

```

1 C:\Users\slab\anaconda3\envs\pytorch1\python.exe D:\UULi\test_code\k_arm_test\main.py
2 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-0000000000
3 ***Pre-Screening開始***
4 可能的攻擊方式: Label Specific Backdoor Attack
5 可能的 target-victim 配對: ['5-4']
6 可能的 target-victim 配對: ['5-4']
7 ***Trigger Reverse Engineering開始***
8 Target: 5, victim: 4, Loss: 1.4645, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:584.51, Cost:0.00 best_reg:585.27 avg_loss_reg:585.27: 14% | 135/1000 [13:47<1:28:20, 6.13s/it]
9 early stop 所有
10 ***Trigger Reverse Engineering結束***
11 Target Class: 5 Victim Class: 4 Trigger Size: 584.5062866210938 Optimization Steps: 136
12 ***Symmetric Check開始***
13 Target: 4, victim: 5, Loss: 1.8918, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:527.20, Cost:0.00 best_reg:534.79 avg_loss_reg:534.79: 100% | 136/136 [13:45<00:00, 6.07s/it]
14 ***Symmetric Check結束***
15 *****檢測結果: Model是安全的(Benign)
16 檢測結果: Model是安全的(Benign)
17 整體耗時: 1664.0562598705292
18 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-0000000001
19 ***Pre-Screening開始***
20 ***Pre-Screening結束***
21 可能的攻擊方式: Label Specific Backdoor Attack
22 可能的 target-victim 配對: ['0-2', '2-0', '2-3', '3-2', '4-5', '5-4', '6-7', '6-9', '6-10', '7-3', '7-6', '7-8', '9-10', '10-9']
23 ***Trigger Reverse Engineering開始***
24 Target: 10, victim: 9, Loss: 3.8212, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:140.21, Cost:0.03 best_reg:143.06 avg_loss_reg:137.11: 38% | 385/1000 [05:36<08:57, 1.14it/s]
25 early stop 所有
26 ***Trigger Reverse Engineering結束***
27 Target Class: 10 Victim Class: 9 Trigger Size: 140.2120819091797 Optimization Steps: 116
28 ***Symmetric Check開始***
29 Target: 9, victim: 10, Loss: 5.9592, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:147.86, Cost:0.04 best_reg:148.80 avg_loss_reg:148.80: 85% | 99/116 [01:30<00:15, 1.10it/s]
30 early stop 所有
31 ***Symmetric Check結束***
32 *****檢測結果: Model是安全的(Benign)
33 檢測結果: Model是安全的(Benign)
34 整體耗時: 432.83162903785706
35 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-0000000002
36 ***Pre-Screening開始***
37 ***Pre-Screening結束***
38 可能的攻擊方式: Label Specific Backdoor Attack
39 可能的 target-victim 配對: ['0-3', '1-2', '1-12', '1-10', '2-3', '2-12', '2-17', '3-2', '5-13', '6-7', '7-8', '7-17', '9-3', '10-20', '12-2', '12-10', '12-11', '14-22', '14-11', '14-13', '15-13', '17-18', '18-12', '18-17', '19-21', '20-21', '21-17', '22-12', '22-13']
40 ***Trigger Reverse Engineering開始***
41 Target: 7, victim: 8, Loss: 0.9186, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:108.16, Cost:0.01 best_reg:108.97 avg_loss_reg:108.97: 54% | 542/1000 [14:20<12:07, 1.59s/it]
42 early stop 所有
43 ***Trigger Reverse Engineering結束***
44 Target Class: 7 Victim Class: 8 Trigger Size: 108.15702819824219 Optimization Steps: 128
45 ***Symmetric Check開始***
46 Target: 8, victim: 7, Loss: 4.2450, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:227.92, Cost:0.02 best_reg:229.15 avg_loss_reg:229.15: 93% | 119/128 [03:10<00:14, 1.60s/it]
47 early stop 所有
48 ***Symmetric Check結束***
49 *****檢測結果: Model是安全的(Benign)
50 檢測結果: Model是安全的(Benign)
51 整體耗時: 1061.66953086853033
52 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-0000000003
53 ***Pre-Screening開始***
54 ***Pre-Screening結束***
55 可能的攻擊方式: Label Specific Backdoor Attack
56 可能的 target-victim 配對: ['0-5', '3-2']
57 ***Trigger Reverse Engineering開始***
58 Target: 3, victim: 2, Loss: 8.2946, Acc: 0.00%, CE_Loss: 8.29, Reg_Loss:2535.91, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2525.93: 2% | 21/1000 [00:14<11:27, 1.42it/s]
59 ***Trigger Reverse Engineering結束***
60 Target Class: 0 Victim Class: 5 Trigger Size: 10000000000.0 Optimization Steps: 11
61 *****檢測結果: Model是安全的(Benign)
62 檢測結果: Model是安全的(Benign)
63 整體耗時: 16.350885152816772
64 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-0000000004
65 ***Pre-Screening開始***
66 ***Pre-Screening結束***
67 可能的攻擊方式: Label Specific Backdoor Attack
68 可能的 target-victim 配對: ['3-2']
69 ***Trigger Reverse Engineering開始***
70 Target: 3, victim: 2, Loss: 1.5550, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:87.41, Cost:0.02 best_reg:87.49 avg_loss_reg:87.08: 11% | 111/1000 [10:28<1:23:55, 5.66s/it]
71 0% | 0/112 [00:00 < ?, ?it/s]early stop 所有

```

```
72 ***Trigger Reverse Engineering 結束***  
73 Target Class: 3 Victim Class: 2 Trigger Size: 87.41078186035156 Optimization Steps: 112  
74 ***Symmetric Check開始***  
75 Target: 2, victim: 3, Loss: 3.2985, Acc: 95.00%, CE_Loss: 0.27, Reg_Loss:598.89, Cost:0.01 best_reg:623.76 avg_loss_reg:607.06: 100%|████████| 112/112 [10:08<00:00, 5.43s/it]  
76 ***Symmetric Check結束***  
77 *****檢測結束*****  
78 檢測結果: Model是安全的(Benign)  
79 整體耗時: 1248.842206478119  
80 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000005-----  
81 ***Pre-Screening開始***  
82 ***Pre-Screening結束***  
83 可能的攻擊方式: Label Specific Backdoor Attack  
84 可能的 target-victim 配對: [5-2]  
85 ***Trigger Reverse Engineering 開始***  
86 Target: 5, victim: 2, Loss: 1.9492, Acc: 100.00%, CE_Loss: 0.33, Reg_Loss:319.00, Cost:0.01 best_reg:319.39 avg_loss_reg:319.39: 18%|████| 175/1000 [09:53<46:39, 3.39s/it]  
87 early stop 所有  
88 ***Trigger Reverse Engineering 結束***  
89 Target Class: 5 Victim Class: 2 Trigger Size: 319.00030517578125 Optimization Steps: 176  
90 ***Symmetric Check開始***  
91 Target: 2, victim: 5, Loss: 1.1515, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:993.02, Cost:0.00 best_reg:980.25 avg_loss_reg:991.94: 100%|████████| 176/176 [09:54<00:00, 3.38s/it]  
92 ***Symmetric Check結束***  
93 *****檢測結束*****  
94 檢測結果: Model是安全的(Benign)  
95 整體耗時: 1193.2117941379547  
96 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000006-----  
97 ***Pre-Screening開始***  
98 ***Pre-Screening結束***  
99 ***檢測結束***  
100 檢測結果: Model是安全的(Benign)  
101 整體耗時: 19.261308908462524  
102 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000007-----  
103 ***Pre-Screening開始***  
104 ***Pre-Screening結束***  
105 可能的攻擊方式: Label Specific Backdoor Attack  
106 可能的 target-victim 配對: [0-1', '4-7', '7-4']  
107 ***Trigger Reverse Engineering 開始***  
108 Target: 4, victim: 7, Loss: 1.1163, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:207.17, Cost:0.01 best_reg:207.29 avg_loss_reg:207.35: 17%|████| 168/1000 [15:25<1:16:22, 5.51s/it]  
109 early stop 所有  
110 ***Trigger Reverse Engineering 結束***  
111 Target Class: 4 Victim Class: 7 Trigger Size: 207.17459106445312 Optimization Steps: 117  
112 ***Symmetric Check開始***  
113 Target: 7, victim: 4, Loss: 1.0057, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:3167.37, Cost:0.00 best_reg:3286.24 avg_loss_reg:3286.24: 100%|████████| 117/117 [10:34<00:00, 5.43s/it]  
114 ***Symmetric Check結束***  
115 *****檢測結束*****  
116 檢測結果: Model含有後門(Abnormal)  
117 整體耗時: 1572.5823483467102  
118 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000008-----  
119 ***Pre-Screening開始***  
120 ***Pre-Screening結束***  
121 ***檢測結束***  
122 檢測結果: Model是安全的(Benign)  
123 整體耗時: 5.416816234588623  
124 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000009-----  
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: [0-18', '0-19', '2-5', '2-12', '3-1', '5-6', '7-11', '8-7', '9-10', '10-7', '11-7', '12-5', '14-0', '14-13', '15-16', '16-15']  
129 ***Trigger Reverse Engineering 開始***  
130 Target: 11, victim: 7, Loss: 2.7093, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:498.94, Cost:0.01 best_reg:499.64 avg_loss_reg:499.64: 54%|████| 543/1000 [31:33<26:33, 3.49s/it]  
131 early stop 所有  
132 ***Trigger Reverse Engineering 結束***  
133 Target Class: 11 Victim Class: 7 Trigger Size: 498.9437255859375 Optimization Steps: 205  
134 ***Symmetric Check開始***  
135 Target: 7, victim: 11, Loss: 1.6747, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:295.83, Cost:0.01 best_reg:296.36 avg_loss_reg:296.63: 68%|████| 139/205 [08:05<03:50, 3.50s/it]  
136 early stop 所有  
137 ***Symmetric Check結束***  
138 *****檢測結束*****  
139 檢測結果: Model是安全的(Benign)  
140 整體耗時: 2393.040383049774  
141 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000010-----  
142 ***Pre-Screening開始***
```

```
143 ***Pre-Screening結束***  
144 可能的攻擊方式: Label Specific Backdoor Attack  
145 可能的 target-victim 配對: ['12-11', '13-11', '13-12']  
146 ***Trigger Reverse Engineering開始***  
147 Target: 13, victim: 11, Loss: 6.7275, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:373.24, Cost:0.02 best_reg:373.34 avg_loss_reg:373.34: 20%|████| 135/138 [04:18<00:05, 1.91s/it]  
148 early stop 所有  
149 ***Trigger Reverse Engineering結束***  
150 Target Class: 13 Victim Class: 11 Trigger Size: 373.2357482910156 Optimization Steps: 138  
151 ***Symmetric Check開始***  
152 Target: 11, victim: 13, Loss: 4.6726, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:260.59, Cost:0.02 best_reg:261.16 avg_loss_reg:261.16: 98%|████| 135/138 [04:18<00:05, 1.91s/it]  
153 early stop 所有  
154 ***Symmetric Check結束***  
155 *****檢測結果: Model是安全的(Benign)*****  
156 檢測結果: Model是安全的(Benign)  
157 整體耗時: 654.291360616684  
158 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000011-----  
159 ***Pre-Screening開始***  
160 ***Pre-Screening結束***  
161 可能的攻擊方式: Label Specific Backdoor Attack  
162 可能的 target-victim 配對: ['1-2', '3-5', '5-4', '6-7', '7-6', '8-0']  
163 ***Trigger Reverse Engineering開始***  
164 Target: 5, victim: 4, Loss: 0.3666, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:123.57, Cost:0.00 best_reg:124.44 avg_loss_reg:124.44: 46%|████| 463/1000 [07:53<09:09, 1.02s/it]  
165 early stop 所有  
166 ***Trigger Reverse Engineering結束***  
167 Target Class: 5 Victim Class: 4 Trigger Size: 123.57212829589844 Optimization Steps: 223  
168 ***Symmetric Check開始***  
169 Target: 4, victim: 5, Loss: 2.9841, Acc: 100.00%, CE_Loss: 0.65, Reg_Loss:461.88, Cost:0.01 best_reg:465.64 avg_loss_reg:468.02: 75%|████| 168/223 [02:52<00:56, 1.02s/it]  
170 early stop 所有  
171 ***Symmetric Check結束***  
172 *****檢測結果: Model是安全的(Benign)*****  
173 檢測結果: Model是安全的(Benign)  
174 整體耗時: 651.2950201034546  
175 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000012-----  
176 ***Pre-Screening開始***  
177 ***Pre-Screening結束***  
178 可能的攻擊方式: Label Specific Backdoor Attack  
179 可能的 target-victim 配對: ['17-15']  
180 ***Trigger Reverse Engineering開始***  
181 Target: 17, victim: 15, Loss: 1.6195, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:659.15 avg_loss_reg:659.15: 14%|████| 145/1000 [07:31<44:24, 3.12s/it]  
182 early stop 所有  
183 ***Trigger Reverse Engineering結束***  
184 Target Class: 17 Victim Class: 15 Trigger Size: 657.82916259776562 Optimization Steps: 146  
185 ***Symmetric Check開始***  
186 Target: 15, victim: 17, Loss: 4.8683, Acc: 95.00%, CE_Loss: 0.28, Reg_Loss:1358.57, Cost:0.00 best_reg:1383.04 avg_loss_reg:1343.11: 100%|████| 146/146 [07:32<00:00, 3.10s/it]  
187 ***Symmetric Check結束***  
188 *****檢測結果: Model是安全的(Benign)*****  
189 檢測結果: Model是安全的(Benign)  
190 整體耗時: 917.2007367610931  
191 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000013-----  
192 ***Pre-Screening開始***  
193 ***Pre-Screening結束***  
194 可能的攻擊方式: Label Specific Backdoor Attack  
195 可能的 target-victim 配對: ['1-8', '2-1', '2-6']  
196 ***Trigger Reverse Engineering開始***  
197 Target: 2, victim: 6, Loss: 9.8620, Acc: 0.00%, CE_Loss: 9.86, Reg_Loss:2546.91, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2532.89: 3%|████| 32/1000 [00:20<10:09, 1.59s/it]  
198 ***Trigger Reverse Engineering結束***  
199 Target Class: 1 Victim Class: 8 Trigger Size: 1000000000.0 Optimization Steps: 11  
200 *****檢測結果: Model是安全的(Benign)*****  
201 檢測結果: Model是安全的(Benign)  
202 整體耗時: 22.319307804107666  
203 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000014-----  
204 ***Pre-Screening開始***  
205 ***Pre-Screening結束***  
206 ***檢測結束***  
207 檢測結果: Model是安全的(Benign)  
208 整體耗時: 8.74295115410862  
209 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000015-----  
210 ***Pre-Screening開始***  
211 ***Pre-Screening結束***  
212 可能的攻擊方式: Label Specific Backdoor Attack  
213 可能的 target-victim 配對: ['1-2', '4-5', '5-0', '5-4']
```

```
214 ***Trigger Reverse Engineering 開始***  
215 Target: 1, victim: 2, Loss: 0.5308, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:201.77, Cost:0.00 best_reg:219.76 avg_loss_reg:200.34: 22% █ | 216/1000 [12:38<45:53, 3.51s/t]  
216 early stop 所有  
217 ***Trigger Reverse Engineering 結束***  
218 Target Class: 1 Victim Class: 2 Trigger Size: 201.76866149902344 Optimization Steps: 151  
219 ***Symmetric Check開始***  
220 Target: 2, victim: 1, Loss: 1.7600, Acc: 90.00%, CE_Loss: 0.17, Reg_Loss:209.71, Cost:0.01 best_reg:214.07 avg_loss_reg:211.19: 100% █ | 151/151 [09:15<00:00, 3.68s/t]  
221 ***Symmetric Check結束***  
222 *****檢測結束*****  
223 檢測結果: Model是安全的(Benign)  
224 整體耗時: 13221.1608629226685
```

```
225 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000016-----  
226 ***Pre-Screening 開始***  
227 可能的攻擊方式: Universal Backdoor Attack  
228 可能的 target class: 14  
229 可能的 victim classes: ALL  
230 可能的 target-victim 配對: [1-0, '7-4', '9-7', '9-10', '10-9', '10-14', '11-12', '13-2']  
231 ***Trigger Reverse Engineering 開始***  
232 Target: 14, victim: 12, Loss: 0.8590, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:169.67, Cost:0.01 best_reg:168.77 avg_loss_reg:169.71: 10% █ | 98/1000 [42:57<6:35:23, 26.305/t]  
233 early stop 所有  
234 ***Trigger Reverse Engineering 結束***  
235 Target Class: 14 Victim Class: all Trigger Size: 168.7716735839438 Optimization Steps: 99  
236 *****檢測結束*****  
237 檢測結果: Model含有後門(Abnormal)  
238 整體耗時: 2587.3155765533447  
239 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000017-----  
240 ***Pre-Screening 開始***  
241 ***Pre-Screening 結束***  
242 可能的攻擊方式: Label Specific Backdoor Attack  
243 可能的 target-victim 配對: ['1-0', '7-4', '9-7', '9-10', '10-9', '10-14', '11-12', '13-2']  
244 ***Trigger Reverse Engineering 開始***  
245 Target: 10, victim: 9, Loss: 4.2454, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:348.40, Cost:0.01 best_reg:348.97 avg_loss_reg:348.97: 23% █ | 228/1000 [03:03<10:20, 1.24it/s]  
246 early stop 所有  
247 ***Trigger Reverse Engineering 結束***  
248 Target Class: 9 Victim Class: 9 Trigger Size: 348.40411376953 25 Optimization Steps: 119  
249 ***Symmetric Check開始***  
250 Target: 9, victim: 10, Loss: 3.4414, Acc: 90.00%, CE_Loss: 0.27, Reg_Loss:278.01, Cost:0.01 best_reg:282.17 avg_loss_reg:282.17: 100% █ | 119/119 [01:35<00:00, 1.25it/s]  
251 ***Symmetric Check結束***  
252 *****檢測結束*****  
253 檢測結果: Model是安全的(Benign)  
254 整體耗時: 283.29552268981934  
255 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000018-----  
256 ***Pre-Screening 開始***  
257 ***Pre-Screening 結束***  
258 可能的攻擊方式: Label Specific Backdoor Attack  
259 可能的 target-victim 配對: ['3-7', '3-6', '3-5']  
260 ***Trigger Reverse Engineering 開始***  
261 Target: 3, victim: 5, Loss: 1.4272, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:10.75, Cost:0.01 best_reg:11.96 avg_loss_reg:11.96: 10% █ | 100/1000 [00:31<04:42, 3.19it/s]  
262 0% | 0/65 [00:00:<?, ?]it/searly stop 所有  
263 ***Trigger Reverse Engineering 結束***  
264 Target Class: 3 Victim Class: 5 Trigger Size: 10.745586395263672 Optimization Steps: 65  
265 *****檢測結束*****  
266 Target: 5, victim: 3, Loss: 18.6709, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:1613.43, Cost:0.01 best_reg:1688.66 avg_loss_reg:1688.66: 100% █ | 65/65 [00:20<00:00, 3.21it/s]  
267 ***Symmetric Check結束***  
268 *****檢測結束*****  
269 檢測結果: Model含有後門(Abnormal)  
270 整體耗時: 56.46527862548828  
271 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000019-----  
272 ***Pre-Screening 開始***  
273 ***Pre-Screening 結束***  
274 可能的攻擊方式: Label Specific Backdoor Attack  
275 可能的 target-victim 配對: ['4-5', '6-0', '6-12', '8-0', '12-15', '14-0', '15-12']  
276 ***Trigger Reverse Engineering 開始***  
277 Target: 4, victim: 5, Loss: 3.1536, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:264.26, Cost:0.01 best_reg:265.94 avg_loss_reg:265.94: 25% █ | 253/1000 [22:19<1:05:54, 5.29s/t]  
278 early stop 所有  
279 ***Trigger Reverse Engineering 結束***  
280 Target Class: 4 Victim Class: 5 Trigger Size: 264.2559509277344 Optimization Steps: 128  
281 ***Symmetric Check開始***  
282 Target: 5, victim: 4, Loss: 95.00%, CE_Loss: 0.26, Reg_Loss:546.21, Cost:0.01 best_reg:558.34 avg_loss_reg:550.76: 100% █ | 128/128 [11:30<00:00, 5.39s/t]  
283 ***Symmetric Check結束***  
284 *****檢測結束*****
```

```
285 檢測結果: Model是安全的(Benign)
286 整體耗時: 2044.8717439174652 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000020-----
287     ***Pre-Screening開始***
288     ***Pre-Screening結束***
289     可能的攻擊方式: Label Specific Backdoor Attack
290     可能的 target-victim 配對: ['1-5', '2-4']
291     ***Trigger Reverse Engineering開始***
292     Target: 2, victim: 4, Loss: 3.4585, Acc: 0.00%, CE_Loss: 3.46, Reg_Loss:2497.30, Cost:0.00 best_Reg:10000000000.00 avg_loss_Reg:2498.32: 2%| | 21/1000 [00:12<09:43, 1.68s/it]
293     Target Class: 1 Victim Class: 5 Trigger Size: 10000000000 Optimization Steps: 11
294     ***Trigger Reverse Engineering結束***
295     Target Class: 1 Victim Class: 5 Trigger Size: 10000000000 Optimization Steps: 11
296     *****檢測結果*****
297     檢測結果: Model是安全的(Benign)
298     整體耗時: 14.646475076675415 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000021-----
299     ***Pre-Screening開始***
300     ***Pre-Screening結束***
301     可能的攻擊方式: Universal Backdoor Attack
302     可能的 victim classes: ALL
303     可能的 target class: 21
304     可能的 victim classes: ALL
305     ***Trigger Reverse Engineering結束***
306     Target: 21, victim: 20, Loss: 0.4411, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:87.14, Cost:0.01 best_Reg:84.86 avg_loss_Reg:87.02: 8%| | 76/1000 [2:11:48<26:42:25, 104.05s/it]
307     early stop 所有
308     ***Trigger Reverse Engineering結束***
309     Target Class: 21 Victim Class: all Trigger Size: 84.85630852835519 Optimization Steps: 77
310     *****檢測結果*****
311     檢測結果: Model含有後門(Abnormal)
312     整體耗時: 7934.120084285736 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000022-----
313     ***Pre-Screening開始***
314     ***Pre-Screening結束***
315     可能的攻擊方式: Label Specific Backdoor Attack
316     可能的 target-victim 配對: [0-18', '3-2', '10-13', '12-13', '12-18', '19-21', '20-18']
317     ***Trigger Reverse Engineering開始***
318     Target Class: 12 Victim Class: 18 Trigger Size: 44.44329833984375 Optimization Steps: 87
319     Target: 12, victim: 18, Loss: 2.6564, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:44.44, Cost:0.06 best_Reg:46.24 avg_loss_Reg:46.24: 27%| | 268/1000 [19:27<53:07, 4.35s/it]
320     early stop 所有
321     ***Trigger Reverse Engineering結束***
322     Target Class: 12 Victim Class: 18 Trigger Size: 44.44329833984375 Optimization Steps: 87
323     ***Symmetric Check開始***
324     Target: 18, victim: 12, Loss: 1.2199, Acc: 55.00%, CE_Loss: 1.22, Reg_Loss:8156.61, Cost:0.00 best_Reg:10000000000.00 avg_loss_Reg:8085.12: 100%| | 87/87 [06:20<00:00, 4.37s/it]
325     ***Symmetric Check結束*****
326     *****檢測結果*****
327     檢測結果: Model含有後門(Abnormal)
328     整體耗時: 1570.797575712204 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000023-----
329     ***Pre-Screening開始***
330     ***Pre-Screening結束***
331     可能的攻擊方式: Label Specific Backdoor Attack
332     可能的 target-victim 配對: ['3-6', '3-2', '3-5']
333     ***Trigger Reverse Engineering開始***
334     Target: 3, victim: 6, Loss: 0.7519, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:26.55, Cost:0.03 best_Reg:26.63 avg_loss_Reg:27.02: 14%| | 140/1000 [13:22<1:22:10, 5.73s/it]
335     early stop 所有
336     ***Trigger Reverse Engineering結束***
337     Target Class: 3 Victim Class: 6 Trigger Size: 26.55321502685547 Optimization Steps: 92
338     ***Symmetric Check開始***
339     Target: 6, victim: 3, Loss: 1.9374, Acc: 95.00%, CE_Loss: 0.30, Reg_Loss:729.84, Cost:0.00 best_Reg:818.32 avg_loss_Reg:740.86: 100%| | 92/92 [08:42<00:00, 5.67s/it]
340     ***Symmetric Check結束*****
341     檢測結果: Model含有後門(Abnormal)
342     整體耗時: 1338.4169886112213 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000024-----
343     ***Pre-Screening開始***
344     ***Pre-Screening結束***
345     可能的攻擊方式: Label Specific Backdoor Attack
346     可能的 target-victim 配對: ['2-3', '3-4', '4-2', '4-3', '4-11', '5-6', '5-12', '6-5', '6-12', '7-8', '8-7', '9-8', '10-11', '11-9']
347     ***Trigger Reverse Engineering開始***
348     Target: 3, victim: 4, Loss: 4.2179, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:31.57, Cost:0.13 best_Reg:33.03 avg_loss_Reg:33.03: 44%| | 439/1000 [07:37<09:45, 1.04s/it]
349     0%| | 0/84 [00:00:<, ?it]early stop 所有
350     ***Trigger Reverse Engineering結束***
351     Target Class: 3 Victim Class: 4 Trigger Size: 31.574466705322266 Optimization Steps: 84
352     ***Symmetric Check開始***
353     Target Class: 3 Victim Class: 4 Trigger Size: 31.574466705322266 Optimization Steps: 84
354     ***Symmetric Check結束***
```

```

356 Target: 4, victim: 3, Loss: 5.1056, Acc: 90.00%, CE_Loss: 0.37, Reg_Loss:184.75, Cost:0.03 best_reg:205.92 avg_loss_reg:193.42: 100% |████████| 84/84 [01:27 < 00:00, 1.04s/it]
357 ***Symmetric Check結束*** 
358 *****檢測結束***** 
359 檢測結果: Model是安全的(Benign)
360 整體耗時: 550.8776593208313
361 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000025-----
362 ***Pre-Screening開始*** 
363 可能的攻擊方式: Label Specific Backdoor Attack
364 可能的 target-victim 配對: [5-8', 7-6']
365 ***Trigger Reverse Engineering開始*** 
366 Target: 5, victim: 8, Loss: 2.1796, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:606.92, Cost:0.00 best_reg:607.36 avg_loss_reg:606.73: 22% |████| 220/1000 [05:51 < 20:45, 1.60s/it]
367 0% | 0/200 [00:00 < ?, ?it/s]early stop 所有
368 ***Trigger Reverse Engineering結束*** 
369 Target Class: 5 Victim Class: 8 Trigger Size: 606.9244384765625 Optimization Steps: 200
370 Target Class: 8, victim: 5, Loss: 1.2477, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:347.26, Cost:0.00 best_reg:349.28 avg_loss_reg:349.28: 88% |████| 177/200 [04:43 < 00:36, 1.60s/it]
371 ***Symmetric Check開始*** 
372 Target: 8, victim: 5, Loss: 1.2477, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:347.26, Cost:0.00 best_reg:349.28 avg_loss_reg:349.28: 88% |████| 177/200 [04:43 < 00:36, 1.60s/it]
373 early stop 所有
374 ***Symmetric Check結束*** 
375 *****檢測結束***** 
376 檢測結果: Model是安全的(Benign)
377 整體耗時: 641.4115657806396
378 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000026-----
379 ***Pre-Screening開始*** 
380 ***Pre-Screening結束*** 
381 可能的攻擊方式: Label Specific Backdoor Attack
382 可能的 target-victim 配對: [0-16', 1-0', 1-3', 3-15', 5-16', 8-6', 8-7', 8-10', 9-10', 9-11', 11-10', 13-15', 13-17', 15-17', 17-6', 17-15', 19-12]
383 ***Trigger Reverse Engineering開始*** 
384 Target: 13, victim: 15, Loss: 1.0026, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:89.82, Cost:0.01 best_reg:90.90 avg_loss_reg:88.78: 59% |████| 590/1000 [41:26 < 28:47, 4.21s/it]
385 early stop 所有
386 ***Trigger Reverse Engineering結束*** 
387 Target Class: 13 Victim Class: 15 Trigger Size: 89.81779479980469 Optimization Steps: 260
388 ***Symmetric Check開始*** 
389 Target: 15, victim: 13, Loss: 1.8935, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:519.75, Cost:0.00 best_reg:520.46 avg_loss_reg:520.46: 58% |████| 152/260 [11:02 < 07:50, 4.36s/it]
390 early stop 所有
391 ***Symmetric Check結束*** 
392 *****檢測結束***** 
393 檢測結果: Model是安全的(Benign)
394 整體耗時: 3163.8967386212921
395 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000027-----
396 ***Pre-Screening開始*** 
397 ***Pre-Screening結束*** 
398 ***檢測結束*** 
399 檢測結果: Model是安全的(Benign)
400 整體耗時: 7.04800009927478
401 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000028-----
402 ***Pre-Screening開始*** 
403 ***Pre-Screening結束*** 
404 可能的攻擊方式: Label Specific Backdoor Attack
405 可能的 target-victim 配對: [0-3', 3-4', 4-5']
406 ***Trigger Reverse Engineering開始*** 
407 Target: 4, victim: 5, Loss: 12.9612, Acc: 0.00%, CE_Loss: 12.96, Reg_Loss:2564.29, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2547.72: 4% |████| 42/1000 [03:45 < 1:25:37, 5.36s/it]
408 ***Trigger Reverse Engineering結束*** 
409 Target Class: 0 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 21
410 *****檢測結束***** 
411 檢測結果: Model是安全的(Benign)
412 整體耗時: 234.15252161026
413 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000029-----
414 ***Pre-Screening開始*** 
415 ***Pre-Screening結束*** 
416 可能的攻擊方式: Label Specific Backdoor Attack
417 可能的 target-victim 配對: [0-1', 0-20', 1-0', 1-12', 1-14', 3-4', 3-6', 4-6', 5-4', 6-3', 6-4', 7-8', 7-9', 7-10', 8-2', 8-3', 8-15', 9-2', 9-16', 9-8', 10-7', 10-9', 10-11', 11-12', 11-13', 12-11', 13-11', 13-20', 13-4', 14-15', 15-16', 15-19', 16-19', 16-17', 15', 19-17]
418 ***Trigger Reverse Engineering開始*** 
419 Target: 11, victim: 12, Loss: 15.9272, Acc: 95.00%, CE_Loss: 0.20, Reg_Loss:409.13, Cost:0.04 best_reg:466.65 avg_loss_reg:466.65: 100% |████████| 1000/1000 [17:02 < 00:00, 1.02s/it]
420 ***Trigger Reverse Engineering結束*** 
421 Target Class: 11 Victim Class: 12 Trigger Size: 466.6546936035156 Optimization Steps: 68
422 ***Symmetric Check開始*** 
423 Target: 12, victim: 11, Loss: 8.0876, Acc: 95.00%, CE_Loss: 0.30, Reg_Loss:1537.52, Cost:0.01 best_reg:1754.22 avg_loss_reg:1573.05: 100% |████| 68/68 [01:07 < 00:00, 1.00s/it]
424 ***Symmetric Check結束*** 
425 *****檢測結束***** 

