

```

1 C:\Users\slab\anaconda3\envs\pytorch1_2_0\python.exe D:\UUUi\test_code\k_arm_test\main.py
2 -----掃描檔案: D:\UUUi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-0000000000
3 ***Pre-Screening開始***
4 可能的攻擊方式: Universal Backdoor Attack
5 可能的 target class: 2
6 可能的 victim classes: ALL
7 可能的 victim classes: ALL
8 ***Trigger Reverse Engineering開始***
9 Target: 2, victim: 4, Loss: 0.2135, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:63.20, Cost:0.00 best_reg:63.08 avg_loss_reg:63.74: 7%| | 66/1000 [13:44<3:14:24, 12.49s/it]
10 early stop 所有
11 ***Trigger Reverse Engineering結束***
12 Target Class: all Trigger Size:63.07805800437927 Optimization Steps: 67
13 *****檢測結果: Model含有後門(Abnormal)
14 檢測結果: Model含有後門(Abnormal)
15 整體耗時: 828.2831335067749
16 -----掃描檔案: D:\UUUi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-0000000001
17 ***Pre-Screening開始***
18 ***Pre-Screening結束***
19 ***檢測結束***
20 檢測結果: Model是安全的(Benign)
21 整體耗時: 4.70327615737915
22 -----掃描檔案: D:\UUUi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-0000000002
23 ***Pre-Screening開始***
24 ***Pre-Screening結束***
25 可能的攻擊方式: Universal Backdoor Attack
26 可能的 target class: 3
27 可能的 victim classes: ALL
28 ***Trigger Reverse Engineering開始***
29 Target: 3, victim: 4, Loss: 0.3418, Acc: 90.00%, CE_Loss: 0.18, Reg_Loss:70.53, Cost:0.00 best_reg:79.39 avg_loss_reg:76.94: 5%| | 52/1000 [18:54<5:44:34, 21.81s/it]
30 early stop 所有
31 ***Trigger Reverse Engineering結束***
32 Target Class: 3 Victim Class: all Trigger Size: 79.38817358016968 Optimization Steps: 53
33 *****檢測結果: Model含有後門(Abnormal)
34 檢測結果: Model含有後門(Abnormal)
35 整體耗時: 1137.9138464927673
36 -----掃描檔案: D:\UUUi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-0000000003
37 ***Pre-Screening開始***
38 ***Pre-Screening結束***
39 可能的攻擊方式: Universal Backdoor Attack
40 可能的 target class: 3
41 可能的 victim classes: ALL
42 ***Trigger Reverse Engineering開始***
43 Target: 3, victim: 4, Loss: 0.1769, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:229.93, Cost:0.00 best_reg:240.02 avg_loss_reg:229.81: 5%| | 47/1000 [18:30<6:15:25, 23.64s/it]
44 early stop 所有
45 ***Trigger Reverse Engineering結束***
46 Target Class: 3 Victim Class: all Trigger Size: 240.02048683166504 Optimization Steps: 48
47 *****檢測結果: Model含有後門(Abnormal)
48 檢測結果: Model含有後門(Abnormal)
49 整體耗時: 1116.0000867843628
50 -----掃描檔案: D:\UUUi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-0000000004
51 ***Pre-Screening開始***
52 ***Pre-Screening結束***
53 ***檢測結果: Model是安全的(Benign)
54 檢測結果: Model是安全的(Benign)
55 整體耗時: 3.82447743158325
56 -----掃描檔案: D:\UUUi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-0000000005
57 ***Pre-Screening開始***
58 ***Pre-Screening結束***
59 可能的攻擊方式: Label Specific Backdoor Attack
60 可能的 target-victim 配對: ['0-1', '1-0']
61 ***Trigger Reverse Engineering開始***
62 Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.61: 20%| | 200/1000 [06:11<24:47, 1.86s/it]
63 early stop 所有
64 ***Trigger Reverse Engineering結束***
65 Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180
66 ***Symmetric Check開始***
67 Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10: 68%| | 676/1000 [20:52<10:00, 1.85s/it]
68 early stop 所有
69 ***Symmetric Check結束***
70 *****檢測結果: Model是安全的(Benign)
71 檢測結果: Model是安全的(Benign)

```

```
72 整體耗時: 1627.9121837615967 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000006-----
73 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000006-----
74 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000006-----
75 可能的攻擊方式: Label Specific Backdoor Attack
76 可能的 target-victim 配對: ['0-1', '1-0']
77 可能的 target Reverse Engineering 開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000006-----
78 ***Trigger Reverse Engineering 開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000006-----
79 Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.40 avg_loss_reg:45.61: 20%| 200/1000 [06:49<27:18, 2.05s/it]
80 early stop 所有
81 ***Trigger Reverse Engineering 結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000006-----
82 Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180
83 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000007-----
84 Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10: 68%| 676/1000 [22:42<10:53, 2.02s/it]
85 early stop 所有
86 ***Symmetric Check結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000007-----
87 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000007-----
88 檢測結果: Model是安全的(Benign)
89 整體耗時: 1775.5744450092316 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000007-----
