**數位鑑識期末報告**

****

組別 第七組

組員

B0444254張嘉怡

B0444110徐宛萱

B0444227洪芝盈

B0444208曾妍菲

B0444105李品萱

壹、前言

一、案件情況說明

* 在一起涉嫌侵犯商業秘密案件中，A公司聲稱離職技術人員趙能嘉洩露了公司機密項目的技術資料。

* 現辦案機關委託鑑定機構對其工作電腦進行鑑定，以查找相關的證據。

* 現查明A公司的機密項目資料以“JMXM”加三位數字形式命名，存放在名為“JSZL”的文件服務器上，僅限公司內部局域網訪問。

* 公司要求員工的工作電腦不得訪問互聯網或私自外接存儲設備。

* 趙能嘉於2016年4月28日上午辦理了離職手續，4月29日交還了工作電腦。辦案機關於4月30日對趙能嘉的工作電腦進行了保全，製作了硬盤鏡像文件。

二、分析需求:

1. 證明有上網行為
2. 證明有瀏覽網路磁碟機
3. 證明有外傳資料
4. 非法資料存在本機
5. 非法資料存在外接裝置

三、需求解讀

使用工具: Autopsy

主要使用方法: keyword search搜尋

四、思考分析方式:

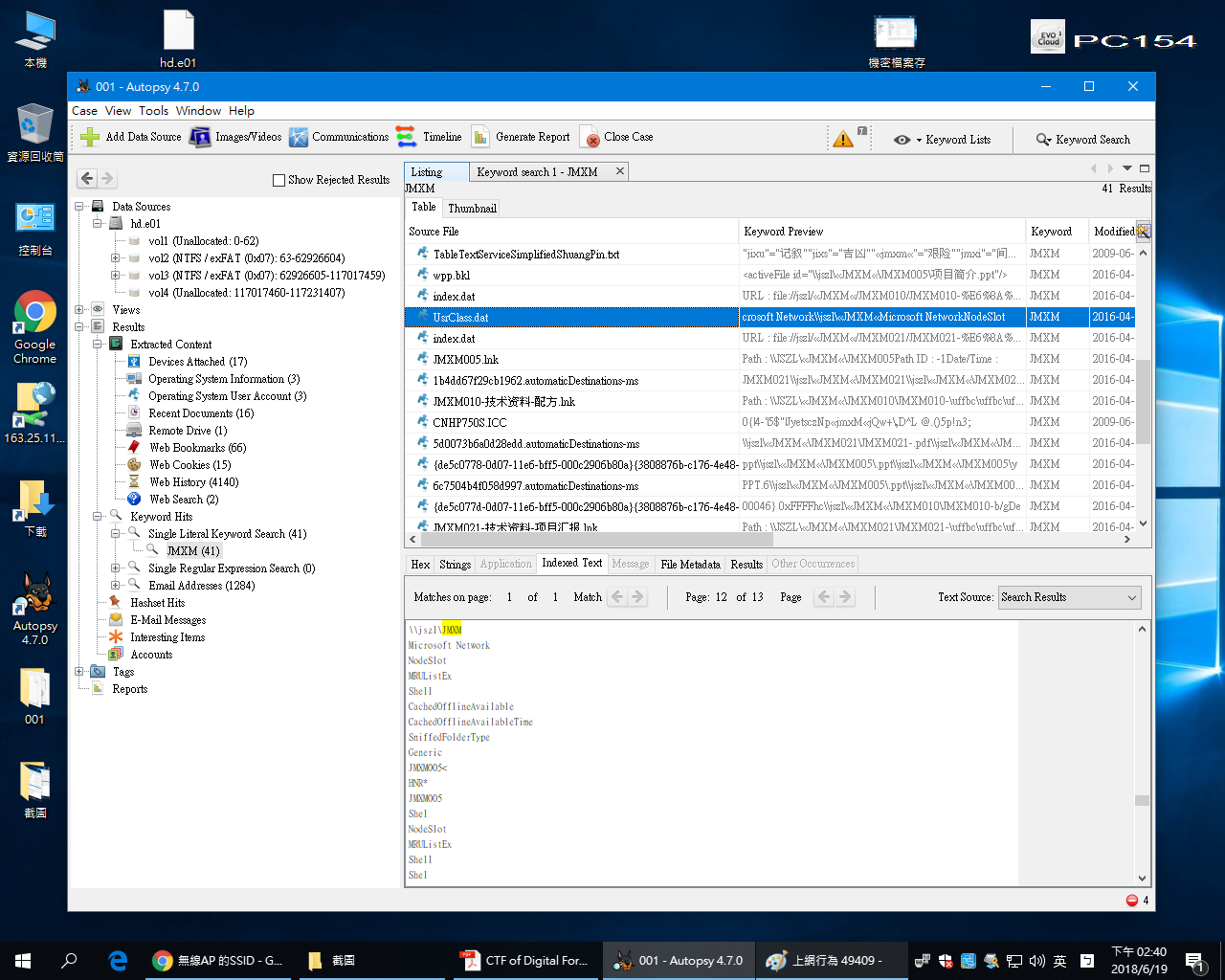
1. 由於我們每個人都比較熟悉autopsy的操作，因此決定大家皆使用autopsy作為工具，來尋找各個證據的所在位置。
2. 因為此題說明員工辦理完離職手續的時間為2016年4月28日上午，所以我們特別注意4月28日以後該員工所做出的各種行為。
3. 題目中提及現查明A公司的機密項目資料是以“JMXM”加三位數字形式命名，存放在名為“JSZL”的文件服務器上，因此，我們也特別留意有出現這兩組關鍵字的各個檔案和資料。

