資安 期末報告

K060A104 黃彥睿

數位鑑識種類


行動裝置鑑識
作業系統鑑識
特定檔案鑑識
網路封包鑑識
Digital
Forensics
惡意行為鑑識
儲存媒體鑑識
遠端鑑識
雲端鑑識

Forensics 領域

- 大約分別為領域：
- 數位鑑識
- 電腦鑑識
- 手機鑑識

數位鑑識

- 以科學的方式採集、保存、分析及呈現數位證據，以可幫助回答電腦與網路案件相關的時間(when)、 內容(what)、相關人員(who)、地點(where)、目 的(why)、如何發生(how)

數位鑑識流程

Evidence Collection
證據採集

→

Evidence Preservation
證據保全

→

Evidence Analysis
證據分析

→

Evidence Presentation
證據呈現

數位鑑識作業階段

報告及法院呈現(Present)

1. 僅呈現與本案相關證據
2. 舉證之所在，敗訴之所在

鑑識分析(Analysis)

1. 分析攻擊或資安事件來源
2. 還原攻擊或案件原貌
3. 列出案件相關時間軸

證據封存及運送(Preserve)

1. 防止數位證物遭到破壞
2. 確保證據監管鏈不中斷

現場蒐證(Identify , Collect)

1. 辨識數位證物
2. 防止數位證據被污染
3. 需完整取得數位證據並執行驗證

電腦鑑識

- 可分為live-analysis及dead-analysis (Carrier, 2003)
- Dead-analysis – 傳統進行電腦鑑識時關閉目標主機,進行證據(記憶體、硬碟) 的收集與分析。
- Live-analysis受到重視,目的為收集揮發性資訊 – 關閉目標主機的同時,可能會造成揮發性資訊的流失。 – 揮發性資訊：執行中的程序(process)、網路連線狀態、 登入的使用者、開啟的檔案、記憶體使用狀況、即時 通訊記錄、GPS資料等等。

