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

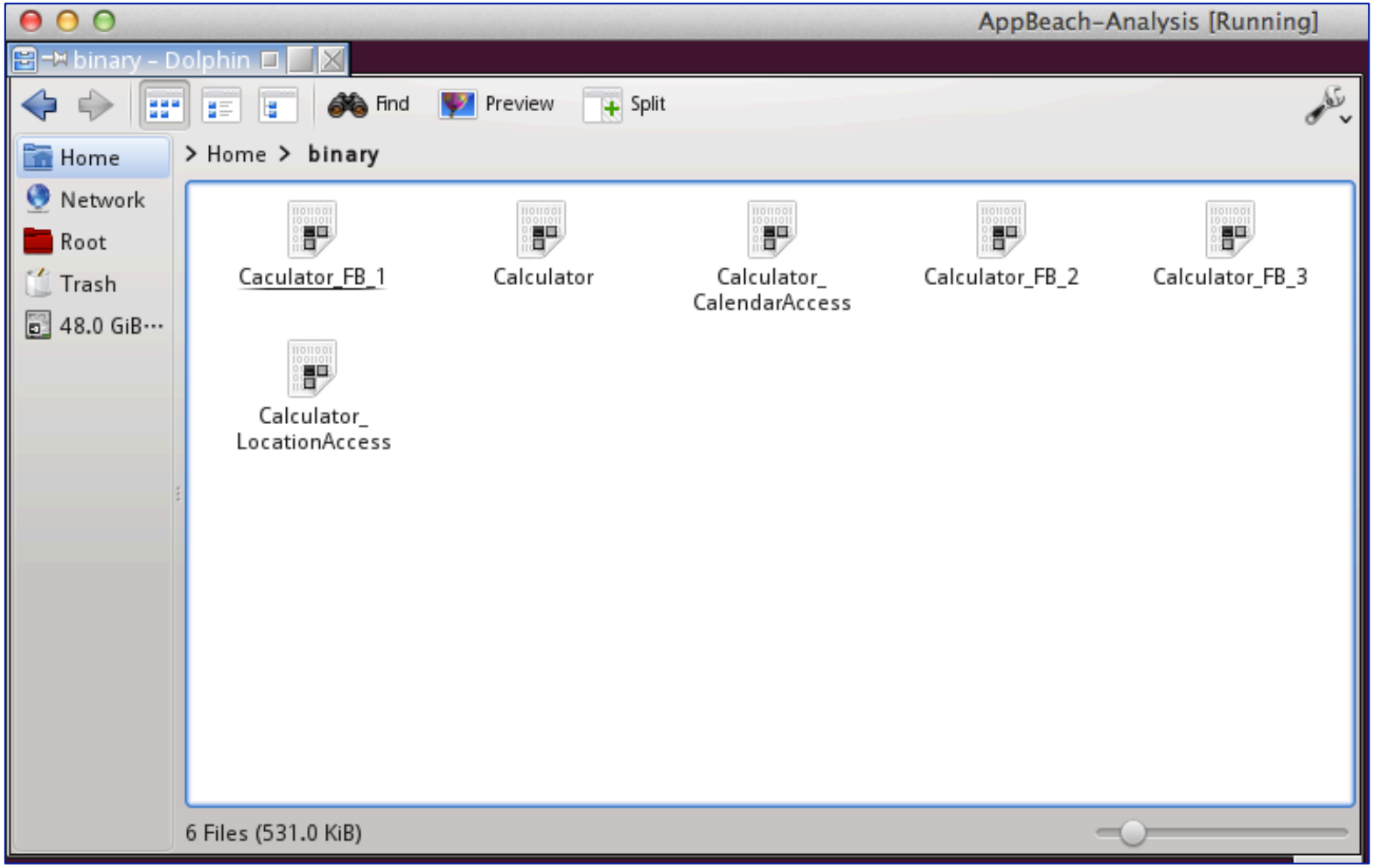
step1: 拿到六份binary

