國立虎尾科技大學人事服務電子（e）報

109 年 12 月　　國立虎尾科技大學人事室編製

「人事服務電子報」(簡稱人事ｅ報)，內容涵蓋、教職員喜訊、每月新知、法令宣導、人事動態、環保節能、生活知識、各類活動訊息等。各單位如有須同仁瞭解事項，都可透過本報轉知，本報為溝通之橋樑，每月透過電子郵件傳送全體同仁參考，如有任何訊息，歡迎來信提供及指教。(來信信箱：personel@nfu.edu.tw)

壹、每月新知

一、提供大墩陽光冬令營九折優惠活動，該網站：
http://okgogo.org/0d/109DM01.docx

二、有關公務人員退休撫卹基金管理委員會與第一商業銀行、合作金庫商業銀行合作辦理之「參加退撫基金人員指定用途貸款」，延長申請期限至民國 111 年 12 月 31 日止，請查照。(109 年 12 月 16 日本校虎科大人字第 1090011967 號函)

三、學校採購業務主管涉洩密 案例

案情摘要

○○學校 A 校長、B 總務主任、C 輔導主任承辦政府採購業務， 於 106 至 107 年間辦理教學參訪採購案，A 校長明知不得對廠商為無正當理由之差別待遇，且不得於開標前洩漏足以造成限 制或不公平競爭之相關資料，仍在該採購案上網公告前，聯繫 業者並指示 B 總務主任、C 輔導主任，將招標文件中時間、地點及人數等應予保密之資料，告知特定業者，使該業者得以事 前準備，造成不公平競爭之情形。

問題癥結

(一)欠缺政府採購法保密觀念

政府採購法第 34 條規定：「機關辦理採購，其招標文件於公告前應予保密。但須公開說明或藉以公開徵求廠商提供參考資料 者，不在此限（第 1 項)。機關辦理招標，不得於開標前洩漏底價，領標、投標廠商之名稱與家數及其他足以造成限制競爭或 不公平競爭之相關資料（第 2 項)。」本案相關人員欠缺對於政府採購法保密規定之認識。

(二)對於採購程序專業性不足

政府採購法施行細則第 34 條規定：「機關依本法第三十四條第一項規定向廠商公開說明或公開徵求廠商提供招標文件之參考 資料者，應刊登政府採購公報或公開於主管機關之資訊網路。」 本案相關人員未審酌提供該採購文件資料，是否足以造成不公 平競爭

及影響其他廠商權益情形，即便宜行事將招標文件內容 洩漏予特定業者。

預防作為：

(一)機關學校辦理採購，招標文件內容於招標公告前必須保密，但須向廠商公開說明或公開徵求廠商提供招標文件之參考資料者，其內容可於公告前公開，依政府採購法施行細則第 34 條規定， 以刊登政府採購公報或公開於主管機關之資訊網路方式辦理， 使廠商藉此獲得招標資料。

(二)應適時向機關學校承辦採購業務之相關人員進行案例宣導，避免觸犯刑法第 132 條公務員洩漏國防以外秘密罪。

相關法令規定：

(一)刑法第 132 條，公務員洩漏國防以外秘密罪。

(二)政府採購法第 34 條，機關辦理採購，其招標文件於公告前應予保密。

(三)政府採購法施行細則第 34 條，依政府採購法第 34 條第 1 項規定向廠商公開說明或公開徵求廠商提供招標文件之參考資料者， 應刊登政府採購公報或公開於主管機關之資訊網路。

貳、法規訂定或修正

一、檢送銓敘部 109 年 12 月 11 日部退一字第 10953031001 號令修正發布之「公教人員保險準備金管理及運用辦法」第 7 條修正條文、修正總說明、修正條文對照表及發布令影本各 1 份，請查照。(109 年 12 月 15 日本校虎科大人字第 1090011928 號書函)

二、修正本校教師升等申覆處理要點，該要點並業置於本校人事室網頁-「人事規章」-「教師聘任升等」項下，請自行下載運用。(109 年 12 月 21 日本校虎科大人字第 1092300756 號)

三、「教育部設置國家講座辦法」第 2 條、第 6 條、第 7 條，業經教育部於中華民國 109 年 12 月 3 日以臺教高（五）字第 1090154342B 號令修正發布，檢送發布令影本（含法規條文）1 份。(109 年 12 月 7 日本校虎科大人字第 1090011502 號)