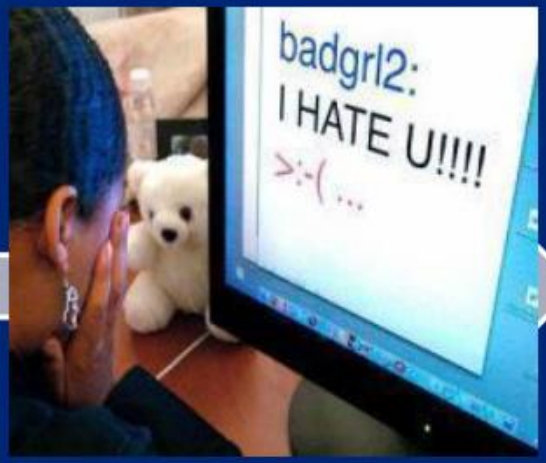
哪些是數位證據？

實體設備

- 電腦/伺服器/筆記型電腦
- 儲存媒體(硬碟、隨身碟、記憶卡)
- 行動影音設備
- 網路設備

資料型式

- 各種格式檔案
- 系統Metadata
- 揮發性資料(記憶體)
- 未被分配磁區



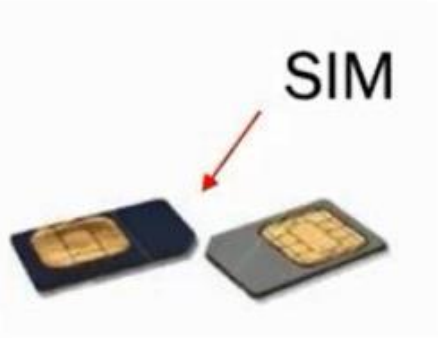
證據資訊

- 上網行為
- 系統Log
- 被刪除資料
- 程式執行紀錄
- 通聯紀錄
- 電郵內容

鑑識軟體工具的功能

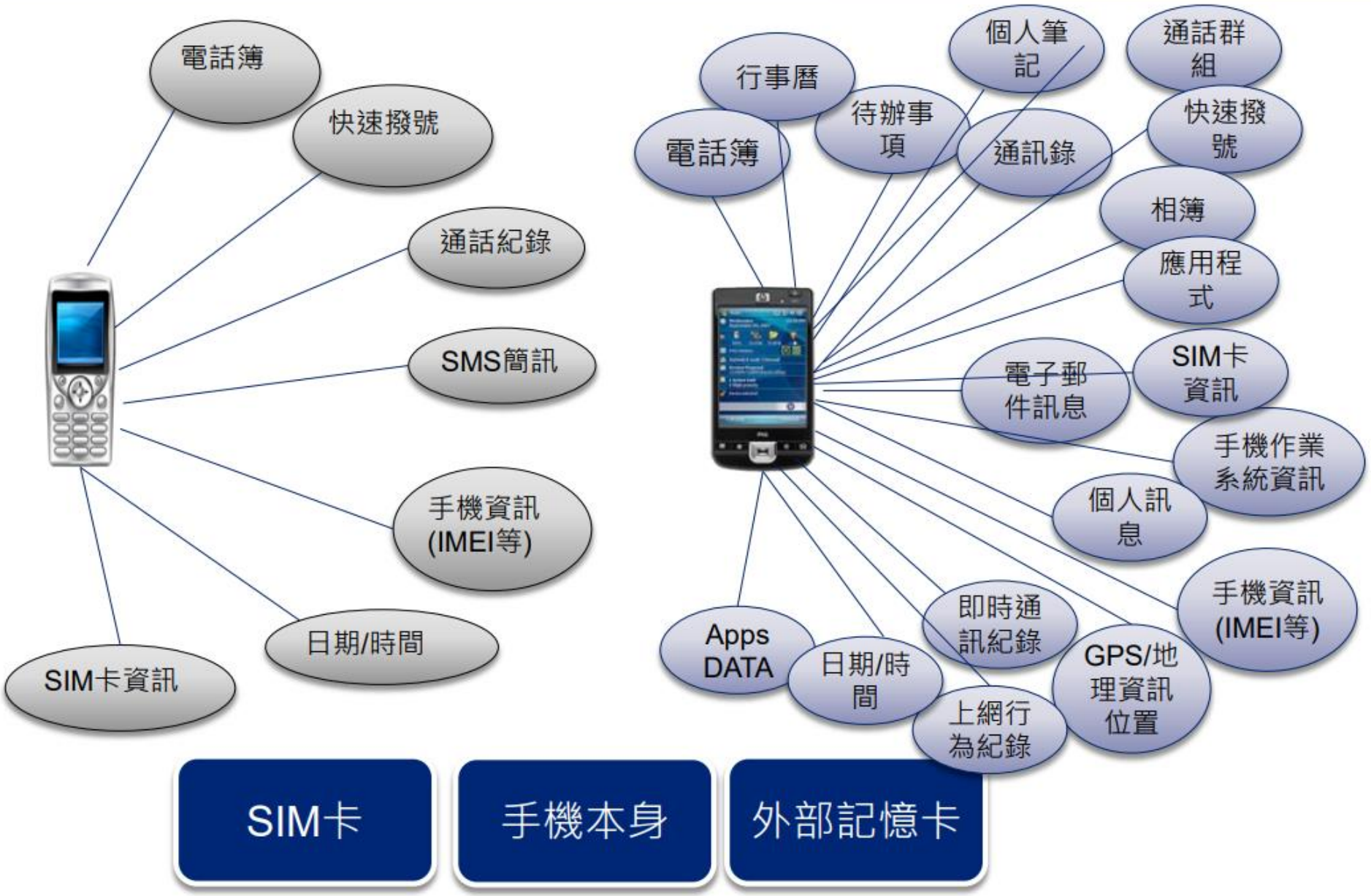
功能項目	說明
映像檔製作	用來製作磁碟映像檔的工具
鑑識分析	針對映像檔還原、分析的工具
鑑識報告	用來產生最後的鑑識報表
資訊收集	對目標電腦系統收集相關資訊的工具
網路探測	用來探測目標電腦的開啟的埠號及服務等的工具
弱點評估	用來探測目標電腦弱點的工具
滲透測試	可針對目標的弱點進行滲透測試的工具
入侵及誘捕	可用來架設誘捕系統的工具
無線網路安全	用來擷取無線網路封包並進行分析的工具
加解密工具	可用於加解密的相關工具
安全程式碼檢測	用來檢測程式碼弱點的工具
其他	密碼破解、病毒檢測等等

