

```
1 C:\Users\slab\anaconda3\envs\pytorch1\python.exe D:\UULi\test_code\k_arm_test\main.py  
2 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000739  
3 ***Pre-Screening開始***  
4 ***Pre-Screening結束***  
5 ***檢測結束***  
6 檢測結果: Model是安全的(Benign)  
7 藝體耗時: 14.463637590408325  
8 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000740  
9 ***Pre-Screening開始***  
10 ***Pre-Screening結束***  
11 ***檢測結束***  
12 檢測結果: Model是安全的(Benign)  
13 藝體耗時: 11.918782711029053  
14 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000741  
15 ***Pre-Screening開始***  
16 ***Pre-Screening結束***  
17 ***檢測結束***  
18 檢測結果: Model是安全的(Benign)  
19 藝體耗時: 11.29201364517212  
20 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000742  
21 ***Pre-Screening開始***  
22 ***Pre-Screening結束***  
23 可能的攻擊方式: Label Specific Backdoor Attack  
24 可能的 target-victim 配對: ['0-1', '0-20', '1-2', '1-21', '2-1', '2-21', '3-15', '3-17', '3-18', '4-10', '4-16', '4-21', '5-12', '6-13', '8-16', '9-10', '9-16', '10-16', '13-0', '13-18', '15-3', '15-17', '15-1', '17-19', '20-0']  
25 ***Trigger Reverse Engineering開始***  
26 Target: 0, victim: 20, Loss: 1.0485, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss: 923.24, Cost:0.00 best_reg:923.38 avg_loss_reg:913.63: 50% █ | 498/1000 [53:53 < 54:19, 6.49s/it]  
27 early stop 所有  
28 ***Trigger Reverse Engineering結束***  
29 Target Class: 0 Victim Class: 20 Trigger Size: 923.2374267578125 Optimization Steps: 194  
30 ***Symmetric Check開始***  
31 Target: 20, victim: 0, Loss: 0.0549, Acc: 95.00%, CE_Loss: 0.05, Reg_Loss: 2175.83, Cost:0.00 best_reg:2056.74 avg_loss_reg:2164.89: 100% █ | 194/194 [20:27 < 00:00, 6.33s/it]  
32 ***Symmetric Check結束***  
33 ***檢測結束***  
34 檢測結果: Model是安全的(Benign)  
35 藝體耗時: 4492.413516521454  
36 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000743  
37 ***Pre-Screening開始***  
38 ***Pre-Screening結束***  
39 可能的攻擊方式: Label Specific Backdoor Attack  
40 可能的 target-victim 配對: ['15-20', '16-13', '17-2', '17-9']  
41 ***Trigger Reverse Engineering開始***  
42 Target: 17, victim: 9, Loss: 9.8410, Acc: 0.00%, CE_Loss: 9.84, Reg_Loss: 2598.01, Cost:0.00 best_reg:100000000000.00 avg_loss_reg:2573.26: 4% █ | 43/1000 [00:54 < 20:08, 1.26s/it]  
43 ***Trigger Reverse Engineering結束***  
44 Target Class: 15 Victim Class: 20 Trigger Size: 10000000000.0 Optimization Steps: 11  
45 ***檢測結束***  
46 檢測結果: Model是安全的(Benign)  
47 藝體耗時: 63.71432447433472  
48 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000744  
49 ***Pre-Screening開始***  
50 ***Pre-Screening結束***  
51 ***檢測結束***  
52 檢測結果: Model是安全的(Benign)  
53 藝體耗時: 11.266184568405151  
54 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000745  
55 ***Pre-Screening開始***  
56 ***Pre-Screening結束***  
57 可能的攻擊方式: Label Specific Backdoor Attack  
58 可能的 target-victim 配對: ['1-12', '1-13', '3-12']  
59 ***Trigger Reverse Engineering開始***  
60 Target: 3, victim: 12, Loss: 2.3220, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss: 57.29, Cost:0.04 best_reg:57.67 avg_loss_reg:57.67: 17% █ | 172/1000 [06:23 < 30:47, 2.22s/it]  
61 early stop 所有  
62 ***Trigger Reverse Engineering結束***  
63 Target Class: 3 Victim Class: 12 Trigger Size: 57.289920806884766 Optimization Steps: 98  
64 ***Symmetric Check開始***  
65 Target: 12, victim: 3, Loss: 3.9909, Acc: 80.00%, CE_Loss: 0.85, Reg_Loss: 10608.85, Cost:0.00 best_reg:17686.52 avg_loss_reg:10556.41: 100% █ | 98/98 [03:37 < 00:00, 2.22s/it]  
66 ***Symmetric Check結束***  
67 ***檢測結束***  
68 檢測結果: Model含有後門(Abnormal)  
69 藝體耗時: 612.1732649803162  
70 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000746  
71 ***Pre-Screening開始***
```

```
72 ***Pre-Screening結束***  
73 ***檢測結束***  
74 檢測結果: Model是安全的(Benign)  
75 整體耗時: 24.231024503707886  
76 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000747-----  
77 ***Pre-Screening開始***  
78 ***Pre-Screening結束***  
79 可能的攻擊方式: Label Specific Backdoor Attack  
80 可能的 target-victim 配對: [0-20, '1-21', '2-21', '2-23', '3-15', '3-17', '4-8', '4-18', '7-19', '8-0', '8-6', '8-12', '9-0', '10-18', '11-9', '12-6', '13-3', '13-6', '14-1', '14-6', '14-8', '15-3', '15-8', '16-8', '17-1', '18-9', '18-12', '20-0', '20-21', '21-1', '21-22', '21-6', '23-0', '23-22']  
81 ***Trigger Reverse Engineering開始***  
82 Target: 23, victim: 22, Loss: 7.5071, Acc: 0.00%, CE_Loss: 7.51, Reg_Loss: 2559.41, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2544.12: 53%|████| 526/1000 [59:48<53:53, 6.82s/it]  
83 ***Trigger Reverse Engineering結束***  
84 Target Class: 0 Victim Class: 20 Trigger Size: 1000000000.0 Optimization Steps: 21  
85 *****檢測結束*****  
86 檢測結果: Model是安全的(Benign)  
87 整體耗時: 3634.072234772186-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000748-----  
88 ***Pre-Screening開始***  
89 ***Pre-Screening結束***  
90 ***Pre-Screening結束***  
91 ***檢測結束***  
92 檢測結果: Model是安全的(Benign)  
93 整體耗時: 24.299894094467163-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000749-----  
94 ***Pre-Screening開始***  
95 ***Pre-Screening結束***  
96 ***Pre-Screening結束***  
97 ***檢測結束***  
98 檢測結果: Model是安全的(Benign)  
99 整體耗時: 7.203389883041382-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000750-----  
100 ***Pre-Screening開始***  
101 ***Pre-Screening結束***  
102 ***Pre-Screening結束***  
103 可能的攻擊方式: Label Specific Backdoor Attack  
104 可能的 target-victim 配對: ['1-5', '15-1', '15-5']  
105 ***Trigger Reverse Engineering開始***  
106 Target: 15, victim: 5, Loss: 10.8797, Acc: 0.00%, CE_Loss: 10.88, Reg_Loss: 2533.32, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2523.06: 3%|████| 32/1000 [00:12<06:24, 2.52it/s]  
107 ***Trigger Reverse Engineering結束***  
108 Target Class: 1 Victim Class: 5 Trigger Size: 1000000000.0 Optimization Steps: 11  
109 *****檢測結束*****  
110 檢測結果: Model是安全的(Benign)  
111 整體耗時: 18.310994148254395-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000751-----  
112 ***Pre-Screening開始***  
113 ***Pre-Screening結束***  
114 ***Pre-Screening結束***  
115 可能的攻擊方式: Label Specific Backdoor Attack  
116 可能的 target-victim 配對: ['0-6', '5-6', '8-0', '8-6', '9-2', '11-2', '14-1']  
117 ***Trigger Reverse Engineering開始***  
118 Target: 8, victim: 6, Loss: 0.7750, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss: 145.16, Cost:0.01 best_reg:145.17 avg_loss_reg:145.17: 26%|████| 265/1000 [02:44<07:36, 1.61it/s]  
119 early stop 所有  
120 ***Trigger Reverse Engineering結束***  
121 Target Class: 8 Victim Class: 6 Trigger Size: 145.16424560546875 Optimization Steps: 134  
122 ***Symmetric Check開始***  
123 Target: 6, victim: 8, Loss: 4.2537, Acc: 70.00%, CE_Loss: 0.60, Reg_Loss: 2436.57, Cost:0.00 best_reg:2563.51 avg_loss_reg:2455.95: 100%|████| 134/134 [01:24<00:00, 1.59it/s]  
124 ***Symmetric Check結束***  
125 *****檢測結束*****  
126 檢測結果: Model含有後門(Anonymous)  
127 整體耗時: 255.505932121276855-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000752-----  
128 ***Pre-Screening開始***  
129 ***Pre-Screening結束***  
130 ***Pre-Screening結束***  
131 可能的攻擊方式: Label Specific Backdoor Attack  
132 可能的 target-victim 配對: ['0-13', '0-14', '2-14', '13-0']  
133 ***Trigger Reverse Engineering開始***  
134 Target: 0, victim: 13, Loss: 2.0598, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss: 108.70, Cost:0.02 best_reg:109.62 avg_loss_reg:109.62: 17%|████| 169/1000 [01:03<05:10, 2.67it/s]  
135 early stop 所有  
136 ***Trigger Reverse Engineering結束***  
137 Target Class: 0 Victim Class: 13 Trigger Size: 108.70454406738281 Optimization Steps: 137  
138 ***Symmetric Check開始***  
139 Target: 13, victim: 0, Loss: 2.8038, Acc: 100.00%, CE_Loss: 0.46, Reg_Loss: 308.37, Cost:0.01 best_reg:310.69 avg_loss_reg:310.69: 100%|████| 137/137 [00:54<00:00, 2.51it/s]  
