse Engineering 結束***  

767 Target Class: 10 Victim Class: 8 Trigger Size: 649.28515625 Optimization Steps: 170  

768 ***Symmetric Check開始***  

769 Target: 8, victim: 10, Loss: 3.1938, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:895.27, Cost:0.00 best_reg:894.97 avg_loss_reg:894.97: 100% █ | 170/170 [00:17<00:00, 9.99it/s]  

770 ***Symmetric Check結束***  

771 ***Pre-Screening 結束***  

772 檢測結果: Model是安全的(Benign)  

773 整體耗時: 42.49762296676636  

774 -----掃描檔案: D:\UUUI\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000519-----  

775 ***Pre-Screening 開始***  

776 ***Pre-Screening 結束***  

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

778 可能的 target-victim 配對: ['3-13', '9-13', '11-18', '21-2']  

779 ***Trigger Reverse Engineering 開始***  

780 Target: 21, victim: 2, Loss: 8.1945, Acc: 0.00%, CE_Loss: 8.19, Reg_Loss:2571.05, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2554.36: 5% █ | 53/1000 [01:27<26:08, 1.66s/it]

```

```

781 ***Trigger Reverse Engineering 結束 ***
782 Target Class: 3 Victim Class: 13 Trigger Size: 1000000000.0 Optimization Steps: 11
783 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000520-----
784 檢測結果: Model是安全的(Benign)
785 整體耗時: 104.89127492904663
786 -----



787 ***Pre-Screening開始***
788 ***Pre-Screening結束***
789 可能的攻擊方式: Universal Backdoor Attack
790 可能的 target class: 1
791 可能的 victim classes: ALL
792 ***Trigger Reverse Engineering開始***
793 Target: 1, victim: 19, Loss: 4.6352, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:4633.54, Cost:0.00 best_reg:4591.62 avg_loss_reg:4600.78: 16%|■ | 162/1000 [1:34:30<8:08:52, 35.00s/it]
794 early stop 所有
795 ***Trigger Reverse Engineering結束***


796 Target Class: 1 Victim Class: all Trigger Size: 4591.620465959822 Optimization Steps: 163
797 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000521-----
798 檢測結果: Model是安全的(Benign)
799 整體耗時: 5689.902697563171
800 -----



801 ***Pre-Screening開始***
802 ***Pre-Screening結束***
803 可能的攻擊方式: Universal Backdoor Attack
804 可能的 target class: 16
805 可能的 victim classes: ALL
806 ***Trigger Reverse Engineering開始***
807 Target: 16, victim: 16, Loss: 0.1710, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:114.01, Cost:0.00 best_reg:118.79 avg_loss_reg:113.04: 5%|■ | 54/1000 [11:12<3:16:26, 12.46s/it]
808 early stop 所有
809 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000522-----
810 Target Class: 16 Victim Class: all Trigger Size: 118.78918711344402 Optimization Steps: 55
811 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000523-----
812 檢測結果: Model含有後門(Abnormal)
813 整體耗時: 684.5530257225037
814 -----



815 ***Pre-Screening開始***
816 ***Pre-Screening結束***
817 可能的攻擊方式: Label Specific Backdoor Attack
818 可能的 target-victim 配對: ['1-7', '1-18', '17-18']
819 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000524-----
820 Target: 17, victim: 18, Loss: 0.3620, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:874.48, Cost:0.00 best_reg:877.01 avg_loss_reg:864.72: 24%|■ | 236/1000 [10:54<35:18, 2.77s/it]
821 0%| 0/215 [0:00:<?, ?] it/s|early stop 所有
822 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000525-----
823 Target Class: 17 Victim Class: 18 Trigger Size: 874.4785766601562 Optimization Steps: 215
824 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000526-----
825 Target: 18, victim: 17, Loss: 0.7516, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:902.30, Cost:0.00 best_reg:896.43 avg_loss_reg:901.21: 100%|■ | 215/215 [09:54<00:00, 2.77s/it]
826 ***Symmetric Check結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000527-----
827 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000528-----
828 檢測結果: Model是安全的(Benign)
829 整體耗時: 1266.2277092933655
830 -----



831 ***Pre-Screening開始***
832 ***Pre-Screening結束***
833 ***檢測結束***
834 檢測結果: Model是安全的(Benign)
835 整體耗時: 10.091041088104248
836 -----



837 ***Pre-Screening開始***
838 ***Pre-Screening結束***
839 可能的攻擊方式: Label Specific Backdoor Attack
840 可能的 target-victim 配對: ['0-13', '6-5']
841 ***Trigger Reverse Engineering開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000529-----
842 Target: 6, victim: 5, Loss: 10.6030, Acc: 0.00%, CE_Loss: 10.60, Reg_Loss:2575.43, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2556.40: 2%| | 21/1000 [00:23<17:52, 1.10s/it]
843 ***Trigger Reverse Engineering結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000530-----
844 Target Class: 0 Victim Class: 13 Trigger Size: 10000000000.0 Optimization Steps: 11
845 *****檢測結束*****-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000531-----
846 檢測結果: Model是安全的(Benign)
847 整體耗時: 31.139619827270508
848 -----



849 ***Pre-Screening開始***
850 ***Pre-Screening結束***
851 可能的攻擊方式: Label Specific Backdoor Attack

```

```

852 可能的 target-victim 配對: ['4-3']
853 ***Trigger Reverse Engineering 開始***
854 Target: 4, victim: 3, Loss: 5.8719, Acc: 25.00%, CE_Loss: 5.87, Reg_Loss:3329.36, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:3133.80: 2%| | 20/1000 [00:10<08:26, 1.93it/s]
855 ***Trigger Reverse Engineering 結束***
856 Target Class: 4 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 21
857 *****檢測結果: Model是安全的(Benign)
858 整體耗時: 16.903932309829712-----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000526-----
859 *****Pre-Screening 開始****
860 *****Pre-Screening 結束****
861 *****檢測結果: Model是安全的(Benign)
862 *****Pre-Screening 結束****
863 *****檢測結果: Model是安全的(Benign)
864 檢測結果: Model是安全的(Benign)
865 整體耗時: 8.114787578582764-----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000527-----
866 *****Pre-Screening 開始****
867 *****Pre-Screening 結束****
868 *****Pre-Screening 結束****
869 *****檢測結果: Model是安全的(Benign)
870 檢測結果: Model是安全的(Benign)
871 整體耗時: 21.072645902633667-----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000528-----
872 *****Pre-Screening 開始****
873 *****Pre-Screening 結束****
874 *****Pre-Screening 結束****
875 *****檢測結果: Model是安全的(Benign)
876 檢測結果: Model是安全的(Benign)
877 整體耗時: 13.481308937072754-----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000529-----
878 *****Pre-Screening 開始****
879 *****Pre-Screening 結束****
880 *****Pre-Screening 結束****
881 可能的攻擊方式: Label Specific Backdoor Attack
882 可能的 target-victim 配對: [3-17]
883 ***Trigger Reverse Engineering 開始***
884 Target: 3, victim: 17, Loss: 12.1405, Acc: 0.00%, CE_Loss: 12.14, Reg_Loss:2548.70, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2532.64: 1%| | 10/1000 [00:03<06:34, 2.51it/s]
885 ***Trigger Reverse Engineering 結束***
886 Target Class: 3 Victim Class: 17 Trigger Size: 1000000000.0 Optimization Steps: 11
887 *****檢測結果: Model是安全的(Benign)
888 檢測結果: Model是安全的(Benign)
889 整體耗時: 10.650186538696289-----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000530-----
890 *****Pre-Screening 開始****
891 *****Pre-Screening 結束****
892 *****Pre-Screening 結束****
893 可能的攻擊方式: Label Specific Backdoor Attack
894 可能的 target-victim 配對: ['4-19', '4-12', '4-0', '13-19', '16-19']
895 ***Trigger Reverse Engineering 開始***
896 Target: 16, victim: 19, Loss: 13.0143, Acc: 0.00%, CE_Loss: 13.01, Reg_Loss:2552.64, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2537.83: 5%| | 54/1000 [01:21<23:49, 1.51it/s]
897 ***Trigger Reverse Engineering 結束***
898 Target Class: 4 Victim Class: 19 Trigger Size: 1000000000.0 Optimization Steps: 11
899 檢測結果: Model是安全的(Benign)
900 檢測結果: Model是安全的(Benign)
901 整體耗時: 93.3172583483887-----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000531-----
902 *****Pre-Screening 開始****
903 *****Pre-Screening 結束****
904 *****Pre-Screening 結束****
905 可能的攻擊方式: Label Specific Backdoor Attack
906 可能的 target-victim 配對: ['0-19', '0-23', '1-7', '1-8', '1-13', '2-4', '2-8', '2-13', '3-20', '4-5', '4-7', '15-6', '15-7', '15-8', '14-20', '14-21', '12-9', '13-7', '13-8', '14-20', '14-21', '12-14', '13-2', '13-7', '13-8', '14-20', '14-21', '12-21', '22-19', '21-22', '19-23', '17-20', '17-21', '22-23', '23-0', '23-19']
907 ***Trigger Reverse Engineering 開始***
908 Target: 15, victim: 6, Loss: 0.9246, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:810.35, Cost:0.00 best_reg:812.94 avg_loss_reg:812.94: 70%| | 704/1000 [37:06<15:36, 3.16s/it]
909 early stop 所有
910 ***Trigger Reverse Engineering 結束***
911 Target Class: 15 Victim Class: 6 Trigger Size: 810.35009765625 Optimization Steps: 172
912 ***Symmetric Check開始***
913 Target: 6, victim: 15, Loss: 0.5054, Acc: 95.00%, CE_Loss: 0.24, Reg_Loss:10224.56, Cost:0.00 best_reg:18157.05 avg_loss_reg:10174.34: 100%| | 172/172 [08:47<00:00, 3.07s/it]
914 ***Symmetric Check結束****
915 *****檢測結果: Model含有後門(Abnormal)
916 檢測結果: Model是安全的(Benign)
917 整體耗時: 2773.907059907913-----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000532-----
918 *****Pre-Screening 開始****
919 *****Pre-Screening 結束****
920 *****檢測結果: Model是安全的(Benign)
921 *****檢測結果: Model是安全的(Benign)
922 檢測結果: Model是安全的(Benign)

```

```

923 整體耗時: 18.164676904678345 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000533
924 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000533
925 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000533
926 可能的攻擊方式: Label Specific Backdoor Attack
927 可能的 target-victim 配對: ['12-0']
928 ***Trigger Reverse Engineering 開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000533
929 Target: 12, victim: 0, Loss: 0.9127, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:796.95, Cost:0.00 best_reg:797.85 avg_loss_reg:798.12: 21%[■] | 210/1000 [02:01 <07:35, 1.73it/s]
930 Target: 0, victim: 12, Loss: 2.9927, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:815.62, Cost:0.00 best_reg:834.10 avg_loss_reg:825.07: 60%[■] | 126/211 [01:13 <00:49, 1.71it/s]
931 early stop 所有
932 ***Trigger Reverse Engineering 結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000533
933 Target Class: 12 Victim Class: 0 Trigger Size: 796.9490356445312 Optimization Steps: 211
934 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000533
935 Target: 0, victim: 12, Loss: 2.9927, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:815.62, Cost:0.00 best_reg:834.10 avg_loss_reg:825.07: 60%[■] | 126/211 [01:13 <00:49, 1.71it/s]
936 early stop 所有
937 ***Symmetric Check 結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000533
938 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000533
939 檢測結果: Model是安全的(Benign)
940 整體耗時: 200.77342987060547 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000534
941 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000534
942 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000534
943 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000534
944 可能的攻擊方式: Label Specific Backdoor Attack
945 可能的 target-victim 配對: ['0-3','3-0']
946 ***Trigger Reverse Engineering 開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000534
947 Target: 3, victim: 0, Loss: 10.4018, Acc: 0.00%, CE_Loss: 10.40, Reg_Loss:2536.95, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2528.01: 2%[■] | 21/1000 [00:01 <01:31, 10.69it/s]
948 ***Trigger Reverse Engineering 結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000534
949 Target Class: 0 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 11
950 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000535
951 檢測結果: Model是安全的(Benign)
952 整體耗時: 3.8334460258483887 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000535
953 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000535
954 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000535
955 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000535
956 可能的攻擊方式: Universal Backdoor Attack
957 可能的 target class: 0
958 可能的 victim classes: ALL
959 ***Trigger Reverse Engineering 開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000535
960 Target: 0, victim: 8, Loss: 1.9468, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:6567.68, Cost:0.00 best_reg:6586.20 avg_loss_reg:6572.04: 14%[■] | 139/1000 [44:54 <4:38:10, 19.39s/it]
961 early stop 所有
962 ***Trigger Reverse Engineering 結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000535
963 Target Class: 0 Victim Class: all Trigger Size: 6586.198079427083 Optimization Steps: 140
964 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000535
965 檢測結果: Model是安全的(Benign)
966 整體耗時: 2708.246204137802 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000536
967 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000536
968 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000536
969 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000536
970 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000536
971 檢測結果: Model是安全的(Benign)
972 整體耗時: 9.330997228622437 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000537
973 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000537
974 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000537
975 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000537
976 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000537
977 檢測結果: Model是安全的(Benign)
978 整體耗時: 5.170516014099121 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000538
979 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000538
980 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000538
981 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000538
982 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000538
983 檢測結果: Model是安全的(Benign)
984 整體耗時: 10.363024711608887 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000540
985 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000540
986 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000540
987 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000540
988 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000540
989 檢測結果: Model是安全的(Benign)
990 整體耗時: 10.898921012878418 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000540
991 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000540
992 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000540
993 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000540

```

```

994 可能的攻擊方式: Label Specific Backdoor Attack
995 可能的 target-victim 配對: ['5-4']
996 ***Trigger Reverse Engineering開始***
997 Target: 5, victim: 4, Loss: 11.2666, Acc: 0.00%, CE_Loss: 11.27, Reg_Loss:2544.13, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2529.88: 1% | 10/1000 [00:21<35:07, 2.13s/it]
998 ***Trigger Reverse Engineering結束***
999 Target Class: 5 Victim Class: 4 Trigger Size: 1000000000.00 Optimization Steps: 11
1000 *****檢測結果: Model是安全的(Benign)
1001 檢測結果: Model是安全的(Benign)
1002 整體耗時: 28.147724866867065
1003 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000541-----
1004 ***Pre-Screening開始***
1005 ***Pre-Screening結束***
1006 可能的攻擊方式: Label Specific Backdoor Attack
1007 可能的 target-victim 配對: ['2-1', '19-11', '19-15']
1008 ***Trigger Reverse Engineering開始***
1009 Target: 19, victim: 15, Loss: 3.2307, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:408.44, Cost:0.01 best_reg:408.81 avg_loss_reg:408.81: 22% | 224/1000 [06:26<22:18, 1.73s/it]
1010 early stop 所有
1011 ***Trigger Reverse Engineering結束***
1012 Target Class: 19 Victim Class: 15 Trigger Size: 408.43609619140625 Optimization Steps: 131
1013 ***Symmetric Check開始***
1014 Target: 15, victim: 19, Loss: 2.6477, Acc: 90.00%, CE_Loss: 0.48, Reg_Loss:4881.30, Cost:0.00 best_reg:5132.06 avg_loss_reg:4920.69: 100% | 131/131 [03:51<00:00, 1.76s/it]
1015 ***Symmetric Check結束***
1016 *****檢測結束*****
1017 檢測結果: Model含有後門(Abnormal)
1018 整體耗時: 635.1289131641388
1019 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000542-----
1020 ***Pre-Screening開始***
1021 ***Pre-Screening結束***
1022 ***檢測結束***
1023 檢測結果: Model是安全的(Benign)
1024 整體耗時: 7.723332643508911
1025 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000543-----
1026 ***Pre-Screening開始***
1027 ***Pre-Screening結束***
1028 可能的攻擊方式: Label Specific Backdoor Attack
1029 可能的 target-victim 配對: ['9-0', '13-1', '14-1']
1030 ***Trigger Reverse Engineering開始***
1031 Target: 14, victim: 1, Loss: 6.0228, Acc: 0.00%, CE_Loss: 6.02, Reg_Loss:2560.02, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2538.76: 4% | 42/1000 [01:45<40:01, 2.51s/it]
1032 ***Trigger Reverse Engineering結束***
1033 Target Class: 9 Victim Class: 0 Trigger Size: 10000000000.00 Optimization Steps: 11
1034 *****檢測結束*****
1035 檢測結果: Model是安全的(Benign)
1036 整體耗時: 124.54310584068298
1037 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000544-----
1038 ***Pre-Screening開始***
1039 ***Pre-Screening結束***
1040 ***檢測結束***
1041 檢測結果: Model是安全的(Benign)
1042 整體耗時: 4.861485242843628
1043 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000545-----
1044 ***Pre-Screening開始***
1045 ***Pre-Screening結束***
1046 ***檢測結束***
1047 檢測結果: Model是安全的(Benign)
1048 整體耗時: 8.604986190795898
1049 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000546-----
1050 ***Pre-Screening開始***
1051 ***Pre-Screening結束***
1052 可能的攻擊方式: Label Specific Backdoor Attack
1053 可能的 target-victim 配對: ['6-0', '6-7']
1054 ***Trigger Reverse Engineering開始***
1055 Target: 6, victim: 7, Loss: 4.3019, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:160.28, Cost:0.03 best_reg:160.54 avg_loss_reg:161.87: 16% | 155/1000 [00:24<02:12, 6.38it/s]
1056 early stop 所有
1057 ***Trigger Reverse Engineering結束***
1058 Target Class: 6 Victim Class: 7 Trigger Size: 160.28134155273438 Optimization Steps: 148
1059 ***Symmetric Check開始***
1060 Target: 7, victim: 6, Loss: 0.7409, Acc: 100.00%, CE_Loss: 0.58, Reg_Loss:6210.67, Cost:0.00 best_reg:6099.01 avg_loss_reg:6156.56: 100% | 148/148 [00:22<00:00, 6.50it/s]
1061 ***Symmetric Check結束***
1062 *****檢測結束*****
1063 檢測結果: Model含有後門(Abnormal)
1064 整體耗時: 53.23779606819153

```