參、 人事法令宣導

一、考試、任（聘）免、敘薪、兼職：

(一)檢送銓敘部民國 109 年 11 月 30 日部法一字第 10953034301 號令影本 1 份，請查照。(109 年 12 月 9 日本校虎科大人字第 1090011742 號書函)

(二)重申各系(室、中心）及學院辦理教師升等事宜，應落實審查機制，並依相關規定及期程辦理，以保障教師權益。(109 年 12 月 2

日本校虎科大人字第 1092300712 號）

肆、 人事動態

異動情形	服務單位	職稱	姓名	生效日期	備註
回職復薪	國際事務處 境外學生事務組	助理員	林怡君	109.12.10	
留職停薪	電子計算機中心	助理員	謝蕙如	109.06.01	延長留職停薪期間 109.12.1~110.5.31
留職停薪	國際事務處 境外學生事務組	助理員	謝宛庭	109.09.26	延長留職停薪期間 109.12.26~110.12.25
離職	國際事務處 境外學生事務組	助理員	黃雅祺	109.12.10	聘期屆滿

伍、宣導事項：

智慧財產權 Q&A

一、請問如果將國外抖音或是演講翻譯後，放在自己的 Youtube 會違法嗎?在 FB 看到的搞笑影片都可以下載重置賦予新意義上傳嗎?想經營頻道但是擔心法律問題。

A1：

一、國外抖音或是演講翻譯放在自己的 Youtube？

翻譯屬於著作權的「改作」行為，將翻譯後的作品上傳到自己 Youtube 屬於著作權的「公開傳輸」行為，以上皆為利用他人著作之行為，建議應事先取得權利人授權，以避免因違反著作權法而承擔民、刑事責任。

二、在 FB 看到的搞笑影片都可以下載重置（來信所提重置，應是指上傳）賦予新意義上傳嗎？

(一)按著作權法第51條規定：「供個人或家庭為非營利之目的，在合理範圍內，得利用圖書館及非供公眾使用之機器重製已公開發表之著作。」因此，如果單純以個人非營利目的，將影片下載自行觀看，可以主張上述合理使用，較無疑問。

(二)至於所稱「重置賦予新意義」，仍要先釐清是否屬於上述「改作」行為。這裡必須強調，現行著作權法僅能保護著作之「表達」，而不保護表達所隱含之「概念」(例如思想、程序、製程、系統...等，可參考智慧財產局函釋電子郵件1000413b)，用意在於避免保護「概念」後，使他人得以著作權法壟斷此一「概念」，並且阻礙運用此「概念」所可能產生各種「表達」。因此，

如果只是參考搞笑影片的「概念」，由於此並非著作權保護的範疇，因此重新拍攝及製作影片，並不及於原作品著作權的保護範圍。但如果是涉及「表達」層次，例如直接使用搞笑影片的台詞對話，就仍建議事先取得權利人授權。

三、補充提醒的是，主張合理使用的風險：

(一)如有侵害著作權情形時，主張成立「合理使用」為常見之免責理由。

(二)然而判斷是否成立「合理使用」須參酌諸多因素（如利用他人著作比例、質量、性質、市場價值影響等），且最終仍需交由司法機關依個案情形進行最後裁決，而無法自行認定。因此較不建議自行認定利用他人著作之行為，符合「合理使用」而主張免除相關責任。

【眾勤法律事務所副所長 陳全正律師 解答】以上資料摘自經濟部智慧財產局 原創我挺你 FB

更多相關訊息可連結

經濟部智慧財產局 原創我挺你

FB(https://www.facebook.com/copyright.com.tw/)

二、在舉辦活動時，有邀請一位書法家揮毫一句話，後來雙方也同意做專屬授權，如果想要把這個作品拿來申請商標並製作商品販售，這樣的話是可行的嗎?

A2：

一、首先應說明的是，商標權和著作權為不同法律概念，商標權功用在於使消費者認知、區別商品或服務來源；著作權則是為保障著作人著作權益，兩者保護目的不同。

二、如果創作內容同時符合著作權法(為獨立創作且非抄襲而來之「原創性」及需具有最低創作高度之「創作性」)與商標法（識別性）保護要件，則可同時受著作權法與商標法保護，互不衝突。