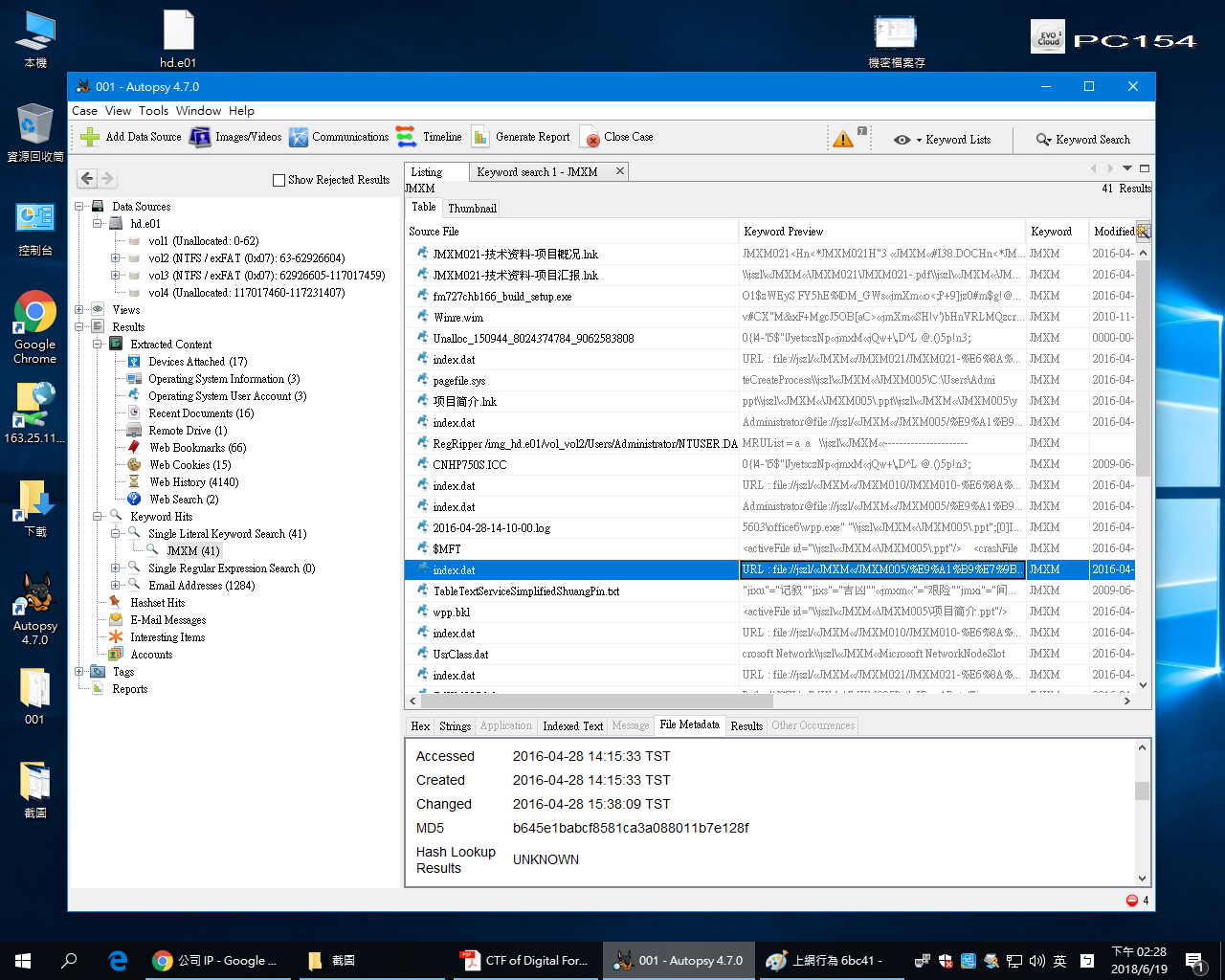
貳、解題過程

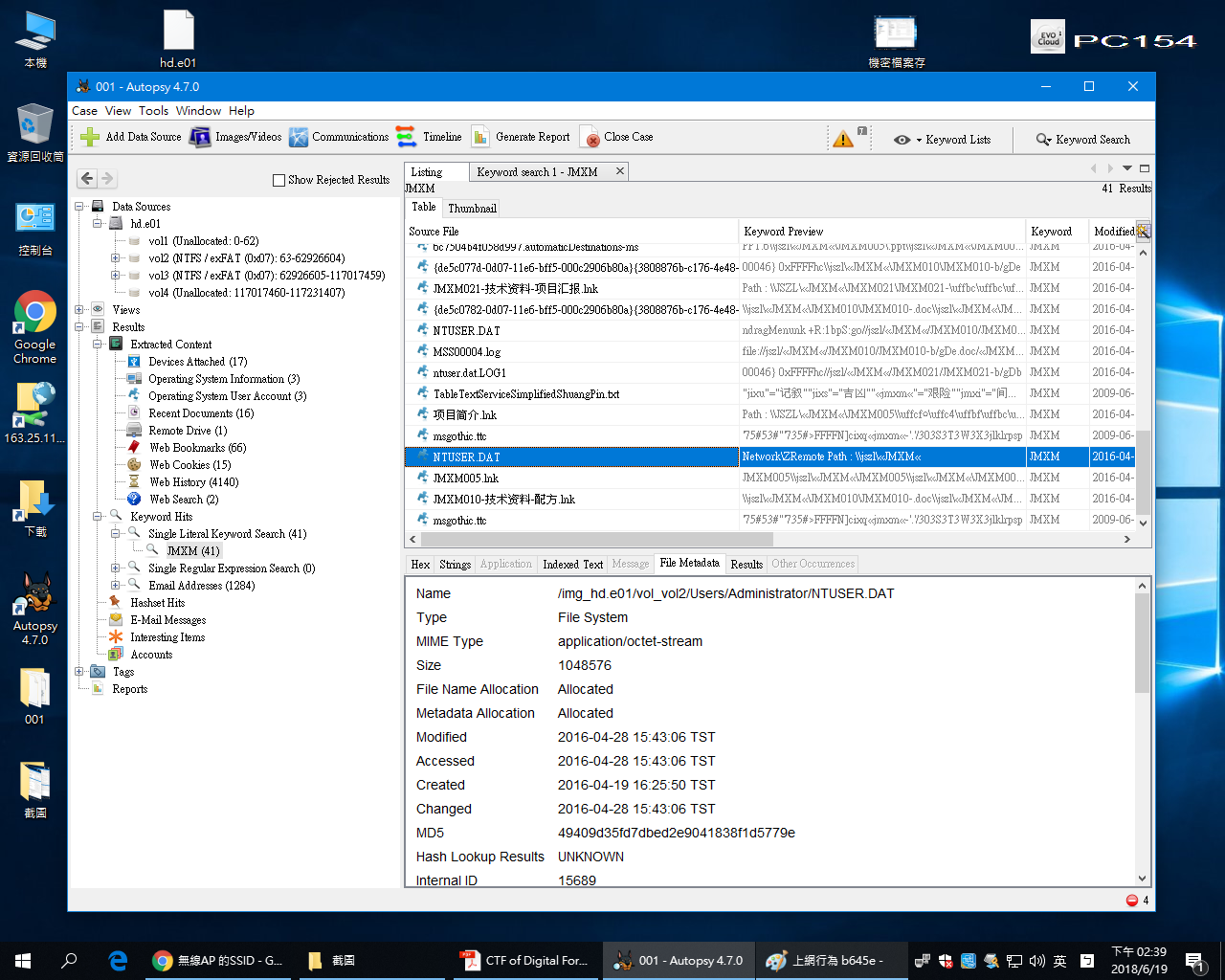
一、證明有上網行為

* 上網的行為非常多種，並非僅侷限於網頁和郵件，舉凡所有可使用的網路應用系統，例如 ERP 、PDM等資訊交換系統，都可以作為證明上網行為的一種證據。
* 在尋找上網行為的證明時，我們觀察到在web history 找尋日期為2016年4月的活動紀錄，比對之後找到.dat檔案，證明上網行為。