```

1065 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000547 -----
1066 ***Pre-Screening開始***
1067 ***Pre-Screening結束***
1068 ***檢測結束***
1069 檢測結果: Model是安全的(Benign)
1070 整體耗時: 5.283130407333374
1071 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000548 -----
1072 ***Pre-Screening開始***
1073 ***Pre-Screening結束***
1074 可能的攻擊方式: Label Specific Backdoor Attack
1075 可能的 target-victim 配對: ['2-4', '2-11', '3-4', '6-0', '6-4', '6-11', '7-11', '9-0', '10-0']
1076 ***Trigger Reverse Engineering開始***
1077 Target: 10, victim: 0 Loss: 7.1067, Acc: 0.00%, CE_Loss: 7.11, Reg_Loss:2572.20, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2557.04: 12% █ | 118/1000 [00:10<01:19, 11.15it/s]
1078 ***Trigger Reverse Engineering結束***
1079 Target Class: 2 Victim Class: 4 Trigger Size: 1000000000.0 Optimization Steps: 11
1080 *****檢測結束*****檢測結果: Model是安全的(Benign)
1081 整體耗時: 15.330056428909302
1082 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000549 -----
1083 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000550 -----
1084 ***Pre-Screening開始***
1085 ***Pre-Screening結束***
1086 可能的攻擊方式: Universal Backdoor Attack
1087 可能的 target class: 17
1088 可能的 victim classes: ALL
1089 ***Trigger Reverse Engineering結束***
1090 Target: 17, victim: 22, Loss: 0.4714, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:41.38, Cost:0.01 best_reg:41.25 avg_loss_reg:41.47: 7% █ | 68/1000 [08:23<1:55:01, 7.40s/it]
1091 early stop 所有
1092 ***Trigger Reverse Engineering結束***
1093 Target Class: 17 Victim Class: 41.25106334686279 Optimization Steps: 69
1094 *****檢測結束*****檢測結果: Model含有後門(Abnormal)
1095 檢測結果: Model是安全的(Benign)
1096 整體耗時: 509.0661692619324
1097 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000550 -----
1098 ***Pre-Screening開始***
1099 ***Pre-Screening結束***
1100 可能的攻擊方式: Label Specific Backdoor Attack
1101 可能的 target-victim 配對: ['1-3', '2-4', '3-0', '3-1', '4-2']
1102 ***Trigger Reverse Engineering開始***
1103 Target: 4, victim: 2, Loss: 10.7499, Acc: 0.00%, CE_Loss: 10.75, Reg_Loss:2570.34, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2552.69: 6% █ | 64/1000 [01:09<17:02, 1.09s/it]
1104 ***Trigger Reverse Engineering結束***
1105 Target Class: 1 Victim Class: 3 Trigger Size: 10000000000.0 Optimization Steps: 11
1106 *****檢測結束*****檢測結果: Model是安全的(Benign)
1107 整體耗時: 73.91453909873962
1108 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000551 -----
1109 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000552 -----
1110 ***Pre-Screening開始***
1111 ***Pre-Screening結束***
1112 可能的攻擊方式: Label Specific Backdoor Attack
1113 可能的 target-victim 配對: ['3-15', '13-2', '13-5', '15-3', '21-1']
1114 ***Trigger Reverse Engineering開始***
1115 Target: 21, victim: 1, Loss: 4.2196, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:154.43, Cost:0.03 best_reg:155.00 avg_loss_reg:155.38: 21% █ | 208/1000 [02:10<08:18, 1.59it/s]
1116 early stop 所有
1117 ***Trigger Reverse Engineering結束***
1118 Target Class: 21 Victim Class: 1 Trigger Size: 154.434814453125 Optimization Steps: 155
1119 ***Symmetric Check開始***
1120 Target: 1, victim: 21, Loss: 3.1639, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:384.59, Cost:0.01 best_reg:390.54 avg_loss_reg:384.37: 100% █ | 155/155 [01:31<00:00, 1.70it/s]
1121 ***Symmetric Check結束***
1122 *****檢測結束*****檢測結果: Model是安全的(Benign)
1123 檢測結果: Model是安全的(Benign)
1124 整體耗時: 231.13523888587952
1125 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000552 -----
1126 ***Pre-Screening開始***
1127 ***Pre-Screening結束***
1128 可能的攻擊方式: Label Specific Backdoor Attack
1129 可能的 target-victim 配對: ['0-6', '18-10']
1130 ***Trigger Reverse Engineering開始***
1131 Target: 18, victim: 10 Loss: 7.7960, Acc: 10.00%, CE_Loss: 7.80, Reg_Loss:3467.33, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3251.88: 3% █ | 31/1000 [01:13<38:09, 2.36s/it]
1132 ***Trigger Reverse Engineering結束***
1133 Target Class: 0 Victim Class: 6 Trigger Size: 1000000000.0 Optimization Steps: 11
1134 *****檢測結束*****檢測結果: Model是安全的(Benign)
1135 檢測結果: Model是安全的(Benign)

```

```
1136 整體耗時: 85.15221929550171 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000553
1137 ***Pre-Screening開始*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000553
1138 ***Pre-Screening結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000553
1139 ***檢測結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000553
1140 檢測結果: Model是安全的(Benign)
1141 檢測結果: Model是安全的(Benign)
1142 整體耗時: 5.172771692276001 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000554
1143 ***Pre-Screening開始*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000554
1144 ***Pre-Screening結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000554
1145 ***檢測結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000554
1146 檢測結果: Model是安全的(Benign)
1147 檢測結果: Model是安全的(Benign)
1148 檢測結果: Model是安全的(Benign)
1149 整體耗時: 10.7808127027893 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000555
1150 ***Pre-Screening開始*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000555
1151 ***Pre-Screening結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000555
1152 可能的攻擊方式: Label Specific Backdoor Attack
1153 可能的 target-victim 配對: ['4-2']
1154 ***Trigger Reverse Engineering開始*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000555
1155 Target: 4, victim: 2 | Loss: 11.9984, Acc: 0.00%, CE_Loss: 12.00, Reg_Loss:2572.55, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2553.41: 1% | 10/1000 [00:42<1:10:35, 4.28s/it]
1156 ***Trigger Reverse Engineering結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000555
1157 Target Class: 4 Victim Class: 2 Trigger Size: 1000000000.0 Optimization Steps: 11 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000555
1158 *****檢測結束***** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000555
1159 檢測結果: Model是安全的(Benign)
1160 檢測結果: Model是安全的(Benign)
1161 整體耗時: 71.22577786445618 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000556
1162 ***Pre-Screening開始*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000556
1163 ***Pre-Screening結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000556
1164 可能的攻擊方式: Label Specific Backdoor Attack | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000556
1165 可能的 target-victim 配對: ['0-1', '0-5', '0-6', '1-0', '2-8', '6-3', '6-4', '8-2'] | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000556
1166 ***Trigger Reverse Engineering開始*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000556
1167 Target: 8, victim: 2 | Loss: 9.1414, Acc: 0.00%, CE_Loss: 9.14, Reg_Loss:2555.63, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2541.75: 9% | 10/1000 [00:07<01:19, 11.48s/it]
1168 ***Trigger Reverse Engineering結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000556
1169 Target Class: 0 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000556
1170 *****檢測結束***** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000556
1171 檢測結果: Model是安全的(Benign)
1172 整體耗時: 12.035704374313354 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000557
1173 ***Pre-Screening開始*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000557
1174 ***Pre-Screening結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000557
1175 ***Pre-Screening結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000557
1176 ***檢測結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000557
1177 檢測結果: Model是安全的(Benign)
1178 整體耗時: 9.943172216415405 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000558
1179 ***Pre-Screening開始*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000558
1180 ***Pre-Screening結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000558
1181 ***Pre-Screening結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000558
1182 ***檢測結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000558
1183 檢測結果: Model是安全的(Benign)
1184 整體耗時: 9.047840595245361 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000559
1185 ***Pre-Screening開始*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000559
1186 ***Pre-Screening結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000559
1187 ***Pre-Screening結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000559
1188 可能的攻擊方式: Universal Backdoor Attack
1189 可能的 target class: 11 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000559
1190 可能的 victim classes: ALL | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000559
1191 ***Trigger Reverse Engineering開始*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000559
1192 Target: 11, victim: 14, Loss: 0.3756, Acc: 93.75%, CE_Loss: 0.15, Reg_Loss:508.26, Cost:0.00 best_reg:546.90 avg_loss_reg:509.27: 4% | 10/1000 [08:04<2:51:20, 10.77s/it]
1193 early stop 所有 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000560
1194 ***Trigger Reverse Engineering結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000560
1195 Target Class: 11 Victim Class: all Trigger Size: 546.9043518066406 Optimization Steps: 46 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000560
1196 *****檢測結束***** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000560
1197 檢測結果: Model含有後門(Abnormal)
1198 整體耗時: 49.1.95978236198425 | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000560
1199 ***Pre-Screening開始*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000560
1200 ***Pre-Screening結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000560
1201 可能的攻擊方式: Label Specific Backdoor Attack
1202 可能的 target-victim 配對: ['2-6']
1203 可能的 target-victim 配對: ['2-6']
1204 ***Trigger Reverse Engineering開始*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000560
1205 Target: 2, victim: 6, Loss: 10.8139, Acc: 0.00%, CE_Loss: 10.81, Reg_Loss:2575.44, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2557.24: 1% | 10/1000 [00:01<02:19, 7.08s/it]
1206 ***Trigger Reverse Engineering結束*** | 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000560
```

```

1207 Target Class: 2 Victim Class: 6 Trigger Size: 10000000000.0 Optimization Steps: 11
1208 *****檢測結束*****
1209 檢測結果: Model是安全的(Benign)
1210 整體耗時: 3.5101823806762695
1211 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000561-----
1212 ***Pre-Screening開始
1213 ***Pre-Screening結束***
1214 ***檢測結束***
1215 檢測結果: Model是安全的(Benign)
1216 整體耗時: 14.23822283744812
1217 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000562-----
1218 ***Pre-Screening開始
1219 ***Pre-Screening結束***
1220 ***檢測結束***
1221 檢測結果: Model是安全的(Benign)
1222 整體耗時: 5.083018064498901
1223 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000563-----
1224 ***Pre-Screening開始
1225 ***Pre-Screening結束***
1226 可能的攻擊方式: Universal Backdoor Attack
1227 可能的 target class: 0
1228 可能的 victim classes: ALL
1229 ***Trigger Reverse Engineering開始***
1230 Target: 0, victim: 22, Loss: 2.5627, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss: 5760.08, Cost: 0.00 best_reg: 5601.66 avg_loss_reg: 5669.43: 14% █ | 138/1000 [30:07 < 3:08:08, 13.10s/it]
1231 early stop 所有
1232 ***Trigger Reverse Engineering結束***
1233 Target Class: 0 Victim Class: all Trigger Size: 5601.6558837890625 Optimization Steps: 139
1234 *****檢測結束*****
1235 檢測結果: Model是安全的(Benign)
1236 整體耗時: 1819.8704240322113
1237 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000564-----
1238 ***Pre-Screening開始
1239 ***Pre-Screening結束***
1240 可能的攻擊方式: Label Specific Backdoor Attack
1241 可能的 target-victim 配對: [-1-0, '16-0', '19-0', '19-1']
1242 ***Trigger Reverse Engineering開始***
1243 Target: 16, victim: 0, Loss: 2.0069, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss: 1802.23, Cost: 0.00 best_reg: 1802.64 avg_loss_reg: 1794.10: 44% █ | 435/1000 [02:20 < 03:03, 3.09it/s]
1244 early stop 所有
1245 ***Trigger Reverse Engineering結束***
1246 Target Class: 16 Victim Class: 0 Trigger Size: 1802.22705078125 Optimization Steps: 402
1247 *****檢測結束*****
1248 檢測結果: Model是安全的(Benign)
1249 整體耗時: 147.16095519065857
1250 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000565-----
1251 ***Pre-Screening開始
1252 ***Pre-Screening結束***
1253 ***檢測結束***
1254 檢測結果: Model是安全的(Benign)
1255 整體耗時: 15.910375356674194
1256 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000566-----
1257 ***Pre-Screening開始
1258 ***Pre-Screening結束***
1259 可能的攻擊方式: Label Specific Backdoor Attack
1260 可能的 target-victim 配對: [-6-4, '6-12', '8-4', '8-7', '8-12', '10-1', '14-0', '15-3', '15-4', '15-10']
1261 ***Trigger Reverse Engineering開始***
1262 Target: 15, victim: 3, Loss: 3.9901, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss: 340.05, Cost: 0.01 best_reg: 340.41 avg_loss_reg: 3224.75: 26% █ | 263/1000 [06:29 < 18:10, 1.48s/it]
1263 early stop 所有
1264 ***Trigger Reverse Engineering結束***
1265 Target Class: 15 Victim Class: 3 Trigger Size: 340.0464782714844 Optimization Steps: 83
1266 ***Symmetric Check開始***
1267 Target: 3, victim: 15, Loss: 1.3524, Acc: 100.00%, CE_Loss: 0.41, Reg_Loss: 3196.65, Cost: 0.00 best_reg: 3224.75 avg_loss_reg: 3224.75: 100% █ | 83/83 [02:02 < 00:00, 1.48s/it]
1268 ***Symmetric Check結束***
1269 檢測結果: Model是安全的(Benign)
1270 檢測結果: Model是安全的(Benign)
1271 整體耗時: 522.8435864448547
1272 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000567-----
1273 ***Pre-Screening開始
1274 ***Pre-Screening結束***
1275 可能的攻擊方式: Universal Backdoor Attack
1276 可能的 target class: 0
1277 可能的 victim classes: ALL

```

1278 \*\*\*Trigger Reverse Engineering 開始\*\*\*  
1279 Target: 0, victim: 17, Loss: 0.4422, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss:38.73, Cost:0.01 best\_reg:38.48 avg\_loss\_reg:38.97. 8% █ | 79/1000 [22:26<4:21:32, 17.04s/it]  
1280 early stop 所有

1281 \*\*\*Trigger Reverse Engineering 結束\*\*\*  
1282 Target Class: 0 Victim Class: all Trigger Size: 38.482114473978676 Optimization Steps: 80

1283 \*\*\*\*\*檢測結束\*\*\*\*\*

1284 檢測結果: Model含後門(Abnormal)  
1285 整體耗時: 1355.764173746109

1286 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000568-----

1287 \*\*\*Pre-Screening 開始\*\*\*  
1288 \*\*\*Pre-Screening 結束\*\*\*  
1289 可能的攻擊方式: Universal Backdoor Attack  
1290 可能的 target class: 1  
1291 可能的 victim classes: ALL

1292 \*\*\*Trigger Reverse Engineering 開始\*\*\*  
1293 Target: 1, victim: 3, Loss: 0.1663, Acc: 100.00%, CE\_Loss: 0.07, Reg\_Loss:1083.62, Cost:0.00 best\_reg:1082.14 avg\_loss\_reg:1065.09: 18% █ | 184/1000 [20:12<1:29:35, 6.59s/it]  
1294 early stop 所有

1295 \*\*\*Trigger Reverse Engineering 結束\*\*\*  
1296 Target Class: 1 Victim Class: all Trigger Size: 1080.9166259765625 Optimization Steps: 185

1297 \*\*\*\*\*檢測結束\*\*\*\*\*

1298 檢測結果: Model含後門(Abnormal)  
1299 整體耗時: 1220.8266117572784

1300 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000569-----

1301 \*\*\*Pre-Screening 開始\*\*\*  
1302 \*\*\*Pre-Screening 結束\*\*\*  
1303 \*\*\*檢測結束\*\*\*  
1304 檢測結果: Model是安全的(Benign)  
1305 整體耗時: 7.250255346298218

1306 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000570-----

1307 \*\*\*Pre-Screening 開始\*\*\*  
1308 \*\*\*Pre-Screening 結束\*\*\*  
1309 可能的攻擊方式: Label Specific Backdoor Attack  
1310 可能的 target-victim 配對: ['0-19', '0-21', '0-22', '1-19', '11-21', '14-5', '15-17', '19-1', '20-19', '22-21', '23-1']

1311 \*\*\*Trigger Reverse Engineering 開始\*\*\*  
1312 Target: 14, victim: 5, Loss: 3.1244, Acc: 100.00%, CE\_Loss: 0.26, Reg\_Loss:1274.44, Cost:0.00 best\_reg:1275.46 avg\_loss\_reg:1275.46: 30% █ | 302/1000 [10:18<23:49, 2.05s/it]  
1313 early stop 所有

1314 \*\*\*Trigger Reverse Engineering 結束\*\*\*  
1315 Target Class: 5 Trigger Size: 1274.4359130859375 Optimization Steps: 192

1316 \*\*\*\*\*檢測結束\*\*\*\*\*

1317 檢測結果: Model是安全的(Benign)  
1318 整體耗時: 629.776487827301

1319 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000571-----

1320 \*\*\*Pre-Screening 開始\*\*\*  
1321 \*\*\*Pre-Screening 結束\*\*\*  
1322 \*\*\*檢測結束\*\*\*  
1323 檢測結果: Model是安全的(Benign)  
1324 整體耗時: 13.191042423248291

1325 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000572-----

1326 \*\*\*Pre-Screening 開始\*\*\*  
1327 \*\*\*Pre-Screening 結束\*\*\*  
1328 可能的攻擊方式: Label Specific Backdoor Attack  
1329 可能的 target-victim 配對: ['1-10', '1-13', '2-5', '10-7', '12-0', '13-0']

1330 \*\*\*Trigger Reverse Engineering 開始\*\*\*  
1331 Target: 10, victim: 7, Loss: 2.8645, Acc: 100.00%, CE\_Loss: 0.17, Reg\_Loss:105.16, Cost:0.03 best\_reg:105.50 avg\_loss\_reg:106.69: 18% █ | 179/1000 [01:16<05:52, 2.33it/s]  
1332 early stop 所有

1333 \*\*\*Trigger Reverse Engineering 結束\*\*\*  
1334 Target Class: 7 Victim Class: 10 Trigger Size: 105.16439056396484 Optimization Steps: 114

1335 \*\*\*Symmetric Check 開始\*\*\*  
1336 Target: 7, victim: 10, Loss: 6.9945, Acc: 45.00%, CE\_Loss: 1.03, Reg\_Loss:13426.21, Cost:0.00 best\_reg:23001.96 avg\_loss\_reg:13776.85: 100% █ | 114/114 [00:48<00:00, 2.34it/s]  
1337 \*\*\*Symmetric Check 結束\*\*\*  
1338 \*\*\*\*\*檢測結束\*\*\*\*\*

1339 檢測結果: Model含後門(Abnormal)  
1340 整體耗時: 133.418167142578

1341 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000573-----

1342 \*\*\*Pre-Screening 開始\*\*\*  
1343 \*\*\*Pre-Screening 結束\*\*\*  
1344 \*\*\*檢測結束\*\*\*  
1345 檢測結果: Model是安全的(Benign)  
1346 整體耗時: 7.728898763656616

1347 \*\*\*Pre-Screening 開始\*\*\*  
1348 \*\*\*Pre-Screening 結束\*\*\*

```

1349 ***Pre-Screening結束***  

1350 可能的攻擊方式: Label Specific Backdoor Attack  

1351 可能的 target-victim 配對: ['6-1', '7-1', '10-17']  

1352 ***Trigger Reverse Engineering開始***  

1353 Target: 7, victim: 1, Loss: 1.1416, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss: 885.23, Cost:0.00 best_reg:887.64 avg_loss_reg:886.31: 62%|████| | 623/1000 [05:44<03:28, 1.81it/s]  

1354 early stop 所有  

1355 ***Trigger Reverse Engineering結束***  

1356 Target Class: 7 Victim Class: 1 Trigger Size: 885.226806640625 Optimization Steps: 404  

1357 ***Symmetric Check開始***  

1358 Target: 1, victim: 7, Loss: 2.5171, Acc: 15.00%, CE_Loss: 2.52, Reg_Loss: 5782.18, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:5757.54: 50%|████| | 200/404 [01:51<01:53, 1.80it/s]  

1359 ***Symmetric Check結束***  

1360 ***Symmetric Check開始***  

1361 檢測結果: Model含有後門(Abnormal)  