三、建議應釐清授權契約內容，再就書法揮毫成果為後續利用為宜

(一)書法揮毫成果屬於「美術著作」(可參考：智慧財產局函釋 智著字第10900007330號)。

(二)所詢問題雖提及已取得「專屬授權」，但應釐清下列事項：

1.所取得之「專屬授權」，應僅是針對著作權法相關權利進行約定，且可能對權利行使設有期間、地區等若干限制，不利於後續將著作作為商標使用。因此最終仍需審視雙方是否就書法揮毫成果，可否作為申請商標並製作相關商品銷售有所約定。

2.如無相關約定且未經著作權人同意，將揮毫成果申請商標，將可能因商標申請過程中（如填具申請文件）需使用到著

作內容，而涉及「重製」、「改作」他人著作之行為（可參考：智慧財產法院103年度民商訴字第24號判決）。

3.縱使後續成功申請商標，也可能因侵害他人著作權為由，遭撤銷商標註冊。

(三)建議應取得著作權人明確同意後，再就書法揮毫成果進行商標申請為宜。

【眾勤法律事務所副所長 陳全正律師 解答】

以上資料摘自經濟部智慧財產局 原創我挺你 FB

更多相關訊息可連結

經濟部智慧財產局 原創我挺你

FB(https://www.facebook.com/copyright.com.tw/)

三、教科書通常都由文字、圖像所組成，如果符合「原創性」（為獨立創作且非抄襲而來）及「創作性」（需具有最低創作高度）此二要件，則文字（語文著作）、圖像（美術著作）皆受著作權法保護。

A3：

一、教科書通常都由文字、圖像所組成，如果符合「原創性」（為獨立創作且非抄襲而來）及「創作性」（需具有最低創作高度）此二要件，則文字（語文著作）、圖像（美術著作）皆受著作權法保護。

二、所詢問題之行為，須分別進行檢視是否有侵害他人著作權之風險

（一）「編排方式」如僅為「概念」相似，則參考他人編排方式編製教材，較無侵害他人著作權之疑慮；若「編排方式」已構成「表達」層次之近似，則建議應取得權利人授權為宜。

1.現行著作權法僅能保護著作之「表達」，而不保護表達所隱含之「概念」（例如思想、程序、製程、系統...等，可參考智慧財產局函釋電子郵件 1000413b），用意在於避免保護「概念」後，使他人得以著作權法壟斷此一「概念」，並且阻礙運用此「概念」所可能產生各種「表達」。

2.而「編排方式」如果是可歸類於抽象層次之「概念」，像是為了教學鋪陳所需，例如「章節由淺入深的安排」、「先教導基本知識再進行隨堂測驗」等設計，則此種情形下，參考他人「編排方式」編製教材，較無侵害他人著作權之疑慮。

3.然而，若「編排方式」已涉及具體呈現之「表達」，如文字、圖像具體編排呈現方式、版面設計、插圖選用等素材構成近似時，則此種情形下，參考他人「編排方式」編製教材，屬於利用他人著作之行為，建議應取得權利人授權為宜。

（二）參照補習班教科書文字編製之行為，建議應取得權利人授權為宜由於教科書文字屬於語文著作，如果參考他人教科書文字內

容再行編製，則視實際編製行為，如為複製部分內容（屬於「重製」行為）、改寫部分內容（屬於「改作」行為）等，皆為利用他人著作之行為，建議應事先取得權利人授權，以避免因違反著作權法而承擔民、刑事責任。

三、未經授權利用他人著作之行為，「營利與否」僅是可否主張「合理使用」作為免責的判斷依據之一

（一）如有侵害著作權情形時，主張成立「合理使用」為常見之免責理由。

（二）然而判斷是否成立「合理使用」須參酌諸多因素（如利用他人著作比例、質量、性質、市場價值影響等），「營利行為與否」僅為其中一個判斷因素、並非唯一標準，而且最終仍需交由司法機關依個案情形進行最後裁決，而無法自行認定。因此較不建議以「無營利行為」為由，自行認定利用他人著作之行為，符合「合理使用」而主張免除相關責任。

【眾勤法律事務所副所長 陳全正律師 解答】以上資料摘自經濟部智慧財產局 原創我挺你 FB

更多相關訊息可連結

經濟部智慧財產局 原創我挺你

FB(https://www.facebook.com/copyright.com.tw/)

四、如果是以他人自製遊戲裡的某個 logo 作為週邊的話，算不算侵權呢?

