# HackerFrogs Afterschool
# Digital Forensics: Wireshark Pt 2

Class:
Digital Forensics

Workshop Number:
AS-FOR-04

Document Version:
1.75

Special Requirements:
Registered account at picoctf.org

# Welcome to HackerFrogs Afterschool!

Hey there HackerFrogs!

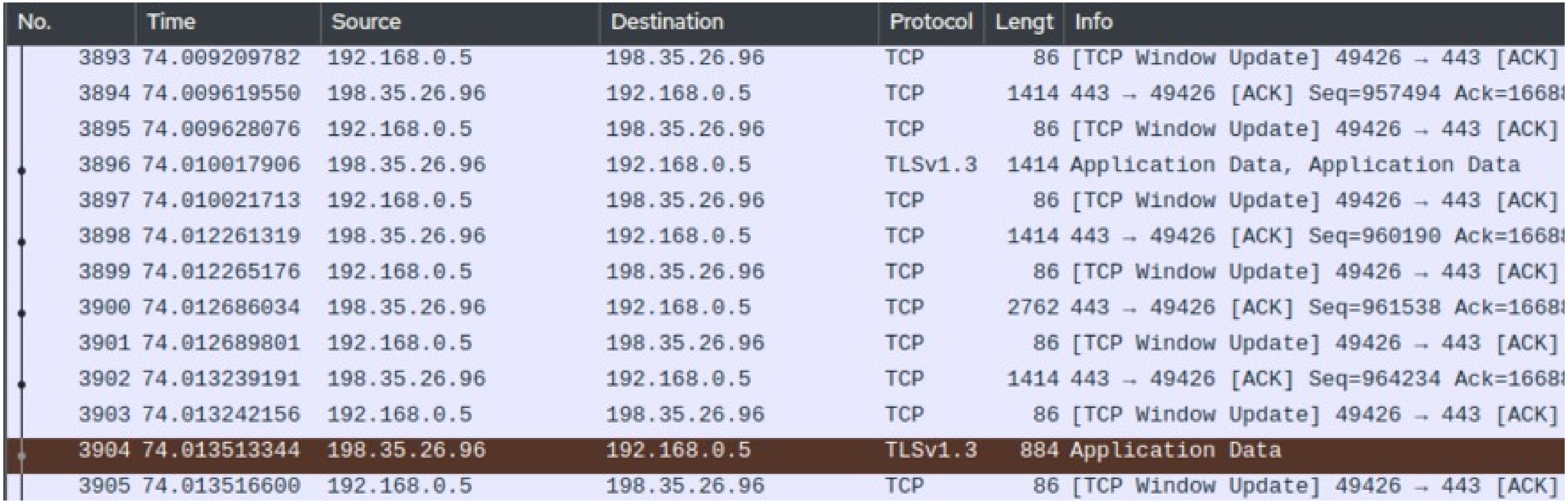
This is the fourth intro to Digital Forensics workshop.

In the previous workshop we learned about the following Digital Forensic concepts:

# Network Traffic

Any time a network device sends data from one device to another, network traffic is generated as network packets are sent back and forth