1362 整體耗時: 462.5950481891632  

1363 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000575-----  

1364 ***Pre-Screening開始***  

1365 ***Pre-Screening結束***  

1366 可能的攻擊方式: Label Specific Backdoor Attack  

1367 可能的 target-victim 配對: ['5-7']  

1368 ***Trigger Reverse Engineering開始***  

1369 Target: 5, victim: 7, Loss: 4.0861, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss: 68.50, Cost:0.06 best_reg:69.83 avg_loss_reg:69.83: 6%|████| | 62/1000 [00:10<02:33, 6.12it/s]  

1370 0%| 0/63 [00:00<?, ?it/s]early stop 所有  

1371 ***Trigger Reverse Engineering結束***  

1372 Target Class: 5 Victim Class: 7 Trigger Size: 68.50019836425781 Optimization Steps: 63  

1373 ***Symmetric Check開始***  

1374 Target: 7, victim: 5, Loss: 1.7385, Acc: 0.00%, CE_Loss: 1.74, Reg_Loss: 6983.76, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:6907.92: 100%|████| | 63/63 [00:10<00:00, 6.15it/s]  

1375 ***Symmetric Check結束***  

1376 ***Symmetric Check開始***  

1377 檢測結果: Model含有後門(Abnormal)  

1378 整體耗時: 23.665568113327026 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000576-----  

1379 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000579-----  

1380 ***Pre-Screening開始***  

1381 ***Pre-Screening結束***  

1382 可能的攻擊方式: Label Specific Backdoor Attack  

1383 可能的 target-victim 配對: ['4-1', '13-1', '15-1']  

1384 ***Trigger Reverse Engineering開始***  

1385 Target: 15, victim: 1, Loss: 0.9409, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss: 553.89, Cost:0.00 best_reg:556.13 avg_loss_reg:556.13: 26%|████| | 265/1000 [08:14<22:51, 1.87s/it]  

1386 early stop 所有  

1387 ***Trigger Reverse Engineering結束***  

1388 Target Class: 15 Victim Class: 1 Trigger Size: 553.8919677734375 Optimization Steps: 224  

1389 ***Symmetric Check開始***  

1390 Target: 1, victim: 15, Loss: 2.3771, Acc: 100.00%, CE_Loss: 0.37, Reg_Loss: 3013.40, Cost:0.00 best_reg:3006.39 avg_loss_reg:3059.09: 100%|████| | 224/224 [06:56<00:00, 1.86s/it]  

1391 ***Symmetric Check結束***  

1392 ***Symmetric Check開始***  

1393 檢測結果: Model是安全的(Benign)  

1394 整體耗時: 925.6421337127686 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000577-----  

1395 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000578-----  

1396 ***Pre-Screening開始***  

1397 ***Pre-Screening結束***  

1398 可能的攻擊方式: Universal Backdoor Attack  

1399 可能的 target class: 3  

1400 可能的 victim classes: ALL  

1401 ***Trigger Reverse Engineering開始***  

1402 Target: 3, victim: 3, Loss: 1.1826, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss: 525.45, Cost:0.00 best_reg:526.20 avg_loss_reg:526.20: 12%|████| | 1402 Target: 3, victim: 3, Loss: 1.1826, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss: 525.45, Cost:0.00 best_reg:526.20 avg_loss_reg:526.20: 12%|████| | 116/1000 [10:51<1:22:43, 5.61s/it]  

1403 early stop 所有  

1404 ***Trigger Reverse Engineering結束***  

1405 Target Class: 3 Victim Class: all Trigger Size: 524.2131958007812 Optimization Steps: 117  

1406 ***Symmetric Check開始***  

1407 檢測結果: Model含有後門(Abnormal)  

1408 整體耗時: 657.6650137901306 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000579-----  

1409 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000578-----  

1410 ***Pre-Screening開始***  

1411 ***Pre-Screening結束***  

1412 ***檢測結束***  

1413 檢測結果: Model是安全的(Benign)  

1414 整體耗時: 3.848979115325928 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000579-----  

1415 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000579-----  

1416 ***Pre-Screening開始***  

1417 ***Pre-Screening結束***  

1418 ***檢測結束***  

1419 檢測結果: Model是安全的(Benign)

```

1420 整體耗時: 2.0602707862854004

1421    \*\*\*Pre-Screening開始\*\*\*

1422    可能的攻擊方式: Label Specific Backdoor Attack

1423    可能的target-victim 配對: ['2-1', '4-2']

1424    可能的Trigger Reverse Engineering開始\*\*\*

1425    可能的 target-victim 配對: ['2-1', '4-2']

1426    可能的攻擊方式: Label Specific Backdoor Attack

1427    Target: 4, victim: 2, Loss: 11.4366, Acc: 0.00%, CE\_Loss: 11.44, Reg\_Loss:2566.08, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:2547.23: 2%| | 21/1000 [00:37&lt;29:25, 1.80s/it]

1428    \*\*\*Trigger Reverse Engineering結束\*\*\*

1429    Target Class: 2 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11

1430    \*\*\*\*\*檢測結果: Model是安全的(Benign)

1431    檢測結果: Model是安全的(Benign)

1432    整體耗時: 45.692739725112915

1433    -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000580-----

1434    \*\*\*Pre-Screening開始\*\*\*

1435    可能的攻擊方式: Label Specific Backdoor Attack

1436    可能的 target-victim 配對: ['0-22', '2-13', '3-5', '3-19', '4-11', '4-19', '4-13', '6-22', '9-5', '10-11', '10-5', '10-3', '11-12', '11-19', '12-4', '12-11', '19-11', '19-12', '23-22']

1437    可能的 target-victim 配對: ['0-22', '2-13', '3-5', '3-19', '4-11', '4-19', '4-13', '6-22', '9-5', '10-11', '10-5', '10-3', '11-12', '11-19', '12-4', '12-11', '19-11', '19-12', '23-22']

1438    \*\*\*Trigger Reverse Engineering開始\*\*\*

1439    Target: 19, victim: 12, Loss: 1.1265, Acc: 100.00%, CE\_Loss: 0.15, Reg\_Loss:433.39, Cost:0.00 best\_reg:441.04 avg\_loss\_reg:441.04: 68%| | 676/1000 [08:07&lt;03:53, 1.39it/s]

1440    early stop 所有

1441    \*\*\*Trigger Reverse Engineering結束\*\*\*

1442    Target Class: 19 Victim Class: 12 Trigger Size: 433.3880310058594 Optimization Steps: 218

1443    \*\*\*Symmetric Check開始\*\*\*

1444    Target: 12, victim: 19, Loss: 3.7701, Acc: 90.00%, CE\_Loss: 0.41, Reg\_Loss:11348.51, Cost:0.00 best\_reg:17046.46 avg\_loss\_reg:17046.46 avg\_loss\_reg:11788.08: 100%| | 218/218 [02:51&lt;00:00, 1.27it/s]

1445    \*\*\*Symmetric Check結束\*\*\*

1446    \*\*\*\*\*檢測結果: Model含有後門(Abnormal)

1447    檢測結果: Model含有後門(Abnormal)

1448    整體耗時: 670.4567940235138

1449    -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000582-----

1450    \*\*\*Pre-Screening開始\*\*\*

1451    \*\*\*Pre-Screening結束\*\*\*

1452    可能的攻擊方式: Label Specific Backdoor Attack

1453    可能的 target-victim 配對: ['0-3', '0-15', '1-9', '4-7', '4-12', '5-7', '5-12', '6-4', '6-10', '8-9', '8-4', '8-1', '10-7', '14-2']

1454    \*\*\*Trigger Reverse Engineering開始\*\*\*

1455    Target: 8, victim: 1, Loss: 3.8778, Acc: 100.00%, CE\_Loss: 0.15, Reg\_Loss:145.44, Cost:0.03 best\_reg:147.14 avg\_loss\_reg:144.11: 32%| | 317/1000 [09:29&lt;20:27, 1.80s/it]

1456    early stop 所有

1457    \*\*\*Trigger Reverse Engineering結束\*\*\*

1458    Target Class: 8 Victim Class: 1 Trigger Size: 145.4407958984375 Optimization Steps: 95

1459    \*\*\*Symmetric Check開始\*\*\*

1460    Target: 1, victim: 8, Loss: 0.6991, Acc: 70.00%, CE\_Loss: 0.70, Reg\_Loss:16981.65, Cost:0.00 best\_reg:16894.49: 100%| | 95/95 [02:47&lt;00:00, 1.76s/it]

1461    \*\*\*Symmetric Check結束\*\*\*

1462    \*\*\*\*\*檢測結果: Model含有後門(Abnormal)

1463    檢測結果: Model含有後門(Abnormal)

1464    整體耗時: 753.8526568412781

1465    -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000583-----

1466    \*\*\*Pre-Screening開始\*\*\*

1467    \*\*\*Pre-Screening結束\*\*\*

1468    可能的攻擊方式: Label Specific Backdoor Attack

1469    可能的 target-victim 配對: ['3-0']

1470    \*\*\*Trigger Reverse Engineering開始\*\*\*

1471    Target: 3, victim: 0, Loss: 6.4178, Acc: 10.00%, CE\_Loss: 6.42, Reg\_Loss:3052.59, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:2927.46: 2%| | 20/1000 [00:05&lt;04:06, 3.97it/s]

1472    \*\*\*Trigger Reverse Engineering結束\*\*\*

1473    Target Class: 3 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 21

1474    \*\*\*\*\*檢測結果: Model是安全的(Benign)

1475    檢測結果: Model是安全的(Benign)

1476    整體耗時: 10.48058295249939

1477    -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000584-----

1478    \*\*\*Pre-Screening開始\*\*\*

1479    \*\*\*Pre-Screening結束\*\*\*

1480    \*\*\*\*\*檢測結果: Universal Backdoor Attack

1481    可能的 target class: 1

1482    可能的 victim classes: ALL

1483    -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000585-----

1484    \*\*\*Pre-Screening開始\*\*\*

1485    \*\*\*Pre-Screening結束\*\*\*

1486    可能的攻擊方式: Universal Backdoor Attack

1487    可能的 target class: 1

1488    可能的 victim classes: ALL

1489    \*\*\*Trigger Reverse Engineering開始\*\*\*

1490    Target: 1, victim: 11, Loss: 8.1480, Acc: 93.75%, CE\_Loss: 0.08, Reg\_Loss:5381.90, Cost:0.00 best\_reg:5472.41 avg\_loss\_reg:5391.04: 11%| | 109/1000 [53:25&lt;7:16:43, 29.41s/it]

```

1491 early stop 所有
1492 ***Trigger Reverse Engineering結束***
1493 Target Class: 1 Victim Class: 5472.410705566406 Optimization Steps: 110
1494 ****可能的攻擊方式: Label Specific Backdoor Attack
1495 檢測結果: Model是安全的(Benign)
1496 整體耗時: 3221.573541164398
1497 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000586-----
1498 ***Pre-Screening開始***
1499 ***Pre-Screening結束***
1500 可能的攻擊方式: Label Specific Backdoor Attack
1501 可能的 target-victim 配對: ['2-16', '20-21']
1502 ***Trigger Reverse Engineering開始***
1503 Target: 20, victim: 21. Loss: 9.1024, Acc: 0.00%, CE_Loss: 9.10, Reg_Loss:2565.97, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2547.92: 2%| | 21/1000 [00:02<01:35, 10.29it/s]
1504 ***Trigger Reverse Engineering結束***
1505 Target Class: 2 Victim Class: 16 Trigger Size: 1000000000.0 Optimization Steps: 11
1506 ****可能的攻擊方式: Model是安全的(Benign)
1507 檢測結果: Model是安全的(Benign)
1508 整體耗時: 12.5337878036499023
1509 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000587-----
1510 ***Pre-Screening開始***
1511 ***Pre-Screening結束***
1512 ***檢測結束***
1513 檢測結果: Model是安全的(Benign)
1514 整體耗時: 5.3591225147247314
1515 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000588-----
1516 ***Pre-Screening開始***
1517 ***Pre-Screening結束***
1518 可能的攻擊方式: Label Specific Backdoor Attack
1519 可能的 target-victim 配對: ['2-11', '3-6', '3-13']
1520 ***Trigger Reverse Engineering開始***
1521 Target: 3, victim: 13. Loss: 6.0264, Acc: 20.00%, CE_Loss: 6.03, Reg_Loss:3227.76, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:3049.81: 5%| | 52/1000 [00:11<03:33, 4.44it/s]
1522 ***Trigger Reverse Engineering結束***
1523 Target Class: 2 Victim Class: 11 Trigger Size: 1000000000.0 Optimization Steps: 11
1524 ****可能的攻擊方式: Model是安全的(Benign)
1525 檢測結果: Model是安全的(Benign)
1526 整體耗時: 17.26356029510498
1527 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000589-----
1528 ***Pre-Screening開始***
1529 ***Pre-Screening結束***
1530 可能的攻擊方式: Label Specific Backdoor Attack
1531 可能的 target-victim 配對: ['6-1', '6-2']
1532 ***Trigger Reverse Engineering開始***
1533 Target: 6, victim: 1. Loss: 1.8757, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:105.00, Cost:0.02 best_reg:105.08 avg_loss_reg:105.08: 16%| | 162/1000 [00:18<01:35, 8.81it/s]
1534 early stop 所有
1535 ***Trigger Reverse Engineering結束***
1536 Target Class: 6 Victim Class: 1 Trigger Size: 105.00366973876953 Optimization Steps: 118
1537 ***Symmetric Check開始***
1538 Target: 1, victim: 6. Loss: 7.5190, Acc: 30.00%, CE_Loss: 0.86, Reg_Loss:6657.34, Cost:0.00 best_reg:14625.24 avg_loss_reg:7214.89: 100%| | 118/118 [00:13<00:00, 8.84it/s]
1539 ***Symmetric Check結束***
1540 ****可能的攻擊方式: Model含有後門(Abnormal)
1541 檢測結果: Model含有後門(Abnormal)
1542 整體耗時: 36.819767236709595
1543 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000590-----
1544 ***Pre-Screening開始***
1545 ***Pre-Screening結束***
1546 可能的攻擊方式: Label Specific Backdoor Attack
1547 可能的 target-victim 配對: ['1-8', '1-5', '1-0', '3-6']
1548 ***Trigger Reverse Engineering開始***
1549 Target: 3, victim: 6. Loss: 7.6629, Acc: 10.00%, CE_Loss: 7.66, Reg_Loss:4138.95, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:3696.73: 5%| | 153/1000 [00:38<11:29, 1.37it/s]
1550 ***Trigger Reverse Engineering結束***
1551 Target Class: 1 Victim Class: 8 Trigger Size: 1000000000.0 Optimization Steps: 11
1552 ****可能的攻擊方式: Model是安全的(Benign)
1553 檢測結果: Model是安全的(Benign)
1554 整體耗時: 46.060728311538696
1555 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000591-----
1556 ***Pre-Screening開始***
1557 ***Pre-Screening結束***
1558 可能的攻擊方式: Label Specific Backdoor Attack
1559 可能的 target-victim 配對: ['18-1']
1560 ***Trigger Reverse Engineering開始***
1561 Target: 18, victim: 1. Loss: 5.1753, Acc: 20.00%, CE_Loss: 5.18, Reg_Loss:2927.72, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2819.88: 2%| | 20/1000 [00:01<01:28, 11.11it/s]

```

```

1562 ***Trigger Reverse Engineering結束***
1563 Target Class: 18 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 21
1564 *****檢測結果: Model是安全的(Benign)
1565 檢測結果: Model是安全的(Benign)
1566 整體耗時: 6.83770489692688
1567 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000592-----
1568 ***Pre-Screening開始***
1569 ***Pre-Screening結束***
1570 可能的攻擊方式: Label Specific Backdoor Attack
1571 可能的 target-victim 配對: ['1-15', '2-6', '3-14', '3-16', '5-9', '6-7', '6-13', '7-13', '8-13', '9-5', '10-2', '11-2', '12-15', '13-7', '14-4', '15-1', '15-17', '16-15', '17-1']
1572 ***Trigger Reverse Engineering開始***
1573 Target: 15, victim: 1, Loss: 0.6364, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss: 1793.33, Cost: 0.00 best_Reg: 1796.31 avg_Loss_Reg: 1830.53: 100% █ | 1000/1000 [43:36<0:00:00, 2.62s/it]
1574 ***Trigger Reverse Engineering結束***
1575 Target Class: 15 Victim Class: 1 Trigger Size: 1793.328125 Optimization Steps: 637
1576 *****檢測結果: Model是安全的(Benign)
1577 檢測結果: Model是安全的(Benign)
1578 整體耗時: 2629.294574022293
1579 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000593-----
1580 ***Pre-Screening開始***
1581 ***Pre-Screening結束***
1582 可能的攻擊方式: Label Specific Backdoor Attack
1583 可能的 target-victim 配對: ['2-12', '3-2', '4-1', '5-2', '5-6', '7-12', '8-2', '9-0', '9-1', '9-6', '10-4', '10-6', '11-0', '15-1']
1584 ***Trigger Reverse Engineering開始***
1585 Target: 15, victim: 1, Loss: 8.1671, Acc: 0.00%, CE_Loss: 8.17, Reg_Loss: 2548.50, Cost: 0.00 best_Reg: 1000000000.00 avg_Loss_Reg: 2537.87: 15% █ | 153/1000 [0:0:13<0:1:16, 11.01it/s]
1586 ***Trigger Reverse Engineering結束***
1587 Target Class: 2 Victim Class: 2 Trigger Size: 1000000000.0 Optimization Steps: 11
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: 23.261059284210205
1591 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000594-----
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', '1-4', '1-6', '2-4', '4-12', '5-14', '5-16', '6-12', '8-14', '11-4', '11-12', '14-3', '14-5', '16-5']
1596 ***Trigger Reverse Engineering開始***
1597 Target: 5, victim: 14, Loss: 0.5870, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss: 2331.19, Cost: 0.00 best_Reg: 2323.82 avg_Loss_Reg: 2323.82: 100% █ | 1000/1000 [36:15<0:00:00, 2.18s/it]
1598 ***Trigger Reverse Engineering結束***
1599 Target Class: 5 Victim Class: 14 Trigger Size: 2323.8232421875 Optimization Steps: 856
1600 *****檢測結果: Model是安全的(Benign)
1601 檢測結果: Model是安全的(Benign)
1602 整體耗時: 2190.445847272873
1603 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000595-----
1604 ***Pre-Screening開始***
1605 ***Pre-Screening結束***
1606 可能的攻擊方式: Label Specific Backdoor Attack
1607 可能的 target-victim 配對: ['3-15', '10-0', '14-4', '14-15', '17-15']
1608 ***Trigger Reverse Engineering開始***
1609 Target: 14, victim: 4, Loss: 1.4724, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss: 182.89, Cost: 0.01 best_Reg: 183.46 avg_Loss_Reg: 183.46: 21% █ | 207/1000 [0:8:18<31:51, 2.41s/it]
1610 early stop 所有
1611 ***Trigger Reverse Engineering結束***
1612 Target Class: 14 Victim Class: 4 Trigger Size: 182.8880615234375 Optimization Steps: 133
1613 ***Symmetric Check開始***
1614 Target: 4, victim: 14, Loss: 0.5284, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss: 3916.53, Cost: 0.00 best_Reg: 12222.59 avg_Loss_Reg: 3888.32: 100% █ | 133/133 [05:21<0:00:00, 2.42s/it]
1615 ***Symmetric Check結束***
1616 *****檢測結果: Model含有後門(Abnormal)
1617 檢測結果: Model是安全的(Benign)
1618 整體耗時: 833.0767560005188
1619 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000596-----
1620 ***Pre-Screening開始***
1621 ***Pre-Screening結束***
1622 ***檢測結果: Model是安全的(Benign)
1623 檢測結果: Model是安全的(Benign)
1624 整體耗時: 12.070361614227295
1625 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000597-----
1626 ***Pre-Screening開始***
1627 ***Pre-Screening結束***
1628 ***檢測結果: Model是安全的(Benign)
1629 檢測結果: Model是安全的(Benign)
1630 整體耗時: 10.730490922927856
1631 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000598-----
1632 ***Pre-Screening開始***

```