A4 :

一、使用他人美術著作，原則上應取得著作權利人同意為宜。

（一） 首先應說明的是，LOGO 如符合「原創性」（為獨立創作且非抄襲而來）及「創作性」（需具有最低創作高度）此二要件，則能受著作權法保護，屬於「美術著作」。（可參考：智慧財產局函釋電子郵件 1080530b）。

（二） 在 LOGO 受著作權法保護的前提下，如將 LOGO 製作為週邊商品，則涉及「改作」、「重製」等利用他人著作之行為，且屬於商業用途，建議應獲得權利人同意授權，使用上才比較不具風險（違反著作權法需承擔民、刑事責任）。

二、使用他人商標，應先取得商標權人同意，以免遭司法訴追。

（一） 另應提醒的是，此次所詢問題，應一併留意「商標權」議題。因商業實務上，LOGO 時常註冊為商標權，如將他人商標製作為週邊商品，涉及「商標商品化」議題。而遊戲廠商將遊戲裡面的 logo、名稱註冊成商標，以強化保護，也是常見的策略（例如，先前暴雪【blizzard】就因遊戲「魔獸世界」中被廠商抄襲 logo 等提起商標等訴訟）。

（二）「商標商品化」議題中，關鍵在於是否屬於「使用商標」，進而認定有無侵害他人商標權。實務上之判斷基準為「交易過程中，將他人商標進行商品化之功用為使消費者可以辨識商品來源，並且以此作為行銷目的」（可參考：智慧財產法院 106 年度刑智上易字第 14 號判決意旨）。實務上亦有認為如果消費者對於商品來源或授權關係產生混淆或誤認的情形，即構成商標權侵害，例如未經權利人同意，便將知名精品商標如 CHANEL、GUCCI、YSL 英文字樣商標製成耳環、胸針等飾品，法院即認為此種行為使消費者誤認飾品係來自於商標權人，屬商標權侵害（可參考：臺灣臺南地方法院 108 年度智易字第 28 號判決）。

（三）綜合上述說明，將他人已註冊商標之 LOGO 製作為週邊商品，若屬於「使用商標」行為，應先取得商標權人同意，以避免侵害商標權（違反商標法同樣需承擔民、刑事責任）。

三、最後須留意的是，LOGO 是否具有「創作性」而可否受著作權法保護、LOGO 商品化是否為「使用商標」皆需由司法機關進行最後裁決，而無法自行認定。

【眾勤法律事務所副所長 陳全正律師 解答】

以上資料摘自經濟部智慧財產局 原創我挺你 FB

更多相關訊息可連結

經濟部智慧財產局 原創我挺你

FB(https://www.facebook.com/copyright.com.tw/)

資安暨個資宣導

一、政策宣導

『國立虎尾科技大學資通安全管理政策』

https://nfucc.nfu.edu.tw/images/pdfs/IMS-M-001.pdf

『國立虎尾科技大學個人資料保護管理政策』

https://www.nfu.edu.tw/images/IMS-M-003.pdf

『國立虎尾科技大學資通安全暨個人資料保護推動委員會設置要點』

https://nfucc.nfu.edu.tw/zh/nfu-pims/2020-01-17-08-40-12

本校資安通報聯絡方式：network@nfu.edu.tw

二、新聞快遞

(1)駭客以 Google 表單作為網釣跳板，竊取 AT&T 憑證

美國行動安全業者 Zimperium 於本周警告，有一群駭客專門利用 Google 表單（Google Forms）進行網釣攻擊，他們假冒逾 25 種品牌發出問卷調查，但要求使用者必須先輸入憑證才能提交問卷，以搜刮受害

者的憑證，而在這波攻擊中，有接近 75%的目的是為了獲取 AT&T 或是 AT&T 與 Yahoo 聯名的 AT&T-Yahoo 網路服務登入憑證。

Google 表單為 Google 所提供的調查管理軟體，它與 Google 文件(類似 Office 的 word 文件)、Google 試算表(類似 Office 的 Excel)及 Google 簡報(類似 Office 的 Power point 文件)的都是屬於 Google 編輯器的功能，可以透過問卷調查蒐集使用者的意見，並將結果自動匯入試算表。

在相關的攻擊中，駭客偽裝成超過 25 個不同的品牌，除了 AT&T 之外，被假冒的品牌還有 AOL、花旗銀行、Google 文件(類似 Office 的 word 文件)、Microsoft OneDrive、Microsoft Outlook、Office 365、T-Mobile 及 Zimbra 等，在使用者填完問卷之後要求使用者輸入憑證以提交問卷。