# PCAP Files



| No. | Time | Source | Destination | Protocol | Lengt | Info |
|---|---|---|---|---|---|---|
| 3893 | 74.009209782 | 192.168.0.5 | 198.35.26.96 | TCP | 86 | [TCP Window Update] 49426 → 443 [ACK] |
| 3894 | 74.009619550 | 198.35.26.96 | 192.168.0.5 | TCP | 1414 | 443 → 49426 [ACK] Seq=957494 Ack=1668 |
| 3895 | 74.009628076 | 192.168.0.5 | 198.35.26.96 | TCP | 86 | [TCP Window Update] 49426 → 443 [ACK] |
| 3896 | 74.010017906 | 198.35.26.96 | 192.168.0.5 | TLSv1.3 | 1414 | Application Data, Application Data |
| 3897 | 74.010021713 | 192.168.0.5 | 198.35.26.96 | TCP | 86 | [TCP Window Update] 49426 → 443 [ACK] |
| 3898 | 74.012261319 | 198.35.26.96 | 192.168.0.5 | TCP | 1414 | 443 → 49426 [ACK] Seq=960190 Ack=1668 |
| 3899 | 74.012265176 | 192.168.0.5 | 198.35.26.96 | TCP | 86 | [TCP Window Update] 49426 → 443 [ACK] |
| 3900 | 74.012686034 | 198.35.26.96 | 192.168.0.5 | TCP | 2762 | 443 → 49426 [ACK] Seq=961538 Ack=1668 |
| 3901 | 74.012689801 | 192.168.0.5 | 198.35.26.96 | TCP | 86 | [TCP Window Update] 49426 → 443 [ACK] |
| 3902 | 74.013239191 | 198.35.26.96 | 192.168.0.5 | TCP | 1414 | 443 → 49426 [ACK] Seq=964234 Ack=1668 |
| 3903 | 74.013242156 | 192.168.0.5 | 198.35.26.96 | TCP | 86 | [TCP Window Update] 49426 → 443 [ACK] |
| 3904 | 74.013513344 | 198.35.26.96 | 192.168.0.5 | TLSv1.3 | 884 | Application Data |
| 3905 | 74.013516600 | 192.168.0.5 | 198.35.26.96 | TCP | 86 | [TCP Window Update] 49426 → 443 [ACK] |

Files which contain a collection of network traffic are called packet capture (PCAP) files, and one specialty of digital forensics is the analysis of network traffic and PCAP files.
]

# Wireshark

Wireshark is a program which is widely used for network traffic analysis, and we'll learn to use it to analyze PCAP files.