140 ***Symmetric Check結束***  
141 *****檢測結束*****
```

```
142 檢測結果: Model是安全的(Benign)
143 整體耗時: 123.67250084877014 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000753
144 ***Pre-Screening開始***
145 ***Pre-Screening結束***
147 ***檢測結束***
148 檢測結果: Model是安全的(Benign)
149 整體耗時: 19.224700450897217 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000754
150
151 ***Pre-Screening開始***
152 ***Pre-Screening結束***
153 可能的攻擊方式: Label Specific Backdoor Attack
154 可能的 target-victim 配對: [0-1', '0-10', '1-10', '5-0', '7-1', '8-1', '10-0', '12-10']
155 ***Trigger Reverse Engineering開始***
156 Target: 1, victim: 0, Loss: 3.1015, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:51.88, Cost:0.06 best_reg:52.69: 17% █ | 174/1000 [02:17<10:54, 1.26it/s]
157 early stop 所有
158 ***Trigger Reverse Engineering結束***
159 Target Class: 0 Victim Class: 0 Trigger Size:51.879005432128906 Optimization Steps: 73
160 ***Symmetric Check開始***
161 Target: 0, victim: 1, Loss: 0.9551, Acc: 60.00%, Reg_Loss:13927.54, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:13906.94: 100% █ | 73/73 [00:57<00:00, 1.26it/s]
162 ***Symmetric Check結束***
163
164 檢測結果: Model含 有後門(Abnormal)
165 整體耗時: 201.69213438034058 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000755
166
167 ***Pre-Screening開始***
168 ***Pre-Screening結束***
169 可能的攻擊方式: Label Specific Backdoor Attack
170 可能的 target-victim 配對: [0-10]
171 ***Trigger Reverse Engineering開始***
172 Target: 0, victim: 10, Loss: 8.3246, Acc: 0.00%, CE_Loss: 8.32, Reg_Loss:2578.51, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2558.93: 1% | 10/1000 [00:31<51:39, 3.13s/t]
173 ***Trigger Reverse Engineering結束***
174 Target Class: 0 Victim Class: 10 Trigger Size: 10000000000.0 Optimization Steps: 11
175 ***Pre-Screening結束***
176 檢測結果: Model是安全的(Benign)
177 整體耗時: 46.552051305770874 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000756
178
179 ***Pre-Screening開始***
180 ***Pre-Screening結束***
181 可能的攻擊方式: Label Specific Backdoor Attack
182 可能的 target-victim 配對: [0-2', '0-5', '0-20', '4-11', '7-4', '7-10', '9-10', '9-16', '10-4', '10-16', '16-10', '18-6', '19-1', '20-4', '21-1']
183 ***Trigger Reverse Engineering開始***
184 Target: 0, victim: 20, Loss: 3.6779, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:308.73, Cost:0.01 best_reg:309.32 avg_loss_reg:310.01: 43% █ | 429/1000 [04:47<06:22, 1.49it/s]
185 0%
1/0/84 [00:00:<?, ?]it/searly stop 所有
186 ***Trigger Reverse Engineering結束***
187 Target Class: 0 Victim Class: 20 Trigger Size: 308.7345886230469 Optimization Steps: 184
188 ***Symmetric Check開始***
189 Target: 20, victim: 0 Loss: 0.0909, Acc: 100.00%, CE_Loss: 0.09, Reg_Loss:3841.01, Cost:0.00 best_reg:3812.84 avg_loss_reg:3812.84: 100% █ | 184/184 [01:59<00:00, 1.54it/s]
190 ***Symmetric Check結束***
191 ***Pre-Screening結束***
192 檢測結果: Model含 有後門(Abnormal)
193 整體耗時: 414.66723704338074 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000757
194
195 ***Pre-Screening開始***
196 ***Pre-Screening結束***
197 ***檢測結束***
198 檢測結果: Model是安全的(Benign)
199 整體耗時: 2.20637652581787
200
201 ***Pre-Screening開始***
202 ***Pre-Screening結束***
203 ***檢測結束***
204 檢測結果: Model是安全的(Benign)
205 整體耗時: 32.071468353271484 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000759
206
207 ***Pre-Screening開始***
208 ***Pre-Screening結束***
209 ***檢測結束***
210 檢測結果: Model是安全的(Benign)
211 整體耗時: 16.205012321472168 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000760
212
```

```
213 ***Pre-Screening開始***  
214 ***Pre-Screening結束***  
215 可能的攻擊方式: Label Specific Backdoor Attack  
216 可能的 target-victim 配對: ['4-7', '8-7', '11-7', '13-7', '15-4', '15-7']  
217 ***Trigger Reverse Engineering開始***  
218 Target: 15, victim: 7, Loss: 8.6291, Acc: 0.00%, CE_Loss: 8.63, Reg_Loss:2552.70, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2539.20: 8% █ | 75/1000 [01:10<14:27, 1.07it/s]  
219 ***Trigger Reverse Engineering結束***  
220 Target Class: 4 Victim Class: 7 Trigger Size:1000000000.0 Optimization Steps: 11  
221 *****檢測結束*****  
222 檢測結果: Model是安全的(Benign)  
223 整體耗時: 79.27002263069153  
224 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000761-----  
225 ***Pre-Screening開始***  
226 ***Pre-Screening結束***  
227 ***檢測結束***  
228 檢測結果: Model是安全的(Benign)  
229 整體耗時: 15.682577848434448  
230 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000762-----  
231 ***Pre-Screening開始***  
232 ***Pre-Screening結束***  
233 可能的攻擊方式: Label Specific Backdoor Attack  
234 可能的 target-victim 配對: ['7-4']  
235 ***Trigger Reverse Engineering開始***  
236 Target: 7, victim: 4, Loss: 2.7750, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:528.10, Cost:0.01 best_reg:528.73 avg_loss_reg:528.73: 16% █ | 158/1000 [17:04<1:31:00, 6.48s/it]  
237 early stop 所有  
238 ***Trigger Reverse Engineering結束***  
239 Target Class: 7 Victim Class: 4 Trigger Size: 528.1007080078125 Optimization Steps: 159  
240 ***Symmetric Check開始***  
241 Target: 4, victim: 7, Loss: 3.8423, Acc: 70.00%, CE_Loss: 0.45, Reg_Loss:3393.25, Cost:0.00 best_reg:3542.63 avg_loss_reg:3424.00: 100% █ | 159/159 [16:57<00:00, 6.40s/it]  
242 ***Symmetric Check結束***  
243 *****檢測結束*****  
244 檢測結果: Model是安全的(Benign)  
245 整體耗時: 2064.601437330246  
246 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000763-----  
247 ***Pre-Screening開始***  
248 ***Pre-Screening結束***  
249 ***檢測結束***  
250 檢測結果: Model是安全的(Benign)  
251 整體耗時: 9.846359729/66846  
252 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000764-----  
253 ***Pre-Screening開始***  
254 ***Pre-Screening結束***  
255 可能的攻擊方式: Label Specific Backdoor Attack  
256 可能的 target-victim 配對: ['14-2']  
257 ***Trigger Reverse Engineering開始***  
258 Target: 14, victim: 2, Loss: 7.5442, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:189.11, Cost:0.04 best_reg:190.61 avg_loss_reg:191.65: 12% █ | 123/1000 [02:34<18:20, 1.26s/it]  
259 early stop 所有  
260 ***Trigger Reverse Engineering結束***  
261 Target Class: 14 Victim Class: 2 Trigger Size: 189.10995483398438 Optimization Steps: 124  
262 ***Symmetric Check開始***  
263 Target: 2, victim: 14, Loss: 0.9953, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:2609.09, Cost:0.00 best_reg:2585.07 avg_loss_reg:2609.31: 100% █ | 124/124 [02:34<00:00, 1.24s/it]  
264 ***Symmetric Check結束***  
265 *****檢測結束*****  
266 檢測結果: Model含有後門(Abnormal)  
267 整體耗時: 316.583899974823  
268 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000765-----  
269 ***Pre-Screening開始***  
270 ***Pre-Screening結束***  
271 可能的攻擊方式: Label Specific Backdoor Attack  
272 可能的 target-victim 配對: ['2-10', '5-11', '6-13', '9-13', '10-5']  
273 ***Trigger Reverse Engineering開始***  
274 Target: 9, victim: 13, Loss: 3.8025, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:28.38, Cost:0.13 best_reg:30.13 avg_loss_reg:30.13: 16% █ | 160/1000 [00:38<03:20, 4.18it/s]  
275 early stop 所有  
276 ***Trigger Reverse Engineering結束***  
277 Target Class: 9 Victim Class: 13 Trigger Size: 28.38150405883789 Optimization Steps: 64  
278 ***Symmetric Check開始***  
279 Target: 13, victim: 9, Loss: 1.4509, Acc: 30.00%, CE_Loss: 1.45, Reg_Loss:14291.08, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:14139.52: 100% █ | 64/64 [00:14<00:00, 4.37it/s]  
280 ***Symmetric Check結束***  
281 *****檢測結束*****  
282 檢測結果: Model含有後門(Abnormal)  
283 整體耗時: 58.130786657333374
```

```

284     ***Pre-Screening開始***  

285     ***Pre-Screening結束***  

286     ***Pre-Screening結束***  

287     ***檢測結果結束***  

288     檢測結果: Model是安全的(Benign)  

289     整體耗時: 6.899338722229004  

290     -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000766-----  

291     ***Pre-Screening開始***  

292     ***Pre-Screening結束***  

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