```

```
426 檢測結果: Model是安全的(Benign)
427 整體耗時: 1097.9811899662018 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000030-----
428 ***Pre-Screening開始****
429 ***Pre-Screening結束****
430 可能的攻擊方式: Label Specific Backdoor Attack
431 可能的 target-victim 配對: ['7-1', '7-6']
432 ***Trigger Reverse Engineering開始****
433 Target: 7, victim: 6, Loss: 1.0043, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:42.75, Cost:0.02 best_reg:44.51 avg_loss_reg:42.55: 12%| | 122/1000 [03:36<25:54, 1.77s/t]
434 Target: 7, victim: 6, Loss: 1.0043, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:42.75, Cost:0.02 best_reg:44.51 avg_loss_reg:42.55: 12%| | 122/1000 [03:36<25:54, 1.77s/t]
435 early stop 所有
436 ***Trigger Reverse Engineering結束****
437 Target Class: 7 Victim Class: 6 Trigger Size:42.750850677490234 Optimization Steps: 112
438 ***Symmetric Check開始****
439 Target: 6, victim: 7, Loss: 0.5270, Acc: 90.00%, CE_Loss: 0.41, Reg_Loss:1323.80, Cost:0.00 best_reg:4083.97 avg_loss_reg:1314.18: 100%| | 112/112 [03:24<00:00, 1.83s/t]
440 ***Symmetric Check結束****
441 *****檢測結束*****
442 檢測結果: Model含有後門(Abnormal)
443 整體耗時: 424.00752115249634 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000031-----
444 *****Pre-Screening開始****
445 *****Pre-Screening結束****
446 可能的攻擊方式: Label Specific Backdoor Attack
447 可能的 target-victim 配對: ['5-6', '5-7', '6-5']
448 ***Trigger Reverse Engineering開始****
449 Target: 6, victim: 5, Loss: 1.2770, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:227.56, Cost:0.01 best_reg:227.56 avg_loss_reg:228.84: 18%| | 184/1000 [16:16<1:12:11, 5.31s/t]
450 Target: 5, victim: 6, Loss: 1.0506, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:424.79, Cost:0.00 best_reg:420.95 avg_loss_reg:425.13: 100%| | 131/131 [11:33<00:00, 5.30s/t]
451 early stop 所有
452 ***Trigger Reverse Engineering結束****
453 Target Class: 6 Victim Class: 5 Trigger Size:227.56475830078125 Optimization Steps: 131
454 ***Symmetric Check開始****
455 Target: 5, victim: 6, Loss: 1.0506, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:424.79, Cost:0.00 best_reg:4228.84 avg_loss_reg:4228.84: 18%| | 184/1000 [16:16<1:12:11, 5.31s/t]
456 檢測結果: Model是安全的(Benign)
457 *****檢測結束*****
458 檢測結果: Model是安全的(Benign)
459 整體耗時: 1680.543764591217 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000032-----
460 *****Pre-Screening開始****
461 *****Pre-Screening結束****
462 可能的攻擊方式: Label Specific Backdoor Attack
463 可能的 target-victim 配對: ['1-5', '1-6', '1-8', '2-3', '3-2', '4-5', '6-15', '7-1', '7-11', '7-12', '8-10', '9-8', '9-11', '10-15', '11-7', '12-13', '12-14', '13-12', '13-14', '14-12', '14-5', '14-13', '15-10']
464 ***Trigger Reverse Engineering開始****
465 Target: 2, victim: 3, Loss: 3.2788, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:266.66, Cost:0.01 best_reg:267.09 avg_loss_reg:267.09: 52%| | 523/1000 [27:40<25:14, 3.18s/t]
466 Target: 2, victim: 3, Loss: 3.2788, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:266.66, Cost:0.01 best_reg:267.09 avg_loss_reg:267.09: 52%| | 523/1000 [27:40<25:14, 3.18s/t]
467 early stop 所有
468 ***Trigger Reverse Engineering結束****
469 Target Class: 2 Victim Class: 3 Trigger Size:266.6648254394531 Optimization Steps: 116
470 ***Symmetric Check開始****
471 Target: 3, victim: 2, Loss: 3.9591, Acc: 100.00%, CE_Loss: 0.34, Reg_Loss:476.82, Cost:0.01 best_reg:479.48 avg_loss_reg:479.52: 100%| | 116/116 [05:53<00:00, 3.05s/t]
472 *****檢測結束*****
473 *****檢測結束*****
474 檢測結果: Model是安全的(Benign)
475 整體耗時: 2026.1261434555054 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000033-----
476 *****Pre-Screening開始****
477 *****Pre-Screening結束****
478 可能的攻擊方式: Label Specific Backdoor Attack
479 可能的 target-victim 配對: ['5-6', '6-5']
480 ***Trigger Reverse Engineering開始****
481 Target: 5, victim: 6, Loss: 6.4207, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:240.92, Cost:0.03 best_reg:242.48 avg_loss_reg:242.48: 15%| | 150/1000 [07:31<42:37, 3.01s/t]
482 Target: 5, victim: 6, Loss: 6.4207, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:240.92, Cost:0.03 best_reg:242.48 avg_loss_reg:242.48: 15%| | 150/1000 [07:31<42:37, 3.01s/t]
483 early stop 所有
484 ***Trigger Reverse Engineering結束****
485 Target Class: 5 Victim Class: 6 Trigger Size:240.91769409179688 Optimization Steps: 106
486 ***Symmetric Check開始****
487 Target: 6, victim: 5, Loss: 4.2776, Acc: 90.00%, CE_Loss: 0.37, Reg_Loss:515.20, Cost:0.01 best_reg:523.25 avg_loss_reg:517.95: 100%| | 106/106 [05:30<00:00, 3.11s/t]
488 *****檢測結束*****
489 *****檢測結束*****
490 檢測結果: Model是安全的(Benign)
491 整體耗時: 790.4845879077911 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000034-----
492 *****Pre-Screening開始****
493 *****Pre-Screening結束****
494 可能的攻擊方式: Label Specific Backdoor Attack
495 可能的 target-victim 配對: ['4-5', '4-6', '7-1', '7-4']
```

```

497 ***Trigger Reverse Engineering 開始***  

498 Target: 7, victim: 4, Loss: 2.4180, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss: 61.43, Cost: 0.04 best_reg:63.77 avg_loss_reg:62.13: 12% █ | 117/1000 [10:45<1:21:13, 5.52s/it]  

499 early stop 所有  

500 ***Trigger Reverse Engineering 結束***  

501 Target Class: 7 Victim Class: 4 Trigger Size: 61.42675018310547 Optimization Steps: 73  

502 ***Symmetric Check開始***  

503 Target: 4, victim: 7, Loss: 0.1955, Acc: 95.00%, CE_Loss: 0.20, Reg_Loss: 9030.64, Cost: 0.00 best_reg:10000000000.00 avg_loss_reg:8933.84: 100% █ | 73/73 [06:37<0:00:00, 5.45s/it]  

504 ***Symmetric Check結束***  

505 *****檢測結束*****  

506 檢測結果: Model含有後門(Abnormal)  

507 整體耗時: 1052.5545837187918  

508 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000035-----  

509 ***Pre-Screening 開始***  

510 ***Pre-Screening 結束***  

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

512 可能的 target-victim 配對: ['0-1', '3-13', '4-5', '5-4', '5-6', '9-10', '12-4', '12-13', '13-14', '14-13', '15-2', '15-8', '17-11']  

513 ***Trigger Reverse Engineering 開始***  

514 Target: 12, victim: 4, Loss: 1.5888, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss: 128.21, Cost: 0.01 best_reg:128.68 avg_loss_reg:128.68: 39% █ | 386/1000 [05:08<08:10, 1.25s/it]  

515 early stop 所有  

516 ***Trigger Reverse Engineering 結束***  

517 Target Class: 12 Victim Class: 4 Trigger Size: 128.20550537109375 Optimization Steps: 89  

518 ***Symmetric Check開始***  

519 Target: 4, victim: 12, Loss: 9.2024, Acc: 90.00%, CE_Loss: 0.45, Reg_Loss: 5833.84, Cost: 0.00 best_reg:6623.27 avg_loss_reg:6209.74: 100% █ | 89/89 [01:11<00:00, 1.25s/it]  

520 ***Symmetric Check結束***  

521 *****檢測結束*****  

522 檢測結果: Model含有後門(Abnormal)  

523 整體耗時: 386.32221673965454  

524 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000036-----  

525 ***Pre-Screening 開始***  

526 ***Pre-Screening 結束***  

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

528 可能的 target-victim 配對: ['3-1', '3-13', '4-3', '10-12', '11-12', '11-15', '16-15']  

529 ***Trigger Reverse Engineering 開始***  

530 Target: 3, victim: 1, Loss: 1.4200, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss: 52.12, Cost: 0.03 best_reg:52.92 avg_loss_reg:52.92: 30% █ | 301/1000 [26:02<1:00:29, 5.19s/it]  

531 early stop 所有  

532 ***Trigger Reverse Engineering 結束***  

533 Target Class: 3 Victim Class: 1 Trigger Size: 52.11592102050781 Optimization Steps: 77  

534 ***Symmetric Check開始***  

535 Target: 1, victim: 3, Loss: 2.4761, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss: 2354.79, Cost: 0.00 best_reg:2431.72 avg_loss_reg:2431.72: 100% █ | 77/77 [06:47<00:00, 5.19s/it]  

536 *****檢測結束*****  

537 *****檢測結束*****  

538 檢測結果: Model含有後門(Abnormal)  

539 整體耗時: 1985.7354328632355  

540 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000037-----  

541 ***Pre-Screening 開始***  

542 ***Pre-Screening 結束***  

543 ***檢測結束***  

544 檢測結果: Model是安全的(Benign)  

545 整體耗時: 2.1266300678253174-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000038-----  

546 ***Pre-Screening 開始***  

547 ***Pre-Screening 結束***  

548 ***Pre-Screening 結束***  

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

550 可能的 target-victim 配對: ['3-2']  

551 ***Trigger Reverse Engineering 開始***  

552 Target: 3, victim: 2, Loss: 14.0997, Acc: 0.00%, CE_Loss: 14.10, Reg_Loss: 2525.27, Cost: 0.00 best_reg:10000000000.00 avg_loss_reg:2516.15: 1% | 10/1000 [00:34<56:42, 3.44s/it]  

553 ***Trigger Reverse Engineering 結束***  

554 Target Class: 3 Victim Class: 2 Trigger Size: 1000000000.0 Optimization Steps: 11  

555 *****檢測結束*****  

556 檢測結果: Model是安全的(Benign)  

557 整體耗時: 39.14864802360535-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000039-----  

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: ['1-0', '6-1']  

562 ***Trigger Reverse Engineering 開始***  

563 Target: 1, victim: 0, Loss: 4.1925, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss: 234.74, Cost: 0.02 best_reg:236.12 avg_loss_reg:236.12: 12% █ | 125/1000 [15:53<1:51:12, 7.63s/it]  

564 Target Class: 0 Victim Class: 0 Trigger Size: 234.73757934570312 Optimization Steps: 115  

565 early stop 所有  

566 ***Trigger Reverse Engineering 結束***  

567 Target Class: 1 Victim Class: 1 Trigger Size: 0 Optimization Steps: 115

