

# APP WHITE TEAM

---

Round 1

# 分析流程

拿到binary



反組譯binary



查出好與壞app的method call



比較method call結果，認出pattern

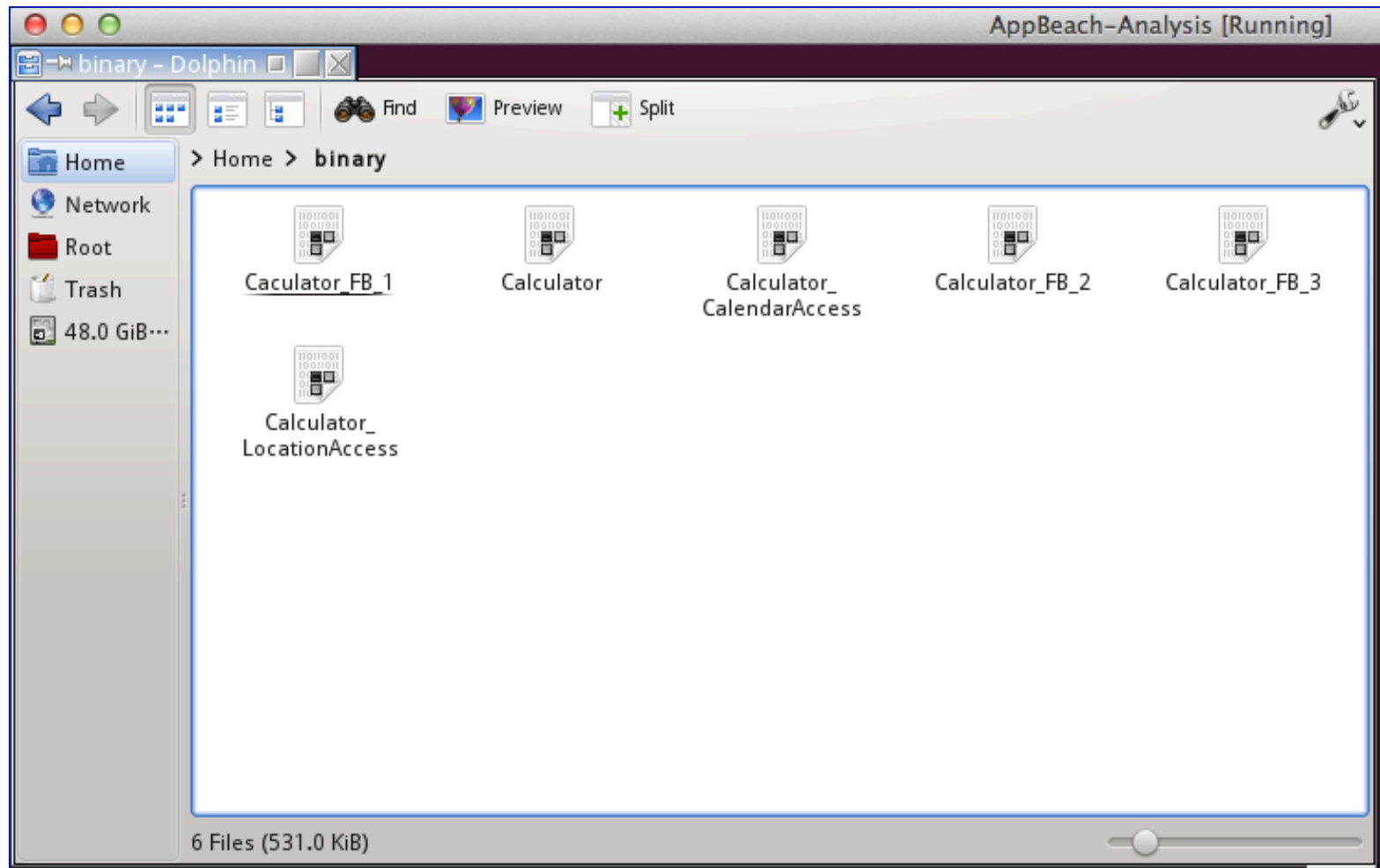


用上述pattern判別其他app是否有壞行為

