Forensics in CTF - part 2

oalieno

What is Forensics

- 在 CTF 比賽中，Forensics 可能會是以下幾種類型
  - File Format Analysis
  - Steganography
  - **Memory Dump Analysis**
  - **Network Packet Analysis**
  - ...

What is Forensics

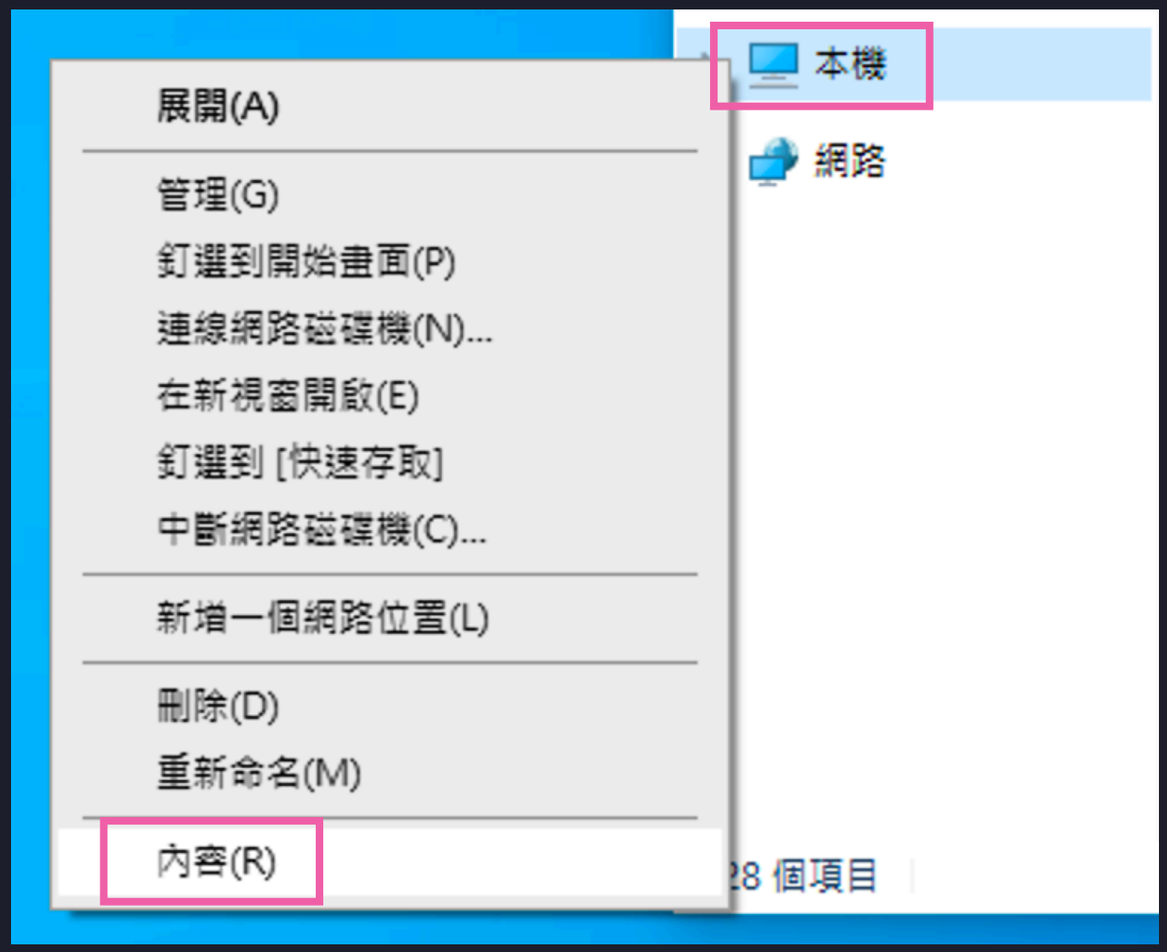
chtsecurity.com/service/m401

- Forensics 這個字的意思就是**鑑識**、**取證**，原本是用在法律案件中的犯罪鑑識、取證
- 如今，新型態的資安案件的出現，Forensics 也可以指資安事件的鑑識、取證
- 主要目的是在協助客戶緊急應變、入侵管道定位、受影響範圍評估及回復受駭系統