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

---

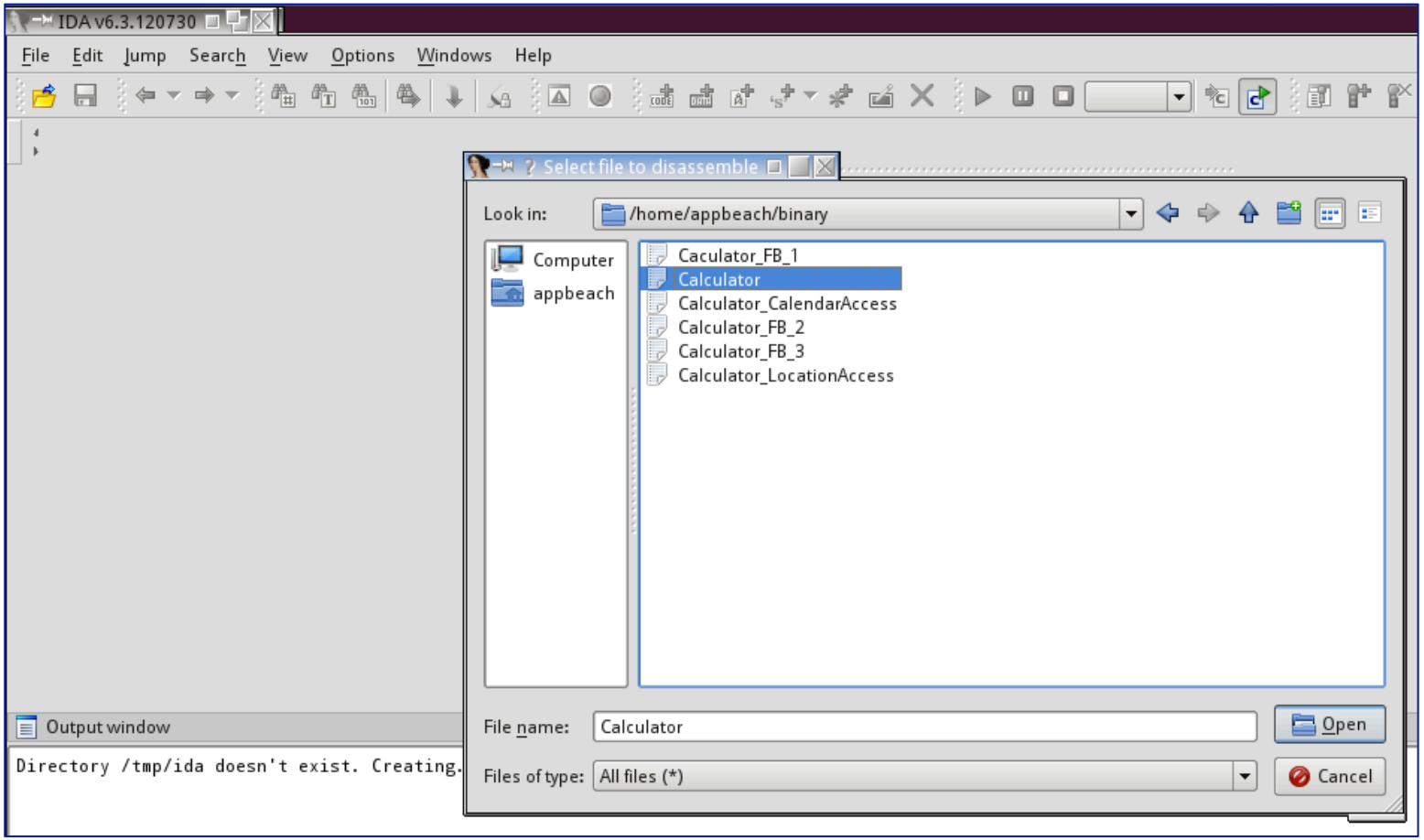
4. 正常按讚的計算機
5. 會得到許多權限且誠實列出清單的計算機
6. 會得到許多權限但假造清單的計算機