294     可能的 target-victim 配對: ['2-0','2-6']  

295     ***Trigger Reverse Engineering開始***  

296     Target: 2, victim: 6, Loss: 2.6971, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss: 0.00, Reg_Loss_Reg:68.77: 11% █ | 110/1000 [12:31<1:41:22, 6.83s/it]  

297     early stop 所有  

298     ***Trigger Reverse Engineering結束***  

299     Target Class: 2 Victim Class: 6 Trigger Size: 70.12055969238281 Optimization Steps: 83  

300     ***Symmetric Check開始***  

301     Target: 6, victim: 2, Loss: 0.3983, Acc: 95.00%, CE_Loss: 0.40, Reg_Loss:13638.58, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:13604.31: 100% █ | 83/83 [09:20<00:00, 6.76s/it]  

302     ***Symmetric Check結束***  

303     *****檢測結束*****  

304     檢測結果: Model含有效門(Abnormal)  

305     整體耗時: 1326.538011789322 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000768-----  

306     ***Pre-Screening開始***  

307     ***Pre-Screening結束***  

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

309     可能的 target-victim 配對: ['9-12', '21-0']  

310     ***Trigger Reverse Engineering開始***  

311     Target: 21, victim: 0, Loss: 11.6559, Acc: 0.00%, CE_Loss: 11.66, Reg_Loss:2580.42, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2560.60: 3% | | 31/1000 [01:36<50:07, 3.10s/it]  

312     ***Trigger Reverse Engineering結束***  

313     Target Class: 9 Victim Class: 12 Trigger Size: 10000000000.0 Optimization Steps: 21  

314     ***檢測結束***  

315     檢測結果: Model是安全的(Benign)  

316     檢測結果: Model是安全的(Benign)  

317     整體耗時: 115.56473016738892 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000769-----  

318     ***Pre-Screening開始***  

319     ***Pre-Screening結束***  

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

321     可能的 target-victim 配對: ['1-8']  

322     ***Trigger Reverse Engineering開始***  

323     Target: 1, victim: 8, Loss: 8.2211, Acc: 10.00%, CE_Loss: 8.22, Reg_Loss:3189.18, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3014.48: 2% | | 20/1000 [00:26<21:48, 1.34s/it]  

324     ***Trigger Reverse Engineering結束***  

325     Target Class: 1 Victim Class: 8 Trigger Size: 10000000000.0 Optimization Steps: 21  

326     ***檢測結束***  

327     檢測結果: Model是安全的(Benign)  

328     檢測結果: Model是安全的(Benign)  

329     整體耗時: 34.30594301223755 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000770-----  

330     ***Pre-Screening開始***  

331     ***Pre-Screening結束***  

332     ***檢測結束***  

333     ***檢測結束***  

334     檢測結果: Model是安全的(Benign)  

335     整體耗時: 17.935478925704956 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000771-----  

336     ***Pre-Screening開始***  

337     ***Pre-Screening結束***  

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

339     可能的 target-victim 配對: ['0-6']  

340     ***Trigger Reverse Engineering開始***  

341     Target: 0, victim: 6, Loss: 6.2525, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:106.59, Cost:0.06 best_reg:106.69 avg_loss_reg:106.69: 8% █ | | 83/1000 [03:07<34:27, 2.25s/it]  

342     0% | 0/84 [00:00<?, ?] it/sleary stop 所有  

343     ***Trigger Reverse Engineering結束***  

344     Target Class: 0 Victim Class: 6 Trigger Size: 106.58892059326172 Optimization Steps: 84  

345     ***Symmetric Check開始***  

346     Target: 6, victim: 0, Loss: 0.8821, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:2463.58, Cost:0.00 best_reg:2494.91 avg_loss_reg:2494.91: 100% █ | | 84/84 [03:02<00:00, 2.18s/it]  

347     ***Symmetric Check結束***  

348     檢測結果: Model含有效門(Abnormal)  

349     *****檢測結束*****  

350     檢測結果: Model含有效門(Abnormal)  

351     整體耗時: 378.447524185955 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000772-----  

352     ***Pre-Screening開始***  

353     ***Pre-Screening結束***  

354     ***Pre-Screening結束***
```

```

355 可能的攻擊方式: Universal Backdoor Attack
356 可能的 target class: 11
357 可能的 victim classes: ALL
358 ***Trigger Reverse Engineering開始***
359 Target: 11, victim: 14, Loss: 0.1391, Acc: 96.88%, CE_Loss: 0.05, Reg_Loss:93.46, Cost:0.00 best_reg:94.09 avg_loss_reg:92.66: 6% █ | 57/1000 [38:22 < 10:34:44, 40.39s/it]
360 early stop 所有
361 ***Trigger Reverse Engineering結束***+
362 Target Class: 11 Victim Class: all Trigger Size: 94.08768463134766 Optimization Steps: 58
363 *****檢測結果: Model倉有後門(Abnormal)*****
364 檢測結果: Model倉有後門(Abnormal)
365 整體耗時: 2317.1598744392395
366 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000773-----
367 ***Pre-Screening開始***+
368 ***Pre-Screening結束***+
369 可能的攻擊方式: Label Specific Backdoor Attack
370 可能的 target-victim 配對: ['15-0']
371 ***Trigger Reverse Engineering開始***
372 Target: 15, victim: 0 Loss: 7.2363, Acc: 20.00%, CE_Loss: 7.24, Reg_Loss:3141.40, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3031.11: 2% █ | 20/1000 [02:18 < 1:52:59, 6.92s/it]
373 Target Class: 15 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 21
374 Target Class: 15 Victim Class: 0 Trigger Size: 10000000000.0 Optimization Steps: 21
375 *****檢測結果: Model是安全的(Benign)*****
376 檢測結果: Model是安全的(Benign)
377 整體耗時: 167.57727789878845
378 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000774-----
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: ['9-7']
383 ***Trigger Reverse Engineering開始***
384 Target: 9, victim: 7, Loss: 2.1305, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:36.66, Cost:0.06 best_reg:37.42 avg_loss_reg:36.11: 8% █ | 79/1000 [00:59 < 11:30, 1.33it/s]
385 0% | 0/80 [00:00 < ?, ?it/s]early stop 所有
386 ***Trigger Reverse Engineering結束***+
387 Target Class: 9 Victim Class: 7 Trigger Size: 36.661293029785156 Optimization Steps: 80
388 ***Symmetric Check開始***+
389 Target: 7, victim: 9, Loss: 1.4239, Acc: 30.00%, CE_Loss: 1.42, Reg_Loss:5385.00, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:5373.69: 100% █ | 80/80 [00:59 < 00:00, 1.35it/s]
390 *****檢測結果: Symmetric Check結束*****+
391 *****檢測結果: Model倉有後門(Abnormal)*****
392 檢測結果: Model倉有後門(Abnormal)
393 整體耗時: 127.45027923583984
394 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000775-----
395 ***Pre-Screening開始***+
396 ***Pre-Screening結束***+
397 ***檢測結果: Model是安全的(Benign)*****
398 檢測結果: Model是安全的(Benign)
399 整體耗時: 2.869412660598755
400 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000776-----
401 ***Pre-Screening開始***+
402 ***Pre-Screening結束***+
403 可能的攻擊方式: Label Specific Backdoor Attack
404 可能的 target-victim 配對: ['11-6']
405 ***Trigger Reverse Engineering開始***
406 Target: 11, victim: 6, Loss: 2.3677, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:2170.13, Cost:0.00 best_reg:2179.99 avg_loss_reg:2171.31: 24% █ | 241/1000 [43:42 < 2:17:39, 10.88s/it]
407 early stop 所有
408 ***Trigger Reverse Engineering結束***+
409 Target Class: 11 Victim Class: 6 Trigger Size: 2170.130859375 Optimization Steps: 242
410 *****檢測結果: Model是安全的(Benign)*****
411 檢測結果: Model是安全的(Benign)
412 整體耗時: 2666.1472220420837
413 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000777-----
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: ['1-5','2-10','9-5','10-2','12-11']
418 ***Trigger Reverse Engineering開始***
419 Target: 1, victim: 5, Loss: 0.8391, Acc: 100.00%, CE_Loss: 0.15, Reg_Loss:688.32, Cost:0.00 best_reg:700.22 avg_loss_reg:687.22: 37% █ | 369/1000 [20:08 < 34:26, 3.27s/it]
420 0% | 0/260 [00:00 < ?, ?it/s]early stop 所有
421 ***Trigger Reverse Engineering結束***+
422 Target Class: 1 Victim Class: 5 Trigger Size: 688.3182373046875 Optimization Steps: 260
423 ***Symmetric Check開始***+
424 Target: 5, victim: 1, Loss: 1.6722, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:3243.79, Cost:0.00 best_reg:3223.84 avg_loss_reg:3267.67: 100% █ | 260/260 [13:59 < 00:00, 3.23s/it]
425 ***Symmetric Check結束***+