```

```

568 ***Symmetric Check開始***  

569 Target: 0, victim: 1, Loss: 2.3691, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:961.51, Cost:0.00 best_reg:963.48 avg_loss_reg:963.48: 100% | [115/115 [14:31<00:00, 7.58s/it]  

570 ***Symmetric Check結束***  

571 *****檢測結果: Model是安全的(Benign)  

572 整體耗時: 1859.352138519287  

573  

574 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000040-----  

575 ***Pre-Screening開始***  

576 ***Pre-Screening結束***  

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

578 可能的 target-victim 配對: ['1-4', '3-2', '6-7']  

579 ***Trigger Reverse Engineering開始***  

580 Target: 3, victim: 2, Loss: 4.5895, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:77.42, Cost:0.06 best_reg:80.62 avg_loss_reg:80.62: 15% | 146/1000 [01:46<10:23, 1.37it/s]  

581 0% | 0/95 [00:00 < ?, ?it/s]early stop 所有  

582 ***Trigger Reverse Engineering結束***  

583 Target Class: 3 Victim Class: 2 Trigger Size:77.41842651367188 Optimization Steps: 95  

584 ***Symmetric Check開始***  

585 Target: 2, victim: 3, Loss: 8.6492, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:145.14, Cost:0.06 best_reg:147.24 avg_loss_reg:147.24: 97% | 92/95 [01:07<00:02, 1.36it/s]  

586 early stop 所有  

587 ***Symmetric Check結束***  

588 *****檢測結束*****  

589 檢測結果: Model是安全的(Benign)  

590 整體耗時: 178.9745192527771-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000041-----  

591  

592 ***Pre-Screening開始***  

593 ***Pre-Screening結束***  

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

595 可能的 target-victim 配對: ['2-3', '4-20', '6-5', '6-7', '8-9', '10-11', '11-10', '11-5', '11-19', '12-11', '12-7', '12-13', '13-15', '13-20', '14-10', '14-12', '15-12', '15-13', '17-19']  

596 ***Trigger Reverse Engineering開始***  

597 Target: 12, victim: 7, Loss: 1.0420, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:35.25, Cost:0.03 best_reg:42.20 avg_loss_reg:35.34: 52% | 520/1000 [45:44<42:13, 5.28s/it]  

598 early stop 所有  

599 ***Trigger Reverse Engineering結束***  

600 Target Class: 12 Victim Class: 7 Trigger Size: 35.25355911254883 Optimization Steps: 99  

601 ***Symmetric Check開始***  

602 Target: 7, victim: 12, Loss: 1.4433, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:2587.32, Cost:0.00 best_reg:2607.61 avg_loss_reg:2607.91: 100% | 99/99 [08:57<00:00, 5.43s/it]  

603 *****檢測結束*****  

604 ***Symmetric Check結束***  

605 檢測結果: Model含有後門(Abnormal)  

606 整體耗時: 3303.74055047989-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000042-----  

607  

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: ['3-5', '3-6']  

612 ***Trigger Reverse Engineering開始***  

613 Target: 3, victim: 5, Loss: 5.2590, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:127.81, Cost:0.04 best_reg:130.82 avg_loss_reg:130.82: 11% | 112/1000 [04:44<37:37, 2.54s/it]  

614 early stop 所有  

615 ***Trigger Reverse Engineering結束***  

616 Target Class: 3 Victim Class: 5 Trigger Size: 127.80994415283203 Optimization Steps: 102  

617 ***Symmetric Check開始***  

618 Target: 5, victim: 3, Loss: 3.7109, Acc: 80.00%, CE_Loss: 0.36, Reg_Loss:441.58, Cost:0.01 best_reg:467.91 avg_loss_reg:446.05: 100% | 102/102 [04:09<00:00, 2.45s/it]  

619 *****檢測結束*****  

620 ***Symmetric Check結束***  

621 檢測結果: Model是安全的(Benign)  

622 整體耗時: 540.8245801925659-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000043-----  

623  

624 ***Pre-Screening開始***  

625 ***Pre-Screening結束***  

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

627 可能的 target-victim 配對: ['7-4', '7-6']  

628 ***Trigger Reverse Engineering開始***  

629 Target: 7, victim: 6, Loss: 1.3164, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:72.96, Cost:0.02 best_reg:72.99 avg_loss_reg:72.99: 10% | 102/1000 [08:50<1:17:54, 5.21s/it]  

630 0% | 0/88 [00:00 < ?, ?it/s]early stop 所有  

631 ***Trigger Reverse Engineering結束***  

632 Target Class: 7 Victim Class: 6 Trigger Size: 72.95845031738281 Optimization Steps: 88  

633 ***Symmetric Check開始***  

634 Target: 6, victim: 7, Loss: 2.9850, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:1183.58, Cost:0.00 best_reg:1403.26 avg_loss_reg:1184.30: 100% | 88/88 [07:43<00:00, 5.27s/it]  

635 *****檢測結束*****  

636 檢測結果: Model含有後門(Abnormal)  

637 整體耗時: 1028.6959199005396

```

```

639     ***Pre-Screening開始***  

640     ***Pre-Screening結束***  

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

642     可能的 target-victim 配對: ['0-1', '1-0', '2-0', '3-2', '3-7', '4-5', '4-12', '4-3', '5-3', '5-4', '6-7', '6-8', '7-3', '7-6', '8-6', '10-11', '11-10', '11-13', '12-4', '12-11', '12-13']  

643     ***Trigger Reverse Engineering開始***  

644     Target: 6, victim: 7, Loss: 3.4545, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss: 56.33, Cost: 0.06 best_reg: 59.85 avg_loss: 57% █ | 566/1000 [03:26<02:38, 2.74it/s]  

645     early stop 所有  

646     ***Trigger Reverse Engineering結束***  

647     Target Class: 6 Victim Class: 7 Trigger Size: 56.3314208984375 Optimization Steps: 92  

648     ***Symmetric Check開始***  

649     Target: 7, victim: 6, Loss: 6.8110, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss: 75.28, Cost: 0.09 best_reg: 75.98 avg_loss: 75.98: 99% █ | 91/92 [00:32<00:00, 2.81it/s]  

650     early stop 所有  

651     ***Symmetric Check結束***  

652     *****檢測結束*****  

653     檢測結果: Model是安全的(Benign)  

654     整體耗時: 244.1977732181549  

655     檢測結果: Model是安全的(Benign)  

656     *****檢測結束*****  

657     ***Pre-Screening開始***  

658     ***Pre-Screening結束***  

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

660     可能的 target-victim 配對: ['3-0', '3-2', '5-1', '5-2', '5-8']  

661     ***Trigger Reverse Engineering開始***  

662     Target: 3, victim: 0, Loss: 6.0237, Acc: 100.00%, CE_Loss: 0.34, Reg_Loss: 221.67, Cost: 0.03 best_reg: 221.70 avg_loss: 221.98: 21% █ | 209/1000 [11:28<43:25, 3.29s/it]  

663     0% | 0/116 [00:00:<?, ?it/s]early stop 所有  

664     ***Trigger Reverse Engineering結束***  

665     Target Class: 3 Victim Class: 0 Trigger Size: 221.67190551757812 Optimization Steps: 116  

666     ***Symmetric Check開始***  

667     Target: 0, victim: 3, Loss: 9.5172, Acc: 100.00%, CE_Loss: 0.39, Reg_Loss: 237.38, Cost: 0.04 best_reg: 240.17 avg_loss: 237.49: 96% █ | 111/116 [06:05<00:16, 3.29s/it]  

668     early stop 所有  

669     ***Symmetric Check結束***  

670     *****檢測結束*****  

671     檢測結果: Model是安全的(Benign)  

672     整體耗時: 1066.5303678512573  

673     *****檢測結束*****  

674     ***Pre-Screening開始***  

675     ***Pre-Screening結束***  

676     *****檢測結束***  

677     檢測結果: Model是安全的(Benign)  

678     整體耗時: 10.626201629638672  

679     *****檢測結束*****  

680     ***Pre-Screening開始***  

681     可能的攻擊方式: Universal Backdoor Attack  

682     可能的 target class: 17  

683     可能的 victim classes: ALL  

684     ***Trigger Reverse Engineering開始***  

685     Target: 17, victim: 20, Loss: 0.2860, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss: 56.49, Cost: 0.01 best_reg: 55.59 avg_loss: 55.59: 12% █ | 118/1000 [1:40:52<12:33:58, 51.29s/it]  

686     early stop 所有  

687     ***Trigger Reverse Engineering結束***  

688     Target Class: 17 Victim Class: all Trigger Size: 55.58759716578892 Optimization Steps: 119  

689     *****檢測結束*****  

690     檢測結果: Model含有後門(Abnormal)  

691     整體耗時: 6069.0852355834122  

692     *****檢測結束*****  

693     ***Pre-Screening開始***  

694     ***Pre-Screening結束***  

695     ***Pre-Screening結束***  

696     *****檢測結束***  

697     檢測結果: Model是安全的(Benign)  

698     整體耗時: 36.06670904159546  

699     *****檢測結束*****  

700     ***Pre-Screening開始***  

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

702     可能的 target-victim 配對: ['0-1', '1-0', '2-1', '5-4', '7-4', '7-9', '7-10', '9-10', '10-9']  

703     ***Trigger Reverse Engineering開始***  

704     Target: 0, victim: 1, Loss: 2.0766, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss: 109.79, Cost: 0.02 best_reg: 116.40 avg_loss: 107.46: 34% █ | 339/1000 [05:12<10:09, 1.08it/s]  

705     0% | 0/125 [00:00:<?, ?it/s]early stop 所有  

706     ***Trigger Reverse Engineering結束***  

707     Target Class: 0 Victim Class: 1 Trigger Size: 109.7872314453125 Optimization Steps: 125  

708     ***Symmetric Check開始***  

709     *****檢測結束*****
```

```

710 Target: 1, victim: 0, Loss: 2.6397, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:212.13, Cost:0.01 best_reg:215.11 avg_loss_reg:212.80: 98%| [ 123/125 [01:48<00:01, 1.14it/s]
711 early stop 所有
712 ***Symmetric Check結束***+
713 *****檢測結束*****+
714 檢測結果: Model是安全的(Benign)
715 整體耗時: 427.27389335632324
716 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000050-----
717 ***Pre-Screening開始***+
718 ***Pre-Screening結束***+
719 可能的攻擊方式: Label Specific Backdoor Attack
720 可能的 target-victim 配對: ['0-1', '0-18', '1-0', '1-5', '3-4', '4-11', '5-2', '5-6', '5-7', '7-17', '8-10', '8-11', '9-10', '9-8', '9-17', '10-7', '10-11', '11-10', '12-14', '12-18', '14-18', '15-8', '15-2', '19-5']
721 ***Trigger Reverse Engineering開始***+
722 Target: 11, victim: 10, Loss: 2.3545, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:179.97, Cost:0.01 best_reg:180.04 avg_loss_reg:180.04: 59%| [ 586/1000 [40:29<28:36, 4.15s/it]
723 early stop 所有
724 ***Trigger Reverse Engineering結束***+
725 Target Class: 11 Victim Class: 10 Trigger Size: 179.97471618652344 Optimization Steps: 122
726 ***Symmetric Check開始***+
727 Target: 10, victim: 11, Loss: 1.5358, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:82.82, Cost:0.02 best_reg:83.63 avg_loss_reg:83.63: 100%| [ 122/122 [08:47<00:00, 4.33s/it]
728 ***Symmetric Check結束***+
729 *****檢測結束*****+
730 檢測結果: Model是安全的(Benign)
731 整體耗時: 2974.149044275284 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000051
732
733 ***Pre-Screening開始***+
734 ***Pre-Screening結束***+
735 可能的攻擊方式: Label Specific Backdoor Attack
736 可能的 target-victim 配對: ['4-2', '5-0']
737 ***Trigger Reverse Engineering開始***+
738 Target: 5, victim: 0, Loss: 16.5900, Acc: 0.00%, CE_Loss: 16.59, Reg_Loss:2546.57, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2532.36: 2%| [ 21/1000 [00:10<08:11, 1.99it/s]
739 ***Trigger Reverse Engineering結束***+
740 Target Class: 4 Victim Class: 2 Trigger Size: 1000000000.0 Optimization Steps: 11
741 *****檢測結束*****+
742 檢測結果: Model是安全的(Benign)
743 整體耗時: 20.71783494949408
744 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000052
745 ***Pre-Screening開始***+
746 ***Pre-Screening結束***+
747 可能的攻擊方式: Label Specific Backdoor Attack
748 可能的 target-victim 配對: ['2-5', '2-6', '7-6', '9-12', '12-9']
749 ***Trigger Reverse Engineering開始***+
750 Target: 12, victim: 9, Loss: 4.0734, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:224.93, Cost:0.02 best_reg:225.76 avg_loss_reg:225.76: 22%| [ 221/1000 [06:27<22:45, 1.75s/it]
751 early stop 所有
752 ***Trigger Reverse Engineering結束***+
753 Target Class: 12 Victim Class: 9 Trigger Size: 224.92709350585938 Optimization Steps: 119
754 ***Symmetric Check開始***+
755 Target: 9, victim: 12, Loss: 2.6803, Acc: 90.00%, CE_Loss: 0.21, Reg_Loss:144.66, Cost:0.02 best_reg:151.57 avg_loss_reg:144.11: 100%| [ 119/119 [03:27<00:00, 1.74s/it]
756 ***Symmetric Check結束***+
757 *****檢測結束*****+
758 檢測結果: Model是安全的(Benign)
759 整體耗時: 606.2266697883606 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000053
760
761 ***Pre-Screening開始***+
762 ***Pre-Screening結束***+
763 可能的攻擊方式: Label Specific Backdoor Attack
764 可能的 target-victim 配對: ['6-5', '6-3', '6-2']
765 ***Trigger Reverse Engineering開始***+
766 Target: 6, victim: 5, Loss: 1.0140, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:269.29, Cost:0.00 best_reg:270.34 avg_loss_reg:268.18: 21%| [ 206/1000 [02:35<09:58, 1.33it/s]
767 0% | 0/175 [00:00 < ?, ?it/s]early stop 所有
768 ***Trigger Reverse Engineering結束***+
769 Target Class: 5 Victim Class: 5 Trigger Size: 269.29278564453125 Optimization Steps: 175
770 ***Symmetric Check開始***+
771 Target: 5, victim: 6, Loss: 2.3440, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:421.05, Cost:0.01 best_reg:421.41 avg_loss_reg:424.57: 97%| [ 169/175 [02:08<00:04, 1.32it/s]
772 early stop 所有
773 ***Symmetric Check結束***+
774 *****檢測結束*****+
775 檢測結果: Model是安全的(Benign)
776 整體耗時: 289.1358935900879 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000054
777
778 ***Pre-Screening開始***+
779 ***Pre-Screening結束***+
780 可能的攻擊方式: Label Specific Backdoor Attack

```

```

781 可能的 target-victim 配對: ['2-1', '5-0']
782 ***Trigger Reverse Engineering 開始***
783 Target: 2, victim: 1, Loss: 2.3741, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:134.80, Cost:0.02 best_reg:135.33 avg_loss_reg:135.33: 12% | 124/1000 [06:15<44:14, 3.03s/it]
784 early stop 所有
785 ***Trigger Reverse Engineering 結束***
786 Target Class: 2 Victim Class: 1 Trigger Size: 134.7955322265625 Optimization Steps: 114
787 ***Symmetric Check開始***
788 Target: 1, victim: 2, Loss: 2.9652, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:250.67, Cost:0.01 best_reg:258.61 avg_loss_reg:258.61: 100% | 114/114 [05:43<00:00, 3.02s/it]
789 ***Symmetric Check結束***
790 *****檢測結果: Model是安全的(Benign)
791 檢測結果: Model是安全的(Benign)
792 整體耗時: 728.6107451915741
793 -----掃描檔案: D:\UU\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000055-----
794 ***Pre-Screening 開始***
795 ***Pre-Screening 結束***
796 可能的攻擊方式: Label Specific Backdoor Attack
797 可能的 target-victim 配對: ['0-1', '1-0', '2-3', '3-4']
798 ***Trigger Reverse Engineering 開始***
799 Target: 1, victim: 0, Loss: 1.3594, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:499.55, Cost:0.00 best_reg:501.87 avg_loss_reg:501.87: 19% | 187/1000 [13:13<57:27, 4.24s/it]
800 early stop 所有
801 ***Trigger Reverse Engineering 結束***
802 Target Class: 1 Victim Class: 0 Trigger Size: 499.554443359375 Optimization Steps: 154
803 ***Symmetric Check開始***
804 Target: 0, victim: 1, Loss: 1.0064, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:175.25, Cost:0.01 best_reg:176.15 avg_loss_reg:175.60: 91% | 140/154 [09:58<00:59, 4.27s/it]
805 early stop 所有
806 ***Symmetric Check結束***
807 *****檢測結果: Model是安全的(Benign)
808 檢測結果: Model是安全的(Benign)
809 整體耗時: 1399.4221584796906
810 -----掃描檔案: D:\UU\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000056-----
811 ***Pre-Screening 開始***
812 ***Pre-Screening 結束***
813 可能的攻擊方式: Universal Backdoor Attack
814 可能的 target class: ALL
815 可能的 victim classes: ALL
816 ***Trigger Reverse Engineering 開始***
817 Target: 7, victim: 12, Loss: 0.8452, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:367.35, Cost:0.00 best_reg:366.09 avg_loss_reg:367.18: 7% | 72/1000 [10:58<14:10:15, 54.97s/it]
818 early stop 所有
819 ***Trigger Reverse Engineering 結束***
820 Target Class: all Trigger Size: 366.08656819661456 Optimization Steps: 73
821 *****檢測結果: Model含有後門(Abnormal)
822 檢測結果: Model含有後門(Abnormal)
823 整體耗時: 3974.322370290756
824 -----掃描檔案: D:\UU\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000057-----
825 ***Pre-Screening 開始***
826 ***Pre-Screening 結束***
827 ***檢測結果: Model是安全的(Benign)
828 檢測結果: Model是安全的(Benign)
829 整體耗時: 26.39915418624878
830 -----掃描檔案: D:\UU\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000058-----
831 ***Pre-Screening 開始***
832 ***Pre-Screening 結束***
833 可能的攻擊方式: Label Specific Backdoor Attack
834 可能的 target-victim 配對: ['0-20', '7-8', '18-15']
835 ***Trigger Reverse Engineering 開始***
836 Target: 18, victim: 15, Loss: 5.4842, Acc: 100.00%, CE_Loss: 0.46, Reg_Loss:294.10, Cost:0.02 best_reg:295.92 avg_loss_reg:295.92: 21% | 210/1000 [14:51<55:55, 4.25s/it]
837 early stop 所有
838 ***Trigger Reverse Engineering 結束***
839 Target Class: 18 Victim Class: 15 Trigger Size: 294.101806640625 Optimization Steps: 123
840 ***Symmetric Check開始***
841 Target: 15, victim: 18, Loss: 2.0128, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:359.05, Cost:0.01 best_reg:359.15 avg_loss_reg:359.22: 100% | 123/123 [08:40<00:00, 4.23s/it]
842 ***Symmetric Check結束***
843 *****檢測結果: Model是安全的(Benign)
844 檢測結果: Model是安全的(Benign)
845 整體耗時: 1437.5482561588287
846 -----掃描檔案: D:\UU\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000059-----
847 ***Pre-Screening 開始***
848 ***Pre-Screening 結束***
849 可能的攻擊方式: Label Specific Backdoor Attack
850 可能的 target-victim 配對: ['0-2', '2-0', '4-5', '9-11', '10-9']
851 ***Trigger Reverse Engineering 開始***

```

```

852 Target: 4, victim: 5, Loss: 0.7637, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:56.69, Cost:0.01 best_reg:60.94 avg_loss_reg:57.04: 26% █ | 264/1000 [02:34<07:11, 1.71it/s]
853 early stop 所有
854 ***Trigger Reverse Engineering 結束***+
855 Target Class: 4 Victim Class: 5 Trigger Size: 56.691673278808594 Optimization Steps: 127
856 ***Symmetric Check開始***+
857 Target: 5, victim: 4, Loss: 1.8086, Acc: 95.00%, CE_Loss: 0.23, Reg_Loss:207.70, Cost:0.01 best_reg:218.47 avg_loss_reg:208.79: 100%| █ | 127/127 [01:14<00:00, 1.70it/s]
858 ***Symmetric Check結束***+
859 檢測結果: Model是安全的(Benign)
860 整體耗時: 235.1965465546543 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000060-----
861
862
863 ***Pre-Screening 開始***+
864 ***Pre-Screening 結束***+
865 可能的攻擊方式: Label Specific Backdoor Attack
866 可能的 target-victim 配對: ['0-5']
867 ***Trigger Reverse Engineering 開始***+
868 Target: 0, victim: 5, Loss: 10.6913, Acc: 0.00%, CE_Loss: 10.69, Reg_Loss:2535.99, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2525.07: 1%| | 10/1000 [00:36<59:37, 3.61s/it]
869 ***Trigger Reverse Engineering 結束***+
870 Target Class: 0 Victim Class: 5 Trigger Size: 1000000000.0 Optimization Steps: 11
871 ***Symmetric Check結束***+
872 檢測結果: Model是安全的(Benign)
873 整體耗時: 44.413042306900024 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000061-----
874
875 ***Pre-Screening 開始***+
876 ***Pre-Screening 結束***+
877 ***檢測結束***+
878 檢測結果: Model是安全的(Benign)
879 整體耗時: 16.79815983772278 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000062-----
880
881 ***Pre-Screening 開始***+
882 ***Pre-Screening 結束***+
883 可能的攻擊方式: Label Specific Backdoor Attack
884 可能的 target-victim 配對: ['3-1']
885 ***Trigger Reverse Engineering 開始***+
886 Target: 3, victim: 1, Loss: 1.3765, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:555.07, Cost:0.00 best_reg:558.38 avg_loss_reg:561.20: 18%| █ | 175/1000 [17:58<1:24:44, 6.16s/it]
887 early stop 所有
888 ***Trigger Reverse Engineering 結束***+
889 Target Class: 3 Victim Class: 1 Trigger Size: 555.07470703125 Optimization Steps: 176
890 ***Symmetric Check開始***+
891 Target: 1, victim: 3, Loss: 1.2039, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:1028.47, Cost:0.00 best_reg:1017.77 avg_loss_reg:1017.77: 100%| █ | 176/176 [17:58<00:00, 6.13s/it]
892 ***Symmetric Check結束***+
893 檢測結果: Model是安全的(Benign)
894 整體耗時: 2169.2881154602051 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000063-----
895
896
897 ***Pre-Screening 開始***+
898 ***Pre-Screening 結束***+
899 ***檢測結束***+
900 檢測結果: Model是安全的(Benign)
901 整體耗時: 9.406555652618408 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000064-----
902
903 ***Pre-Screening 開始***+
904 ***Pre-Screening 結束***+
905 可能的攻擊方式: Universal Backdoor Attack
906 可能的 target class: 5
907 可能的 victim classes: ALL
908 ***Trigger Reverse Engineering 開始***+
909 Target: 5, victim: 12, Loss: 0.5216, Acc: 86.36%, CE_Loss: 0.18, Reg_Loss:20.22, Cost:0.02 best_reg:21.56 avg_loss_reg:20.47: 5%| █ | 53/1000 [19:00<5:39:33, 21.51s/it]
910 early stop 所有
911 ***Trigger Reverse Engineering 結束***+
912 Target Class: 5 Victim Class: all Trigger Size: 21.56311798095703 Optimization Steps: 54
913 ***Symmetric Check結束***+
914 檢測結果: Model含有後門(Abnormal)
915 整體耗時: 1149.59379329953 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000065-----
916
917 ***Pre-Screening 開始***+
918 ***Pre-Screening 結束***+
919 可能的攻擊方式: Label Specific Backdoor Attack
920 可能的 target-victim 配對: ['0-1', '1-0', '2-1', '3-5', '5-3', '5-8', '6-7', '9-14', '9-15', '11-10', '13-0', '13-7', '13-15', '14-12', '15-9']
921 ***Trigger Reverse Engineering 開始***+
922 Target: 6, victim: 7, Loss: 1.6144, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:191.55, Cost:0.01 best_reg:191.71 avg_loss_reg:191.71: 50%| █ | 504/1000 [53:59<53:07, 6.43s/it]