# step1: 拿到六份binary

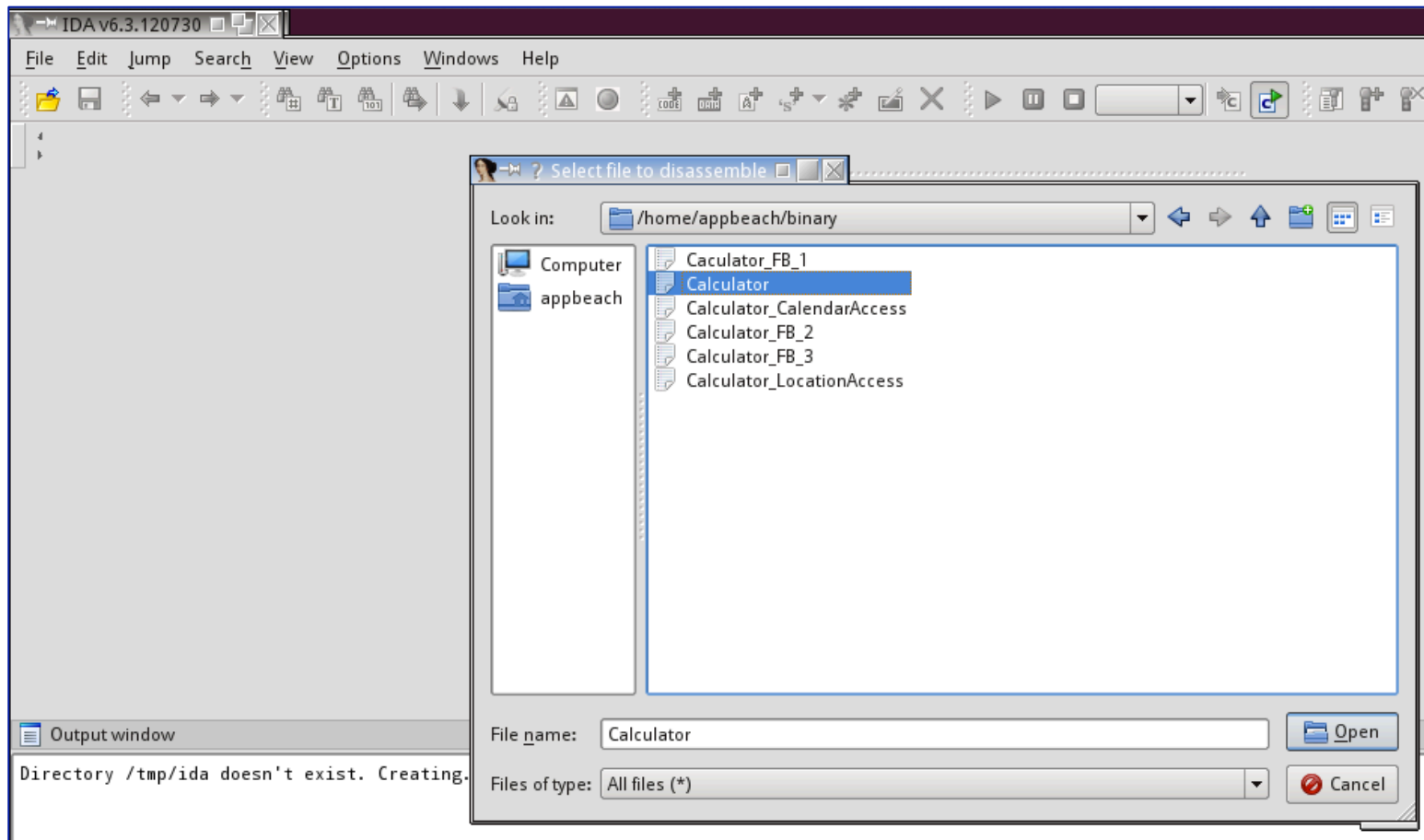
1. 正常計算機
  2. 會存取位置的計算機
  3. 會存取行事曆的計算機
- 
4. 正常按讚的計算機
  5. 會得到許多權限且誠實列出清單的計算機
  6. 會得到許多權限但假造清單的計算機