# This Workshop's Topics

- Wireshark practice

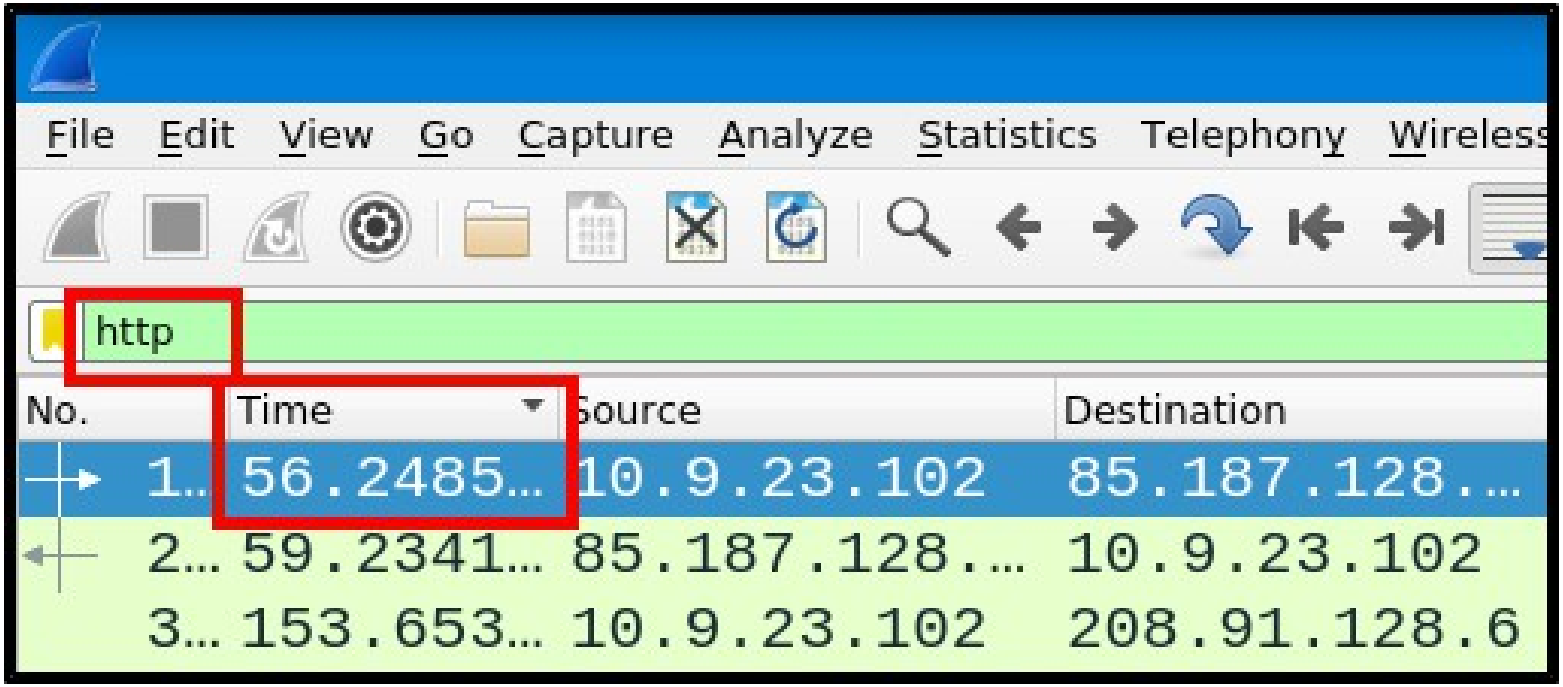
- TryHackMe: Carnage Room

# TryHackMe: Carnage Room

Let's begin our Wireshark practice with a TryHackMe room:

https://tryhackme.com/room/c2carnage

# Q1: What was the date and time for the first HTTP connection to the malicious IP



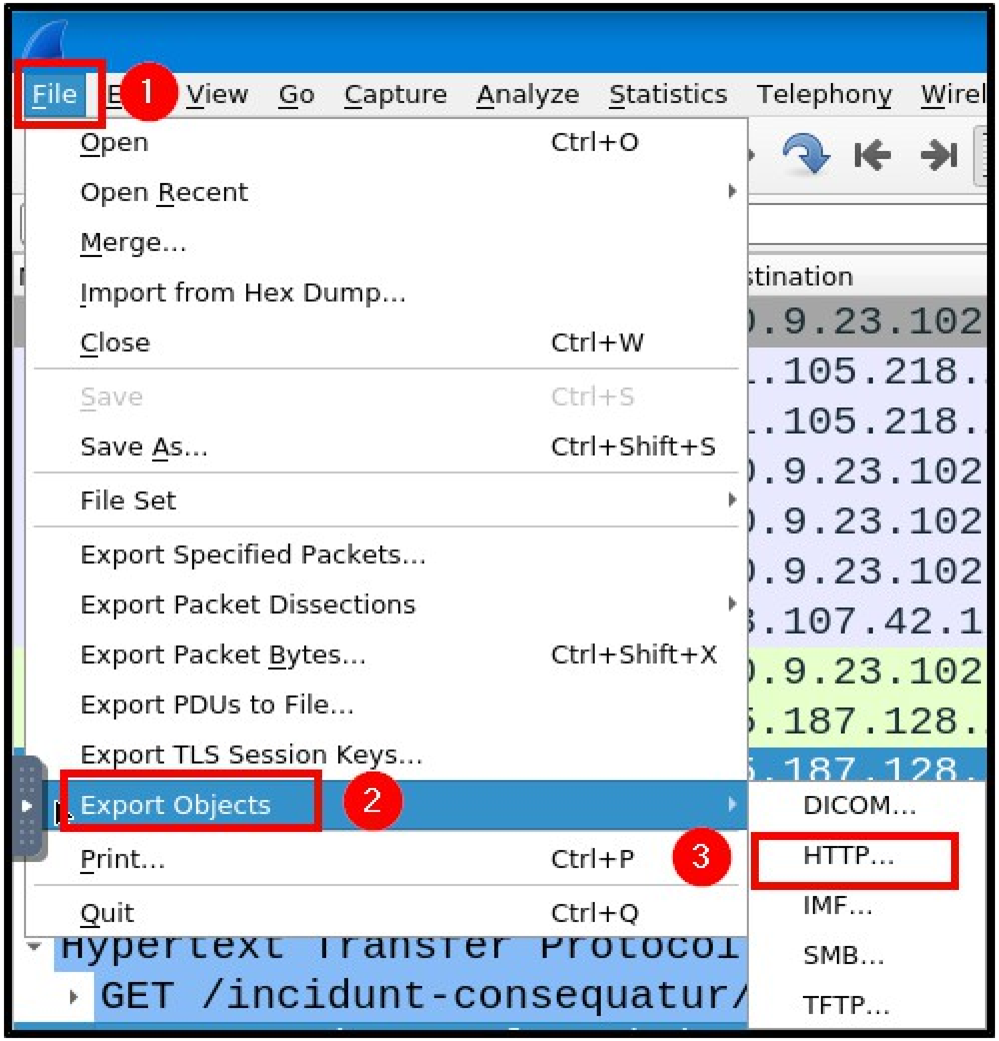
http

| No. | Time | Source | Destination |
|---|---|---|---|
| 1… | 56.2485… | 10.9.23.102 | 85.187.128.… |
| 2… | 59.2341… | 85.187.128.… | 10.9.23.102 |
| 3… | 153.653… | 10.9.23.102 | 208.91.128.6 |

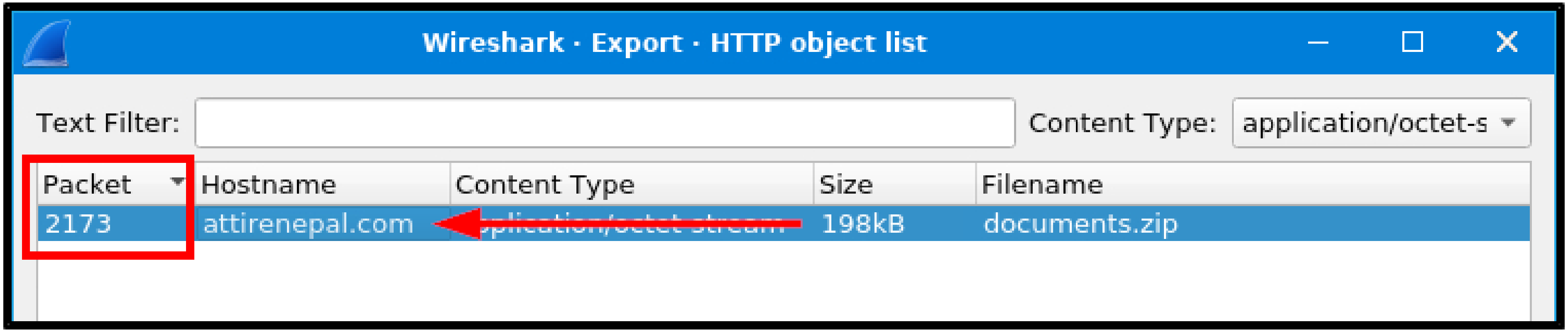
There are two things we need to pay attention to in this question: HTTP packets and ordering the packets by time

# Q2: What is the name of the zip file that was downloaded?

We can use the **Export Objects** option in Wireshark to look for files downloaded in the PCAP file, and most files are downloaded using the HTTP protocol