```

1633 ***Pre-Screening結束***  

1634 ***檢測結束***  

1635 檢測結果: Model是安全的(Benign)  

1636 整體耗時: 11.590410947799683  

1637 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000599  

1638 ***Pre-Screening開始***  

1639 ***Pre-Screening結束***  

1640 可能的攻擊方式: Label Specific Backdoor Attack  

1641 可能的 target-victim 配對: ['10-13']  

1642 ***Trigger Reverse Engineering開始***  

1643 Target: 10, victim: 13, Loss: 2.7095, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:233.05, Cost:0.01 best_reg:233.12 avg_loss_reg:233.58: 9% █ | 93/1000 [06:11<1:00:19, 3.99s/it]  

1644 early stop 所有  

1645 ***Trigger Reverse Engineering結束***  

1646 Target Class: 10 Victim Class: 13 Trigger Size: 233.04537963867188 Optimization Steps: 94  

1647 ***Symmetric Check開始***  

1648 Target: 13, victim: 10, Loss: 5.1421, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:11221.29, Cost:0.00 best_reg:11387.69 avg_loss_reg:11387.69: 100% █ | 94/94 [06:11<0:00:00, 3.95s/it]  

1649 ***Symmetric Check結束***  

1650 *****檢測結束*****  

1651 檢測結果: Model有後門(Abnormal)  

1652 整體耗時: 761.268774167786  

1653 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000600  

1654 ***Pre-Screening開始***  

1655 ***Pre-Screening結束***  

1656 ***檢測結束***  

1657 檢測結果: Model是安全的(Benign)  

1658 整體耗時: 23.153509616851807  

1659 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000601  

1660 ***Pre-Screening開始***  

1661 ***Pre-Screening結束***  

1662 ***檢測結束***  

1663 檢測結果: Model是安全的(Benign)  

1664 整體耗時: 10.348154067993164  

1665 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000602  

1666 ***Pre-Screening開始***  

1667 可能的攻擊方式: Label Specific Backdoor Attack  

1668 可能的 target-victim 配對: ['7-9']  

1669 ***Trigger Reverse Engineering開始***  

1670 Target: 7, victim: 9, Loss: 1.8292, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:221.81 avg_loss_reg:222.50: 14% █ | 137/1000 [02:36<16:23, 1.14s/it]  

1671 Target: 7, victim: 9, Loss: 220.4362030029297 Optimization Steps: 138  

1672 early stop 所有  

1673 ***Trigger Reverse Engineering結束***  

1674 Target Class: 7 Victim Class: 9 Trigger Size: 220.4362030029297 Optimization Steps: 138  

1675 ***Symmetric Check開始***  

1676 Target: 9, victim: 7, Loss: 1.7706, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:7196.47, Cost:0.00 best_reg:7225.23 avg_loss_reg:7225.23: 100% █ | 138/138 [02:35<0:00:00, 1.13s/it]  

1677 ***Symmetric Check結束***  

1678 *****檢測結束*****  

1679 檢測結果: Model有後門(Abnormal)  

1680 整體耗時: 321.98487973213196  

1681 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000603  

1682 ***Pre-Screening開始***  

1683 ***Pre-Screening結束***  

1684 ***檢測結束***  

1685 檢測結果: Model是安全的(Benign)  

1686 整體耗時: 5.742900848388672  

1687 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000604  

1688 ***Pre-Screening開始***  

1689 ***Pre-Screening結束***  

1690 ***檢測結束***  

1691 檢測結果: Model是安全的(Benign)  

1692 整體耗時: 1.9415292739868164  

1693 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000605  

1694 ***Pre-Screening開始***  

1695 ***Pre-Screening結束***  

1696 可能的攻擊方式: Universal Backdoor Attack  

1697 可能的 target class: 10  

1698 可能的 victim classes: ALL  

1699 ***Trigger Reverse Engineering開始***  

1700 Target: 10, victim: 12, Loss: 1.1488, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:222.86, Cost:0.01 best_reg:217.52 avg_loss_reg:218.45: 11% █ | 106/1000 [02:47<23:35, 1.58s/it]  

1701 early stop 所有  

1702 ***Trigger Reverse Engineering結束***  

1703 Target Class: 10 Victim Class: all Trigger Size: 217.5201782226626 Optimization Steps: 107

```

```
1704 *****檢測結束*****  
1705 檢測結果: Model含有後門(Abnormal)  
1706 整體耗時: 172.85949182510376  
1707 *****Pre-Screening開始*****  
1708 *****Pre-Screening結束***  
1709 *****Pre-Screening結束***  
1710 *****檢測結束***  
1711 檢測結果: Model是安全的(Benign)  
1712 整體耗時: 28.435882329940796  
1713 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000607*****  
1714 ***Pre-Screening開始***  
1715 ***Pre-Screening結束***  
1716 ***檢測結束***  
1717 檢測結果: Model是安全的(Benign)  
1718 整體耗時: 19.791624184469604  
1719 *****Pre-Screening開始*****  
1720 *****Pre-Screening結束***  
1721 *****Pre-Screening結束***  
1722 *****檢測結束***  
1723 檢測結果: Model是安全的(Benign)  
1724 整體耗時: 8.467063188552856  
1725 *****Pre-Screening開始*****  
1726 *****Pre-Screening結束***  
1727 *****Pre-Screening結束***  
1728 可能的攻擊方式: Label Specific Backdoor Attack  
1729 可能的target-victim 配對: ['3-8', '11-3']  
1730 ***Trigger Reverse Engineering開始***  
1731 Target: 11, victim: 3, Loss: 8.5467, Acc: 0.00%, CE_Loss: 8.55, Reg_Loss:2531.10, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2523.77: 2%| | 21/1000 [00:01<01:30, 10.87it/s]  
1732 ***Trigger Reverse Engineering結束***  
1733 Target Class: 3 Victim Class: 8 Trigger Size: 1000000000.0 Optimization Steps: 11  
1734 *****檢測結束*****  
1735 檢測結果: Model是安全的(Benign)  
1736 整體耗時: 6.82317042350769  
1737 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000610*****  
1738 *****Pre-Screening開始***  
1739 *****Pre-Screening結束***  
1740 *****檢測結束***  
1741 檢測結果: Model是安全的(Benign)  
1742 整體耗時: 14.730799913406372  
1743 *****Pre-Screening結束*****  
1744 ***Pre-Screening開始***  
1745 ***Pre-Screening結束***  
1746 ***檢測結束***  
1747 檢測結果: Model是安全的(Benign)  
1748 整體耗時: 3.3323225498199463  
1749 *****Pre-Screening開始***  
1750 *****Pre-Screening結束***  
1751 *****Pre-Screening結束***  
1752 可能的攻擊方式: Label Specific Backdoor Attack  
1753 可能的target-victim 配對: ['1-6', '1-19', '2-5', '10-7', '15-5', '18-6', '19-18']  
1754 ***Trigger Reverse Engineering開始***  
1755 Target: 19, victim: 18, Loss: 5.6812, Acc: 0.00%, CE_Loss: 5.68, Reg_Loss:2556.37, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2541.53: 9%| | 86/1000 [03:09<33:38, 2.21s/it]  
1756 ***Trigger Reverse Engineering結束***  
1757 Target Class: 1 Victim Class: 6 Trigger Size: 1000000000.0 Optimization Steps: 11  
1758 *****檢測結束*****  
1759 檢測結果: Model是安全的(Benign)  
1760 整體耗時: 209.46600341796875  
1761 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000613*****  
1762 *****Pre-Screening開始***  
1763 *****Pre-Screening結束***  
1764 可能的攻擊方式: Label Specific Backdoor Attack  
1765 可能的target-victim 配對: ['4-0']  
1766 ***Trigger Reverse Engineering開始***  
1767 Target: 4, victim: 0, Loss: 6.8558, Acc: 0.00%, CE_Loss: 6.86, Reg_Loss:2547.51, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2533.54: 1%| | 10/1000 [00:08<13:23, 1.23it/s]  
1768 ***Trigger Reverse Engineering結束***  
1769 Target Class: 4 Victim Class: 0 Trigger Size: 1000000000 Optimization Steps: 11  
1770 *****檢測結束*****  
1771 檢測結果: Model是安全的(Benign)  
1772 整體耗時: 16.902014017105103  
1773 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000614*****  
1774 ***Pre-Screening開始***
```

1775 \*\*\*Pre-Screening結束\*\*\*  
1776 \*\*\*檢測結束\*\*\*  
1777 檢測結果: Model是安全的(Benign)  
1778 整體耗時: 4.804539203643799  
1779 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000615-----  
1780 \*\*\*Pre-Screening開始\*\*\*  
1781 \*\*\*Pre-Screening結束\*\*\*  
1782 可能的攻擊方式: Universal Backdoor Attack  
1783 可能的 target class: 0  
1784 可能的 victim classes: ALL  
1785 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1786 Target: 0, victim: 12, Loss: 1.0222, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss: 2299.88, Cost: 0.00 best\_reg: 2290.21 avg\_loss\_reg: 2331.96: 11% █ | 108/1000 [29:20 <4:02:21, 16.30s/it]  
1787 early stop 所有  
1788 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1789 Target Class: 0 Victim Class: all Trigger Size: 2290.21376953125 Optimization Steps: 109  
1790 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000616-----  
1791 檢測結果: Model是安全的(Benign)  
1792 整體耗時: 1773.8662333488464  
1793 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000616-----  
1794 \*\*\*Pre-Screening開始\*\*\*  
1795 \*\*\*Pre-Screening結束\*\*\*  
1796 可能的攻擊方式: Label Specific Backdoor Attack  
1797 可能的 target-victim 配對: [2, 10, '3, 10']  
1798 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1799 Target: 3, victim: 10, Loss: 13.3420, Acc: 0.00%, CE\_Loss: 13.34, Reg\_Loss: 2525.62, Cost: 0.00 best\_reg: 10000000000.00 avg\_loss\_reg: 2518.22: 2% | | 21/1000 [00:01 <01:25, 11.40s/it]  
1800 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1801 Target Class: 2 Victim Class: 10 Trigger Size: 1000000000.0 Optimization Steps: 11  
1802 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000616-----  
1803 檢測結果: Model是安全的(Benign)  
1804 整體耗時: 6.882972478866577  
1805 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000617-----  
1806 \*\*\*Pre-Screening開始\*\*\*  
1807 \*\*\*Pre-Screening結束\*\*\*  
1808 可能的攻擊方式: Label Specific Backdoor Attack  
1809 可能的 target-victim 配對: [0-6, '7-0, '11-6']  
1810 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1811 Target: 11, victim: 6, Loss: 3.9676, Acc: 0.00%, CE\_Loss: 3.97, Reg\_Loss: 2593.75, Cost: 0.00 best\_reg: 10000000000.00 avg\_loss\_reg: 2571.87: 3% | | 32/1000 [00:55 <27:53, 1.73s/it]  
1812 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1813 Target Class: 0 Victim Class: 6 Trigger Size: 10000000000.0 Optimization Steps: 11  
1814 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000618-----  
1815 檢測結果: Model是安全的(Benign)  
1816 整體耗時: 68.95675468444824  
1817 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000618-----  
1818 \*\*\*Pre-Screening開始\*\*\*  
1819 \*\*\*Pre-Screening結束\*\*\*  
1820 \*\*\*檢測結束\*\*\*  
1821 檢測結果: Model是安全的(Benign)  
1822 整體耗時: 5.971666574478149  
1823 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000619-----  
1824 \*\*\*Pre-Screening開始\*\*\*  
1825 \*\*\*Pre-Screening結束\*\*\*  
1826 \*\*\*檢測結束\*\*\*  
1827 檢測結果: Model是安全的(Benign)  
1828 整體耗時: 9.411704301834106  
1829 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000620-----  
1830 \*\*\*Pre-Screening開始\*\*\*  
1831 \*\*\*Pre-Screening結束\*\*\*  
1832 可能的攻擊方式: Label Specific Backdoor Attack  
1833 可能的 target-victim 配對: [8-0]  
1834 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1835 Target: 8, victim: 0, Loss: 3.0129, Acc: 100.00%, CE\_Loss: 0.24, Reg\_Loss: 365.14, Cost: 0.01 best\_reg: 370.49 avg\_loss\_reg: 362.58: 14% █ | | 145/1000 [03:06 <18:17, 1.28s/it]  
1836 early stop 所有  
1837 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1838 Target Class: 8 Victim Class: 0 Trigger Size: 365.1361083984375 Optimization Steps: 146  
1839 \*\*\*Symmetric Check開始\*\*\*  
1840 Target: 0, victim: 8, Loss: 1.6848, Acc: 100.00%, CE\_Loss: 0.28, Reg\_Loss: 1400.89, Cost: 0.00 best\_reg: 1367.34 avg\_loss\_reg: 1394.87: 100% █ | | 146/146 [03:06 <00:00, 1.28s/it]  
1841 \*\*\*Symmetric Check結束\*\*\*  
1842 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000621-----  
1843 檢測結果: Model是安全的(Benign)  
1844 整體耗時: 383.116474151613  
1845 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000621-----

```

1846 ***Pre-Screening開始***  

1847 ***Pre-Screening結束***  

1848 可能的攻擊方式: Universal Backdoor Attack  

1849 可能的 target class: 0  

1850 可能的 victim classes: ALL  

1851 ***Trigger Reverse Engineering開始***  

1852 Target: 0, victim: 9, Loss: 0.3661, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:505.61, Cost:0.00 best_reg:505.39 avg_loss_reg:501.41: 8% █ | 79/1000 [03:39<42:36, 2.78s/it]  

1853 early stop 所有  

1854 ***Trigger Reverse Engineering結束***  

1855 Target Class: 0 Victim Class: all Trigger Size: 505.3899884905134 Optimization Steps: 80  

1856 *****檢測結束*****  

1857 檢測結果: Model含有後門(Abnormal)  

1858 整體耗時: 225.0068655014038  

1859 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000622-----  

1860 ***Pre-Screening開始***  

1861 ***Pre-Screening結束***  

1862 ***檢測結束***  

1863 檢測結果: Model是安全的(Benign)  

1864 整體耗時: 8.5148446559906  

1865 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000623-----  

1866 ***Pre-Screening開始***  

1867 ***Pre-Screening結束***  

1868 ***檢測結束***  

1869 檢測結果: Model是安全的(Benign)  

1870 整體耗時: 5.803854703903198  

1871 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000624-----  

1872 ***Pre-Screening開始***  

1873 ***Pre-Screening結束***  

1874 ***檢測結束***  

1875 檢測結果: Model是安全的(Benign)  

1876 整體耗時: 13.249783992767334  

1877 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000625-----  

1878 ***Pre-Screening開始***  

1879 ***Pre-Screening結束***  

1880 ***檢測結束***  

1881 檢測結果: Model是安全的(Benign)  

1882 整體耗時: 5.3142478466033936  

1883 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000626-----  

1884 ***Pre-Screening開始***  

1885 ***Pre-Screening結束***  

1886 ***檢測結束***  

1887 檢測結果: Model是安全的(Benign)  

1888 整體耗時: 7.930661678314209  

1889 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000627-----  

1890 ***Pre-Screening開始***  

1891 ***Pre-Screening結束***  

1892 可能的攻擊方式: Label Specific Backdoor Attack  

1893 可能的 target-victim 配對: ['15-0']  

1894 ***Trigger Reverse Engineering開始***  

1895 Target: 15, victim: 0, Loss: 14.0721, Acc: 0.00%, CE_Loss: 14.07, Reg_Loss:2546.60, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2536.25: 1% | 10/1000 [00:28<46:50, 2.84s/it]  

1896 ***Trigger Reverse Engineering結束***  

1897 Target Class: 15 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 11  

1898 ***檢測結束***  

1899 檢測結果: Model是安全的(Benign)  

1900 整體耗時: 51.637799978256226  

1901 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000628-----  

1902 ***Pre-Screening開始***  

1903 ***Pre-Screening結束***  

1904 可能的攻擊方式: Label Specific Backdoor Attack  

1905 可能的 target-victim 配對: ['14-2']  

1906 ***Trigger Reverse Engineering開始***  

1907 Target: 14, victim: 2, Loss: 3.3185, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:54.92, Cost:0.06 best_reg:63.08 avg_loss_reg:54.68: 11% █ | 106/1000 [00:08<01:14, 11.98s/it]  

1908 early stop 所有  

1909 ***Trigger Reverse Engineering結束***  

1910 Target Class: 14 Victim Class: 2 Trigger Size: 54.91869354248047 Optimization Steps: 107  

1911 ***Symmetric Check開始***  

1912 Target: 2, victim: 14, Loss: 6.0680, Acc: 90.00%, CE_Loss: 0.33, Reg_Loss:335.71, Cost:0.02 best_reg:362.55 avg_loss_reg:348.53: 100% █ | 107/107 [00:08<00:00, 12.03s/it]  

1913 ***Symmetric Check結束***  

1914 ***檢測結束***  

1915 檢測結果: Model是安全的(Benign)  