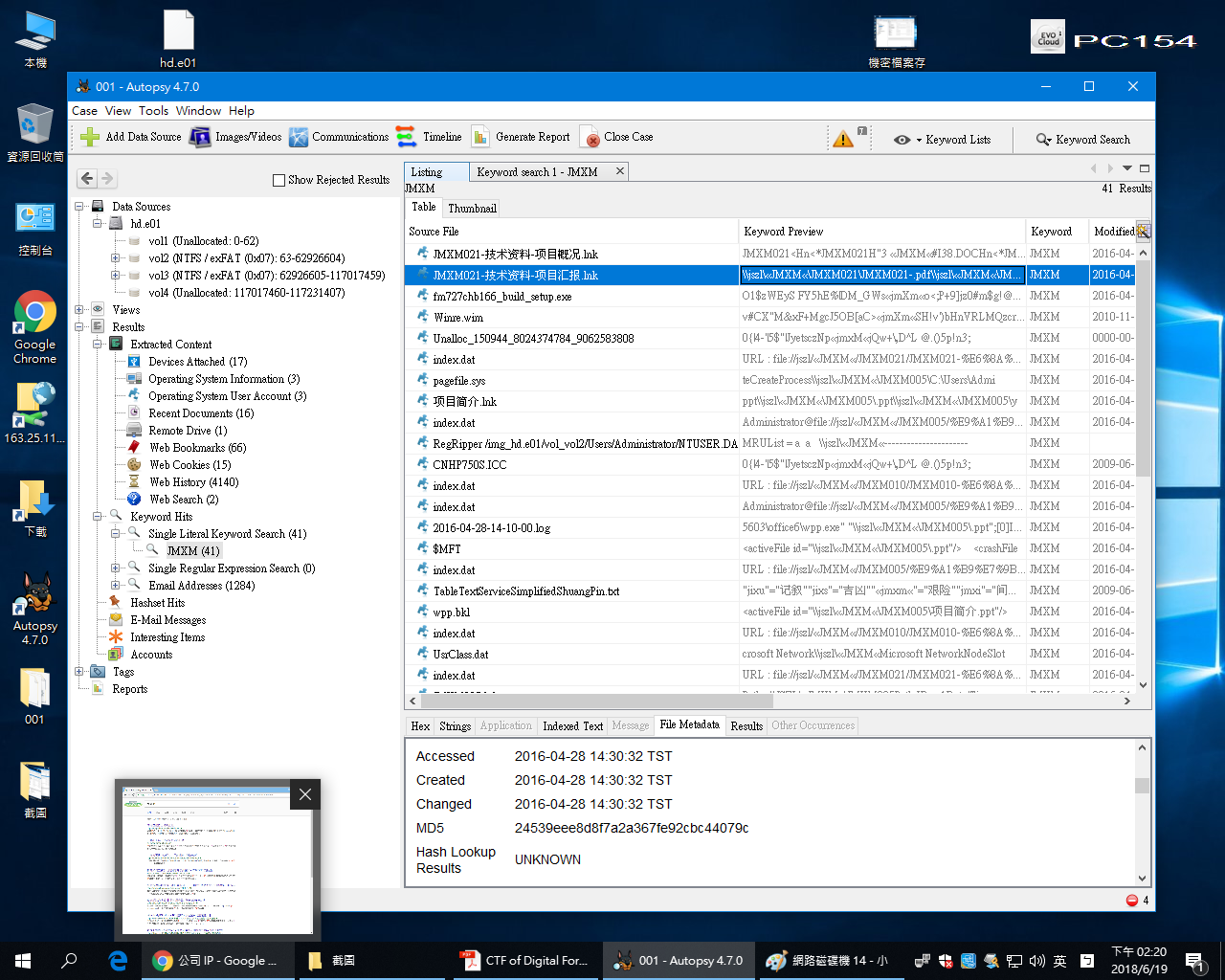




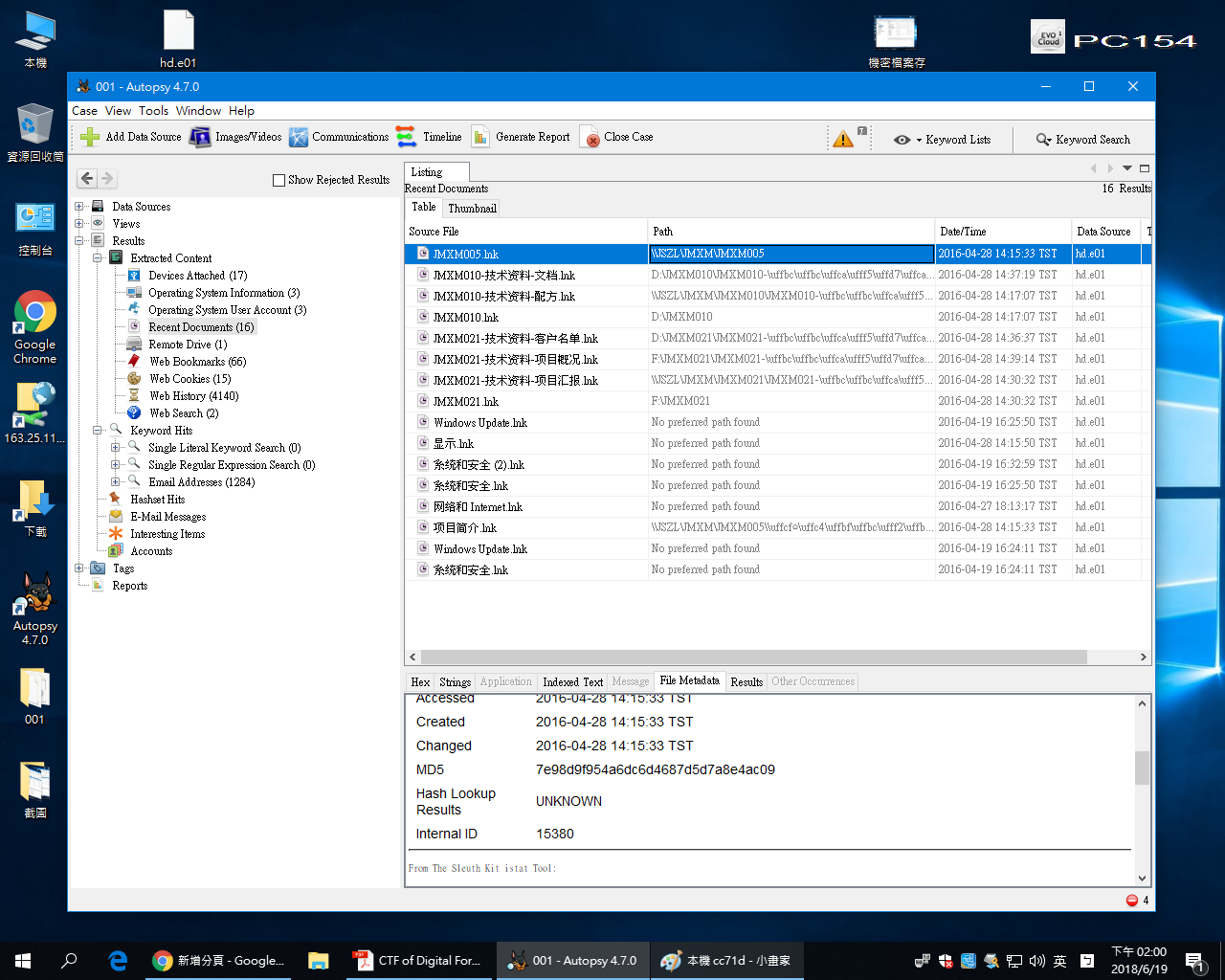


二、證明有瀏覽網路磁碟機

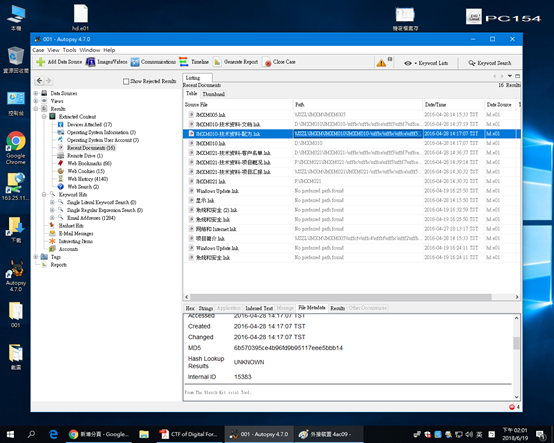
* 使用keyword search 以剛剛找到存在本機的公司機密檔名搜尋，搜尋結果中找日期接近的(2016年4月)，縮小搜尋範圍，找到更多更多儲存在本機的公司機密。
* JMXM021-技術資料-項目匯報:24539eee8d8f7a2a367fe92cbc44079c
* JMXM010-技術資料-配方: 6b570395ce4b96fd9b95117eee5bbb14
* JMXM005: 7e98d9f954a6dc6d4687d5d7a8e4ac09