# Q3: What was the domain hosting the malicious zip file?



Wireshark · Export · HTTP object list

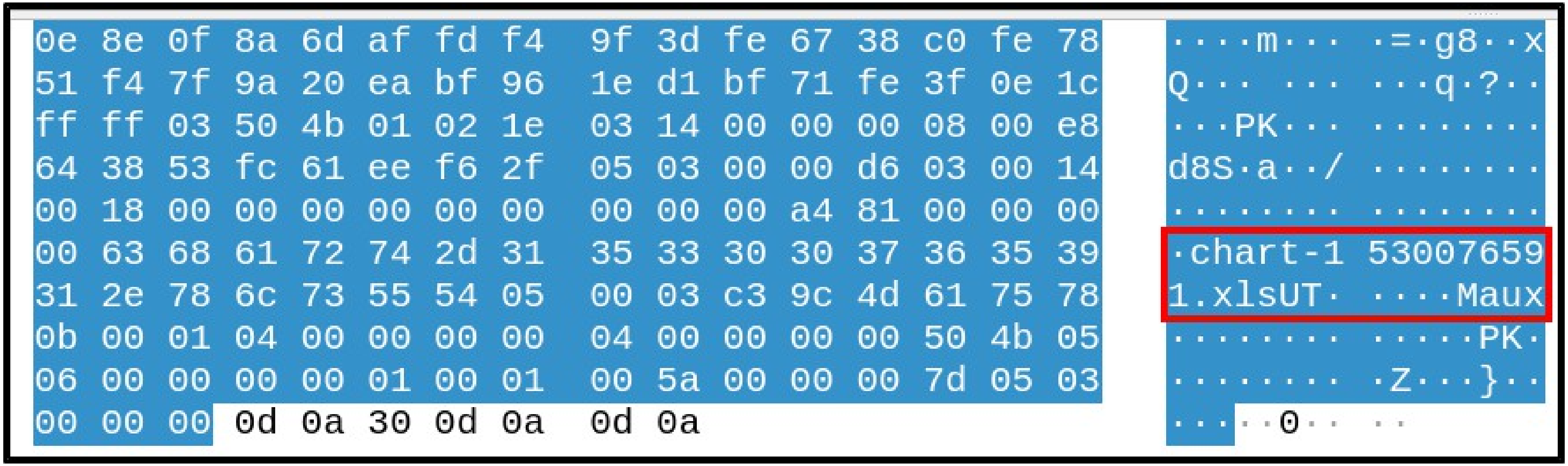
Text Filter:

Content Type: application/octet-s

| Packet | Hostname | Content Type | Size | Filename |
|---|---|---|---|---|
| 2173 | attirenepal.com | application/octet-stream | 198kB | documents.zip |

When you click on a particular file in the Wireshark object export list, it will select the associated packet in the Packet List view

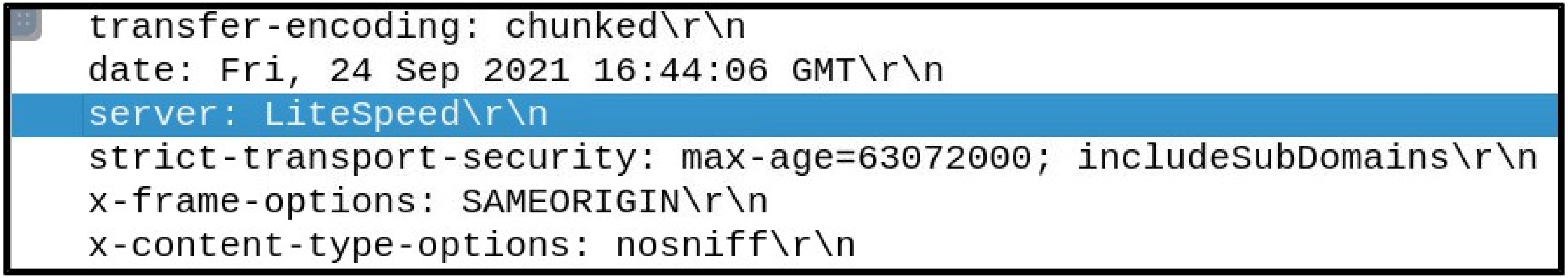
# Q4: Without downloading the file, what is the name of the file in the zip file?



```
0e 8e 0f 8a 6d af fd f4  9f 3d fe 67 38 c0 fe 78   ····m···  ·=·g8··x
51 f4 7f 9a 20 ea bf 96  1e d1 bf 71 fe 3f 0e 1c   Q··· ···  ···q·?··
ff ff 03 50 4b 01 02 1e  03 14 00 00 00 08 00 e8   ···PK···  ········
64 38 53 fc 61 ee f6 2f  05 03 00 00 d6 03 00 14   d8S·a··/  ········
00 18 00 00 00 00 00 00  00 00 00 a4 81 00 00 00   ········  ········
00 63 68 61 72 74 2d 31  35 33 30 30 37 36 35 39   ·chart-1  53007659
31 2e 78 6c 73 55 54 05  00 03 c3 9c 4d 61 75 78   1.xlsUT·  ····Maux
0b 00 01 04 00 00 00 00  04 00 00 00 00 50 4b 05   ········  ·····PK·
06 00 00 00 00 01 00 01  00 5a 00 00 00 7d 05 03   ········  ·Z···}··
00 00 00 0d 0a 30 0d 0a  0d 0a                     ·····0··  ··
```

