

```
File - main
1 C:\Users\slab\anaconda3\envs\pytorch1\python.exe D:\UULi\test_code\k_arm_test\main.py
2 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-0000000000
3 ***Pre-Screening開始***
4 ***Pre-Screening結束***
5 可能的攻擊方式: Label Specific Backdoor Attack
6 可能的 target-victim 配對: ['0-4', '0-7']
7 ***Trigger Reverse Engineering開始***
8 Target: 0, victim: 7, Loss: 1.2152, Acc: 100.00%, CE_Loss: 0.25, Reg_Loss:126.82, Cost:0.01 best_reg:128.16 avg_loss_reg:128.16: 20% | 199/1000 [01:35<06:23, 2.09it/s]
9 early stop 所有
10 ***Trigger Reverse Engineering結束***
11 Target Class: 0 Victim Class: 7 Trigger Size: 126.82<107543945312 Optimization Steps: 175
12 ***Symmetric Check開始***
13 Target: 7, victim: 0, Loss: 1.3250, Acc: 100.00%, CE_Loss: 0.29, Reg_Loss:1037.77, Cost:0.00 best_reg:1023.94 avg_loss_reg:1037.90: 100% | 175/175 [00:41<00:00, 4.19it/s]
14 ***Symmetric Check結束***
15 *****檢測結束*****
16 檢測結果: Model含有後門(Abnormal)
17 整體耗時: 143.3811902999878
18 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-0000000001
19 ***Pre-Screening開始
20 ***Pre-Screening結束***
21 可能的攻擊方式: Universal Backdoor Attack
22 可能的 target class: 0
23 可能的 victim classes: ALL
24 ***Trigger Reverse Engineering開始***
25 Target: 0, victim: 4, Loss: 2.8775, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:2877.28, Cost:0.00 best_reg:2917.16 avg_loss_reg:2906.83: 16% | 160/1000 [53:03<4:38:35, 19.90s/it]
26 early stop 所有
27 ***Trigger Reverse Engineering結束***
28 Target Class: 0 Victim Class: all Trigger Size: 2885.2230224609375 Optimization Steps: 161
29 *****檢測結束*****
30 檢測結果: Model是安全的(Benign)
31 整體耗時: 3192.053612947464
32 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-0000000002
33 ***Pre-Screening開始
34 ***Pre-Screening結束***
35 檢測結果: Model是安全的(Benign)
36 整體耗時: 17.16268491744995
37 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-0000000003
38 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-0000000004
39 ***Pre-Screening開始
40 ***Pre-Screening結束***
41 可能的攻擊方式: Label Specific Backdoor Attack
42 可能的 target-victim 配對: ['0-5', '0-8', '1-6']
43 ***Trigger Reverse Engineering開始***
44 Target: 1, victim: 6, Loss: 7.0571, Acc: 100.00%, CE_Loss: 0.37, Reg_Loss:586.96, Cost:0.01 best_reg:587.16 avg_loss_reg:587.16: 19% | 143/143 [00:17<00:00, 8.13it/s]
45 early stop 所有
46 ***Trigger Reverse Engineering結束***
47 Target Class: 1 Victim Class: 6 Trigger Size: 586.9552001953125 Optimization Steps: 143
48 ***Symmetric Check開始***
49 Target: 6, victim: 1, Loss: 2.3611, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:4602.23, Cost:0.00 best_reg:4594.92 avg_loss_reg:4610.98: 100% | 186/1000 [00:22<01:40, 8.11it/s]
50 ***Symmetric Check結束***
51 -----檢測結束*****
52 檢測結果: Model是安全的(Benign)
53 整體耗時: 47.97521257400513
54 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-0000000005
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: ['12-14']
59 ***Trigger Reverse Engineering開始***
60 Target: 12, victim: 14, Loss: 2.0957, Acc: 15.00%, CE_Loss: 2.10, Reg_Loss:10596.28, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:10290.79: 2% | 20/1000 [00:01<01:36, 10.14it/s]
61 ***Trigger Reverse Engineering結束***
62 Target Class: 12 Victim Class: 14 Trigger Size: 1000000000.00 Optimization Steps: 21
63 *****檢測結束*****
64 檢測結果: Model是安全的(Benign)
65 整體耗時: 9.749948740005493
66 -----掃描檔案: D:\UULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-0000000006
67 ***Pre-Screening開始
68 ***Pre-Screening結束***
69 可能的攻擊方式: Universal Backdoor Attack
70 可能的 target class: 0
71 可能的 victim classes: ALL
```