```

```

923 early stop 所有
924 ***Trigger Reverse Engineering 結束 ***
925 Target Class: 6 Victim Class: 7 Trigger Size: 191.5477752685547 Optimization Steps: 146
926 ***Symmetric Check開始 ***
927 Target: 7, victim: 6, Loss: 3.5974, Acc: 90.00%, CE_Loss: 0.41, Reg_Loss:629.94, Cost:0.01 best_reg:641.49 avg_loss_reg:631.31: 100%|████████| | 146/146 [15:38<00:00, 6.43s/it]
928 ***Symmetric Check結束 ***
929 *****檢測結束*****  

930 檢測結果: Model是安全的(Benign)
931 整體耗時: 4199.947261571884
932 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000066-----  

933 ***Pre-Screening 開始 ***
934 ***Pre-Screening 結束 ***
935 可能的攻擊方式: Label Specific Backdoor Attack
936 可能的 target-victim 配對: ['0-8', '1-2', '9-11', '11-9', '12-9', '12-11', '12-2']
937 ***Trigger Reverse Engineering 開始 ***
938 Target: 12, victim: 9, Loss: 1.7277, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:91.33, Cost:0.02 best_reg:92.16 avg_loss_reg:92.16: 28%|████| | 276/1000 [14:06<37:01, 3.07s/it]
939 early stop 所有
940 ***Trigger Reverse Engineering 結束 ***
941 Target Class: 12 Victim Class: 9 Trigger Size:91.32717895507812 Optimization Steps: 118
942 ***Symmetric Check開始 ***
943 Target: 9, victim: 12, Loss: 2.0706, Acc: 70.00%, CE_Loss: 0.46, Reg_Loss:477.28, Cost:0.00 best_reg:538.66 avg_loss_reg:482.10: 100%|████████| | 118/118 [05:44<00:00, 2.92s/it]
944 ***Symmetric Check結束 ***
945 *****檢測結束*****  

946 檢測結果: Model是安全的(Benign)
947 整體耗時: 1204.5142858028412
948 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000067-----  

949 ***Pre-Screening 開始 ***
950 ***Pre-Screening 結束 ***
951 可能的攻擊方式: Label Specific Backdoor Attack
952 可能的 target-victim 配對: ['8-15', '9-8', '15-8']
953 ***Trigger Reverse Engineering 開始 ***
954 Target: 9, victim: 8, Loss: 2.5096, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:475.89, Cost:0.01 best_reg:476.18 avg_loss_reg:476.24: 16%|████| | 161/1000 [06:52<35:48, 2.56s/it]
955 early stop 所有
956 ***Trigger Reverse Engineering 結束 ***
957 Target Class: 9 Victim Class: 8 Trigger Size:475.8892822265625 Optimization Steps: 139
958 ***Symmetric Check開始 ***
959 Target: 8, victim: 9, Loss: 7.5727, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:422.87, Cost:0.02 best_reg:431.67 avg_loss_reg:425.38: 86%|████| | 119/139 [05:06<00:51, 2.57s/it]
960 early stop 所有
961 ***Symmetric Check結束 ***
962 *****檢測結束*****  

963 檢測結果: Model是安全的(Benign)
964 整體耗時: 733.9020366668701
965 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000068-----  

966 ***Pre-Screening 開始 ***
967 ***Pre-Screening 結束 ***
968 可能的攻擊方式: Label Specific Backdoor Attack
969 可能的 target-victim 配對: ['6-4', '9-4']
970 ***Trigger Reverse Engineering 開始 ***
971 Target: 9, victim: 4, Loss: 3.5863, Acc: 20.00%, CE_Loss: 3.59, Reg_Loss:2665.24, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2599.76: 3%|████| | 31/1000 [01:20<41:42, 2.58s/it]
972 ***Trigger Reverse Engineering 結束 ***
973 Target Class: 6 Victim Class: 4 Trigger Size:1000000000.0 Optimization Steps: 11
974 *****檢測結束*****  

975 檢測結果: Model是安全的(Benign)
976 整體耗時: 89.92737865447998
977 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000069-----  

978 ***Pre-Screening 開始 ***
979 ***Pre-Screening 結束 ***
980 可能的攻擊方式: Label Specific Backdoor Attack
981 可能的 target-victim 配對: ['0-7', '1-2', '1-9', '2-1', '2-16', '3-4', '4-3', '5-3', '5-4', '5-17', '6-5', '7-0', '8-10', '8-9', '8-15', '9-1', '9-8', '10-8', '10-16', '11-0', '11-1', '11-18', '12-11', '13-11', '13-17', '14-13', '14-15', '14-17', '15-8', '15-14', '16-10', '16-18', '17-4', '17-13', '17-15', '18-16', '18-14', '18-10']
982 ***Trigger Reverse Engineering 開始 ***
983 Target: 9, victim: 8, Loss: 4.8282, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:3174.23, Cost:0.00 best_reg:3391.67 avg_loss_reg:3391.67: 100%|████████| | 1000/1000 [1:26:30<00:00, 5.19s/it]
984 ***Trigger Reverse Engineering 結束 ***
985 Target Class: 14 Victim Class: 15 Trigger Size: 2181.711181640625 Optimization Steps: 35
986 *****檢測結束*****  

987 檢測結果: Model是安全的(Benign)
988 整體耗時: 5209.6555235385895
989 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000070-----  

990 ***Pre-Screening 開始 ***
991 ***Pre-Screening 結束 ***
992 可能的攻擊方式: Label Specific Backdoor Attack

```

```

993 可能的 target-victim 配對: ['2-3', '4-6', '5-6', '6-0', '6-5', '7-10', '8-9', '10-7', '11-0', '11-10']
994 ***Trigger Reverse Engineering開始***
995 Target: 6, victim: 0, Loss: 3.3467, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:191.60, Cost:0.02 best_reg:192.42 avg_loss_reg:189.87: 39%|████| | 391/1000 [40:58<1:03:48, 6.29s/it]
996 early stop 所有
997 ***Trigger Reverse Engineering結束***
998 Target Class: 6 Victim Class: 0 Trigger Size: 191.60260009765625 Optimization Steps: 89
999 ***Symmetric Check開始***
1000 Target: 0, victim: 6, Loss: 1.8565, Acc: 95.00%, CE_Loss: 0.20, Reg_Loss:490.25, Cost:0.00 best_reg:590.02 avg_loss_reg:502.44: 100%|████| 89/89 [09:34<00:00, 6.46s/it]
1001 ***Symmetric Check結束***
1002 *****檢測結果: Model是安全的(Benign)
1003 檢測結果: Model是安全的(Benign)
1004 整體耗時: 3050.8941009044647
1005 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000071-----
1006 ***Pre-Screening開始***
1007 ***Pre-Screening結束***
1008 可能的攻擊方式: Label Specific Backdoor Attack
1009 可能的target-victim 配對: ['0-2', '1-2', '3-4', '5-0', '8-9', '9-18', '10-4', '16-2', '17-18']
1010 ***Trigger Reverse Engineering開始***
1011 Target: 3, victim: 4, Loss: 1.8273, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:150.97, Cost:0.01 best_reg:151.15 avg_loss_reg:151.15: 26%|████| | 264/1000 [30:36<1:25:19, 6.96s/it]
1012 0%| | 0/125 [0:00:<?, ?it/s]early stop 所有
1013 ***Trigger Reverse Engineering結束***
1014 Target Class: 3 Victim Class: 4 Trigger Size: 150.9722900390625 Optimization Steps: 125
1015 ***Symmetric Check開始***
1016 Target: 4, victim: 3, Loss: 4.5776, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:384.24, Cost:0.01 best_reg:390.33 avg_loss_reg:390.33: 96%|████| | 120/125 [14:03<00:35, 7.03s/it]
1017 early stop 所有
1018 ***Symmetric Check結束***
1019 *****檢測結果: Model是安全的(Benign)
1020 檢測結果: Model是安全的(Benign)
1021 整體耗時: 2702.7054691314697
1022 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000072-----
1023 ***Pre-Screening開始***
1024 ***Pre-Screening結束***
1025 ***檢測結果: Model是安全的(Benign)
1026 檢測結果: Model是安全的(Benign)
1027 整體耗時: 4.984390735626221
1028 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000073-----
1029 ***Pre-Screening開始***
1030 ***Pre-Screening結束***
1031 可能的攻擊方式: Label Specific Backdoor Attack
1032 可能的target-victim 配對: ['2-0', '2-1', '2-16', '3-10', '5-6', '6-5', '6-8', '14-9', '14-15', '15-9', '15-14', '15-16']
1033 ***Trigger Reverse Engineering開始***
1034 Target: 2, victim: 0, Loss: 1.2036, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:214.32, Cost:0.01 best_reg:214.49 avg_loss_reg:214.69: 37%|████| | 369/1000 [05:09<08:50, 1.19it/s]
1035 0%| | 0/141 [0:00:<?, ?it/s]early stop 所有
1036 ***Trigger Reverse Engineering結束***
1037 Target Class: 2 Victim Class: 0 Trigger Size: 214.32220458984375 Optimization Steps: 141
1038 ***Symmetric Check開始***
1039 Target: 0, victim: 2, Loss: 2.5570, Acc: 95.00%, CE_Loss: 0.41, Reg_Loss:635.36, Cost:0.00 best_reg:647.61 avg_loss_reg:628.84: 100%|████| | 141/141 [01:58<00:00, 1.19it/s]
1040 ***Symmetric Check結束***
1041 *****檢測結果: Model是安全的(Benign)
1042 檢測結果: Model是安全的(Benign)
1043 整體耗時: 435.88667249679565
1044 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000074-----
1045 ***Pre-Screening開始***
1046 ***Pre-Screening結束***
1047 可能的攻擊方式: Label Specific Backdoor Attack
1048 可能的target-victim 配對: ['5-6', '7-5', '8-4']
1049 ***Trigger Reverse Engineering開始***
1050 Target: 5, victim: 6, Loss: 3.9303, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:63.92, Cost:0.06 best_reg:66.76 avg_loss_reg:60.53: 15%|████| | 148/1000 [01:33<08:55, 1.59it/s]
1051 early stop 所有
1052 ***Trigger Reverse Engineering結束***
1053 Target Class: 5 Victim Class: 6 Trigger Size: 63.91997528076172 Optimization Steps: 104
1054 ***Symmetric Check開始***
1055 Target: 6, victim: 5, Loss: 5.0198, Acc: 95.00%, CE_Loss: 0.21, Reg_Loss:187.55, Cost:0.03 best_reg:201.28 avg_loss_reg:190.53: 100%|████| | 104/104 [01:04<00:00, 1.61it/s]
1056 ***Symmetric Check結束***
1057 *****檢測結果: Model是安全的(Benign)
1058 檢測結果: Model是安全的(Benign)
1059 整體耗時: 166.82569551467896
1060 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000075-----
1061 ***Pre-Screening開始***
1062 ***Pre-Screening結束***
1063 可能的攻擊方式: Label Specific Backdoor Attack

```

```

1064 可能的 target-victim 配對: ['0-2', '1-2', '2-0', '3-21', '3-12', '3-7', '4-8', '6-5', '6-14', '9-7', '10-14', '11-2', '11-19', '11-10', '14-10', '16-19', '17-19', '18-19', '20-10', '21-4', '21-12']
1065 ***Trigger Reverse Engineering開始***
1066 Target: 9, victim: 7, Loss: 1.154, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss: 91.69, Cost: 0.01 best_reg: 95.35 avg_loss_reg: 92.34: 62% | 618/1000 [16:19<10:05, 1.58s/it]
early stop 所有
1067 ***Trigger Reverse Engineering結束***
1068 Target Class: 9 Victim Class: 7 Trigger Size: 91.69285583496094 Optimization Steps: 123
1069 Target: 7, victim: 9, Loss: 2.3178, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss: 426.68, Cost: 0.01 best_reg: 435.33 avg_loss_reg: 418.48: 100% | 123/123 [03:14<00:00, 1.58s/it]
1070 ***Symmetric Check開始***
1071 ***Symmetric Check結束***
1072 ***Symmetric Check結果: Model是安全的(Benign)
1073 檢測結果: Model是安全的(Benign)
1074 檢測結果: Model是安全的(Benign)
1075 整體耗時: 1185.3788326058197
1076 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000076-----
1077 ***Pre-Screening開始***
1078 ***Pre-Screening結束***
1079 可能的攻擊方式: Label Specific Backdoor Attack
1080 可能的 target-victim 配對: ['0-1', '1-0']
1081 ***Trigger Reverse Engineering開始***
1082 Target: 1, victim: 0, Loss: 2.2630, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss: 36.09, Cost: 0.06 best_reg: 36.62 avg_loss_reg: 36.62: 12% | 121/1000 [01:11<08:42, 1.68it/s]
1083 early stop 所有
1084 ***Trigger Reverse Engineering結束***
1085 Target Class: 1 Victim Class: 0 Trigger Size: 36.0929069519043 Optimization Steps: 95
1086 ***Symmetric Check開始***
1087 Target: 0, victim: 1, Loss: 2.6154, Acc: 90.00%, CE_Loss: 0.36, Reg_Loss: 58.76, Cost: 0.04 best_reg: 59.97 avg_loss_reg: 59.97: 100% | 95/95 [00:55<00:00, 1.71it/s]
1088 ***Symmetric Check結束***
1089 檢測結果: Model是安全的(Benign)
1090 檢測結果: Model是安全的(Benign)
1091 整體耗時: 129.46330070495605
1092 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000077-----
1093 ***Pre-Screening開始***
1094 ***Pre-Screening結束***
1095 可能的攻擊方式: Label Specific Backdoor Attack
1096 可能的 target-victim 配對: ['0-2', '1-3', '1-4', '3-1', '7-5', '7-6']
1097 ***Trigger Reverse Engineering開始***
1098 Target: 1, victim: 3, Loss: 1.1013, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss: 91.75, Cost: 0.01 best_reg: 92.28 avg_loss_reg: 92.28: 28% | 284/1000 [03:26<08:39, 1.38it/s]
1099 early stop 所有
1100 ***Trigger Reverse Engineering結束***
1101 Target Class: 1 Victim Class: 3 Trigger Size: 91.74713134765625 Optimization Steps: 113
1102 ***Symmetric Check開始***
1103 Target: 3, victim: 1, Loss: 5.1711, Acc: 90.00%, CE_Loss: 0.34, Reg_Loss: 282.77, Cost: 0.02 best_reg: 295.43 avg_loss_reg: 284.99: 100% | 113/113 [01:22<00:00, 1.37it/s]
1104 ***Symmetric Check結束***
1105 檢測結果: Model是安全的(Benign)
1106 檢測結果: Model是安全的(Benign)
1107 整體耗時: 293.5281820297241
1108 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000078-----
1109 ***Pre-Screening開始***
1110 ***Pre-Screening結束***
1111 可能的攻擊方式: Label Specific Backdoor Attack
1112 可能的 target-victim 配對: ['0-8']
1113 ***Trigger Reverse Engineering開始***
1114 Target: 0, victim: 8, Loss: 2.0859, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss: 363.79, Cost: 0.01 best_reg: 364.24 avg_loss_reg: 364.24: 16% | 156/1000 [16:28<1:29:07, 6.34s/it]
1115 early stop 所有
1116 ***Trigger Reverse Engineering結束***
1117 Target Class: 0 Victim Class: 8 Trigger Size: 363.786865234375 Optimization Steps: 157
1118 ***Symmetric Check開始***
1119 Target: 8, victim: 0, Loss: 2.4076, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss: 279.92, Cost: 0.01 best_reg: 280.71 avg_loss_reg: 283.36: 94% | 147/157 [15:31<01:03, 6.34s/it]
1120 early stop 所有
1121 ***Symmetric Check結束***
1122 檢測結果: Model是安全的(Benign)
1123 整體耗時: 1934.0635585920715
1124 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000079-----
1125 ***Pre-Screening開始***
1126 ***Pre-Screening結束***
1127 可能的攻擊方式: Label Specific Backdoor Attack
1128 可能的 target-victim 配對: ['0-15', '2-0', '3-4', '5-6', '10-9', '10-8', '12-11', '13-5', '14-11', '15-20', '19-17']
1129 檢測結果: Model是安全的(Benign)
1130 ***Trigger Reverse Engineering開始***
1131 Target: 10, victim: 20, Loss: 1.5523, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss: 82.27, Cost: 0.02 best_reg: 82.37 avg_loss_reg: 82.37: 33% | 133/1000 [11:43<23:41, 2.13s/it]
1132 early stop 所有
1133 ***Trigger Reverse Engineering結束***
1134 Target Class: 10 Victim Class: 20 Trigger Size: 82.26667785644531 Optimization Steps: 106

```

```
1135 ***Symmetric Check開始***  
1136 Target: 20, victim: 10, Loss: 8.0781, Acc: 60.00%, CE_Loss: 0.98, Reg_Loss:2102.25, Cost:0.00 best_reg:2184.44 avg_loss_reg:2145.25: 100%|████████| 106/106 [03:49<00:00, 2.16s/it]  
1137 ***Symmetric Check結束***  
1138 檢測結果: Model含有後門(Abnormal)  
1139 整體耗時: 953.129403591156  
1140  
1141 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000080-----  
1142 ***Pre-Screening開始***  
1143 ***Pre-Screening結束***  
1144 可能的攻擊方式: Label Specific Backdoor Attack  
1145 可能的 target-victim 配對: ['1-2', '1-6', '3-0', '3-4', '3-6', '5-9', '6-10', '7-0', '8-13', '9-10', '9-14', '10-12', '10-16', '11-0', '11-2', '12-8', '12-10', '12-13', '14-16', '16-17', '16-18', '17-9', '18-15', '18-16', '18-17']  
1146 ***Trigger Reverse Engineering開始***  
1147 Target: 3, victim: 4, Loss: 2.1437, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:264.71, Cost:0.01 best_reg:267.29 avg_loss_reg:267.29: 65%|████| 653/1000 [13:25<07:08, 1.23s/it]  
1148 0%  
1149 ***Trigger Reverse Engineering結束***  
1150 Target Class: 3 Victim Class: 4 Trigger Size: 264.70855712890625 Optimization Steps: 135  
1151 ***Symmetric Check開始***  
1152 Target: 4, victim: 3, Loss: 3.2015, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:389.21, Cost:0.01 best_reg:387.23 avg_loss_reg:389.44: 100%|████| 135/135 [02:45<00:00, 1.23s/it]  
1153 ***Symmetric Check結束***  
1154 檢測結果: Model是安全的(Benign)  
1155 整體耗時: 979.3001549243927  
1156  
1157 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000081-----  
1158 ***Pre-Screening開始***  
1159 ***Pre-Screening結束***  
1160 可能的攻擊方式: Label Specific Backdoor Attack  
1161 可能的 target-victim 配對: ['6-7', '8-7', '9-7', '17-16']  
1162 ***Trigger Reverse Engineering開始***  
1163 Target: 8, victim: 7, Loss: 3.0843, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:169.81, Cost:0.02 best_reg:173.74 avg_loss_reg:165.80: 15%|████| 153/1000 [04:50<26:50, 1.90s/it]  
1164 early stop 所有  
1165 ***Trigger Reverse Engineering結束***  
1166 Target Class: 8 Victim Class: 7 Trigger Size: 169.80502319335938 Optimization Steps: 120  
1167 ***Symmetric Check開始***  
1168 Target: 7, victim: 8, Loss: 4.1089, Acc: 100.00%, CE_Loss: 0.49, Reg_Loss:1606.58, Cost:0.00 best_reg:1627.00 avg_loss_reg:1615.16: 100%|████| 120/120 [03:47<00:00, 1.89s/it]  
1169 ***Symmetric Check結束***  
1170 檢測結果: Model是安全的(Benign)  
1171 檢測結果: Model是安全的(Benign)  
1172 整體耗時: 528.9841530323029  
1173 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000082-----  
1174 ***Pre-Screening開始***  
1175 ***Pre-Screening結束***  
1176 可能的攻擊方式: Label Specific Backdoor Attack  
1177 可能的 target-victim 配對: ['2-1', '2-3', '2-4', '3-1', '4-0', '5-0', '6-7', '6-9', '6-13', '7-5', '8-9', '9-0', '10-11', '11-10', '11-12', '12-10', '12-11']  
1178 ***Trigger Reverse Engineering開始***  
1179 Target: 6, victim: 7, Loss: 3.2495, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:183.69, Cost:0.02 best_reg:184.09 avg_loss_reg:184.36: 43%|████| 430/1000 [07:52<10:26, 1.10s/it]  
1180 early stop 所有  
1181 ***Trigger Reverse Engineering結束***  
1182 Target Class: 6 Victim Class: 7 Trigger Size: 183.6914825439453 Optimization Steps: 109  
1183 ***Symmetric Check開始***  
1184 Target: 7, victim: 6, Loss: 7.1935, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:182.44, Cost:0.04 best_reg:183.62 avg_loss_reg:183.62: 92%|████| 100/109 [01:50<00:09, 1.11s/it]  
1185 early stop 所有  
1186 ***Symmetric Check結束***  
1187 檢測結果: Model是安全的(Benign)  
1188 檢測結果: Model是安全的(Benign)  
1189 整體耗時: 589.9919376373291  
1190 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000083-----  
1191 ***Pre-Screening開始***  
1192 ***Pre-Screening結束***  
1193 可能的攻擊方式: Label Specific Backdoor Attack  
1194 可能的 target-victim 配對: ['1-2', '1-3', '1-12', '2-1', '2-3', '2-21', '3-9', '4-0', '4-5', '5-4', '6-0', '7-6', '7-20', '8-10', '8-11', '8-9', '9-12', '9-10', '9-8', '10-8', '10-12', '10-9', '11-9', '11-8', '11-11', '12-11', '13-12', '13-21', '14-16', '15-16', '16-15', '17-20', '18-8', '19-11', '19-10', '19-12', '19-13', '19-14', '19-15', '19-16', '19-17', '20-17', '20-18', '20-19', '21-10']  
1195 ***Trigger Reverse Engineering開始***  
1196 Target: 11, victim: 8, Loss: 1.9703, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:69.52, Cost:0.03 best_reg:69.80 avg_loss_reg:69.80: 79%|████| 786/1000 [06:50<01:51, 1.92it/s]  
1197 early stop 所有  
1198 ***Trigger Reverse Engineering結束***  
1199 Target Class: 11 Victim Class: 8 Trigger Size: 69.52107238769531 Optimization Steps: 101  
1200 ***Symmetric Check開始***  
1201 Target: 8, victim: 11, Loss: 3.7878, Acc: 100.00%, CE_Loss: 0.44, Reg_Loss:440.74, Cost:0.01 best_reg:445.85 avg_loss_reg:445.85: 100%|████| 101/101 [00:52<00:00, 1.91it/s]  
1202 ***Symmetric Check結束***  
1203 檢測結果: Model是安全的(Benign)  
1204 檢測結果: Model是安全的(Benign)
```