90 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000007-----
91 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000007-----
92 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000007-----
93 可能的攻擊方式: Label Specific Backdoor Attack
94 可能的 target-victim 配對: ['1-3', '1-4']
95 ***Trigger Reverse Engineering 開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000007-----
96 Target: 1, victim: 3, Loss: 0.4389, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:85.39, Cost:0.01 best_reg:85.17 avg_loss_reg:84.85: 100%| 1000/1000 [54:42<00:00, 3.28s/it]
97 ***Trigger Reverse Engineering 結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000007-----
98 Target Class: 1 Victim Class: 3 Trigger Size: 85.17329025268555 Optimization Steps: 982
99 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000007-----
100 Target: 3, victim: 1, Loss: 1.2631, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:71.62, Cost:0.02 best_reg:72.47 avg_loss_reg:71.65: 100%| 1000/1000 [54:41<00:00, 3.28s/it]
101 ***Symmetric Check結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000008-----
102 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000008-----
103 檢測結果: Model是安全的(Benign)
104 整體耗時: 6572.10943558319 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000008-----
105 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000008-----
106 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000008-----
107 可能的攻擊方式: Label Specific Backdoor Attack
108 可能的 target-victim 配對: ['3-1', '3-1']
109 可能的 target-victim 配對: ['1-3', '3-1']
110 ***Trigger Reverse Engineering 開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000008-----
111 Target: 1, victim: 3, Loss: 0.6401, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:125.66, Cost:0.01 best_reg:126.49 avg_loss_reg:126.49: 29%| 286/1000 [10:57<27:22, 2.30s/it]
112 early stop 所有
113 ***Trigger Reverse Engineering 結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000008-----
114 Target Class: 1 Victim Class: 3 Trigger Size: 125.77005767822266 Optimization Steps: 264
115 ***Symmetric Check開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000008-----
116 Target: 3, victim: 1, Loss: 0.1343, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:126.84, Cost:0.00 best_reg:127.01 avg_loss_reg:125.80: 27%| 266/1000 [10:12<28:09, 2.30s/it]
117 early stop 所有
118 ***Symmetric Check結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000008-----
119 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000008-----
120 檢測結果: Model是安全的(Benign)
121 整體耗時: 1278.0683135986328 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000010-----
122 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000010-----
123 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000010-----
124 可能的攻擊方式: Universal Backdoor Attack
125 可能的 target class: 0
126 可能的 victim classes: ALL
127 可能的 victim classes: ALL
128 ***Trigger Reverse Engineering 結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000010-----
129 Target: 0, victim: 4, Loss: 0.3445, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:20.12, Cost:0.02 best_reg:20.07 avg_loss_reg:19.87: 8%| 80/1000 [29:11<5:35:38, 21.89s/it]
130 early stop 所有
131 ***Trigger Reverse Engineering 結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000010-----
132 Target Class: 0 Victim Class: all Trigger Size: 20.0680912733078 Optimization Steps: 81
133 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000010-----
134 檢測結果: Model含有後門(Abnormal)
135 整體耗時: 1758.829291343689 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000011-----
136 ***Pre-Screening開始***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000011-----
137 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000011-----
138 ***Pre-Screening結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000011-----
139 ***檢測結束***-----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000011-----
140 檢測結果: Model是安全的(Benign)
141 整體耗時: 8.534503936767578 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000012-----
```

```

143 ***Pre-Screening開始****
144 ***Pre-Screening結束****
145 可能的攻擊方式: Label Specific Backdoor Attack
146 可能的 target-victim 配對: [0-1, '1-0']
147 ***Trigger Reverse Engineering 開始****
148 Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.40 avg_loss_reg:45.61: 20% █ | 200/1000 [08:02 < 32.08, 2.41s/it]
149 early stop 所有
150 ***Trigger Reverse Engineering 結束****
151 Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180
152 ***Symmetric Check開始****