手機鑑識



- 資料存於下列3個地方:
  1. 手持裝置內記憶體
  2. SIM卡
  3. 記憶卡

行動裝置上有哪些資料

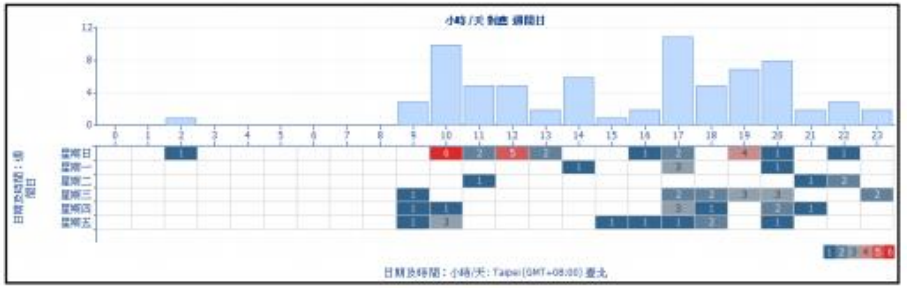

電話簿
快速撥號
通話紀錄
SMS簡訊
手機資訊
(IMEI等)
日期/時間
SIM卡資訊
行事曆
個人筆記
通話群組
電話簿
待辦事項
通訊錄
快速撥號
相簿
應用程式
電子郵件訊息
SIM卡資訊
手機作業系統資訊
個人訊息
手機資訊
(IMEI等)
即時通訊紀錄
Apps DATA
日期/時間
GPS/地理資訊位置
上網行為紀錄
SIM卡
手機本身
外部記憶卡