1916 整體耗時: 22.747052669525146

```

File - main -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000629-----

1917     \*\*\*Pre-Screening開始\*\*\*  
 1918     \*\*\*Pre-Screening結束\*\*\*  
 1919     \*\*\*Pre-Screening結束\*\*\*  
 1920     \*\*\*檢測結果: Model是安全的(Benign)  
 1921     整體耗時: 7.465019226074219  
 1922     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000630-----  
 1923     \*\*\*檢測結果: Model是安全的(Benign)  
 1924     整體耗時: 17.69011359161377  
 1925     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000631-----  
 1926     \*\*\*檢測結果: Model是安全的(Benign)  
 1927     整體耗時: 17.69011359161377  
 1928     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000632-----  
 1929     \*\*\*Pre-Screening開始\*\*\*  
 1930     \*\*\*Pre-Screening結束\*\*\*  
 1931     \*\*\*Pre-Screening結束\*\*\*  
 1932     \*\*\*檢測結果: Model是安全的(Benign)  
 1933     整體耗時: 8.609151601791382  
 1934     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000633-----  
 1935     \*\*\*Pre-Screening開始\*\*\*  
 1936     \*\*\*Pre-Screening結束\*\*\*  
 1937     \*\*\*Pre-Screening開始\*\*\*  
 1938     \*\*\*檢測結果: Model是安全的(Benign)  
 1939     整體耗時: 5.30630087852478  
 1940     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000634-----  
 1941     \*\*\*Pre-Screening開始\*\*\*  
 1942     \*\*\*Pre-Screening結束\*\*\*  
 1943     可能的攻擊方式: Universal Backdoor Attack  
 1944     可能的 target class: 2  
 1945     可能的 victim classes: ALL  
 1946     -----檢測結果: Model含有後門(Abnormal)  
 1947     \*\*\*Trigger Reverse Engineering開始\*\*\*  
 1948     Target: 2, victim: 4, Loss: 0.3813, Acc: 100.00%, CE\_Loss: 0.04, Reg\_Loss:20.07, Cost:0.02 best\_reg:21.51 avg\_loss\_reg:19.74: 6% █ | 58/1000 [01:35<25:53, 1.65s/it]  
 1949     early stop 所有  
 1950     \*\*\*Trigger Reverse Engineering結束\*\*\*  
 1951     Target Class: all Target Size: 21.50739049911499 Optimization Steps: 59  
 1952     -----檢測結果: Model含有後門(Abnormal)  
 1953     整體耗時: 100.25975275039673  
 1954     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000635-----  
 1955     \*\*\*Pre-Screening開始\*\*\*  
 1956     \*\*\*Pre-Screening結束\*\*\*  
 1957     -----檢測結果: Model是安全的(Benign)  
 1958     可能的攻擊方式: Label Specific Backdoor Attack  
 1959     可能的 target-victim 配對: [0-21', '1-0', '1-9', '1-20', '2-13', '2-17', '3-10', '3-13', '4-13', '4-18', '6-4', '6-5', '6-14', '8-19', '10-3', '10-18', '10-20', '11-12', '11-18', '12-18', '13-4', '13-18', '14-17', '15-17', '16-3', '16-14', '16-21', '17-10', '17-14', '17-17', '17-18', '13-19', '21-22', '22-1', '22-9', '22-21']  
 1960     \*\*\*Trigger Reverse Engineering開始\*\*\*  
 1961     Target: 22, victim: 21, Loss: 2.5122, Acc: 100.00%, CE\_Loss: 0.33, Reg\_Loss:971.88, Cost:0.00 best\_reg:983.72 avg\_loss\_reg:983.72: 84% █ | 841/1000 [32:16<06:06, 2.30s/it]  
 1962     early stop 所有  
 1963     \*\*\*Trigger Reverse Engineering結束\*\*\*  
 1964     Target Class: 22 Victim Class: 21 Trigger Size: 971.88031005855938 Optimization Steps: 192  
 1965     \*\*\*Symmetric Check開始\*\*\*  
 1966     Target: 21, victim: 22, Loss: 1.0115, Acc: 95.00%, CE\_Loss: 0.21, Reg\_Loss:537.31, Cost:0.00 best\_reg:556.47 avg\_loss\_reg:538.50: 100% █ | 192/192 [07:04<00:00, 2.21s/it]  
 1967     \*\*\*Symmetric Check結束\*\*\*  
 1968     -----檢測結果: Model是安全的(Benign)  
 1969     整體耗時: 2380.1892080307007  
 1970     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000636-----  
 1971     \*\*\*Pre-Screening開始\*\*\*  
 1972     \*\*\*Pre-Screening結束\*\*\*  
 1973     -----檢測結果: Model是安全的(Benign)  
 1974     可能的攻擊方式: Label Specific Backdoor Attack  
 1975     可能的 target-victim 配對: [1-3', '2-2', '8-2', '8-3', '18-4', '19-3', '22-3']  
 1976     \*\*\*Trigger Reverse Engineering開始\*\*\*  
 1977     Target: 8, victim: 2, Loss: 1.3425, Acc: 100.00%, CE\_Loss: 0.08, Reg\_Loss:49.22, Cost:0.03 best\_reg:49.67 avg\_loss\_reg:49.27: 15% █ | 154/1000 [08:51<48:39, 3.45s/it]  
 1978     early stop 所有  
 1979     \*\*\*Trigger Reverse Engineering結束\*\*\*  
 1980     Target Class: 8 Victim Class: 2 Trigger Size: 49.220436096191406 Optimization Steps: 87  
 1981     \*\*\*Symmetric Check開始\*\*\*  
 1982     Target: 2, victim: 8, Loss: 2.2699, Acc: 35.00%, CE\_Loss: 2.27, Reg\_Loss:23774.01, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:23644.20: 100% █ | 87/87 [04:58<00:00, 3.43s/it]  
 1983     \*\*\*Symmetric Check結束\*\*\*  
 1984     -----檢測結果: Model含有後門(Abnormal)  
 1985     整體耗時: 859.0679321289062

1987 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000637-----  
 1988 \*\*\*Pre-Screening開始\*\*\*  
 1989 \*\*\*Pre-Screening結束\*\*\*  
 1990 \*\*\*檢測結束\*\*\*  
 1991 檢測結果: Model是安全的(Benign)  
 1992 整體耗時: 5.470768590109253  
 1993 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000637-----  
 1994 \*\*\*Pre-Screening開始\*\*\*  
 1995 \*\*\*Pre-Screening結束\*\*\*  
 1996 \*\*\*檢測結束\*\*\*  
 1997 檢測結果: Model是安全的(Benign)  
 1998 整體耗時: 19.734752416610718  
 1999 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000638-----  
 2000 \*\*\*Pre-Screening開始\*\*\*  
 2001 \*\*\*Pre-Screening結束\*\*\*  
 2002 可能的攻擊方式: Label Specific Backdoor Attack  
 2003 可能的 target-victim 配對: ['11-12']  
 2004 \*\*\*Trigger Reverse Engineering開始\*\*\*  
 2005 Target: 11, victim: 12, Loss: 7.0287, Acc: 0.00%, CE\_Loss: 7.03, Reg\_Loss:2536.67, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:2526.50: 1% | 10/1000 [00:30<50:45, 3.08s/it]  
 2006 \*\*\*Trigger Reverse Engineering結束\*\*\*  
 2007 Target Class: 11 Victim Class: 12 Trigger Size: 1000000000.0 Optimization Steps: 11  
 2008 \*\*\*檢測結束\*\*\*  
 2009 檢測結果: Model是安全的(Benign)  
 2010 整體耗時: 45.817421197891235  
 2011 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000639-----  
 2012 \*\*\*Pre-Screening開始\*\*\*  
 2013 \*\*\*Pre-Screening結束\*\*\*  
 2014 可能的攻擊方式: Universal Backdoor Attack  
 2015 可能的 target class: 3  
 2016 可能的 victim classes: ALL  
 2017 \*\*\*Trigger Reverse Engineering開始\*\*\*  
 2018 Target: 3, victim: 22, Loss: 0.1504, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss:761.22, Cost:0.00 best\_reg:803.79 avg\_loss\_reg:755.62: 6% | 60/1000 [1:09:24<18:07:24, 69.41s/it]  
 2019 early stop 所有  
 2020 \*\*\*Trigger Reverse Engineering結束\*\*\*  
 2021 Target Class: 3 Victim Class: all Trigger Size: 803.7866048177083 Optimization Steps: 61  
 2022 \*\*\*檢測結束\*\*\*  
 2023 檢測結果: Model含有後門(Abnormal)  
 2024 整體耗時: 4183.792681932449  
 2025 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000640-----  
 2026 \*\*\*Pre-Screening開始\*\*\*  
 2027 \*\*\*Pre-Screening結束\*\*\*  
 2028 \*\*\*檢測結束\*\*\*  
 2029 檢測結果: Model是安全的(Benign)  
 2030 整體耗時: 8.523850917816162  
 2031 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000641-----  
 2032 \*\*\*Pre-Screening開始\*\*\*  
 2033 \*\*\*Pre-Screening結束\*\*\*  
 2034 \*\*\*檢測結束\*\*\*  
 2035 檢測結果: Model是安全的(Benign)  
 2036 整體耗時: 8.645679712295532  
 2037 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000642-----  
 2038 \*\*\*Pre-Screening開始\*\*\*  
 2039 \*\*\*Pre-Screening結束\*\*\*  
 2040 \*\*\*檢測結束\*\*\*  
 2041 檢測結果: Model是安全的(Benign)  
 2042 整體耗時: 5.1350061893463135  
 2043 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000643-----  
 2044 \*\*\*Pre-Screening開始\*\*\*  
 2045 \*\*\*Pre-Screening結束\*\*\*  
 2046 可能的攻擊方式: Label Specific Backdoor Attack  
 2047 可能的 target-victim 配對: ['4-1', '4-11']  
 2048 \*\*\*Trigger Reverse Engineering開始\*\*\*  
 2049 Target: 4, victim: 11, Loss: 3.8687, Acc: 100.00%, CE\_Loss: 0.13, Reg\_Loss:97.13, Cost:0.04 best\_reg:98.29 avg\_loss\_reg:98.29: 13% | 129/1000 [00:11<01:16, 11.38it/s]  
 2050 early stop 所有  
 2051 \*\*\*Trigger Reverse Engineering結束\*\*\*  
 2052 Target Class: 4 Victim Class: 11 Trigger Size: 97.13165283203125 Optimization Steps: 90  
 2053 \*\*\*Symmetric Check開始\*\*\*  
 2054 Target: 11, victim: 4, Loss: 4.7368, Acc: 90.00%, CE\_Loss: 0.53, Reg\_Loss:1871.25, Cost:0.00 best\_reg:2087.29 avg\_loss\_reg:1909.97: 100% | 90/90 [00:07<00:00, 11.55it/s]  
 2055 \*\*\*Symmetric Check結束\*\*\*  
 2056 \*\*\*檢測結束\*\*\*  
 2057 檢測結果: Model含有後門(Abnormal)

```

2058 整體耗時: 23.7772928714752197 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000644-----
2059
2060 ***Pre-Screening開始****
2061 可能的攻擊方式: Label Specific Backdoor Attack
2062 可能的target-victim 配對: [0-1', '5-13', '18-1', '19-1']
2063
2064 ***Trigger Reverse Engineering開始****
2065 Target: 19, victim: 1, Loss: 11.0630, Acc: 0.00%, CE_Loss: 11.06, Reg_Loss:2538.95, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2530.16: 5%| | 53/1000 [01:30<26:49, 1.70s/it]
2066 ***Trigger Reverse Engineering結束****
2067 Target Class: 0 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 21
2068 ****檢測結果: Model是安全的(Benign)
2069 檢測結果: Model是安全的(Benign)
2070 整體耗時: 106.82014775276184 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000645-----
2071
2072 ***Pre-Screening開始****
2073 ***Pre-Screening結束****
2074 可能的攻擊方式: Label Specific Backdoor Attack
2075 可能的target-victim 配對: [8-1']
2076 ***Trigger Reverse Engineering開始****
2077 Target: 8, victim: 1, Loss: 7.1400, Acc: 0.00%, CE_Loss: 7.14, Reg_Loss:2558.43, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2546.68: 1%| | 10/1000 [00:07<11:34, 1.43it/s]
2078 ***Trigger Reverse Engineering結束****
2079 Target Class: 8 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11
2080 ****檢測結果: Model是安全的(Benign)
2081 檢測結果: Model是安全的(Benign)
2082 整體耗時: 14.01607561114502 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000646-----
2083
2084 ***Pre-Screening開始****
2085 ***Pre-Screening結束****
2086 可能的攻擊方式: Label Specific Backdoor Attack
2087 可能的target-victim 配對: [0-6', '0-15', '2-10', '3-5', '4-8', '5-10', '5-3', '6-0', '6-12', '6-13', '7-8', '8-5', '8-3', '8-14', '10-2', '10-4', '10-5', '11-1', '13-12', '15-14', '15-1', '15-11']
2088 ***Trigger Reverse Engineering開始****
2089 Target: 8, victim: 3, Loss: 3.6248, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:94.26, Cost:0.04 best_reg:95.69 avg_loss_reg:95.69: 37%| | 370/1000 [08:23<14:17, 1.36s/it]
2090 early stop 所有
2091 ***Trigger Reverse Engineering結束****
2092 Target Class: 8 Victim Class: 3 Trigger Size: 94.2336489868164 Optimization Steps: 72
2093 ***Symmetric Check開始****
2094 Target: 3, victim: 8, Loss: 1.0692, Acc: 70.00%, CE_Loss: 1.07, Reg_Loss:12001.84, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:11945.58: 100%| | 72/72 [01:30<00:00, 1.26s/it]
2095 ***Symmetric Check結束****
2096 ****檢測結果: Model含有後門(ABnormal)
2097 檢測結果: Model是安全的(Benign)
2098 整體耗時: 605.6252410411835 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000647-----
2099
2100 ***Pre-Screening開始****
2101 ***Pre-Screening結束****
2102 可能的攻擊方式: Label Specific Backdoor Attack
2103 可能的target-victim 配對: [1-13', '2-14', '3-13', '9-1', '9-14', '11-5', '12-5', '12-16', '15-6', '17-16']
2104 ***Trigger Reverse Engineering開始****
2105 Target: 9, victim: 1, Loss: 1.3749, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:1281.17, Cost:0.00 best_reg:1281.72 avg_loss_reg:1281.72: 35%| | 352/1000 [21:29<39:33, 3.66s/it]
2106 early stop 所有
2107 ***Trigger Reverse Engineering結束****
2108 Target Class: 9 Victim Class: 1 Trigger Size: 1281.17138671875 Optimization Steps: 176
2109 ****檢測結果: Model是安全的(Benign)
2110 檢測結果: Model是安全的(Benign)
2111 整體耗時: 1314.2148549556732 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000648-----
2112
2113 ***Pre-Screening開始****
2114 ***Pre-Screening結束****
2115 ***檢測結果: Model是安全的(Benign)
2116 檢測結果: Model是安全的(Benign)
2117 整體耗時: 20.29254722595215 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000649-----
2118
2119 ***Pre-Screening開始****
2120 ***Pre-Screening結束****
2121 ***檢測結果: Model是安全的(Benign)
2122 檢測結果: Model是安全的(Benign)
2123 整體耗時: 12.354369401931763 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000650-----
2124
2125 ***Pre-Screening開始****
2126 ***Pre-Screening結束****
2127 可能的攻擊方式: Label Specific Backdoor Attack
2128 可能的target-victim 配對: [5-11', '8-11', '10-11']

```

```
2129 ***Trigger Reverse Engineering開始***  
2130 Target: 10, victim: 11, Loss: 7.4590, Acc: 0.00%, CE_Loss: 7.46, Reg_Loss:2497.12, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2497.88: 3% | 32/1000 [00:18<09:17, 1.74it/s]  
2131 ***Trigger Reverse Engineering結束***  
2132 Target Class: 5 Victim Class: 11 Trigger Size: 1000000000.0 Optimization Steps: 11  
2133 *****檢測結束*****  
2134 檢測結果: Model是安全的(Benign)  
2135 整體耗時: 27.135023832321167  
2136 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000651-----  
2137 ***Pre-Screening開始***  
2138 ***Pre-Screening結束***  
2139 可能的攻擊方式: Universal Backdoor Attack  
2140 可能的 target class: 2  
2141 可能的 victim classes: ALL  
2142 ***Trigger Reverse Engineering開始***  
2143 Target: 2, victim: 22, Loss: 2.8162, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:4224.23, Cost:0.00 best_reg:4220.36 avg_loss_reg:4223.00: 20% | 203/1000 [2:03:18<8:04:05, 36.44s/it]  
2144 early stop 所有  
2145 ***Trigger Reverse Engineering結束***  
2146 Target Class: 2 Victim Class: all Trigger Size: 4220.36181640625 Optimization Steps: 204  
2147 *****檢測結束*****  
2148 檢測結果: Model是安全的(Benign)  
2149 整體耗時: 7416.994409561157  
2150 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000652-----  
2151 ***Pre-Screening開始***  
2152 ***Pre-Screening結束***  
2153 可能的攻擊方式: Label Specific Backdoor Attack  
2154 可能的 target-victim 配對: ['3-8', '3-10']  
2155 ***Trigger Reverse Engineering開始***  
2156 Target: 3, victim: 10, Loss: 3.1053, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:118.10, Cost:0.03 best_reg:119.13 avg_loss_reg:112.37: 13% | 128/1000 [04:38<31:36, 2.18s/it]  
2157 early stop 所有  
2158 ***Trigger Reverse Engineering結束***  
2159 Target Class: 3 Victim Class: 10 Trigger Size: 118.10035705566406 Optimization Steps: 91  
2160 ***Symmetric Check開始***  
2161 Target: 10, victim: 3, Loss: 1.0420, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:4297.76, Cost:0.00 best_reg:4374.31 avg_loss_reg:4374.31: 100% | 91/91 [03:16<00:00, 2.16s/it]  
2162 ***Symmetric Check結束***  
2163 *****檢測結束*****  
2164 檢測結果: Model含有後門(Abnormal)  
2165 整體耗時: 483.4890127182007  
2166 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000653-----  
2167 ***Pre-Screening開始***  
2168 ***Pre-Screening結束***  
2169 可能的攻擊方式: Label Specific Backdoor Attack  
2170 可能的 target-victim 配對: ['2-1', '2-3', '3-2', '3-4', '3-8', '6-10', '6-7', '6-5', '7-5', '7-6', '8-2']  
2171 ***Trigger Reverse Engineering開始***  
2172 Target: 6, victim: 5, Loss: 1.7442, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:1020.60, Cost:0.00 best_reg:1021.02 avg_loss_reg:1020.48: 60% | 603/1000 [13:33<08:55, 1.35s/it]  
2173 early stop 所有  
2174 ***Trigger Reverse Engineering結束***  
2175 Target Class: 6 Victim Class: 5 Trigger Size: 1020.60205078125 Optimization Steps: 416  
2176 *****檢測結束*****  
2177 檢測結果: Model是安全的(Benign)  
2178 整體耗時: 823.4601445198059  
2179 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000654-----  
2180 ***Pre-Screening開始***  
2181 ***Pre-Screening結束***  
2182 可能的攻擊方式: Label Specific Backdoor Attack  
2183 可能的 target-victim 配對: ['13-6']  
2184 ***Trigger Reverse Engineering開始***  
2185 Target: 13, victim: 6, Loss: 1.8131, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:1048.42, Cost:0.00 best_reg:1050.15 avg_loss_reg:1052.32: 94% | 940/1000 [23:59<01:31, 1.53s/it]  
2186 early stop 所有  
2187 ***Trigger Reverse Engineering結束***  
2188 Target Class: 13 Victim Class: 6 Trigger Size: 1048.416015625 Optimization Steps: 941  
2189 *****檢測結束*****  
2190 檢測結果: Model是安全的(Benign)  
2191 整體耗時: 1451.3768366197968  
2192 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000655-----  
2193 ***Pre-Screening開始***  
2194 ***Pre-Screening結束***  
2195 可能的攻擊方式: Label Specific Backdoor Attack  
2196 可能的 target-victim 配對: ['5-2', '5-6']  
2197 ***Trigger Reverse Engineering開始***  
2198 Target: 5, victim: 6, Loss: 3.2949, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:36.93, Cost:0.09 best_reg:39.55 avg_loss_reg:39.55: 8% | 81/1000 [00:35<06:47, 2.26it/s]  
2199 early stop 所有
```