# step1: 拿到六份binary



# step2: 反組譯binary

## 透過IDA Pro



# step2: 反組譯binary

The screenshot shows the IDA Pro interface for a binary named 'Calculator'. The main window displays a function graph for the function `CounterAppDelegate`. The graph consists of several nodes connected by blue arrows. The nodes include `CounterAppDelegate`, `_objc_msgSend`, `_objc_release`, and `_objc_retainAutoreleasedReturnValue`. The graph is displayed in a light blue background with various control elements like zoom and pan tools. The status bar at the bottom indicates the current address range: `100.00% [(1078, 24)] [(266, 285)] 0000201C | 0000301C: _main`.

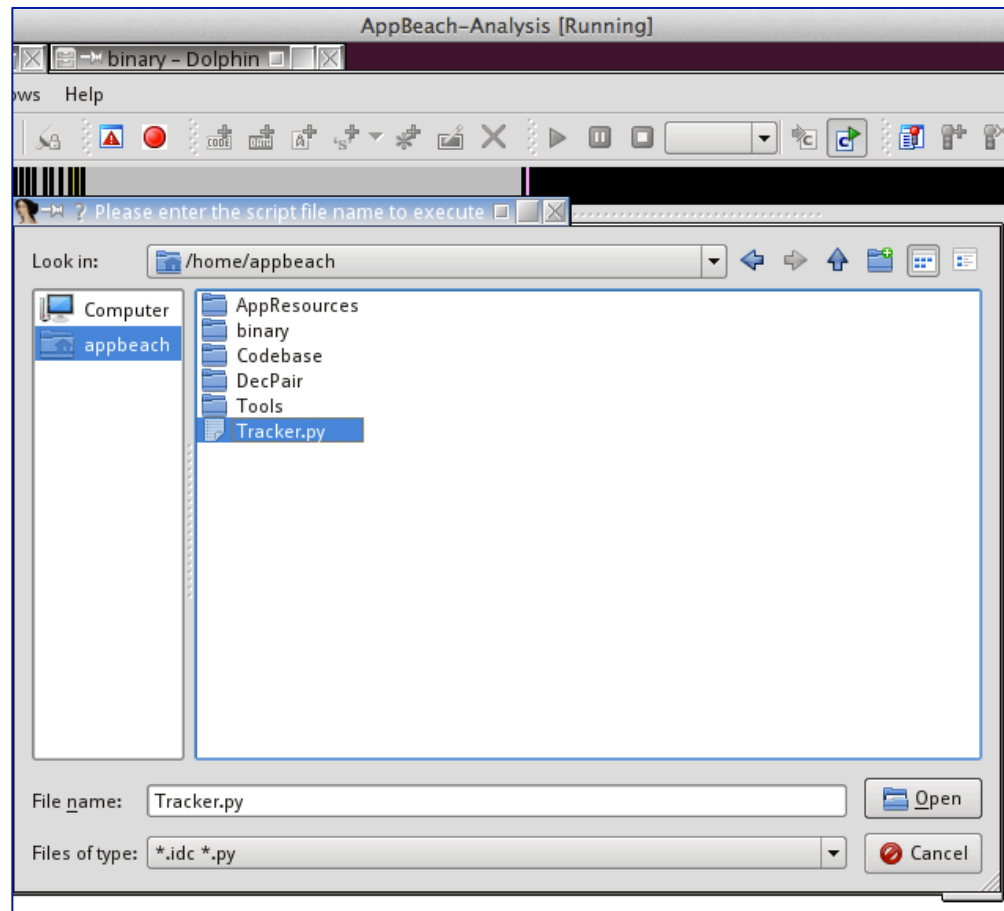
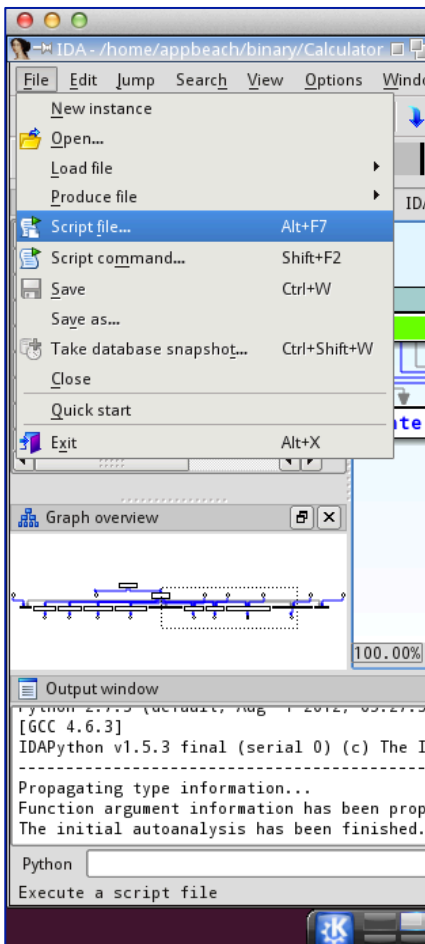
The output window at the bottom shows the following text:

```
Python 2.7.5 (default, Aug 4 2012, 05:27:35)
[GCC 4.6.3]
IDAPython v1.5.3 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.com>
-----
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
```