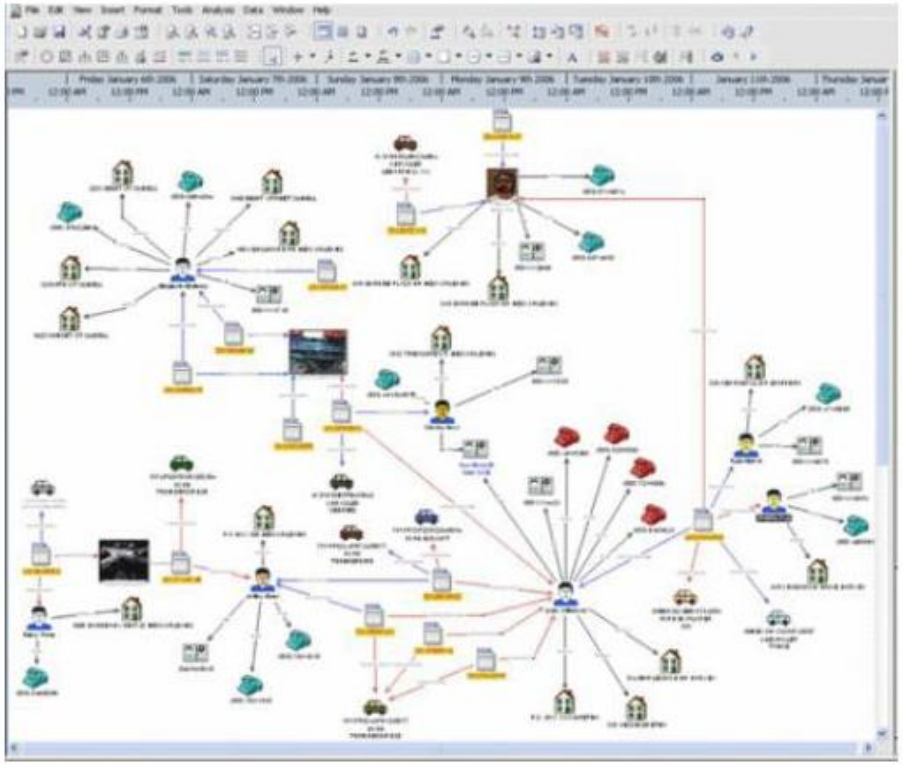
手機鑑識方式

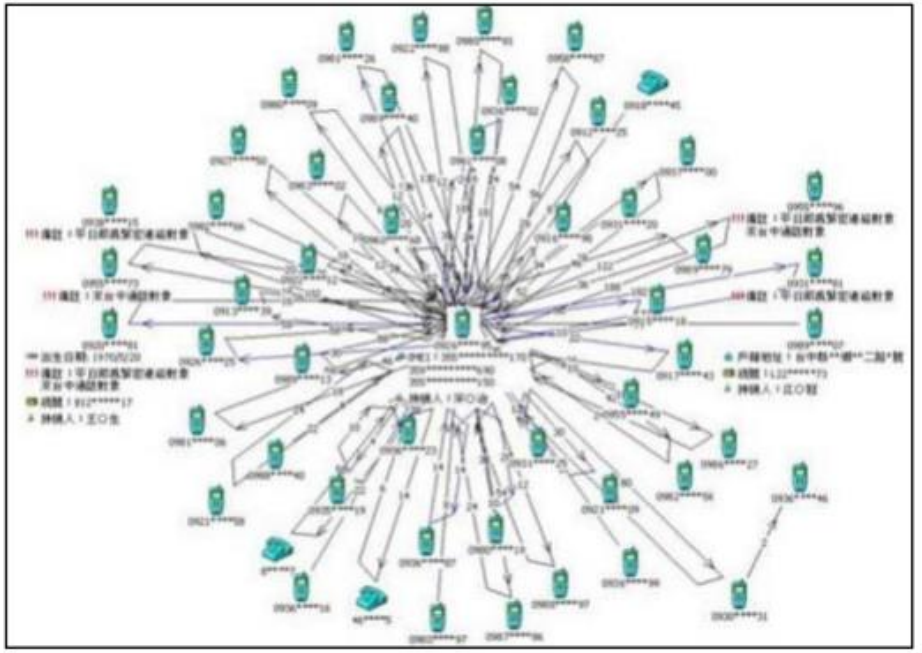
行動裝置鑑識分析

通聯紀錄之分析及視覺化軟體

1) 計算撥打次數
2) 區分撥接通話
3) 時間序列分析







實作

```
root@kali:~/CTF_ex2018/Forensic/memory# volatility -f forensic_100.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/CTF_ex2018/Forensic/memory/forensic_100.raw)
                      PAE type : PAE
                           DTB : 0x34c000L
                          KDBG : 0x80545ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2016-12-06 05:28:47 UTC+0000
     Image local date and time : 2016-12-06 14:28:47 +0900
```

```
root@kali:~/CTF_ex2018/Forensic/memory# volatility -f forensic_100.raw --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------
0x823c8660 System                    4      0     58      259 ------      0
0x81a18020 smss.exe                540      4      3       19 ------      0 2016-12-06 05:27:04 UTC+0000
0x81ef6da0 csrss.exe               604    540     11      480      0      0 2016-12-06 05:27:07 UTC+0000
0x82173da0 winlogon.exe            628    540     24      541      0      0 2016-12-06 05:27:07 UTC+0000
0x8216e670 services.exe            672    628     15      286      0      0 2016-12-06 05:27:07 UTC+0000
0x81f8c9a0 lsass.exe               684    628     26      374      0      0 2016-12-06 05:27:07 UTC+0000
0x82154880 vmacthlp.exe            836    672      1       25      0      0 2016-12-06 05:27:08 UTC+0000
0x81e18da0 svchost.exe             848    672     20      216      0      0 2016-12-06 05:27:08 UTC+0000
0x82151ca8 svchost.exe             936    672     10      272      0      0 2016-12-06 05:27:08 UTC+0000
0x82312450 svchost.exe            1036    672     87     1514      0      0 2016-12-06 05:27:08 UTC+0000
0x81f92778 svchost.exe            1088    672      7       83      0      0 2016-12-06 05:27:08 UTC+0000
0x81e41928 svchost.exe            1320    672     12      183      0      0 2016-12-06 05:27:10 UTC+0000
0x8231f698 explorer.exe           1556   1520     15      466      0      0 2016-12-06 05:27:10 UTC+0000
0x81f0dbe0 spoolsv.exe            1644    672     15      133      0      0 2016-12-06 05:27:10 UTC+0000
0x81e4f560 svchost.exe            1704    672      5      107      0      0 2016-12-06 05:27:10 UTC+0000
0x81f65da0 svchost.exe            1776    672      2       23      0      0 2016-12-06 05:27:10 UTC+0000
0x821f8438 vmtoolsd.exe           1856   1556      3      129      0      0 2016-12-06 05:27:11 UTC+0000
0x82170da0 ctfmon.exe             1872   1556      1       87      0      0 2016-12-06 05:27:11 UTC+0000
0x81f00558 VGAuthService.e         196    672      2       60      0      0 2016-12-06 05:27:13 UTC+0000
0x81e4b4b0 vmtoolsd.exe            312    672      9      265      0      0 2016-12-06 05:27:13 UTC+0000