File - main

```
72 ***Trigger Reverse Engineering開始***  
73 Target: 0, victim: 12, Loss: 1.7018, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:3809.92, Cost:0.00 best_reg:3799.33 avg_loss_reg:3818.20: 12%■ | 115/1000 [32:50<4:12:42, 17.13s/it]  
74 early stop 所有  
75 ***Trigger Reverse Engineering結束***  
76 Target Class: 0 Victim Class: all Trigger Size: 3799.326904296875 Optimization Steps: 116  
77 *****檢測結束*****  
78 檢測結果: Model是安全的(Benign)  
79 整體耗時: 1981.7125210762024  
80 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000006-----  
81 ***Pre-Screening開始***  
82 ***Pre-Screening結束***  
83 可能的攻擊方式: Universal Backdoor Attack  
84 可能的 target class: 10  
85 可能的 victim classes: ALL  
86 ***Trigger Reverse Engineering開始***  
87 Target: 10, victim: 12, Loss: 0.3737, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:830.03, Cost:0.00 best_reg:824.60 avg_loss_reg:830.00: 6%■ | 65/1000 [13:09<3:09:13, 12.14s/it]  
88 early stop 所有  
89 ***Trigger Reverse Engineering結束***  
90 Target Class: 10 Victim Class: all Trigger Size: 824.5954318576389 Optimization Steps: 66  
91 *****檢測結束*****  
92 檢測結果: Model含有後門(Abnormal)  
93 整體耗時: 796.86796691452  
94 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000007-----  
95 ***Pre-Screening開始***  
96 ***Pre-Screening結束***  
97 可能的攻擊方式: Label Specific Backdoor Attack  
98 可能的 target-victim 配對: ['1-20', '9-20']  
99 ***Trigger Reverse Engineering開始***  
100 Target: 9, victim: 20, Loss: 12.8278, Acc: 0.00%, CE_Loss: 12.83, Reg_Loss:4661.28, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:4187.59: 3%■ | 31/1000 [00:04<02:18, 6.99it/s]  
101 ***Trigger Reverse Engineering結束***  
102 Target Class: 1 Victim Class: 20 Trigger Size: 1000000000.00 Optimization Steps: 21  
103 *****檢測結束*****  
104 檢測結果: Model是安全的(Benign)  
105 整體耗時: 13.618326187133789  
106 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000008-----  
107 ***Pre-Screening開始***  
108 ***Pre-Screening結束***  
109 ***檢測結束***  
110 檢測結果: Model是安全的(Benign)  
111 整體耗時: 20.378050804138184  
112 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000009-----  
113 ***Pre-Screening開始***  
114 ***Pre-Screening結束***  
115 可能的攻擊方式: Universal Backdoor Attack  
116 可能的 target class: 4  
117 可能的 victim classes: ALL  
118 ***Trigger Reverse Engineering開始***  
119 Target: 4, victim: 19, Loss: 0.7130, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:93.90, Cost:0.01 best_reg:93.60 avg_loss_reg:93.72: 13%■ | 126/1000 [1:13:08<8:27:22, 34.83s/it]  
120 early stop 所有  
121 ***Trigger Reverse Engineering結束***  
122 Target Class: 4 Victim Class: all Trigger Size: 93.59891401018415 Optimization Steps: 127  
123 *****檢測結束*****  
124 檢測結果: Model含有後門(Abnormal)  
125 整體耗時: 4404.524069309235  
126 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000010-----  
127 ***Pre-Screening開始***  
128 ***Pre-Screening結束***  
129 ***檢測結束***  
130 檢測結果: Model是安全的(Benign)  
131 整體耗時: 7.02983458895874  
132 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000011-----  
133 ***Pre-Screening開始***  
134 ***Pre-Screening結束***  
135 ***檢測結束***  
136 檢測結果: Model是安全的(Benign)  
137 整體耗時: 11.033855676651001  
138 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000012-----  
139 ***Pre-Screening開始***  
140 ***Pre-Screening結束***  
141 ***檢測結束***  
142 檢測結果: Model是安全的(Benign)
```

```
143 整體耗時: 19.06214928627014 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000013-----
144 ***Pre-Screening開始***  
145 可能的攻擊方式: Label Specific Backdoor Attack  
146 可能的 target-victim 配對: [0-15, '2-1', '2-10', '3-4', '4-14', '5-10', '7-1', '7-9', '11-1', '11-10', '11-15', '12-4', '12-14', '15-14', '16-4]  
147 ***Trigger Reverse Engineering開始***  
148 Target: 11, victim: 10, Loss: 2.2766, Acc: 80.00%, CE_Loss: 0.52, Reg_Loss:347.43, Cost:0.01 best_Reg:369.78 avg_Loss_Reg:347.94: 100%|██████████| 1000/1000 [05:50<00:00, 2.85it/s]  
149 ***Trigger Reverse Engineering結束***  
150 Target Class: 11 Victim Class: 10 Trigger Size: 369.7843322753906 Optimization Steps: 737  
151 ***Symmetric Check開始***  
152 Target: 10, victim: 11, Loss: 1.9861, Acc: 100.00%, CE_Loss: 0.47, Reg_Loss:3406.63, Cost:0.00 best_Reg:3517.16 avg_Loss_Reg:3389.91: 37%|████| 270/737 [01:36<02:46, 2.80it/s]  
153 early stop 所有  
154 ***Symmetric Check結束***  
155 *****檢測結束*****  
156 *****Symmetric Check結束*****  
157 *****檢測結束*****  
158 檢測結果: Model含有後門(Abnormal)  
159 整體耗時: 455.95215368270874-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000014-----
160 ***Pre-Screening開始***  
161 ***Pre-Screening結束***  
162 ***Pre-Screening結果***  
163 ***檢測結束***  
164 檢測結果: Model是安全的(Benign)  
165 整體耗時: 11.162314891815186-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000015-----
166 ***Pre-Screening開始***  
167 ***Pre-Screening結束***  
168 ***Pre-Screening結果***  
169 ***檢測結束***  
170 檢測結果: Model是安全的(Benign)  
171 整體耗時: 7.533128499984741-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000016-----
172 ***Pre-Screening開始***  
173 ***Pre-Screening結束***  
174 ***Pre-Screening結果***  
175 ***檢測結束***  
176 檢測結果: Model是安全的(Benign)  
177 整體耗時: 18.214077949523926-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000017-----
178 ***Pre-Screening開始***  
179 ***Pre-Screening結束***  
180 ***檢測結束***  
181 ***檢測結果***  
182 檢測結果: Model是安全的(Benign)  
183 整體耗時: 7.3451619148254395-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000018-----
184 ***Pre-Screening開始***  
185 ***Pre-Screening結束***  
186 ***Pre-Screening結果***  
187 ***檢測結束***  
188 檢測結果: Model是安全的(Benign)  
189 整體耗時: 17.032463312149048-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000019-----
190 ***Pre-Screening開始***  
191 ***Pre-Screening結束***  
192 ***Pre-Screening結果***  
193 ***檢測結束***  
194 檢測結果: Model是安全的(Benign)  
195 整體耗時: 15.84819483757019-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000020-----
196 ***Pre-Screening開始***  
197 ***Pre-Screening結束***  
198 ***Pre-Screening結果***  
199 ***檢測結束***  
200 檢測結果: Model是安全的(Benign)  
201 整體耗時: 3.020597457885742-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000021-----
202 ***Pre-Screening開始***  
203 ***Pre-Screening結束***  
204 ***Pre-Screening結果***  
205 ***檢測結束***  
206 檢測結果: Model是安全的(Benign)  
207 整體耗時: 11.349288940429688-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000022-----
208 ***Pre-Screening開始***  
209 ***Pre-Screening結束***  
210 可能的攻擊方式: Label Specific Backdoor Attack  
211 可能的 target-victim 配對: [0-11, '1-6', '1-7', '1-9, '2-0', '2-10', '3-11', '5-6', '5-8', '6-5', '7-1', '7-8', '9-3', '10-2]  
212 可能的 target-victim 配對: [0-11, '1-6', '1-7', '1-9, '2-0', '2-10', '3-11', '5-6', '5-8', '6-5', '7-1', '7-8', '9-3', '10-2]  
213 ***Trigger Reverse Engineering開始***
```

```
File - main
214 Target: 5, victim: 6, Loss: 2.1971, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:52.26 avg_loss_reg:49.73: 92% | 921/1000 [01:09<00:05, 13.30it/s]
215 early stop 所有
216 ***Trigger Reverse Engineering 結束***+
217 Target Class: 5 Victim Class: 6 Trigger Size: 52.01518249511719 Optimization Steps: 99
218 ***Symmetric Check開始***
219 Target: 6, victim: 5, Loss: 3.0382, Acc: 90.00%, CE_Loss: 0.36, Reg_Loss:2680.72, Cost:0.00 best_reg:2704.34 avg_loss_reg:2704.34: 100% | 99/99 [00:07<00:00, 13.36it/s]
220 ***Symmetric Check結束***+
221 *****檢測結果: Model含有後門(Abnormal)
222 整體耗時: 82.72049069404602
223 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000023-----
224 ***Pre-Screening 開始 ***
225 ***Pre-Screening 結束 ***
226 可能的攻擊方式: Label Specific Backdoor Attack
227 可能的 target-victim 配對: ['3-8', '9-6', '12-1', '12-8', '13-0']
228 可能的 target-victim 配對: ['8-5', '8-9']
229 ***Trigger Reverse Engineering 開始 ***
230 Target: 9, victim: 6, Loss: 1.9746, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:2619.71, Cost:0.00 best_reg:2606.74 avg_loss_reg:2623.04: 100% | 1000/1000 [03:55<00:00, 4.24it/s]
231 ***Trigger Reverse Engineering 結束 ***
232 Target Class: 9 Victim Class: 6 Trigger Size: 2606.74072265625 Optimization Steps: 84
233 -----檢測結果: Model是安全的(Benign)
234 檢測結果: Model是安全的(Benign)
235 整體耗時: 243.1950716972351
236 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000024-----
237 ***Pre-Screening 開始 ***
238 ***Pre-Screening 結束 ***
239 可能的攻擊方式: Label Specific Backdoor Attack
240 可能的 target-victim 配對: ['8-5', '8-9']
241 ***Trigger Reverse Engineering 開始 ***
242 Target: 8, victim: 9, Loss: 10.0454, Acc: 0.00%, CE_Loss: 10.05, Reg_Loss:9443.11, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:8184.87: 2% | 121/1000 [01:16<59:13, 3.63s/it]
243 ***Trigger Reverse Engineering 結束 ***
244 Target Class: 5 Victim Class: 5 Trigger Size: 1000000000.0 Optimization Steps: 11
245 -----檢測結果: Model是安全的(Benign)
246 檢測結果: Model是安全的(Benign)
247 整體耗時: 91.67607402801514
248 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000025-----
249 ***Pre-Screening 開始 ***
250 ***Pre-Screening 結束 ***
251 ***檢測結果: Model是安全的(Benign)
252 整體耗時: 6.06888422827026
253 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000026-----
254 -----檢測結果: Model是安全的(Benign)
255 -----檢測結果: Model是安全的(Benign)
256 可能的攻擊方式: Label Specific Backdoor Attack
257 可能的 target-victim 配對: ['9-10', '9-16', '11-16']
258 可能的 target-victim 配對: ['9-10', '9-16', '11-16']
259 ***Trigger Reverse Engineering 開始 ***
260 Target: 11, victim: 16, Loss: 9.1888, Acc: 0.00%, CE_Loss: 9.19, Reg_Loss:5686.14, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:5189.52: 3% | 132/1000 [00:04<02:29, 6.46it/s]
261 ***Trigger Reverse Engineering 結束 ***
262 Target Class: 9 Victim Class: 10 Trigger Size: 1000000000.0 Optimization Steps: 11
263 -----檢測結果: Model是安全的(Benign)
264 檢測結果: Model是安全的(Benign)
265 整體耗時: 11.62276577949524
266 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000027-----
267 ***Pre-Screening 開始 ***
268 ***Pre-Screening 結束 ***
269 可能的攻擊方式: Universal Backdoor Attack
270 可能的 target class: ALL
271 可能的 victim classes: ALL
272 ***Trigger Reverse Engineering 開始 ***
273 Target: 6, victim: 19, Loss: 0.7005, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:1043.19, Cost:0.00 best_reg:1035.95 avg_loss_reg:1048.86: 6% | 161/1000 [42:35<10:55:42, 41.90s/it]
274 early stop 所有
275 ***Trigger Reverse Engineering 結束 ***
276 Target Class: all Trigger Size: 1035.9530290876116 Optimization Steps: 62
277 *****檢測結果: Model含有後門(Abnormal)
278 檢測結果: Model是安全的(Benign)
279 整體耗時: 2576.4609031677246
280 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000028-----
281 ***Pre-Screening 開始 ***
282 ***Pre-Screening 結束 ***
283 可能的攻擊方式: Label Specific Backdoor Attack
284 可能的 target-victim 配對: ['2-8']
```

```
285 ***Trigger Reverse Engineering 開始***  
286 Target: 2, victim: 8, Loss: 1.1946, Acc: 100.00%, CE_Loss: 0.34, Reg_Loss: 856.11, Cost: 0.00 best_reg: 825.53 avg_loss_reg: 849.33: 100% | [1000/1000 [47:38<00:00, 2.86s/it]  
287 0% | 0/1000 [00:00:<?, ?it/s] ***Trigger Reverse Engineering 結束***  
288 Target Class: 2 Victim Class: 8 Trigger Size: 825.5343017578125 Optimization Steps: 1000  
289 ***Symmetric Check開始***  
290 Target: 8, victim: 2, Loss: 0.4777, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss: 4076.33, Cost: 0.00 best_reg: 4082.44 avg_loss_reg: 4068.14: 60% | [598/1000 [28:32<19:11, 2.86s/it]  
291 early stop 所有  
292 ***Symmetric Check 結束***  
293 *****檢測結束*****  
294 檢測結果: Model是安全的(Benign)  
295 整體耗時: 4586.448591709137  
296 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000029-----  
297 ***Pre-Screening 開始***  
298 ***Pre-Screening 結束***  
299 可能的攻擊方式: Label Specific Backdoor Attack  
300 可能的 target-victim 配對: ['8-2', '8-6']  
301 ***Trigger Reverse Engineering 開始***  
302 Target: 8, victim: 6, Loss: 9.3851, Acc: 0.00%, CE_Loss: 9.39, Reg_Loss: 8232.51, Cost: 0.00 best_reg: 10000000000.00 avg_loss_reg: 7180.10: 2% | [21/1000 [00:03<02:32, 6.43it/s]  
303 ***Trigger Reverse Engineering 結束***  
304 Target Class: 8 Victim Class: 2 Trigger Size: 10000000000.0 Optimization Steps: 11  
305 *****檢測結束*****  
306 檢測結果: Model是安全的(Benign)  
307 整體耗時: 9.702200174331665-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000030-----  
308 ***Pre-Screening 開始***  
309 ***Pre-Screening 結束***  
310 ***Pre-Screening 開始***  
311 可能的攻擊方式: Label Specific Backdoor Attack  
312 可能的 target-victim 配對: ['1-3', '1-5', '4-1']  
313 ***Trigger Reverse Engineering 開始***  
314 Target: 4, victim: 1, Loss: 3.1035, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss: 6496.22, Cost: 0.00 best_reg: 6508.56 avg_loss_reg: 6591.90: 39% | [386/1000 [01:45<02:48, 3.65it/s]  
315 early stop 所有  
316 ***Trigger Reverse Engineering 結束***  
317 Target Class: 4 Victim Class: 1 Trigger Size: 6496.22265625 Optimization Steps: 355  
318 *****檢測結束*****  
319 檢測結果: Model是安全的(Benign)  
320 整體耗時: 112.96368670463562-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000031-----  
321 ***Pre-Screening 開始***  
322 ***Pre-Screening 結束***  
323 可能的攻擊方式: Label Specific Backdoor Attack  
324 可能的 target-victim 配對: ['1-0', '3-4', '4-3']  
325 ***Trigger Reverse Engineering 開始***  
326 Target: 4, victim: 3, Loss: 2.8234, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss: 1153.52, Cost: 0.00 best_reg: 1153.74 avg_loss_reg: 1170.53: 52% | [525/1000 [19:16<17:26, 2.20s/it]  
327 Target Class: 4 Victim Class: 3 Trigger Size: 6496.22265625 Optimization Steps: 355  
328 early stop 所有  
329 ***Trigger Reverse Engineering 結束***  
330 Target Class: 4 Victim Class: 3 Trigger Size: 1153.5166015625 Optimization Steps: 494  
331 *****檢測結束*****  
332 檢測結果: Model是安全的(Benign)  
333 整體耗時: 1166.9934563363678-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000032-----  
334 ***Pre-Screening 開始***  
335 ***Pre-Screening 結束***  
336 ***Pre-Screening 結束***  
337 可能的攻擊方式: Label Specific Backdoor Attack  
338 可能的 target-victim 配對: ['2-4', '2-8', '8-4']  
339 ***Trigger Reverse Engineering 開始***  
340 Target: 2, victim: 8, Loss: 4.1474, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss: 102.63, Cost: 0.04 best_reg: 102.68 avg_loss_reg: 102.94: 37% | [367/1000 [08:05<13:56, 1.32s/it]  
341 0% | 0/328 [00:00:<?, ?it/s] early stop 所有  
342 ***Trigger Reverse Engineering 結束***  
343 Target Class: 2 Victim Class: 8 Trigger Size: 102.63076782226562 Optimization Steps: 328  
344 ***Symmetric Check開始***  
345 Target: 8, victim: 2, Loss: 1.3894, Acc: 90.00%, CE_Loss: 0.53, Reg_Loss: 858.46, Cost: 0.00 best_reg: 854.27 avg_loss_reg: 852.34: 100% | [328/328 [07:10<00:00, 1.31s/it]  
346 ***Symmetric Check 結束***  
347 *****檢測結束*****  
348 檢測結果: Model含有後門(Abnormal)  
349 整體耗時: 928.257605526733-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000033-----  
350 ***Pre-Screening 開始***  
351 ***Pre-Screening 結束***  
352 ***檢測結束***  
353 檢測結果: Model是安全的(Benign)  
354 整體耗時: 11.457124948501587  
355
```

```

356   ***Pre-Screening開始***           -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000034-----
357   ***Pre-Screening結束***           358   ***Pre-Screening結束***           359   ***檢測結果: Model是安全的(Benign)
360   檢測結果: Model是安全的(Benign)   361   整體耗時: 7.0207507610321045      -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000035-----
362   ***Pre-Screening結束***           363   ***Pre-Screening開始***           364   ***Pre-Screening結束***           365   ***檢測結果: Model是安全的(Benign)
366   檢測結果: Model是安全的(Benign)  367   整體耗時: 6.862086057662964      -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000036-----
368   ***Pre-Screening結束***           369   ***Pre-Screening開始***           370   ***Pre-Screening結束***           371   可能的攻擊方式: Label Specific Backdoor Attack
372   可能的 target-victim 配對: ['1-8', '2-9', '3-4', '3-6', '4-7', '5-7', '6-7', '8-1', '8-10', '8-11', '9-2', '9-6', '10-1', '10-8', '10-14', '13-11', '14-0', '14-13', '15-14']
373   ***Trigger Reverse Engineering 開始***           374   Target: 8, victim: 1, Loss: 0.7839, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss: 3420.82, Cost:0.00 best_reg:3425.66 avg_loss_reg:3417.02: 82%|██████████| |816/1000 [1:01:43 < 13:55, 4.54s/it]
375   early-stop 所有
376   ***Trigger Reverse Engineering 結束***           377   Target Class: 8 Victim Class: 1 Trigger Size: 3420.816162109375 Optimization Steps: 360
378   *****檢測結束*****               379   檢測結果: Model是安全的(Benign)
380   整體耗時: 3728.9489817619324      -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000037-----
381   ***Pre-Screening開始***           382   ***Pre-Screening結束***           383   ***Pre-Screening開始***           384   可能的攻擊方式: Label Specific Backdoor Attack
385   可能的 target-victim 配對: ['10-13', '14-4']
386   ***Trigger Reverse Engineering 開始***           387   Target: 14, victim: 4, Loss: 3.2437, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss: 122.09, Cost:0.03 best_reg:123.58 avg_loss_reg:123.58: 13%|████| |129/1000 [0:04:5 < 05:07, 2.83it/s]
388   0%| |0/119 [00:00:< ?] it/s early stop 所有
389   ***Trigger Reverse Engineering 結束***           390   Target Class: 14 Victim Class: 4 Trigger Size: 122.093017578125 Optimization Steps: 119
391   ***Symmetric Check開始***           392   Target: 4, victim: 14, Loss: 2.0966, Acc: 95.00%, CE_Loss: 0.49, Reg_Loss: 5436.89, Cost:0.00 best_reg:6240.88 avg_loss_reg:5482.51: 100%|████| |119/1119 [00:41 < 00:00, 2.84it/s]
393   ***Symmetric Check結束***           394   *****檢測結束*****               395   檢測結果: Model含有後門(Abnormal)
396   整體耗時: 95.08255219459534      -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000038-----
397   ***Pre-Screening開始***           398   ***Pre-Screening結束***           399   ***Pre-Screening開始***           400   ***Pre-Screening結束***           401   檢測結果: Model是安全的(Benign)
402   整體耗時: 17.49670171737671      -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000039-----
403   ***Pre-Screening開始***           404   ***Pre-Screening結束***           405   ***Pre-Screening開始***           406   可能的攻擊方式: Label Specific Backdoor Attack
407   可能的 target-victim 配對: ['1-2', '1-5', '8-5', '12-5']
408   ***Trigger Reverse Engineering 開始***           409   Target: 1, victim: 5, Loss: 11.0995, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss: 187.10, Cost:0.06 best_reg:187.90 avg_loss_reg:187.90: 13%|████| |132/1000 [0:01:12 < 01:12, 11.89it/s]
410   early stop 所有
411   ***Trigger Reverse Engineering 結束***           412   Target Class: 1 Victim Class: 5 Trigger Size: 187.09918212890625 Optimization Steps: 88
413   ***Symmetric Check開始***           414   Target: 5, victim: 1, Loss: 2.9641, Acc: 100.00%, CE_Loss: 0.49, Reg_Loss: 1100.89, Cost:0.00 best_reg:1134.87 avg_loss_reg:1111.82: 100%|████| |88/88 [00:06 < 00:00, 12.86it/s]
415   ***Symmetric Check結束***           416   *****檢測結束*****               417   檢測結果: Model是安全的(Benign)
418   整體耗時: 24.501861095428467      -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000040-----
419   ***Pre-Screening開始***           420   ***Pre-Screening結束***           421   ***Pre-Screening開始***           422   可能的攻擊方式: Universal Backdoor Attack
423   可能的 target class: 2
424   可能的 victim classes: ALL
425   ***Trigger Reverse Engineering 開始***           426   Target: 2, victim: 9, Loss: 0.2163, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss: 96.13, Cost:0.00 best_reg:116.95 avg_loss_reg:96.81: 10%|████| |104/1000 [27:53 < 4:00:15, 16.09s/it]