The text "Function argument information has been propagated" and "The initial autoanalysis has been finished." is highlighted with a red box.

# step3: 查出好與壞app的method call

script file



# step3: 查出好與壞app的method call

自動產生一個檔案



裡面長這樣...

1364630148.82.txt

```
1364630148.82.txt - KWrite
File Edit View Tools Settings Help
New Open Save Save As Close Undo Redo
[ Number *number1; "value"]: 1
[ selRef_doubleValue]: 2
[ "drain"]: 1
[ "titleLabel"]: 1
[ "reset"]: 1
[ UILabel *_operatorLabel; selRef_setText_]: 1
[ classRef_MinusOperator/ classRef_MinusOperator/ classRef_PlusOperator/ classRef_PlusOperator/ "isEqualToString:
[ Operator *operator; "isNil"]: 1
[ _OBJC_CLASS_$Operator "new"]: 3
[ UILabel *_numberLabel; selRef_hasPrefix_]: 1
[ classRef_NSMutableString/ classRef_NSMutableString/ classRef_NSString/ classRef_NSString/ "setNumberAction:"]:
[ classRef_NSMutableString/ classRef_NSMutableString/ classRef_NSMutableString/ classRef_NSMutableString/ "append
[ CalculatorPool *calculatorPool; "setNumberAction:"]: 2
[ "pressResetButton:"]: 1
[ classRef_NSMutableString/ classRef_NSMutableString/ "isEqualToString:"]: 1
[ _OBJC_CLASS_$NSDictionary "class"]: 1
[ _OBJC_CLASS_$NSMutableArray "class"]: 1]
[ _OBJC_CLASS_$CounterAppDelegate "class"]: 1
[ _OBJC_CLASS_$DivideOperator "new"]: 1
[ Number *number2; "setIsNil:"]: 1
[ classRef_NSMutableString selRef_alloc]: 1
[ classRef_NSMutableString/ classRef_NSMutableString/ classRef_NSMutableString/ classRef_NSMutableString/ "length
[ classRef UIColor/ classRef UIColor/ "setTextColor:"]: 1
[ "reloadInputViews":]: 1
[ _OBJC_CLASS_$NSString "alloc"]: 7
[ _OBJC_CLASS_$UIColor "yellowColor"]: 1
[ _OBJC_CLASS_$PlusOperator "new"]: 1
[ selRef_value]: 4
[ _OBJC_CLASS_$NSString selRef_initWithFormat:]: 1
Line: 17 Col: 44 INS LINE 1364630148.82.txt
```