```

2200 ***Trigger Reverse Engineering結束***  

2201 Target Class: 5 Victim Class: 6 Trigger Size: 36.931026458740234 Optimization Steps: 70  

2202 ***Symmetric Check開始***  

2203 Target: 6, victim: 5, Loss: 1.9218, Acc: 10.00%, CE_Loss: 1.92, Reg_Loss:6522.63, Cost:0.00 best_Reg:10000000000.00 avg_loss_Reg:6451.48: 100%|██████████| 70/70 [00:30<00:00, 2.28it/s]  

2204 ***Symmetric Check結束***  

2205 *****檢測結束*****  

2206 檢測結果: Model含有後門(Abnormal)  

2207 整體耗時: 71.0315477848053  

2208 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000656-----  

2209 ***Pre-Screening開始***  

2210 ***Pre-Screening結束***  

2211 可能的攻擊方式: Universal Backdoor Attack  

2212 可能的 target class: 23  

2213 可能的 victim classes: ALL  

2214 ***Trigger Reverse Engineering開始***  

2215 Target: 23, victim: 22, Loss: 0.2336, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:46.10, Cost:0.01 best_Reg:44.92 avg_loss_Reg:45.48: 10%|████| 96/1000 [13:50<2:10:23, 8.65s/it]  

2216 early stop 所有  

2217 ***Trigger Reverse Engineering結束***  

2218 Target Class: 23 Victim Class: all Trigger Size: 44.92218526204427 Optimization Steps: 97  

2219 *****檢測結束*****  

2220 檢測結果: Model含有後門(Abnormal)  

2221 整體耗時: 837.3877494335175-----  

2222 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000657-----  

2223 ***Pre-Screening開始***  

2224 ***Pre-Screening結束***  

2225 ***檢測結束***  

2226 檢測結果: Model是安全的(Benign)  

2227 整體耗時: 11.432076692581177-----  

2228 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000658-----  

2229 ***Pre-Screening開始***  

2230 ***Pre-Screening結束***  

2231 ***檢測結束***  

2232 檢測結果: Model是安全的(Benign)  

2233 整體耗時: 16.57835030555725-----  

2234 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000659-----  

2235 ***Pre-Screening開始***  

2236 ***Pre-Screening結束***  

2237 可能的攻擊方式: Label Specific Backdoor Attack  

2238 可能的 target-victim 配對: ['4-0', '4-2']  

2239 ***Trigger Reverse Engineering開始***  

2240 Target: 4, victim: 2, Loss: 5.4997, Acc: 0.00%, CE_Loss: 5.50, Reg_Loss:2578.87, Cost:0.00 best_Reg:100000000000.00 avg_loss_Reg:2558.30: 2%|████| 21/1000 [00:05<04:00, 4.08it/s]  

2241 ***Trigger Reverse Engineering結束***  

2242 Target Class: 4 Victim Class: 0 Trigger Size: 100000000000.0 Optimization Steps: 11  

2243 *****檢測結束*****  

2244 檢測結果: Model是安全的(Benign)  

2245 整體耗時: 8.3324453830718994-----  

2246 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000660-----  

2247 ***Pre-Screening開始***  

2248 ***Pre-Screening結束***  

2249 可能的攻擊方式: Label Specific Backdoor Attack  

2250 可能的 target-victim 配對: ['0-6']  

2251 ***Trigger Reverse Engineering開始***  

2252 Target: 0, victim: 6, Loss: 12.4748, Acc: 0.00%, CE_Loss: 12.47, Reg_Loss:2558.86, Cost:0.00 best_Reg:10000000000.00 avg_loss_Reg:2545.27: 1%|████| 10/1000 [00:02<04:43, 3.49it/s]  

2253 ***Trigger Reverse Engineering結束***  

2254 Target Class: 0 Victim Class: 6 Trigger Size: 10000000000.0 Optimization Steps: 11  

2255 *****檢測結束*****  

2256 檢測結果: Model是安全的(Benign)  

2257 整體耗時: 9.11338496208191-----  

2258 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000661-----  

2259 ***Pre-Screening開始***  

2260 ***Pre-Screening結束***  

2261 可能的攻擊方式: Label Specific Backdoor Attack  

2262 可能的 target-victim 配對: ['2-13']  

2263 ***Trigger Reverse Engineering開始***  

2264 Target: 2, victim: 13, Loss: 13.1293, Acc: 0.00%, CE_Loss: 13.13, Reg_Loss:2546.42, Cost:0.00 best_Reg:10000000000.00 avg_loss_Reg:2535.49: 1%|████| 10/1000 [00:01<02:10, 7.56it/s]  

2265 ***Trigger Reverse Engineering結束***  

2266 Target Class: 2 Victim Class: 13 Trigger Size: 10000000000.0 Optimization Steps: 11  

2267 *****檢測結束*****  

2268 檢測結果: Model是安全的(Benign)  

2269 整體耗時: 6.998090028762817-----  

2270 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000662-----
```

```
2271 ***Pre-Screening開始***  
2272 ***Pre-Screening結束***  
2273 可能的攻擊方式: Label Specific Backdoor Attack  
2274 可能的 target-victim 配對: ['0-10', '5-1', '9-6', '9-11']  
2275 ***Trigger Reverse Engineering開始***  
2276 Target: 9, victim: 6, Loss: 6.0371, Acc: 100.00%, CE_Loss: 0.38, Reg_Loss:3768.44, Cost:0.00 best_reg:3777.02 avg_loss_reg:3777.02: 31%|████| 309/1000 [09:53<22:07, 1.92s/it]  
2277 early stop 所有  
2278 ***Trigger Reverse Engineering結束***  
2279 Target Class: 9 Victim Class: 6 Trigger Size: 3768.43701171875 Optimization Steps: 276  
2280 ****檢測結果: Model是安全的(Benign)  
2281 檢測結果: Model是安全的(Benign)  
2282 整體耗時: 603.9759449958801  
2283 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000663-----  
2284 ***Pre-Screening開始***  
2285 ***Pre-Screening結束***  
2286 可能的攻擊方式: Universal Backdoor Attack  
2287 可能的 target class: 4  
2288 可能的 victim classes: ALL  
2289 ***Trigger Reverse Engineering開始***  
2290 Target: 4, victim: 4, Loss: 0.5035, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:2548.90, Cost:0.00 best_reg:2543.55 avg_loss_reg:2514.48: 23%|████| 230/1000 [31:36<1:45:48, 8.24s/it]  
2291 early stop 所有  
2292 ***Trigger Reverse Engineering結束***  
2293 Target Class: 4 Victim Class: all Trigger Size: 2543.5538940429688 Optimization Steps: 231  
2294 ****檢測結果: Model是安全的(Benign)  
2295 檢測結果: Model是安全的(Benign)  
2296 整體耗時: 1902.447039604187  
2297 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000664-----  
2298 ***Pre-Screening開始***  
2299 ***Pre-Screening結束***  
2300 可能的攻擊方式: Label Specific Backdoor Attack  
2301 可能的 target-victim 配對: ['0-3', '2-5', '7-1']  
2302 ***Trigger Reverse Engineering開始***  
2303 Target: 2, victim: 5, Loss: 0.1659, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:2118.79, Cost:0.00 best_reg:2088.90 avg_loss_reg:2115.60: 100%|████| 1000/1000 [45:13<00:00, 2.71s/it]  
2304 ***Trigger Reverse Engineering結束***  
2305 Target Class: 2 Victim Class: 5 Trigger Size: 2088.895751953125 Optimization Steps: 977  
2306 ****檢測結果: Model是安全的(Benign)  
2307 檢測結果: Model是安全的(Benign)  
2308 整體耗時: 2730.6394517421722  
2309 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000665-----  
2310 ***Pre-Screening開始***  
2311 ***Pre-Screening結束***  
2312 可能的攻擊方式: Label Specific Backdoor Attack  
2313 可能的 target-victim 配對: ['1-0']  
2314 ***Trigger Reverse Engineering開始***  
2315 Target: 1, victim: 0, Loss: 7.2909, Acc: 0.00%, CE_Loss: 7.29, Reg_Loss:2537.58, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2526.24: 1%| 10/1000 [00:15<26:13, 1.59s/it]  
2316 ***Trigger Reverse Engineering結束***  
2317 Target Class: 1 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11  
2318 ****檢測結果: Model是安全的(Benign)  
2319 檢測結果: Model是安全的(Benign)  
2320 整體耗時: 34.70030760765076  
2321 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000666-----  
2322 ***Pre-Screening開始***  
2323 ***Pre-Screening結束***  
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: 5.526058912277222  
2327 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000667-----  
2328 ***Pre-Screening開始***  
2329 ***Pre-Screening結束***  
2330 ***檢測結果: Model是安全的(Benign)  
2331 檢測結果: Model是安全的(Benign)  
2332 整體耗時: 15.331050634384155  
2333 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000668-----  
2334 ***Pre-Screening開始***  
2335 ***Pre-Screening結束***  
2336 ***檢測結果: Model是安全的(Benign)  
2337 檢測結果: Model是安全的(Benign)  
2338 整體耗時: 12.466902017593384  
2339 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000669-----  
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: 12.110922773880005  
2345 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000670-----  
2346 ***Pre-Screening開始***  
2347 ***Pre-Screening結束***  
2348 ***檢測結束***  
2349 檢測結果: Model是安全的(Benign)  
2350 整體耗時: 10.919736623764038  
2351 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000671-----  
2352 ***Pre-Screening開始***  
2353 ***Pre-Screening結束***  
2354 ***檢測結束***  
2355 檢測結果: Model是安全的(Benign)  
2356 整體耗時: 7.17254114151001  
2357 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000672-----  
2358 ***Pre-Screening開始***  
2359 ***Pre-Screening結束***  
2360 可能的攻擊方式: Label Specific Backdoor Attack  
2361 可能的 target-victim 配對: ['2-16', '3-11', '10-3', '10-4', '11-3', '12-4']  
2362 ***Trigger Reverse Engineering開始***  
2363 Target: 2, victim: 16, Loss: 1.1595, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:690.64, Cost:0.00 best_reg:703.23 avg_loss_reg:694.91: 30%|████| | 302/1000 [01:05<02:30, 4.64it/s]  
2364 early stop 所有  
2365 ***Trigger Reverse Engineering結束***  
2366 Target Class: 2 Victim Class: 16 Trigger Size: 690.636962890625 Optimization Steps: 218  
2367 ***Symmetric Check開始***  
2368 Target: 16, victim: 2, Loss: 1.9598, Acc: 95.00%, CE_Loss: 0.36, Reg_Loss:1602.38, Cost:0.00 best_reg:1649.82 avg_loss_reg:1608.71: 100%|████| | 218/218 [00:46<00:00, 4.65it/s]  
2369 ***Symmetric Check結束***  
2370 *****檢測結束*****  
2371 檢測結果: Model是安全的(Benign)  
2372 整體耗時: 118.14670515060425  
2373 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000673-----  
2374 ***Pre-Screening開始***  
2375 ***Pre-Screening結束***  
2376 ***檢測結束***  
2377 檢測結果: Model是安全的(Benign)  
2378 整體耗時: 16.57869577407837  
2379 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000674-----  
2380 ***Pre-Screening開始***  
2381 ***Pre-Screening結束***  
2382 可能的攻擊方式: Label Specific Backdoor Attack  
2383 可能的 target-victim 配對: ['9-14']  
2384 ***Trigger Reverse Engineering開始***  
2385 Target: 9, victim: 14, Loss: 4.3517, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:32.76, Cost:0.00 best_reg:34.57: 6%|████| | 64/1000 [01:22<20:01, 1.28s/it]  
2386 0%| 0/65 [00:00<?, ?]it/searly stop 所有  
2387 ***Trigger Reverse Engineering結束***  
2388 Target Class: 9 Victim Class: 14 Trigger Size: 32.75567626953125 Optimization Steps: 65  
2389 ***Symmetric Check開始***  
2390 Target: 14, victim: 9, Loss: 2.4571, Acc: 20.00%, CE_Loss: 2.46, Reg_Loss:14820.69, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:14760.00: 100%|████| | 65/65 [01:22<00:00, 1.26s/it]  
2391 ***Symmetric Check結束***  
2392 *****檢測結束*****  
2393 檢測結果: Model含有後門(Abnormal)  
2394 整體耗時: 179.68475675582886  
2395 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000675-----  
2396 ***Pre-Screening開始***  
2397 ***Pre-Screening結束***  
2398 ***檢測結束***  
2399 檢測結果: Model是安全的(Benign)  
2400 整體耗時: 2.130906820297241  
2401 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000676-----  
2402 ***Pre-Screening開始***  
2403 ***Pre-Screening結束***  
2404 ***檢測結束***  
2405 檢測結果: Model是安全的(Benign)  
2406 整體耗時: 12.780931234359741  
2407 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000677-----  
2408 ***Pre-Screening開始***  
2409 ***Pre-Screening結束***  
2410 ***檢測結束***  
2411 檢測結果: Model是安全的(Benign)  
2412 整體耗時: 8.777793407440186
```

File - main ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000678-----

2413     \*\*\*Pre-Screening開始\*\*\*  
2414     \*\*\*Pre-Screening結束\*\*\*  
2415     \*\*\*Pre-Screening結束\*\*\*  
2416     可能的攻擊方式: Label Specific Backdoor Attack  
2417     可能的 target-victim 配對: ['1-20']  
2418     \*\*\*Trigger Reverse Engineering開始\*\*\*  
2419     Target: 1, victim: 20, Loss: 1.0873, Acc: 100.00%, CE\_Loss: 0.16, Reg\_Loss:411.37, Cost:0.00 best\_reg:415.51 avg\_loss\_reg:415.51: 18%|████| 184/1000 [14:08<1:02:43, 4.61s/it]  
2420     early stop 所有  
2421     \*\*\*Trigger Reverse Engineering結束\*\*\*  
2422     Target Class: 1 Victim Class: 20 Trigger Size: 411.36968994140625 Optimization Steps: 185  
2423     \*\*\*Symmetric Check開始\*\*\*  
2424     Target: 20, victim: 1, Loss: 1.7781, Acc: 95.00%, CE\_Loss: 0.35, Reg\_Loss:952.76, Cost:0.00 best\_reg:999.21 avg\_loss\_reg:950.30: 100%|██████████| 185/185 [14:09<00:00, 4.59s/it]  
2425     \*\*\*Symmetric Check結束\*\*\*  
2426     \*\*\*\*\*檢測結果: Model是安全的(Benign)  
2427     檢測結果: Model是安全的(Benign)  
2428     整體耗時: 1727.386981765747  
2429     ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000679-----  
2430     \*\*\*Pre-Screening開始\*\*\*  
2431     \*\*\*Pre-Screening結束\*\*\*  
2432     可能的攻擊方式: Label Specific Backdoor Attack  
2433     可能的 target-victim 配對: ['4-0']  
2434     \*\*\*Trigger Reverse Engineering開始\*\*\*  
2435     Target: 4, victim: 0, Loss: 2.0641, Acc: 25.00%, CE\_Loss: 2.06, Reg\_Loss:3002.70, Cost:0.00 best\_reg:10000000000.00 avg\_loss\_reg:2882.85: 2%|████| 120/1000 [01:30<1:13:45, 4.52s/it]  
2436     \*\*\*Trigger Reverse Engineering結束\*\*\*  
2437     Target Class: 4 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 21  
2438     \*\*\*\*\*檢測結果: Model是安全的(Benign)  
2439     檢測結果: Model是安全的(Benign)  
2440     整體耗時: 112.15475869178772  
2441     ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000680-----  
2442     \*\*\*Pre-Screening開始\*\*\*  
2443     \*\*\*Pre-Screening結束\*\*\*  
2444     \*\*\*\*\*檢測結果: Model是安全的(Benign)  
2445     檢測結果: Model是安全的(Benign)  
2446     整體耗時: 1.5067570209503174  
2447     ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000681-----  
2448     \*\*\*Pre-Screening開始\*\*\*  
2449     \*\*\*Pre-Screening結束\*\*\*  
2450     可能的攻擊方式: Label Specific Backdoor Attack  
2451     可能的 target-victim 配對: ['0-15']  
2452     \*\*\*Trigger Reverse Engineering開始\*\*\*  
2453     Target: 0, victim: 15, Loss: 1.2714, Acc: 100.00%, CE\_Loss: 0.12, Reg\_Loss:512.88, Cost:0.00 best\_reg:514.32 avg\_loss\_reg:514.32: 20%|████| 198/1000 [07:12<29:11, 2.18s/it]  
2454     early stop 所有  
2455     \*\*\*Trigger Reverse Engineering結束\*\*\*  
2456     Target Class: 0 Victim Class: 15 Trigger Size: 512.8826904296875 Optimization Steps: 199  
2457     \*\*\*Symmetric Check開始\*\*\*  
2458     Target: 15, victim: 0, Loss: 4.0109, Acc: 100.00%, CE\_Loss: 0.45, Reg\_Loss:1054.06, Cost:0.00 best\_reg:1047.92 avg\_loss\_reg:1043.06: 100%|████| 199/199 [07:12<00:00, 2.17s/it]  
2459     \*\*\*Symmetric Check結束\*\*\*  
2460     \*\*\*\*\*檢測結果: Model是安全的(Benign)  
2461     檢測結果: Model是安全的(Benign)  
2462     整體耗時: 881.8849618434906  
2463     ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000682-----  
2464     \*\*\*Pre-Screening開始\*\*\*  
2465     \*\*\*Pre-Screening結束\*\*\*  
2466     可能的攻擊方式: Label Specific Backdoor Attack  
2467     可能的 target-victim 配對: ['0-1', '1-0', '3-6', '3-8', '7-8', '10-2', '11-6']  
2468     \*\*\*Trigger Reverse Engineering開始\*\*\*  
2469     Target: 11, victim: 6, Loss: 13.7306, Acc: 0.00%, CE\_Loss: 13.73, Reg\_Loss:2560.59, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:2544.49: 10%|████| 96/1000 [00:43<06:46, 2.22it/s]  
2470     \*\*\*Trigger Reverse Engineering結束\*\*\*  
2471     Target Class: 0 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11  
2472     \*\*\*\*\*檢測結果: Model是安全的(Benign)  
2473     檢測結果: Model是安全的(Benign)  
2474     整體耗時: 49.2242/90837860  
2475     ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000683-----  
2476     \*\*\*Pre-Screening開始\*\*\*  
2477     \*\*\*Pre-Screening結束\*\*\*  
2478     \*\*\*\*\*檢測結果: Model是安全的(Benign)  
2479     檢測結果: Model是安全的(Benign)  
2480     整體耗時: 18.853120803833008  
2481     ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000684-----  
2482     \*\*\*Pre-Screening開始\*\*\*  
2483     \*\*\*Pre-Screening結束\*\*\*