```

```
426 *****檢測結束*****  
427 檢測結果: Model是安全的(Benign)  
428 整體耗時: 2063.03804397583  
429 *****Pre-Screening開始***  
430 *****Pre-Screening結束***  
432 *****檢測結束***  
433 檢測結果: Model是安全的(Benign)  
434 整體耗時: 2.58328676237549  
435 *****Pre-Screening開始***  
436 *****Pre-Screening結束***  
437 *****Pre-Screening結束***  
438 *****檢測結束***  
439 檢測結果: Model是安全的(Benign)  
440 整體耗時: 2.704631805419922  
441 *****Pre-Screening開始***  
442 *****Pre-Screening結束***  
443 *****Pre-Screening結束***  
444 *****檢測結束***  
445 檢測結果: Model是安全的(Benign)  
446 整體耗時: 19.656209230422974  
447 *****Pre-Screening開始***  
448 *****Pre-Screening結束***  
449 *****Pre-Screening結束***  
450 可能的攻擊方式: Label Specific Backdoor Attack  
451 可能的 target-victim 配對: ['1-5']  
452 ***Trigger Reverse Engineering 開始***  
453 Target: 1, victim: 5, Loss: 12.8363, Acc: 0.00%, CE_Loss: 12.84, Reg_Loss: 2577.17, Cost: 0.00 best_reg: 1000000000.00 avg_loss_reg: 2558.08; 1%| | 10/1000 [0:30 < 50:08, 3.04s/it]  
454 ***Trigger Reverse Engineering 結束***  
455 Target Class: 1 Victim Class: 5 Trigger Size: 1000000000.0 Optimization Steps: 11  
456 *****檢測結束*****  
457 檢測結果: Model是安全的(Benign)  
458 整體耗時: 43.1914324760437  
459 *****檢測結束*****  
460 *****Pre-Screening開始***  
461 *****Pre-Screening結束***  
462 *****檢測結束***  
463 檢測結果: Model是安全的(Benign)  
464 整體耗時: 21.898661136627197  
465 *****Pre-Screening開始***  
466 *****Pre-Screening結束***  
467 *****Pre-Screening結束***  
468 *****檢測結束***  
469 檢測結果: Model是安全的(Benign)  
470 整體耗時: 7.11773419380188  
471 *****Pre-Screening開始***  
472 *****Pre-Screening結束***  
473 *****Pre-Screening結束***  
474 *****檢測結束***  
475 檢測結果: Model是安全的(Benign)  
476 整體耗時: 2.686446189880371  
477 *****Pre-Screening開始***  
478 *****Pre-Screening結束***  
479 *****Pre-Screening結束***  
480 可能的攻擊方式: Label Specific Backdoor Attack  
481 可能的 target-victim 配對: ['7-16', '10-6', '13-8']  
482 ***Trigger Reverse Engineering 開始***  
483 Target: 13, victim: 8, Loss: 1.7891, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss: 487.60, Cost: 0.00 best_reg: 489.38 avg_loss_reg: 1416.41: 100%| | 189/1000 [05:48 < 24:53, 1.84s/it]  
484 early stop 所有  
485 ***Trigger Reverse Engineering 結束***  
486 Target Class: 13 Victim Class: 8 Trigger Size: 487.60400390625 Optimization Steps: 168  
487 ***Symmetric Check開始***  
488 Target: 8, victim: 13, Loss: 0.6030, Acc: 90.00%, CE_Loss: 0.44, Reg_Loss: 14243.52, Cost: 0.00 best_reg: 21949.79 avg_loss_reg: 168/168 [05:07 < 00:00, 1.83s/it]  
489 ***Symmetric Check 結束***  
490 *****檢測結束*****  
491 檢測結果: Model含有後門(Abnormal)  
492 整體耗時: 666.1707537174225  
493 *****檢測結束***  
494 *****Pre-Screening開始***  
495 *****Pre-Screening結束***  
496 *****檢測結束***
```

```
497 檢測結果: Model是安全的(Benign)
498 整體耗時: 34.32105898857117 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000787-----
499 ***Pre-Screening開始****
500 ***Pre-Screening結束****
501 ***Pre-Screening結束****
502 ***檢測結果****
503 檢測結果: Model是安全的(Benign)
504 整體耗時: 14.376377582550049 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000788-----
505 ***Pre-Screening開始****
506 ***Pre-Screening結束****
507 ***Pre-Screening結束****
508 ***檢測結果****
509 檢測結果: Model是安全的(Benign)
510 整體耗時: 13.573931455612183 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000789-----
511 ***Pre-Screening開始****
512 ***Pre-Screening結束****
513 ***Pre-Screening結束****
514 ***檢測結果****
515 檢測結果: Model是安全的(Benign)
516 整體耗時: 21.163976907730103 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000790-----
517 ***Pre-Screening開始****
518 ***Pre-Screening結束****
519 ***Pre-Screening結束****
520 ***檢測結果****
521 檢測結果: Model是安全的(Benign)
522 整體耗時: 6.014713287353516 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000791-----
523 ***Pre-Screening開始****
524 ***Pre-Screening結束****
525 ***Pre-Screening結束****
526 可能的攻擊方式: Universal Backdoor Attack
527 可能的 target class: 2
528 可能的 victim classes: ALL
529 ***Trigger Reverse Engineering 開始****
530 Target: 2, victim: 9, Loss: 0.9456, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:578.73, Cost:0.00 best_reg:558.53 avg_loss_reg:565.11: 11% █ | 110/1000 [57:07 < 7:42:14, 31.16s/it]
531 early stop 所有
532 ***Trigger Reverse Engineering 結束****
533 Target Class: 2 Victim Class: all Trigger Size: 558.5330657958984 Optimization Steps: 111
534 *****檢測結束*****
535 檢測結果: Model含有後門(Abnormal)
536 整體耗時: 3447.483966112137 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000792-----
537 ***Pre-Screening開始****
538 ***Pre-Screening結束****
539 ***Pre-Screening結束****
540 ***檢測結果****
541 檢測結果: Model是安全的(Benign)
542 整體耗時: 13.42529582977295 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000793-----
543 ***Pre-Screening開始****
544 ***Pre-Screening結束****
545 ***Pre-Screening結束****
546 可能的攻擊方式: Universal Backdoor Attack
547 可能的 target class: 8
548 可能的 victim classes: ALL
549 ***Trigger Reverse Engineering 開始****
550 Target: 8, victim: 22, Loss: 0.5168, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:740.33, Cost:0.00 best_reg:730.90 avg_loss_reg:734.34: 8% █ | 81/1000 [1:20:20 < 15:1:28, 59.51s/it]
551 early stop 所有
552 ***Trigger Reverse Engineering 結束****
553 Target Class: 8 Victim Class: all Trigger Size: 730.9016723632812 Optimization Steps: 82
554 *****檢測結束*****
555 檢測結果: Model含有後門(Abnormal)
556 整體耗時: 4834.056268930435 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000794-----
557 ***Pre-Screening開始****
558 ***Pre-Screening結束****
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: [6-1]
562 ***Trigger Reverse Engineering 開始****
563 Target: 6, victim: 1, Loss: 12.7432, Acc: 0.00%, CE_Loss: 12.74, Reg_Loss:2539.56, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2530.27: 1% | 10/1000 [01:12 < 1:59:47, 7.26s/it]
564 ***Trigger Reverse Engineering 結束****
565 Target Class: 6 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11
566 *****檢測結束*****
567 檢測結果: Model是安全的(Benign)
```