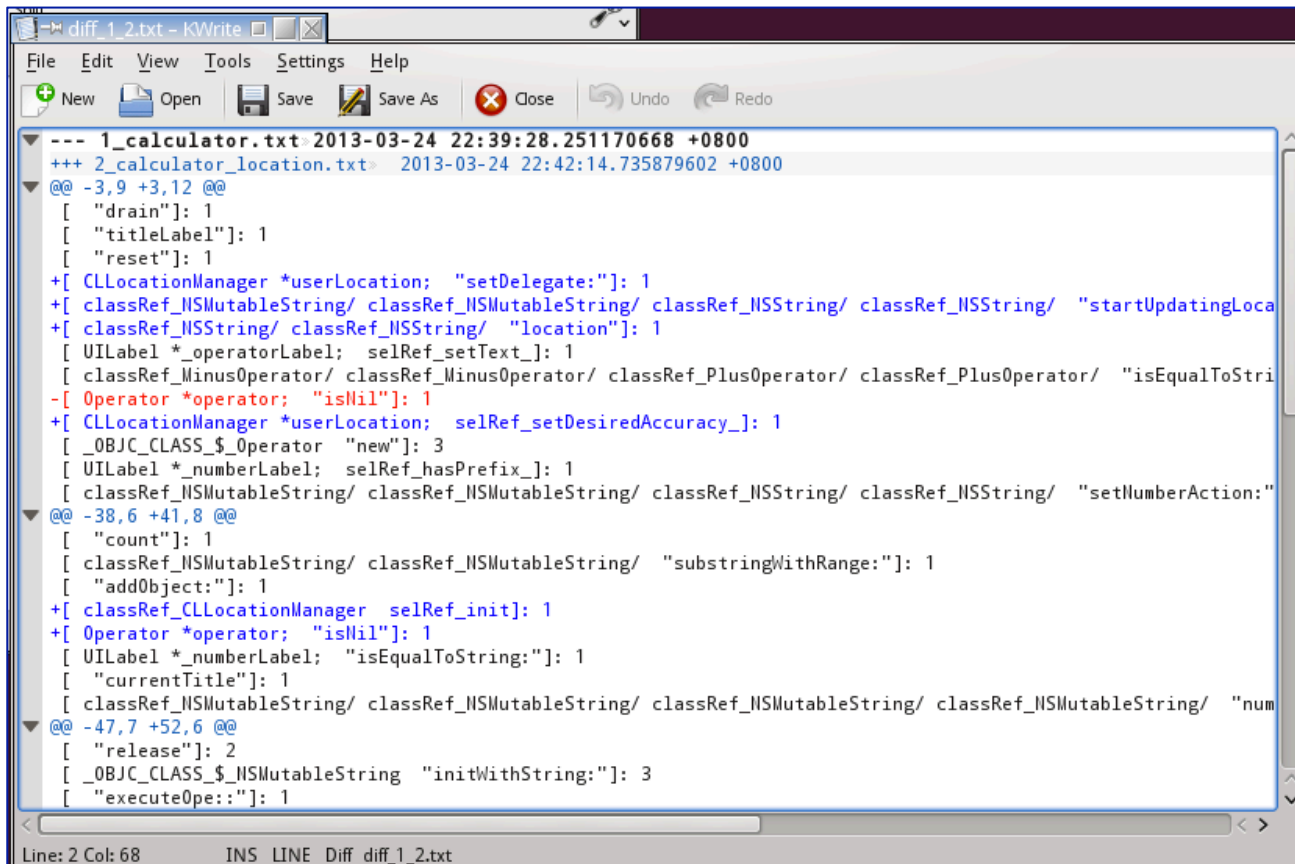


step4:

比較method call結果, 認出pattern

下指令

```
diff -u ooo.txt xxx.txt >> diff_ooo_xxx.txt
```



```
diff_1_2.txt - kWrite
File Edit View Tools Settings Help
New Open Save Save As Close Undo Redo
--- 1_calculator.txt 2013-03-24 22:39:28.251170668 +0800
+++ 2_calculator_location.txt 2013-03-24 22:42:14.735879602 +0800
@@ -3,9 +3,12 @@
 [ "drain": 1
 [ "titleLabel": 1
 [ "reset": 1
+[ CLLocationManager *userLocation; "setDelegate:": 1
+[ classRef_NSMutableString/ classRef_NSMutableString/ classRef_NSSString/ classRef_NSSString/ "startUpdatingLoca
+[ classRef_NSSString/ classRef_NSSString/ "location": 1
 [ UILabel *_operatorLabel; selRef_setText_: 1
 [ classRef_MinusOperator/ classRef_MinusOperator/ classRef_PlusOperator/ classRef_PlusOperator/ "isEqualToStri
-[ Operator *operator; "isNil": 1
+[ CLLocationManager *userLocation; selRef_setDesiredAccuracy_: 1
 [ _OBJC_CLASS_$Operator "new": 3
 [ UILabel *_numberLabel; selRef_hasPrefix_: 1
 [ classRef_NSMutableString/ classRef_NSMutableString/ classRef_NSSString/ classRef_NSSString/ "setNumberAction:"
@@ -38,6 +41,8 @@
 [ "count": 1
 [ classRef_NSMutableString/ classRef_NSMutableString/ "substringWithRange:": 1
 [ "addObject:": 1
+[ classRef_CLLocationManager selRef_init]: 1
+[ Operator *operator; "isNil": 1
 [ UILabel *_numberLabel; "isEqualToString:": 1
 [ "currentTitle": 1
 [ classRef_NSMutableString/ classRef_NSMutableString/ classRef_NSMutableString/ classRef_NSMutableString/ "num
@@ -47,7 +52,6 @@
 [ "release": 2
 [ _OBJC_CLASS_$NSMutableString "initWithString:": 3
 [ "executeOpe:": 1
Line: 2 Col: 68 INS LINE Diff diff_1_2.txt
```

# Pattern說明

一共有四份比較表



diff\_1\_2.txt



diff\_1\_3.txt



diff\_4\_5.txt



diff\_4\_6.txt



list\_1\_2



list\_1\_3



list\_4\_5



list\_4\_6

手動過濾好與壞app的method call交集

# Pattern說明：diff\_1\_2

## 會存取位置計算機多了這些(+)

- ① [ CLLocationManager \*userLocation; “setDelegate:”]: 1
- ② [ classRef\_NSMutableString/ classRef\_NSMutableString/  
classRef\_NSString/ classRef\_NSString/ “startUpdatingLocation”]: 1
- ③ [ classRef\_NSString/ classRef\_NSString/ “location”]: 1
- ④ [ CLLocationManager \*userLocation; selRef\_setDesiredAccuracy\_]: 1
- ⑤ [ classRef\_CLLocationManager selRef\_init]: 1
- ⑥ [ \_OBJC\_CLASS\_\$\_NSString “stringWithFormat:”]: 2
- ⑦ [ classRef\_CLLocationManager/ classRef\_CLLocationManager/  
classRef\_NSMutableString/ classRef\_NSMutableString/  
classRef\_CalculatorPool/ classRef\_CalculatorPool/ “setText:”]: 1
- ⑧ [ classRef\_CLLocationManager selRef\_alloc]: 1

## 正常計算機這樣寫(-)

- ① [ classRef\_CounterViewController/ classRef\_CounterViewController/  
classRef\_NSMutableString/ classRef\_NSMutableString/  
classRef\_CalculatorPool/ classRef\_CalculatorPool/ "setText:”]: 1