```
2484 可能的攻擊方式: Label Specific Backdoor Attack
2485 可能的 target-victim 配對: ['3-8']
2486 ***Trigger Reverse Engineering開始***
2487 Target: 3, victim: 8, Loss: 0.6416, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:235.20, Cost:0.00 best_reg:223.51 avg_loss_reg:231.05: 100%|████████| 1000/1000 [09:39<00:00, 1.73it/s]
2488 0%| 0/1000 [00:00:<?, it/s]***Trigger Reverse Engineering結束***
2489 Target Class: 3 Victim Class: 8 Trigger Size: 223.5057373046875 Optimization Steps: 1000
2490 ***Symmetric Check開始***
2491 Target: 8, victim: 3, Loss: 4.1772, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:2578.38, Cost:0.00 best_reg:2579.81 avg_loss_reg:2594.51: 34%|████| 343/1000 [03:19<06:22, 1.72it/s]
2492 early stop 所有
2493 ***Symmetric Check結束****
2494 ****Pre-Screening開始****
2495 檢測結果: Model含有後門(Abnormal)
2496 整體耗時: 787.1261568069458
2497 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000685-----
2498
2499 ****Pre-Screening結束****
2500 可能的攻擊方式: Universal Backdoor Attack
2501 可能的 target class: 11
2502 可能的 victim classes: ALL
2503 ***Trigger Reverse Engineering開始***
2504 Target: 11, victim: 16, Loss: 0.1108, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:166.26, Cost:0.00 best_reg:168.92 avg_loss_reg:165.75: 10%|████| 95/1000 [09:29<1:30:21, 5.99s/it]
2505 early stop 所有
2506 ***Trigger Reverse Engineering結束***
2507 Target Class: 11 Victim Class: all Trigger Size: 168.91581217447916 Optimization Steps: 96
2508 ****Pre-Screening結束****
2509 檢測結果: Model含有後門(Abnormal)
2510 整體耗時: 576.4152617454529
2511 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000686-----
2512 ****Pre-Screening開始****
2513 ****Pre-Screening結束****
2514 可能的攻擊方式: Label Specific Backdoor Attack
2515 可能的 target-victim 配對: ['2-1']
2516 ***Trigger Reverse Engineering開始***
2517 Target: 2, victim: 1, Loss: 1.2857, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:237.73, Cost:0.01 best_reg:238.45 avg_loss_reg:238.45: 15%|████| 146/1000 [00:23<02:14, 6.34it/s]
2518 early stop 所有
2519 ***Trigger Reverse Engineering結束***
2520 Target Class: 2 Victim Class: 1 Trigger Size: 237.72679138183594 Optimization Steps: 147
2521 ***Symmetric Check開始***
2522 Target: 1, victim: 2, Loss: 1.1302, Acc: 95.00%, CE_Loss: 0.12, Reg_Loss:1519.89, Cost:0.00 best_reg:1569.70 avg_loss_reg:1520.63: 100%|████| 147/147 [00:23<00:00, 6.34it/s]
2523 ****Pre-Screening結束****
2524 ****Pre-Screening結束****
2525 檢測結果: Model是安全的(Benign)
2526 整體耗時: 52.078930139541626
2527 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000687-----
2528 ****Pre-Screening開始****
2529 ****Pre-Screening結束****
2530 可能的攻擊方式: Label Specific Backdoor Attack
2531 可能的 target-victim 配對: ['0-3']
2532 ***Trigger Reverse Engineering開始***
2533 Target: 0, victim: 3, Loss: 4.4993, Acc: 20.00%, CE_Loss: 4.50, Reg_Loss:3479.14, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:3234.86: 2%| 20/1000 [00:40<33:13, 2.03s/it]
2534 ***Trigger Reverse Engineering結束***
2535 Target Class: 0 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 21
2536 ****Pre-Screening結束****
2537 檢測結果: Model是安全的(Benign)
2538 整體耗時: 47.284698724746704
2539 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000688-----
2540 ****Pre-Screening開始****
2541 ****Pre-Screening結束****
2542 可能的攻擊方式: Label Specific Backdoor Attack
2543 可能的 target-victim 配對: ['12-0']
2544 ***Trigger Reverse Engineering開始***
2545 Target: 12, victim: 0, Loss: 7.3933, Acc: 0.00%, CE_Loss: 7.39, Reg_Loss:2550.46, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2539.51: 1%| 10/1000 [00:12<20:56, 1.27s/it]
2546 ***Trigger Reverse Engineering結束***
2547 Target Class: 12 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 11
2548 ****Pre-Screening結束****
2549 檢測結果: Model是安全的(Benign)
2550 整體耗時: 23.71685028076172
2551 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000689-----
2552 ***Pre-Screening開始****
2553 ***Pre-Screening結束****
2554 可能的攻擊方式: Universal Backdoor Attack
```

```

2555 可能的 target class: 8
2556 可能的 victim classes: ALL
2557 ***Trigger Reverse Engineering開始***
2558 Target: 8, victim: 12, Loss: 2.9553, Acc: 91.67%, CE_Loss: 0.46, Reg_Loss:12.81, Cost:0.19 best_reg:12.83 avg_loss_reg:12.78: 10% | 103/1000 [1:04:17<9:19:53, 37.45s/it]
2559 early stop 所有
2560 ***Trigger Reverse Engineering結束***
2561 Target Class: 8 Victim Class: all Trigger Size: 12.82270728217231 Optimization Steps: 104
2562 檢測結果: Model含後門(Abnormal)
2563 整體耗時: 3876.8685262203217
2564
2565 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000690-----
2566 ***Pre-Screening開始***
2567 ***Pre-Screening結束***
2568 可能的攻擊方式: Label Specific Backdoor Attack
2569 可能的 target-victim 配對: ['2-9']
2570 ***Trigger Reverse Engineering開始***
2571 Target: 2, victim: 9 Loss: 11.7419, Acc: 0.00%, CE_Loss: 11.74, Reg_Loss:2531.56, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2526.17: 1% | 10/1000 [00:11<19:15, 1.17s/it]
2572 ***Trigger Reverse Engineering結束***
2573 Target Class: 2 Victim Class: 9 Trigger Size: 11
2574 檢測結果: Model是安全的(Benign)
2575 整體耗時: 19.89568018913269
2576
2577 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000691-----
2578 ***Pre-Screening開始***
2579 ***Pre-Screening結束***
2580 可能的攻擊方式: Universal Backdoor Attack
2581 可能的 target class: 2
2582 可能的 victim classes: ALL
2583 ***Trigger Reverse Engineering開始***
2584 Target: 2, victim: 4 Loss: 0.3427, Acc: 95.83%, CE_Loss: 0.03, Reg_Loss:92.49, Cost:0.00 best_reg:93.21 avg_loss_reg:91.92: 6% | 65/1000 [01:23<20:06, 1.29s/it]
2585 early stop 所有
2586 ***Trigger Reverse Engineering結束***
2587 Target Class: 2 Victim Class: all Trigger Size: 93.21238708496094 Optimization Steps: 66
2588 檢測結果: Model含後門(Abnormal)
2589 檢測結果: Model含後門(Abnormal)
2590 整體耗時: 89.10876369476318
2591
2592 ***Pre-Screening開始***
2593 ***Pre-Screening結束***
2594 檢測結果: Model是安全的(Benign)
2595 整體耗時: 20.58068509237671
2596
2597 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000692-----
2598 ***Pre-Screening開始***
2599 ***Pre-Screening結束***
2600 可能的攻擊方式: Label Specific Backdoor Attack
2601 可能的 target-victim 配對: ['0-19', '5-6', '5-21', '9-10', '10-9', '12-11', '13-3', '13-21', '14-21', '14-21', '15-6', '16-9', '16-9', '16-10', '17-6', '18-21', '20-6']
2602 ***Trigger Reverse Engineering開始***
2603 Target: 16, victim: 9 Loss: 1.4494, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:549.04, Cost:0.00 best_reg:558.36 avg_loss_reg:558.36: 36% | 365/1000 [13:08<22:52, 2.16s/it]
2604 early stop 所有
2605 ***Trigger Reverse Engineering結束***
2606 Target Class: 16 Victim Class: 9 Trigger Size: 549.0377807617188 Optimization Steps: 174
2607 ***Symmetric Check開始***
2608 Target: 9, victim: 16 Loss: 2.6490, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:3645.03, Cost:0.00 best_reg:3634.60 avg_loss_reg:946.09: 100% | 174/174 [06:15<00:00, 2.16s/it]
2609 ***Symmetric Check結束***
2610 檢測結果: Model是安全的(Benign)
2611 整體耗時: 1184.7377574443817
2612
2613 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000694-----
2614 ***Pre-Screening開始***
2615 ***Pre-Screening結束***
2616 可能的攻擊方式: Label Specific Backdoor Attack
2617 可能的 target-victim 配對: ['8-4']
2618 ***Trigger Reverse Engineering開始***
2619 Target: 8, victim: 4 Loss: 3.4796, Acc: 90.00%, CE_Loss: 0.28, Reg_Loss:947.28, Cost:0.00 best_reg:946.05 avg_loss_reg:946.09: 100% | 1000/1000 [11:14<00:00, 1.48s/it]
2620 ***Trigger Reverse Engineering結束***
2621 Target Class: 8 Victim Class: 4 Trigger Size: 946.0474853515625 Optimization Steps: 1000
2622 ***Symmetric Check開始***
2623 Target: 4, victim: 8 Loss: 2.6015, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:3454.75, Cost:0.00 best_reg:3457.81 avg_loss_reg:3474.77: 51% | 513/1000 [05:46<05:28, 1.48s/it]
2624 early stop 所有
2625 ***Symmetric Check結束***

```

```
2626 **** 檢測結果: Model是安全的(Benign)
2627 整體耗時: 1027.8068509101868
2628 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000695
2629 ***Pre-Screening開始****
2630 ***Pre-Screening結束****
2631 ***檢測結束****
2632 檢測結果: Model是安全的(Benign)
2633 整體耗時: 13.718286037445068
2634 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000696
2635 ***Pre-Screening開始****
2636 可能的攻擊方式: Label Specific Backdoor Attack
2637 可能的 target-victim 配對: ['2-3', '3-2', '21-2']
2638 ***Trigger Reverse Engineering開始****
2639 Target: 21, victim: 2, Loss: 10.3151, Acc: 0.00%, CE_Loss: 10.32, Reg_Loss:2521.05, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2514.59: 3% | 32/1000 [01:12<36:26, 2.26s/it]
2640 ***Trigger Reverse Engineering結束****
2641 Target Class: 2 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 11
2642 ***Trigger Reverse Engineering結束****
2643 Target Class: 2 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 11
2644 檢測結果: Model是安全的(Benign)
2645 整體耗時: 94.64382028579712
2646 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000697
2647 ***Pre-Screening開始****
2648 可能的攻擊方式: Universal Backdoor Attack
2649 ***Pre-Screening結束****
2650 可能的 target class: 0
2651 可能的 victim classes: ALL
2652 可能的 victim classes: ALL
2653 ***Trigger Reverse Engineering開始****
2654 Target: 0, victim: 3, Loss: 0.4455, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:23.58, Cost:0.02 best_reg:23.59 avg_loss_reg:23.52: 6% | 64/1000 [00:31<07:41, 2.03it/s]
2655 early stop 所有
2656 ***Trigger Reverse Engineering結束****
2657 Target Class: 0 Victim Class: all Trigger Size: 25.389612197875977 Optimization Steps: 65
2658 *****檢測結束*****
2659 檢測結果: Model含有後門(Abnormal)
2660 整體耗時: 33.49763107299805
2661 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000698
2662 ***Pre-Screening開始****
2663 可能的攻擊方式: Label Specific Backdoor Attack
2664 可能的 target-victim 配對: ['1-16', '2-3', '3-2', '4-11', '16-1', '17-2']
2665 ***Trigger Reverse Engineering開始****
2666 Target: 3, victim: 2, Loss: 1.6123, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:640.10, Cost:0.00 best_reg:640.45 avg_loss_reg:644.78: 91% | 914/1000 [27:16<02:34, 1.79s/it]
2667 Target: 3, victim: 3, Loss: 3.5070, Acc: 90.00%, CE_Loss: 0.32, Reg_Loss:3188.06, Cost:0.00 best_reg:3234.84 avg_loss_reg:3187.92: 100% | 726/726 [19:50<00:00, 1.64s/it]
2668 early stop 所有
2669 ***Trigger Reverse Engineering結束****
2670 Target Class: 3 Victim Class: 2 Trigger Size: 640.1043701171875 Optimization Steps: 726
2671 ***Symmetric Check開始****
2672 Target: 2, victim: 3, Loss: 3.5070, Acc: 90.00%, CE_Loss: 0.32, Reg_Loss:3188.06, Cost:0.00 best_reg:3234.84 avg_loss_reg:3187.92: 100% | 726/726 [19:50<00:00, 1.64s/it]
2673 ***Symmetric Check結束****
2674 檢測結果: Model是安全的(Benign)
2675 整體耗時: 2841.84239724617
2676 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000699
2677 ***Pre-Screening開始****
2678 ***Pre-Screening結束****
2679 可能的攻擊方式: Label Specific Backdoor Attack
2680 可能的 target-victim 配對: ['11-1']
2681 ***Trigger Reverse Engineering開始****
2682 Target: 11, victim: 1, Loss: 9.4002, Acc: 5.00%, CE_Loss: 9.40, Reg_Loss:2858.24, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2771.65: 2% | 20/1000 [00:09<07:59, 2.04it/s]
2683 ***Trigger Reverse Engineering結束****
2684 Target Class: 11 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 21
2685 Target Class: 11 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 21
2686 *****檢測結束*****
2687 檢測結果: Model是安全的(Benign)
2688 整體耗時: 20.151041984558105
2689 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000700
2690 ***Pre-Screening開始****
2691 ***Pre-Screening結束****
2692 可能的攻擊方式: Label Specific Backdoor Attack
2693 可能的 target-victim 配對: ['7-0', '7-11']
2694 ***Trigger Reverse Engineering開始****
2695 Target: 7, victim: 11, Loss: 2.8605, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:48.64, Cost:0.06 best_reg:48.89 avg_loss_reg:48.98: 10% | 104/1000 [03:30<30:11, 2.02s/it]
2696 early stop 所有
```

```
2697 ***Trigger Reverse Engineering結束***  
2698 Target Class: 7 Victim Class: 11 Trigger Size: 48.642311096191406 Optimization Steps: 70  
2699 ***Symmetric Check開始***  
2700 Target: 11, victim: 7, Loss: 0.9386, Acc: 80.00%, CE_Loss: 0.94, Reg_Loss: 14407.58, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:14319.05: 100%|██████████| 70/70 [02:20<00:00, 2.01s/it]
```

```
2701 ***Symmetric Check結束***  
2702 *****檢測結果*****  
2703 檢測結果: Model含有後門(Abnormal)  
2704 整體耗時: 363.8659639426422
```

```
2705 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000701-----
```

```
2706 ***Pre-Screening開始***  
2707 ***Pre-Screening結束***  
2708 ***檢測結束***  
2709 檢測結果: Model是安全的(Benign)  
2710 整體耗時: 4.618107080459595
```

```
2711 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000702-----
```

```
2712 ***Pre-Screening開始***  
2713 ***Pre-Screening結束***  
2714 ***檢測結束***  
2715 檢測結果: Model是安全的(Benign)  
2716 整體耗時: 6.191958427429199
```

```
2717 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000703-----
```

```
2718 ***Pre-Screening開始***  
2719 ***Pre-Screening結束***  
2720 ***檢測結束***  
2721 檢測結果: Model是安全的(Benign)  
2722 整體耗時: 23.481870651245117
```

```
2723 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000704-----
```

```
2724 ***Pre-Screening開始***  
2725 ***Pre-Screening結束***  
2726 可能的攻擊方式: Universal Backdoor Attack
```

```
2727 可能的 target class: 0  
2728 可能的 victim classes: ALL
```

```
2729 ***Trigger Reverse Engineering開始***  
2730 Target: 0, victim: 4, Loss: 10.8198, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:4788.56, Cost:0.00 best_reg:4779.12 avg_loss_reg:4787.68: 19%|██████████| 193/1000 [47:26<3:18:20, 14.75s/it]
```

```
2731 early stop 所有  
2732 ***Trigger Reverse Engineering結束***  
2733 Target Class: 0 Victim Class: all Trigger Size: 4778.8970947265625 Optimization Steps: 194
```

```
2734 *****檢測結束*****  
2735 檢測結果: Model是安全的(Benign)  
2736 整體耗時: 2859.2218952178955
```

```
2737 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000705-----
```

```
2738 ***Pre-Screening開始***  
2739 ***Pre-Screening結束***  
2740 ***檢測結束***  
2741 檢測結果: Model是安全的(Benign)
```

```
2742 整體耗時: 10.072410106658936
```

```
2743 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000706-----
```

```
2744 ***Pre-Screening開始***  
2745 ***Pre-Screening結束***  
2746 可能的攻擊方式: Label Specific Backdoor Attack
```

```
2747 可能的 target-victim 配對: [0-1]  
2748 ***Trigger Reverse Engineering開始***  
2749 Target: 0, victim: 1, Loss: 10.3407, Acc: 0.00%, CE_Loss: 10.34, Reg_Loss:2559.91, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2544.72: 1%| 10/1000 [00:01<02:04, 7.98it/s]
```

```
2750 ***Trigger Reverse Engineering結束***  
2751 Target Class: 0 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11
```

```
2752 *****檢測結束*****  
2753 檢測結果: Model是安全的(Benign)
```

```
2754 整體耗時: 6.113981008529663
```

```
2755 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000707-----
```

```
2756 ***Pre-Screening開始***  
2757 ***Pre-Screening結束***  
2758 可能的攻擊方式: Label Specific Backdoor Attack
```

```
2759 可能的 target-victim 配對: [9-1]  
2760 ***Trigger Reverse Engineering開始***  
2761 Target: 9, victim: 1, Loss: 12.2789, Acc: 0.00%, CE_Loss: 12.28, Reg_Loss:2579.03, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2560.01: 1%| 10/1000 [00:01<02:35, 6.36it/s]
```

```
2762 ***Trigger Reverse Engineering結束***  
2763 Target Class: 9 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11
```

```
2764 *****檢測結束*****  
2765 檢測結果: Model是安全的(Benign)
```

```
2766 整體耗時: 6.911442756652832
```

```
2767 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000708-----
```

```

2768 ***Pre-Screening開始***
2769 ***Pre-Screening結束***
2770 ***檢測結束***  

2771 檢測結果: Model是安全的(Benign)
2772 整體耗時: 5.035977840423584  

2773 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000709-----  

2774 ***Pre-Screening開始***
2775 ***Pre-Screening結束***  

2776 可能的攻擊方式: Label Specific Backdoor Attack
2777 可能的 target-victim 配對: ['2-12', '7-2', '7-12', '14-12']
2778 ***Trigger Reverse Engineering開始***  

2779 Target: 14, victim: 12, Loss: 10.3063, Acc: 0.00%, CE_Loss: 10.31, Reg_Loss:2579.40, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2559.17: 4%| | 43/1000 [00:04<01:47, 8.92it/s]  