For zip files, the names of the files inside them are included in the file contents, and can be viewed through the Packet Bytes view in Wireshark

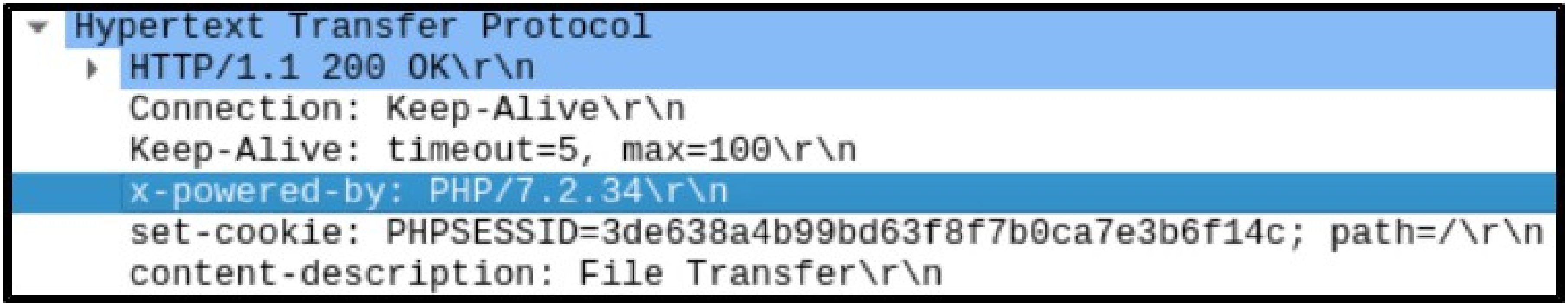
# Q5: What is the name of the webserver of the malicious IP from which the zip file was downloaded?



```
transfer-encoding: chunked\r\n
date: Fri, 24 Sep 2021 16:44:06 GMT\r\n
server: LiteSpeed\r\n
strict-transport-security: max-age=63072000; includeSubDomains\r\n
x-frame-options: SAMEORIGIN\r\n
x-content-type-options: nosniff\r\n
```

This question is asking for the name of the software the webserver is using

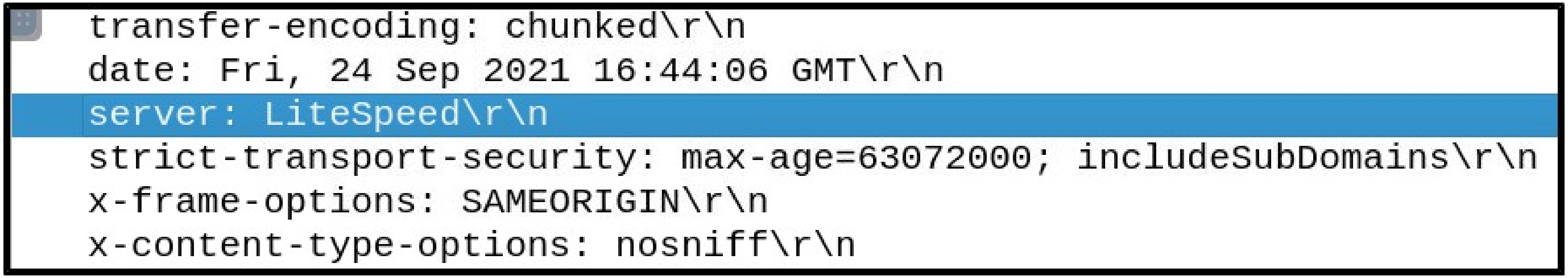
# Q6: What is the version of the webserver from the previous question?



```
▾ Hypertext Transfer Protocol
   ▸ HTTP/1.1 200 OK\r\n
     Connection: Keep-Alive\r\n
     Keep-Alive: timeout=5, max=100\r\n
     x-powered-by: PHP/7.2.34\r\n
     set-cookie: PHPSESSID=3de638a4b99bd63f8f7b0ca7e3b6f14c; path=/\r\n
     content-description: File Transfer\r\n
```