一七〇五 重刊足曲

```

1276 ***Symmetric Check開始***  

1277 Target: 3, victim: 4, Loss: 1.3166, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:359.17, Cost:0.00 best_reg:360.57 avg_loss_reg:360.57: 100%|████████| 118/118 [01:53<00:00, 1.04it/s]  

1278 ***Symmetric Check結束***  

1279 ****可能的攻擊方式: Label Specific Backdoor Attack  

1280 檢測結果: Model是安全的(Benign)  

1281 整體耗時: 286.28641152381897  

1282 -----掃描檔案: D:\UUUI\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000090-----  

1283 ***Pre-Screening開始***  

1284 ***Pre-Screening結束***  

1285 可能的攻擊方式: Label Specific Backdoor Attack  

1286 可能的 target-victim 配對: [0-8, '0-14', '2-1', '2-15', '2-16', '3-8', '3-14', '4-6', '5-6', '6-5', '6-21', '8-14', '9-10', '10-9', '10-11', '11-13', '11-20', '12-9', '12-10', '12-14', '13-11', '13-23', '15-16', '15-17', '17-15', '17-16', '18-5', '18-5', '18-21', '18-22', '19-22', '21-22', '23-6', '23-9]  

1287 ***Trigger Reverse Engineering開始***  

1288 Target: 12, victim: 10 Loss: 5.3765, Acc: 90.00%, CE_Loss: 0.34, Reg_Loss:294.86, Cost:0.02 best_reg:380.15 avg_loss_reg:319.31: 100%|████████| 1000/1000 [09:07<00:00, 1.83it/s]  

1289 ***Trigger Reverse Engineering結束***  

1290 Target Class: 12 Victim Class: 10 Trigger Size: 380.1536560058594 Optimization Steps: 60  

1291 ***Symmetric Check開始***  

1292 Target: 10, victim: 12, Loss: 5.4382, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:1589.22, Cost:0.00 best_reg:1678.02 avg_loss_reg:1678.02: 100%|████████| 60/60 [00:33<00:00, 1.77it/s]  

1293 ***Symmetric Check結束***  

1294 檢測結果: Model是安全的(Benign)  

1295 整體耗時: 589.2769432067871  

1296 -----掃描檔案: D:\UUUI\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000091-----  

1297 ***Pre-Screening開始***  

1298 ***Pre-Screening結束***  

1299 ***Pre-Screening結束***  

1300 可能的攻擊方式: Label Specific Backdoor Attack  

1301 可能的 target-victim 配對: [2-3, '3-2', '3-4', '4-3', '7-6', '7-12', '8-6', '10-9', '11-12', '12-7', '12-8', '12-11']  

1302 ***Trigger Reverse Engineering開始***  

1303 Target: 4, victim: 3, Loss: 3.5115, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:87.89, Cost:0.04 best_reg:87.95 avg_loss_reg:87.95: 31%|████| 313/1000 [02:59<06:34, 1.74it/s]  

1304 early stop 所有  

1305 ***Trigger Reverse Engineering結束***  

1306 Target Class: 4 Victim Class: 3 Trigger Size: 87.88641357421875 Optimization Steps: 81  

1307 ***Symmetric Check開始***  

1308 Target: 3, victim: 4, Loss: 3.9256, Acc: 90.00%, CE_Loss: 0.42, Reg_Loss:461.16, Cost:0.01 best_reg:471.63 avg_loss_reg:471.63: 100%|████████| 81/81 [00:45<00:00, 1.79it/s]  

1309 ***Symmetric Check結束***  

1310 檢測結果: Model是安全的(Benign)  

1311 檢測結果: Model是安全的(Benign)  

1312 整體耗時: 231.07721042633057  

1313 -----掃描檔案: D:\UUUI\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000092-----  

1314 ***Pre-Screening開始***  

1315 ***Pre-Screening結束***  

1316 可能的攻擊方式: Label Specific Backdoor Attack  

1317 可能的 target-victim 配對: [0-2, '1-4', '2-3', '2-5', '4-5', '4-15', '5-4', '6-7', '6-8', '7-8', '8-6', '8-7', '8-14', '9-11', '10-6', '10-9', '11-9', '11-10', '12-10', '12-13', '12-15', '13-5', '13-14', '15-16', '16-15']  

1318 ***Trigger Reverse Engineering開始***  

1319 Target: 12, victim: 15, Loss: 1.9431, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:69.87 avg_loss_reg:69.87: 71%|████| 708/1000 [08:26<03:28, 1.40it/s]  

1320 early stop 所有  

1321 ***Trigger Reverse Engineering結束***  

1322 Target Class: 12 Victim Class: 15 Trigger Size: 69.1041259765625 Optimization Steps: 104  

1323 ***Symmetric Check開始***  

1324 Target: 15, victim: 12, Loss: 6.2717, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:794.78, Cost:0.01 best_reg:822.21 avg_loss_reg:822.21: 100%|████████| 104/104 [01:12<00:00, 1.44it/s]  

1325 ***Symmetric Check結束***  

1326 檢測結果: Model含有後門(Abnormal)  

1327 整體耗時: 584.6442468166351  

1328 -----掃描檔案: D:\UUUI\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000093-----  

1329 ***Pre-Screening開始***  

1330 ***Pre-Screening結束***  

1331 ***Pre-Screening結束***  

1332 可能的攻擊方式: Label Specific Backdoor Attack  

1333 可能的 target-victim 配對: ['3-6', '3-7']  

1334 ***Trigger Reverse Engineering開始***  

1335 Target: 3, victim: 7, Loss: 3.6395, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:27.70, Cost:0.13 best_reg:30.00 avg_loss_reg:30.00: 10%|████| 103/1000 [03:21<29:18, 1.96s/it]  

1336 early stop 所有  

1337 ***Trigger Reverse Engineering結束***  

1338 Target Class: 3 Victim Class: 7 Trigger Size: 27.704566955566406 Optimization Steps: 80  

1339 ***Symmetric Check開始***  

1340 Target: 7, victim: 3, Loss: 5.1191, Acc: 100.00%, CE_Loss: 0.40, Reg_Loss:621.52, Cost:0.01 best_reg:633.30 avg_loss_reg:633.30: 100%|████████| 80/80 [02:34<00:00, 1.94s/it]  

1341 ***Symmetric Check結束***  

1342 檢測結果: Model含有後門(Abnormal)  

1343 整體耗時: 362.07052397727966  

1344 -----掃描檔案: D:\UUUI\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000094-----  

1345 ***Pre-Screening開始***  


```

```

1347 ***Pre-Screening結束***  

1348 可能的攻擊方式: Label Specific Backdoor Attack  

1349 可能的 target-victim 配對: ['0-1', '0-2', '2-11', '5-9', '11-2', '11-4', '11-10']  

1350 ***Trigger Reverse Engineering開始***  

1351 Target: 0, victim: 2, Loss: 1.5848, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss: 953.10, Cost:0.00 best_reg:965.52 avg_loss_reg:969.45: 28% | 276/1000 [07:13<18:56, 1.57s/it]  

1352 early stop 所有  

1353 ***Trigger Reverse Engineering結束***  

1354 Target Class: 0 Victim Class: 2 Trigger Size: 953.09765625 Optimization Steps: 162  

1355 ***Symmetric Check開始***  

1356 Target: 2, victim: 0, Loss: 2.1655, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss: 400.73, Cost:0.01 best_reg:402.84 avg_loss_reg:402.84: 90% | 146/162 [03:49<00:25, 1.57s/it]  

1357 early stop 所有  

1358 ***Symmetric Check結束***  

1359 *****檢測結果: Model是安全的(Benign)*****  

1360 整體耗時: 670.9291820526123  

1361 檔案路徑: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000095-----  

1362 ***Pre-Screening開始***  

1363 ***Pre-Screening結束***  

1364 可能的攻擊方式: Label Specific Backdoor Attack  

1365 可能的 target-victim 配對: ['0-1', '0-13', '4-5', '7-14', '8-9', '8-14', '10-9', '10-12', '12-13', '13-3', '13-5', '13-12', '14-5']  

1366 可能的 target-victim 配對: ['0-1', '0-13', '4-5', '7-14', '8-9', '8-14', '10-9', '10-12', '12-13', '13-3', '13-5', '13-12', '14-5']  

1367 ***Trigger Reverse Engineering開始***  

1368 Target: 4, victim: 5, Loss: 2.1643, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss: 263.96, Cost:0.01 best_reg:265.68 avg_loss_reg:264.85: 34% | 342/1000 [06:57<13:23, 1.22s/it]  

1369 0% | 0/129 [00:00:<?, ?it/s]early stop 所有  

1370 ***Trigger Reverse Engineering結束***  

1371 Target Class: 4 Victim Class: 5 Trigger Size: 263.95562744140625 Optimization Steps: 129  

1372 ***Symmetric Check開始***  

1373 Target: 5, victim: 4, Loss: 3.7029, Acc: 100.00%, CE_Loss: 0.34, Reg_Loss: 295.58, Cost:0.01 best_reg:295.40 avg_loss_reg:297.05: 100% | 129/129 [02:36<00:00, 1.21s/it]  

1374 ***Symmetric Check結束***  

1375 *****檢測結果: Model是安全的(Benign)*****  

1376 檢測結果: Model是安全的(Benign)  

1377 整體耗時: 581.4466481208801  

1378 *****檢測結果: Model是安全的(Benign)*****  

1379 ***Pre-Screening開始***  

1380 ***Pre-Screening結束***  

1381 可能的攻擊方式: Label Specific Backdoor Attack  

1382 可能的 target-victim 配對: ['5-4']  

1383 ***Trigger Reverse Engineering開始***  

1384 Target: 5, victim: 4, Loss: 1.5058, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss: 406.49, Cost:0.00 best_reg:409.87 avg_loss_reg:402.75: 17% | 168/1000 [04:28<22:08, 1.60s/it]  

1385 0% | 0/169 [00:00:<?, ?it/s]early stop 所有  

1386 ***Trigger Reverse Engineering結束***  

1387 Target Class: 5 Victim Class: 4 Trigger Size: 406.49334716796875 Optimization Steps: 169  

1388 ***Symmetric Check開始***  

1389 Target: 4, victim: 5, Loss: 5.2443, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss: 195.35, Cost:0.03 best_reg:198.74 avg_loss_reg:193.10: 69% | 117/169 [03:06<01:22, 1.60s/it]  

1390 early stop 所有  

1391 ***Symmetric Check結束***  

1392 *****檢測結果: Model是安全的(Benign)*****  

1393 檢測結果: Model是安全的(Benign)  

1394 整體耗時: 461.97503228323364  

1395 -----  

1396 ***Pre-Screening開始***  

1397 ***Pre-Screening結束***  

1398 可能的攻擊方式: Label Specific Backdoor Attack  

1399 可能的 target-victim 配對: ['14-15', '14-21', '15-14', '19-18']  

1400 ***Trigger Reverse Engineering開始***  

1401 Target: 19, victim: 18, Loss: 4.2652, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss: 522.81, Cost:0.01 best_reg:526.78 avg_loss_reg:513.96: 24% | 235/1000 [06:52<22:22, 1.75s/it]  

1402 early stop 所有  

1403 ***Trigger Reverse Engineering結束***  

1404 Target Class: 18 Victim Class: 18 Trigger Size: 522.811767578125 Optimization Steps: 132  

1405 ***Symmetric Check開始***  

1406 Target: 18, victim: 19, Loss: 3.5714, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss: 652.05, Cost:0.01 best_reg:652.60 avg_loss_reg:653.71: 100% | 132/132 [03:47<00:00, 1.72s/it]  

1407 ***Symmetric Check結束***  

1408 *****檢測結果: Model是安全的(Benign)*****  

1409 檢測結果: Model是安全的(Benign)  

1410 整體耗時: 650.479921512604  

1411 -----  

1412 ***Pre-Screening開始***  

1413 ***Pre-Screening結束***  

1414 可能的攻擊方式: Universal Backdoor Attack  

1415 可能的 target class: 13  

1416 可能的 victim classes: All  

1417 ***Trigger Reverse Engineering開始***
```

File - main  
1418 Target: 13, victim: 14, Loss: 1.7963, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss: 105.01, Cost:0.02 best\_Reg:104.48 avg\_Loss\_Reg:106.90: 12% | 118/1000 [1:55:40 <14:24:37, 58.82s/it]  
1419 early stop 所有  
1420 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1421 Target Class: 13 Victim Class: all Trigger Size: 104.47900009155273 Optimization Steps: 119  
1422 \*\*\*\*\*檢測結果: Model含有後門(Abnormal)  
1423 檢測結果: Model含有後門(Abnormal)  
1424 整體耗時: 6960.125637292862  
1425 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000099-----  
1426 \*\*\*Pre-Screening開始\*\*\*  
1427 \*\*\*Pre-Screening結束\*\*\*  
1428 可能的攻擊方式: Label Specific Backdoor Attack  
1429 可能的 target-victim 配對: ['0-2', '0-12', '1-2', '7-9', '13-12']  
1430 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1431 Target: 7, victim: 9, Loss: 1.9461, Acc: 100.00%, CE\_Loss: 0.17, Reg\_Loss:234.06, Cost:0.01 best\_Reg:234.54 avg\_Loss\_Reg:236.64: 18% | 183/1000 [04:58 <22:14, 1.63s/it]  
1432 early stop 所有  
1433 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1434 Target Class: 7 Victim Class: 9 Trigger Size: 234.05921936035156 Optimization Steps: 139  
1435 \*\*\*Symmetric Check開始\*\*\*  
1436 Target: 9, victim: 7, Loss: 2.2361, Acc: 95.00%, CE\_Loss: 0.20, Reg\_Loss:602.12, Cost:0.00 best\_Reg:612.81 avg\_Loss\_Reg:603.72: 100% | 139/139 [03:45 <00:00, 1.62s/it]  
1437 \*\*\*Symmetric Check結束\*\*\*  
1438 \*\*\*\*\*檢測結果: Model是安全的(Benign)  
1439 檢測結果: Model是安全的(Benign)  
1440 整體耗時: 534.2451767921448  
1441 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000100-----  
1442 \*\*\*Pre-Screening開始\*\*\*  
1443 \*\*\*Pre-Screening結束\*\*\*  
1444 可能的攻擊方式: Label Specific Backdoor Attack  
1445 可能的 target-victim 配對: ['4-1']  
1446 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1447 Target: 4, victim: 1, Loss: 2.2783, Acc: 100.00%, CE\_Loss: 0.06, Reg\_Loss:86.41, Cost:0.03 best\_Reg:86.99 avg\_Loss\_Reg:86.99: 11% | 111/1000 [06:30 <52:04, 3.51s/it]  
1448 early stop 所有  
1449 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1450 Target Class: 4 Victim Class: 1 Trigger Size: 86.41303253173828 Optimization Steps: 112  
1451 \*\*\*Symmetric Check開始\*\*\*  
1452 Target: 1, victim: 4, Loss: 2.6272, Acc: 95.00%, CE\_Loss: 0.43, Reg\_Loss:2201.43, Cost:0.00 best\_Reg:2331.92 avg\_Loss\_Reg:2230.76: 100% | 112/112 [06:29 <00:00, 3.48s/it]  
1453 \*\*\*\*\*檢測結果: Model含有後門(Abnormal)  
1454 \*\*\*\*\*檢測結果: Model含有後門(Abnormal)  
1455 檢測結果: Model含有後門(Abnormal)  
1456 整體耗時: 788.648716497375  
1457 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000101-----  
1458 \*\*\*Pre-Screening開始\*\*\*  
1459 \*\*\*Pre-Screening結束\*\*\*  
1460 可能的攻擊方式: Label Specific Backdoor Attack  
1461 可能的 target-victim 配對: ['2-1', '2-3', '3-4', '6-5', '9-7', '10-17', '15-17', '16-0', '16-4', '16-17', '17-15', '17-16']  
1462 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1463 Target: 16, victim: 4, Loss: 3.8713, Acc: 100.00%, CE\_Loss: 0.05, Reg\_Loss:66.21, Cost:0.06 best\_Reg:66.45 avg\_Loss\_Reg:66.45: 36% | 355/1000 [09:27 <17:11, 1.60s/it]  
1464 early stop 所有  
1465 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1466 Target Class: 16 Victim Class: 4 Trigger Size: 66.21123504638672 Optimization Steps: 76  
1467 \*\*\*Symmetric Check開始\*\*\*  
1468 Target: 4, victim: 16, Loss: 5.3340, Acc: 85.00%, CE\_Loss: 0.60, Reg\_Loss:3158.64, Cost:0.00 best\_Reg:4286.39 avg\_Loss\_Reg:3219.71: 100% | 76/76 [02:00 <00:00, 1.59s/it]  
1469 \*\*\*\*\*檢測結果: Model含有後門(Abnormal)  
1470 \*\*\*\*\*檢測結果: Model含有後門(Abnormal)  
1471 檢測結果: Model含有後門(Abnormal)  
1472 整體耗時: 699.126929983978  
1473 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000102-----  
1474 \*\*\*Pre-Screening開始\*\*\*  
1475 \*\*\*Pre-Screening結束\*\*\*  
1476 檢測結果: Model是安全的(Benign)  
1477 檢測結果: Model是安全的(Benign)  
1478 整體耗時: 6.2286293506622314  
1479 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000103-----  
1480 \*\*\*Pre-Screening開始\*\*\*  
1481 \*\*\*Pre-Screening結束\*\*\*  
1482 可能的攻擊方式: Label Specific Backdoor Attack  
1483 可能的 target-victim 配對: ['5-6']  
1484 \*\*\*Trigger Reverse Engineering開始\*\*\*  
1485 Target: 5, victim: 6, Loss: 1.3246, Acc: 100.00%, CE\_Loss: 0.11, Reg\_Loss:361.22, Cost:0.00 best\_Reg:361.93 avg\_Loss\_Reg:361.79: 14% | 144/1000 [07:27 <44:19, 3.11s/it]  
1486 early stop 所有  
1487 \*\*\*Trigger Reverse Engineering結束\*\*\*  
1488 Target Class: 5 Victim Class: 6 Trigger Size: 361.216064453125 Optimization Steps: 145

```

1489 ***Symmetric Check開始***  

1490 Target: 6, victim: 5, Loss: 1.0979, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:272.24, Cost:0.00 best_reg:272.56 avg_loss_reg:272.56: 92%|████████| | 133/145 [06:54<00:37, 3.12s/it]  

1491 early stop 所有  

1492 ***Symmetric Check結束***  

1493 ****Pre-Screening結束****  

1494 檢測結果: Model是安全的(Benign)  

1495 整體耗時: 871.0345122814178  

1496 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000104-----  

1497 ***Pre-Screening開始***  

1498 ***Pre-Screening結束***  

1499 可能的攻擊方式: Label Specific Backdoor Attack  

1500 可能的 target-victim 配對: ['0-1', '1-0', '4-5', '6-7', '6-8', '8-6', '8-7', '10-9', '10-11', '11-10']  

1501 ***Trigger Reverse Engineering開始***  

1502 Target: 11, victim: 10, Loss: 1.9514, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:63.94, Cost:0.03 best_reg:68.60 avg_loss_reg:63.51: 37%|████| | 369/1000 [04:33<07:47, 1.35it/s]  

1503 early stop 所有  

1504 ***Trigger Reverse Engineering結束***  

1505 Target Class: 11 Victim Class: 10 Trigger Size: 63.94379425048828 Optimization Steps: 123  

1506 ***Symmetric Check開始***  

1507 Target: 10, victim: 11, Loss: 1.9296, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:96.64, Cost:0.02 best_reg:97.33 avg_loss_reg:97.33: 89%|████| | 110/123 [01:23<00:09, 1.31it/s]  

1508 early stop 所有  

1509 ***Pre-Screening開始***  

1510 ****Pre-Screening結束****  

1511 檢測結果: Model是安全的(Benign)  

1512 整體耗時: 363.1817283630371-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000105-----  

1513  

1514 ***Pre-Screening開始***  

1515 ***Pre-Screening結束***  

1516 可能的攻擊方式: Label Specific Backdoor Attack  

1517 可能的 target-victim 配對: ['0-1', '0-2', '1-0', '1-2', '2-0', '4-9', '4-13', '5-6', '6-5', '8-9', '11-12', '12-11', '12-13', '13-12', '17-13']  

1518 ***Trigger Reverse Engineering開始***  

1519 Target: 11, victim: 12, Loss: 2.4650, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:451.61, Cost:0.01 best_reg:452.81 avg_loss_reg:452.81: 47%|████| | 473/1000 [27.58<31:10, 3.55s/it]  

1520 early stop 所有  

1521 ***Trigger Reverse Engineering結束***  

1522 Target Class: 11 Victim Class: 12 Trigger Size: 451.6145324707031 Optimization Steps: 121  

1523 ***Symmetric Check開始***  

1524 Target: 12, victim: 11, Loss: 5.2288, Acc: 80.00%, CE_Loss: 0.43, Reg_Loss:421.59, Cost:0.01 best_reg:439.97 avg_loss_reg:439.97: 100%|████| | 121/121 [07:04<00:00, 3.51s/it]  

1525 ***Symmetric Check結束***  

1526  

1527 檢測結果: Model是安全的(Benign)  

1528 整體耗時: 2117.608879804611-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000106-----  

1529  

1530 ***Pre-Screening開始***  

1531 ****Pre-Screening結束****  

1532 可能的攻擊方式: Universal Backdoor Attack  

1533 可能的 target class: 2  

1534 可能的 victim classes: ALL  

1535 ***Trigger Reverse Engineering開始***  

1536 Target: 2, victim: 12, Loss: 0.7036, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:363.11, Cost:0.00 best_reg:367.69 avg_loss_reg:358.63: 6%|████| | 64/1000 [48:36<11:50:53, 45.57s/it]  

1537 early stop 所有  

1538 ***Trigger Reverse Engineering結束***  

1539 Target Class: 2 Victim Class: all Trigger Size: 367.68621215820315 Optimization Steps: 65  

1540 ***Trigger Reverse Engineering結束***  

1541 檢測結果: Model含有後門(Abnormal)  

1542 整體耗時: 2938.888060569763-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000107-----  

1543  

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: ['4-3', '20-16']  

1548 ***Trigger Reverse Engineering開始***  

1549 Target: 4, victim: 3, Loss: 3.0681, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:165.09, Cost:0.02 best_reg:169.81 avg_loss_reg:169.81: 12%|████| | 121/1000 [00:55<06:42, 2.19it/s]  

1550 early stop 所有  

1551 ***Trigger Reverse Engineering結束***  

1552 Target Class: 4 Victim Class: 3 Trigger Size: 165.09390258789062 Optimization Steps: 111  

1553 ***Symmetric Check開始***  

1554 Target: 3, victim: 4, Loss: 3.8735, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:72.29, Cost:0.01 best_reg:736.65 avg_loss_reg:736.65: 100%|████| | 111/111 [00:51<00:00, 2.16it/s]  

1555 ***Symmetric Check結束***  

1556 檢測結果: Model是安全的(Benign)  

1557 整體耗時: 117.91414546966553-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000108-----  

1558  

1559