整體耗時: 92.16798639297485
569 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000795-----
570 ***Pre-Screening開始***
571 可能的攻擊方式: Label Specific Backdoor Attack
572 可能的 target-victim 配對: [0-1', '4-5', '5-0', '5-3']
573 ***Trigger Reverse Engineering 開始***
574 Target: 5, victim: 3, Loss: 9.0277, Acc: 0.00%, CE_Loss: 9.03, Reg_Loss:2542.16, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2532.33: 4% █ | 43/1000 [02:21 < 52:30, 3.29s/it]
575 Target Class: 0 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11
576 ***Trigger Reverse Engineering 結束***
577 Target Class: 0 Victim Class: 1 Trigger Size: 1000000000.0 Optimization Steps: 11
578 *****檢測結束*****
579 檢測結果: Model是安全的(Benign)
580 整體耗時: 150.16335463523865
581 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000796-----
582 ***Pre-Screening開始***
583 ***Pre-Screening 結束***
584 ***檢測結束***
585 檢測結果: Model是安全的(Benign)
586 整體耗時: 19.273258447647095
587 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000797-----
588 ***Pre-Screening開始***
589 ***Pre-Screening 結束***
590 可能的攻擊方式: Universal Backdoor Attack
591 可能的 target class: 1
592 可能的 victim classes: ALL
593 ***Trigger Reverse Engineering 開始***
594 Target: 1, victim: 19, Loss: 1.2937, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:6532.86, Cost:0.00 best_reg:6585.44 avg_loss_reg:6503.59: 12% █ | 122/1000 [44:12 < 5:18:10, 21.74s/it]
595 early stop 所有
596 ***Trigger Reverse Engineering 結束***
597 Target Class: all Trigger Size: 6585.442731584822 Optimization Steps: 123
598 *****檢測結束*****
599 檢測結果: Model是安全的(Benign)
600 整體耗時: 2668.064249277115
601 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000798-----
602 ***Pre-Screening開始***
603 ***Pre-Screening 結束***
604 ***檢測結束***
605 檢測結果: Model是安全的(Benign)
606 整體耗時: 31.05341386795044
607 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000799-----
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: [0-2', '0-3', '0-4']
612 ***Trigger Reverse Engineering 開始***
613 Target: 0, victim: 3, Loss: 5.4244, Acc: 100.00%, CE_Loss: 0.37, Reg_Loss:295.78, Cost:0.02 best_reg:299.45 avg_loss_reg:299.45: 18% █ | 185/1000 [00:44 < 03:14, 4.19it/s]
614 0% | 0/163 [00:00 < ?, ?it/s]early stop 所有
615 ***Trigger Reverse Engineering 結束***
616 Target Class: 0 Victim Class: 3 Trigger Size: 295.7810363769531 Optimization Steps: 163
617 ***Symmetric Check開始***
618 Target: 3, victim: 0, Loss: 2.0759, Acc: 100.00%, CE_Loss: 0.37, Reg_Loss:1701.28, Cost:0.00 best_reg:1701.88 avg_loss_reg:1701.88: 100% █ | 163/163 [00:38 < 00:00, 4.23it/s]
619 ***Symmetric Check 結束***
620 *****檢測結束*****
621 檢測結果: Model是安全的(Benign)
622 整體耗時: 84.23969006538391
623 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000800-----
624 ***Pre-Screening開始***
625 ***Pre-Screening 結束***
626 可能的攻擊方式: Universal Backdoor Attack
627 可能的 target class: 0
628 可能的 victim classes: ALL
629 ***Trigger Reverse Engineering 開始***
630 Target: 0, victim: 20, Loss: 0.1459, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:1024.20, Cost:0.00 best_reg:1026.09 avg_loss_reg:1008.44: 7% █ | 72/1000 [1:31:07 < 19:34:36, 75.94s/it]
631 early stop 所有
632 ***Trigger Reverse Engineering 結束***
633 Target Class: all Trigger Size: 1026.0934491838727 Optimization Steps: 73
634 *****檢測結束*****
635 檢測結果: Model含有後門(Abnormal)
636 整體耗時: 5484.463182926178
637 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000801-----
638 ***Pre-Screening開始***

```

639 ***Pre-Screening結束***  

640 ***檢測結果***  

641 檢測結果: Model是安全的(Benign)  

642 整體耗時: 8.984658002853394  

643 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000802-----  

644 ***Pre-Screening開始***  

645 ***Pre-Screening結束***  

646 可能的攻擊方式: Universal Backdoor Attack  

647 可能的 target class: 0  

648 可能的 victim classes: ALL  

649 ***Trigger Reverse Engineering開始***  

650 Target: 0, victim: 3, Loss: 1.759, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:19.43, Cost:0.09 best_reg:19.59 avg_loss_reg:19.59: 6% █ | 63/1000 [03:14<48:16, 3.09s/it]  

651 early stop 所有  

652 ***Trigger Reverse Engineering結束***  

653 Target Class: 0 Victim Class: all Trigger Size: 19.48233127593994 Optimization Steps: 64  

654 -----檢測結束*****  

655 檢測結果: Model含有後門(Abnormal)  

656 整體耗時: 196.71590375900269  

657 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000803-----  

658 ***Pre-Screening開始***  

659 ***Pre-Screening結束***  

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

661 可能的 target-victim 配對: ['9_0','11_0']  

662 ***Trigger Reverse Engineering開始***  

663 Target: 11, victim: 0, Loss: 7.0466, Acc: 0.00%, CE_Loss: 7.05, Reg_Loss:2556.58, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2542.14: 2% | | 21/1000 [02:04<1:36:47, 5.93s/it]  

664 ***Trigger Reverse Engineering結束***  

665 Target Class: 0 Victim Class: 0 Trigger Size: 1000000000.0 Optimization Steps: 11  

666 -----檢測結束*****  

667 檢測結果: Model是安全的(Benign)  

668 整體耗時: 143.06681632995605  

669 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000804-----  

670 ***Pre-Screening開始***  

671 ***Pre-Screening結束***  

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

673 可能的 target-victim 配對: ['1-7','1-11','10-8','12-11','15-9']  

674 ***Trigger Reverse Engineering開始***  

675 Target: 1, victim: 11, Loss: 1.5253, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:390.88, Cost:0.00 best_reg:392.85 avg_loss_reg:392.85: 30% █ | | 301/1000 [03:00<07:00, 1.66it/s]  

676 early stop 所有  

677 ***Trigger Reverse Engineering結束***  

678 Target Class: 1 Victim Class: 11 Trigger Size: 390.88421630859375 Optimization Steps: 257  

679 ***Symmetric Check開始***  

680 Target: 11, victim: 1, Loss: 1.8034, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:1025.44, Cost:0.00 best_reg:1020.51 avg_loss_reg:1025.47: 100% █ | | 257/257 [02:29<00:00, 1.72it/s]  

681 ***Symmetric Check結束***  

682 -----檢測結束*****  

683 檢測結果: Model是安全的(Benign)  

684 整體耗時: 337.3044583797455  

685 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000805-----  

686 ***Pre-Screening開始***  

687 ***Pre-Screening結束***  

688 可能的攻擊方式: Universal Backdoor Attack  

689 可能的 target class: 11  

690 可能的 victim classes: ALL  

691 ***Trigger Reverse Engineering開始***  

692 Target: 11, victim: 9, Loss: 0.4463, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:126.55, Cost:0.00 best_reg:127.59 avg_loss_reg:126.11: 7% █ | | 72/1000 [38:16<8:13:23, 31.90s/it]  

693 early stop 所有  

694 ***Trigger Reverse Engineering結束***  

695 Target Class: 11 Victim Class: all Trigger Size: 127.58805847167969 Optimization Steps: 73  

696 -----檢測結束*****  

697 檢測結果: Model含有後門(Abnormal)  

698 整體耗時: 2310.836585044861  

699 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000806-----  

700 ***Pre-Screening開始***  

701 ***Pre-Screening結束***  

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

703 可能的 target-victim 配對: ['7-8']  

704 ***Trigger Reverse Engineering開始***  

705 Target: 7, victim: 8, Loss: 2.7551, Acc: 100.00%, CE_Loss: 0.27, Reg_Loss:490.34, Cost:0.01 best_reg:496.34 avg_loss_reg:496.34: 14% █ | | 144/1000 [08:47<52:18, 3.67s/it]  

706 early stop 所有  

707 ***Trigger Reverse Engineering結束***  

708 Target Class: 7 Victim Class: 8 Trigger Size: 490.33782958984375 Optimization Steps: 145  

709 ***Symmetric Check開始***  