step1: 拿到六份binary

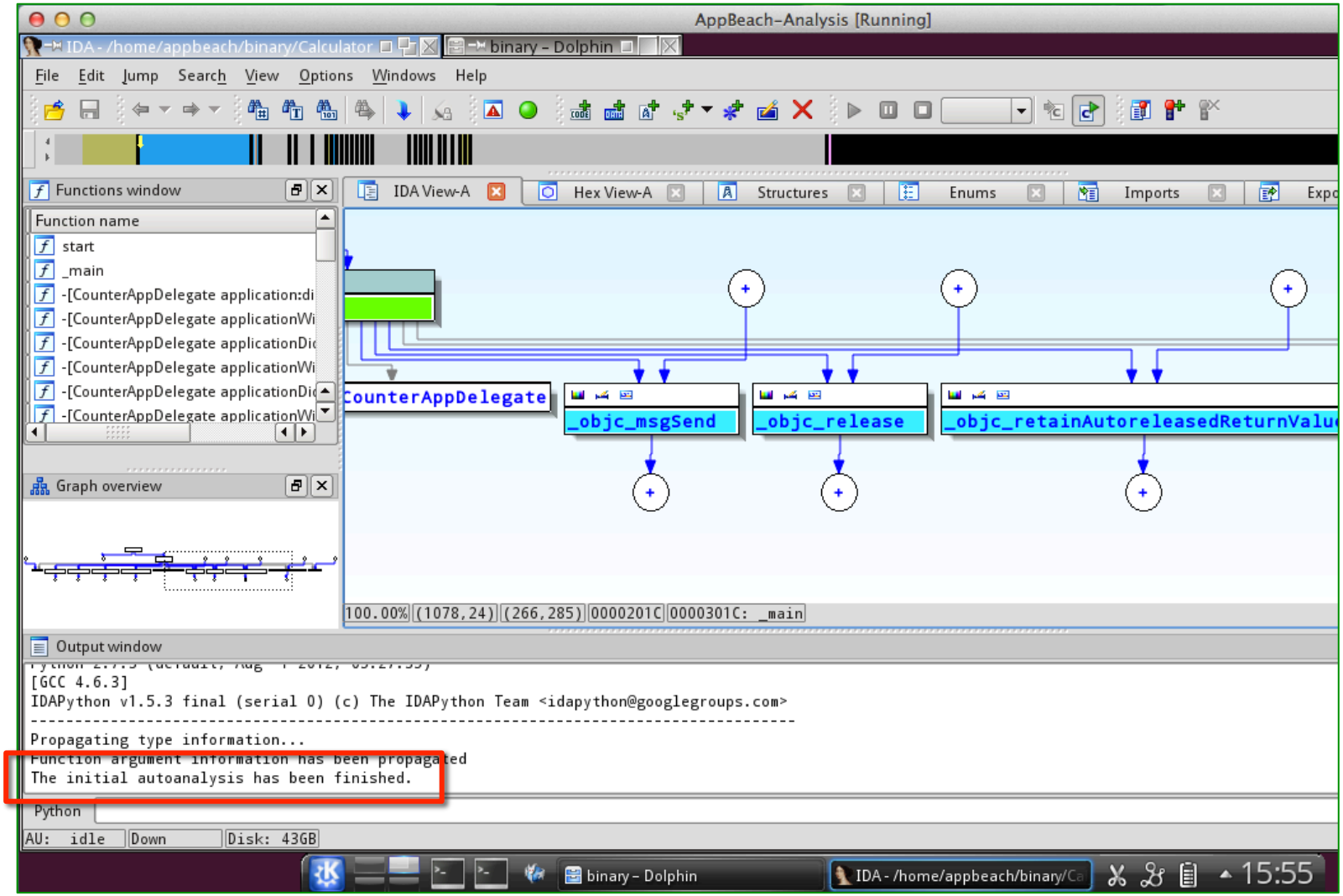


step2: 反組譯binary

透過IDA Pro

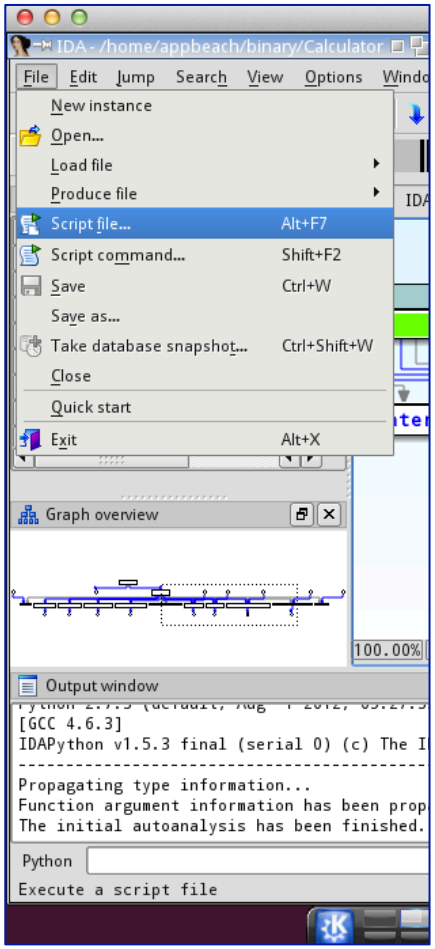


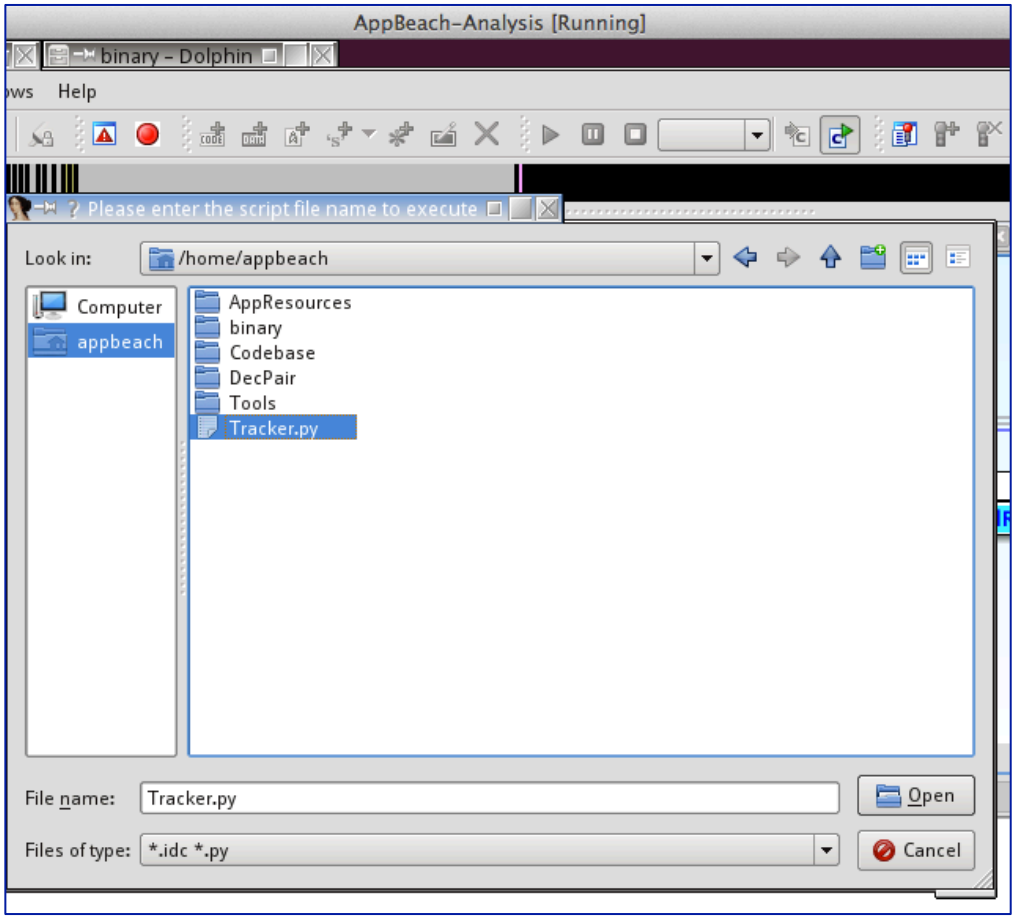
step2: 反組譯binary



step3: 查出好與壞app的method call

script file

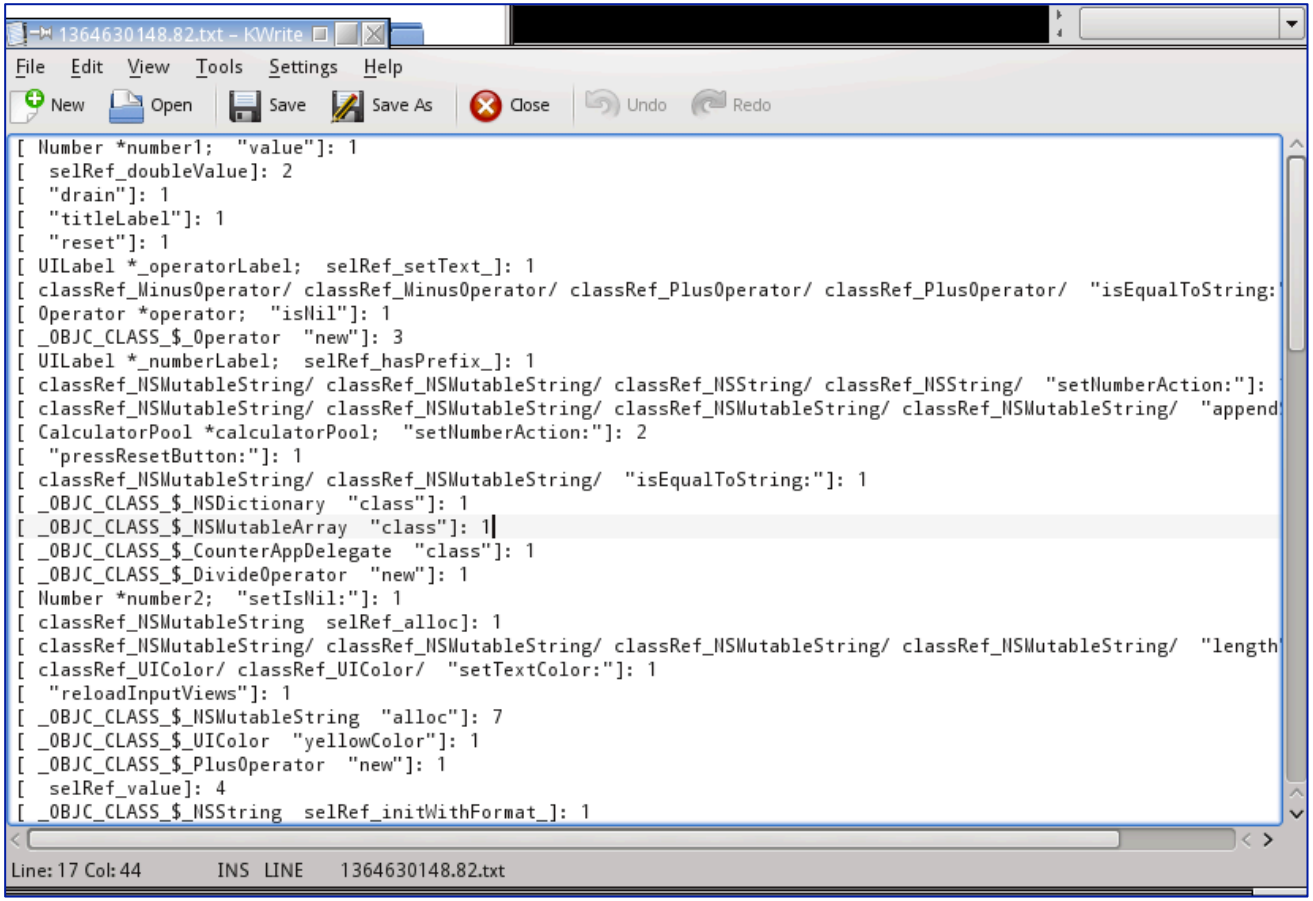




step3: 查出好與壞app的method call

自動產生一個檔案  裡面長這樣…

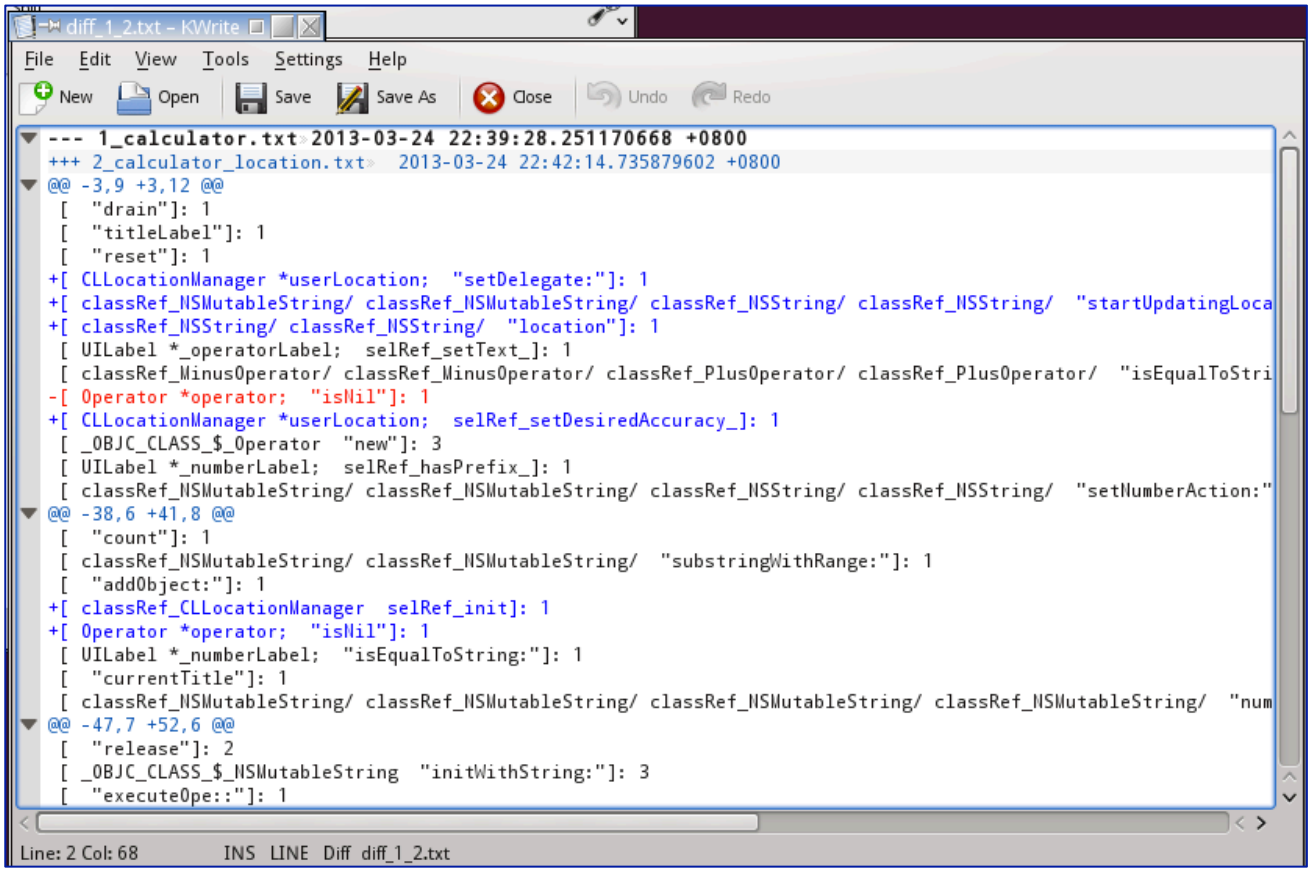
1364630148.82.txt



step4:
比較method call結果，　認出pattern

下指令

diff –u ooo.txt xxx.txt >> diff_ooo_xxx.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(+)