Memory Dump Analysis

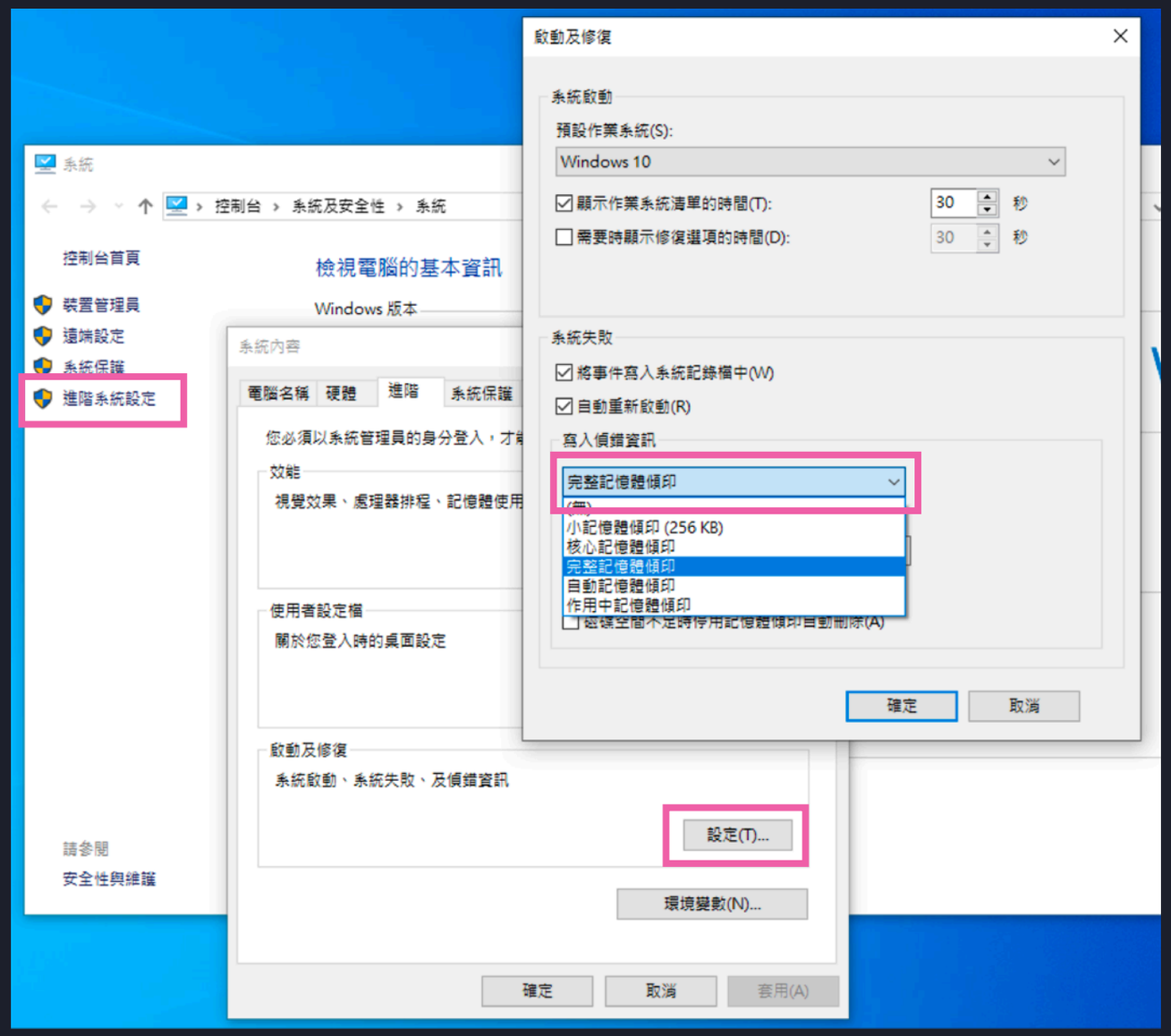
Dump Memory

檔案總管 → 本機 → 內容



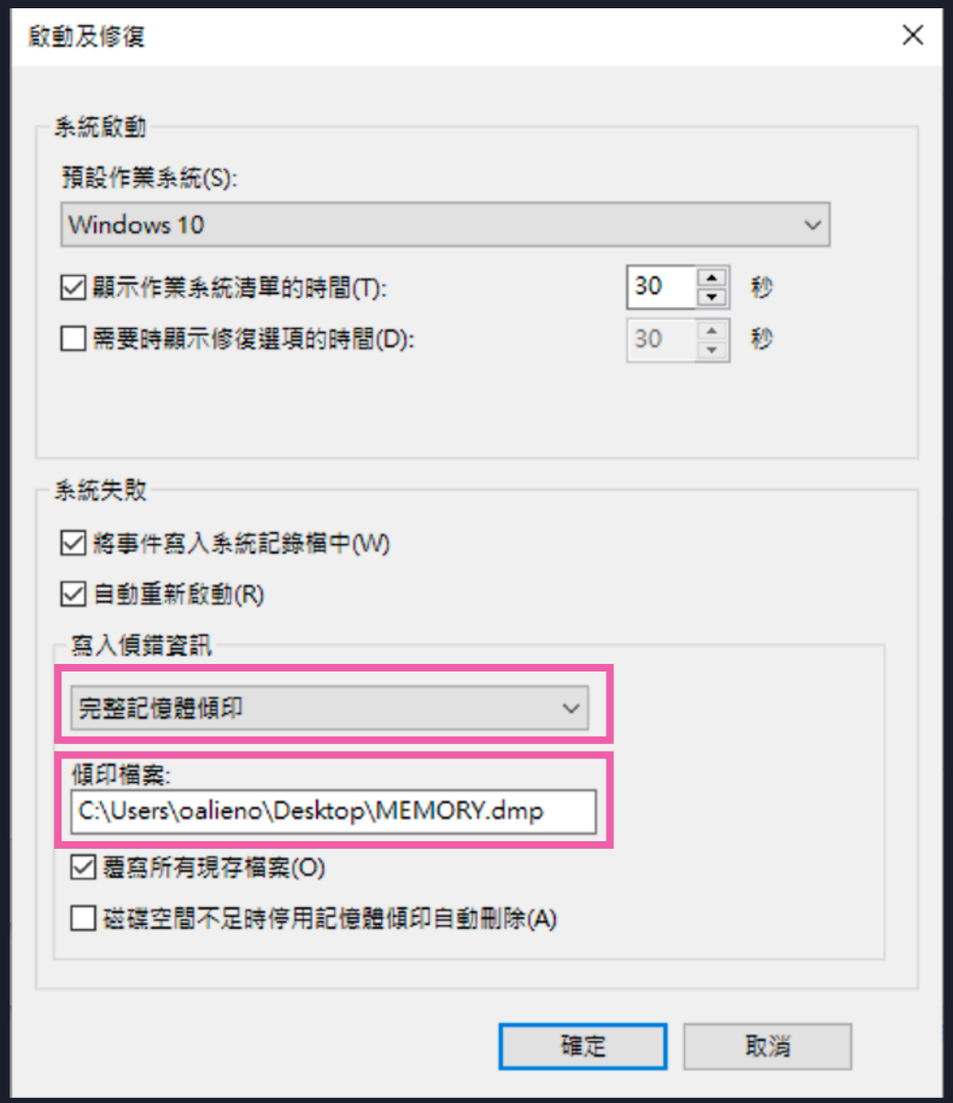
Dump Memory

進階系統設定 → 進階 → 啟動及修復 → 寫入偵錯資訊



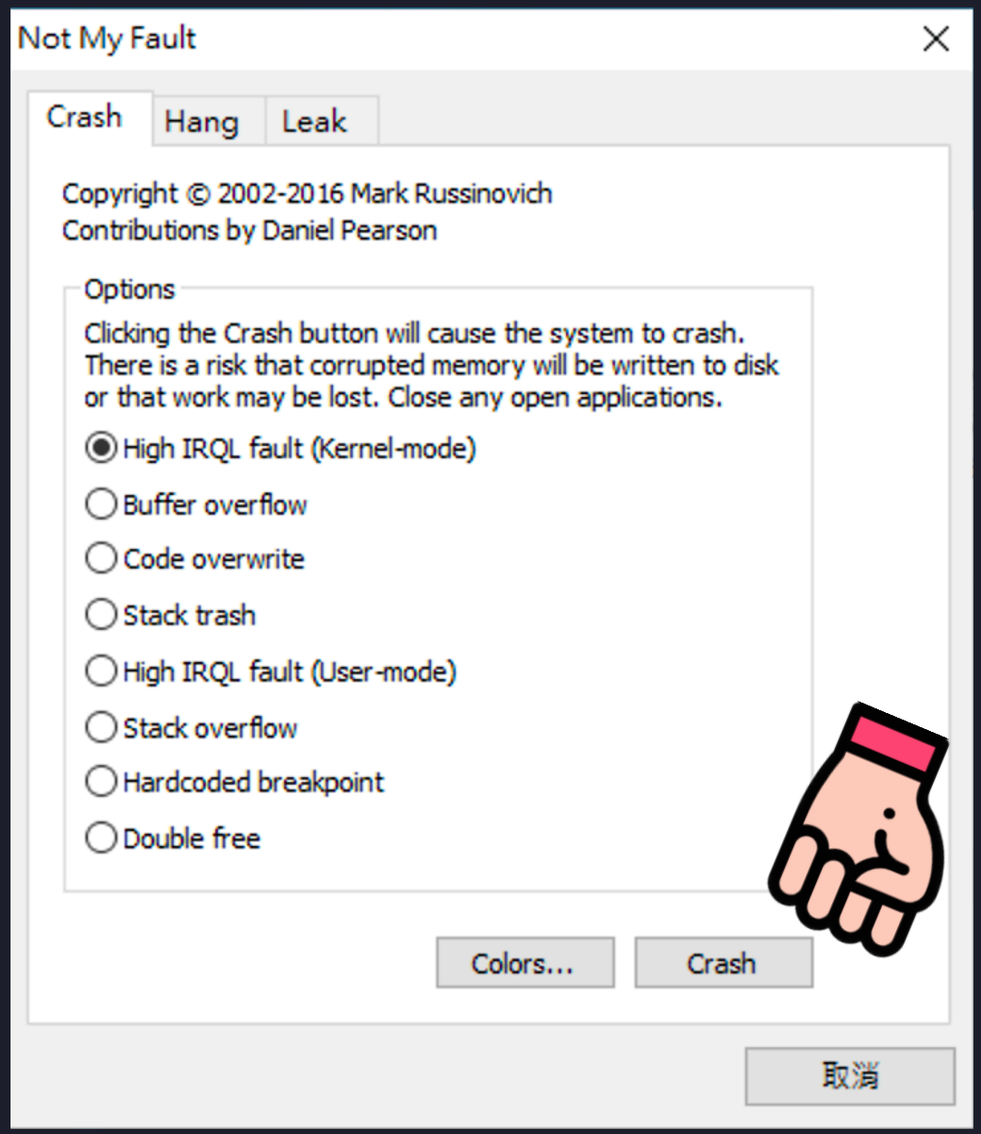
Dump Memory

- 設定完整記憶體傾印可以拿到比較完整的訊息，不過檔案會變很大
- 可以設定一下傾印檔案到你喜歡的路徑



Crash It !!!

https://docs.microsoft.com/en-us/sysinternals/downloads/notmyfault



:(

您的電腦發生問題，因此必須重新啟動。
我們剛剛正在
收集某些錯誤資訊，接著我們會為您重新啟動。

已完成 100%

如需此問題與可能修正的詳細資訊，請瀏覽 https://www.windows.com/stopcode

致電支援人員時，請提供此資訊:

停止代碼: DRIVER_IRQL_NOT_LESS_OR_EQUAL

失敗的項目: myfault.sys

Get Dump Memory

- 在電腦掛掉之後，就會根據剛剛的設定產生 memory dump
- 那我們就可以去分析這個 memory dump
- 然後釐清到底發生什麼事情了

volatility

- Volatile memory extraction utility framework
- RAM 就是一種 Volatile memory
- 有很多 plugin 可以用
- 用這個工具來分析 memory dump 出來的檔案吧

imageinfo

```
volatility -f file imageinfo
```

```
~ volatility -f Mem_Evidence.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/oalieno_eecs04/Mem_Evidence.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800027f60a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800027f7d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-06-29 07:30:00 UTC+0000
     Image local date and time : 2019-06-29 13:00:00 +0530
```

pslist

volatility -f file --profile=Win7SP1x64 pslist

```
~ volatility -f Mem_Evidence.raw --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8000ca0040 System                    4      0     79      509 ------      0 2019-06-29 07:28:07 UTC+0000
0xfffffa80014af950 smss.exe                256      4      3       32 ------      0 2019-06-29 07:28:07 UTC+0000
0xfffffa8001c57b30 csrss.exe               328    320     11      385      0      0 2019-06-29 07:28:14 UTC+0000
0xfffffa8000ca8960 csrss.exe               376    368      7      200      1      0 2019-06-29 07:28:15 UTC+0000
0xfffffa8001c6f760 wininit.exe             384    320      3       75      0      0 2019-06-29 07:28:15 UTC+0000
0xfffffa8001c751f0 winlogon.exe            412    368      6      119      1      0 2019-06-29 07:28:15 UTC+0000
0xfffffa8001bc1b30 services.exe            472    384     13      193      0      0 2019-06-29 07:28:17 UTC+0000
0xfffffa8001cb5940 lsass.exe               480    384      8      582      0      0 2019-06-29 07:28:17 UTC+0000
0xfffffa8001cc1b30 lsm.exe                 488    384     12      187      0      0 2019-06-29 07:28:17 UTC+0000
0xfffffa8001d02b30 svchost.exe             580    472     11      358      0      0 2019-06-29 07:28:21 UTC+0000
0xfffffa8001d30b30 VBoxService.ex          640    472     14      137      0      0 2019-06-29 07:28:21 UTC+0000
0xfffffa8001d43a70 svchost.exe             708    472      7      260      0      0 2019-06-29 07:28:22 UTC+0000
0xfffffa8001dacb30 svchost.exe             804    472     19      393      0      0 2019-06-29 07:28:23 UTC+0000
0xfffffa8001db9b30 svchost.exe             840    472     21      431      0      0 2019-06-29 07:28:24 UTC+0000
0xfffffa8001dc6850 svchost.exe             864    472     37      917      0      0 2019-06-29 07:28:24 UTC+0000
0xfffffa8001df1060 audiodg.exe             952    804      7      131      0      0 2019-06-29 07:28:26 UTC+0000
0xfffffa8001e1b890 svchost.exe             220    472     16      323      0      0 2019-06-29 07:28:27 UTC+0000
0xfffffa8001e45630 svchost.exe             484    472     18      376      0      0 2019-06-29 07:28:29 UTC+0000
0xfffffa8001eaab30 spoolsv.exe            1132    472     15      286      0      0 2019-06-29 07:28:32 UTC+0000
0xfffffa8001ed7b30 svchost.exe            1176    472     21      307      0      0 2019-06-29 07:28:33 UTC+0000
0xfffffa8001f452e0 svchost.exe            1276    472     14      220      0      0 2019-06-29 07:28:34 UTC+0000
0xfffffa8001f81b30 taskhost.exe           1804    472     10      161      1      0 2019-06-29 07:28:42 UTC+0000
0xfffffa8001ff9630 taskeng.exe            1824    864      6       82      0      0 2019-06-29 07:28:42 UTC+0000
0xfffffa80020bbb30 dwm.exe                1908    840      5       77      1      0 2019-06-29 07:28:43 UTC+0000
```

filescan

```
volatility -f file --profile=Win7SP1x64 filescan
```

```
~ volatility -f Mem_Evidence.raw --profile=Win7SP1x64 filescan
Volatility Foundation Volatility Framework 2.6
Offset(P)            #Ptr   #Hnd Access Name
------------------ ------ ------ ------ ----
0x000000003e8009a0      1      1 R--rwd \Device\HarddiskVolume2\Windows\System32\catroot
0x000000003e800f20     14      0 R--r-d \Device\HarddiskVolume2\Windows\System32\SearchIndexer.exe
0x000000003e8012d0     14      0 R--r-d \Device\HarddiskVolume2\Windows\System32\esent.dll
0x000000003e8027c0      1      1 R--rw- \Device\HarddiskVolume2\Windows\System32
0x000000003e80d320      1      1 R--rw- \Device\HarddiskVolume2\Windows\winsxs\amd64_microsoft.wir
0x000000003e812070     10      0 R--r-d \Device\HarddiskVolume2\Windows\System32\msidle.dll
0x000000003e812c00      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\netman.dll
0x000000003e816070      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\rasdlg.dll
0x000000003e819960     17      0 RW-rwd \Device\HarddiskVolume2\$Directory
0x000000003e819f20      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\ActionCenter.dll
```

plugins

- 除了內建的 plugins 還有很多別人寫的
- 比如這個 volatility-plugins
- 官方社群的 github 上面也有很多
- 每年還會有 plugin contest