```

```
427 early stop 所有
428 ***Trigger Reverse Engineering結束***
429 Target Class: 2 Victim Class: all Trigger Size: 116.95089530944824 Optimization Steps: 105
430 *****檢測結束*****
431 檢測結果: Model含有後門(Abnormal)
432 整體耗時: 1683.2260296344757
433 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000041-----
434 ***Pre-Screening開始***
435 ***Pre-Screening結束***
436 可能的攻擊方式: Label Specific Backdoor Attack
437 可能的 target-victim 配對: [0-20, '7-11', '8-1', '8-7', '8-11', '10-0', '10-9', '12-9', '13-1', '13-3', '13-19', '14-5', '14-9', '15-7', '17-19', '20-0]
438 ***Trigger Reverse Engineering開始***
439 Target: 0, victim: 20 Loss: 0.8362, Acc: 95.00%, CE_Loss: 0.15, Reg_Loss:1024.87, Cost:0.00 best_reg:1035.90 avg_loss_reg:1019.59: 100% █ 1000/1000 [04:18<00:00, 3.87it/s]
440 ***Trigger Reverse Engineering結束***
441 Target Class: 0 Victim Class: 20 Trigger Size: 1035.896728515625 Optimization Steps: 253
442 *****檢測結束*****
443 檢測結果: Model是安全的(Benign)
444 整體耗時: 267.22953629493713
445 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000042-----
446 ***Pre-Screening開始***
447 ***Pre-Screening結束***
448 可能的攻擊方式: Label Specific Backdoor Attack
449 可能的 target-victim 配對: ['4-9', '4-10', '11-10']
450 ***Trigger Reverse Engineering開始***
451 Target: 4, victim: 10, Loss: 1.2234, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:28.89, Cost:0.04 best_reg:29.29 avg_loss_reg:29.29: 13% █ | 133/1000 [07:51<51:12, 3.54s/it]
452 early stop 所有
453 ***Trigger Reverse Engineering結束***
454 Target Class: 4 Victim Class: 10 Trigger Size: 28.88616943359375 Optimization Steps: 101
455 ***Symmetric Check開始***
456 Target: 10, victim: 4, Loss: 1.3092, Acc: 90.00%, CE_Loss: 0.50, Reg_Loss:6149.09, Cost:0.00 best_reg:13050.65 avg_loss_reg:6123.76: 100% █ | 101/101 [05:52<00:00, 3.49s/it]
457 ***Trigger Reverse Engineering結束***
458 *****檢測結束*****
459 檢測結果: Model含有後門(Abnormal)
460 整體耗時: 840.2945759296417
461 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000043-----
462 ***Pre-Screening開始***
463 ***Pre-Screening結束***
464 ***檢測結束***
465 檢測結果: Model是安全的(Benign)
466 整體耗時: 12.33970832824707
467 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000044-----
468 ***Pre-Screening開始***
469 ***Pre-Screening結束***
470 可能的攻擊方式: Label Specific Backdoor Attack
471 可能的 target-victim 配對: ['0-6']
472 ***Trigger Reverse Engineering開始***
473 Target: 0, victim: 6, Loss: 9.3379, Acc: 0.00%, CE_Loss: 9.34, Reg_Loss:7412.15, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:6636.06: 1% | | 10/1000 [00:04<06:39, 2.48it/s]
474 ***Trigger Reverse Engineering結束***
475 Target Class: 0 Victim Class: 6 Trigger Size: 10000000000.0 Optimization Steps: 11
476 *****檢測結束*****
477 檢測結果: Model是安全的(Benign)
478 整體耗時: 10.74479614511108
479 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000045-----
480 ***Pre-Screening開始***
481 ***Pre-Screening結束***
482 ***檢測結束***
483 檢測結果: Model是安全的(Benign)
484 整體耗時: 17.440627574920654
485 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000046-----
486 ***Pre-Screening開始***
487 ***Pre-Screening結束***
488 ***檢測結束***
489 檢測結果: Model是安全的(Benign)
490 整體耗時: 6.48016095161438
491 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000047-----
492 ***Pre-Screening開始***
493 ***Pre-Screening結束***
494 ***檢測結束***
495 檢測結果: Model是安全的(Benign)
496 整體耗時: 6.2277478456497192
497 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000048-----
```

```

498 ***Pre-Screening開始***  

499 ***Pre-Screening結束***  

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

501 可能的 target-victim 配對: ['5-7']  

502 ***Trigger Reverse Engineering 開始***  

503 Target: 5, victim: 7, Loss: 2.6458, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:93.91, Cost:0.03 best_reg:94.40 avg_loss_reg:95.16: 15% █ | 150/1000 [02:26<13:50, 1.02it/s]  

504 early stop 所有  

505 ***Trigger Reverse Engineering 結束***  

506 Target Class: 5 Victim Class: 7 Trigger Size: 93.91307067871094 Optimization Steps: 151  

507 ***Symmetric Check開始***  

508 Target: 7, victim: 5, Loss: 2.7724, Acc: 90.00%, CE_Loss: 0.50, Reg_Loss:2272.82, Cost:0.00 best_reg:2371.15 avg_loss_reg:2278.85: 100% █ | 151/151 [02:19<00:00, 1.08it/s]  

509 ***Symmetric Check結束***  

510 *****檢測結果: Model含有後門(Abnormal)  

511 整體耗時: 298.35584568977356  

512 檢測結果: Model含有後門(Abnormal)  

513 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000049-----  

514 ***Pre-Screening 開始***  

515 ***Pre-Screening 結束***  

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

517 可能的 target-victim 配對: ['3-2', '6-1']  

518 ***Trigger Reverse Engineering 開始***  

519 Target: 3, victim: 2, Loss: 1.3675, Acc: 100.00%, CE_Loss: 0.17, Reg_Loss:355.85, Cost:0.00 best_reg:358.17 avg_loss_reg:358.17: 19% █ | 187/1000 [00:20<01:27, 9.29it/s]  

520 0% | 0/177 [00:00:<?, ?it/s]early stop 所有  

521 ***Trigger Reverse Engineering 結束***  

522 Target Class: 3 Victim Class: 2 Trigger Size: 355.851806640625 Optimization Steps: 177  

523 ***Symmetric Check開始***  

524 Target: 2, victim: 3, Loss: 3.0817, Acc: 90.00%, CE_Loss: 0.68, Reg_Loss:1068.52, Cost:0.00 best_reg:1072.62 avg_loss_reg:1068.78: 100% █ | 177/177 [00:16<00:00, 10.54it/s]  

525 ***Symmetric Check結束***  

526 *****檢測結果: Model是安全的(Benign)  

527 檢測結果: Model是安全的(Benign)  

528 整體耗時: 43.169769048690796  

529 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000050-----  

530 ***Pre-Screening 開始***  

531 ***Pre-Screening 結束***  

532 *****檢測結果: Model是安全的(Benign)  

533 檢測結果: Model是安全的(Benign)  

534 整體耗時: 6.67685866555896  

535 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000051-----  

536 ***Pre-Screening 開始***  

537 ***Pre-Screening 結束***  

538 *****檢測結果: Model是安全的(Benign)  

539 檢測結果: Model是安全的(Benign)  

540 整體耗時: 9.77845788020142  

541 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000052-----  

542 ***Pre-Screening 開始***  

543 ***Pre-Screening 結束***  

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

545 可能的 target-victim 配對: ['2-4', '2-6']  

546 ***Trigger Reverse Engineering 開始***  

547 Target: 2, victim: 6, Loss: 2.9305, Acc: 100.00%, CE_Loss: 0.05, Reg_Loss:33.25, Cost:0.09 best_reg:33.77 avg_loss_reg:33.77: 18% █ | 182/1000 [00:55<04:08, 3.29it/s]  

548 early stop 所有  

549 ***Trigger Reverse Engineering 結束***  

550 Target Class: 2 Victim Class: 6 Trigger Size: 33.24592208862305 Optimization Steps: 77  

551 ***Symmetric Check開始***  

552 Target: 6, victim: 2, Loss: 1.3824, Acc: 100.00%, CE_Loss: 0.52, Reg_Loss:9792.31, Cost:0.00 best_reg:9257.17 avg_loss_reg:9785.06: 100% █ | 77/77 [00:23<00:00, 3.31it/s]  

553 ***Symmetric Check結束***  

554 *****檢測結果: Model含有後門(Abnormal)  

555 檢測結果: Model含有後門(Abnormal)  

556 整體耗時: 85.99053597450256  

557 *****掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000053-----  

558 ***Pre-Screening 開始***  

559 ***Pre-Screening 結束***  

560 可能的攻擊方式: Universal Backdoor Attack  

561 可能的 target class: 1  

562 可能的 victim classes: ALL  

563 ***Trigger Reverse Engineering 開始***  

564 Target: 1, victim: 22, Loss: 1.4065, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:10502.64, Cost:0.00 best_reg:10413.47 avg_loss_reg:10432.45: 16% █ | 165/1000 [2:11:04<11:03:21, 47.67s/it]  

565 early stop 所有  

566 ***Trigger Reverse Engineering 結束***  

567 Target Class: all Trigger Size: 10413.472778320312 Optimization Steps: 166  

568 *****檢測結果: Model含有後門(Abnormal)