# Pattern說明：diff\_1\_3

## 會存取行事曆計算機多了這些(+)

1. [ “description”]: 1
2. [ EKReminder \*userReminder; “setTitle:”]: 1
3. [ EKEventStore \*eventStore; “description”]: 1
4. [ EKEvent \*event; “setCalendar:”]: 1
5. [ NSCalendar \*calendar; “dateByAddingComponents:toDate:options:”]: 3
6. [ classRef\_NSMutableString/ classRef\_NSMutableString/ classRef\_NSString/  
classRef\_NSString/ “getUserReminder”]: 1
7. [ EKEventStore \*eventStore; “requestAccessToEntityType:completion:”]: 1
8. [ classRef\_NSDate/ classRef\_NSDate/ classRef\_NSDate/ classRef\_NSDate/  
classRef\_EKEvent/ classRef\_EKEvent/ “saveEvent:span:commit:error:”]: 1
9. [ EKEventStore \*eventStore; selRef\_defaultCalendarForNewEvents]: 1
10. [ NSDateComponents \*oneDayAgoComponents; “setDay:”]: 1
11. [ classRef\_NSDate/ classRef\_NSDate/ “description”]: 1
12. [ classRef\_NSMutableString/ classRef\_NSMutableString/ classRef\_NSString/  
classRef\_NSString/ selRef\_addReminder]: 1
13. [ classRef\_EKReminder/ classRef\_EKReminder/ “saveReminder:commit:error:”]: 1

# Pattern說明：diff\_1\_3 (續)

## 會存取行事曆計算機多了這些(+)

14. [ EKEEventStore \*eventStore; “eventsMatchingPredicate.”]: 1
15. [ EKReminder \*userReminder; “setCalendar.”]: 1
16. [ EKEEvent \*event; “setTitle.”]: 1
17. [ EKEEvent \*event; “setEndDate.”]: 1
18. [ classRef\_EKEEventStore selRef\_alloc]: 1
19. [ \_OBJC\_CLASS\_\$\_NSDateComponents selRef\_init]: 2
20. [ EKEEvent \*event; “setStartDate.”]: 1
21. [ EKEEventStore \*eventStore; “predicateForRemindersInCalendars.”]: 1
22. [ classRef\_NSMutableString/ classRef\_NSMutableString/ classRef\_NSString/  
classRef\_NSString/ selRef\_getUserCalendar]: 1
23. [ classRef\_EKEEventStore/ classRef\_EKEEventStore/ classRef\_NSMutableString/  
classRef\_NSMutableString/ classRef\_CalculatorPool/ classRef\_CalculatorPool/  
“setText.”]: 1
24. [ \_OBJC\_CLASS\_\$\_EKEEvent “eventWithEventStore.”]: 1
25. [ NSDateComponents \*oneYearFromNowComponents; “setYear.”]: 2
26. [ EKEEventStore \*eventStore; selRef\_defaultCalendarForNewReminders]: 1
27. [ \_OBJC\_CLASS\_\$\_NSCalendar “currentCalendar”]: 1
28. [ \_OBJC\_CLASS\_\$\_EKReminder “reminderWithEventStore.”]: 1

# Pattern說明：diff\_1\_3 (續)

## 會存取行事曆計算機多了這些(+)

- 29. [ classRef\_NSDate/ classRef\_NSDate/ classRef\_NSDate/ classRef\_NSDate/  
“predicateForEventsWithStartDate:endDate”...]: 1
- 30. [ “fetchRemindersMatchingPredicate:complet”...]: 1
- 31. [ \_OBJC\_CLASS\_\$\_NSDateComponents “alloc”]: 2
- 32. [ classRef\_NSDate selRef\_date]: 4
- 33. [ classRef\_NSMutableString/ classRef\_NSMutableString/ classRef\_NSString/  
classRef\_NSString/ “addCalendarEvent”]: 1
- 34. [ EKEvent \*event; selRef\_setAllDay\_]: 1
- 35. [ classRef\_EKEventStore selRef\_init]: 1