證明有瀏覽網路磁碟機-4079c



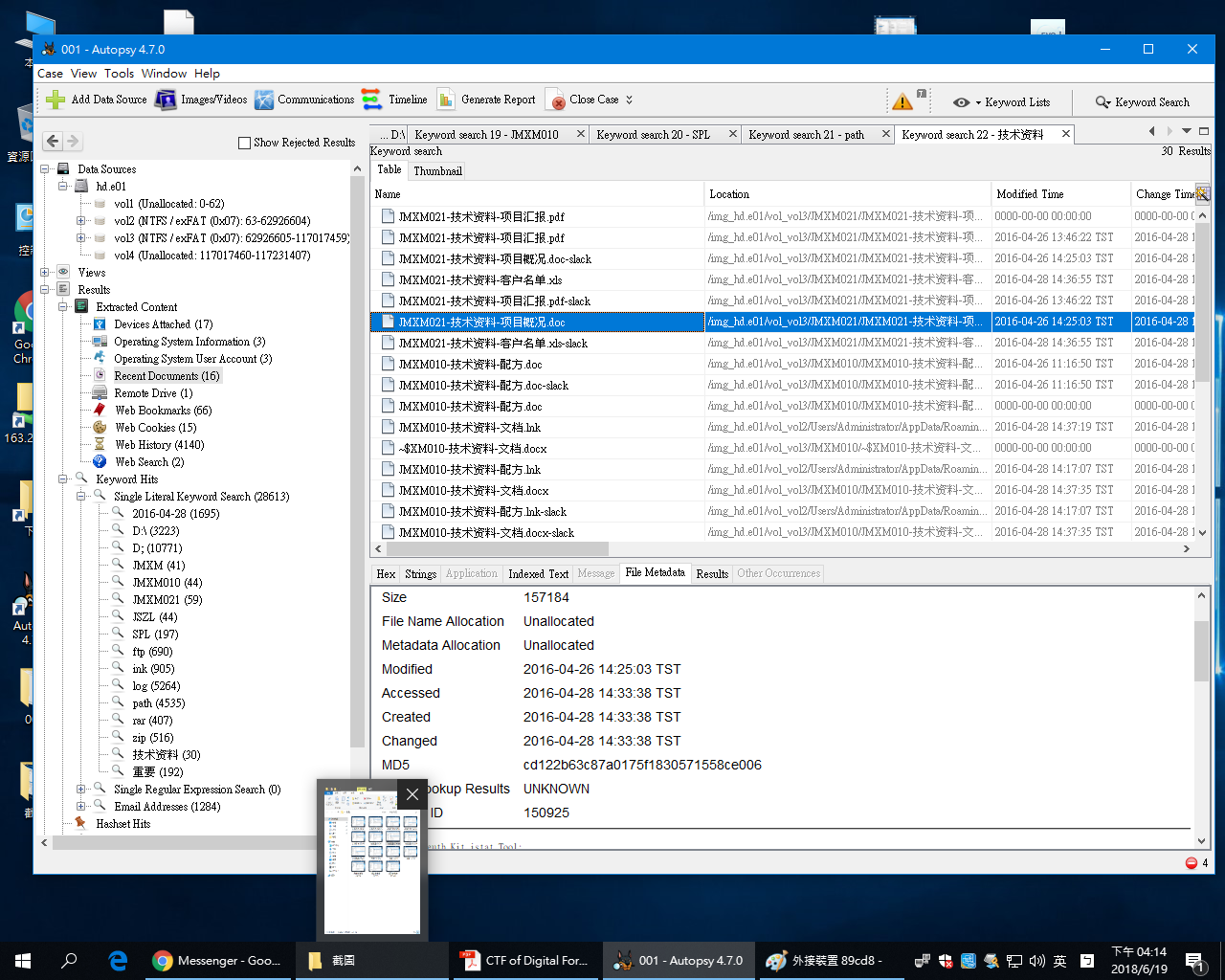
證明有瀏覽網路磁碟機-4ac09

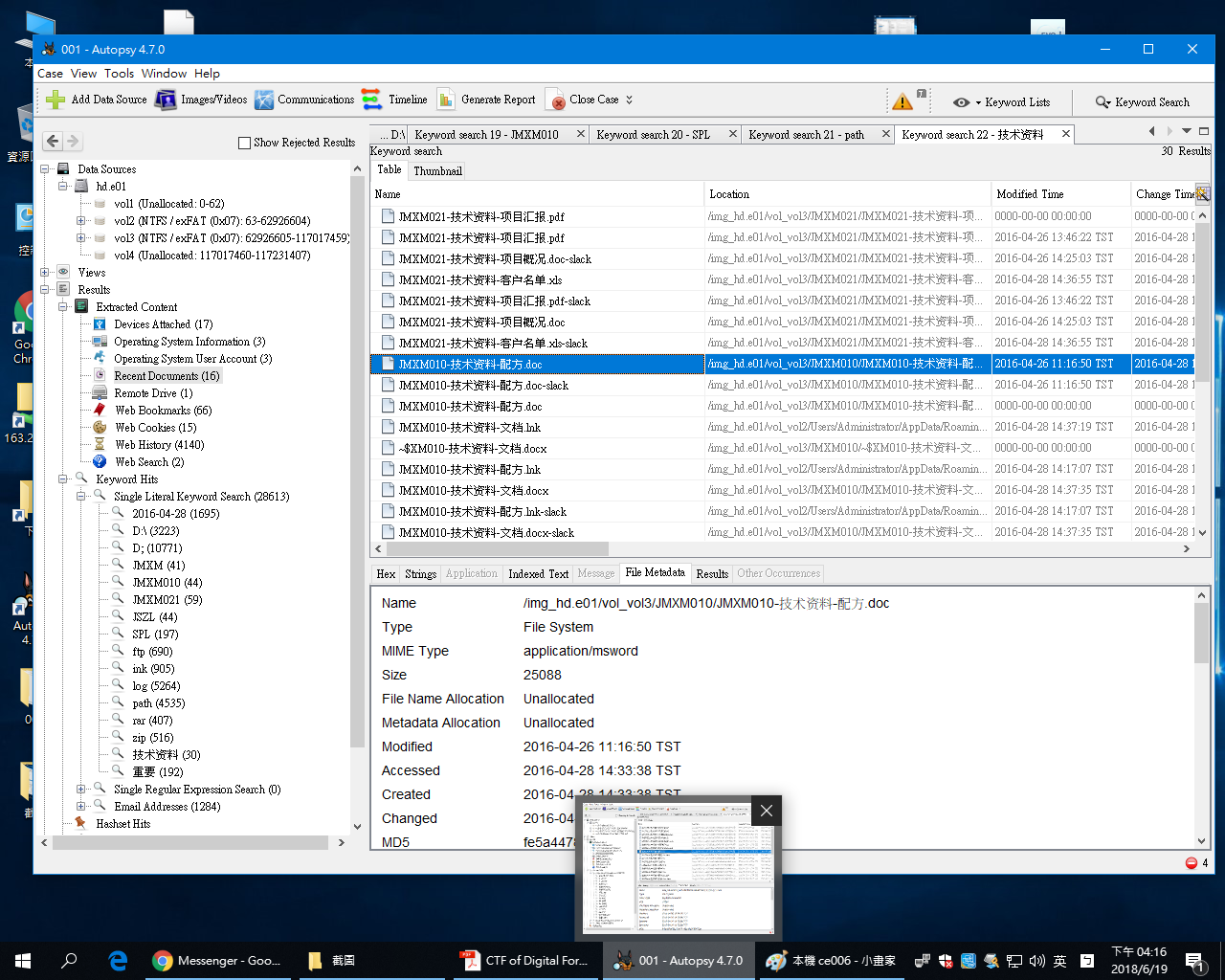


證明有瀏覽網路磁碟機-bbb14

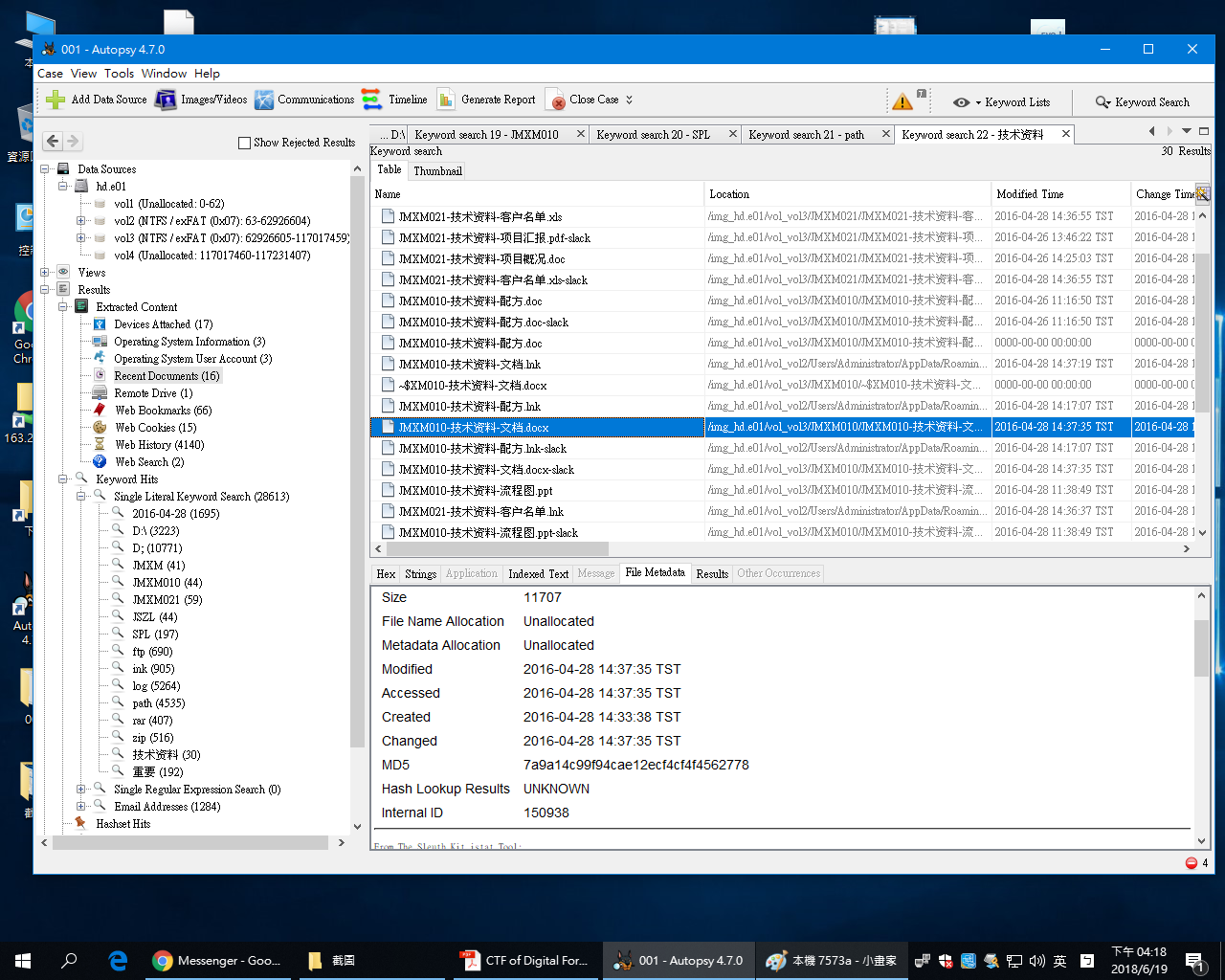
三、非法資料存在本機

* 先看recenting activity，看到有些資料傳送的日期是4月28且path在本機端或是外接裝置，覺得可疑，比對之後發現確實是符合題目要找的公司機密，另外網路磁碟機也是看path還有日期，在recenting activity裡找到。
* JMXM021-技術資料-項目概況:cd122b63c87a0175f1830571558ce006
* JMXM010-技術資料-配方: fe5a4478555234b57142e40a7397573a
* JMXM010-技術資料-文檔: 7a9a14c99f94cae12ecf4cf4f4562778
* JMXM021-技術資料-客戶名單:9f622f21c5b76b7a09fc6aef820cc71d
* 文檔.docx: 17a6e10b098a2baa42059bd8b901317c
* 客戶名單.xls: fa3a309b81002665006e96463f8f7f54
* JMXM010-技術資料-配方: fe5a4478555234b57142e40a7397573a
* JMXM010.lnk: d2eb5d987a9cab467e1dd7425c3cad1f