```

569 檢測結果: Model是安全的(Benign)

570 整體耗時: 7882.57908153339 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000054-----

571 \*\*\*Pre-Screening開始\*\*\*

572 \*\*\*Pre-Screening結束\*\*\*

573 \*\*\*Pre-Screening結束\*\*\*

574 \*\*\*檢測結果\*\*\*

575 檢測結果: Model是安全的(Benign)

576 整體耗時: 15.206706047058105 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000055-----

577 \*\*\*Pre-Screening開始\*\*\*

578 \*\*\*Pre-Screening結束\*\*\*

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

580 可能的 target-victim 配對: ['14-12']

581 \*\*\*Trigger Reverse Engineering開始\*\*\*

582 Target: 14, victim: 12, Loss: 2.1084, Acc: 100.00%, CE\_Loss: 0.15, Reg\_Loss:869.05, Cost:0.00 best\_reg:872.22 avg\_loss\_reg:872.22: 20%|████| | 196/1000 [00:34&lt;02:22, 5.63it/s]

583 early stop 所有

584 \*\*\*Trigger Reverse Engineering結束\*\*\*

585 Target Class: 14 Victim Class: 12 Trigger Size: 869.0472412109375 Optimization Steps: 197

586 \*\*\*Symmetric Check開始\*\*\*

587 Target: 12, victim: 14, Loss: 3.9850, Acc: 100.00%, CE\_Loss: 0.24, Reg\_Loss:493.30, Cost:0.01 best\_reg:493.49 avg\_loss\_reg:494.81: 67%|████| | 132/197 [00:23&lt;00:11, 5.66it/s]

588 Target: 12, victim: 14, Loss: 3.9850, Acc: 100.00%, CE\_Loss: 0.24, Reg\_Loss:493.30, Cost:0.01 best\_reg:493.49 avg\_loss\_reg:494.81: 67%|████| | 132/197 [00:23&lt;00:11, 5.66it/s]

589 early stop 所有

590 \*\*\*Symmetric Check結束\*\*\*

591 \*\*\*\*檢測結果\*\*\*\*檢測結束\*\*\*\*\*

592 檢測結果: Model是安全的(Benign)

593 整體耗時: 65.45136713981628 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000056-----

594 \*\*\*Pre-Screening開始\*\*\*

595 \*\*\*Pre-Screening結束\*\*\*

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

597 可能的 target-victim 配對: ['1-7', '1-8', '1-16', '2-11', '6-10', '7-8', '16-7']

598 \*\*\*Trigger Reverse Engineering開始\*\*\*

599 Target: 1, victim: 7, Loss: 3.0634, Acc: 100.00%, CE\_Loss: 0.21, Reg\_Loss:375.17, Cost:0.01 best\_reg:375.33 avg\_loss\_reg:377.98: 44%|████| | 442/1000 [01:00&lt;01:16, 7.28it/s]

600 early stop 所有

601 \*\*\*Trigger Reverse Engineering結束\*\*\*

602 Target Class: 1 Victim Class: 7 Trigger Size: 375.1672668457031 Optimization Steps: 198

603 \*\*\*Symmetric Check開始\*\*\*

604 Target: 7, victim: 1, Loss: 0.3828, Acc: 90.00%, CE\_Loss: 0.38, Reg\_Loss:1683.765, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:16780.40: 100%|████| | 198/198 [00:29&lt;00:00, 6.63it/s]

605 Target: 7, victim: 1, Loss: 0.3828, Acc: 90.00%, CE\_Loss: 0.38, Reg\_Loss:1683.765, Cost:0.00 best\_reg:1000000000.00 avg\_loss\_reg:16780.40: 100%|████| | 198/198 [00:29&lt;00:00, 6.63it/s]

606 \*\*\*Symmetric Check結束\*\*\*

607 \*\*\*\*檢測結果\*\*\*\*檢測結束\*\*\*\*\*

608 檢測結果: Model含有後門(Abnormal)

609 整體耗時: 97.91662311553955 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000057-----

610 \*\*\*Pre-Screening開始\*\*\*

611 \*\*\*Pre-Screening結束\*\*\*

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

613 可能的 target-victim 配對: ['10-1-1']

614 \*\*\*Trigger Reverse Engineering開始\*\*\*

615 Target: 10, victim: 1, Loss: 1.7425, Acc: 100.00%, CE\_Loss: 0.14, Reg\_Loss:1598.79, Cost:0.00 best\_reg:1599.59 avg\_loss\_reg:1601.99: 33%|████| | 327/1000 [01:11&lt;02:26, 4.58it/s]

616 early stop 所有

617 \*\*\*Trigger Reverse Engineering結束\*\*\*

618 Target Class: 10 Victim Class: 1 Trigger Size: 1598.789306640625 Optimization Steps: 328

619 Target Class: 10 Victim Class: 1 Trigger Size: 1598.789306640625 Optimization Steps: 328

620 \*\*\*檢測結果\*\*\*\*檢測結束\*\*\*\*\*

621 檢測結果: Model是安全的(Benign)