153 Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10: 68% █ | 676/1000 [27.01 < 12:57, 2.40s/it]

154 early stop 所有
155 ***Symmetric Check結束****
156 檢測結果: Model是安全的(Benign)
157 檢測結果: Model含有後門(Abnormal)
158 整體耗時: 2111.062262058258 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000013-----
```

---

```

159 ***Pre-Screening開始****
160 ***Pre-Screening結束****
161 ***Pre-Screening結果: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000013-----
```

---

```

162 可能的攻擊方式: Universal Backdoor Attack
163 可能的 target class: ALL
164 可能的 victim classes: ALL
165 ***Trigger Reverse Engineering 開始****
166 Target: 1, victim: 4, Loss: 0.4686, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:310.07, Cost:0.00 best_reg:306.49 avg_loss_reg:303.28: 12% █ | 117/1000 [37:14 < 4:41:01, 19.10s/it]
167 early stop 所有
168 ***Trigger Reverse Engineering 結束****
169 Target Class: 1 Victim Class: all Trigger Size: 306.49031257629395 Optimization Steps: 118
170 ***Pre-Screening開始****
171 檢測結果: Model含有後門(Abnormal)
172 整體耗時: 2241.4676427841187 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000014-----
```

---

```

173 ***Pre-Screening結束****
174 ***Pre-Screening開始****
175 ***Pre-Screening結束****
176 可能的攻擊方式: Universal Backdoor Attack
177 可能的 target class: 3
178 可能的 victim classes: ALL
179 ***Trigger Reverse Engineering 開始****
180 Target: 3, victim: 4, Loss: 1.0423, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:27.11, Cost:0.04 best_reg:27.05 avg_loss_reg:27.35: 7% █ | 70/1000 [26:37 < 5:53:43, 22.82s/it]
181 early stop 所有
182 ***Trigger Reverse Engineering 結束****
183 Target Class: 3 Victim Class: all Trigger Size: 27.04645323753357 Optimization Steps: 71
184 ***Pre-Screening開始****
185 檢測結果: Model含有後門(Abnormal)
186 整體耗時: 1605.182599067688 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000015-----
```

---

```

187 ***Pre-Screening結束****
188 ***Pre-Screening開始****
189 ***Pre-Screening結束****
190 可能的攻擊方式: Universal Backdoor Attack
191 可能的 target class: 2
192 可能的 victim classes: ALL
193 ***Trigger Reverse Engineering 開始****
194 Target: 2, victim: 4, Loss: 0.2567, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:170.54, Cost:0.00 best_reg:172.29 avg_loss_reg:168.89: 10% █ | 97/1000 [41:17 < 6:24:26, 25.54s/it]
195 early stop 所有
196 ***Trigger Reverse Engineering 結束****
197 Target Class: 2 Victim Class: all Trigger Size: 172.2930526733984 Optimization Steps: 98
198 ***Pre-Screening開始****
199 檢測結果: Model含有後門(Abnormal)
200 整體耗時: 2486.9387426376343 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000016-----
```

---

```

201 ***Pre-Screening開始****
202 ***Pre-Screening結束****
203 ***Pre-Screening結果: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000016-----
```

---

```

204 可能的攻擊方式: Universal Backdoor Attack
205 可能的 target class: 3
206 可能的 victim classes: ALL
207 ***Trigger Reverse Engineering 開始****
208 Target: 3, victim: 4, Loss: 0.4802, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:42.16, Cost:0.01 best_reg:42.68 avg_loss_reg:42.06: 6% █ | 60/1000 [21:19 < 5:34:11, 21.33s/it]
209 early stop 所有
210 ***Trigger Reverse Engineering 結束****
211 Target Class: 3 Victim Class: all Trigger Size: 42.67514705657959 Optimization Steps: 61
212 ***Pre-Screening開始****
213 檢測結果: Model含有後門(Abnormal)
```

```
214 整體耗時: 1287.5432851314545 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000017-----
215 *****Pre-Screening開始*****
216 *****Pre-Screening結束*****
217 可能的攻擊方式: Universal Backdoor Attack
218 可能的 target class: 0
219 可能的 victim classes: ALL
220 Target Class: 0 Victim Class: all Trigger Size: 789.9558792114258 Optimization Steps: 82
221 ***Trigger Reverse Engineering開始****
222 Target: 0, victim: 4, Loss: 0.5637, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:786.66, Cost:0.00 best_reg:789.96 avg_loss_reg:778.54: 8% █ | 81/1000 [32:06<6:04:13, 23.78s/it]
223 early stop 所有
224 ***Trigger Reverse Engineering結束****
225 Target Class: 0 Victim Class: all Trigger Size: 789.9558792114258 Optimization Steps: 82
226 *****Symmetric Check結束*****
227 檢測結果: Model含有後門(Abnormal)
228 整體耗時: 1934.4419870376587 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000018-----
229 *****Pre-Screening開始*****
230 *****Pre-Screening結束*****
231 可能的攻擊方式: Label Specific Backdoor Attack
232 可能的 target-victim 配對: ['0-1', '1-0']
233 可能的 target-victim 配對: ['0-1', '1-0']
234 ***Trigger Reverse Engineering開始****
235 Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.40 avg_loss_reg:45.61: 20% █ | 200/1000 [07:53<31:33, 2.37s/it]
236 early stop 所有
237 ***Trigger Reverse Engineering結束****