chromehistory

```
volatility —plugins=volatility-plugins/ -f file --profile=Win7SP1x64 chromehistory
```

```
~ volatility --plugins=volatility-plugins/ -f Challenge.raw --profile=Win7SP1x64 chromehistory
Volatility Foundation Volatility Framework 2.6
Index  URL                                                                                  Title
------ ------------------------------------------------------------------------------------ ------------------------------------
   106 http://codechef.com/                                                                 Programming Competition,Programming C
   105 https://leetcode.com/                                                                LeetCode - The World's Leading Online
   103 http://codeforces.com/                                                               Codeforces
    99 https://www.google.com/search?q=HTML5&s...cd2A20QxA0wGHoECA0QBw&biw=1920&bih=861      HTML5 - Google Search
    92 https://www.google.com/search?q=python&...9i60.1327j0j7&sourceid=chrome&ie=UTF-8     python - Google Search
    91 https://www.google.com/search?q=bitbuck...j0l5.8221j0j7&sourceid=chrome&ie=UTF-8     bitbucket - Google Search
    89 https://gitlab.com/                                                                   The first single application for the
    87 https://www.google.com/search?q=github+...60l3.2766j0j7&sourceid=chrome&ie=UTF-8     github students - Google Search
    74 https://www.google.com/search?q=xss&oq=...9i57.1231j0j7&sourceid=chrome&ie=UTF-8     xss - Google Search
    73 https://www.google.com/search?q=google+...60l4.8083j0j7&sourceid=chrome&ie=UTF-8     google translate - Google Search
    60 https://github.com/                                                                   The world’s leading software developm
```

練習題

InCTF 2019 - Just Do It

InCTF 2019 - Notch It Up

Network Packet Analysis

wireshark

- 免費開源的網路封包分析軟體
- commandl line 版的：tshark
- python package：pyshark

pcap v.s. pcapng

- pcapng 就是 pcap next generation 的縮寫
- 所以 pcapng 就是強化版的 pcap
- 可以用 editcap 指令把 pcapng 轉成 pcap

```
editcap -F libpcap -T ether file.pcapng file.pcap
```

Filter

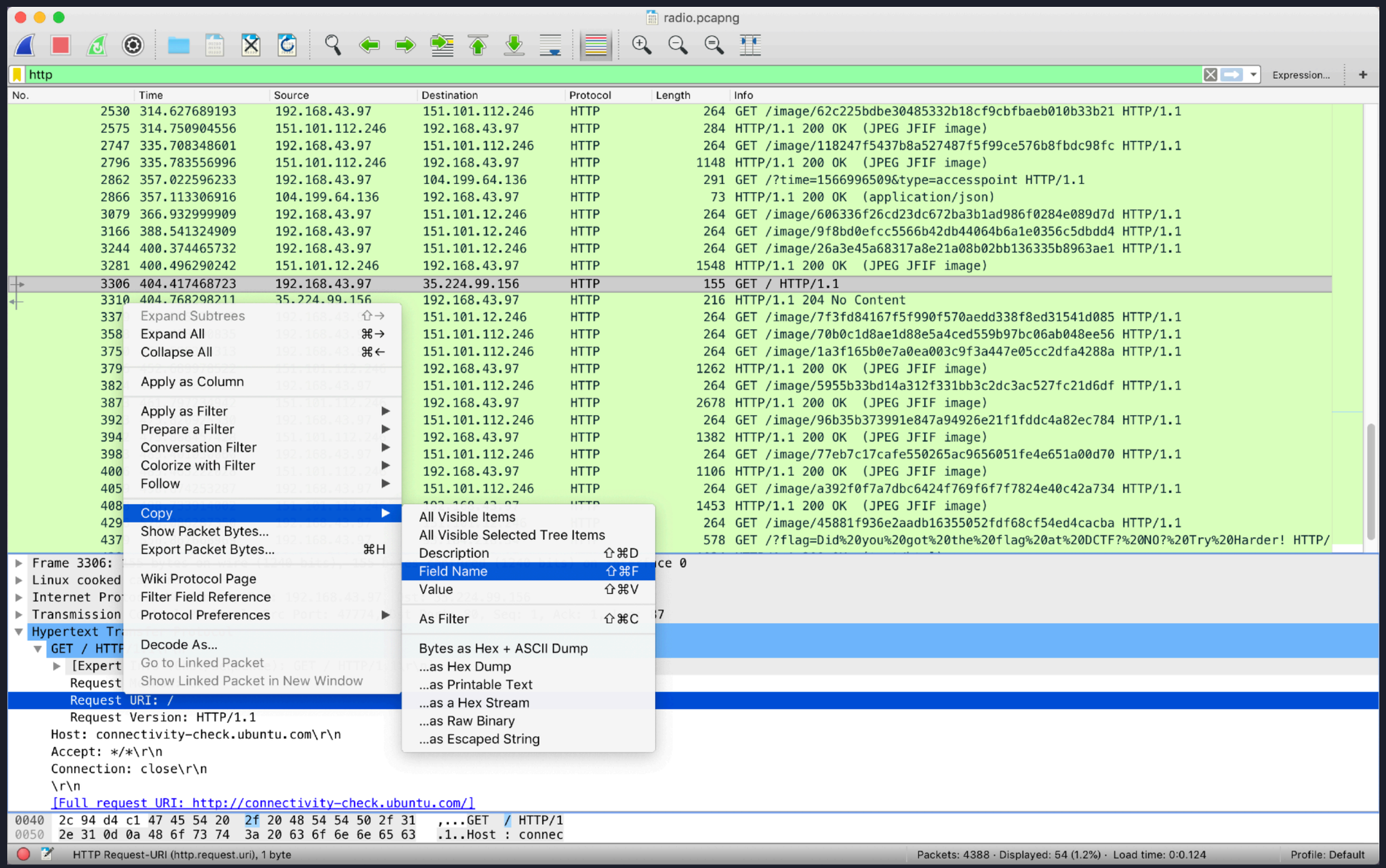
```
http
```

```
ip.src == 192.168.0.1 && ip.dst == 127.0.0.1
```