622 整體耗時: 79.20686292648315 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000058-----

623 \*\*\*Pre-Screening開始\*\*\*

624 \*\*\*Pre-Screening結束\*\*\*

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

626 可能的 target-victim 配對: ['8-1', '11-15', '17-4', '18-1']

627 \*\*\*Trigger Reverse Engineering開始\*\*\*

628 Target: 8, victim: 1, Loss: 1.1323, Acc: 100.00%, CE\_Loss: 0.20, Reg\_Loss:2106.23, Cost:0.00 best\_reg:2106.46 avg\_loss\_reg:2116.32: 45%|████| | 450/1000 [02:13&lt;02:42, 3.38it/s]

629 early stop 所有

630 \*\*\*Trigger Reverse Engineering結束\*\*\*

631 Target Class: 8 Victim Class: 1 Trigger Size: 2106.2275390625 Optimization Steps: 341

632 \*\*\*檢測結果\*\*\*\*檢測結束\*\*\*\*\*

633 檢測結果: Model是安全的(Benign)

634 整體耗時: 141.9574490623474 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000059-----

635 \*\*\*Pre-Screening開始\*\*\*

636 \*\*\*Pre-Screening結束\*\*\*

637 \*\*\*檢測結果\*\*\*

```

File - main
640 檢測結果: Model是安全的(Benign)
641 整體耗時: 15.082679986953735 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000060-----
642 ***Pre-Screening開始*** 
643 ***Pre-Screening結束*** 
644 可能的攻擊方式: Label Specific Backdoor Attack
645 可能的 target-victim 配對: ['2-9', '6-1', '6-2', '6-9', '9-2']
646 ***Trigger Reverse Engineering開始*** 
647 Target: 9, victim: 2, Loss: 9.7215, Acc: 20.00%, CE_Loss: 9.72, Reg_Loss:811138, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:7699.41: 10%|■ | 104/1000 [06:08<52:58, 3.55s/t]
648 Target Class: 2 Victim Class: 9 Trigger Size: 1000000000 Optimization Steps: 21
649 ***Trigger Reverse Engineering結束*** 
650 Target Class: 2 Victim Class: 9 Trigger Size: 1000000000 Optimization Steps: 21
651 *****檢測結束***** 
652 檢測結果: Model是安全的(Benign)
653 整體耗時: 387.7729549407959 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000061-----
654 *****檢測結束***** 
655 ***Pre-Screening開始*** 
656 ***Pre-Screening結束*** 
657 可能的攻擊方式: Label Specific Backdoor Attack
658 可能的 target-victim 配對: ['0-12', '2-6', '3-12', '12-0', '12-3']
659 ***Trigger Reverse Engineering開始*** 
660 Target: 12, victim: 3, Loss: 2.1712, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:11.54, Cost:0.02 best_reg:115.16: 31%|■ | 311/1000 [00:47<01:44, 6.58it/s]
661 early stop 所有
662 ***Trigger Reverse Engineering結束*** 
663 Target Class: 12 Victim Class: 3 Trigger Size: 116.53671264648438 Optimization Steps: 160
664 ***Symmetric Check開始*** 
665 Target: 3, victim: 12, Loss: 1.6584, Acc: 90.00%, CE_Loss: 0.32, Reg_Loss:593.10, Cost:0.00 best_reg:612.83 avg_loss_reg:595.38: 100%|■ | 160/160 [00:24<00:00, 6.41it/s]
666 ***Symmetric Check結束*** 
667 *****檢測結束***** 
668 檢測結果: Model是安全的(Benign)
669 整體耗時: 78.82564687728882 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000062-----
670 *****檢測結束***** 
671 ***Pre-Screening開始*** 
672 ***Pre-Screening結束*** 
673 可能的攻擊方式: Label Specific Backdoor Attack
674 可能的 target-victim 配對: ['1-2', '1-22', '2-1', '2-23', '3-14', '3-15', '3-23', '4-8', '5-8', '6-8', '10-8', '14-2', '15-3', '15-14', '17-15', '18-12', '21-15', '21-19', '21-22', '22-11']
675 ***Trigger Reverse Engineering開始*** 
676 Target: 1, victim: 22, Loss: 4.5194, Acc: 100.00%, CE_Loss: 0.38, Reg_Loss:818.42, Cost:0.01 best_reg:807.95 avg_loss_reg:818.14: 100%|■ | 1000/1000 [01:45<00:00, 9.46it/s]
677 ***Trigger Reverse Engineering結束*** 
678 Target Class: 1 Victim Class: 22 Trigger Size: 807.9522094726562 Optimization Steps: 385
679 ***Symmetric Check開始*** 
680 Target: 22, victim: 1, Loss: 2.9883, Acc: 100.00%, CE_Loss: 0.38, Reg_Loss:343.09, Cost:0.01 best_reg:345.20 avg_loss_reg:344.14: 70%|■ | 271/385 [00:34<00:14, 7.94it/s]
681 early stop 所有
682 ***Symmetric Check結束*** 
683 *****檢測結束***** 
684 檢測結果: Model是安全的(Benign)
685 整體耗時: 146.68693208694458 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000063-----
686 *****檢測結束***** 
687 ***Pre-Screening開始*** 
688 ***Pre-Screening結束*** 
689 可能的攻擊方式: Label Specific Backdoor Attack
690 可能的 target-victim 配對: ['2-1', '5-3']
691 ***Trigger Reverse Engineering開始*** 
692 Target: 2, victim: 1, Loss: 1.7349, Acc: 100.00%, CE_Loss: 0.19, Reg_Loss:688.51, Cost:0.00 best_reg:666.02 avg_loss_reg:689.23: 100%|■ | 1000/1000 [02:08<00:00, 7.81it/s]
693 ***Trigger Reverse Engineering結束*** 
694 Target Class: 2 Victim Class: 1 Trigger Size: 666.021728515625 Optimization Steps: 601
695 ***Symmetric Check開始*** 
696 Target: 1, victim: 2, Loss: 1.4397, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:374.66, Cost:0.00 best_reg:389.78 avg_loss_reg:372.44: 21%|■ | 128/601 [00:16<00:59, 7.99it/s]
697 early stop 所有
698 ***Symmetric Check結束*** 
699 *****檢測結束***** 
700 檢測結果: Model是安全的(Benign)
701 整體耗時: 150.4124014377594 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000064-----
702 *****檢測結束***** 
703 ***Pre-Screening開始*** 
704 ***Pre-Screening結束*** 
705 可能的攻擊方式: Universal Backdoor Attack
706 可能的 target class: 1
707 可能的 victim classes: ALL
708 ***Trigger Reverse Engineering開始*** 
709 Target: 1, victim: 9, Loss: 0.3352, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:219.82, Cost:0.00 best_reg:216.37 avg_loss_reg:218.93: 8%|■ | 81/1000 [29:25<5:33:45, 21.79s/t]
710 early stop 所有

```

```

711 ***Trigger Reverse Engineering結束***  

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

713 *****檢測結束*****  

714 檢測結果: Model含有後門(Abnormal)  

715 整體耗時: 1774.000016450882  

716 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000065-----  

717 ***Pre-Screening開始***  

718 ***Pre-Screening結束***  

719 ***檢測結束***  

720 檢測結果: Model是安全的(Benign)  

721 整體耗時: 18.231248140335083  

722 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000066-----  

723 ***Pre-Screening開始***  

724 ***Pre-Screening結束***  

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

726 可能的 target-victim 配對: ['7-8']  

727 ***Trigger Reverse Engineering開始***  

728 Target: 7, victim: 8, Loss: 1.9397, Acc: 20.00%, CE_Loss: 1.94, Reg_Loss:9182.88, Cost:0.00 best_reg:10000000000.00 avg_loss_reg:8865.10: 2%| | 20/1000 [00:16<13:25, 1.22it/s]  

729 ***Trigger Reverse Engineering結束***  

730 Target Class: 7 Victim Class: 8 Trigger Size: 10000000000.0 Optimization Steps: 21  

731 *****檢測結束*****  

732 檢測結果: Model是安全的(Benign)  

733 整體耗時: 27.21014904975891  

734 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000067-----  

735 ***Pre-Screening開始***  

736 ***Pre-Screening結束***  

737 可能的 target class: 1  

738 可能的 victim classes: ALL  

739 可能的 victim classes: ALL  

740 ***Trigger Reverse Engineering開始***  

741 Target: 1, victim: 16, Loss: 0.0364, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:888.93, Cost:0.00 best_reg:862.01 avg_loss_reg:894.71: 7%| | 70/1000 [1:15:06<16:37:58, 64.39s/it]  

742 early stop 所有  

743 ***Trigger Reverse Engineering結束***  

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

745 *****檢測結束*****  

746 檢測結果: Model含有後門(Abnormal)  

747 整體耗時: 4533.974607229233  

748 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000068-----  

749 ***Pre-Screening開始***  

750 ***Pre-Screening結束***  

751 可能的攻擊方式: Universal Backdoor Attack  

752 可能的 target class: 0  

753 可能的 victim classes: ALL  

754 ***Trigger Reverse Engineering開始***  

755 Target: 0, victim: 3, Loss: 21.5826, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:561.41, Cost:0.04 best_reg:591.35 avg_loss_reg:591.35: 11%| | 114/1000 [21:06<2:44:06, 11.11s/it]  

756 early stop 所有  

757 ***Trigger Reverse Engineering結束***  

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

759 *****檢測結束*****  

760 檢測結果: Model含有後門(Abnormal)  

761 整體耗時: 1274.459157705307  

762 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000069-----  

763 ***Pre-Screening開始***  

764 ***Pre-Screening結束***  

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

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

767 ***Trigger Reverse Engineering開始***  

768 Target: 4, victim: 13, Loss: 2.2120, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:77.73, Cost:0.03 best_reg:79.74 avg_loss_reg:79.74: 14%| | 144/1000 [00:22<02:13, 6.39it/s]  

769 early stop 所有  

770 ***Trigger Reverse Engineering結束***  

771 Target Class: 4 Victim Class: 13 Trigger Size: 77.72793579101562 Optimization Steps: 94  

772 ***Symmetric Check開始***  

773 Target: 13, victim: 4, Loss: 1.6180, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:6628.50, Cost:0.00 best_reg:6571.07 avg_loss_reg:6684.57: 100%| | 94/94 [00:15<00:00, 6.26it/s]  

774 ***Symmetric Check結束***  

775 *****檢測結束*****  

776 檢測結果: Model含有後門(Abnormal)  

777 整體耗時: 45.588940143585205  

778 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000070-----  

779 ***Pre-Screening開始***  

780 ***Pre-Screening結束***  

781 ***檢測結束***