迄今已有愈來愈多合法服務被駭客濫用以作為網釣攻擊的跳板，Google 文件(類似 Office 的 word 文件)也因類似的原因受到駭客青睞，例如它解決了由駭客代管的網域問題，而且透過合法網域還能躲避偵測，不過，熟悉 Google 文件(類似 Office 的 word 文件)的使用者就會知道，Google 曾經呼籲千萬不要透過 Google 表單提交憑證。

此外，在使用者填入憑證之後，駭客還把「登入」(Login) 的字眼改成「提交」(Submit)，以避免引起使用者的猜疑。

Zimperium 指出，過去用來辨識是否為網釣頁面的 HTTPS 協定可能不再那麼有效，因為現在的網釣攻擊中，採用 HTTPS 安全傳輸的比例已達到 60%，遠高於去年初的 12%。

資料來源：IThome

https://www.ithome.com.tw/news/140968

(2)某大學資安大出包！5年學生個資寄給200人

大學校園內學生來來去去，每所學校人數高達數千上萬人，每學期還有新舊學生交替，但大學校園傳出學生個資全部外洩，兇手還是自家學校的通識中心，校方表示，「他也是新進人員，因為夾檔他選錯了，實在也是無心之過。」。

有學生收到通識中心寄來的講座通知電子信，發現有附件好奇打開，赫然發現裡頭竟然是 104~108 學年度，所有入學學生的個人資料，就這樣隨信夾帶，寄送給 200 多位收件者，裡頭除了身分證手機等基本資料，就連入學方式和身分註記都有，學生個資全都露，校方回應「未來做好加密的動作，再來後端也要微控發送 email 或其他途徑，學校有沒有可能攔截的，有個資疑慮的，學校覺得很抱歉。」

學校發現後承認疏忽，將會召開會議深切檢討究責，承諾未

來將嚴格把關，但寄出的信件如同覆水難收，就怕學生個資遭到有心人士利用甚至犯罪，亡羊補牢，恐怕已經來不及。

因此提醒本校同仁遞送郵件前，請再次確認郵件內容，如有含有個資資料，請記得將檔案加密傳送。

資料來源：YAHOO!新聞

https://tw.news.yahoo.com/%E4%B8%AD%E6%AD%A3%E5%A4%A7%E5%AD%B8%E8%B3%87%E5%AE%89%E5%A4%A7%E5%87%BA%E5%8C%85-5%E5%B9%B4%E5%AD%B8%E7%94%9F%E5%80%8B%E8%B3%87%E5%AF%84%E7%B5%A6200%E4%BA%BA-061633536.html?guccounter=1

(3)資安廠商公布 2020 年最多人使用的前 200 組密碼

資安廠商公布 2020 年全球網友最常使用的 200 組密碼、這些密碼被洩漏的次數，以及駭侵者破解這類密碼所需的時間；**同時呼籲大眾不要使用這些常見密碼**。

資安廠商 NordPass 日前發表研究報告，公布該公司觀測到的**2020 年全球網友最常使用的 200 組密碼**。網友最常使用前十大密碼，以及駭侵者破解這類密碼所需的時間，分別如下表：

編號	最常使用密碼	破解密碼所需時間
1	123456	1 秒內
2	123456789	1 秒內
3	picture1	3 小時
4	password	1 秒內
5	12345678	1 秒內
6	111111	1 秒內
7	123123	1 秒內
8	12345	1 秒內
9	1234567890	1 秒內
10	senha （西班牙文的「密碼」）	10 秒

在報告中，NordPass 也分析的這些常用密碼的類型，包括易記的數字組合、人名、常用裝置名稱、運動名稱、食物名稱、熱門遊戲或電影片名或主角名稱、勵志或罵人語句、鍵盤上字母與數字的排列順序，甚至就是「密碼」這個字的拼法等等。

NordPass 呼籲大眾，在**設定新密碼時**，除了**避免使用這些常見密碼**，並使用**超過 12 個字元、混合使用大小寫字母、數字與特殊符號的強式密碼**之外，為避免密碼不好記，也應**使用密碼管理工具**，並**設定多階段登入驗證**。

資料來源：TWCERT/CC

https://www.twcert.org.tw/tw/cp-104-4173-b8050-1.html

(4)臉書修補 Messenger 上可遭竊聽的安全漏洞

Google Project Zero 發現的一項安全漏洞，讓登入 Messenger 的駭客在撥電話給 Android 版 Messenger 用戶的同時也傳送一個特製訊息，一旦受話方也同時在二個裝置登入同一帳號，即使該用戶未接聽，駭客便能在響鈴時聽到對方的聲音，臉書針對該漏洞提供 6 萬美元的獎勵金