238 Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180
239 *****Symmetric Check開始*****
240 Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10: 68% █ | 676/1000 [26:23<12:38, 2.34s/it]
241 early stop 所有
242 *****Symmetric Check結束*****
243 *****Symmetric Check結束*****
244 檢測結果: Model是安全的(Benign)
245 整體耗時: 2064.5317862033844 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000020-----
246 *****Pre-Screening開始*****
247 *****Pre-Screening結束*****
248 可能的攻擊方式: Universal Backdoor Attack
249 可能的 target class: 4
250 可能的 victim classes: ALL
251 可能的 victim classes: ALL
252 ***Trigger Reverse Engineering開始****
253 Target: 4, victim: 4, Loss: 0.2084, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:312.59, Cost:0.00 best_reg:308.60 avg_loss_reg:305.98: 4% █ | 45/1000 [19:12<6:47:34, 25.61s/it]
254 early stop 所有
255 ***Trigger Reverse Engineering結束*****
256 Target Class: 4 Victim Class: all Trigger Size: 308.6006031036377 Optimization Steps: 46
257 *****Symmetric Check結束*****
258 檢測結果: Model含有後門(Abnormal)
259 整體耗時: 1165.4435005187988 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000021-----
260 *****Pre-Screening開始*****
261 *****Pre-Screening結束*****
262 *****Pre-Screening結束*****
263 *****檢測結束*****
264 檢測結果: Model是安全的(Benign)
265 整體耗時: 8.925481796264648 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000022-----
266 *****Pre-Screening開始*****
267 *****Pre-Screening結束*****
268 可能的攻擊方式: Universal Backdoor Attack
269 可能的 target class: 0
270 可能的 victim classes: ALL
271 可能的 victim classes: ALL
272 ***Trigger Reverse Engineering開始****
273 Target: 0, victim: 4, Loss: 0.3501, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:100.11, Cost:0.00 best_reg:102.53 avg_loss_reg:99.75: 4% █ | 39/1000 [15:11<6:14:31, 23.38s/it]
274 early stop 所有
275 ***Trigger Reverse Engineering結束*****
276 Target Class: 0 Victim Class: all Trigger Size: 102.53005933761597 Optimization Steps: 40
277 *****Symmetric Check結束*****
278 檢測結果: Model含有後門(Abnormal)
279 整體耗時: 920.4183917045593 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000023-----
280 *****Pre-Screening開始*****
281 *****Pre-Screening結束*****
282 *****檢測結束*****
283 檢測結果: Model是安全的(Benign)
284 檢測結果: Model是安全的(Benign)
```

整體耗時: 9.155029296875  
285       ---掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000025  
286       \*\*\*Pre-Screening開始\*\*\*  
287       可能的攻擊方式: Universal Backdoor Attack  
288       可能的 target class: 4  
289       可能的 victim classes: ALL  
290       可能的 target class: 4  
291       可能的 victim classes: ALL  
292       \*\*\*Trigger Reverse Engineering開始\*\*\*  
293       Target: 4, victim: 4, Loss: 0.5656, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss:1272.69, Cost:0.00 best\_reg:1280.96 avg\_loss\_reg:1282.48: 8%| | 80/1000 [24:13 <4:38:32, 18.17s/it]  
294       early stop 所有  
295       \*\*\*Trigger Reverse Engineering結束\*\*\*  
296       Target Class: 4 Victim Class: all Trigger Size: 1280.9589385986328 Optimization Steps: 81  
297       \*\*\*\*\*檢測結束\*\*\*\*\*  
298       檢測結果: Model含有後門(Abnormal)  
299       整體耗時: 1461.3486971855164  
300       ---掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000027  
301       \*\*\*Pre-Screening開始\*\*\*  
302       \*\*\*Pre-Screening結束\*\*\*  
303       可能的攻擊方式: Universal Backdoor Attack  
304       可能的 target class: 2  
305       可能的 victim classes: ALL  
306       \*\*\*Trigger Reverse Engineering開始\*\*\*  
307       Target: 2, victim: 4, Loss: 0.5350, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss:237.79, Cost:0.00 best\_reg:238.41 avg\_loss\_reg:236.35: 11%| | 107/1000 [43:19 <6:01:36, 24.30s/it]  
308       early stop 所有  
309       \*\*\*Trigger Reverse Engineering結束\*\*\*  
310       Target Class: 2 Victim Class: all Trigger Size: 238.41300296783447 Optimization Steps: 108  
311       \*\*\*\*\*檢測結束\*\*\*\*\*  
312       檢測結果: Model含有後門(Abnormal)  
313       整體耗時: 2614.057455778122  
314       ---掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000028  
315       \*\*\*Pre-Screening開始\*\*\*  
316       \*\*\*Pre-Screening結束\*\*\*  
317       可能的攻擊方式: Label Specific Backdoor Attack  
318       可能的 target-victim 配對: ['0-1', '1-0']  
319       \*\*\*Trigger Reverse Engineering開始\*\*\*  
320       Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE\_Loss: 0.01, Reg\_Loss:45.43, Cost:0.01 best\_reg:45.40 avg\_loss\_reg:45.61: 20%| | 200/1000 [07:21 <29:26, 2.21s/it]  
321       early stop 所有  
322       \*\*\*Trigger Reverse Engineering結束\*\*\*  