```

782 檢測結果: Model是安全的(Benign)  
整體耗時: 14.26063823699512 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000071-----  
784 \*\*\*Pre-Screening開始\*\*\*  
785 \*\*\*Pre-Screening結束\*\*\*  
786 \*\*\*Pre-Screening結束\*\*\*  
787 \*\*\*檢測結束\*\*\*  
788 檢測結果: Model是安全的(Benign)  
整體耗時: 13.7104651927948 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000072-----  
789 Target: 1, victim: 2, Loss: 3.4264, Acc: 100.00%, CE\_Loss: 0.44, Reg\_Loss:262.37, Cost:0.01 best\_reg:263.63 avg\_loss\_reg:263.63: 15% | 153/1000 [00:19<01:49, 7.72it/s]  
790 Target: 1, victim: 2, Loss: 3.4264, Acc: 100.00%, CE\_Loss: 0.44, Reg\_Loss:262.37, Cost:0.01 best\_reg:263.63 avg\_loss\_reg:263.63: 15% | 153/1000 [00:19<01:49, 7.72it/s]  
791 \*\*\*Pre-Screening開始\*\*\*  
792 \*\*\*Pre-Screening結束\*\*\*  
793 可能的攻擊方式: Label Specific Backdoor Attack  
可能的 target-victim 配對: ['1-2']  
794 \*\*\*Trigger Reverse Engineering開始\*\*\*  
795 Target Class: 1 Victim Class: 2 Trigger Size: 262.37188720703125 Optimization Steps: 154  
796 Target: 1, victim: 1, Loss: 2.7897, Acc: 100.00%, CE\_Loss: 0.34, Reg\_Loss:727.15, Cost:0.00 best\_reg:724.93 avg\_loss\_reg:726.05: 100% | 154/154 [00:20<00:00, 7.67it/s]  
797 early stop 所有  
798 \*\*\*Trigger Reverse Engineering結束\*\*\*  
799 Target Class: 1 Victim Class: 2 Trigger Size: 262.37188720703125 Optimization Steps: 154  
800 \*\*\*Symmetric Check開始\*\*\*  
801 Target: 2, victim: 1, Loss: 2.7897, Acc: 100.00%, CE\_Loss: 0.34, Reg\_Loss:727.15, Cost:0.00 best\_reg:724.93 avg\_loss\_reg:726.05: 100% | 154/154 [00:20<00:00, 7.67it/s]  
802 \*\*\*Symmetric Check結束\*\*\*  
803 \*\*\*\*\*檢測結束\*\*\*\*\*  
804 檢測結果: Model是安全的(Benign)  
整體耗時: 46.706992854608765 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000073-----  
805 \*\*\*Pre-Screening開始\*\*\*  
806 \*\*\*Pre-Screening結束\*\*\*  
807 \*\*\*Pre-Screening開始\*\*\*  
808 \*\*\*Pre-Screening結束\*\*\*  
809 \*\*\*檢測結束\*\*\*  
810 檢測結果: Model是安全的(Benign)  
整體耗時: 10.553327798843384 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000074-----  
811 Target: 2, victim: 12, Loss: 0.1760, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss:78.20, Cost:0.00 best\_reg:77.17 avg\_loss\_reg:77.29: 5% | 150/1000 [10:04<3:11:23, 12.09s/it]  
812 Target Class: 2 Victim Class: all Trigger Size: 77.1730228000217 Optimization Steps: 51  
813 \*\*\*Pre-Screening開始\*\*\*  
814 \*\*\*Pre-Screening結束\*\*\*  
815 可能的攻擊方式: Universal Backdoor Attack  
可能的 target class: 2  
可能的 victim classes: ALL  
816 可能的 target class: 2  
可能的 victim classes: ALL  
817 可能的 target-victim 配對: ['5-3', '5-7']  
818 \*\*\*Trigger Reverse Engineering開始\*\*\*  
819 Target: 2, victim: 12, Loss: 0.1760, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss:78.20, Cost:0.00 best\_reg:78.20, Cost:0.00 best\_reg:77.17 avg\_loss\_reg:77.29: 5% | 150/1000 [10:04<3:11:23, 12.09s/it]  
820 early stop 所有  
821 \*\*\*Trigger Reverse Engineering結束\*\*\*  
822 Target Class: 2 Victim Class: all Trigger Size: 77.1730228000217 Optimization Steps: 51  
823 \*\*\*\*\*檢測結束\*\*\*\*\*  
824 檢測結果: Model含有後門(Abnormal)  
整體耗時: 610.8321437835693 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000075-----  
825 Target: 3, victim: 5, Loss: 5.7649, Acc: 90.00%, CE\_Loss: 0.46, Reg\_Loss:3534.16, Cost:0.00 best\_reg:3607.45 avg\_loss\_reg:3607.45: 100% | 93/93 [00:09<00:00, 9.97it/s]  
826 \*\*\*Pre-Screening開始\*\*\*  
827 \*\*\*Pre-Screening結束\*\*\*  
828 可能的攻擊方式: Label Specific Backdoor Attack  
可能的 target-victim 配對: ['5-3', '5-7']  
829 \*\*\*Trigger Reverse Engineering開始\*\*\*  
830 Target: 5, victim: 3, Loss: 6.3245, Acc: 100.00%, CE\_Loss: 0.26, Reg\_Loss:105.18, Cost:0.06 best\_reg:105.94 avg\_loss\_reg:105.94: 12% | 1119/1000 [00:12<01:29, 9.82it/s]  
831 \*\*\*Trigger Reverse Engineering開始\*\*\*  
832 Target: 5, victim: 3, Loss: 6.3245, Acc: 100.00%, CE\_Loss: 0.26, Reg\_Loss:105.18, Cost:0.06 best\_reg:105.94 avg\_loss\_reg:105.94: 12% | 1119/1000 [00:12<01:29, 9.82it/s]  
833 0% | 0/93 [00:00<?, ?it/s]early stop 所有  
834 \*\*\*Trigger Reverse Engineering結束\*\*\*  
835 Target Class: 5 Victim Class: 3 Trigger Size: 105.18342590332031 Optimization Steps: 93  
836 \*\*\*Symmetric Check開始\*\*\*  
837 Target: 3, victim: 5, Loss: 5.7649, Acc: 90.00%, CE\_Loss: 0.46, Reg\_Loss:3534.16, Cost:0.00 best\_reg:3607.45 avg\_loss\_reg:3607.45: 100% | 93/93 [00:09<00:00, 9.97it/s]  
838 \*\*\*Symmetric Check結束\*\*\*  
839 \*\*\*\*\*檢測結束\*\*\*\*\*  
840 檢測結果: Model含有後門(Abnormal)  
整體耗時: 27.79301691055298 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000076-----  
841 Target: 8, victim: 9, Loss: 2.5488, Acc: 100.00%, CE\_Loss: 0.23, Reg\_Loss:1030.73, Cost:0.00 best\_reg:1030.82 avg\_loss\_reg:1061.13: 38% | 378/1000 [03:19<05:27, 1.90it/s]  
842 \*\*\*Pre-Screening開始\*\*\*  
843 \*\*\*Pre-Screening結束\*\*\*  
844 可能的攻擊方式: Label Specific Backdoor Attack  
可能的 target-victim 配對: ['8-9']  
845 \*\*\*Trigger Reverse Engineering開始\*\*\*  
846 可能的 target-victim 配對: ['8-9']  
847 \*\*\*Trigger Reverse Engineering開始\*\*\*  
848 Target: 8, victim: 9, Loss: 2.5488, Acc: 100.00%, CE\_Loss: 0.23, Reg\_Loss:1030.73, Cost:0.00 best\_reg:1030.82 avg\_loss\_reg:1061.13: 38% | 378/1000 [03:19<05:27, 1.90it/s]  
849 early stop 所有  
850 \*\*\*Trigger Reverse Engineering結束\*\*\*  
851 Target Class: 8 Victim Class: 9 Trigger Size: 1030.734619140625 Optimization Steps: 379  
852 \*\*\*\*\*檢測結束\*\*\*\*\*

```
853 檢測結果: Model是安全的(Benign)
854 整體耗時: 207.6089973449707 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000077-----
855 ***Pre-Screening開始***
856 ***Pre-Screening結束***
857 ***Pre-Screening結束***
858 ***檢測結果***
859 檢測結果: Model是安全的(Benign)
860 整體耗時: 6.644656895911865 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000078-----
861 ***Pre-Screening開始***
862 ***Pre-Screening結束***
863 ***Pre-Screening結束***
864 ***檢測結果***
865 檢測結果: Model是安全的(Benign)
866 整體耗時: 12.439175367355347 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000079-----
867 ***Pre-Screening開始***
868 ***Pre-Screening結束***
869 ***Pre-Screening結束***
870 可能的攻擊方式: Label Specific Backdoor Attack
871 可能的 target-victim 配對: ['9-1', '21-1']
872 ***Trigger Reverse Engineering開始***
873 Target: 9, victim: 1, Loss: 0.9025, Acc: 100.00%, CE_Loss: 0.31, Reg_Loss:4501.87, Cost:0.00 best_reg:4506.67 avg_loss_reg:4512.84: 61%|████| | 611/1000 [34:53 < 22:12, 3.43s/it]
874 early stop 所有
875 ***Trigger Reverse Engineering結束***
876 Target Class: 9 Victim Class: 1 Trigger Size: 4501.8662109375 Optimization Steps: 591
877 *****檢測結束*****
878 檢測結果: Model是安全的(Benign)
879 整體耗時: 2115.706650706787 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000080-----
880 ***Pre-Screening開始***
881 ***Pre-Screening結束***
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: ['3-10', '13-10']
885 ***Trigger Reverse Engineering開始***
886 Target: 13, victim: 10, Loss: 1.4792, Acc: 100.00%, CE_Loss: 0.12, Reg_Loss:6869.00, Cost:0.00 best_reg:6873.51 avg_loss_reg:6873.51: 56%|████| | 565/1000 [31:56 < 24:35, 3.39s/it]
887 early stop 所有
888 ***Trigger Reverse Engineering結束***
889 Target Class: 13 Victim Class: 10 Trigger Size: 6869.001953125 Optimization Steps: 394
890 *****檢測結束*****
891 檢測結果: Model是安全的(Benign)
892 整體耗時: 1937.7479786872864 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000081-----
893 ***Pre-Screening開始***
894 ***Pre-Screening結束***
895 ***Pre-Screening結束***
896 ***檢測結果***
897 檢測結果: Model是安全的(Benign)
898 整體耗時: 15.795825004577637 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000082-----
899 ***Pre-Screening開始***
900 ***Pre-Screening結束***
901 ***Pre-Screening結束***
902 可能的攻擊方式: Universal Backdoor Attack
903 可能的 target class: 2
904 可能的 victim classes: ALL
905 ***Trigger Reverse Engineering開始***
906 Target: 2, victim: 9, Loss: 0.1716, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:255.17, Cost:0.00 best_reg:5811.71 avg_loss_reg:318.77: 2%| | 17/1000 [03:54 < 3:46:15, 13.81s/it]
907 early stop 所有
908 ***Trigger Reverse Engineering結束***
909 Target Class: 2 Victim Class: all Trigger Size: 5811.7144775390625 Optimization Steps: 18
910 *****檢測結束*****
911 檢測結果: Model是安全的(Benign)
912 整體耗時: 242.2243571281433 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000083-----
913 ***Pre-Screening開始***
914 ***Pre-Screening結束***
915 ***Pre-Screening結束***
916 可能的攻擊方式: Label Specific Backdoor Attack
917 可能的 target-victim 配對: ['2-7']
918 ***Trigger Reverse Engineering開始***
919 Target: 2, victim: 7, Loss: 0.8094, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:311.98, Cost:0.00 best_reg:313.97 avg_loss_reg:313.97: 15%|████| | 146/1000 [00:18 < 01:47, 7.94it/s]
920 early stop 所有
921 ***Trigger Reverse Engineering結束***
922 Target Class: 2 Victim Class: 7 Trigger Size: 311.98199462890625 Optimization Steps: 147
923 ***Symmetric Check開始***
```

```

924 Target: 7, victim: 2, Loss: 0.9666, Acc: 100.00%, CE_Loss: 0.24, Reg_Loss:1638.13, Cost:0.00 best_reg:1666.78 avg_loss_reg:1666.78: 100% | [REDACTED] | 147/147 [00:17<00:00, 8.46it/s]
925 ***Symmetric Check結束*** 
926 *****檢測結束***** 
927 檢測結果: Model是安全的(Benign)
928 整體耗時: 42.177544832229614
929 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000084----- 
930 ***Pre-Screening開始*** 
931 可能的攻擊方式: Universal Backdoor Attack
932 可能的 target class: 0
933 可能的 victim classes: ALL
934 可能的 victim class: ALL
935 ***Trigger Reverse Engineering開始*** 
936 Target: 0, victim: 6, Loss: 0.6189, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:171.54, Cost:0.00 best_reg:171.89 avg_loss_reg:171.05: 11% | [REDACTED] | 106/1000 [38:08<5:21:40, 21.59s/it]
937 early stop 所有
938 ***Trigger Reverse Engineering結束*** 
939 Target Class: 0 Victim Class: all Trigger Size: 171.70403442382812 Optimization Steps: 107
940 *****檢測結束***** 
941 檢測結果: Model含有後門(Abnormal)
942 整體耗時: 2296.520660877228
943 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000085----- 
944 ***Pre-Screening開始*** 
945 ***Pre-Screening結束*** 
946 可能的攻擊方式: Label Specific Backdoor Attack
947 可能的 target-victim 配對: ['0-1', '0-18', '0-19', '8-7', '8-16', '12-17', '19-18']
948 ***Trigger Reverse Engineering開始*** 
949 Target: 19, victim: 18, Loss: 1.4830, Acc: 100.00%, CE_Loss: 0.32, Reg_Loss:1167.94, Cost:0.00 best_reg:1182.68 avg_loss_reg:1171.06: 41% | [REDACTED] | 409/1000 [24:45<35:47, 3.63s/it]
950 early stop 所有
951 ***Trigger Reverse Engineering結束*** 
952 Target Class: 19 Victim Class: 18 Trigger Size: 1167.9443359375 Optimization Steps: 205
953 *****檢測結束***** 
954 檢測結果: Model是安全的(Benign)
955 整體耗時: 1512.9597244262695
956 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000086----- 
957 ***Pre-Screening開始*** 
958 ***Pre-Screening結束*** 
959 *****檢測結束***** 
960 檢測結果: Model是安全的(Benign)
961 整體耗時: 17.805039882659912
962 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000087----- 
963 ***Pre-Screening開始*** 
964 ***Pre-Screening結束*** 
965 *****檢測結束***** 
966 檢測結果: Model是安全的(Benign)
967 整體耗時: 6.194135665893555
968 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000088----- 
969 ***Pre-Screening開始*** 
970 ***Pre-Screening結束*** 
971 可能的攻擊方式: Label Specific Backdoor Attack
972 可能的 target-victim 配對: ['0-1', '0-23', '3-4', '3-19', '9-4', '11-4', '11-19', '16-2', '17-3', '17-9', '18-4', '18-19', '19-4', '23-0']
973 ***Trigger Reverse Engineering開始*** 
974 Target: 18, victim: 4, Loss: 4.4473, Acc: 100.00%, CE_Loss: 0.23, Reg_Loss:73.16, Cost:0.06 best_reg:73.45 avg_loss_reg:73.45: 50% | [REDACTED] | 496/1000 [01:14<01:15, 6.67it/s]
975 early stop 所有
976 ***Trigger Reverse Engineering結束*** 
977 Target Class: 18 Victim Class: 4 Trigger Size: 73.15617370605469 Optimization Steps: 81
978 ***Symmetric Check開始*** 
979 Target: 4, victim: 18, Loss: 0.5927, Acc: 80.00%, CE_Loss: 0.59, Reg_Loss:29864.18, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:29799.39: 100% | [REDACTED] | 81/81 [00:14<00:00, 5.74it/s]
980 ***Symmetric Check結束*** 
981 *****檢測結束***** 
982 檢測結果: Model含有後門(Abnormal)
983 整體耗時: 95.38706994056702
984 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000089----- 
985 ***Pre-Screening開始*** 
986 ***Pre-Screening結束*** 
987 可能的攻擊方式: Universal Backdoor Attack
988 可能的 target class: 9
989 可能的 victim classes: ALL
990 ***Trigger Reverse Engineering開始*** 
991 Target: 9, victim: 19, Loss: 0.1386, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:264.28, Cost:0.00 best_reg:339.97 avg_loss_reg:265.44: 3% | [REDACTED] | 27/1000 [07:45<4:39:32, 17.24s/it]
992 early stop 所有
993 ***Trigger Reverse Engineering結束*** 
994 Target Class: 9 Victim Class: all Trigger Size: 339.9654017857143 Optimization Steps: 28