We're looking for a software version number for this question

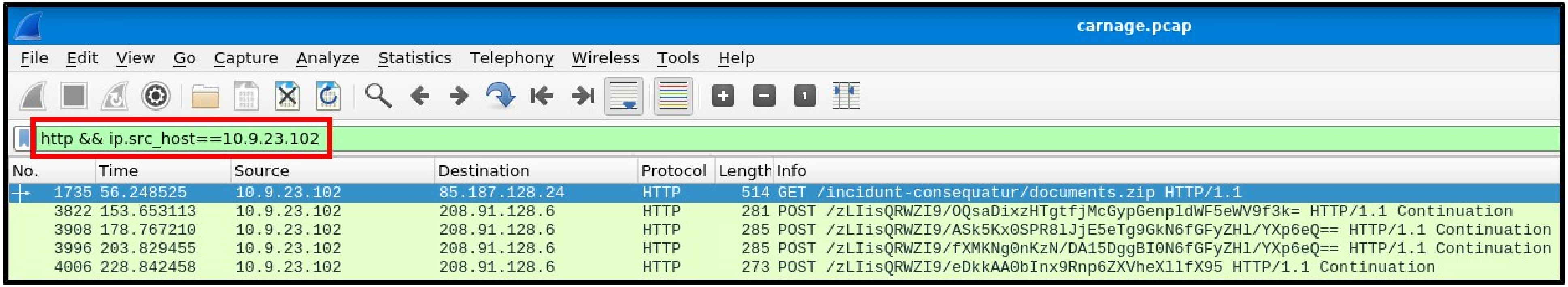
# Let's Move Away From The Official Questions



```
transfer-encoding: chunked\r\n
date: Fri, 24 Sep 2021 16:44:06 GMT\r\n
server: LiteSpeed\r\n
strict-transport-security: max-age=63072000; includeSubDomains\r\n
x-frame-options: SAMEORIGIN\r\n
x-content-type-options: nosniff\r\n
```

The official questions from now on are a bit difficult, so let's answer some different questions

# B1: How many HTTP packets were sent from source IP 10.9.23.102?


carnage.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

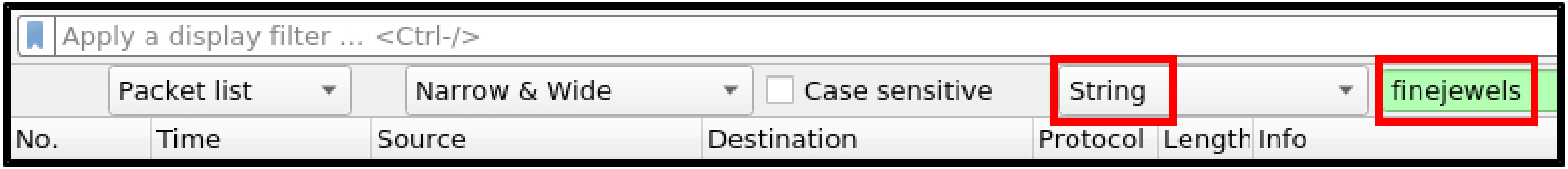
```
http && ip.src_host==10.9.23.102
```

```
No.   Time       Source       Destination    Protocol Length Info
 1735 56.248525  10.9.23.102  85.187.128.24  HTTP      514 GET /incidunt-consequatur/documents.zip HTTP/1.1
 3822 153.653113 10.9.23.102  208.91.128.6   HTTP      281 POST /zLIisQRWZI9/OQsaDixzHTgtfjMcGypGenpldWF5eWV9f3k= HTTP/1.1 Continuation
 3908 178.767210 10.9.23.102  208.91.128.6   HTTP      285 POST /zLIisQRWZI9/ASk5Kx0SPR8lJjE5eTg9GkN6fGFyZHl/YXp6eQ== HTTP/1.1 Continuation
 3996 203.829455 10.9.23.102  208.91.128.6   HTTP      285 POST /zLIisQRWZI9/fXMKNg0nKzN/DA15DggBI0N6fGFyZHl/YXp6eQ== HTTP/1.1 Continuation
 4006 228.842458 10.9.23.102  208.91.128.6   HTTP      273 POST /zLIisQRWZI9/eDkkAA0bInx9Rnp6ZXVheXllfX95 HTTP/1.1 Continuation
```