```

```

1560 ***Pre-Screening開始***
1561 ***Pre-Screening結束***
1562 可能的攻擊方式:Label Specific Backdoor Attack
1563 可能的 target-victim 配對: ['5-4']
1564 ***Trigger Reverse Engineering開始***
1565 Target: 5, victim: 4, Loss: 4.5439, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:256.25, Cost:0.02 best_reg:259.15 avg_loss_reg:259.15: 12% █ | 117/1000 [04:22<32:57, 2.24s/it]
1566 0% | 0/118 [00:00<?, ?t/s]early stop 所有
1567 ***Trigger Reverse Engineering結束***
1568 Target Class: 5 Victim Class: 4 Trigger Size: 256.2516174316406 Optimization Steps: 118
1569 ***Symmetric Check開始***
1570 Target: 4, victim: 5, Loss: 5.1796, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:193.12, Cost:0.03 best_reg:194.85 avg_loss_reg:194.85: 90% █ | 106/118 [03:57<00:26, 2.24s/it]
1571 early stop 所有
1572 ***Symmetric Check結束***
1573 ****Pre-Screening結束****
1574 檢測結果: Model是安全的(Benign)
1575 整體耗時: 510.287034034729
1576 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000109-----
1577 ***Pre-Screening開始***
1578 ****Pre-Screening結束***
1579 可能的攻擊方式: Label Specific Backdoor Attack
1580 可能的 target-victim 配對: ['6-0']
1581 ***Trigger Reverse Engineering開始***
1582 Target: 6, victim: 0, Loss: 2.4947, Acc: 100.00%, CE_Loss: 0.07, Reg_Loss:28.04, Cost:0.09 best_reg:28.99 avg_loss_reg:28.99: 6% █ | 65/1000 [02:50<40:46, 2.62s/it]
1583 early stop 所有
1584 ***Trigger Reverse Engineering結束***
1585 Target Class: 6 Victim Class: 0 Trigger Size: 28.038414001464844 Optimization Steps: 66
1586 ***Symmetric Check開始***
1587 Target: 0, victim: 6, Loss: 0.2435, Acc: 90.00%, CE_Loss: 0.24, Reg_Loss:11105.07, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:11071.01: 100% █ | 66/66 [02:49<00:00, 2.57s/it]
1588 ***Symmetric Check結束***
1589 ****Pre-Screening結束****
1590 檢測結果: Model含右後門(Abnormal)
1591 整體耗時: 346.94814705848694
1592 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000110-----
1593 ****Pre-Screening開始***
1594 ****Pre-Screening結束***
1595 可能的攻擊方式: Label Specific Backdoor Attack
1596 可能的 target-victim 配對: ['2-3', '3-0', '3-1']
1597 ***Trigger Reverse Engineering開始***
1598 Target: 3, victim: 0, Loss: 0.8395, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:65.39, Cost:0.01 best_reg:65.61 avg_loss_reg:65.89: 15% █ | 151/1000 [03:56<22:11, 1.57s/it]
1599 early stop 所有
1600 ***Trigger Reverse Engineering結束***
1601 Target Class: 3 Victim Class: 0 Trigger Size: 65.3886947631836 Optimization Steps: 109
1602 ***Symmetric Check開始***
1603 Target: 0, victim: 3, Loss: 4.3591, Acc: 80.00%, CE_Loss: 0.67, Reg_Loss:1638.11, Cost:0.00 best_reg:1731.56 avg_loss_reg:1605.43: 100% █ | 109/109 [02:50<00:00, 1.57s/it]
1604 ***Symmetric Check結束***
1605 ****Pre-Screening結束****
1606 檢測結果: Model含右後門(Abnormal)
1607 整體耗時: 411.64203338487244
1608 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000111-----
1609 ****Pre-Screening開始***
1610 ****Pre-Screening結束***
1611 可能的攻擊方式: Label Specific Backdoor Attack
1612 可能的 target-victim 配對: ['2-4', '3-1']
1613 ***Trigger Reverse Engineering開始***
1614 Target: 3, victim: 1, Loss: 2.5371, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:62.36, Cost:0.04 best_reg:62.73 avg_loss_reg:62.73: 13% █ | 127/1000 [07:01<48:14, 3.32s/it]
1615 early stop 所有
1616 ***Trigger Reverse Engineering結束***
1617 Target Class: 3 Victim Class: 1 Trigger Size: 62.36111068725586 Optimization Steps: 96
1618 ***Symmetric Check開始***
1619 Target: 1, victim: 3, Loss: 12.7388, Acc: 90.00%, CE_Loss: 0.46, Reg_Loss:478.94, Cost:0.03 best_reg:509.06 avg_loss_reg:485.13: 100% █ | 96/96 [05:15<00:00, 3.29s/it]
1620 ***Symmetric Check結束***
1621 ****Pre-Screening結束****
1622 檢測結果: Model是安全的(Benign)
1623 整體耗時: 751.0286712646484
1624 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000112-----
1625 ****Pre-Screening開始***
1626 ****Pre-Screening結束***
1627 可能的攻擊方式: Label Specific Backdoor Attack
1628 可能的 target-victim 配對: ['0-1', '1-2', '2-8', '3-18', '6-10', '8-15', '8-10', '8-11', '9-11', '10-4', '10-11', '12-11', '13-18', '14-15', '15-0', '15-10', '15-14', '17-14', '18-2']
1629 ***Trigger Reverse Engineering開始***
1630 Target: 0, victim: 1, Loss: 1.9968, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:162.47, Cost:0.01 best_reg:162.94 avg_loss_reg:162.94: 47% █ | 469/1000 [14:06<15:58, 1.80s/it]

```

```

1631 early stop 所有
1632 ***Trigger Reverse Engineering結束***
1633 Target Class: 0 Victim Class: 1 Trigger Size: 162.4669189453125 Optimization Steps: 125
1634 ***Symmetric Check開始***
1635 Target: 1, victim: 0, Loss: 2.8401, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:347.15, Cost:0.01 best_Reg:347.16 avg_Loss_Reg:347.16: 97%|██████████| | 121/125 [03:47<00:07, 1.88s/it]
1636 early stop 所有
1637 ***Symmetric Check結束***
1638 *****檢測結果: Model是安全的(Benign)
1639 檢測結果: Model是安全的(Benign)
1640 整體耗時: 1085.906078338623
1641 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000113-----
1642 ***Pre-Screening開始***
1643 ***Pre-Screening結束***
1644 可能的攻擊方式: Label Specific Backdoor Attack
1645 可能的target-victim 配對: ['0-1', '1-6', '1-9', '1-16', '2-5', '2-13', '3-2', '3-14', '3-16', '4-5', '4-15', '5-4', '5-15', '5-13', '6-8', '6-1', '6-10', '7-6', '7-11', '7-17', '8-1', '8-10', '8-15', '9-8', '10-1', '10-7', '11-4', '11-7', '11-8', '12-2', '13-5', '13-17', '14-3', '14-5', '15-4', '15-18', '16-3']
1646 ***Trigger Reverse Engineering開始***
1647 Target: 6, victim: 8, Loss: 1.8318, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:20.70, Cost:0.09 best_Reg:22.32 avg_Loss_Reg:22.32: 89%|██████████| | 886/1000 [08:41<01:07, 1.70it/s]
1648 early stop 所有
1649 ***Trigger Reverse Engineering結束***
1650 Target Class: 6 Victim Class: 8 Trigger Size: 20.697288513183594 Optimization Steps: 68
1651 ***Symmetric Check開始***
1652 Target: 8, victim: 6, Loss: 6.0641, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:510.32, Cost:0.01 best_Reg:539.62 avg_Loss_Reg:539.62: 100%|██████████| | 68/68 [00:39<00:00, 1.73it/s]
1653 ***Symmetric Check結束***
1654 *****檢測結果: Model是安全的(Benign)
1655 檢測結果: Model含有後門(Abnormal)
1656 整體耗時: 567.4964289128479
1657 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000114-----
1658 ***Pre-Screening開始***
1659 ***Pre-Screening結束***
1660 可能的攻擊方式: Label Specific Backdoor Attack
1661 可能的 target-victim 配對: ['1-0', '4-5', '5-4', '6-7']
1662 ***Trigger Reverse Engineering開始***
1663 Target: 4, victim: 5, Loss: 2.1294, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:117.06, Cost:0.02 best_Reg:117.27 avg_Loss_Reg:117.27: 21%|██████████| | 209/1000 [00:49<03:05, 4.26it/s]
1664 early stop 所有
1665 ***Trigger Reverse Engineering結束***
1666 Target Class: 4 Victim Class: 5 Trigger Size: 117.05807495117188 Optimization Steps: 107
1667 ***Symmetric Check開始***
1668 Target: 5, victim: 4, Loss: 7.3185, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:620.32, Cost:0.01 best_Reg:635.57 avg_Loss_Reg:635.57: 100%|██████████| | 107/107 [00:24<00:00, 4.29it/s]
1669 ***Symmetric Check結束***
1670 *****檢測結果: Model是安全的(Benign)
1671 檢測結果: Model是安全的(Benign)
1672 整體耗時: 75.74338817596436
1673 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000115-----
1674 ***Pre-Screening開始***
1675 ***Pre-Screening結束***
1676 可能的攻擊方式: Label Specific Backdoor Attack
1677 可能的 target-victim 配對: ['7-0']
1678 ***Trigger Reverse Engineering開始***
1679 Target: 7, victim: 0, Loss: 1.4147, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:382.63, Cost:0.00 best_Reg:385.27 avg_Loss_Reg:385.27: 16%|██████████| | 163/1000 [08:05<41:32, 2.98s/it]
1680 early stop 所有
1681 ***Trigger Reverse Engineering結束***
1682 Target Class: 7 Victim Class: 0 Trigger Size: 382.6292419433594 Optimization Steps: 164
1683 ***Symmetric Check開始***
1684 Target: 0, victim: 7, Loss: 5.9056, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:223.56, Cost:0.03 best_Reg:226.47 avg_Loss_Reg:226.47: 68%|██████████| | 111/164 [05:33<02:39, 3.00s/it]
1685 early stop 所有
1686 ***Symmetric Check結束***
1687 *****檢測結果: Model是安全的(Benign)
1688 檢測結果: Model是安全的(Benign)
1689 整體耗時: 826.9991669654846
1690 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000116-----
1691 ***Pre-Screening開始***
1692 ***Pre-Screening結束***
1693 可能的攻擊方式: Label Specific Backdoor Attack
1694 可能的 target-victim 配對: ['2-4', '3-8']
1695 ***Trigger Reverse Engineering開始***
1696 Target: 3, victim: 8, Loss: 1.2394, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:717.09, Cost:0.00 best_Reg:717.47 avg_Loss_Reg:717.47: 32%|██████████| | 322/1000 [05:24<11:23, 1.01s/it]
1697 early stop 所有
1698 ***Trigger Reverse Engineering結束***
1699 Target Class: 3 Victim Class: 8 Trigger Size: 717.0944213867188 Optimization Steps: 180
1700 ***Symmetric Check開始***

```

```

1701 Target: 8, victim: 3, Loss: 3.2231, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:586.81, Cost:0.01 best_reg:585.57 avg_loss_reg:585.71: 100%|████████| 180/180 [03:01<00:00, 1.01s/it]
1702 ***Symmetric Check結束*** 檢測結果: Model是安全的(Benign)
1703 整體耗時: 512.6645107269287 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000117-----
1704 檢測結果: Model Specific Backdoor Attack
1705 可能的攻擊方式: Label Specific Backdoor Attack
1706 可能的 target-victim 配對: ['1-0', '1-20', '2-3', '4-8', '5-4', '6-0', '6-4', '6-20', '10-15', '11-17', '11-20', '12-16', '13-9', '14-15', '14-10', '14-13', '15-13', '15-10', '15-14', '18-19', '19-16', '20-1'] -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000117-----
1707 ***Pre-Screening開始*** 檢測結果: Model是安全的(Benign)
1708 ***Pre-Screening結束*** 檢測結果: Model是安全的(Benign)
1709 可能的攻擊方式: Label Specific Backdoor Attack
1710 可能的 target-victim 配對: ['1-0', '1-20', '2-3', '4-8', '5-4', '6-0', '6-4', '6-20', '10-15', '11-17', '11-20', '12-16', '13-9', '14-15', '14-10', '14-13', '15-13', '15-10', '15-14', '18-19', '19-16', '20-1'] -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000117-----
1711 ***Trigger Reverse Engineering開始*** 檢測結果: Model是安全的(Benign)
1712 Target: 15, victim: 10, Loss: 1.6581, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:126.23, Cost:0.01 best_reg:128.95 avg_loss_reg:128.95: 54%|████| 544/1000 [05:23<04:30, 1.68it/s]
1713 early stop 所有
1714 ***Trigger Reverse Engineering結束*** 檢測結果: Model是安全的(Benign)
1715 Target Class: 15 Victim Class: 10 Trigger Size: 126.22673034667969 Optimization Steps: 124
1716 ***Symmetric Check開始*** 檢測結果: Model是安全的(Benign)
1717 Target: 10, victim: 15, Loss: 0.7991, Acc: 90.00%, CE_Loss: 0.20, Reg_Loss:397.88, Cost:0.00 best_reg:408.56 avg_loss_reg:399.83: 100%|████| 124/124 [01:13<00:00, 1.68it/s]
1718 ***Symmetric Check結束*** 檢測結果: Model是安全的(Benign)
1719 ***Symmetric Check結束*** 檢測結果: Model是安全的(Benign)
1720 檢測結果: Model是安全的(Benign)
1721 整體耗時: 404.27442693710327 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000118-----
1722 ***Pre-Screening開始*** 檢測結果: Model是安全的(Benign)
1723 ***Pre-Screening結束*** 檢測結果: Model是安全的(Benign)
1724 ***Pre-Screening開始*** 檢測結果: Model是安全的(Benign)
1725 可能的攻擊方式: Label Specific Backdoor Attack
1726 可能的 target-victim 配對: ['0-18', '0-21', '1-2', '3-2', '4-2', '5-6', '7-9', '7-10', '8-9', '8-10', '8-12', '9-10', '11-9', '11-10', '11-21', '12-6', '13-16', '14-15', '15-14', '15-22', '18-0', '18-21', '18-22', '20-21', '21-22', '22-15'] -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000118-----
1727 ***Trigger Reverse Engineering開始*** 檢測結果: Model是安全的(Benign)
1728 Target: 11, victim: 10, Loss: 2.7937, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:67.31, Cost:0.04 best_reg:67.33 avg_loss_reg:67.33: 60%|████| 596/1000 [10:59<07:27, 1.11s/it]
1729 early stop 所有
1730 ***Trigger Reverse Engineering結束*** 檢測結果: Model是安全的(Benign)
1731 Target Class: 11 Victim Class: 10 Trigger Size: 67.31299591064453 Optimization Steps: 112
1732 ***Symmetric Check開始*** 檢測結果: Model是安全的(Benign)
1733 Target: 10, victim: 11, Loss: 4.5236, Acc: 100.00%, CE_Loss: 0.43, Reg_Loss:359.53, Cost:0.01 best_reg:358.30 avg_loss_reg:358.90: 100%|████| 112/112 [02:00<00:00, 1.08s/it]
1734 ***Symmetric Check結束*** 檢測結果: Model是安全的(Benign)
1735 ***Symmetric Check結束*** 檢測結果: Model是安全的(Benign)
1736 檢測結果: Model是安全的(Benign)
1737 整體耗時: 788.702125177765 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000119-----
1738 ***Pre-Screening開始*** 檢測結果: Model是安全的(Benign)
1739 ***Pre-Screening結束*** 檢測結果: Model是安全的(Benign)
1740 ***Pre-Screening開始*** 檢測結果: Model是安全的(Benign)
1741 可能的攻擊方式: Label Specific Backdoor Attack
1742 可能的 target-victim 配對: ['2-0', '6-5', '10-9', '11-10', '12-0', '12-9', '12-10'] -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000119-----
1743 ***Trigger Reverse Engineering開始*** 檢測結果: Model是安全的(Benign)
1744 Target: 12, victim: 9, Loss: 2.2421, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:115.66, Cost:0.02 best_reg:120.01 avg_loss_reg:120.01: 22%|████| 217/1000 [10:46<38:54, 2.98s/it]
1745 early stop 所有
1746 ***Trigger Reverse Engineering結束*** 檢測結果: Model是安全的(Benign)
1747 Target Class: 12 Victim Class: 9 Trigger Size: 115.65518188476562 Optimization Steps: 121
1748 ***Symmetric Check開始*** 檢測結果: Model是安全的(Benign)
1749 Target: 9, victim: 12, Loss: 2.6178, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:317.41, Cost:0.01 best_reg:330.95 avg_loss_reg:315.39: 100%|████| 121/121 [06:21<00:00, 3.15s/it]
1750 ***Symmetric Check結束*** 檢測結果: Model是安全的(Benign)
1751 ***Symmetric Check結束*** 檢測結果: Model是安全的(Benign)
1752 檢測結果: Model是安全的(Benign)
1753 整體耗時: 1043.3193871974945 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000120-----
1754 ***Pre-Screening開始*** 檢測結果: Model是安全的(Benign)
1755 ***Pre-Screening結束*** 檢測結果: Model是安全的(Benign)
1756 ***Pre-Screening開始*** 檢測結果: Model是安全的(Benign)
1757 可能的攻擊方式: Label Specific Backdoor Attack
1758 可能的 target-victim 配對: ['5-2', '5-4'] -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000120-----
1759 ***Trigger Reverse Engineering開始*** 檢測結果: Model是安全的(Benign)
1760 Target: 5, victim: 4, Loss: 1.0518, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:198.28, Cost:0.01 best_reg:203.17 avg_loss_reg:203.17: 15%|████| 153/1000 [02:37<14:31, 1.03s/it]
1761 early stop 所有
1762 ***Trigger Reverse Engineering結束*** 檢測結果: Model是安全的(Benign)
1763 Target Class: 5 Victim Class: 4 Trigger Size: 198.27621459960938 Optimization Steps: 133
1764 ***Symmetric Check開始*** 檢測結果: Model是安全的(Benign)
1765 Target: 4, victim: 5, Loss: 3.5324, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:98.49, Cost:0.00 best_reg:1005.01 avg_loss_reg:1005.01: 100%|████| 133/133 [02:16<00:00, 1.02s/it]
1766 ***Symmetric Check結束*** 檢測結果: Model是安全的(Benign)
1767 ***Symmetric Check結束*** 檢測結果: Model是安全的(Benign)
1768 檢測結果: Model是安全的(Benign)
1769 整體耗時: 299.5324423313141 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000121-----
1770 ***Pre-Screening開始*** 檢測結果: Model是安全的(Benign)
1771 ***Pre-Screening結束*** 檢測結果: Model是安全的(Benign)

```

```

1772 ***Pre-Screening結束***  

1773 可能的攻擊方式: Label Specific Backdoor Attack  

1774 可能的 target-victim 配對: ['3-4']  

1775 ***Trigger Reverse Engineering開始***  

1776 Target: 3, victim: 4, Loss: 6.9917, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:590.24, Cost:0.01 best_reg:595.65 avg_loss_reg:595.65: 13%| 130/1000 [05:43<38:15, 2.64s/it]  

1777 0%| 0/131 [00:00<?, ?] it/searly stop 所有  

1778 ***Trigger Reverse Engineering結束***  

1779 Target Class: 3 Victim Class: 4 Trigger Size: 590.2437744140625 Optimization Steps: 131  

1780 ***Symmetric Check開始***  

1781 Target: 4, victim: 3, Loss: 3.5460, Acc: 95.00%, CE_Loss: 0.35, Reg_Loss:630.44, Cost:0.01 best_reg:636.02 avg_loss_reg:636.02: 100%| 131/131 [05:43<00:00, 2.62s/it]  

1782 ***Symmetric Check結束***  

1783 *****檢測結果*****  

1784 檢測結果: Model是安全的(Benign)  

1785 整體耗時: 695.6213431358337  

1786 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000122-----  

1787 ***Pre-Screening開始***  

1788 ***Pre-Screening結束***  

1789 可能的攻擊方式: Label Specific Backdoor Attack  

1790 可能的 target-victim 配對: ['0-3', '1-2', '1-3', '2-1', '2-3', '2-12', '3-1', '3-2', '6-1', '6-12', '6-14', '8-7', '12-14', '13-12']  

1791 ***Trigger Reverse Engineering開始***  

1792 Target: 12, victim: 14, Loss: 4.3537, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:156.31, Cost:0.03 best_reg:157.77 avg_loss_reg:157.77: 40%| 403/1000 [03:54<05:47, 1.72it/s]  

1793 early stop 所有  

1794 ***Trigger Reverse Engineering結束***  

1795 Target Class: 12 Victim Class: 14 Trigger Size: 156.30853271484375 Optimization Steps: 111  

1796 ***Symmetric Check開始***  

1797 Target: 14, victim: 12, Loss: 3.8831, Acc: 90.00%, CE_Loss: 0.57, Reg_Loss:193.66, Cost:0.02 best_reg:204.40 avg_loss_reg:204.40: 100%| 111/111 [01:04<00:00, 1.71it/s]  

1798 ***Symmetric Check結束***  

1799 *****檢測結果*****  

1800 檢測結果: Model是安全的(Benign)  

1801 整體耗時: 305.4937949180603  

1802 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000123-----  

1803 ***Pre-Screening開始***  

1804 ***Pre-Screening結束***  

1805 可能的攻擊方式: Label Specific Backdoor Attack  

1806 可能的 target-victim 配對: ['3-4', '4-3', '6-3', '18-15']  

1807 ***Trigger Reverse Engineering開始***  

1808 Target: 6, victim: 3, Loss: 4.5250, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:550.12, Cost:0.01 best_reg:551.83 avg_loss_reg:563.55: 32%| 324/1000 [16:38<34:42, 3.08s/it]  

1809 early stop 所有  

1810 ***Trigger Reverse Engineering結束***  

1811 Target Class: 6 Victim Class: 3 Trigger Size: 550.119140625 Optimization Steps: 200  

1812 ***Symmetric Check開始***  

1813 Target: 3, victim: 6, Loss: 1.3999, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:234.26, Cost:0.01 best_reg:235.69 avg_loss_reg:233.82: 84%| 168/200 [08:38<01:38, 3.09s/it]  

1814 early stop 所有  

1815 ***Symmetric Check結束***  

1816 *****檢測結果*****  

1817 檢測結果: Model是安全的(Benign)  

1818 整體耗時: 1532.343826201294  

1819 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000124-----  

1820 ***Pre-Screening開始***  

1821 ***Pre-Screening結束***  

1822 可能的攻擊方式: Label Specific Backdoor Attack  

1823 可能的 target-victim 配對: ['1-0', '4-2', '9-10', '9-11', '10-9', '11-11', '11-5', '11-9', '12-9', '17-18', '18-16']  

1824 ***Trigger Reverse Engineering開始***  

1825 Target: 11, victim: 9, Loss: 2.3399, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:124.16, Cost:0.02 best_reg:126.68 avg_loss_reg:126.68: 36%| 359/1000 [11:38<20:46, 1.94s/it]  

1826 early stop 所有  

1827 ***Trigger Reverse Engineering結束***  

1828 Target Class: 11 Victim Class: 9 Trigger Size: 124.16310119628906 Optimization Steps: 120  

1829 ***Symmetric Check開始***  

1830 Target: 9, victim: 11, Loss: 2.9803, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:241.18, Cost:0.01 best_reg:241.99 avg_loss_reg:241.99: 98%| 118/120 [03:57<00:04, 2.01s/it]  

1831 early stop 所有  

1832 ***Symmetric Check結束***  

1833 *****檢測結果*****  

1834 檢測結果: Model是安全的(Benign)  

1835 整體耗時: 947.5777244567871  

1836 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000125-----  

1837 ***Pre-Screening開始***  

1838 ***Pre-Screening結束***  

1839 *****檢測結果*****  

1840 檢測結果: Model是安全的(Benign)  

1841 整體耗時: 10.717326879501343  

1842 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000126-----  