```

```

995 *****檢測結果*****檢測結束*****
996 檢測結果: Model含有後門(Abnormal)
997 整體耗時: 474.0966110229492
998 *****Pre-Screening開始*****
999 *****Pre-Screening結束*****
1000 可能的攻擊方式: Label Specific Backdoor Attack
1001 可能的 target-victim 配對: ['1-0']
1002 ***Trigger Reverse Engineering開始*****
1003 Target: 1, victim: 0, Loss: 5.0626, Acc: 100.00%, CE_Loss: 0.37, Reg_Loss:926.21, Cost:0.01 best_reg:927.14 avg_loss_reg:927.14: 19% █ | 187/1000 [00:37<02:41, 5.03it/s]
1004 Target: 1, victim: 0, Loss: 5.0626, Acc: 100.00%, CE_Loss: 0.37, Reg_Loss:926.21, Cost:0.01 best_reg:927.14 avg_loss_reg:927.14: 19% █ | 187/1000 [00:37<02:41, 5.03it/s]
1005 0% | 0/188 [00:00<?, ?it/s]early stop 所有
1006 ***Trigger Reverse Engineering結束****
1007 Target Class: 1 Victim Class: 0 Trigger Size: 926.2102661132812 Optimization Steps: 188
1008 ***Symmetric Check開始*****
1009 Target: 0, victim: 1, Loss: 6.2260, Acc: 100.00%, CE_Loss: 0.35, Reg_Loss:1739.66, Cost:0.00 best_reg:1739.85 avg_loss_reg:1739.85: 76% █ | 143/188 [00:27<00:08, 5.18it/s]
1010 early stop 所有
1011 ***Symmetric Check結束*****
1012 ***Pre-Screening開始*****
1013 檢測結果: Model是安全的(Benign)
1014 整體耗時: 71.55773138999939
1015 *****Pre-Screening結束*****
1016 ***Pre-Screening開始*****
1017 ***Pre-Screening結束*****
1018 ***檢測結束****
1019 檢測結果: Model是安全的(Benign)
1020 整體耗時: 7.3559253215789795
1021 *****Pre-Screening結束*****
1022 ***Pre-Screening開始*****
1023 ***Pre-Screening結束*****
1024 可能的攻擊方式: Label Specific Backdoor Attack
1025 可能的 target-victim 配對: [0-5]
1026 ***Trigger Reverse Engineering開始*****
1027 Target: 0, victim: 5, Loss: 2.8211, Acc: 100.00%, CE_Loss: 0.22, Reg_Loss:2600.79, Cost:0.00 best_reg:2554.50 avg_loss_reg:2552.52: 100% █ | 1000/1000 [11:44<00:00, 1.42it/s]
1028 ***Trigger Reverse Engineering結束****
1029 Target Class: 5 Victim Class: 5 Trigger Size: 2554.49853515625 Optimization Steps: 1000
1030 *****檢測結束*****
1031 檢測結果: Model是安全的(Benign)
1032 整體耗時: 712.7076923847198
1033 *****Pre-Screening結束*****
1034 ***Pre-Screening開始*****
1035 ***Pre-Screening結束*****
1036 可能的攻擊方式: Label Specific Backdoor Attack
1037 可能的 target-victim 配對: ['4-6', '10-6', '11-13']
1038 ***Trigger Reverse Engineering開始*****
1039 Target: 11, victim: 13, Loss: 9.5290, Acc: 100.00%, CE_Loss: 0.21, Reg_Loss:242.52, Cost:0.04 best_reg:243.42 avg_loss_reg:240.30: 14% █ | 141/1000 [00:23<02:23, 6.00it/s]
1040 early stop 所有
1041 ***Trigger Reverse Engineering結束*****
1042 Target Class: 11 Victim Class: 13 Trigger Size: 242.5188751220703 Optimization Steps: 120
1043 ***Symmetric Check開始*****
1044 Target: 13, victim: 11, Loss: 4.4305, Acc: 100.00%, CE_Loss: 0.53, Reg_Loss:1154.45, Cost:0.00 best_reg:1151.29 avg_loss_reg:1154.90: 100% █ | 120/120 [00:20<00:00, 5.82it/s]
1045 ***Symmetric Check結束*****
1046 *****檢測結束*****
1047 檢測結果: Model是安全的(Benign)
1048 整體耗時: 51.25985503196716
1049 *****Pre-Screening開始*****
1050 ***Pre-Screening結束*****
1051 ***Pre-Screening開始*****
1052 可能的攻擊方式: Label Specific Backdoor Attack
1053 可能的 target-victim 配對: ['1-2', '2-9', '2-22', '3-15', '4-20', '5-11', '5-20', '6-3', '7-3', '8-2', '8-22', '9-19', '11-20', '12-20', '13-12', '13-20', '15-3', '15-11', '18-15', '18-5', '18-22', '20-5', '21-2', '21-8']
1054 ***Trigger Reverse Engineering開始*****
1055 Target: 9, victim: 19, Loss: 1.4410, Acc: 90.00%, CE_Loss: 0.75, Reg_Loss:2331.50, Cost:0.00 best_reg:2390.04 avg_loss_reg:2325.86: 100% █ | 1000/1000 [18:32<00:00, 1.11s/it]
1056 ***Trigger Reverse Engineering結束*****
1057 Target Class: 9 Victim Class: 19 Trigger Size: 2390.0443359375 Optimization Steps: 528
1058 *****檢測結束*****
1059 檢測結果: Model是安全的(Benign)
1060 整體耗時: 1127.5095200538635
1061 *****Pre-Screening開始*****
1062 ***Pre-Screening結束*****
1063 ***Pre-Screening結束*****
1064 可能的攻擊方式: Label Specific Backdoor Attack
1065 可能的 target-victim 配對: ['2-3', '2-4', '2-5']