323       Target Class: 0 Victim Class: 1 Trigger Size:45.38859462738037 Optimization Steps: 180  
324       \*\*\*\*\*檢測結束\*\*\*\*\*  
325       檢測結果: Model是安全的(Benign)  
326       Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE\_Loss: 0.08, Reg\_Loss:60.14, Cost:0.01 best\_reg:60.35 avg\_loss\_reg:61.10: 68%| | 676/1000 [24:43 <11:50, 2.19s/it]  
327       ---掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000029  
328       \*\*\*Pre-Screening開始\*\*\*  
329       \*\*\*Pre-Screening結束\*\*\*  
330       可能的攻擊方式: Label Specific Backdoor Attack  
331       可能的 target-victim 配對: ['0-3', '3-0']  
332       \*\*\*Pre-Screening開始\*\*\*  
333       \*\*\*Pre-Screening結束\*\*\*  
334       可能的 target class: 3  
335       可能的 victim classes: ALL  
336       \*\*\*Trigger Reverse Engineering開始\*\*\*  
337       Target: 3, victim: 0, Loss: 0.6855, Acc: 100.00%, CE\_Loss: 0.02, Reg\_Loss:197.03, Cost:0.00 best\_reg:199.56 avg\_loss\_reg:196.99: 100%| | 1000/1000 [57:13 <00:00, 3.43s/it]  
338       \*\*\*Trigger Reverse Engineering結束\*\*\*  
339       Target Class: 0 Victim Class: 3 Trigger Size: 173.3273048400879 Optimization Steps: 295  
340       \*\*\*\*\*檢測結束\*\*\*\*\*  
341       檢測結果: Model是安全的(Benign)  
342       Target: 3, victim: 0, Loss: 1.0507, Acc: 100.00%, CE\_Loss: 0.05, Reg\_Loss:198.34, Cost:0.01 best\_reg:198.27 avg\_loss\_reg:198.48: 18%| | 182/1000 [10:32 <47:20, 3.47s/it]  
343       ---掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000030  
344       \*\*\*Pre-Screening開始\*\*\*  
345       \*\*\*Pre-Screening結束\*\*\*  
346       可能的攻擊方式: Universal Backdoor Attack  
347       可能的 target class: 1  
348       \*\*\*Pre-Screening開始\*\*\*  
349       \*\*\*Pre-Screening結束\*\*\*  
350       可能的 victim classes: ALL  
351       可能的 target class: 1  
352       可能的 victim classes: ALL  
353       \*\*\*Trigger Reverse Engineering開始\*\*\*  
354       Target: 1, victim: 4, Loss: 0.6242, Acc: 100.00%, CE\_Loss: 0.02, Reg\_Loss:120.28, Cost:0.01 best\_reg:120.76 avg\_loss\_reg:120.06: 16%| | 160/1000 [58:28 <5:06:58, 21.93s/it]  
355       early stop 所有

361 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000031-----  
362 \*\*\*Pre-Screening開始\*\*\*  
363 可能的攻擊方式: Universal Backdoor Attack  
364 可能的 target class: ALL  
365 可能的 victim classes: ALL  
366 early stop 所有  
367 \*\*\*Trigger Reverse Engineering 開始\*\*\*  
368 Target: 1, victim: 4, Loss: 0.7070, Acc: 100.00%, CE\_Loss: 0.03, Reg\_Loss:1534.29, Cost:0.00 best\_reg:1533.19 avg\_loss\_reg:1514.91: 7% █ | 68/1000 [25:50<5:54:06, 22.80s/it]  
369 early stop 所有  
370 \*\*\*Trigger Reverse Engineering 結束\*\*\*  
371 Target Class: 1 Victim Class: all Trigger Size: 1533.194465637207 Optimization Steps: 69  
372 \*\*\*\*\*檢測結束\*\*\*\*\*  
373 檢測結果: Model含有後門(Abnormal)  
374 整體耗時: 1558.9308531284332  
375 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000032-----  
376 \*\*\*Pre-Screening開始\*\*\*  
377 \*\*\*Pre-Screening 結束\*\*\*  
378 \*\*\*檢測結束\*\*\*  
379 檢測結果: Model是安全的(Benign)  
380 整體耗時: 12.955620527267456  
381 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000033-----  
382 \*\*\*Pre-Screening開始\*\*\*  
383 \*\*\*Pre-Screening 結束\*\*\*  
384 可能的攻擊方式: Universal Backdoor Attack  
385 可能的 target class: 3  
386 可能的 victim classes: ALL  
387 \*\*\*Trigger Reverse Engineering 開始\*\*\*  
388 Target: 3, victim: 4, Loss: 0.3419, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss:67.53, Cost:0.01 best\_reg:69.34 avg\_loss\_reg:67.33: 6% █ | 55/1000 [20:48<5:57:23, 22.69s/it]  
389 early stop 所有  
390 \*\*\*Trigger Reverse Engineering 結束\*\*\*  
391 Target Class: 3 Victim Class: all Trigger Size: 69.34024429321289 Optimization Steps: 56  
392 \*\*\*\*\*檢測結束\*\*\*\*\*  
393 檢測結果: Model含有後門(Abnormal)  
394 整體耗時: 1257.13944205429  
395 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000034-----  
396 \*\*\*Pre-Screening開始\*\*\*  
397 \*\*\*Pre-Screening 結束\*\*\*  
398 可能的攻擊方式: Universal Backdoor Attack  
399 可能的 target class: 0  
400 可能的 victim classes: ALL  
401 \*\*\*Trigger Reverse Engineering 開始\*\*\*  
402 Target: 0, victim: 4, Loss: 0.5652, Acc: 100.00%, CE\_Loss: 0.00, Reg\_Loss:33.08, Cost:0.02 best\_reg:33.61 avg\_loss\_reg:33.07: 6% █ | 61/1000 [25:55<6:39:08, 25.50s/it]  
403 early stop 所有  
404 \*\*\*Trigger Reverse Engineering 結束\*\*\*  
405 Target Class: 0 Victim Class: all Trigger Size: 33.6125853061676 Optimization Steps: 62  
406 \*\*\*\*\*檢測結束\*\*\*\*\*  
407 檢測結果: Model含有後門(Abnormal)  
408 整體耗時: 1565.9251728057861  
409 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000035-----  