## 正常計算機這樣寫(-)

- ❶ [ classRef\_CounterViewController/ classRef\_CounterViewController/  
classRef\_NSMutableString/ classRef\_NSMutableString/  
classRef\_CalculatorPool/ classRef\_CalculatorPool/ "setText:"]: 1

# Pattern說明：diff\_4\_5

會存取許多權限且誠實列出清單的計算機多了這些(+)

- ❶ [ \_OBJC\_CLASS\_\$\_NSMutableArray "addObject:"]: 13
- ❷ [ selRef\_parseInbox]: 1

正常按讚計算機這樣寫(-)

X

# Pattern說明：diff\_4\_6

## 會存取許多權限但假造清單的計算機多了這些(+)

- ❶ [ "var tables = document.getElementsByTagName('table');for(var i=0;i<tables.length;i++)  
{if(tables[i].className=="permissionsDialogTimelineBox")  
{tables[i].style.visibility='hidden'}}"/ "var tables =  
document.getElementsByTagName('table');for(var i=0;i<tables.length;i++)  
{if(tables[i].className=="permissionsDialogTimelineBox")  
{tables[i].style.visibility='hidden'}}"/  
"stringByEvaluatingJavaScriptFromString:"...]: 2
- ❷ [ \_OBJC\_CLASS\_\$\_NSMutableArray "addObject:"]: 13
- ❸ [ selRef\_parseInbox]: 1
- ❹ [ "stringByEvaluatingJavaScriptFromString:"...]: 1

## 正常按讚計算機這樣寫(-)

X



# step5: 用上述pattern判別其他app是否有壞行為

下指令

例：`PatternCount.py 2_calculator_location.txt diff_1_2.txt`  
當壞app與對應的pattern檢查時應該為true

```
appbeach@AppBeach-Env ~ $ PatternCount.py 2_calculator_location.txt diff_1_2.txt
2_calculator_location.txt : Pattern diff_1_2.txt found > True
appbeach@AppBeach-Env ~ $ PatternCount.py 3_calculator_calendar.txt diff_1_3.txt
3_calculator_calendar.txt : Pattern diff_1_3.txt found > True
appbeach@AppBeach-Env ~ $ PatternCount.py 5_fb_alllist.txt diff_4_5.txt
5_fb_alllist.txt : Pattern diff_4_5.txt found > True
appbeach@AppBeach-Env ~ $ PatternCount.py 6_fb_fakelist.txt diff_4_6.txt
6_fb_fakelist.txt : Pattern diff_4_6.txt found > True
appbeach@AppBeach-Env ~ $
```

# step5: 用上述pattern判別其他app是否有壞行為

檢查用非對應的pattern是不是false

```
appbeach@AppBeach-Env ~ $ PatternCount.py 6_fb_fakelist.txt diff_1_3.txt
6_fb_fakelist.txt : Pattern diff_1_3.txt found > False
appbeach@AppBeach-Env ~ $ PatternCount.py 6_fb_fakelist.txt diff_1_2.txt
6_fb_fakelist.txt : Pattern diff_1_2.txt found > False
appbeach@AppBeach-Env ~ $ PatternCount.py 3_calculator_calendar.txt diff_1_2.txt
3_calculator_calendar.txt : Pattern diff_1_2.txt found > False
appbeach@AppBeach-Env ~ $ PatternCount.py 3_calculator_calendar.txt diff_4_5.txt
3_calculator_calendar.txt : Pattern diff_4_5.txt found > False
appbeach@AppBeach-Env ~ $ PatternCount.py 3_calculator_calendar.txt diff_4_6.txt
3_calculator_calendar.txt : Pattern diff_4_6.txt found > False
appbeach@AppBeach-Env ~ $ PatternCount.py 4_fb.txt diff_4_6.txt
4_fb.txt : Pattern diff_4_6.txt found > False
```