# ㄋ【專題工作項目】

| **工作項目** | **進度** | | **備註** |
| --- | --- | --- | --- |
| (一)URL\_CHECK前置layout、.java設定 | | | |
| [Button]Layout menu新增”URL Check” | [button id: fan\_url\_check]  string(en,tw已翻)  其他國翻譯未完成 | | dialog\_add\_entry.xml  string id: url\_check |
| [Listener]新增listener監控 | function startUrlCheckActivity() | | MainActivity.java |
| [Layout]新增URL比對頁面 | 完成 | | activity\_url\_check.xml |
| [Activity]新增跳轉Activity[UrlCheckActivity] | 完成 | | MainActivity.java  AndroidManifest.xml |
| [Button]QRcode掃描 | 完成 | | activity\_url\_check.xml |
| [Layout]新增qr\_code掃描頁面 | 完成 | | activity\_url\_check\_scan\_qrcode.xml |
| (二)URL\_CHECK頁面QR code掃描使用 | | | |
| [Java]新增qr\_code掃描頁面串接程式碼 | 2022/3/21完成 | | UrlCheckActivity\_ScanQrcodeActivity.java |
| 新增相機component和調用條碼分析component | 2022/3/21完成 | |  |
| AVD電腦攝像頭測試(包含條碼偵測測試) | 2022/3/22完成 | | [~~Bug] AVD設定鏡頭不知為何無法啟用~~ |
| [Dialog] Camera get permission | 2022/3/23完成 | | ~~[Bug] 無法開啟鏡頭(權限已經啟用)~~ |
| URL資料傳回URL check | 2022/3/26完成 | | 一掃到條碼便會關閉activity，傳回UrlCheckActivity.java  的String qr\_code\_URL  resultCode更改，傳回intent資料[當初寫成requestCode] |
| [Bug] Scan\_qr\_code按返回鍵無法跳回上一個Activity | 2022/3/24完成 | |  |
| URL\_Check layout設計及QR code掃描頁面設計 | 未完成 | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
| (三)網址檢查部分 | | | |
| [說明] 只用一個String URL\_text 來取得url\_input及qr\_code掃描的內容，網址檢查完畢後再清空此string才不會產生衝突 2022/3/23 | | | |
| [說明] 在branch Judy上進行commit && push 2022/3/24 | | | |
| 新增URL比對資料庫 | 大項 | | Content path資料夾  /data/user/0/com.beemdevelopment.aegis.debug/files  新增的entry放在aegis.json  【問題：掃描QRcode沒辦法得知網站】  解決：變動AddEntry程式碼 |
| 內部儲存體新增file | 2022/3/24完成 | | Domain\_name\_txt.txt file  和AddEntry存的aegis.json同path |
| 變動ScanQRcode那邊匯入資料的部分(在於Aegis掃描QRcode沒有抓到issuer)[Facebook] | 2022/3/25 完成 | | GoogleAuthInfo.java  [[程式碼附圖](#bookmark=id.4d34og8)]  已用GitHub、Discord做過測試 |
| 解析aegis.json檔 | 2022/3/25完成 | | [[附圖1](#bookmark=id.2s8eyo1)]、[[附圖2](#bookmark=id.17dp8vu)]、[[附圖3](#bookmark=id.3rdcrjn)]  新增function create\_issuer\_arrayList  放入aegis.json解析出的issuer(小寫) |
| 比對Host是否包含issuer | 2022/3/26完成 | | 需要考慮放進去的格式及比較格式 |
| Toast提示製作 | 2022/3/26 完成 | |  |
| 新增permisson允許執行網路請求 | 2022/3/26完成 | | AndroidManifest.xml  <https://developer.android.com/training/basics/network-ops/connecting?hl=zh-cn> |
| 子執行緒執行網路要求 | 2022/3/26完成 | | AndroidManifest.xml 要允許網路  同個Process不同thread  Main本身就有一個執行緒了  (得到thread資訊)  <https://www.itread01.com/content/1547310542.html>  **新增子線程執行網路請求**  Handler作為執行緒間通訊的方式 |
| 主Thread和子Thread間傳送數據 | 2022/3/27完成 | | 直接implement Runnable()  就可以直接用到全域變數URL\_text |
| 建立Whois伺服器xml | 2022/3/27 完成 | | 比對TLD 來找到whois server  Res底下xml資料夾whois\_server.xml  [參考資料]  <https://www.biecuoliao.com/pa/4QARRo4.html> |
| Dialog分支及建立 | 流程尚未全部完成 | | [Dialog分支圖解](#_heading=h.1fob9te) |
| Whois 使用 | 2022/3/27 Whois連接伺服器測試成功 | | [[Whois參考資料](#_heading=h.tyjcwt)]  WHOIS通常使用TCP協定43埠。每個域名或IP的WHOIS資訊由對應的管理機構儲存，例如，以.com結尾的域名的WHOIS資訊由.com域名運營商VeriSign管理，中國國家頂級域名.cn域名由CNNIC管理。  通常情況下，域名或IP的資訊可以由公眾自由查詢獲得，具體的查詢方法是**登入由管理機構提供的WHOIS伺服器**，輸入待查詢的域名進行查詢 |