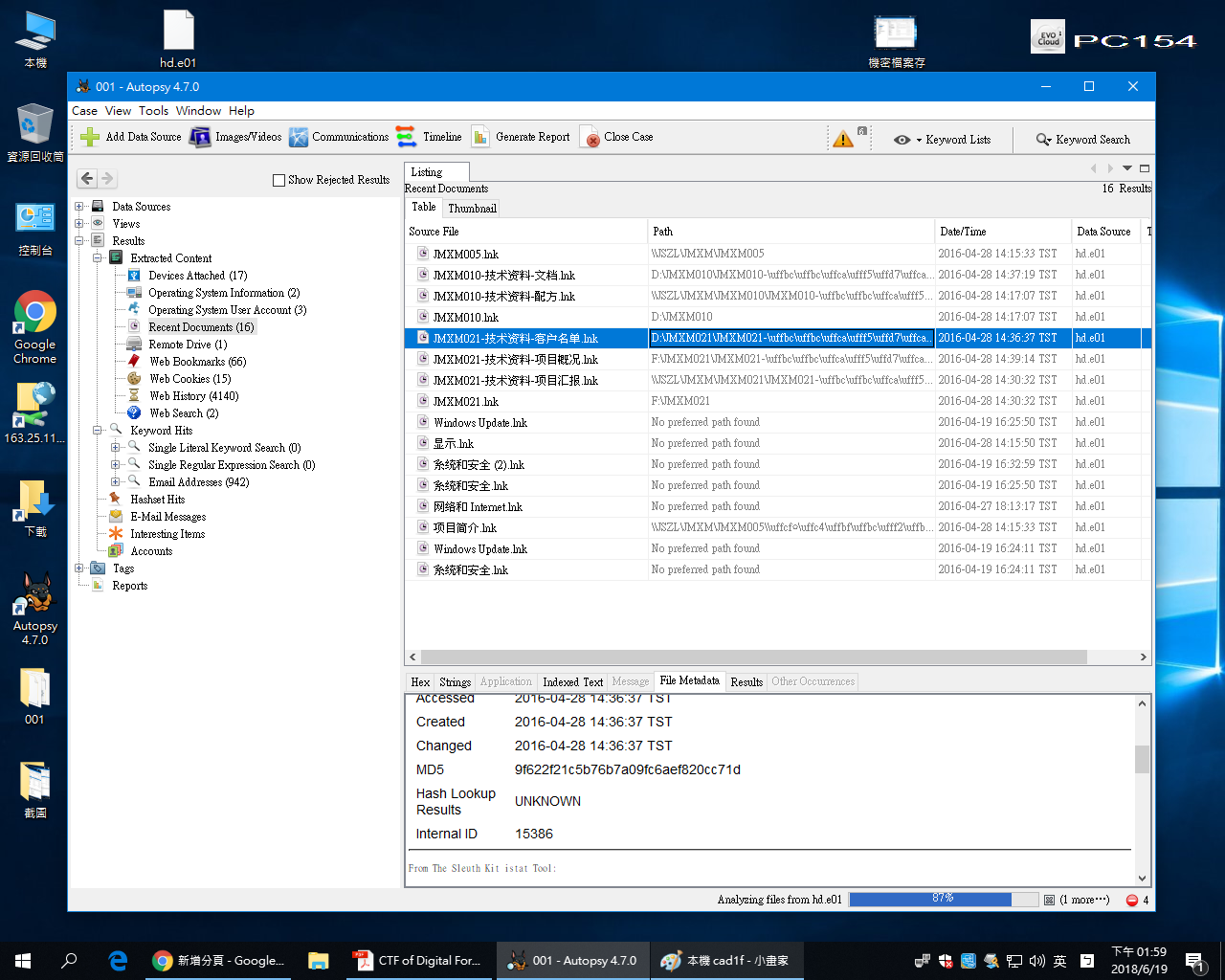
存在本機-ce006



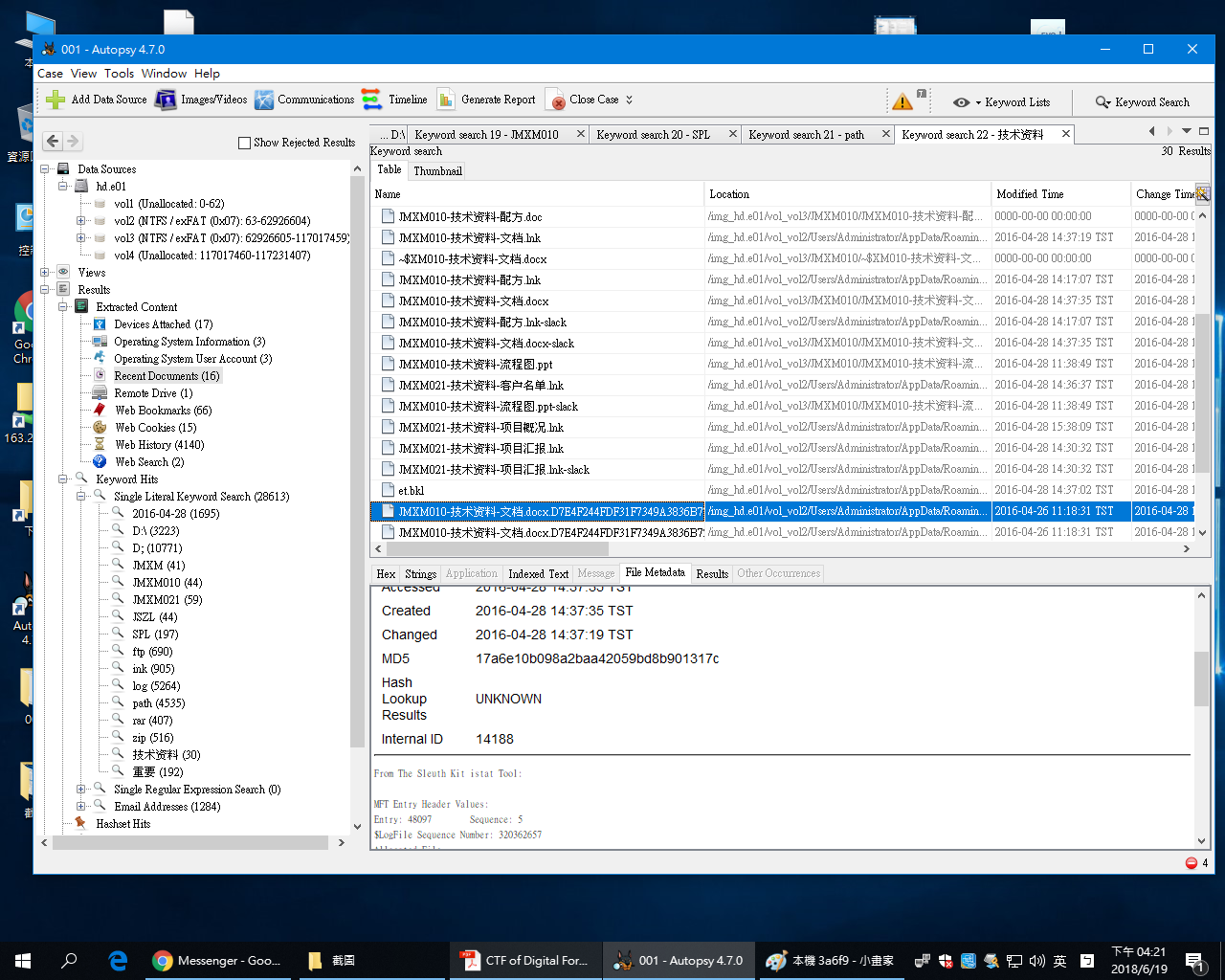
存在本機-7573a



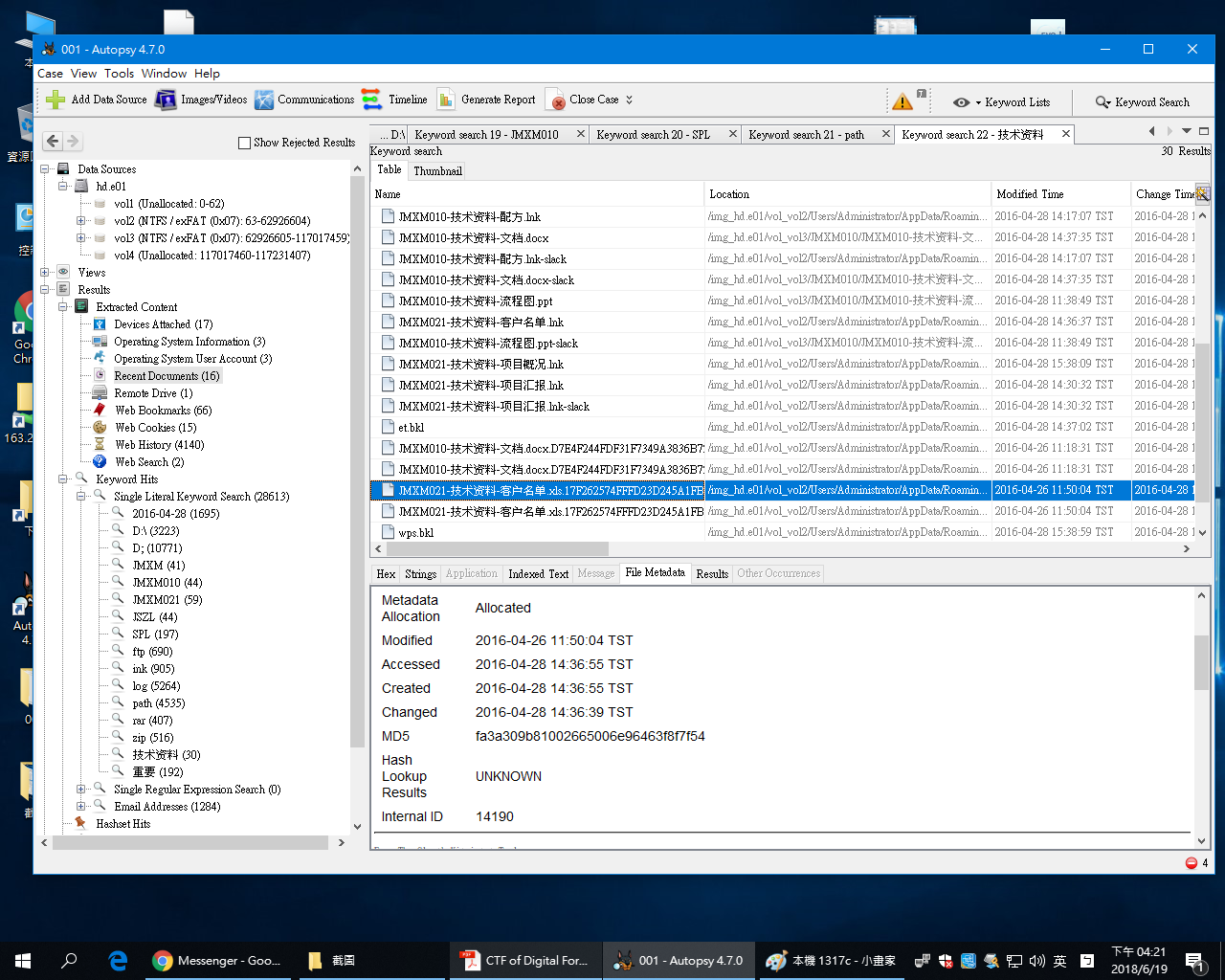
存在本機-62778



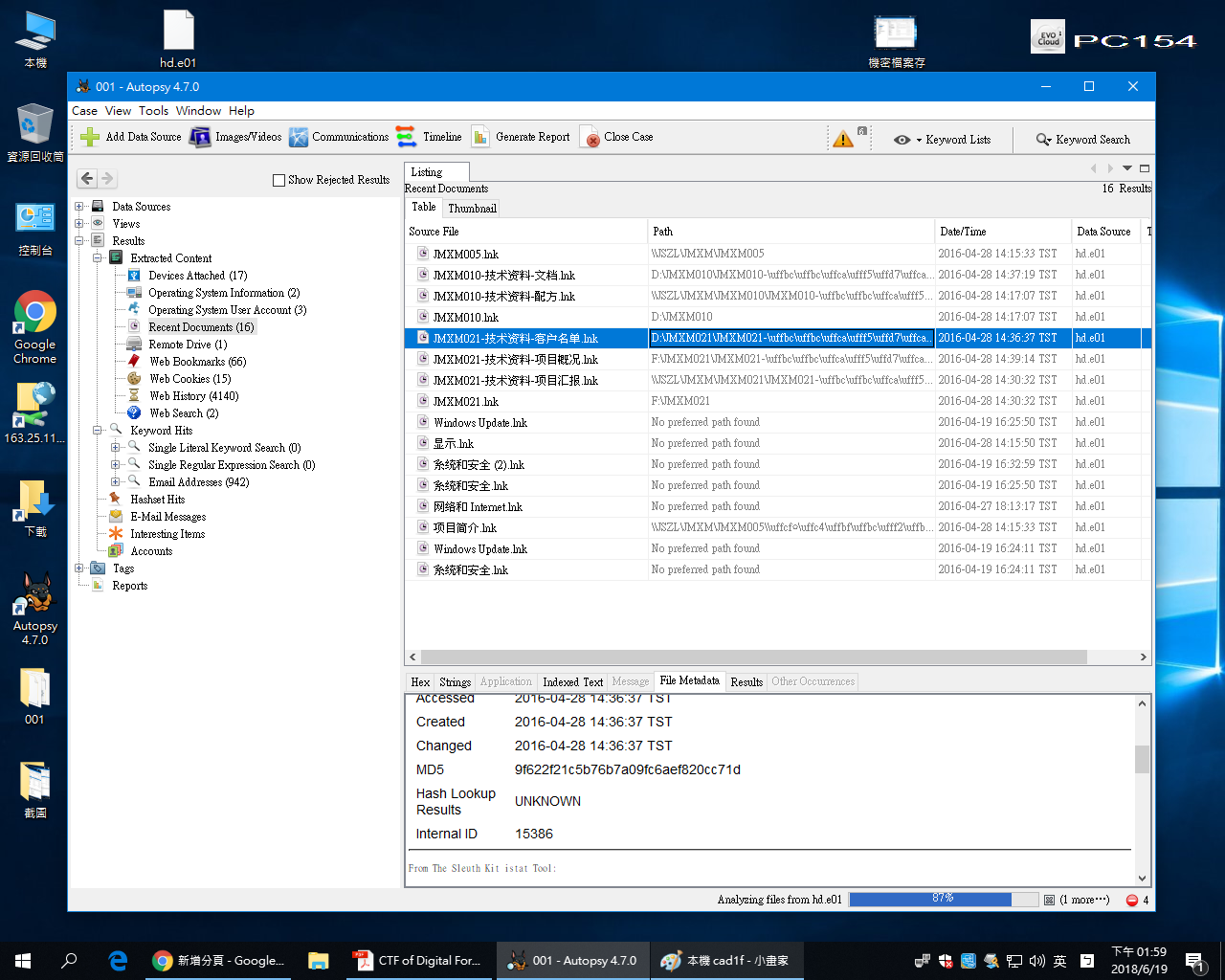
存在本機-cc71d



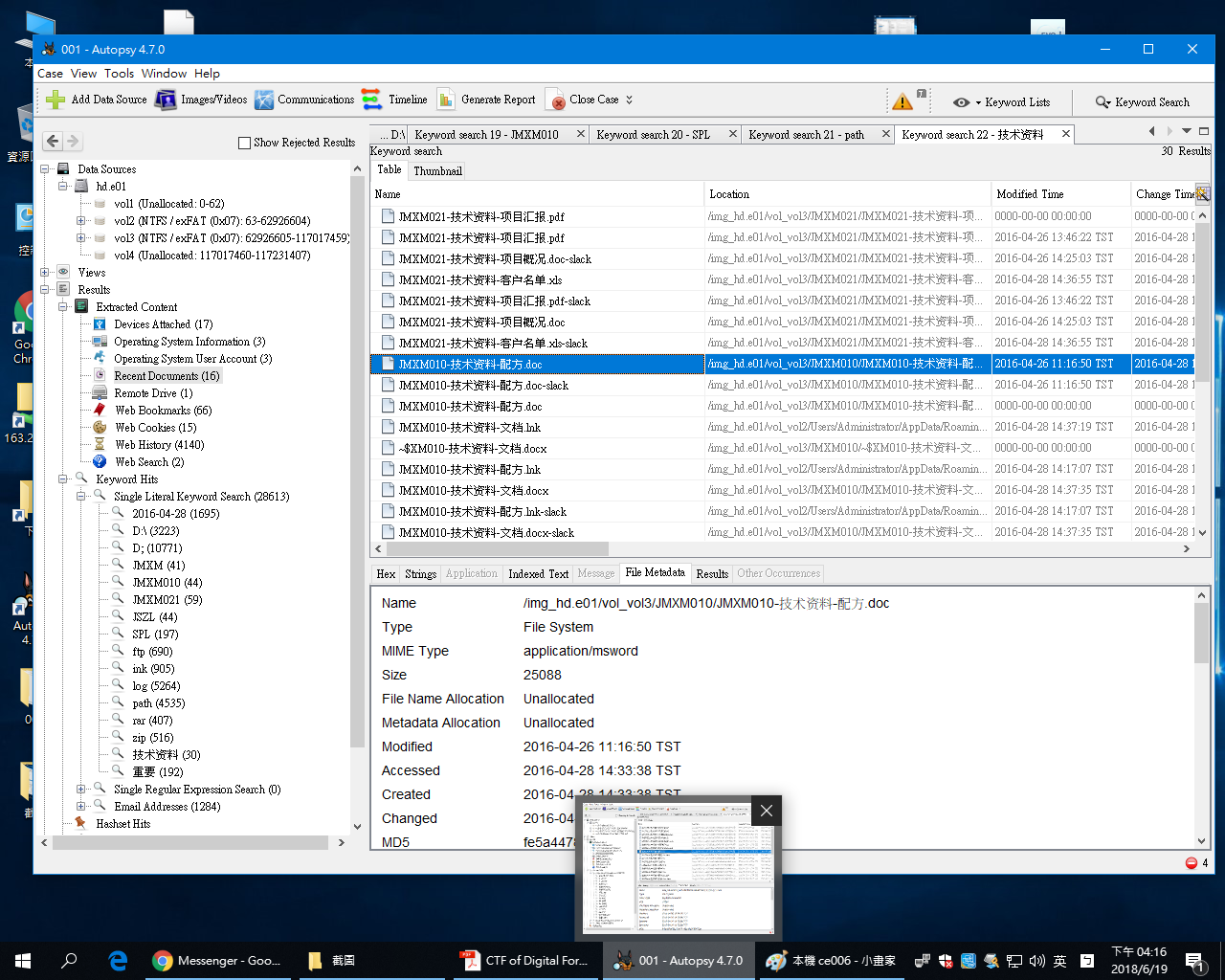
存在本機-1317c



存在本機-f7f54



存在本機-cc71d



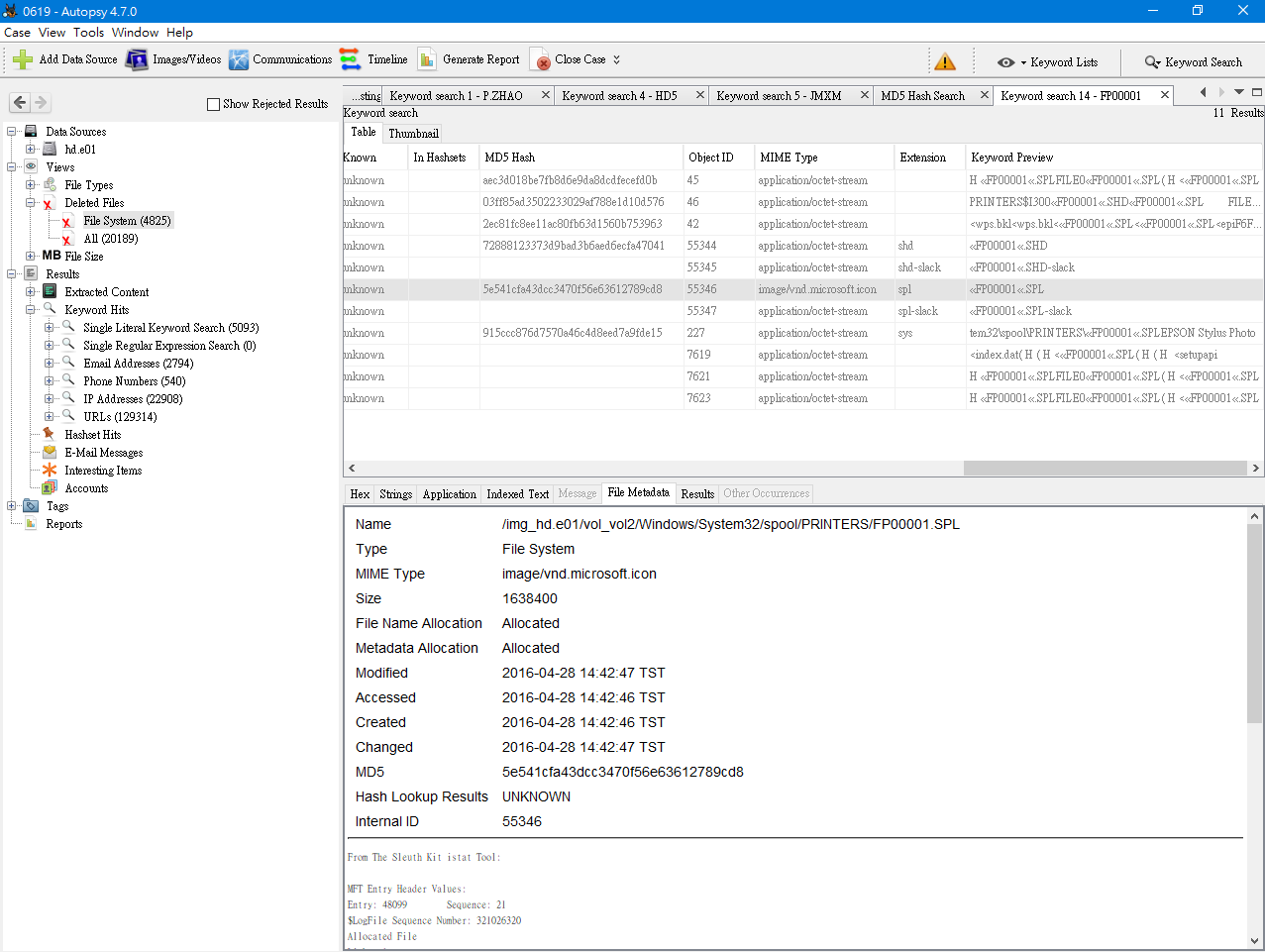
存在本機-7573a



存在本機-cad1f

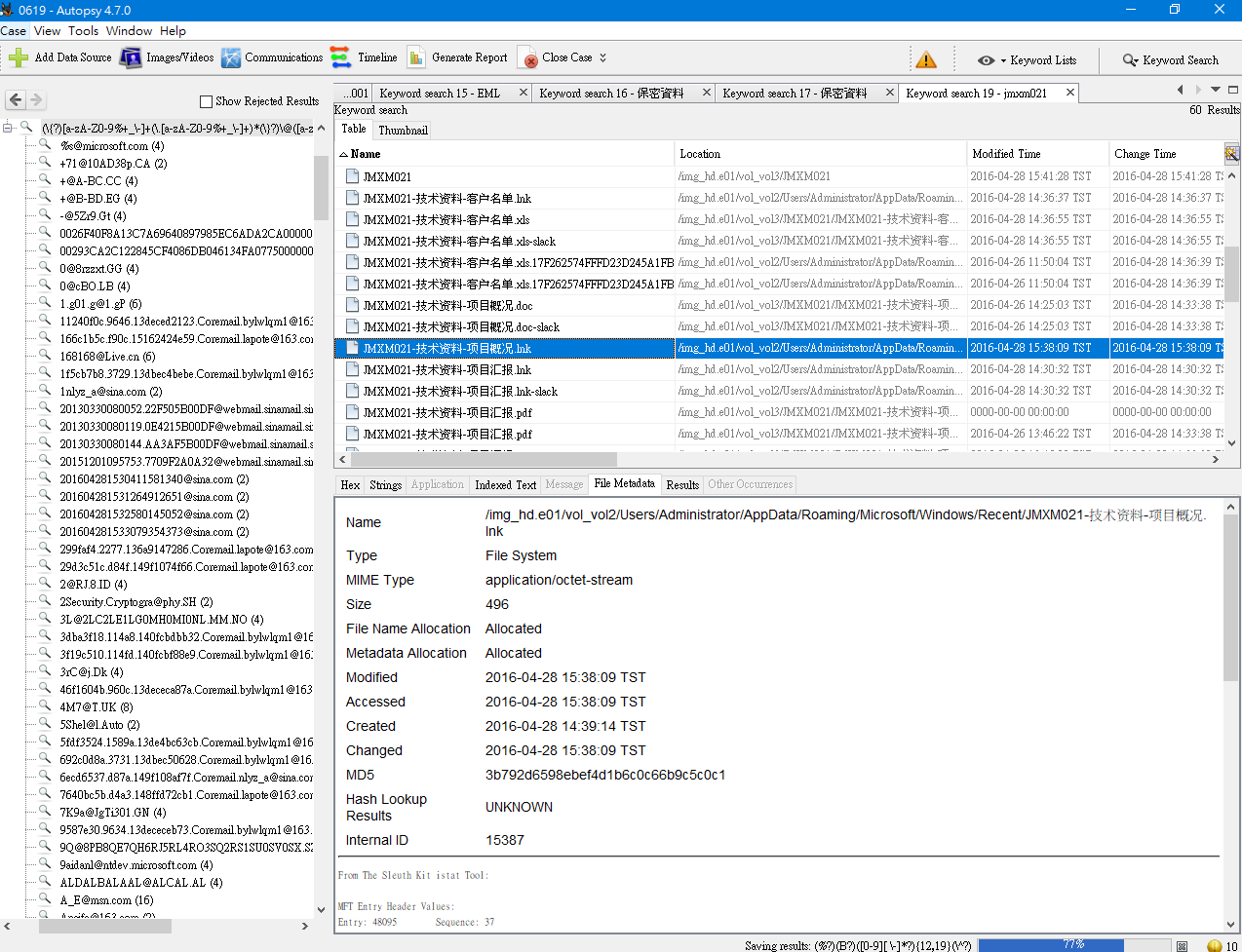
四、非法資料存在外接裝置

* 發現在有將資料燒錄到碟機F槽，並且在將列印的資料移到外接裝置上。