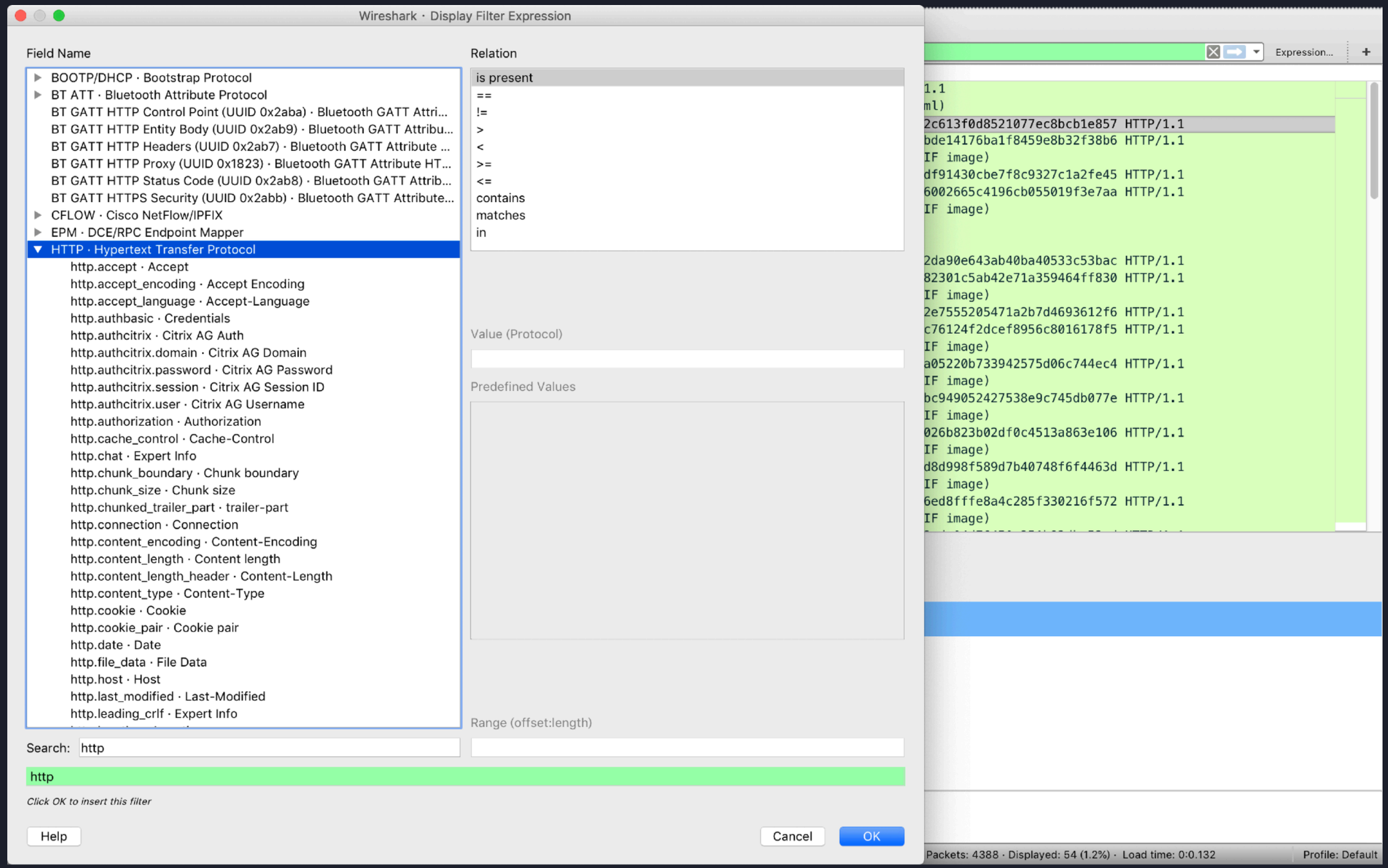
```
http and http.request.uri contains "index"
```

```
frame contains "flag"
```