| Thread的停止及回傳值 | 2022/3/28 完成 | | Function  set\_and\_display\_whois\_message  (String msg) |
| 新增string.xml資料 | 部分完成，最後要再全部都製作string | | R.string.warning  R.id. addURL  R.string.unsafeURL  R.string.safeURL  R.string.parseFail  [串接的話要用  getResource().getString(R.string.XXX)] |
| Domain name的抓取 | 2022/4/4 完成 | | www.google.com.tw  console.us2.crashplanpro.com  <https://www.796t.com/post/NTN0MTI=.html>  [try-catch loop參考]  利用Socket連上whois server還**是沒有辦法透過IP來找尋資訊**，還是得依靠Domain name  <https://segmentfault.com/q/1010000000360070> [參考資料]  [[筆記](#_heading=h.4d34og8)]  **利用InternetDomainName去抓**  Package com.google.common.net  class com.google.common.net.InternetDomainName |
| build.gradle error，加入packagingOptions 避免NETA-INF出錯 | 2022/4/5完成 | |  |
| 增加翻譯功能  auto -> zh\_tw  增加翻譯功能  auto -> zh\_tw | 2022/4/5完成 | | 調用google api翻譯(免費)  <https://blog.csdn.net/yyongsheng/article/details/87007484>  <https://jackromer.github.io/2019/09/05/JAVA%E8%B0%83%E7%94%A8Google%E7%BF%BB%E8%AF%91api/>  <https://translate.googleapis.com/translate_a/single?client=gtx&sl=auto&tl=zh_tw&dt=t&q=text>  [httpURLconnection的設定]  <https://blog.csdn.net/fengyeNom1/article/details/84568046> |
| 解析翻譯結果 | 2022/4/11 完成 | | [[伺服器參數](#_heading=h.1t3h5sf)]  用 \\\* 代替換行符號，避免在翻譯時換行符號被翻譯掉  ~~[Bug] 翻譯長度限制(測試)~~  發現是遇到 # 就會自動終止翻譯  將 #字元先標記為$字元，最後再轉回來 |
| InternetDomain package安全性 |  | |  |
| 蒐集有關2FA的登入網址 | 2022/4/18 完成 | | <https://2fa.directory/int/#communication>  [[登入網址整理(提供2FA的網站](about:blank)) |
| 整理各個伺服器回傳的資料格式 | 2022/4/18完成 | | [[Server回傳格式](about:blank)]  **co.za好像不提供whois server服務**  **.ph好像不提供whois server服務**  **.pt 連不上whois.dns.pt server**  **.ch要求whois.nic.ch存取被拒絕**  **.to搜尋到的東西沒有跑出來(**  **可能是本身測試網址的問題**  **或whois.thnic.net伺服器問題)**  [**https://ti.to/home#/**](https://ti.to/home#/) |
| 欄位分割 一般TLD | 2022/4/21完成(尚未測試) | | <https://www.regextester.com/>  [正則表達線上測試]  <https://developer.mozilla.org/zh-TW/docs/Web/JavaScript/Guide/Regular_Expressions>  \r字元重要(ASCII: 13)  ~~.io TLD會跳掉 > index問題，已修復~~  .se TLD 出錯 |
| 特殊TLD：.ua | 2022/4/21 完成 | | 針對開頭含有%的標籤  % Glue Records:  % =============  nserver: ns1.ukraine.com.ua  ip-address: 2001:67c:2070:c8e3::1  ip-address: 91.206.200.227  做特殊處理 |
| 特殊TLD：.pl | 2022/4/21完成 | | 針對  REGISTRAR:  cyber\_Folks S.A.  ul. Franklina Roosevelta 22  60-829 Poznań  Polska/Poland  tel.: +48.122963663  [info@domeny.pl](mailto:info@domeny.pl)  無法串接做特殊處理 |
| 刪除空白標籤及field前後空白測試 | 2022/4/22測試完成 | |  |
| 特殊TLD：.gov && .net && .cc && .tv && .com | 2022/4/22完成 | | 不做串接 |
| 例外TLD .tw | 2022/4/22完成 | | 有點問題但不影響 |
| 移除非必要資訊(包含：的字串) | 2022/4/22完成 | |  |
| 特殊TLD：.br | 2022/4/23完成 | | 額外對br進行特殊串接處理 |
| 整理顯示欄位關鍵字 | 2022/4/23完成 | | 抓取tag去匹配關鍵字  【[整理關鍵字doc](about:blank)】 |
| 針對特殊TLD .ua做特別關鍵字處理 | 2022/4/23完成 | | Registrar 和 Registrant |
| 測試 | 2022/4/23完成 | | 【[測試名單](about:blank)】  只針對裡面的內容作測試  尚未對【[2FA登入網址](about:blank)】作全部測試 |