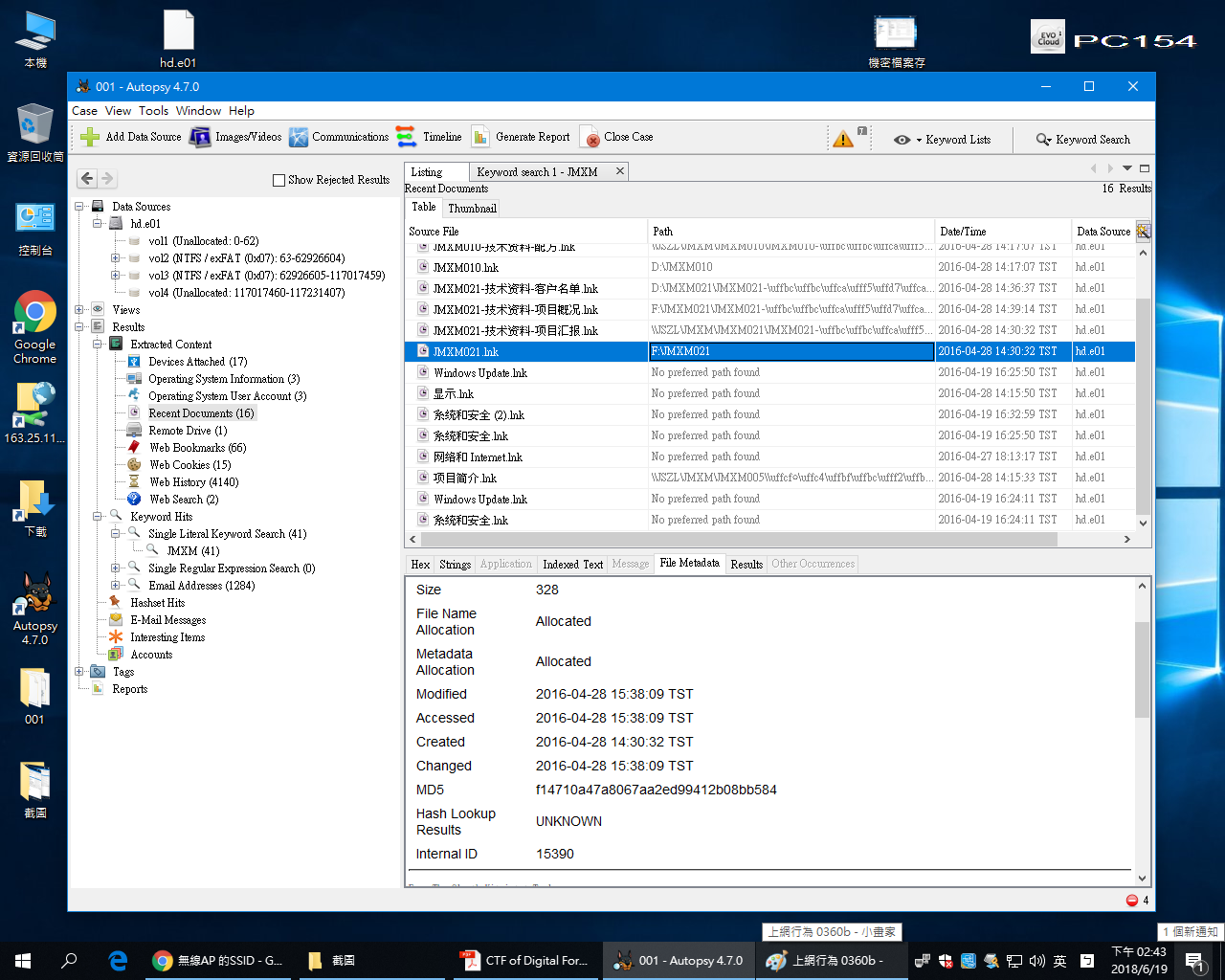
存在外接裝置-89cd8

MD5:5e541cfa43dcc4370f56e63612789cdf



存在外接裝置-5c0c1

MD5:3b792d6598ebef4d1b6c0c66b9c5c0c1

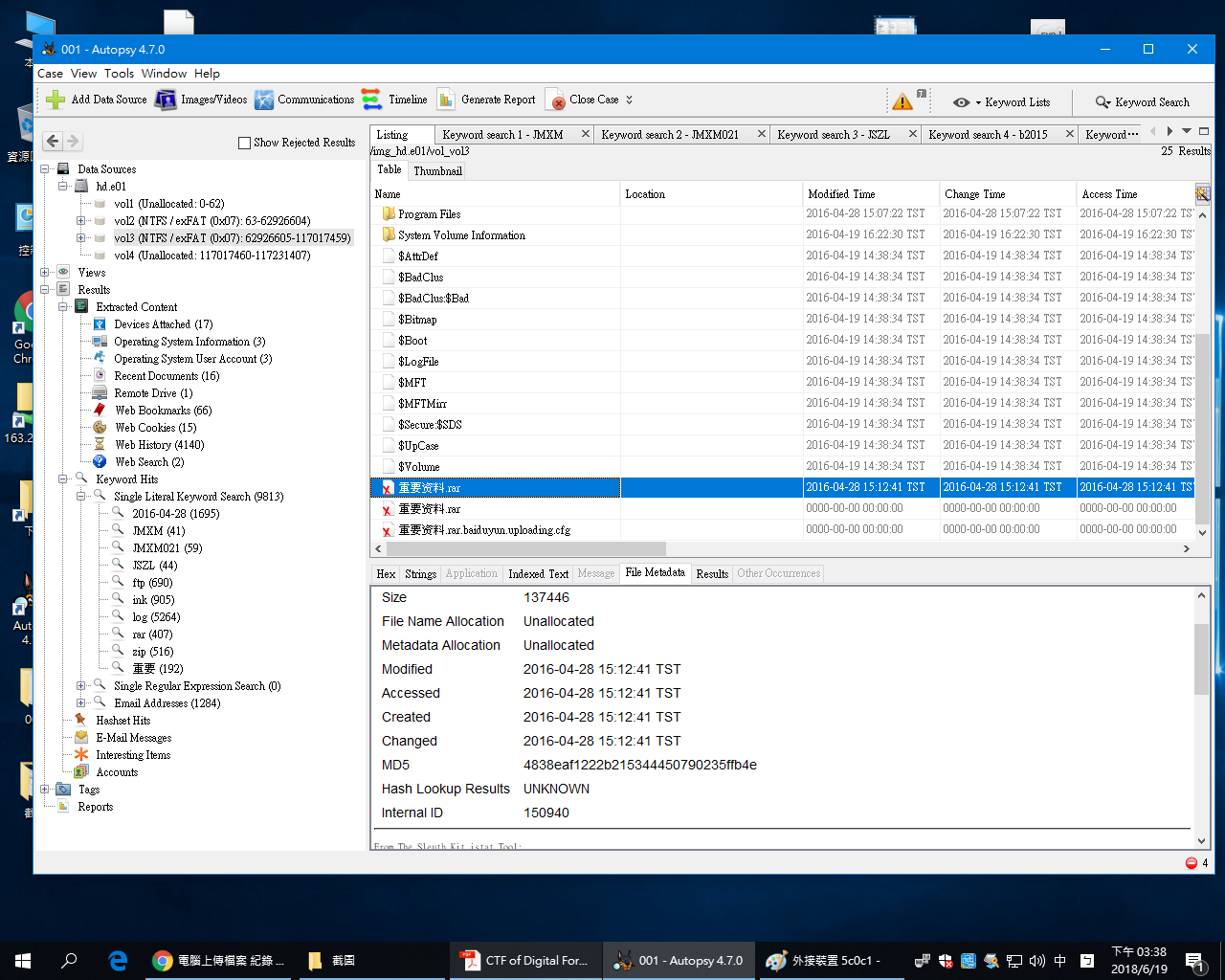


存在外接裝置-bb584

MD5:f14710a47a8067aa2ed99412b08bb584

五、證明有外傳資料

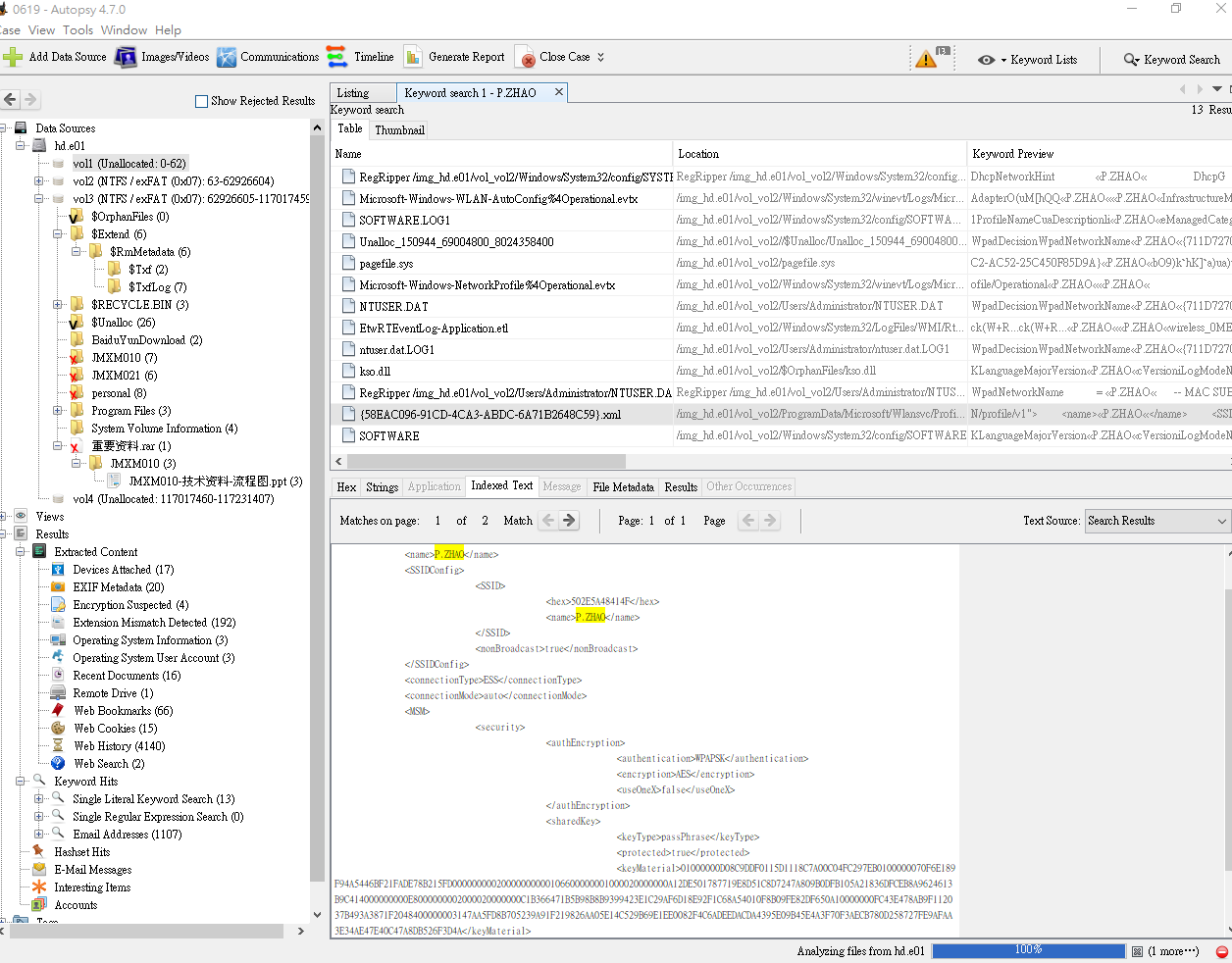
* 在email裡發現有外傳重要資料，可以當作證據。
* 重要資料:4838eaf1222b215344450790235ffb4e



證明有外傳檔案-ffb4e

六、額外加分

將遭刪除的D槽檔案復原後，發現其中有許多重要文件，而在電子信件內容中發現到SSID為P.ZHAO。(下圖截圖錯務！直接搜尋並非正確做法！)