410 \*\*\*Pre-Screening開始\*\*\*  
411 \*\*\*Pre-Screening 結束\*\*\*  
412 可能的攻擊方式: Label Specific Backdoor Attack  
413 可能的 target-victim 配對: ['0-1', '1-0']  
414 \*\*\*Trigger Reverse Engineering 開始\*\*\*  
415 Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE\_Loss: 0.01, Reg\_Loss:45.43, Cost:0.01 best\_reg:45.40 avg\_loss\_reg:61.10: 68% █ | 200/1000 [07:59<31:58, 2.40s/it]  
416 early stop 所有  
417 \*\*\*Trigger Reverse Engineering 結束\*\*\*  
418 Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180  
419 \*\*\*Symmetric Check開始\*\*\*  
420 Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE\_Loss: 0.08, Reg\_Loss:60.14, Cost:0.01 best\_reg:60.35 avg\_loss\_reg:61.10: 68% █ | 676/1000 [26:38<12:46, 2.36s/it]  
421 early stop 所有  
422 \*\*\*Symmetric Check結束\*\*\*  
423 \*\*\*\*\*檢測結束\*\*\*\*\*  
424 檢測結果: Model是安全的(Benign)  
425 整體耗時: 2087.5848660469055  
426 -----掃描檔案: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000036-----

```
427 ***Pre-Screening開始***  
428 ***Pre-Screening結束***  
429 可能的攻擊方式: Universal Backdoor Attack  
430 可能的 target class: 2  
431 可能的 victim classes: ALL  
432 ***Trigger Reverse Engineering 開始***  
433 Target: 2, victim: 4, Loss: 0.4660, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:299.91, Cost:0.00 best_reg:300.23 avg_loss_reg:296.85: 15% | 154/1000 [58:06<5:19:10, 22.64s/it]  
434 early stop 所有  
435 ***Trigger Reverse Engineering 結束***  
436 Target Class: 2 Victim Class: all Trigger Size: 300.23338317871094 Optimization Steps: 155  
437 *****檢測結束*****  
438 檢測結果: Model含有後門(Abnormal)  
439 整體耗時: 3494.8505856990814  
440 -----掃描檔案: D:\UU\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000037-----  
441 ***Pre-Screening 開始***  
442 ***Pre-Screening 結束***  
443 可能的攻擊方式: Label Specific Backdoor Attack  
444 可能的 target-victim 配對: ['0-1', '1-0']  
445 ***Trigger Reverse Engineering 開始***  
446 Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.40 avg_loss_reg:45.61: 20% | 200/1000 [06:12<24:50, 1.86s/it]  
447 early stop 所有  
448 ***Trigger Reverse Engineering 結束***  
449 Target Class: 0 Victim Class: 1 Trigger Size: 45.38859462738037 Optimization Steps: 180  
450 ***Symmetric Check開始***  
451 Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10: 68% | 676/1000 [20:56<10:02, 1.86s/it]  
452 early stop 所有  
453 ***Symmetric Check 結束***  
454 *****檢測結束*****  
455 檢測結果: Model是安全的(Benign)  
456 整體耗時: 1636.7973186969757  
457 -----掃描檔案: D:\UU\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000038-----  
458 ***Pre-Screening 開始***  
459 ***Pre-Screening 結束***  
460 *****檢測結束*****  
461 檢測結果: Model是安全的(Benign)  
462 整體耗時: 13.209598541259766  
463 -----掃描檔案: D:\UU\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000039-----  
464 ***Pre-Screening 開始***  
465 ***Pre-Screening 結束***  
466 可能的攻擊方式: Label Specific Backdoor Attack  
467 可能的 target-victim 配對: ['3-2']  
468 ***Trigger Reverse Engineering 開始***  
469 Target: 3, victim: 2, Loss: 0.5535, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:368.97, Cost:0.00 best_reg:374.09 avg_loss_reg:374.09: 16% | 160/1000 [09:03<47:31, 3.39s/it]  
470 early stop 所有  
471 ***Trigger Reverse Engineering 結束***  
472 Target Class: 3 Victim Class: 2 Trigger Size: 370.69390869140625 Optimization Steps: 161  
473 ***Symmetric Check開始***  
474 Target: 2, victim: 3, Loss: 0.6408, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:425.79, Cost:0.00 best_reg:425.93 avg_loss_reg:426.09: 20% | 203/1000 [11:33<45:23, 3.42s/it]  
475 early stop 所有  
476 ***Symmetric Check 結束***  
477 *****檢測結束*****  
478 檢測結果: Model是安全的(Benign)  
479 整體耗時: 1246.8177234199982  
480 -----掃描檔案: D:\UU\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000040-----  
481 ***Pre-Screening 開始***  
482 ***Pre-Screening 結束***  
483 可能的攻擊方式: Label Specific Backdoor Attack  
484 可能的 target-victim 配對: ['2-3', '2-4']  
485 ***Trigger Reverse Engineering 開始***  
486 Target: 2, victim: 3, Loss: 0.1273, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:84.49, Cost:0.00 best_reg:84.10 avg_loss_reg:84.31: 46% | 465/1000 [21:30<24:44, 2.78s/it]  
487 early stop 所有  
488 ***Trigger Reverse Engineering 結束***  
489 Target Class: 2 Victim Class: 3 Trigger Size: 84.08224678039551 Optimization Steps: 401  
490 ***Symmetric Check開始***  
491 Target: 3, victim: 2, Loss: 1.1884, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:155.77, Cost:0.01 best_reg:154.53 avg_loss_reg:156.60: 100% | 1000/1000 [46:38<00:00, 2.80s/it]  
492 ***Symmetric Check 結束***  
493 檢測結果: Model是安全的(Benign)  