| 發現問題，Whois工具當作輔助，新增釣魚網站檢查網站 |  | | [Java Http連線]  <https://blog.csdn.net/fightingXia/article/details/71775516>  [Java HttpURLConnection 設定user-agent]  <https://dotblogs.com.tw/newmonkey48/2013/01/29/89246>  <https://cache.one/read/16411271>  [Http回應代碼]  <https://blog.csdn.net/sunnylinner/article/details/53884698?utm_medium=distribute.pc_relevant.none-task-blog-2~default~baidujs_baidulandingword~default-0.pc_relevant_antiscanv2&spm=1001.2101.3001.4242.1&utm_relevant_index=3>  [JSOUP請求JSON 及解決jsoup不能完整獲取響應內容的問題]  <https://www.796t.com/content/1542424504.html>  ~~[Java 動態網頁爬蟲]~~  <https://iter01.com/631863.html>  因為有些值是通過非同步渲染所以抓取不到  在程式中使用內建瀏覽器核心，但還要下載Driver驅動(**不能用)**  **法二：反向解析區塊相對應的js檔案，再解析下載下來的json檔案**  **發現靜態爬蟲便可執行** |
| 使用ScamAdviser爬蟲獲得資訊 | 2022/5/8 完成 | | 獲得資訊有：  Trust Score  Website  Title  Domain age  WHOIS registration date  WHOIS last update date  WHOIS renew date |
| 等待網頁完整載入問題 | 無法解決 | |  |
| 反”反爬蟲”機制 |  | | User-Agent設定  Cookie設定 |
| 觀察支援2FA的所有網站的登入網址(找規律) |  | |  |
| 用戶自訂網址加入安全名單 |  | |  |
| 比對的五種方式自訂 |  | |  |
| Auto抓取網頁上網址(不用讓使用者再複製要檢查的網址，然後開app再貼上) |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |
| (四)新手引導介面 | | | |
| [說明]在master的分支上進行commit && push [[branch的使用教學](#_heading=h.3znysh7)] | | | |
| 在[[圖片一](#bookmark=id.1t3h5sf)]的地方新增一個button | | 可能顯示是否要觀看新手教學 | src/main/res/layout/fragment\_done\_slide.xml [layout參考]  新增的檔案也放在 layout資料夾底下，命名規則參考fragment\_done\_slide  [.java]請放在ui/slides底下，命名規則參照底下的檔案 |
| 教學步驟 | | 如何開啟2FA步驟(可能以FB為例子) |  |
| [layout]在 menu\_main.xml 右上角新增一個Button | | 2022/04/02完成 | menu\_main.xml  menu\_action\_mode.xml  button id為action\_2FA |
| [layout]最後一頁增加一個按鈕跳轉2FA介紹 | | 2022/04/02完成 | fragment\_done\_slide.xml |
| [layout]2FA介紹頁面 | | 2022/04/11完成 | fragment\_main\_first.xml  fragment\_main\_second.xml  fragment\_main\_third.xml  fragment\_main\_fourth.xml |
| [java]2FA介紹的設置 | | 2022/04/11完成 | Intro2FAActivity.java  Intro2FAActivity.java  AndroidManifest.xml  要像剛開始的一樣有頁數可看 |
| [java]跳轉2FA介紹Button設置 | |  | Intro2FA  DoneSlide |
| (五)URL另外四種比對 | | | |
| 參考bitwarden auto fill的比較 | |  | <https://bitwarden.com/help/uri-match-detection/#default-match-detection> |
| [java]Base domain | | 2022/05/14需調整 | host\_name要相同 |
| [java]Host | | 2022/05/22已完成 | port要相同 |
| [java]Starts with | | 2022/05/22已完成 | 比到path |
| [java]Exact | | 2022/05/22已完成 | 完全相同 |
|  | |  |  |
| (六)期末報告 | | | |
| 和前一屆的比較  和現有軟體比較   * 舉例和挑幾個做細部比較   現在進度  未來規劃  遇到問題&&改進創新困難點  預設QA | |  |  |
| 跟學長的比較 | |  |  |
| 跟Bitwarden差別 | |  |  |
| 跟andotp差別(為什麼不採用) | |  |  |
| 分工 | |  |  |
|  | |  |  |
| (七)其他功能 | | | |
| [Button]手動輸入URL(文字辨識拍照) | 未設計(未定) | | activity\_url\_check.xml |
| [Java]後段連結URL比對 | 未定 | |  |
| [DataBase]URL比對資料庫 | 未定 | |  |
| **分析網站Information方法研究** | 未定 | | [【檢查網址】](about:blank)**做成說明文件，並詳細說明方法** |
| 匯出\入檔案及備份功能 | 未定 | |  |
| Notification新增彈跳通知(像是steam的驗證代碼) | 未定 | | <https://ithelp.ithome.com.tw/articles/10188916> |
| Password manager功能 | 未定 | |  |