```

```

710 Target: 8, victim: 7, Loss: 3.3355, Acc: 90.00%, CE_Loss: 0.41, Reg_Loss:4394.37, Cost:0.00 best_reg:4504.04 avg_loss_reg:4424.29: 100%|████████| 145/145 [08:46<00:00, 3.63s/it]

711 ***Symmetric Check結束***

712 *****檢測結束***** 

713 檢測結果: Model是安全的(Benign)

714 整體耗時: 1071.4055304527283

715 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000807-----
```

```

716 ***Pre-Screening開始***

717 ***Pre-Screening結束***

718 ***檢測結束***

719 檢測結果: Model是安全的(Benign)

720 整體耗時: 25.581960439682007

721 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000808-----
```

```

722 ***Pre-Screening開始***

723 ***Pre-Screening結束***

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

725 可能的 target-victim 配對: ['1-17', '1-22', '2-17', '3-17', '4-8', '4-21', '5-11', '12-9', '13-8', '14-10', '15-17', '18-11', '23-1', '23-7']

726 ***Trigger Reverse Engineering開始***

727 Target: 23, victim: 1, Loss: 1.3568, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:161.31, Cost:0.01 best_reg:162.18 avg_loss_reg:161.61: 46%|████| 464/1000 [1:01:06<1:10:35, 7.90s/it]

728 early stop 所有

729 ***Trigger Reverse Engineering結束***

730 Target Class: 23 Victim Class: 1 Trigger Size: 161.30975341796875 Optimization Steps: 213

731 ***Symmetric Check開始***

732 Target: 1, victim: 23, Loss: 5.9114, Acc: 100.00%, CE_Loss: 0.36, Reg_Loss:730.72, Cost:0.01 best_reg:732.96 avg_loss_reg:732.08: 86%|████| 184/213 [24:14<03:49, 7.91s/it]

733 early stop 所有

734 ***Symmetric Check結束***

735 *****檢測結束***** 

736 檢測結果: Model是安全的(Benign)

737 整體耗時: 5157.744780778885

738 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000809-----
```

```

739 ***Pre-Screening開始***

740 ***Pre-Screening結束***

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

742 可能的 target-victim 配對: ['2-9', '6-9', '7-14', '13-1']

743 ***Trigger Reverse Engineering開始***

744 Target: 13, victim: 1, Loss: 3.7780, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:1586.43, Cost:0.00 best_reg:1586.75 avg_loss_reg:1587.19: 24%|████| 243/1000 [18:19<57:04, 4.52s/it]

745 early stop 所有

746 ***Trigger Reverse Engineering結束***

747 Target Class: 13 Victim Class: 1 Trigger Size: 1586.426513671875 Optimization Steps: 211

748 *****檢測結束***** 

749 檢測結果: Model是安全的(Benign)

750 整體耗時: 1125.8866560459137

751 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000810-----
```

```

752 ***Pre-Screening開始***

753 ***Pre-Screening結束***

754 ***檢測結束***

755 檢測結果: Model是安全的(Benign)

756 整體耗時: 18.07299256324768

757 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000811-----
```

```

758 ***Pre-Screening開始***

759 ***Pre-Screening結束***

760 ***檢測結束***

761 檢測結果: Model是安全的(Benign)

762 整體耗時: 11.91101622581482

763 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000812-----
```

```

764 ***Pre-Screening開始***

765 ***Pre-Screening結束***

766 ***檢測結束***

767 檢測結果: Model是安全的(Benign)

768 整體耗時: 10.990734338760376

769 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000813-----
```

```

770 ***Pre-Screening開始***

771 ***Pre-Screening結束***

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

773 可能的 target-victim 配對: ['3-1', '3-4', '3-9', '4-12', '4-16', '4-3', '5-3', '5-11', '8-16', '8-3', '8-12', '10-9', '11-12', '12-11', '16-11', '16-12', '19-1']

774 ***Trigger Reverse Engineering開始***

775 Target: 16, victim: 12, Loss: 2.3299, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:408.74, Cost:0.01 best_reg:415.49 avg_loss_reg:411.85: 34%|████| 338/1000 [21:05<41:19, 3.74s/it]

776 early stop 所有

777 ***Trigger Reverse Engineering結束***

778 Target Class: 16 Victim Class: 12 Trigger Size: 408.7350769042969 Optimization Steps: 121

779 ***Symmetric Check開始***

780 Target: 12, victim: 16, Loss: 1.0892, Acc: 60.00%, CE_Loss: 1.09, Reg_Loss:13665.04, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:13660.21: 100%|████| 121/121 [07:22<00:00, 3.65s/it]
```

```
781 ***Symmetric Check結束***  
782 *****檢測結束*****  
783 檢測結果: Model含有後門(Abnormal)  
784 整體耗時: 1726.4608261585236  
785 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000814-----  
786 ***Pre-Screening開始***  
787 ***Pre-Screening結束***  
788 ***檢測結束***  
789 檢測結果: Model是安全的(Benign)  
790 整體耗時: 8.278771162033081  
791 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000815-----  
792 ***Pre-Screening開始***  
793 ***Pre-Screening結束***  
794 ***檢測結束***  
795 檢測結果: Model是安全的(Benign)  
796 整體耗時: 17.821948289871216  
797 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000816-----  
798 ***Pre-Screening開始***  
799 ***Pre-Screening結束***  
800 可能的攻擊方式: Label Specific Backdoor Attack  
801 可能的 target-victim 配對: ['5-6']  
802 ***Trigger Reverse Engineering 開始***  
803 Target: 5, victim: 6, Loss: 7.1757, Acc: 5.00%, CE_Loss: 7.18, Reg_Loss:3142.62, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3009.77: 2%| | 20/1000 [00:16<13:32, 1.21it/s]  
804 ***Trigger Reverse Engineering 結束***  
805 Target Class: 5 Victim Class: 6 Trigger Size: 1000000000.0 Optimization Steps: 21  
806 *****檢測結束*****  
807 檢測結果: Model是安全的(Benign)  
808 整體耗時: 22.332966566085815  
809 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000817-----  
810 ***Pre-Screening開始***  
811 ***Pre-Screening結束***  
812 可能的攻擊方式: Universal Backdoor Attack  
813 可能的 target class: 4  
814 可能的 victim classes: ALL  
815 ***Trigger Reverse Engineering 開始***  
816 Target: 4, victim: 6, Loss: 0.7965, Acc: 96.88%, CE_Loss: 0.33, Reg_Loss:138.17, Cost:0.00 best_reg:136.75 avg_loss_reg:138.10: 9%| | 186/1000 [22:19<3:57:12, 15.57s/t]  
817 early stop 所有  
818 ***Trigger Reverse Engineering 結束***  
819 Target Class: 4 Victim Class: all Trigger Size: 136.74974365234374 Optimization Steps: 87  
820 *****檢測結束*****  
821 檢測結果: Model含有後門(Abnormal)  
822 整體耗時: 1345.1702678203583  
823 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000818-----  
824 ***Pre-Screening開始***  
825 ***Pre-Screening結束***  
826 可能的攻擊方式: Label Specific Backdoor Attack  
827 可能的 target-victim 配對: ['0-12', '1-2', '1-11', '3-2', '6-4', '7-4', '7-11', '8-4', '9-10', '12-1', '13-2', '13-11', '14-13']  
828 ***Trigger Reverse Engineering 開始***  
829 Target: 8, victim: 4, Loss: 3.8578, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:1052.67, Cost:0.00 best_reg:1053.39 avg_loss_reg:1069.02: 43%| | 431/1000 [04:04<05:22, 1.77it/s]  
830 early stop 所有  
831 ***Trigger Reverse Engineering 結束***  
832 Target Class: 8 Victim Class: 4 Trigger Size: 1052.66552734375 Optimization Steps: 268  
833 *****檢測結束*****  
834 檢測結果: Model是安全的(Benign)  
835 整體耗時: 249.66332411766052  
836 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000819-----  
837 ***Pre-Screening開始***  
838 ***Pre-Screening結束***  
839 ***檢測結束***  
840 檢測結果: Model是安全的(Benign)  
841 整體耗時: 15.670140266418457  
842 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000820-----  
843 ***Pre-Screening開始***  
844 ***Pre-Screening結束***  
845 可能的攻擊方式: Label Specific Backdoor Attack  
846 可能的 target-victim 配對: ['13-2']  
847 ***Trigger Reverse Engineering 開始***  
848 Target: 13, victim: 2, Loss: 3.8271, Acc: 100.00%, CE_Loss: 0.39, Reg_Loss:1019.13, Cost:0.00 best_reg:1020.10 avg_loss_reg:1020.10: 28%| | 277/1000 [03:45<09:49, 1.23it/s]  
849 early stop 所有  
850 ***Trigger Reverse Engineering 結束***  
851 Target Class: 13 Victim Class: 2 Trigger Size: 1019.13, Cost:0.00 best_reg:1020.10 avg_loss_reg:1020.10: 28%| | 277/1000 [03:45<09:49, 1.23it/s]
```

```
852 *****檢測結束*****  
853 檢測結果: Model是安全的(Benign)  
854 整體耗時: 232.1439459323883  
855 *****Pre-Screening開始*****  
856 *****Pre-Screening結束*****  
857 *****Pre-Screening結束*****  
858 *****檢測結束*****  
859 檢測結果: Model是安全的(Benign)  
860 整體耗時: 12.125516414642334  
861 *****Pre-Screening開始*****  
862 *****Pre-Screening結束*****  
863 可能的攻擊方式: Label Specific Backdoor Attack  
864 可能的 target-victim 配對: ['2-1']  
865 ***Trigger Reverse Engineering開始***  
866 Target: 2, victim: 1, Loss: 9.0563, Acc: 15.00%, CE_Loss: 9.06, Reg_Loss:3852.34, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:3518.61: 2%| | 20/1000 [02:23 < 1:56:53, 7.16s/it]  
867 Target Class: 2 Victim Class: 1 Trigger Size:10000000000.0 Optimization Steps: 21  
868 ***Trigger Reverse Engineering結束***  
869 Target Class: 2 Victim Class: 1 Trigger Size:10000000000.0 Optimization Steps: 21  
870 *****Pre-Screening結束*****  
871 檢測結果: Model是安全的(Benign)  
872 整體耗時: 163.78042578697205  
873 *****Pre-Screening開始*****  
874 *****Pre-Screening結束*****  
875 可能的攻擊方式: Label Specific Backdoor Attack  
876 可能的 target-victim 配對: ['2-15', '9-15', '10-15', '19-1']  
877 ***Trigger Reverse Engineering開始***  
878 Target: 19, victim: 1, Loss: 10.3378, Acc: 0.00%, CE_Loss: 10.34, Reg_Loss:2542.22, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2532.59: 4%| | 43/1000 [00:41 < 15:33, 1.03it/s]  
879 Target Class: 2 Victim Class: 15 Trigger Size: 1000000000.0 Optimization Steps: 11  
880 ***Trigger Reverse Engineering結束***  
881 Target Class: 2 Victim Class: 15 Trigger Size: 1000000000.0 Optimization Steps: 11  
882 *****Pre-Screening結束*****  
883 檢測結果: Model是安全的(Benign)  
884 整體耗時: 50.26493692398071  
885 *****Pre-Screening開始*****  
886 *****Pre-Screening結束*****  
887 *****Pre-Screening結束*****  
888 *****檢測結束*****  
889 檢測結果: Model是安全的(Benign)  
890 整體耗時: 27.854203701019287  
891 *****Pre-Screening開始*****  
892 *****Pre-Screening結束*****  
893 *****Pre-Screening結束*****  
894 *****檢測結束*****  
895 檢測結果: Model是安全的(Benign)  
896 整體耗時: 17.87335991859436  
897 *****Pre-Screening開始*****  
898 *****Pre-Screening結束*****  
899 *****Pre-Screening結束*****  
900 *****檢測結束*****  
901 檢測結果: Model是安全的(Benign)  
902 整體耗時: 23.094658374786377  
903 *****Pre-Screening開始*****  
904 *****Pre-Screening結束*****  
905 *****Pre-Screening結束*****  
906 可能的攻擊方式: Label Specific Backdoor Attack  
907 可能的 target-victim 配對: ['3-9', '5-9', '6-8']  
908 ***Trigger Reverse Engineering開始***  
909 Target: 6, victim: 8, Loss: 10.1556, Acc: 20.00%, CE_Loss: 10.16, Reg_Loss:2931.77, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2841.27: 6%| | 62/1000 [00:36 < 09:08, 1.71it/s]  
910 ***Trigger Reverse Engineering結束***  
911 Target Class: 3 Victim Class: 9 Trigger Size: 1000000000.0 Optimization Steps: 21  
912 *****Pre-Screening結束*****  
913 檢測結果: Model是安全的(Benign)  
914 整體耗時: 42.6524178381781  
915 *****Pre-Screening開始*****  
916 *****Pre-Screening結束*****  
917 *****Pre-Screening結束*****  
918 *****檢測結束*****  
919 檢測結果: Model是安全的(Benign)  
920 整體耗時: 12.439329147338867  
921 *****Pre-Screening開始*****  
922 *****Pre-Screening結束*****
```

```

923 ***Pre-Screening結束***  

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

925 可能的 target-victim 配對: ['1-2', '1-4', '1-20', '8-7', '12-7', '13-20', '19-20', '20-1', '21-7', '21-8']  

926 ***Trigger Reverse Engineering開始***  

927 Target: 21, victim: 8, Loss: 6.5099, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:111.47, Cost:0.06 best_reg:113.53 avg_loss_reg:113.53: 37% █ | 371/1000 [02:21<04:00, 2.61it/s]  

928 early stop 所有  

929 ***Trigger Reverse Engineering結束***  

930 Target Class: 21 Victim Class: 8 Trigger Size: 111.47022247314453 Optimization Steps: 89  

931 ***Symmetric Check開始***  

932 Target: 8, victim: 21, Loss: 4.2790, Acc: 70.00%, CE_Loss: 0.54, Reg_Loss:328.55, Cost:0.01 best_reg:471.52 avg_loss_reg:336.53: 100% █ | 89/89 [00:34<00:00, 2.57it/s]  

933 ***Symmetric Check結束***  

934 整體耗時: 182.84737386975098  

935 檢測結果: Model是安全的(Benign)  

936 訊息: 整體耗時: 182.84737386975098  

937 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000830-----  

938 ***Pre-Screening開始***  

939 ***Pre-Screening結束***  

940 可能的攻擊方式: Universal Backdoor Attack  

941 可能的 target class: 11  

942 可能的 victim classes: ALL  

943 ***Trigger Reverse Engineering開始***  

944 Target: 11, victim: 11, Loss: 0.2723, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:53.79, Cost:0.01 best_reg:53.38 avg_loss_reg:53.76: 6% █ | 64/1000 [1:03:08<15:23:25, 59.19s/it]  

945 early stop 所有  

946 ***Trigger Reverse Engineering結束***  

947 Target Class: 11 Victim Class: all Trigger Size: 53.376094818115234 Optimization Steps: 65  

948 *****檢測結束*****  

949 檢測結果: Model含有後門(Abnormal)  

950 整體耗時: 3802.1978306770325  

951 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000831-----  

952 ***Pre-Screening開始***  

953 ***Pre-Screening結束***  

954 ***檢測結束***  

955 檢測結果: Model是安全的(Benign)  

956 整體耗時: 12.931822061538696  

957 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000832-----  

958 ***Pre-Screening開始***  

959 ***Pre-Screening結束***  

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

961 可能的 target-victim 配對: ['12-0', '13-9', '16-1']  

962 ***Trigger Reverse Engineering開始***  

963 Target: 13, victim: 9, Loss: 0.8185, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:43.14, Cost:0.02 best_reg:43.39 avg_loss_reg:43.39: 13% █ | 132/1000 [01:22<09:05, 1.59it/s]  

964 early stop 所有  

965 ***Trigger Reverse Engineering結束***  

966 Target Class: 13 Victim Class: 9 Trigger Size: 43.13946533203125 Optimization Steps: 100  

967 ***Symmetric Check開始***  

968 Target: 9, victim: 13, Loss: 3.0269, Acc: 95.00%, CE_Loss: 0.62, Reg_Loss:714.14, Cost:0.00 best_reg:735.42 avg_loss_reg:735.42: 100% █ | 100/100 [01:02<00:00, 1.61it/s]  

969 ***Symmetric Check結束***  

970 *****檢測結束*****  

971 檢測結果: Model含有後門(Abnormal)  

972 整體耗時: 152.39497065544128  

973 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000833-----  

974 ***Pre-Screening開始***  

975 ***Pre-Screening結束***  

976 ***檢測結束***  

977 檢測結果: Model是安全的(Benign)  

978 整體耗時: 2.233386993408203  

979 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000834-----  

980 ***Pre-Screening開始***  

981 ***Pre-Screening結束***  

982 ***檢測結束***  

983 檢測結果: Model是安全的(Benign)  

984 整體耗時: 13.179946422576904  

985 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000835-----  

986 ***Pre-Screening開始***  

987 ***Pre-Screening結束***  

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

989 可能的 target-victim 配對: ['2-5', '4-2', '4-3', '6-0']  

990 ***Trigger Reverse Engineering開始***  

991 Target: 4, victim: 2, Loss: 1.2223, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss:215.50, Cost:0.01 best_reg:215.96 avg_loss_reg:215.96: 31% █ | 312/1000 [55:47<2:03:01, 10.73s/it]  

992 early stop 所有  

993 ***Trigger Reverse Engineering結束***
```