```

```

1066 ***Trigger Reverse Engineering開始****
1067 Target: 2, victim: 5, Loss: 13.6150, Acc: 0.00%, CE_Loss: 13.62, Reg_Loss:5354.46, Cost:0.00 best_reg:1000000000.00 avg_loss_reg:4800.22: 3%| | 32/1000 [00:19<09:57, 1.62it/s]
1068 ***Trigger Reverse Engineering結束****
1069 Target Class: 2 Victim Class: 3 Trigger Size: 1000000000.0 Optimization Steps: 11
1070 *****檢測結果: Model是安全的(Benign)
1071 檢測結果: Model是安全的(Benign)
1072 整體耗時: 23.3623[0647964478]                                     插播檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000096-----
1073 *****Pre-Screening開始****
1074 *****Pre-Screening結束****
1075 可能的攻擊方式: Label Specific Backdoor Attack
1076 可能的 target-victim 配對: ['2-3']
1077 ***Trigger Reverse Engineering開始****
1078 Target Class: 2 Victim Class: 3 Trigger Size: 1068.46, Cost:0.00 best_reg:1069.58 avg_loss_reg:1069.70: 18%| | 183/1000 [00:38<02:53, 4.71it/s]
1079 Target: 2, victim: 3, Loss: 1.7051, Acc: 100.00%, CE_Loss: 0.10, Reg_Loss:1068.46, Cost:0.00 best_reg:1069.58 avg_loss_reg:1069.70: 18%| | 183/1000 [00:38<02:53, 4.71it/s]
1080 early stop 所有
1081 ***Trigger Reverse Engineering結束****
1082 Target Class: 2 Victim Class: 3 Trigger Size: 1068.4608154296875 Optimization Steps: 184
1083 *****檢測結果: Model是安全的(Benign)
1084 整體耗時: 42.21012806892395                                     插播檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000097-----
1085 *****Pre-Screening開始****
1086 *****Pre-Screening結束****
1087 ***Pre-Screening開始****
1088 ***Pre-Screening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: 18.003498315811157                                     插播檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000098-----
1092 *****Pre-Screening開始****
1093 *****Pre-Screening結束****
1094 可能的攻擊方式: Label Specific Backdoor Attack
1095 可能的 target-victim 配對: ['1-3', '1-7', '2-3', '2-6', '4-10', '7-1', '7-4', '7-12', '8-5', '8-6', '11-12']
1096 可能的 target-victim 配對: ['1-3', '1-7', '2-3', '2-6', '4-10', '7-1', '7-4', '7-12', '8-5', '8-6', '11-12']
1097 ***Trigger Reverse Engineering開始****
1098 Target: 1, victim: 7, Loss: 1.7547, Acc: 100.00%, CE_Loss: 0.11, Reg_Loss:324.98, Cost:0.01 best_reg:326.56 avg_loss_reg:326.56: 44%| | 440/1000 [00:58<01:13, 7.58it/s]
1099 0%
| 0/146 [00:00:<?, ?it/s]early stop 所有
1100 ***Trigger Reverse Engineering結束****
1101 Target Class: 1 Victim Class: 7 Trigger Size: 324.9828796386719 Optimization Steps: 146
1102 ***Symmetric Check開始****
1103 Target: 7, victim: 1, Loss: 4.0716, Acc: 100.00%, CE_Loss: 0.26, Reg_Loss:334.25, Cost:0.01 best_reg:335.66 avg_loss_reg:335.66: 69%| | 101/146 [00:15<00:06, 6.58it/s]
1104 early stop 所有
1105 ***Symmetric Check結束****
1106 *****檢測結果: Model是安全的(Benign)
1107 *****檢測結果: Model是安全的(Benign)
1108 整體耗時: 80.1291229724884                                     插播檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-000000099-----
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: ['2-7', '3-1']
1113 可能的 target-victim 配對: ['2-7', '3-1']
1114 ***Trigger Reverse Engineering開始****
1115 Target: 2, victim: 7, Loss: 2.6102, Acc: 100.00%, CE_Loss: 0.18, Reg_Loss:2426.16, Cost:0.00 best_reg:2426.65 avg_loss_reg:2427.65: 41%| | 414/1000 [02:22<03:22, 2.90it/s]
1116 early stop 所有
1117 ***Trigger Reverse Engineering結束****
1118 Target Class: 2 Victim Class: 7 Trigger Size: 2426.15771484375 Optimization Steps: 365
1119 *****檢測結果: Model是安全的(Benign)
1120 檢測結果: Model是安全的(Benign)
1121 整體耗時: 150.3266522884369                                     插播檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000100-----
1122 *****Pre-Screening開始****
1123 *****Pre-Screening結束****
1124 ***Pre-Screening開始****
1125 ***檢測結果****
1126 檢測結果: Model是安全的(Benign)
1127 整體耗時: 20.945130109786987                                     插播檔案: D:\UUULi\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000101-----
1128 *****Pre-Screening開始****
1129 *****Pre-Screening結束****
1130 可能的攻擊方式: Universal Backdoor Attack
1131 可能的 target class: 4
1132 可能的 victim classes: ALL
1133 可能的 victim classes: ALL
1134 ***Trigger Reverse Engineering開始****
1135 Target: 4, victim: 17, Loss: 0.1802, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:270.06, Cost:0.00 best_reg:282.12 avg_loss_reg:277.22: 3%| | 30/1000 [08:57<4:49:27, 17.90it/s]
1136 early stop 所有

```

```
1137 ***Trigger Reverse Engineering結束***  
1138 Target Class: 4 Victim Class: all Trigger Size: 282.1248524983724 Optimization Steps: 31  
1139 *****檢測結束*****  
1140 檢測結果: Model含有後門(Abnormal)  
1141 整體耗時: 546.2802238464355  
1142 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000102-----  
1143 ***Pre-Screening開始***  
1144 ***Pre-Screening結束***  
1145 可能的攻擊方式: Label Specific Backdoor Attack  
1146 可能的 target-victim 配對: ['6-1', '6-2']  
1147 ***Trigger Reverse Engineering開始***  
1148 Target: 6, victim: 2, Loss: 3.8521, Acc: 100.00%, CE_Loss: 0.20, Reg_Loss:42.26, Cost:0.09 best_reg:43.79 avg_loss_reg:42.37: 9% | 88/1000 [00:48<08:23, 1.81it/s]  
1149 0% | 0/73 [00:00<?, ?it/s]early stop 所有  
1150 ***Trigger Reverse Engineering結束***  
1151 Target Class: 6 Victim Class: 2 Trigger Size: 42.26390075683594 Optimization Steps: 73  
1152 ***Symmetric Check開始***  
1153 Target: 2, victim: 6, Loss: 1.4916, Acc: 90.00%, CE_Loss: 0.58, Reg_Loss:4612.52, Cost:0.00 best_reg:10515.01 avg_loss_reg:4601.79: 100% | 73/73 [00:43<00:00, 1.69it/s]  
1154 ***Symmetric Check結束***  
1155 *****檢測結束*****  
1156 檢測結果: Model含有後門(Abnormal)  
1157 整體耗時: 95.27344012260437  
1158 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round3\TrainData\models\unzip\id-00000103-----  
1159 ***Pre-Screening開始***  
1160 ***Pre-Screening結束***  
1161 可能的攻擊方式: Universal Backdoor Attack  
1162 可能的 target class: 7  
1163 可能的 victim classes: ALL  
1164 ***Trigger Reverse Engineering開始***  
1165 Target: 7, victim: 16, Loss: 0.7842, Acc: 96.88%, CE_Loss: 0.27, Reg_Loss:102.49, Cost:0.01 best_reg:115.48 avg_loss_reg:105.86: 3% | 34/1000 [11:01<5:13:15, 19.46s/it]  
1166 Traceback (most recent call last):  
1167 File "D:\UUU\test_code\k_arm\test\main.py", line 87, in <module>  
1168 trigger_reverse_engineering(target_classes, victim_classes, backdoor_type, model, DATA_PATH,  
1169 File "D:\UUU\test_code\k_arm\test\k_arm\reverse.py", line 54, in trigger_reverse_engineering  
1170 pattern, mask, l1_norm, time_cost = scanner.scanning(  
1171 File "D:\UUU\test_code\k_arm\test\k_arm\scanner.py", line 153, in scanning  
1172 f'Target: {target_classes[target_index]}, victim: {labels[0]}, Loss: {loss:.4f}'  
1173 File "C:\Users\slab\anaconda3\envs\pytorch1\lib\site-packages\torch\tensor.py", line 534, in __format__  
1174 return self.item().__format__(format_spec)  
1175 KeyboardInterrupt  
1176  
1177 Process finished with exit code -1073741510 (0xc0000013A: interrupted by Ctrl+C)  
1178
```