# [伺服器參數](#bookmark=id.3znysh7)

**com**

Domain Name: YOUTUBE.COM

Registry Domain ID: 142504053\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

Registrar URL: http://www.markmonitor.com

Updated Date: 2022-01-14T09:38:42Z

Creation Date: 2005-02-15T05:13:12Z

Registry Expiry Date: 2023-02-15T05:13:12Z

Registrar: MarkMonitor Inc.

Registrar IANA ID: 292

Registrar Abuse Contact Email: abusecomplaints@markmonitor.com

Registrar Abuse Contact Phone: +1.2083895740

Domain Status: clientDeleteProhibitedhttps://icann.org/epp#clientDeleteProhibited

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited

Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited

Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited

Name Server: NS1.GOOGLE.COM

Name Server: NS2.GOOGLE.COM

Name Server: NS3.GOOGLE.COM

Name Server: NS4.GOOGLE.COM

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of whois database: 2022-04-05T01:36:15Z <<<

**tw**

Domain Name: google.com.tw

Domain Status:

clientUpdateProhibited,clientTransferProhibited,clientDeleteProhibited

Registrant:

Google Inc.

DNS Admin dns-admin@google.com

+1.6502530000

+1.6506188571

1600 Amphitheatre Parkway

Mountain View, CA

US

Administrative Contact:

DNS Admin dns-admin@google.com

+1.6502530000

+1.6506188571

Technical Contact:

DNS Admin dns-admin@google.com

+1.6502530000

+1.6506188571

Record expires on 2022-11-09 00:00:00 (UTC+8)

Record created on 2000-08-29 10:22:50 (UTC+8)

Domain servers in listed order:

ns1.google.com

ns2.google.com

ns3.google.com

ns4.google.com

Registration Service Provider: Markmonitor, Inc.

Registration Service URL: http://www.markmonitor.com/

Provided by Registry Services, LLC. Registry Gateway Services

# [Domain name的抓取](#bookmark=id.1fob9te)

Public Suffix List： <https://publicsuffix.org/learn/>

<https://github.com/whois-server-list/public-suffix-list>

**Internet Domain name class**

<https://guava.dev/releases/snapshot/api/docs/com/google/common/net/InternetDomainName.html>

如何導入包(package)

<https://blog.csdn.net/JKjiang123/article/details/79178890>

大概意思就是工程生成了不止一個META-INF/proguard/androidx-annotations.pro檔案，看起來是因為多個 jar 包裡包含了同樣的檔案（proguard/androidx-annotations.pro），導致打包時因為擔心相互覆蓋問題而提示出錯<https://blog.csdn.net/weixin_54305517/article/details/121583540>