994 Target Class: 4 Victim Class: 2 Trigger Size: 215.4962158203125 Optimization Steps: 149

995 ***Symmetric Check開始***

996 Target: 2, victim: 4, Loss: 1.0330, Acc: 75.00%, CE_Loss: 1.03, Reg_Loss: 13045.16, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:13099.90: 100%| [■] | 149/149 [26:53 < 00:00, 10.83it/s]

997 ***Symmetric Check結束***

998 ***檢測結果: Model含有所後門(Abnormal)

999 檢測結果: Model含有所後門(Abnormal)

1000 整體耗時: 4988.310601949692

1001 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000836-----

1002 ***Pre-Screening開始***

1003 ***Pre-Screening結束***

1004 可能的攻擊方式: Label Specific Backdoor Attack

1005 可能的 target-victim 配對: ['2-3', '2-5']

1006 ***Trigger Reverse Engineering開始***

1007 Target: 2, victim: 5, Loss: 9.9563, Acc: 0.00%, CE_Loss: 9.96, Reg_Loss: 2576.96, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2559.31: 3%| [■] | 31/10000 [00:07 < 04:00, 4.02it/s]

1008 ***Trigger Reverse Engineering結束***

1009 Target Class: 2 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 21

1010 ***檢測結果: Model是安全的(Benign)

1011 檢測結果: Model是安全的(Benign)

1012 整體耗時: 9.753085613250732

1013 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000837-----

1014 ***Pre-Screening開始***

1015 ***Pre-Screening結束***

1016 可能的攻擊方式: Label Specific Backdoor Attack

1017 可能的 target-victim 配對: ['8-2']

1018 ***Trigger Reverse Engineering開始***

1019 Target: 8, victim: 2, Loss: 11.4747, Acc: 0.00%, CE_Loss: 11.47, Reg_Loss: 2502.02, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2495.25: 1%| [■] | 10/1000 [00:24 < 40:55, 2.48it/s]

1020 ***Trigger Reverse Engineering結束***

1021 Target Class: 8 Victim Class: 2 Trigger Size: 1000000000.0 Optimization Steps: 11

1022 ***檢測結果: Model是安全的(Benign)

1023 檢測結果: Model是安全的(Benign)

1024 整體耗時: 33.46728014945984

1025 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000838-----

1026 ***Pre-Screening開始***

1027 ***Pre-Screening結束***

1028 可能的攻擊方式: Label Specific Backdoor Attack

1029 可能的 target-victim 配對: ['2-3']

1030 ***Trigger Reverse Engineering開始***

1031 Target: 2, victim: 3, Loss: 11.3692, Acc: 0.00%, CE_Loss: 11.37, Reg_Loss: 2559.86, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:2547.47: 1%| [■] | 10/1000 [00:45 < 1:15:53, 4.60it/s]

1032 ***Trigger Reverse Engineering結束***

1033 Target Class: 2 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 11

1034 ***檢測結果: Model是安全的(Benign)

1035 檢測結果: Model是安全的(Benign)

1036 整體耗時: 53.547677107963562

1037 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000839-----

1038 ***Pre-Screening開始***

1039 ***Pre-Screening結束***

1040 可能的攻擊方式: Label Specific Backdoor Attack

1041 可能的 target-victim 配對: ['0-18', '2-1', '16-1', '17-1']

1042 ***Trigger Reverse Engineering開始***

1043 Target: 2, victim: 1, Loss: 1.3686, Acc: 100.00%, CE_Loss: 0.14, Reg_Loss: 47.84, Cost:0.01 best_reg:47.88 avg_loss_reg:47.96: 14%| [■] | 145/1000 [00:58 < 05:44, 2.49it/s]

1044 early stop 所有

1045 ***Trigger Reverse Engineering結束***

1046 Target Class: 2 Victim Class: 1 Trigger Size: 47.833894348144531 Optimization Steps: 102

1047 ***Symmetric Check開始***

1048 Target: 1, victim: 2, Loss: 7.4418, Acc: 90.00%, CE_Loss: 0.44, Reg_Loss: 922.16, Cost:0.01 best_reg:939.39 avg_loss_reg:924.98: 100%| [■] | 102/102 [00:41 < 00:00, 2.48it/s]