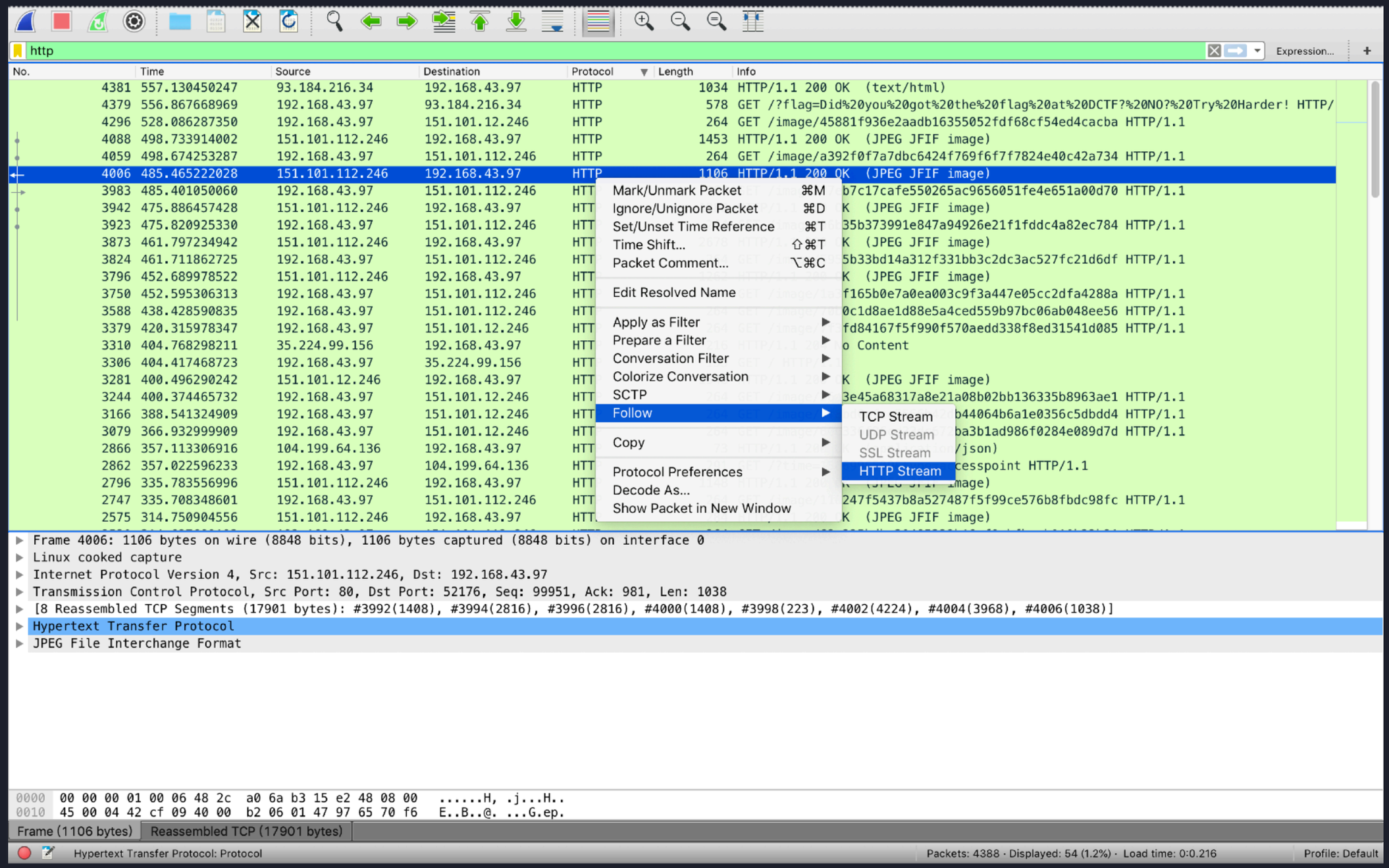
Find Out Field Name



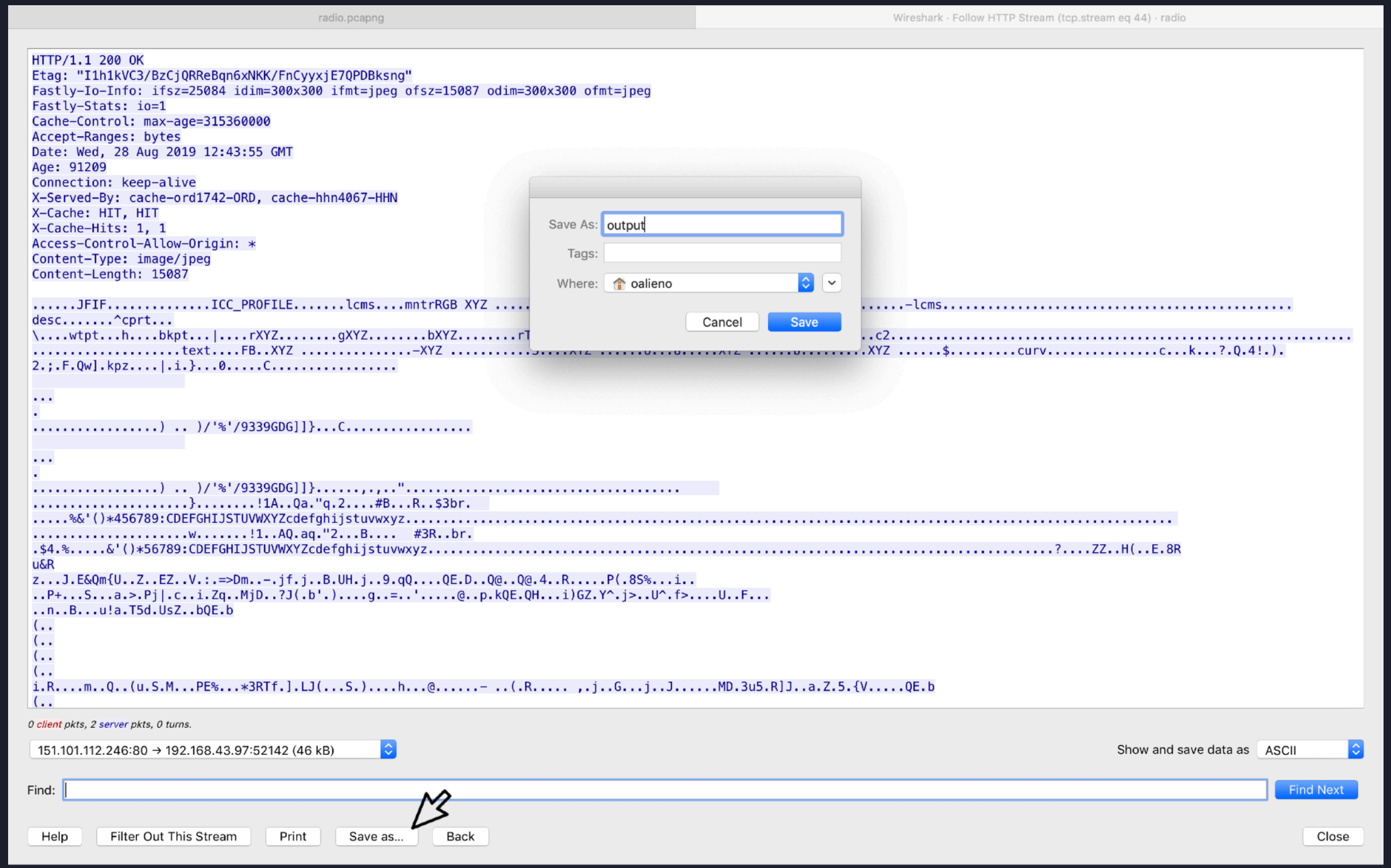
Filter Expression



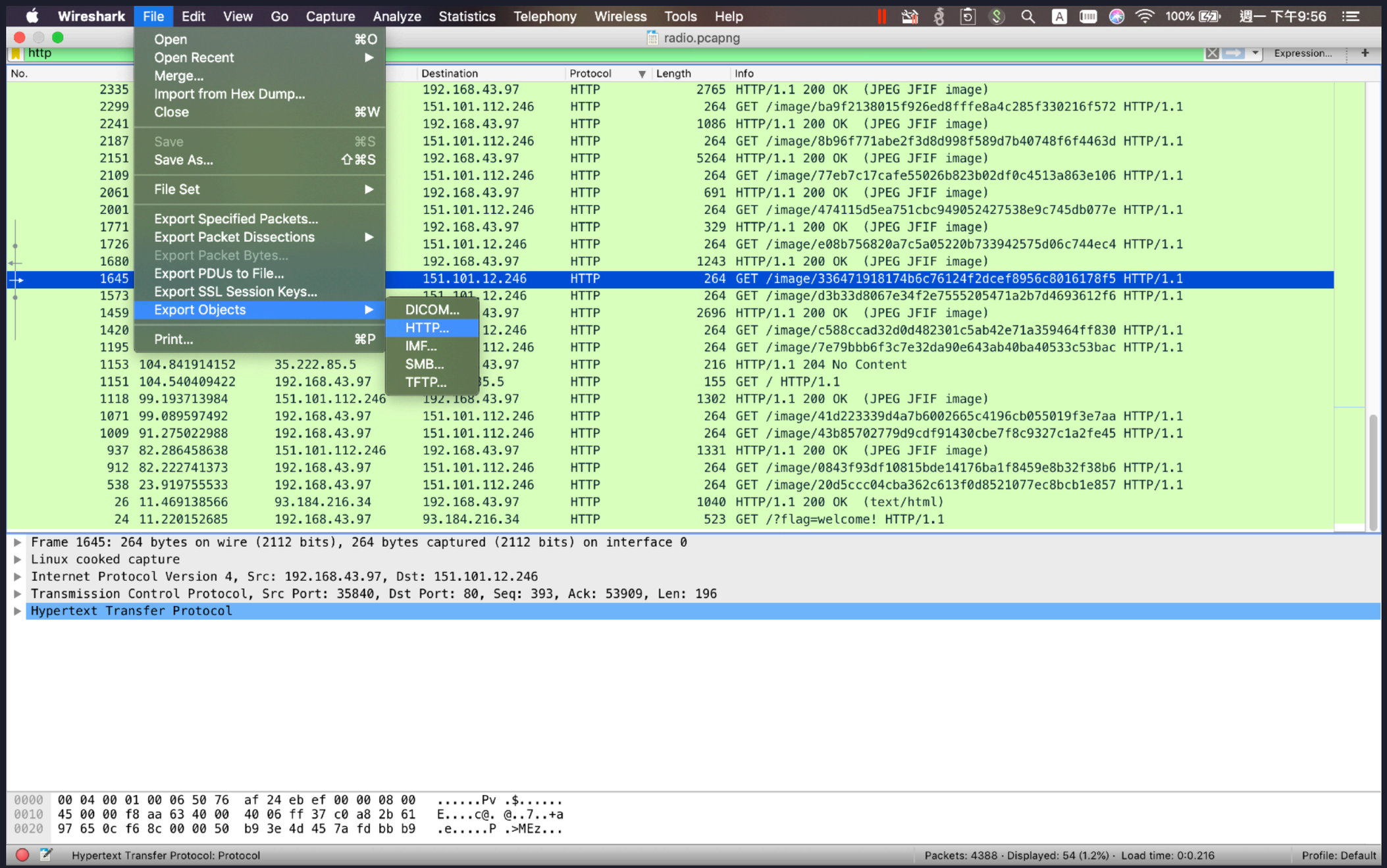
Follow Stream



Save Stream Data



Export Objects



練習題

tshark example

```
tshark -r radio.pcapng -Y "http and http.request.uri contains image" -T fields -e 'http.request.uri'
```

- -r : 要分析的 pcap 檔案
- -Y : filter 規則
- -e : 要 extract 的欄位
- -T : extract 的格式

pyshark example

```
#!/usr/bin/env python3
import pyshark

cap = pyshark.FileCapture('./radio.pcapng', display_filter = "http")

for packet in cap:
    try:
        if 'image' in packet.http.request_uri:
            print(packet.http.request_uri)
    except AttributeError:
        pass
```