<https://www.itread01.com/content/1546532592.html>

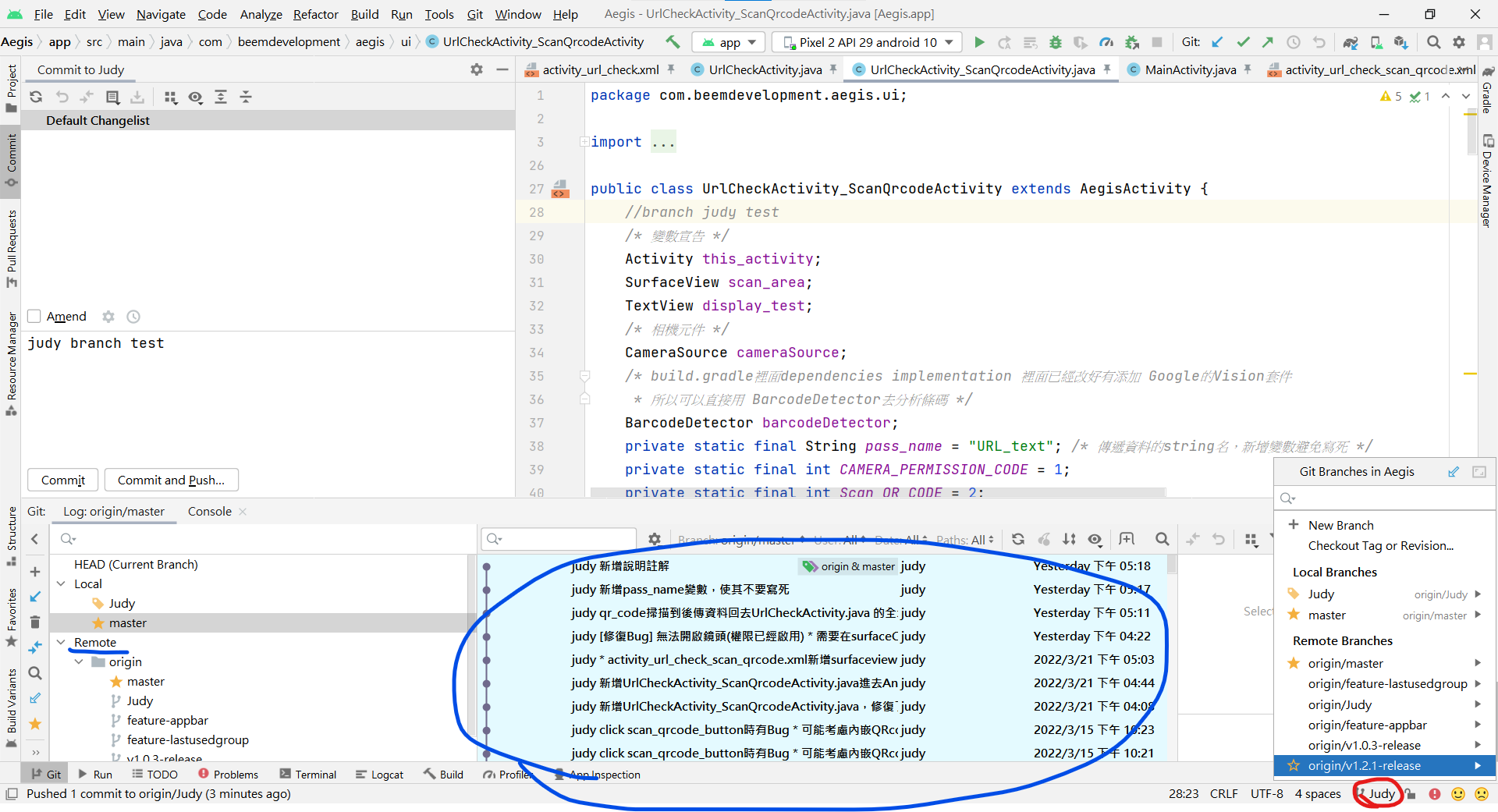
最後用com.google.common.net package

(工程開始已經有dependencies google guava了，可以直接用class)