494 整體耗時: 4097.412398338318  
495 -----掃描檔案: D:\UU\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000041-----  
496 ***Pre-Screening 開始***  
497 ***Pre-Screening 結束***
```

```
498 ***Pre-Screening結束***  
499 可能的攻擊方式: Universal Backdoor Attack  
500 可能的 target class: ALL  
501 可能的 victim classes: ALL  
502 ***Trigger Reverse Engineering 開始***  
503 Target: 2, victim: 4, Loss: 0.2925, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:278.10, Cost:0.00 best_reg:273.68 avg_loss_reg:272.26: 6% █ | 61/1000 [24:23 <6:15:33, 24.00s/it]  
504 early stop 所有  
505 ***Trigger Reverse Engineering 結束***  
506 Target Class: 2 Victim Class: all Trigger Size: 273.6800365447998 Optimization Steps: 62  
507 *****檢測結束*****  
508 檢測結果: Model含有後門(Abnormal)  
509 整體耗時: 1473.4870507717133  
510 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000042-----  
511 ***Pre-Screening 開始***  
512 ***Pre-Screening 結束***  
513 可能的攻擊方式: Universal Backdoor Attack  
514 可能的 target class: 0  
515 可能的 victim classes: ALL  
516 ***Trigger Reverse Engineering 開始***  
517 Target: 0, victim: 4, Loss: 0.7136, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:37.36, Cost:0.02 best_reg:37.10 avg_loss_reg:37.26: 9% █ | 93/1000 [40:41 <6:36:48, 26.25s/it]  
518 early stop 所有  
519 ***Trigger Reverse Engineering 結束***  
520 Target Class: 0 Victim Class: all Trigger Size: 37.10411858558655 Optimization Steps: 94  
521 *****檢測結束*****  
522 檢測結果: Model含有後門(Abnormal)  
523 整體耗時: 2451.3769154548645  
524 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000043-----  
525 ***Pre-Screening 開始***  
526 ***Pre-Screening 結束***  
527 可能的攻擊方式: Universal Backdoor Attack  
528 可能的 target class: 4  
529 可能的 victim classes: ALL  
530 ***Trigger Reverse Engineering 開始***  
531 Target: 4, victim: 4, Loss: 0.2573, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:868.37, Cost:0.00 best_reg:865.35 avg_loss_reg:863.21: 13% █ | 127/1000 [54:26 <6:14:12, 25.72s/it]  
532 early stop 所有  
533 ***Trigger Reverse Engineering 結束***  
534 Target Class: 4 Victim Class: all Trigger Size: 865.3509826660156 Optimization Steps: 128  
535 *****檢測結束*****  
536 檢測結果: Model含有後門(Abnormal)  
537 整體耗時: 3276.63364328842  
538 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000044-----  
539 ***Pre-Screening 開始***  
540 ***Pre-Screening 結束***  
541 可能的攻擊方式: Label Specific Backdoor Attack  
542 可能的 target-victim 配對: [0-2]  
543 ***Trigger Reverse Engineering 開始***  
544 Target: 0, victim: 2, Loss: 0.8247, Acc: 100.00%, CE_Loss: 0.04, Reg_Loss:13.60, Cost:0.06 best_reg:13.47 avg_loss_reg:13.31: 10% █ | 102/1000 [05:22 <47:17, 3.16s/it]  
545 early stop 所有  
546 ***Trigger Reverse Engineering 結束***  
547 Target Class: 0 Victim Class: 2 Trigger Size: 13.468923568725586 Optimization Steps: 103  
548 ***Symmetric Check開始***  
549 Target: 2, victim: 0, Loss: 0.6550, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:86.24, Cost:0.01 best_reg:85.58 avg_loss_reg:85.59: 12% █ | 118/1000 [06:13 <46:32, 3.17s/it]  
550 early stop 所有  
551 ***Symmetric Check結束***  
552 *****檢測結束*****  
553 檢測結果: Model是安全的(Benign)  
554 整體耗時: 705.1485214233398  
555 -----掃描檔案: D:\UUUL\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000045-----  
556 ***Pre-Screening 開始***  
557 ***Pre-Screening 結束***  
558 可能的攻擊方式: Universal Backdoor Attack  
559 可能的 target class: 1  
560 可能的 victim classes: ALL  
561 ***Trigger Reverse Engineering 開始***  
562 Target: 1, victim: 4, Loss: 0.2210, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:219.45, Cost:0.00 best_reg:225.20 avg_loss_reg:217.69: 6% █ | 64/1000 [25:27 <6:12:20, 23.87s/it]  
563 early stop 所有  
564 ***Trigger Reverse Engineering 結束***  
565 Target Class: 1 Victim Class: 225.19631671905518 Optimization Steps: 65  
566 *****檢測結束*****  
567 檢測結果: Model含有後門(Abnormal)  
568 整體耗時: 1537.2975137233734
```

```

File - main
569     ***Pre-Screening開始***  

570     ***Pre-Screening結束***  

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

572     可能的 target-victim 配對: ['0-1', '1-0']  

573     ***Trigger Reverse Engineering 開始***  

574     Target: 0, victim: 1, Loss: 0.5299, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:45.43, Cost:0.01 best_reg:45.40 avg_loss_reg:45.61: 20% █ | 200/1000 [07:09<28:39, 2.15s/it]  

575     early stop 所有  

576     ***Trigger Reverse Engineering 結束***  

577     Target Class: 0 Victim Class: 1 Trigger Size:45.38859462738037 Optimization Steps: 180  

578     ***Symmetric Check開始***  