```

```

1843 ***Pre-Screening開始***
1844 ***Pre-Screening結束***
1845 可能的攻擊方式: Label Specific Backdoor Attack
1846 可能的 target-victim 配對: ['6-11', '7-8', '8-7', '13-12']
1847 ***Trigger Reverse Engineering開始***
1848 Target: 6, victim: 11, Loss: 2.1514, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:79.97, Cost:0.03 best_Reg:80.32 avg_Loss_Reg:78.82: 20%|████|  | 200/1000 [06:28<25:55, 1.94s/it]
1849 early stop 所有
1850 ***Trigger Reverse Engineering結束***
1851 Target Class: 6 Victim Class: 11 Trigger Size: 79.96708679199219 Optimization Steps: 96
1852 ***Symmetric Check開始***
1853 Target: 11, victim: 6, Loss: 9.3264, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:1185.39, Cost:0.01 best_Reg:1198.95 avg_Loss_Reg:1198.95: 100%|████| 96/96 [03:12<00:00, 2.00s/it]
1854 ***Symmetric Check結束***
1855 檢測結果: Model含 有後門 (Abnormal)
1856 整體耗時: 591.0879402160645
1857
1858 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000127-----
1859 ***Pre-Screening開始***
1860 ***Pre-Screening結束***
1861 可能的攻擊方式: Label Specific Backdoor Attack
1862 可能的 target-victim 配對: ['3-4', '4-3']
1863 ***Trigger Reverse Engineering開始***
1864 Target: 4, victim: 3, Loss: 1.4260, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:117.19, Cost:0.01 best_Reg:117.56 avg_Loss_Reg:117.56: 18%|████|  | 177/1000 [02:10<10:07, 1.35it/s]
1865 early stop 所有
1866 ***Trigger Reverse Engineering結束***
1867 Target Class: 3 Victim Class: 3 Trigger Size: 117.18589782714844 Optimization Steps: 140
1868 ***Symmetric Check開始***
1869 Target: 3, victim: 4, Loss: 5.0992, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:190.44, Cost:0.03 best_Reg:191.31 avg_Loss_Reg:191.31: 71%|████|  | 100/140 [01:14<00:29, 1.35it/s]
1870 early stop 所有
1871 ***Symmetric Check結束***
1872
1873 檢測結果: Model是安全的(Benign)
1874 整體耗時: 209.6144425582886
1875
1876 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000128-----
1877 ***Pre-Screening開始***
1878 可能的攻擊方式: Label Specific Backdoor Attack
1879 可能的 target-victim 配對: ['5-3']
1880 ***Trigger Reverse Engineering開始***
1881 Target: 5, victim: 3, Loss: 0.5259, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:18.71, Cost:0.03 best_Reg:18.74 avg_Loss_Reg:18.74: 10%|████|  | 105/1000 [04:42<40:10, 2.69s/it]
1882 0%|  | 0/106 [00:00<?, ?it/s]early stop 所有
1883 ***Trigger Reverse Engineering結束***
1884 Target Class: 5 Victim Class: 3 Trigger Size: 18.708370208740234 Optimization Steps: 106
1885 ***Symmetric Check開始***
1886 Target: 3, victim: 5, Loss: 0.8196, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:734.69, Cost:0.00 best_Reg:753.17 avg_Loss_Reg:753.17: 100%|████| 106/106 [04:43<00:00, 2.67s/it]
1887 ***Symmetric Check結束***
1888 檢測結果: Model含 有後門 (Abnormal)
1889 整體耗時: 576.2841520309448
1890
1891 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000129-----
1892 ***Pre-Screening開始***
1893 ***Pre-Screening結束***
1894 可能的攻擊方式: Label Specific Backdoor Attack
1895 可能的 target-victim 配對: ['4-3', '7-0']
1896 ***Trigger Reverse Engineering開始***
1897 Target: 4, victim: 3, Loss: 0.8140, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:42.84, Cost:0.02 best_Reg:43.23 avg_Loss_Reg:43.23: 12%|████|  | 120/1000 [03:26<25:17, 1.72s/it]
1898 early stop 所有
1899 ***Trigger Reverse Engineering結束***
1900 Target Class: 4 Victim Class: 3 Trigger Size: 42.83763885498047 Optimization Steps: 110
1901 ***Symmetric Check開始***
1902 Target: 3, victim: 4, Loss: 1.0948, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:377.54, Cost:0.00 best_Reg:432.35 avg_Loss_Reg:377.84: 100%|████| 110/110 [03:08<00:00, 1.71s/it]
1903 ***Symmetric Check結束***
1904 檢測結果: Model是安全的(Benign)
1905 整體耗時: 400.0369601249695
1906
1907
1908 ***Pre-Screening開始***
1909 ***Pre-Screening結束***
1910 可能的攻擊方式: Label Specific Backdoor Attack
1911 可能的 target-victim 配對: ['6-5', '6-7', '7-5', '9-5', '13-8', '15-16']
1912 ***Trigger Reverse Engineering開始***
1913 Target: 15, victim: 16, Loss: 3.1505, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:395.42, Cost:0.01 best_Reg:395.10 avg_Loss_Reg:395.10: 30%|████|  | 305/1000 [04:18<09:47, 1.18it/s]

```

```

1914 early stop 所有
1915 ***Trigger Reverse Engineering結束***
1916 Target Class: 15 Victim Class: 16 Trigger Size: 394.4214782714844 Optimization Steps: 130
1917 ***Symmetric Check開始***
1918 Target: 16, victim: 15, Loss: 2.4904, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:299.35, Cost:0.01 best_reg:300.02 avg_loss_reg:300.02: 98%|██████████| 128/130 [01:49<00:01, 1.17it/s]
1919 early stop 所有
1920 ***Symmetric Check結束***
1921 檢測結果: Model是安全的(Benign)
1922 整體耗時: 375.6776239871979
1923
1924 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000131-----
1925 ***Pre-Screening開始***
1926 ***Pre-Screening結束***
1927 可能的攻擊方式: Label Specific Backdoor Attack
1928 可能的 target-victim 配對: ['2-4', '3-4', '4-0', '5-4', '6-4', '7-0', '9-7', '10-7', '15-0', '20-16', '20-19', '21-0']
1929 ***Trigger Reverse Engineering開始***
1930 Target: 2, victim: 4, Loss: 3.2724, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:277.49, Cost:0.01 best_reg:277.77 avg_loss_reg:277.77: 43%|████| 432/1000 [16:15<21:22, 2.26s/it]
1931 early stop 所有
1932 ***Trigger Reverse Engineering結束***
1933 Target Class: 2 Victim Class: 4 Trigger Size: 274.4857482910156 Optimization Steps: 111
1934 ***Symmetric Check開始***
1935 Target: 4, victim: 2, Loss: 5.4364, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:306.08, Cost:0.02 best_reg:307.11 avg_loss_reg:307.11: 100%|████| 111/111 [04:14<00:00, 2.30s/it]
1936 ***Symmetric Check結束***
1937 檢測結果: Model是安全的(Benign)
1938 檢測結果: Model是安全的(Benign)
1939 整體耗時: 1245.7302441596985
1940
1941 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000132-----
1942 ***Pre-Screening開始***
1943 可能的攻擊方式: Label Specific Backdoor Attack
1944 可能的 target-victim 配對: ['3-4', '4-3', '5-2']
1945 ***Trigger Reverse Engineering開始***
1946 Target: 5, victim: 2, Loss: 2.7454, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:31.02, Cost:0.09 best_reg:34.79 avg_loss_reg:34.79: 11%|████| 111/1000 [01:05<08:42, 1.70it/s]
1947 early stop 所有
1948 ***Trigger Reverse Engineering結束***
1949 Target Class: 5 Victim Class: 2 Trigger Size: 31.02216339111328 Optimization Steps: 67
1950 ***Symmetric Check開始***
1951 Target: 2, victim: 5, Loss: 4.5762, Acc: 100.00%, CE_Loss: 0.60, Reg_Loss:1178.76, Cost:0.00 best_reg:1240.46 avg_loss_reg:1240.46: 100%|████| 67/67 [00:39<00:00, 1.71it/s]
1952 ***Symmetric Check結束***
1953 檢測結果: Model含有後門(ABnormal)
1954 檢測結果: Model是安全的(Benign)
1955 整體耗時: 106.6081268787384
1956 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000133-----
1957 ***Pre-Screening開始***
1958 ***Pre-Screening結束***
1959 ***檢測結束***
1960 檢測結果: Model是安全的(Benign)
1961 整體耗時: 16.397372245788574
1962 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000134-----
1963 ***Pre-Screening開始***
1964 ***Pre-Screening結束***
1965 可能的攻擊方式: Label Specific Backdoor Attack
1966 可能的 target-victim 配對: ['0-2', '1-0', '1-2', '4-13', '12-14', '14-12']
1967 ***Trigger Reverse Engineering開始***
1968 Target: 1, victim: 2, Loss: 2.9708, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:553.83, Cost:0.01 best_reg:554.73 avg_loss_reg:556.53: 26%|████| 265/1000 [13:35<37.43, 3.08s/it]
1969 early stop 所有
1970 ***Trigger Reverse Engineering結束***
1971 Target Class: 1 Victim Class: 2 Trigger Size: 553.8289184570312 Optimization Steps: 142
1972 ***Symmetric Check開始***
1973 Target: 2, victim: 1, Loss: 2.9939, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:832.98, Cost:0.00 best_reg:819.21 avg_loss_reg:819.21: 100%|████| 142/142 [07:15<00:00, 3.07s/it]
1974 ***Symmetric Check結束***
1975 檢測結果: Model是安全的(Benign)
1976 檢測結果: Model是安全的(Benign)
1977 整體耗時: 1265.0010001659393
1978 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000135-----
1979 ***Pre-Screening開始***
1980 ***Pre-Screening結束***
1981 可能的攻擊方式: Label Specific Backdoor Attack
1982 可能的 target-victim 配對: ['2-4', '6-3']
1983 ***Trigger Reverse Engineering開始***
1984 Target: 2, victim: 4, Loss: 4.0457, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:29.44, Cost:0.13 best_reg:31.55 avg_loss_reg:31.55: 9%|████| 91/1000 [02:50<28:26, 1.88s/it]

```

```

1985 early stop 所有
1986 ***Trigger Reverse Engineering結束***
1987 Target Class: 2 Victim Class: 4 Trigger Size: 29.444793701171875 Optimization Steps: 81
1988 ***Symmetric Check開始***
1989 Target: 4, victim: 2, Loss: 6.8036, Acc: 90.00%, CE_Loss: 0.34, Reg_Loss:1914.46, Cost:0.00 best_reg:1948.31 avg_loss_reg:1948.31: 100%|██████████| 81/81 [02:30<00:00, 1.86s/it]
1990 ***Symmetric Check結束***
1991 *****
1992 檢測結果: Model含有後門(Abnormal)
1993 整體耗時: 326.468638420105
1994 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000136-----
1995 ***Pre-Screening開始***
1996 可能的攻擊方式: Label Specific Backdoor Attack
1997 可能的target-victim 配對: ['1-0', '8-6', '8-7']
1998 ***Trigger Reverse Engineering開始***
1999 Target: 8, victim: 7, Loss: 3.6840, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:60.22, Cost:0.06 best_reg:61.64 avg_loss_reg:61.64: 17%|████| 174/1000 [02:29<11:48, 1.17it/s]
2000 Target: 8, victim: 7, Loss: 3.5618, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:296.82, Cost:0.01 best_reg:303.47 avg_loss_reg:303.47: 100%|████| 100/100 [01:25<00:00, 1.16it/s]
2001 early stop 所有
2002 ***Trigger Reverse Engineering結束***
2003 Target Class: 7 Victim Class: 7 Trigger Size: 60.22124481201172 Optimization Steps: 100
2004 ***Symmetric Check開始***
2005 Target: 7, victim: 8, Loss: 3.5618, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:0.22, Cost:0.01 best_reg:303.47 avg_loss_reg:303.47: 100%|████| 100/100 [02:29<11:48, 1.17it/s]
2006 ***Symmetric Check結束***
2007 *****
2008 檢測結果: Model是安全的(Benign)
2009 整體耗時: 241.475573272705
2010 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000137-----
2011 ***Pre-Screening開始***
2012 ***Pre-Screening結束***
2013 可能的攻擊方式: Label Specific Backdoor Attack
2014 可能的 target-victim 配對: ['0-1', '1-0', '1-7', '2-9', '2-4', '2-3', '3-2', '4-2', '5-4', '5-6', '6-0', '6-10', '6-12', '7-11', '7-9', '7-13', '8-3', '9-8', '9-11', '10-0', '10-5', '11-7', '11-12', '11-13', '12-6', '12-10', '13-3', '13-12']
2015 ***Trigger Reverse Engineering開始***
2016 Target: 0, victim: 1, Loss: 7.4824, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:187.92, Cost:0.04 best_reg:189.61 avg_loss_reg:189.96: 57%|████| 566/1000 [05:42<04:22, 1.65it/s]
2017 early stop 所有
2018 ***Trigger Reverse Engineering結束***
2019 Target Class: 0 Victim Class: 1 Trigger Size: 187.91848754882812 Optimization Steps: 109
2020 ***Symmetric Check開始***
2021 Target: 1, victim: 0, Loss: 1.6454, Acc: 90.00%, CE_Loss: 0.15, Reg_Loss:295.09, Cost:0.01 best_reg:321.30 avg_loss_reg:297.06: 100%|████| 109/109 [01:04<00:00, 1.69it/s]
2022 ***Symmetric Check結束***
2023 *****
2024 檢測結果: Model是安全的(Benign)
2025 整體耗時: 412.7281537055969
2026 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000138-----
2027 ***Pre-Screening開始***
2028 ***Pre-Screening結束***
2029 可能的攻擊方式: Label Specific Backdoor Attack
2030 可能的 target-victim 配對: ['0-8', '0-13', '1-2', '2-1', '3-5', '3-6', '4-3', '4-6', '4-5', '5-3', '5-6', '5-16', '6-3', '7-8', '7-9', '7-14', '8-9', '8-0', '8-10', '9-1', '9-8', '10-2', '10-8', '10-16', '11-1', '11-12', '11-13', '12-0', '12-7', '13-9', '14-7', '14-15', '14-22', '15-21', '16-14', '16-6', '18-23', '19-15', '19-18', '19-17', '20-21', '20-18', '20-8', '21-9', '21-15', '21-17', '22-14', '22-19', '22-18', '23-22', '23-21']
2031 ***Trigger Reverse Engineering開始***
2032 Target: 20, victim: 21, Loss: 1.7341, Acc: 95.00%, CE_Loss: 0.29, Reg_Loss:285.03, Cost:0.01 best_reg:291.77 avg_loss_reg:292.55: 100%|████| 1000/1000 [55:24<00:00, 3.32s/it]
2033 ***Trigger Reverse Engineering結束***
2034 Target Class: 20 Victim Class: 21 Trigger Size: 291.7674560546875 Optimization Steps: 214
2035 ***Symmetric Check開始***
2036 Target: 21, victim: 20, Loss: 1.6959, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:687.32, Cost:0.00 best_reg:688.03 avg_loss_reg:688.32: 77%|████| 164/214 [09:23<02:51, 3.44s/it]
2037 early stop 所有
2038 ***Symmetric Check結束***
2039 *****
2040 檢測結果: Model是安全的(Benign)
2041 整體耗時: 3905.1686387062073
2042 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000139-----
2043 ***Pre-Screening開始***
2044 ***Pre-Screening結束***
2045 可能的攻擊方式: Label Specific Backdoor Attack
2046 可能的 target-victim 配對: ['6-0', '6-3', '6-2']
2047 ***Trigger Reverse Engineering開始***
2048 Target: 6, victim: 2, Loss: 6.96, Reg_Loss:2537.13, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2524.44: 3%|████| 32/1000 [01:50<55:42, 3.45s/it]
2049 ***Trigger Reverse Engineering結束***
2050 Target Class: 6 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 11
2051 *****
2052 檢測結果: Model是安全的(Benign)
2053 整體耗時: 120.29187750816345
2054 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000140-----

```

```

2055 ***Pre-Screening開始***  

2056 ***Pre-Screening結束***  

2057 ***檢測結束***  

2058 檢測結果: Model是安全的(Benign)  

2059 整體耗時: 23.776296138763428  

2060 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000141-----  

2061 ***Pre-Screening開始***  

2062 可能的攻擊方式: Label Specific Backdoor Attack  

2063 可能的 target-victim 配對: [0-19, '4-13', '5-2', '7-6', '8-9', '9-14', '10-9', '12-9', '14-17', '15-13', '17-14', '18-13', '19-6]  

2064 ***Trigger Reverse Engineering開始***  

2065 Target: 7, victim: 6, Loss: 2.7522, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:495.87, Cost:0.01 best_reg:503.39 avg_loss_reg:497.48: 44% | [REDACTED] | 442/1000 [07:23<09:20, 1.00s/it]  

2066 Target: 7, victim: 6, Loss: 2.7522, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:495.87, Cost:0.01 best_reg:503.39 avg_loss_reg:497.48: 44% | [REDACTED] | 442/1000 [07:23<09:20, 1.00s/it]  

2067 0% | 0/130 [00:00:<?, ?it/s]early stop 所有  

2068 ***Trigger Reverse Engineering結束***  

2069 Target Class: 7 Victim Class: 6 Trigger Size: 495.8712158203125 Optimization Steps: 130  

2070 ***Symmetric Check開始***  

2071 Target: 6, victim: 7, Loss: 2.3971, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:183.48, Cost:0.01 best_reg:186.70 avg_loss_reg:186.70: 95% | [REDACTED] | 123/130 [02:04<00:07, 1.01s/it]  

2072 early stop 所有  

2073 ***Symmetric Check結束***  

2074 *****檢測結束*****  

2075 檢測結果: Model是安全的(Benign)  

2076 整體耗時: 576.9855492115021-----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000142-----  

2077 ***Pre-Screening開始***  

2078 ***Pre-Screening結束***  

2079 ***Pre-Screening開始***  

2080 可能的攻擊方式: Label Specific Backdoor Attack  

2081 可能的 target-victim 配對: [8-6, '10-6', '13-14', '17-18']  

2082 ***Trigger Reverse Engineering開始***  

2083 Target: 13, victim: 14, Loss: 7.5496, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:125.70, Cost:0.06 best_reg:130.17 avg_loss_reg:130.17: 20% | [REDACTED] | 200/1000 [00:50<03:22, 3.95it/s]  

2084 early stop 所有  

2085 ***Trigger Reverse Engineering結束***  

2086 Target Class: 13 Victim Class: 14 Trigger Size: 125.70492553710938 Optimization Steps: 96  

2087 ***Symmetric Check開始***  

2088 Target: 14, victim: 13, Loss: 7.0482, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:117.31, Cost:0.06 best_reg:120.87 avg_loss_reg:120.87: 99% | [REDACTED] | 95/96 [00:24<00:00, 3.94it/s]  

2089 early stop 所有  

2090 ***Symmetric Check結束***  

2091 *****檢測結束*****  

2092 檢測結果: Model是安全的(Benign)  

2093 整體耗時: 79.98512291908264-----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000143-----  

2094 ***Pre-Screening開始***  

2095 ***Pre-Screening結束***  

2096 可能的攻擊方式: Label Specific Backdoor Attack  

2097 可能的 target-victim 配對: [3-4]  

2098 0% | 0/66 [00:00:<?, ?it/s]early stop 所有  

2099 ***Trigger Reverse Engineering開始***  

2100 Target: 3, victim: 4, Loss: 2.9690, Acc: 100.00%, CE_Loss: 0.03, Reg_Loss:50.90, Cost:0.06 best_reg:51.46 avg_loss_reg:51.46: 6% | [REDACTED] | 65/1000 [03:05<44:28, 2.85s/it]  

2101 0% | 0/66 [00:00:<?, ?it/s]early stop 所有  

2102 ***Trigger Reverse Engineering結束***  

2103 Target Class: 3 Victim Class: 4 Trigger Size: 50.90488052368164 Optimization Steps: 66  

2104 ***Symmetric Check開始***  

2105 Target: 4, victim: 3, Loss: 3.2524, Acc: 5.00%, CE_Loss: 3.25, Reg_Loss:11543.80, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:11396.26: 100% | [REDACTED] | 66/66 [03:05<00:00, 2.81s/it]  

2106 ***Symmetric Check結束***  

2107 ***Symmetric Check結束***  

2108 檢測結果: Model含有後門(Abnormal)  

2109 整體耗時: 383.44606041908264-----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000144-----  

2110 ***Pre-Screening開始***  

2111 ***Pre-Screening結束***  

2112 ***Pre-Screening結束***  

2113 ***檢測結束***  

2114 檢測結果: Model是安全的(Benign)  

2115 整體耗時: 5.66572807449341-----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000145-----  

2116 ***Pre-Screening開始***  

2117 ***Pre-Screening結束***  

2118 ***Pre-Screening結束***  

2119 可能的攻擊方式: Label Specific Backdoor Attack  

2120 可能的 target-victim 配對: [0-1, '0-11', '1-0', '2-1', '2-11', '2-14', '4-3', '4-8', '4-14', '6-9', '7-14', '8-9', '8-11', '9-12', '10-3', '10-4', '12-9', '13-12', '14-5', '15-16', '16-15', '18-7', '18-16', '18-17', '19-10', '19-17]  

2121 ***Trigger Reverse Engineering開始***  

2122 Target: 4, victim: 14, Loss: 4.0328, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:148.64, Cost:0.03 best_reg:151.11 avg_loss_reg:151.11: 60% | [REDACTED] | 604/1000 [07:52<05:09, 1.28it/s]  

2123 early stop 所有  

2124 ***Trigger Reverse Engineering結束***  

2125 Target Class: 4 Victim Class: 14 Trigger Size: 148.6416015625 Optimization Steps: 105