# [Dialog分支圖解](#bookmark=id.26in1rg)



# branch 的使用

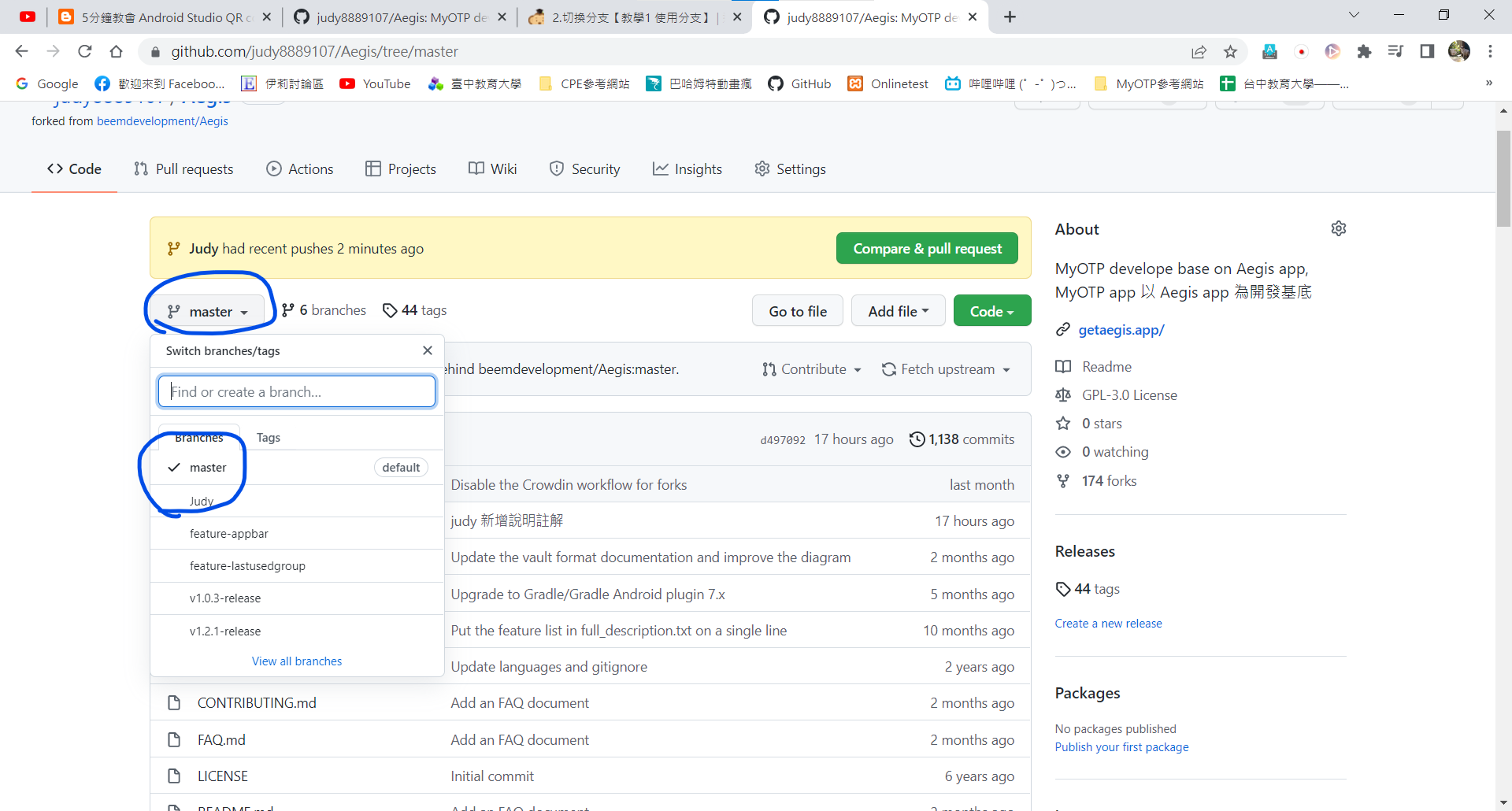


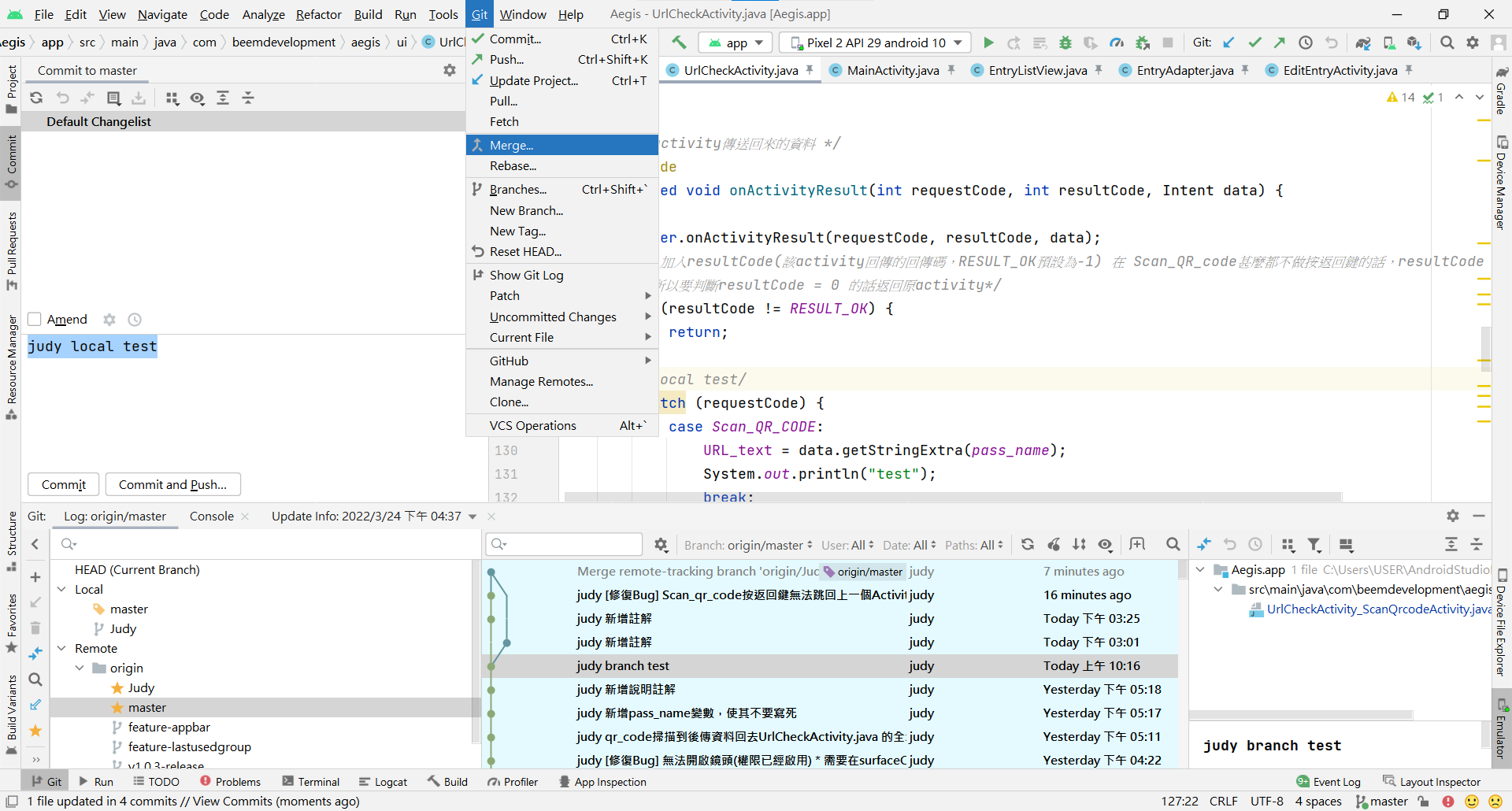
紅色圈起來的地方可以切換branch

藍色的地方則是可以看版本、更改的部分

在不同branch上commit只會顯示在該branch

GitHub這邊可以切換branch來看





假設修改Judy 要合併到master 分支切換到master 後點git的merge選Judy進行合併，merge完之後記得直接按push，按commit不會跳出任何東西