0x81e886f0 GoogleUpdate.ex         372   1984      7      138      0      0 2016-12-06 05:27:13 UTC+0000
0x82062b20 wuauclt.exe             488   1036      7      132      0      0 2016-12-06 05:27:13 UTC+0000
0x81e89200 wmiprvse.exe            596    848     12      255      0      0 2016-12-06 05:27:13 UTC+0000
0x82267900 rundll32.exe           1712   1556      2      144      0      0 2016-12-06 05:27:16 UTC+0000
0x81f46238 alg.exe                2028    672      7      104      0      0 2016-12-06 05:27:16 UTC+0000
0x81e56228 wscntfy.exe             720   1036      1       37      0      0 2016-12-06 05:27:18 UTC+0000
0x8225bda0 IEXPLORE.EXE            380   1776     22      385      0      0 2016-12-06 05:27:19 UTC+0000
0x8229f7e8 IEXPLORE.EXE           1080    380     19      397      0      0 2016-12-06 05:27:21 UTC+0000
0x81f2cb20 wuauclt.exe            3164   1036      5      107      0      0 2016-12-06 05:28:15 UTC+0000
0x819b4380 tcpview.exe            3308   1556      2       84      0      0 2016-12-06 05:28:42 UTC+0000
0x8216a5e8 DumpIt.exe             3740   1556      1       25      0      0 2016-12-06 05:28:46 UTC+0000
```

```
root@kali:~/CTF_ex2018/Forensic/memory# volatility -f forensic_100.raw --profile=WinXPSP2x86 iehistory
Volatility Foundation Volatility Framework 2.6
**************************************************
Process: 1080 IEXPLORE.EXE
Cache type "DEST" at 0x201ca83
Last modified: 2016-12-06 14:28:40 UTC+0000
Last accessed: 2016-12-06 05:28:42 UTC+0000
URL: SYSTEM@http://crattack.tistory.com/entry/Data-Science-import-pandas-as-pd
Title: Security &amp;amp; Reverse :: [Data Science] Pandas - \),
```

```
root@kali:~/CTF_ex2018/Forensic/memory# curl http://crattack.tistory.com/entry/Data-Science-import-pandas-as-pd
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
<link rel="stylesheet" type="text/css" href="https://t1.daumcdn.net/tistory_admin/blogs/style/menubar.css?_version_=8a80202cfa0d10f58dd999d2db917f1a4af94c40" /><!--[if lt IE 9]><script src="https://t1.daumcdn.net/tistory_admin/lib/jquery/jquery-1.12.4.min.js"></script><![endif]--><!--[if gte IE 9]>
<!--><script src="https://t1.daumcdn.net/tistory_admin/lib/jquery/jquery-3.2.1.min.js"></script><!--<![endif]-->
<script>var tjQuery = jQuery.noConflict(true);</script><style type="text/css">.tt_article_useless_p_margin p {padding-top:0 !important;padding-bottom:0 !important;margin-top:0 !important;margin-bottom:0 !important;}</style><meta name="referrer" content="always"><link rel="icon" href="//t1.daumcdn.net/tistory_admin/static/top/favicon_0630.ico" /><link rel="apple-touch-icon" href="//i1.daumcdn.net/thumb/C180x180/?fname=http%3A%2F%2Fcfile2.uf.tistory.com%2Fimage%2F2545814A52F183913BB3AD">