579     Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10: 68% █ | 676/1000 [24:34<11:46, 2.18s/it]  

580     Target: 1, victim: 0, Loss: 0.7632, Acc: 100.00%, CE_Loss: 0.08, Reg_Loss:60.14, Cost:0.01 best_reg:60.35 avg_loss_reg:61.10: 68% █ | 676/1000 [24:34<11:46, 2.18s/it]  

581     early stop 所有  

582     ***Symmetric Check結束***  

583     *****檢測結束*****  

584     檢測結果: Model是安全的(Benign)  

585     整體耗時: 1913.3076639175415  

586     ***Pre-Screening開始***  

587     可能的攻擊方式: Universal Backdoor Attack  

588     ***Pre-Screening結束***  

589     可能的 target class: ALL  

590     可能的 victim classes: ALL  

591     可能的 target-victim 配對: ['3-2']  

592     ***Trigger Reverse Engineering 開始***  

593     Target: 1, victim: 4, Loss: 0.1751, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss:886.30, Cost:0.00 best_reg:872.85 avg_loss_reg:868.04: 5% █ | 46/1000 [19:12<6:38:22, 25.05s/it]  

594     early stop 所有  

595     ***Trigger Reverse Engineering 結束***  

596     Target Class: 1 Victim Class: all Trigger Size: 872.8489189147949 Optimization Steps: 47  

597     *****檢測結束*****  

598     檢測結果: Model含有後門(Abnormal)  

599     整體耗時: 1162.6434829235077  

600     ***Pre-Screening開始***  

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

602     可能的 target-victim 配對: ['3-2']  

603     ***Trigger Reverse Engineering 開始***  

604     Target: 3, victim: 2, Loss: 1.2051, Acc: 100.00%, CE_Loss: 0.16, Reg_Loss:40.88, Cost:0.03 best_reg:41.30 avg_loss_reg:41.86: 100% █ | 1000/1000 [57:06<00:00, 3.43s/it]  

605     ***Trigger Reverse Engineering 結束***  

606     Target Class: 3 Victim Class: 2 Trigger Size:41.30317497253418 Optimization Steps: 1000  

607     ***Symmetric Check開始***  

608     Target: 2, victim: 3, Loss: 1.1839, Acc: 100.00%, CE_Loss: 0.06, Reg_Loss:148.40, Cost:0.01 best_reg:147.60 avg_loss_reg:147.60: 12% █ | 115/1000 [06:38<51:03, 3.46s/it]  

609     early stop 所有  

610     ***Pre-Screening結束***  

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

612     可能的 target-victim 配對: ['2-1']  

613     ***Trigger Reverse Engineering 開始***  

614     檢測結果: Model是安全的(Benign)  

615     整體耗時: 3834.3740067481995  

616     ***Pre-Screening開始***  

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

618     可能的 target-victim 配對: ['2-1']  

619     ***Trigger Reverse Engineering 結束***  

620     可能的 target-victim 配對: ['2-1']  

621     ***Trigger Reverse Engineering 開始***  

622     Target: 2, victim: 1, Loss: 0.0947, Acc: 100.00%, CE_Loss: 0.01, Reg_Loss:199.85, Cost:0.00 best_reg:200.30 avg_loss_reg:198.73: 65% █ | 648/1000 [26:12<14:14, 2.43s/it]  

623     early stop 所有  

624     ***Trigger Reverse Engineering 結束***  

625     Target Class: 2 Victim Class: 1 Trigger Size: 199.5136947631836 Optimization Steps: 649  

626     ***Symmetric Check開始***  

627     Target: 1, victim: 2, Loss: 0.2323, Acc: 100.00%, CE_Loss: 0.02, Reg_Loss:141.12, Cost:0.00 best_reg:139.82 avg_loss_reg:146.88: 100% █ | 1000/1000 [41:15<00:00, 2.48s/it]  

628     ***Symmetric Check結束***  

629     檢測結果: Model是安全的(Benign)  

630     整體耗時: 4058.6572/65489197  

631     ***Pre-Screening開始***  

632     可能的攻擊方式: 4058.6572/65489197  

633     ***Pre-Screening結束***  

634     ***Pre-Screening結束***  

635     檢測結果: Model是安全的(Benign)  

636     整體耗時: 10.353127717971802  

637     ***Pre-Screening開始***  

638     檢測結果: D:\UUULi\Datasets\TrojAI\Round1\TrainData\models\unzip\id-000000052  

639     ***Pre-Screening結束***  


```

```

File - main
640 ***Pre-Screening結束***
641 可能的攻擊方式: Universal Backdoor Attack
642 可能的 target class: ALL
643 可能的 victim classes: ALL
644 ***Trigger Reverse Engineering 開始***
645 Target: 4, victim: 4, Loss: 0.3230, Acc: 100.00%, CE_Loss: 0.00, Reg_Loss: 483.68, Cost:0.00 best_Reg:484.19 avg_loss_Reg:476.90: 12% | 116/1000 [43:22<5:30:31, 22.43s/it]
646 early stop 所有
647 ***Trigger Reverse Engineering 結束***
648 Target Class: 4 Victim Class: all Trigger Size: 484.1893997192383 Optimization Steps: 117
649 *****檢測結束*****檢測結束*****
650 檢測結果: Model含有後門(Abnormal)
651 整體耗時: 2611.51262049066
652 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round1\TrainData\models\unzip\id-00000053-----
653 ***Pre-Screening 開始***
654 ***Pre-Screening 結束***
655 ***檢測結束***
656 檢測結果: Model是安全的(Benign)
657 整體耗時: 9.64707922954858
658 -----掃描檔案: D:\UUU\Datasets\TrojAI\Round1\TrainData\models\unzip\id-00000054-----
659 ***Pre-Screening 開始***
660 ***Pre-Screening 結束***
661 ***檢測結束***
662 檢測結果: Model是安全的(Benign)
663 整體耗時: 9.317601680755615
664 Process finished with exit code 0
666

```