1049 ***Symmetric Check結束***

1050 ***檢測結果: Model是安全的(Benign)

1051 檢測結果: Model含有所後門(Abnormal)

1052 整體耗時: 105.92292761802673

1053 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000840-----

1054 ***Pre-Screening開始***

1055 ***Pre-Screening結束***

1056 ***檢測結果: Model是安全的(Benign)

1057 檢測結果: Model是安全的(Benign)

1058 整體耗時: 24.6804702819519

1059 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000841-----

1060 ***Pre-Screening開始***

1061 ***Pre-Screening結束***

1062 ***檢測結果: Model是安全的(Benign)

1063 檢測結果: Model是安全的(Benign)

1064 整體耗時: 14.541155815124512

File - main -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000842-----

```

1065 ***Pre-Screening開始
1066 ***Pre-Screening結束
1067 ***Pre-Screening結束
1068 可能的攻擊方式: Label Specific Backdoor Attack
1069 可能的 target-victim 配對: ['6-7', '7-3', '9-2']
1070 ***Trigger Reverse Engineering開始
1071 Target: 9, victim: 2, Loss: 4.8228, Acc: 20.00%, CE_Loss: 4.82, Reg_Loss: 2972.18, Cost: 0.00 best_reg: 1000000000.00 avg_loss_reg: 2853.69; 4% █ | 42/1000 [0:0:10<03:49, 4.17it/s]
1072 ***Trigger Reverse Engineering結束
1073 Target Class: 6 Victim Class: 7 Trigger Size: 1000000000.0 Optimization Steps: 11
1074 *****檢測結果: Model是安全的(Benign)
1075 檢測結果: Model是安全的(Benign)
1076 整體耗時: 15.07412386277771
1077 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000843-----
```

```

1078 ***Pre-Screening開始
1079 ***Pre-Screening結束
1080 ***檢測結果: Model是安全的(Benign)
1081 檢測結果: Model是安全的(Benign)
1082 整體耗時: 5.521037578582764
1083 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000844-----
```

```

1084 ***Pre-Screening開始
1085 ***Pre-Screening結束
1086 可能的攻擊方式: Label Specific Backdoor Attack
1087 可能的 target-victim 配對: ['1-5']
1088 ***Trigger Reverse Engineering開始
1089 Target: 1, victim: 5, Loss: 6.8390, Acc: 0.00%, CE_Loss: 6.84, Reg_Loss: 2612.02, Cost: 0.00 best_reg: 1000000000.00 avg_loss_reg: 2587.21; 1% █ | 10/1000 [0:1:15<2:04:44, 7.56s/it]
1090 ***Trigger Reverse Engineering結束
1091 Target Class: 1 Victim Class: 5 Trigger Size: 1000000000.0 Optimization Steps: 11
1092 *****檢測結果: Model是安全的(Benign)
1093 檢測結果: Model是安全的(Benign)
1094 整體耗時: 96.067770109176636
1095 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000845-----
```

```

1096 ***Pre-Screening開始
1097 ***Pre-Screening結束
1098 可能的攻擊方式: Label Specific Backdoor Attack
1099 可能的 target-victim 配對: ['13-4']
1100 ***Trigger Reverse Engineering開始
1101 Target: 13, victim: 4, Loss: 2.0004, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss: 73.89, Cost: 0.03 best_reg: 73.89 avg_loss_reg: 73.89; 10% █ | 102/1000 [07:48<1:08:47, 4.60s/it]
1102 early stop 所有
1103 ***Trigger Reverse Engineering結束
1104 Target Class: 13 Victim Class: 4 Trigger Size: 73.89019775390625 Optimization Steps: 103
1105 ***Symmetric Check開始
1106 Target: 4, victim: 13, Loss: 9.0002, Acc: 40.00%, CE_Loss: 0.75, Reg_Loss: 12377.69, Cost: 0.00 best_reg: 17592.12 avg_loss_reg: 13215.54; 100% █ | 103/103 [07:49<00:00, 4.55s/it]
1107 ***Symmetric Check結束
1108 *****檢測結果: Model含有後門(Abnormal)
1109 檢測結果: Model是安全的(Benign)
1110 整體耗時: 959.9967269897461
1111 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000846-----
```

1112 ***Pre-Screening開始

1113 ***Pre-Screening結束

1114 可能的攻擊方式: Label Specific Backdoor Attack

1115 可能的 target-victim 配對: ['11-1', '12-9']
1116 ***Trigger Reverse Engineering開始
1117 Target: 12, victim: 9, Loss: 2.3953, Acc: 100.00%, CE_Loss: 0.13, Reg_Loss: 1008.55, Cost: 0.00 best_reg: 1012.11 avg_loss_reg: 1007.04; 18% █ | 177/1000 [19:49<1:32:10, 6.72s/it]
1118 early stop 所有
1119 ***Trigger Reverse Engineering結束
1120 Target Class: 12 Victim Class: 9 Trigger Size: 1008.5536499023438 Optimization Steps: 157
1121 *****檢測結果: Model是安全的(Benign)
1122 檢測結果: Model是安全的(Benign)
1123 整體耗時: 1215.2177982330322
1124 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000847-----

1125 ***Pre-Screening開始

1126 ***Pre-Screening結束
1127 ***檢測結果: Model是安全的(Benign)
1128 檢測結果: Model是安全的(Benign)
1129 整體耗時: 9.37430739402771
1130 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000848-----

1131 ***Pre-Screening開始
1132 ***Pre-Screening結束
1133 ***檢測結果: Model是安全的(Benign)
1134 檢測結果: Model是安全的(Benign)
1135 整體耗時: 8.862825870513916

```

1136     ***Pre-Screening開始
1137     ***Pre-Screening結束
1138     ***Pre-Screening結束
1139 可能的攻擊方式: Universal Backdoor Attack
1140 可能的 target class: 0
1141 可能的 victim classes: ALL
1142 ***Trigger Reverse Engineering開始
1143 Target: 0, victim: 9, Loss: 5.9735, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:3982.34, Cost:0.00 best_reg:3997.50 avg_loss_reg:3997.50: 20% | 199/1000 [1:04:12 <4:18:26, 19.36s/it]
1144 early stop 所有
1145 ***Trigger Reverse Engineering結束
1146 Target Class: 0 Victim Class: all Trigger Size: 3976.3284301757812 Optimization Steps: 200
1147 *****檢測結果: Model是安全的(Benign)
1148 整體耗時: 3864.3802876472473 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000850-----
1149 *****檢測結果: Model是安全的(Benign)
1150 整體耗時: 3864.3802876472473 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000850-----
1151 ***Pre-Screening開始
1152 ***Pre-Screening結束
1153 ***檢測結果: Model是安全的(Benign)
1154 檢測結果: Model是安全的(Benign)
1155 整體耗時: 7.7940763191955664 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000851-----
1156 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000851-----
1157 ***Pre-Screening開始
1158 ***Pre-Screening結束
1159 可能的攻擊方式: Label Specific Backdoor Attack
1160 可能的 target-victim 配對: ['3-4', '3-7', '5-0', '5-6']
1161 ***Trigger Reverse Engineering開始
1162 Target: 3, victim: 7, Loss: 1.3944, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:2737.53, Cost:0.00 best_reg:2747.88 avg_loss_reg:2720.13: 32% | 317/1000 [56.41 <2:02:09, 10.73s/it]
1163 early stop 所有
1164 ***Trigger Reverse Engineering結束
1165 Target Class: 3 Victim Class: 7 Trigger Size: 2737.52734375 Optimization Steps: 274
1166 *****檢測結果: Model是安全的(Benign)
1167 檢測結果: Model是安全的(Benign)
1168 整體耗時: 3435.0818412303925 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000852-----
1169 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000852-----
1170 ***Pre-Screening開始
1171 ***Pre-Screening結束
1172 ***檢測結果: Model是安全的(Benign)
1173 檢測結果: Model是安全的(Benign)
1174 整體耗時: 11:43:7893390655518 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000853-----
1175 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000853-----
1176 ***Pre-Screening開始
1177 ***Pre-Screening結束
1178 ***檢測結果: Model是安全的(Benign)
1179 檢測結果: Model是安全的(Benign)
1180 整體耗時: 9:21:45:26176452637 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000854-----
1181 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000854-----
1182 ***Pre-Screening開始
1183 ***Pre-Screening結束
1184 可能的攻擊方式: Label Specific Backdoor Attack
1185 可能的 target-victim 配對: ['9-3']
1186 ***Trigger Reverse Engineering開始
1187 Target: 9, victim: 3, Loss: 8.6953, Acc: 0.00%, CE_Loss: 8.70, Reg_Loss:2502.26, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:2501.90: 1% | 10/1000 [00:24 <40:37, 2.46s/it]
1188 ***Trigger Reverse Engineering結束
1189 Target Class: 9 Victim Class: 3 Trigger Size: 10000000000.0 Optimization Steps: 11
1190 *****檢測結果: Model是安全的(Benign)
1191 檢測結果: Model是安全的(Benign)
1192 整體耗時: 33:60:719013214111 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000855-----
1193 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000855-----
1194 ***Pre-Screening開始
1195 ***Pre-Screening結束
1196 可能的攻擊方式: Universal Backdoor Attack
1197 可能的 target class: 4
1198 可能的 victim classes: ALL
1199 ***Trigger Reverse Engineering開始
1200

```