<link rel="apple-touch-icon" sizes="76x76" href="//i1.daumcdn.net/thumb/C76x76/?fname=http%3A%2F%2Fcfile2.uf.tistory.com%2Fimage%2F2545814A52F183913BB3AD">
<link rel="apple-touch-icon" sizes="120x120" href="//i1.daumcdn.net/thumb/C120x120/?fname=http%3A%2F%2Fcfile2.uf.tistory.com%2Fimage%2F2545814A52F183913BB3AD">
<link rel="apple-touch-icon" sizes="152x152" href="//i1.daumcdn.net/thumb/C152x152/?fname=http%3A%2F%2Fcfile2.uf.tistory.com%2Fimage%2F2545814A52F183913BB3AD"><meta name="description" content="import pandas as pd ※ pandas[illegible] DataFrame[illegible] read_csv [illegible] &amp;quot;,&amp;quot;[illegible] read_table [illegible] &amp;quot;\t&amp;quot;[illegible] read_fwf [illegible]..">

<!-- BEGIN OPENGRAPH -->
<link rel="canonical" href="http://crattack.tistory.com/entry/Data-Science-import-pandas-as-pd" /><meta property="og:type" content="article"><meta property="og:url" content="http://crattack.tistory.com/entry/Data-Science-import-pandas-as-pd" ><meta property="og:site_name" content="Security &amp;amp;amp; Reverse" ><meta property="og:title" content="[Data Science] Pandas - [illegible], [illegible], [illegible]" ><meta name="by" content="crattack" ><meta property="og:description" content="import pandas as pd ※ pandas[illegible] DataFrame[illegible] read_csv [illegible] &amp;quot;,&amp;quot;[illegible] read_table [illegible] &amp;quot;\t&amp;quot;[illegible] read_fwf [illegible].." ><meta property="og:image" content="http://cfile8.uf.tistory.com/image/2502923E576BA0AA013469" >
<!-- END OPENGRAPH -->
```

```
root@kali:~/CTF_ex2018/Forensic/memory# volatility -f forensic_100.raw --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x018c3cc8 192.168.88.131:1077       180.70.134.87:80          3676
0x0196f6a0 192.168.88.131:1122       175.126.170.70:80         3676
0x0233bbe8 192.168.88.131:1034       153.127.200.178:80        1080
0x02470238 192.168.88.131:1036       172.217.27.78:443         2776
```

```
root@kali:~/CTF_ex2018/Forensic/memory# curl http://153.127.200.178/entry/Data-Science-import-pandas-as-pd
<!DOCTYPE html>
<html>
<head>
        <meta charset="utf-8">
        <title>404 - Page Not Found</title>
        <style type="text/css">

        body { background-color: #fff; margin: 40px; font-family: Arial, Sans-serif; font-size: 12px; color: #000; }

        #container  {
                width: 600px;
                padding: 0px;
                margin: 0 auto;
        }
        #header {
                background-color: #000;
                -webkit-border-radius: 10px 10px 0 0;
                -moz-border-radius: 10px 10px 0 0;
                border-radius: 10px 10px 0 0;
                border: 1px solid #000;
        }
        #header h1 {
                color: #FFF;
                font-weight: bold;
                font-size: 16px;
                padding: 10px;
                margin: 0px;
```