2780 ***Trigger Reverse Engineering結束***  

2781 Target Class: 2 Victim Class: 12 Trigger Size: 1000000000.0 Optimization Steps: 11  

2782 *****檢測結束*****  

2783 檢測結果: Model是安全的(Benign)
2784 整體耗時: 9.917515277862549  

2785 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000710-----  

2786 ***Pre-Screening開始***
2787 ***Pre-Screening結束***  

2788 ***檢測結束***  

2789 檢測結果: Model是安全的(Benign)
2790 整體耗時: 17.292693860168457  

2791 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000711-----  

2792 ***Pre-Screening開始***
2793 ***Pre-Screening結束***  

2794 ***檢測結束***  

2795 檢測結果: Model是安全的(Benign)
2796 整體耗時: 6.8997483825683594  

2797 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000712-----  

2798 ***Pre-Screening開始***
2799 ***Pre-Screening結束***  

2800 可能的攻擊方式: Label Specific Backdoor Attack
2801 可能的 target-victim 配對: ['2-6', '8-6', '15-6', '15-10', '17-18', '21-6']
2802 ***Trigger Reverse Engineering開始***  

2803 Target: 21, victim: 6, Loss: 12.1124, Acc: 0.00%, CE_Loss: 12.11, Reg_Loss:2549.18, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2536.79: 6%| | 65/1000 [00:20<04:57, 3.14it/s]  

2804 ***Trigger Reverse Engineering結束***  

2805 Target Class: 2 Victim Class: 6 Trigger Size: 1000000000.0 Optimization Steps: 11  

2806 *****檢測結束*****  

2807 檢測結果: Model是安全的(Benign)
2808 整體耗時: 27.61710786819458  

2809 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000713-----  

2810 ***Pre-Screening開始***
2811 ***Pre-Screening結束***  

2812 ***檢測結束***  

2813 檢測結果: Model是安全的(Benign)
2814 整體耗時: 13.882686614990234  

2815 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000714-----  

2816 ***Pre-Screening開始***
2817 ***Pre-Screening結束***  

2818 可能的攻擊方式: Universal Backdoor Attack
2819 可能的 target class: 13
2820 可能的 victim classes: ALL  

2821 ***Trigger Reverse Engineering開始***  

2822 Target: 13, victim: 12, Loss: 0.3804, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:570.40, Cost:0.00 best_reg:562.74 avg_loss_reg:565.14: 10%| | 99/1000 [49:27<7:30:09, 29.98s/it]
2823 early stop 所有
2824 ***Trigger Reverse Engineering結束***  

2825 Target Class: 13 Victim Class: all Trigger Size: 562.7442355685764 Optimization Steps: 100  

2826 整體耗時: 2984.7816500663757  

2827 檢測結果: Model含有後門(Abnormal)
2828 整體耗時: 2984.7816500663757  

2829 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000715-----  

2830 ***Pre-Screening開始***
2831 ***Pre-Screening結束***  

2832 可能的攻擊方式: Universal Backdoor Attack
2833 可能的 target class: 2
2834 可能的 victim classes: ALL  

2835 ***Trigger Reverse Engineering開始***  

2836 Target: 2, victim: 14, Loss: 0.4672, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:202.01, Cost:0.00 best_reg:203.81 avg_loss_reg:201.60: 6%| | 65/1000 [38:15<9:10:23, 35.32s/it]  

2837 early stop 所有
2838 ***Trigger Reverse Engineering結束***  


```

```

2839 Target Class: 2 Victim Class: all Trigger Size: 203.8075393676758 Optimization Steps: 66
2840 ****Pre-Screening開始****
2841 檢測結果: Model含有後門(Abnormal)
2842 整體耗時: 2314.777684688568 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000716-----
2843 ****Pre-Screening結束****
2844 可能的攻擊方式: Label Specific Backdoor Attack
2845 可能的 target-victim 配對: [0-6]
2846 ***Trigger Reverse Engineering開始****
2847 可能的 target-victim 配對: [0-6]
2848 Target: 0, victim: 6, Loss: 2.8356, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss: 80125, Cost:0.00 best_reg:803.33 avg_loss_reg:796.24: 12% █ | 121/1000 [0:37<04:35, 3.19it/s]
2849 Target: 0, victim: 6, Loss: 2.8356, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss: 796.24: 12% █ | 121/1000 [0:37<04:35, 3.19it/s]
2850 early stop 所有
2851 ***Trigger Reverse Engineering結束****
2852 Target Class: 0 Victim Class: 6 Trigger Size: 801.2451171875 Optimization Steps: 122
2853 ***Symmetric Check開始****
2854 Target: 6, victim: 0 Loss: 2.2999, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss: 4779.47, Cost:0.00 best_reg:4780.58 avg_loss_reg:4795.71: 100% █ | 122/122 [0:38<00:00, 3.15it/s]
2855 ***Symmetric Check結束****
2856 *****檢測結束*****
2857 檢測結果: Model是安全的(Benign)
2858 整體耗時: 82.74287629127502 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000717-----
2859 -----
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: [3-12', '9-12']
2864 ***Trigger Reverse Engineering開始****
2865 Target: 9, victim: 12, Loss: 1.0474, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss: 612.21, Cost:0.00 best_reg:613.10 avg_loss_reg:613.10: 19% █ | 187/1000 [16:43 <1:12:42, 5.37s/it]
2866 early stop 所有
2867 ***Trigger Reverse Engineering結束****
2868 Target Class: 9 Victim Class: 12 Trigger Size: 612.2073974609375 Optimization Steps: 177
2869 ***Symmetric Check開始****
2870 Target: 12, victim: 9 Loss: 2.4012, Acc: 95.00%, CE_Loss: 0.43, Reg_Loss: 2954.34, Cost:0.00 best_reg:3074.04 avg_loss_reg:2968.75: 100% █ | 177/177 [15:44<00:00, 5.34s/it]
2871 ***Symmetric Check結束****
2872 *****檢測結束*****
2873 檢測結果: Model是安全的(Benign)
2874 整體耗時: 1971.8763029575348 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000718-----
2875 -----
2876 ***Pre-Screening開始****
2877 ***Pre-Screening結束****
2878 ***檢測結束****
2879 檢測結果: Model是安全的(Benign)
2880 整體耗時: 25.312814235687256 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000719-----
2881 -----
2882 ***Pre-Screening開始****
2883 ***Pre-Screening結束****
2884 可能的攻擊方式: Label Specific Backdoor Attack
2885 可能的 target-victim 配對: [10-0]
2886 ***Trigger Reverse Engineering開始****
2887 Target: 10, victim: 0 Loss: 10.1701, Acc: 0.00%, CE_Loss: 10.17, Reg_Loss: 2541.75, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2531.86: 1% | 10/1000 [0:03<06:07, 2.69it/s]
2888 ***Trigger Reverse Engineering結束****
2889 Target Class: 10 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 11
2890 *****檢測結束*****
2891 檢測結果: Model是安全的(Benign)
2892 整體耗時: 9.31330132484436 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000720-----
2893 -----
2894 ***Pre-Screening開始****
2895 ***Pre-Screening結束****
2896 ***檢測結束****
2897 檢測結果: Model是安全的(Benign)
2898 整體耗時: 4.403835773468018 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000721-----
2899 -----
2900 ***Pre-Screening開始****
2901 ***Pre-Screening結束****
2902 可能的攻擊方式: Label Specific Backdoor Attack
2903 可能的 target-victim 配對: [1-2, '11-12', '11-16', '12-16']
2904 ***Trigger Reverse Engineering開始****
2905 Target: 11, victim: 16, Loss: 1.9336, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss: 21.83, Cost:0.09 best_reg:22.51 avg_loss_reg:22.51: 18% █ | 175/1000 [01:15<05:54, 2.32it/s]
2906 early stop 所有
2907 ***Trigger Reverse Engineering結束****
2908 Target Class: 11 Victim Class: 16 Trigger Size: 21.83353042602539 Optimization Steps: 80
2909 ***Symmetric Check開始****

```

```

2910 Target: 16, victim: 11, Loss: 4.5419, Acc: 20.00%, CE_Loss: 4.54, Reg_Loss:12701.46, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:12545.80: 100% | 80/80 [00:34<00:00, 2.33it/s]
2911 ***Symmetric Check結束****
2912 *****檢測結果*****檢測結束*****
2913 檢測結果: Model含有後門(Abnormal)
2914 整體耗時: 116.69450879096985
2915 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000722-----
2916 ***Pre-Screening開始****
2917 ***Pre-Screening結束****
2918 可能的攻擊方式: Label Specific Backdoor Attack
2919 可能的 target-victim 配對: ['11-1']
2920 ***Trigger Reverse Engineering開始****
2921 Target: 11, victim: 1, Loss: 6.0542, Acc: 0.00%, CE_Loss: 6.05, Reg_Loss:2546.54, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2534.49: 1% | 10/1000 [00:01<02:56, 5.59it/s]
2922 ***Trigger Reverse Engineering結束****
2923 Target Class: 11 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11
2924 *****檢測結束*****檢測結果: Model是安全的(Benign)
2925 檢測結果: Model是安全的(Benign)
2926 整體耗時: 9:031298398971558
2927 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000723-----
2928 ***Pre-Screening開始****
2929 ***Pre-Screening結束****
2930 可能的攻擊方式: Label Specific Backdoor Attack
2931 可能的 target-victim 配對: ['0-12', '3-2', '3-8', '4-0', '4-3', '4-7', '5-6', '5-8', '6-12', '6-3', '6-0', '8-2', '8-6', '8-7']
2932 ***Trigger Reverse Engineering開始****
2933 Target: 0, victim: 12, Loss: 1.3666, Acc: 100.00%, CE_Loss: 0.33, Reg_Loss:693.76, Cost:0.00 best_reg:672.58 avg_loss_reg:692.79: 100% | 1000/1000 [03:25<00:00, 4.86it/s]
2934 ***Trigger Reverse Engineering結束****
2935 Target Class: 0 Victim Class: 12 Trigger Size: 672.581787109375 Optimization Steps: 857
2936 ***Symmetric Check開始****
2937 Target: 12, victim: 0, Loss: 2.0937, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:1838.54, Cost:0.00 best_reg:1840.42 avg_loss_reg:1809.74: 47% | 407/857 [01:24<01:33, 4.83it/s]
2938 early stop 所有
2939 ***Symmetric Check結束****
2940 *****檢測結束*****檢測結果: Model是安全的(Benign)
2941 檢測結果: Model是安全的(Benign)
2942 整體耗時: 295.20368337631226
2943 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000724-----
2944 ***Pre-Screening開始****
2945 ***Pre-Screening結束****
2946 ***檢測結束****
2947 檢測結果: Model是安全的(Benign)
2948 整體耗時: 9:10049033164978
2949 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000725-----
2950 ***Pre-Screening開始****
2951 ***Pre-Screening結束****
2952 可能的攻擊方式: Label Specific Backdoor Attack
2953 可能的 target-victim 配對: ['3-15', '9-11', '15-3']
2954 ***Trigger Reverse Engineering開始****
2955 Target: 15, victim: 3, Loss: 11.6112, Acc: 5.00%, CE_Loss: 11.61, Reg_Loss:3915.67, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:3549.89: 6% | 62/1000 [00:23<05:50, 2.68it/s]
2956 ***Trigger Reverse Engineering結束****
2957 Target Class: 3 Victim Class: 15 Trigger Size: 1000000000.0 Optimization Steps: 21
2958 ***檢測結束*****檢測結果: Model是安全的(Benign)
2959 檢測結果: Model是安全的(Benign)
2960 整體耗時: 31.230352732040405
2961 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000726-----
2962 ***Pre-Screening開始****
2963 ***Pre-Screening結束****
2964 ***檢測結束****
2965 檢測結果: Model是安全的(Benign)
2966 整體耗時: 4:968591213226318
2967 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000727-----
2968 ***Pre-Screening開始****
2969 ***Pre-Screening結束****
2970 ***檢測結束****
2971 檢測結果: Model是安全的(Benign)
2972 整體耗時: 5:286365747451782
2973 ----- 插描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000728-----
2974 ***Pre-Screening開始****
2975 ***Pre-Screening結束****
2976 可能的攻擊方式: Label Specific Backdoor Attack
2977 可能的 target-victim 配對: ['13-0']
2978 ***Trigger Reverse Engineering開始****
2979 Target: 13, victim: 0, Loss: 13.6380, Acc: 0.00%, CE_Loss: 13.64, Reg_Loss:2548.91, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2536.98: 1% | 10/1000 [00:11<18:32, 1.12s/it]
2980 ***Trigger Reverse Engineering結束****

```

```

2981 Target Class: 13 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 11
2982 *****檢測結果*****檢測結果*****
2983 檢測結果: Model是安全的(Benign)
2984 整體耗時: 20.9816153049469
2985 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000729-----
2986 ***Pre-Screening開始*****
2987 ***Pre-Screening結束****
2988 ***檢測結束****
2989 檢測結果: Model是安全的(Benign)
2990 整體耗時: 5.113463640213013
2991 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000730-----
2992 ***Pre-Screening開始*****
2993 ***Pre-Screening結束****
2994 可能的攻擊方式: Label Specific Backdoor Attack
2995 可能的 target-victim 配對: ['0-4', '1-9', '4-0', '8-9', '8-10', '9-10']
2996 ***Trigger Reverse Engineering開始****
2997 Target: 8, victim: 9, Loss: 0.9708, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:1023.28, Cost:0.00 best_reg:1025.14 avg_loss_reg:1019.70: 60% [REDACTED] | 595/1000 [07:32<05:08, 1.31it/s]
2998 early stop 所有
2999 ***Trigger Reverse Engineering結束****
3000 Target Class: 8 Victim Class: 9 Trigger Size: 1023.2766723632812 Optimization Steps: 540
3001 *****檢測結束*****
3002 檢測結果: Model是安全的(Benign)
3003 整體耗時: 460.4918522834778
3004 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000731-----
3005 ***Pre-Screening開始*****
3006 ***Pre-Screening結束****
3007 可能的攻擊方式: Label Specific Backdoor Attack
3008 可能的 target-victim 配對: ['0-21', '0-22', '1-9', '1-10', '1-18', '2-7', '2-16', '3-2', '3-13', '4-17', '4-18', '5-6', '5-13', '5-16', '6-13', '6-16', '9-16', '9-2', '10-1', '11-18', '11-19', '13-5', '13-8', '14-1', '15-17', '16-2', '16-6', '16-7', '17-11', '17-15', '18-15', '18-21', '19-12', '19-15', '19-17', '20-0', '20-4', '20-21', '21-0', '21-20', '22-0', '22-20']
3009 ***Trigger Reverse Engineering開始****
3010 Target: 0, victim: 22, Loss: 1.0856, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:1439.53, Cost:0.00 best_reg:1442.64 avg_loss_reg:1444.89: 100% [REDACTED] | 997/1000 [09:25<00:01, 1.76it/s]
3011 early stop 所有
3012 ***Trigger Reverse Engineering結束****
3013 Target Class: 0 Victim Class: 22 Trigger Size: 1439.5318603515625 Optimization Steps: 256
3014 *****檢測結束*****
3015 檢測結果: Model是安全的(Benign)
3016 整體耗時: 572.6002960205078
3017 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000732-----
3018 ***Pre-Screening開始*****
3019 ***Pre-Screening結束****
3020 ***檢測結束****
3021 檢測結果: Model是安全的(Benign)
3022 整體耗時: 4.149557113647461
3023 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000733-----
3024 ***Pre-Screening開始*****
3025 ***Pre-Screening結束****
3026 可能的攻擊方式: Label Specific Backdoor Attack
3027 可能的 target-victim 配對: ['4-2', '4-9', '5-2']
3028 ***Trigger Reverse Engineering開始****
3029 Target: 4, victim: 9, Loss: 2.5614, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:44.31, Cost:0.06 best_reg:45.91 avg_loss_reg:44.52: 12% [REDACTED] | 123/1000 [05:22<38:20, 2.62s/it]
3030 early stop 所有
3031 ***Trigger Reverse Engineering結束****
3032 Target Class: 4 Victim Class: 9 Trigger Size: 44.307952880859375 Optimization Steps: 71
3033 ***Symmetric Check開始****
3034 Target: 9, victim: 4, Loss: 1.5890, Acc: 30.00%, CE_Loss: 1.59, Reg_Loss:22831.02, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:22714.28: 100% [REDACTED] | 71/71 [03:03<00:00, 2.59s/it]
3035 ***Symmetric Check結束*****
3036 *****檢測結束*****
3037 檢測結果: Model含有後門(Abnormal)
3038 整體耗時: 523.4543125629425
3039 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000734-----
3040 ***Pre-Screening開始*****
3041 ***Pre-Screening結束****
3042 可能的攻擊方式: Label Specific Backdoor Attack
3043 可能的 target-victim 配對: ['6-4']
3044 ***Trigger Reverse Engineering開始****
3045 Target: 6, victim: 4, Loss: 5.3666, Acc: 10.00%, CE_Loss: 5.37, Reg_Loss:3301.15, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3139.69: 2% | 120/1000 [00:03<02:43, 6.01it/s]
3046 ***Trigger Reverse Engineering結束****
3047 Target Class: 6 Victim Class: 4 Trigger Size: 10000000000.0 Optimization Steps: 21
3048 *****檢測結束*****
3049 檢測結果: Model是安全的(Benign)
3050 整體耗時: 8.137158155441284

```

```
3051 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000735-----  
3052 ***Pre-Screening開始***  
3053 ***Pre-Screening結束***  
3054 ***檢測結果結束***  
3055 檢測結果: Model是安全的(Benign)  
3056 整體耗時: 14.69479250907898  
3057 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000736-----  
3058 ***Pre-Screening開始***  
3059 ***Pre-Screening結束***  
3060 ***檢測結果結束***  
3061 檢測結果: Model是安全的(Benign)  
3062 整體耗時: 6.977197885513306  
3063 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000737-----  
3064 ***Pre-Screening開始***  
3065 ***Pre-Screening結束***  
3066 可能的攻擊方式: Label Specific Backdoor Attack  
3067 可能的 target-victim 配對: ['2-6', '2-9', '2-11', '5-6', '8-6', '9-2', '11-2']  
3068 ***Trigger Reverse Engineering 開始***  
3069 Target: 5; Victim: 6; Loss: 2.1440; Acc: 100.00%; CE_Loss: 0.14; Reg_Loss: 264.51; Cost: 0.01 best_reg: 267.42 avg_loss_reg: 267.42: 31%|████| 307/1000 [00:35<01:19, 8.71it/s]  
3070 early stop 所有  
3071 ***Trigger Reverse Engineering 結束***  
3072 Target Class: 5; Victim Class: 6; Trigger Size: 264.51239013671875 Optimization Steps: 156  
3073 ***Symmetric Check 開始***  
3074 Target: 6; victim: 5; Loss: 4.8885; Acc: 100.00%; CE_Loss: 0.28; Reg_Loss: 1366.86; Cost: 0.00 best_reg: 1375.47 avg_loss_reg: 1375.47: 100%|████| 156/156 [00:18<00:00, 8.44it/s]  
3075 ***Symmetric Check 結束***  
3076 *****檢測結果結束*****  
3077 檢測結果: Model是安全的(Benign)  
3078 整體耗時: 59.214218854904175  
3079 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000738-----  
3080 ***Pre-Screening開始***  
3081 ***Pre-Screening結束***  
3082 可能的攻擊方式: Universal Backdoor Attack  
3083 可能的 target class: 4  
3084 可能的 victim classes: ALL  
3085 ***Trigger Reverse Engineering 開始***  
3086
```