按 進行Push，會連同原本分支的commit一起push上去

# OTP QR code內容

參考：<https://2fa.directory/int/> [有提供2FA服務的網站]

otpauth://totp/ID:100001534662130?secret=PVPVDQLV6RM3EQLLAV6NRROOB5F6N2US&digits=6&issuer=Facebook

otpauth://totp/GitHub:judy8889107?secret=7RVWRY5D2PYWKXOL&issuer=GitHub

otpauth://totp/Discord:judy8889107@gmail.com?secret=NLPKEDIXRNHUFBAW&issuer=Discord

# [Whois 參考資料](#bookmark=id.gjdgxs)

Whois server：

<https://www.iana.org/domains/root/db>

Whois server不同說明：

<https://www.itread01.com/p/1327035.html>

Whois使用(使用Apache Commons Net查询Whois域名注册信息)：

<https://www.freesion.com/article/64291187769/>

android 基于 socket 的Whois域名查询：

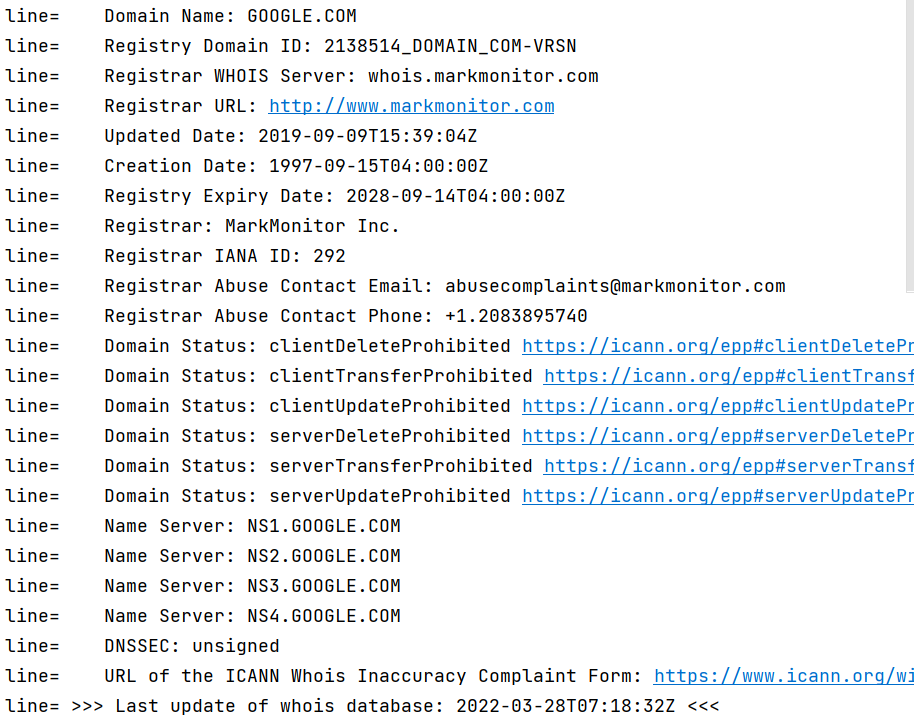
<https://www.biecuoliao.com/pa/4QARRo4.html>