❶ [CLLocationManager *userLocation; “setDelegate:”]: 1
❷ [classRef_NSMutableString/ classRef_NSMutableString/ classRef_NSString/ classRef_NSString/ “startUpdatingLocation”]: 1
❸ [classRef_NSString/ classRef_NSString/ “location”]: 1
❹ [CLLocationManager *userLocation; selRef_setDesiredAccuracy_]: 1
❺ [classRef_CLLocationManager selRef_init]: 1
❻ [_OBJC_CLASS_$_NSString “stringWithFormat:”]: 2
❼ [classRef_CLLocationManager/ classRef_CLLocationManager/ classRef_NSMutableString/ classRef_NSMutableString/ classRef_CalculatorPool/ classRef_CalculatorPool/ “setText:”]: 1
❽ [classRef_CLLocationManager selRef_alloc]: 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_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. [EKEventStore *eventStore; “eventsMatchingPredicate:”]: 1
15. [EKReminder *userReminder; “setCalendar:”]: 1
16. [EKEvent *event; “setTitle:”]: 1
17. [EKEvent *event; “setEndDate:”]: 1
18. [classRef_EKEventStore selRef_alloc]: 1
19. [_OBJC_CLASS_$_NSDateComponents selRef_init]: 2
20. [EKEvent *event; “setStartDate:”]: 1
21. [EKEventStore *eventStore; “predicateForRemindersInCalendars:”]: 1
22. [classRef_NSMutableString/ classRef_NSMutableString/ classRef_NSString/ classRef_NSString/ selRef_getUserCalendar]: 1
23. [classRef_EKEventStore/ classRef_EKEventStore/ classRef_NSMutableString/ classRef_NSMutableString/ classRef_CalculatorPool/ classRef_CalculatorPool/ “setText:”]: 1
24. [_OBJC_CLASS_$_EKEvent “eventWithEventStore:”]: 1
25. [NSDateComponents *oneYearFromNowComponents; “setYear:”]: 2
26. [EKEventStore *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
```

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
```