```

```
2126 ***Symmetric Check開始***  
2127 Target: 14, victim: 4, Loss: 6.084, Acc: 90.00%, CE_Loss: 0.33, Reg_Loss:505.73, Cost:0.01 best_reg:517.89 avg_loss_reg:517.89: 100%|████████| 105/105 [01:22<00:00, 1.28it/s]  
2128 ***Symmetric Check結束***  
2129 ****Symmetric Check結束*****  
2130 檢測結果: Model是安全的(Benign)  
2131 整體耗時: 560.7199630737305  
2132 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000146-----  
2133 ***Pre-Screening開始***  
2134 ***Pre-Screening結束***  
2135 可能的攻擊方式: Label Specific Backdoor Attack  
2136 可能的 target-victim 配對: ['1-'2', '2-'14', '7-'0', '13-'4']  
2137 ***Trigger Reverse Engineering開始***  
2138 Target: 7, victim: 10, Loss: 2.6537, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:309.14, Cost:0.01 best_reg:309.79 avg_loss_reg:312.27: 17%|████| 166/1000 [06:43<33:48, 2.43s/it]  
2139 early stop 所有  
2140 ***Trigger Reverse Engineering結束***  
2141 Target Class: 7 Victim Class: 10 Trigger Size: 309.149982910156 Optimization Steps: 123  
2142 ***Symmetric Check開始***  
2143 Target: 10, victim: 7, Loss: 7.1232, Acc: 90.00%, CE_Loss: 0.50, Reg_Loss:872.46, Cost:0.01 best_reg:902.85 avg_loss_reg:878.10: 100%|████████| 123/123 [05:03<00:00, 2.46s/it]  
2144 ***Symmetric Check結束***  
2145 ****Symmetric Check結束*****  
2146 檢測結果: Model是安全的(Benign)  
2147 整體耗時: 719.8309864997864  
2148 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000147-----  
2149 ***Pre-Screening開始***  
2150 ***Pre-Screening結束***  
2151 ***檢測結束***  
2152 檢測結果: Model是安全的(Benign)  
2153 整體耗時: 6.653322458267212  
2154 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000148-----  
2155 ***Pre-Screening開始***  
2156 ***Pre-Screening結束***  
2157 可能的攻擊方式: Label Specific Backdoor Attack  
2158 可能的 target-victim 配對: ['5-'1']  
2159 ***Trigger Reverse Engineering開始***  
2160 Target: 5, victim: 1, Loss: 9.1225, Acc: 0.00%, CE_Loss: 9.12, Reg_Loss:2552.96, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2536.77: 1%| 10/1000 [00:58<1:37:04, 5.88s/it]  
2161 ***Trigger Reverse Engineering結束***  
2162 Target Class: 5 Victim Class: 1 Trigger Size: 10000000000.00 Optimization Steps: 11  
2163 ****Symmetric Check結束*****  
2164 檢測結果: Model是安全的(Benign)  
2165 整體耗時: 71.76907205581665  
2166 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000149-----  
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: ['1-'9', '2-'0', '5-'6', '6-'5', '8-'10', '9-'13', '10-'8', '13-'1', '13-'6', '13-'9']  
2171 ***Trigger Reverse Engineering開始***  
2172 Target: 10, victim: 8, Loss: 1.5686, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:126.23, Cost:0.01 best_reg:126.26 avg_loss_reg:126.26: 37%|████| 373/1000 [06:16<10:32, 1.01s/it]  
2173 0%| 0/117 [00:00:<?, ?]it/s]early stop 所有  
2174 ***Trigger Reverse Engineering結束***  
2175 Target Class: 10 Victim Class: 8 Trigger Size: 126.23197174072266 Optimization Steps: 117  
2176 ***Symmetric Check開始***  
2177 Target: 8, victim: 10, Loss: 1.4395, Acc: 95.00%, CE_Loss: 0.18, Reg_Loss:16.03, Cost:0.01 best_reg:167.99 avg_loss_reg:167.43: 100%|████████| 117/117 [02:03<00:00, 1.06s/it]  
2178 ***Symmetric Check結束*****  
2179 ****Symmetric Check結束*****  
2180 檢測結果: Model是安全的(Benign)  
2181 整體耗時: 507.0618498325348  
2182 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000150-----  
2183 ***Pre-Screening開始***  
2184 ***Pre-Screening結束***  
2185 可能的攻擊方式: Universal Backdoor Attack  
2186 可能的 target class: 0  
2187 可能的 victim classes: ALL  
2188 ***Trigger Reverse Engineering開始***  
2189 Target: 0, victim: 4, Loss: 5.0200, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:2231.11, Cost:0.00 best_reg:2213.04 avg_loss_reg:2234.28: 13%|████| 131/1000 [43:41<4:49:46, 20.01s/it]  
2190 early stop 所有  
2191 ***Trigger Reverse Engineering結束***  
2192 Target Class: 0 Victim Class: all Trigger Size: 2209.4636840820312 Optimization Steps: 132  
2193 ****Symmetric Check結束*****  
2194 檢測結果: Model是安全的(Benign)  
2195 整體耗時: 2632.6103370868683  
2196 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000151-----
```

```
2197 ***Pre-Screening開始***  
2198 ***Pre-Screening結束***  
2199 可能的攻擊方式: Label Specific Backdoor Attack  
2200 可能的 target-victim 配對: ['3-6']  
2201 ***Trigger Reverse Engineering開始***  
2202 Target: 3, victim: 6, Loss: 11.628, Acc: 0.00%, CE_Loss: 11.62, Reg_Loss: 2554.15, Cost:0.00 best_Reg:1000000000.00 avg_Loss_Reg:2539.58: 1% | 10/1000 [00:46<1:16:27, 4.63s/it]  
2203 ***Trigger Reverse Engineering結束***  
2204 Target Class: 3 Victim Class: 6 Trigger Size: 1000000000.0 Optimization Steps: 11  
2205 *****檢測結果: Model是安全的(Benign)*****  
2206 整體耗時: 59.49239540100098  
2207 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000152-----  
2208 -----  
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: 0  
2213 可能的 victim classes: ALL  
2214 ***Trigger Reverse Engineering開始***  
2215 Target: 0, victim: 12, Loss: 0.7194, Acc: 93.75%, CE_Loss: 0.14, Reg_Loss:33.83, Cost:0.02 best_Reg:35.39 avg_Loss_Reg:35.93: 12% | 124/1000 [32:02<3:46:21, 15.50s/it]  
2216 early stop 所有  
2217 ***Trigger Reverse Engineering結束***  
2218 Target Class: 0 Victim Class: all Trigger Size: 35.39406051635742 Optimization Steps: 125  
2219 *****檢測結束*****  
2220 檢測結果: Model含有後門(Abnormal)  
2221 整體耗時: 1928.2809221744537  
2222 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000153-----  
2223 ***Pre-Screening開始***  
2224 ***Pre-Screening結束***  
2225 可能的攻擊方式: Label Specific Backdoor Attack  
2226 可能的 target-victim 配對: ['0-4', '1-2', '2-0', '2-1', '2-3', '3-1', '3-13', '4-5', '5-14', '6-15', '7-14', '7-15', '8-9', '9-8', '9-12', '11-13', '12-13', '13-11', '13-12', '14-15']  
2227 ***Trigger Reverse Engineering開始***  
2228 Target: 13, victim: 12, Loss: 1.7617, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:316.87, Cost:0.01 best_Reg:317.82 avg_Loss_Reg:316.86: 52% | 523/1000 [20:32<18:44, 2.36s/it]  
2229 early stop 所有  
2230 ***Trigger Reverse Engineering結束***  
2231 Target Class: 13 Victim Class: 12 Trigger Size: 316.87066650390625 Optimization Steps: 139  
2232 ***Symmetric Check開始***  
2233 Target: 12, victim: 13, Loss: 3.2861, Acc: 100.00%, CE_Loss: 0.30, Reg_Loss:262.59, Cost:0.01 best_Reg:266.82 avg_Loss_Reg:254.87: 86% | 119/139 [04:52<00:49, 2.46s/it]  
2234 early stop 所有  
2235 ***Symmetric Check結束***  
2236 *****檢測結束*****  
2237 檢測結果: Model是安全的(Benign)  
2238 整體耗時: 1536.9603927135468  
2239 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000154-----  
2240 ***Pre-Screening開始***  
2241 ***Pre-Screening結束***  
2242 可能的攻擊方式: Label Specific Backdoor Attack  
2243 可能的 target-victim 配對: ['2-0', '2-3', '3-2', '4-5']  
2244 ***Trigger Reverse Engineering開始***  
2245 Target: 3, victim: 2, Loss: 1.1236, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:136.58, Cost:0.01 best_Reg:136.80 avg_Loss_Reg:136.80: 17% | 173/1000 [04:16<20:27, 1.48s/it]  
2246 early stop 所有  
2247 ***Trigger Reverse Engineering結束***  
2248 Target Class: 3 Victim Class: 2 Trigger Size: 136.577879638671875 Optimization Steps: 140  
2249 ***Symmetric Check開始***  
2250 Target: 2, victim: 3, Loss: 4.0775, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:333.89, Cost:0.01 best_Reg:335.88 avg_Loss_Reg:335.88: 94% | 132/140 [03:22<00:12, 1.53s/it]  
2251 early stop 所有  
2252 ***Symmetric Check結束***  
2253 *****檢測結束*****  
2254 檢測結果: Model是安全的(Benign)  
2255 整體耗時: 462.49137473106384  
2256 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000155-----  
2257 ***Pre-Screening開始***  
2258 ***Pre-Screening結束***  
2259 可能的攻擊方式: Label Specific Backdoor Attack  
2260 可能的 target-victim 配對: ['1-4', '2-7', '3-2', '7-9', '8-7', '8-9', '9-7', '10-11', '11-10', '11-14', '11-19', '17-19']  
2261 ***Trigger Reverse Engineering開始***  
2262 Target: 17, victim: 19, Loss: 1.3248, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:142.96, Cost:0.01 best_Reg:143.00 avg_Loss_Reg:143.00: 40% | 399/1000 [09:51<14:50, 1.48s/it]  
2263 early stop 所有  
2264 ***Trigger Reverse Engineering結束***  
2265 Target Class: 17 Victim Class: 19 Trigger Size: 142.96051025390625 Optimization Steps: 130  
2266 ***Symmetric Check開始***  
2267 Target: 19, victim: 17, Loss: 1.4546, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss:172.75, Cost:0.01 best_Reg:171.77 avg_Loss_Reg:171.77: 100% | 130/130 [03:19<00:00, 1.53s/it]
```

```

22668 ***Symmetric Check結束***  

22669 *****檢測結束*****  

2270 檢測結果: Model是安全的(Benign)  

2271 整體耗時: 799.8822538852692  

2272 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000156-----  

2273 ***Pre-Screening開始***  

2274 ***Pre-Screening結束***  

2275 可能的攻擊方式: Label Specific Backdoor Attack  

2276 可能的 target-victim 配對: ['8-5']  

2277 ***Trigger Reverse Engineering開始***  

2278 Target: 8, victim: 5, Loss: 6.5113, Acc: 0.00%, CE_Loss: 6.51, Reg_Loss:2598.83, Cost:0.00 best_Reg:10000000000.00 avg_Loss_Reg:2572.49: 1%| | 10/1000 [00:36<59:43, 3.62s/it]  

2279 ***Trigger Reverse Engineering結束***  

2280 Target Class: 8 Victim Class: 5 Trigger Size: 1000000000.0 Optimization Steps: 11  

2281 *****檢測結束*****  

2282 檢測結果: Model是安全的(Benign)  

2283 整體耗時: 45.05442976951599  

2284 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000157-----  

2285 ***Pre-Screening開始***  

2286 ***Pre-Screening結束***  

2287 可能的攻擊方式: Label Specific Backdoor Attack  

2288 可能的 target-victim 配對: ['7-6']  

2289 ***Trigger Reverse Engineering開始***  

2290 Target: 7, victim: 6, Loss: 5.9989, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:224.28, Cost:0.03 best_Reg:226.74 avg_Loss_Reg:226.74: 10%| | 96/1000 [01:51<17:33, 1.16s/it]  

2291 early stop 所有  

2292 ***Trigger Reverse Engineering結束***  

2293 Target Class: 7 Victim Class: 6 Trigger Size: 224.2831268310547 Optimization Steps: 97  

2294 ***Symmetric Check開始***  

2295 Target: 6, victim: 7, Loss: 2.2574, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:605.85, Cost:0.00 best_Reg:626.93 avg_Loss_Reg:626.93: 100%| | 97/97 [01:51<00:00, 1.15s/it]  

2296 ***Symmetric Check結束***  

2297 *****檢測結束*****  

2298 檢測結果: Model是安全的(Benign)  

2299 整體耗時: 226.773347415924  

2300 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000158-----  

2301 ***Pre-Screening開始***  

2302 ***Pre-Screening結束***  

2303 可能的攻擊方式: Label Specific Backdoor Attack  

2304 可能的 target-victim 配對: ['3-15', '9-8', '17-10', '17-11']  

2305 ***Trigger Reverse Engineering開始***  

2306 Target: 17, victim: 11, Loss: 2.2357, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:611.21, Cost:0.00 best_Reg:617.98 avg_Loss_Reg:624.30: 27%| | 1274/1000 [24:45<1:05:37, 5.42s/it]  

2307 early stop 所有  

2308 ***Trigger Reverse Engineering結束***  

2309 Target Class: 17 Victim Class: 11 Trigger Size: 611.21484375 Optimization Steps: 164  

2310 ***Symmetric Check開始***  

2311 Target: 11, victim: 17, Loss: 1.5146, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:391.45, Cost:0.00 best_Reg:401.44 avg_Loss_Reg:399.60: 100%| | 164/164 [14:45<00:00, 5.40s/it]  

2312 ***Symmetric Check結束***  

2313 *****檢測結束*****  

2314 檢測結果: Model是安全的(Benign)  

2315 整體耗時: 2401.6984424591064  

2316 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000159-----  

2317 ***Pre-Screening開始***  

2318 ***Pre-Screening結束***  

2319 可能的攻擊方式: Label Specific Backdoor Attack  

2320 可能的 target-victim 配對: ['3-2', '6-8', '6-13', '7-6', '7-8', '8-6', '8-10', '10-6', '10-8', '11-15', '15-11', '16-15']  

2321 ***Trigger Reverse Engineering開始***  

2322 Target: 16, victim: 15, Loss: 1.8926, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:148.10, Cost:0.01 best_Reg:148.99 avg_Loss_Reg:148.99: 36%| | 364/1000 [20:11<35:17, 3.33s/it]  

2323 early stop 所有  

2324 ***Trigger Reverse Engineering結束***  

2325 Target Class: 16 Victim Class: 15 Trigger Size: 148.09637451171875 Optimization Steps: 127  

2326 ***Symmetric Check開始***  

2327 Target: 15, victim: 16, Loss: 1.0746, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:409.12, Cost:0.00 best_Reg:425.95 avg_Loss_Reg:405.20: 100%| | 127/127 [06:56<00:00, 3.28s/it]  

2328 ***Symmetric Check結束***  

2329 *****檢測結束*****  

2330 檢測結果: Model是安全的(Benign)  

2331 整體耗時: 1645.4403192996979  

2332 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round2\TrainData\models\unzip\id-00000160-----  

2333 ***Pre-Screening開始***  

2334 ***Pre-Screening結束***  

2335 可能的攻擊方式: Label Specific Backdoor Attack  

2336 可能的 target-victim 配對: ['10-11', '14-13']  

2337 ***Trigger Reverse Engineering開始***  

2338 Target: 14, victim: 13, Loss: 7.6136, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:286.37, Cost:0.03 best_Reg:287.72 avg_Loss_Reg:287.72: 11%| | 109/1000 [03:40<30:03, 2.02s/it]

```

```
2339 early stop 所有
2340 ***Trigger Reverse Engineering結束***
2341 Target Class: 14 Victim Class: 13 Trigger Size: 286.36788940429969 Optimization Steps: 99
2342 ***Symmetric Check開始***
2343 Target: 13, victim: 14, Loss: 11.4595, Acc: 100.00%, CE_Loss: 0.28, Reg_Loss:129.27, Cost:0.09 best_reg:130.57 avg_loss_reg:130.57: 91%|██████████| | 90/99 [03:02<00:18, 2.03s/it]
2344 early stop 所有
2345 ***Symmetric Check結束***
2346 檢測結果: Model是安全的(Benign)
2347 整體耗時: 4:14.283340454410156 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000161-----
2348
2349 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000161-----
```

---

```
2350 ***Pre-Screening開始***
2351 ***Pre-Screening結束***
2352 可能的攻擊方式: Label Specific Backdoor Attack
2353 可能的 target-victim 配對: ['5-3', '8-6']
2354 ***Trigger Reverse Engineering開始***
2355 Target: 8, victim: 6, Loss: 2.2239, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:179.08, Cost:0.01 best_reg:182.72 avg_loss_reg:182.72: 13%|████| | 128/1000 [05:27<37:12, 2.56s/it]
2356 early stop 所有
2357 ***Trigger Reverse Engineering結束***
2358 Target Class: 8 Victim Class: 6 Trigger Size: 179.07894897460938 Optimization Steps: 118
2359 ***Symmetric Check開始***
2360 Target: 6, victim: 8, Loss: 3.5912, Acc: 95.00%, CE_Loss: 0.27, Reg_Loss:291.73, Cost:0.01 best_reg:304.98 avg_loss_reg:294.33: 100%|██████████| | 118/118 [04:55<00:00, 2.51s/it]
2361 ***Symmetric Check結束***
2362 檢測結果: Model是安全的(Benign)
2363 整體耗時: 634.2849185466766 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000162-----
2364
2365 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000162-----
```

---

```
2366 ***Pre-Screening開始***
2367 ***Pre-Screening結束***
2368 可能的攻擊方式: Label Specific Backdoor Attack
2369 可能的 target-victim 配對: ['0-17', '4-8', '5-6', '5-8', '6-5', '6-8', '6-11', '8-7', '8-12', '10-11', '10-12', '11-6', '11-10', '11-12', '13-14', '14-12', '15-17', '19-17']
2370 ***Trigger Reverse Engineering開始***
2371 Target: 10, victim: 12, Loss: 3.2137, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:261.40, Cost:0.01 best_reg:262.83 avg_loss_reg:262.83: 45%|████| | 447/1000 [25:54<32:03, 3.48s/it]
2372 early stop 所有
2373 ***Trigger Reverse Engineering結束***
2374 Target Class: 10 Victim Class: 12 Trigger Size: 261.40325927734375 Optimization Steps: 142
2375 ***Symmetric Check開始***
2376 Target: 12, victim: 10, Loss: 7.5724, Acc: 100.00%, CE_Loss: 0.49, Reg_Loss:276.46, Cost:0.03 best_reg:277.01 avg_loss_reg:277.01: 79%|██████████| | 112/142 [07:34<02:01, 4.05s/it]
2377 early stop 所有
2378 ***Symmetric Check結束***
2379 檢測結果: Model是安全的(Benign)
2380 整體耗時: 2029.6381077766418 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000163-----
2381
2382 -----掃描檔案: D:\UU\Li\Datasets\TrojAI\Round2\TrainData\models\unzip\id-000000163-----
```

---

```
2383 ***Pre-Screening開始***
2384 ***Pre-Screening結束***
2385 可能的攻擊方式: Label Specific Backdoor Attack
2386 可能的 target-victim 配對: ['2-1', '5-3', '6-1', '6-4', '8-13', '9-10', '9-13', '10-9', '10-13', '11-12', '12-11']
2387 ***Trigger Reverse Engineering開始***
2388 Target: 12, victim: 11, Loss: 2.8161, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:2767.58, Cost:0.00 best_reg:2769.93 avg_loss_reg:2819.71: 24%|████| | 235/1000 [02:33<08:20, 1.53s/it]
2389 Traceback (most recent call last):
2390 File "D:\UU\Li\test_code\k_arm_test\main.py", line 158, in <module>
2391 trigger_reverse_engineering(target_classes, victim_classes, backdoor_type, model, DATA_PATH,
2392 File "D:\UU\Li\test_code\k_arm_test\k_arm_test\k_arm\reverse.py", line 54, in trigger_reverse_engineering
2393 pattern, mask, l1_norm, time_cost = scanner.scanning(
2394 File "D:\UU\Li\test_code\k_arm_test\k_arm\scanner.py", line 149, in scanning
2395 f'Target: {target_classes[target_index]}, victim: {labels[0]}, Loss: {loss:.4f},'
2396 File "C:\Users\slab\anaconda3\envs\pytorch\lib\site-packages\torch\tensor.py", line 534, in __format__
2397 return self.item().__format__(format_spec)
2398 KeyboardInterrupt
2399
2400 Process finished with exit code -1073741510 (0xC0000013A: interrupted by Ctrl+C)
```