常用的 WHOIS 伺服器

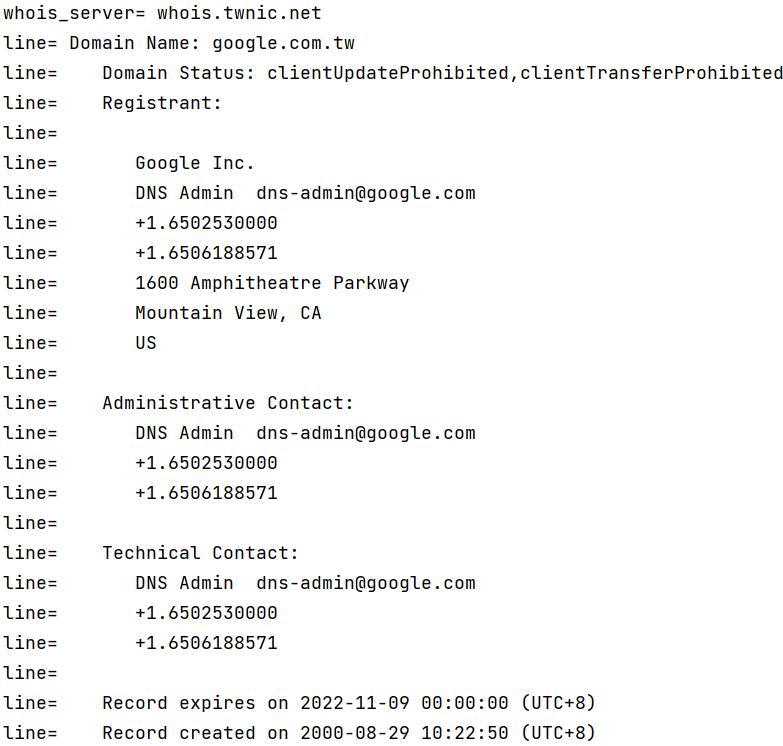
| 機構縮寫 | WHOIS 伺服器地址 | 機構名稱 | 提供查詢內容 |
| --- | --- | --- | --- |
| CERNIC | whois.edu.cn | 中國教育與科研計算機網網路資訊中心 | 中國教育網內的 IP 地址和 .edu.cn 域名資訊 |
| CNNIC | whois.cnnic.net.cn | 中國網際網路絡資訊中心 | .cn 域名（除 .edu.cn）資訊 |
| INTERNIC | whois.internic.net  (WhoisClient  預設) | 網際網路絡資訊中心 | .com，.net，.org，.biz，.info，.name 域名的註冊資訊（只給出註冊代理公司） |
| ARIN | whois.arin.net | 美國 Internet 號碼註冊中心 | 全世界早期網路及現在的美國、加拿大、撒哈拉沙漠以南非洲的 IP 地址資訊 |
| APNIC | whois.apnic.net | 亞洲與太平洋地區網路資訊中心 | 東亞（包括中國大陸和台灣）、南亞、大洋洲的 IP 地址資訊 |
| RIPE | whois.ripe.net | 歐洲 IP 地址註冊中心 | 歐洲、北非、西亞地區的 IP 地址資訊 |
| TWNIC | whois.twnic.net | （中國）台灣網際網路絡資訊中心 | .tw 域名和中國台灣島內的 IP 地址資訊 |
| JPNIC | whois.nic.ad.jp | 日本網際網路絡資訊中心 | .jp 域名和日本境內的 IP 地址資訊 |
| KRNIC | whois.krnic.net | 韓國網際網路絡資訊中心 | .kr 域名和韓國境內的 IP 地址資訊 |
| LACNIC | whois.lacnic.net | 拉丁美洲及加勒比網際網路絡資訊中心 | 拉丁美洲及加勒比海諸島的 IP 地址資訊 |

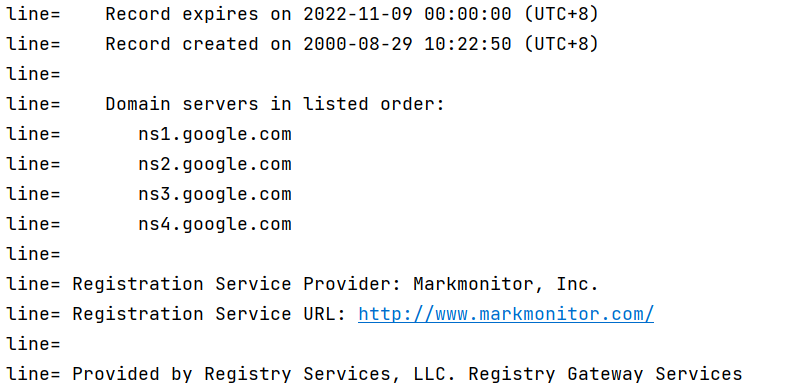
# [Whois query結果字串](#bookmark=id.lnxbz9)

google.com 找到的



google.com.tw





# URI使用

<https://www.jianquoyun.com/d/Loqin#from=https%3A%2F%2Fwww.jianquoyun.com%2F>

URI host= www.jianquoyun.com

URI Authority= www.jianquoyun.com

URIFragment=from=https://www.jianquoyun.com/

URI Path= /d/Loqin

URI Port=-1

URI Query= null

URI RawAuthority= www.jianquoyun.com

URI RawFragment=from=https%3A%2F%2Fwww.jianquoyun.com%2F

URI RawPath= /d/Loqin

URI RawQuery= null

URI RawSchemeSpecificPart=//www.jianquoyun.com/d/Loqin

URI RawUserInfo- null

URI Scheme= https

URINormalize=https:/www.jianquoyun.com/d/Loqin#from=https%3A%2F%2Fwww.jianquoyun.com%2F

URI HashCode=100565027

* 若網址有空白則try會失敗

# URL使用

protocol://host:port/path?query#ref

網址組成

<https://www.jianquoyun.com/d/Loqin#from=https%3A%2F%2Fwww.jianquoyun.com%2F>

Protocol= https

Authority= www.jianquoyun.com

File name= /d/Loqin

Host= www.jianquoyun.com

Path= /d/Loqin

Port=-1

DefaultPort=443

Query= null

Ref=from=https3A%2F%2Fwww.jianquoyun.com%2F

# 附件