SSID-P.ZHAO

參、心得：

此次的課堂解題，我們覺得非常的刺激有趣，雖然和前幾次的課堂解題方式差不多，都是要從眾多檔案及使用紀錄中找尋可能的犯罪證據，然而這次的解題多了遊戲競賽，先找到某一個證據的組別可以加分，使的整個過程又變得更加緊張，而且這次找到的證據多寡，也對我們的學期成績影響深遠，因此在這短短的150分鐘內，我們不敢有任何的疏失與時間浪費，全心投入於尋找證據。也因為競賽規則是越快找到答案的小組得分越高，因此當我們聽到別組說：「找到了！」，或是將小紙條遞給老師時，就使我們的心跳急遽加速。也更加體會到組員們分工合作的重要性，唯有清楚分工才能夠迅速且成功找到正確答案。

經過了一個學期的課程，獲得了許多收穫後，這次的分析方法以及思考模式都與我們所學沒有相差太多，也因此並沒有花費到極大量的時間，便能收穫滿滿。藉由學期上課的過程再搭配課堂實作，我們操作了各種不同的鑑識軟體，也對於不同軟體間的差異以及使用上的不同功能，有了初步的認知及了解。

在整個學期的尾聲，老師以分組競賽的方式進行實作。此種測驗的方式十分吸引我們。一方面可以測試自己上了那麼多個星期的課後，能不能靈活地運用所學找到所需的檔案。另一方面也發現有許多檔案會攜帶，甚至隱藏另一個檔案於原檔案中。實在是令我們意想不到啊！也希望往後這門課新穎的上課模式能繼續延續下去！

肆、分工說明**：**

* B0444254張嘉怡：尋找有上網的檔案、有瀏覽網路磁碟機的檔案、有外傳檔案存在本機的檔案、書面資料
* B0444110徐宛萱：尋找有上網的檔案、有瀏覽網路磁碟機的檔案、有外傳檔案存在本機的檔案、書面資料
* B0444227洪芝盈：尋找有上網的檔案、有瀏覽網路磁碟機的檔案、有外傳檔案存在本機的檔案、書面資料
* B0444208曾妍菲：成功尋找ｓｓｉｄ、尋找有上網的檔案、有瀏覽網路磁碟機的檔案、有外傳檔案存在本機的檔案、書面資料
* B0444105李品萱：成功證明有上網、有瀏覽網路磁碟機、有外傳檔案存在本機、書面資料

伍、正確解答**：**