臉書在本周公布了自 2011 年執行抓漏獎勵專案（Bug Bounty Program）意外揭露了一個藏匿**在 Messenger 上的安全漏洞**。

根據臉書的統計，這 10 年來全球總計有超過 5 萬名研究人員加入該公司的抓漏獎勵專案，其中是由安全研究人員 Selamet Hariyanto 所揭露的內容遞送網路（Content Delivery Network，CDN）漏洞，此一 CDN 是一個由臉書全球多個伺服器所組成的網路，可供應內容予臉書的全球用戶， Silvanovich 提報的是一個藏匿在 Messenger 上的漏洞，**登入 Messenger 的駭客撥電話給受害者時，只要同時傳送一個客製化的訊息，且受害者同時開啟了 Android 上的 Messenger 與另一個同帳號的 Messenger（例如網頁版），即使對方未接聽，也能在響鈴時聽到對方的聲音**。

這個漏洞出現在 Facebook Messenger 在實作 WebRTC 網路影音傳輸協定時發生的錯誤，受此漏洞影響的 Facebook Messenger for **Android 版本為 284.0.0.16.119 與較舊的所有版本**。

Natalie Silvanovich 在提報給 Facebook 的資安漏洞通報中，也提供了重現此漏洞的詳細操作步驟。值得注意的是，欲利用這個漏洞進行攻擊的駭侵者，必須擁有和受害者透過 Facebook Messenger 通話的權限，也就是說必須是受害者的朋友，或經受害者同意透過 Facebook Messenger 通話。

Facebook 於 10 月 6 日時接獲 Natalie Silvanovich 的資安漏洞通報，隨即於 11 月 17 日推出修復此漏洞的更新版本；所有在 Android 裝置上使用 Facebook Messenger 的用戶，應即更新至最新版本，以避免遭此漏洞攻擊。

資料來源：IThome、TWCERT/CC

https://www.ithome.com.tw/news/141252

https://www.twcert.org.tw/tw/cp-104-4176-2d944-1.html

三、資訊科普小知識

拿到嫌犯的手機了，然後呢？想抓到罪證可沒那麼簡單！初探數位鑑識的奧祕

智慧型手機已然成為人們生活中不可或缺的一部份，舉凡記

事、行程提醒、影音娛樂、購物消費、社群聊天、導航等等，皆可一機搞定滿足食衣住行育樂各種需求。正因為如此，我們使用智慧型手機過程中所留存的各種資訊，其實就約等於使用者日常生活的紀錄。

試想看看，倘若鑑識人員可以拿到嫌疑犯的智慧型手機（以下簡稱為手機），是不是就可以知道找出嫌疑犯的各種生活小細節呢？由此可知，手機的取證，已經逐漸成了犯罪調查的重中之重。**只要能有效提取手機裡的各項跡證，便有助於釐清有無與案情相關之處！**

犯罪調查中的重點：智慧型手機！

對鑑識人員而言，雖然手機與電腦同樣都可以當作證物，卻有著很大的差異。桌機、筆電的硬碟是可以拆卸的，然而手機是使用快閃記憶體（Flash）來儲存資料，而且直接焊在電路板上，再加上手機只有一個 USB 埠可資利用的情況之下，如何自手機中提取跡證，便成了鑑識人員的一大挑戰。

簡單流程如下：

首先，打開手機與工作站的 USB 通道→拿來控制手機的「遙控器」：ADB，ADB 的主要作用在於建立手機跟工作站之間的基礎信任關係！但是這份基礎的信任關係是指系統最高權限的使用，文章內容明確說明手機持有人跟系統最高權限的差異，當取得系統最高權限，就可以調閱使用者的在這個手機上留下的資料。

鑑識的奧義：永不言棄，突破手機的「心防」！

透過鑑識人員與手機之間的「攻心大戰」中，想必讀者們對於智慧型手機的取證有了初步的了解，一窺鑑識人員不斷攻略手機的生活。

儘管面臨著重重難關及挑戰，鑑識人員從不輕言放棄，在巴掌大小的手機之間攻城掠地，力求掌握提取跡證的關鍵契機，為還原真相及打擊犯罪貢獻一己之力。

資料來源：泛科學
https://pansci.asia/archives/194360