We can apply more than one display filter at once:

```
http && ip.src_host==10.9.23.102
```

# B2: There's a malware website called finejewels in the packets. What is the full domain name?



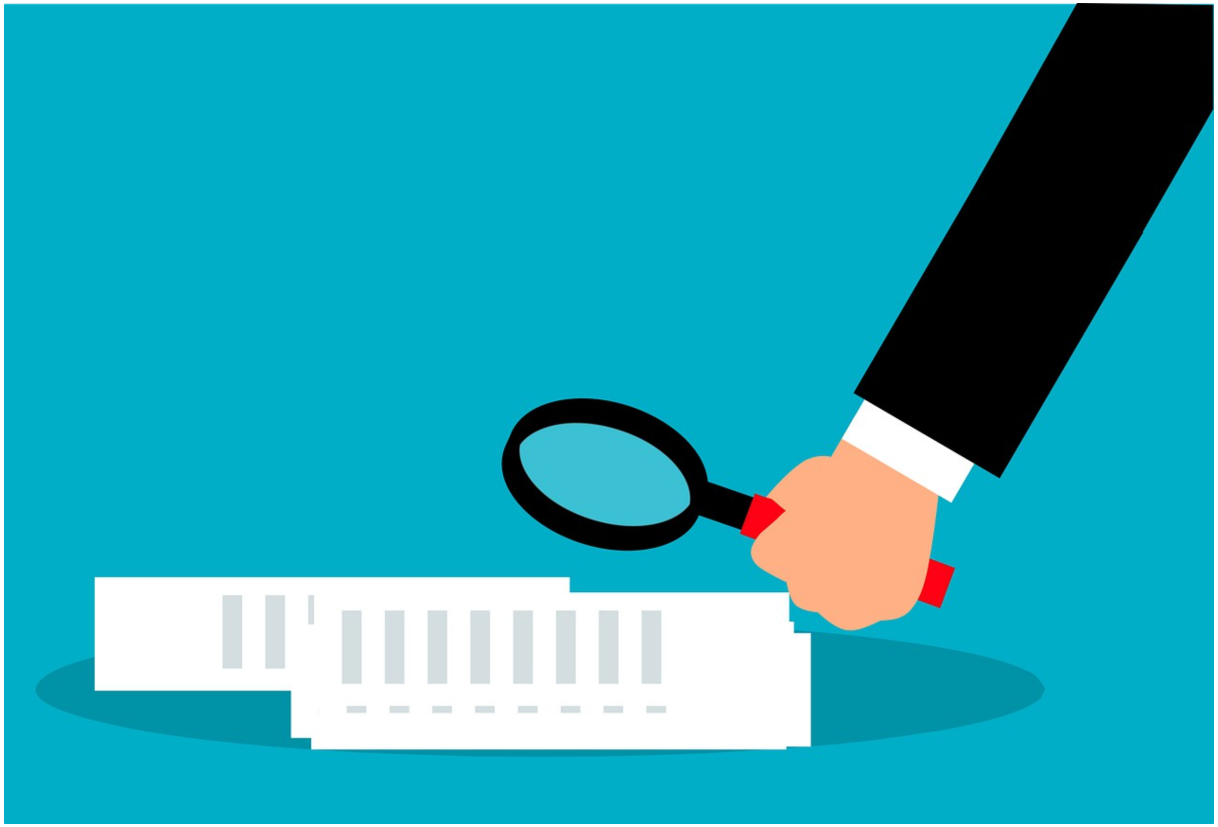
Apply a display filter … <Ctrl-/>

Packet list | Narrow & Wide | □ Case sensitive | String | finejewels

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|

We can use the ctrl+f option in Wireshark to search for text strings in the packet contents

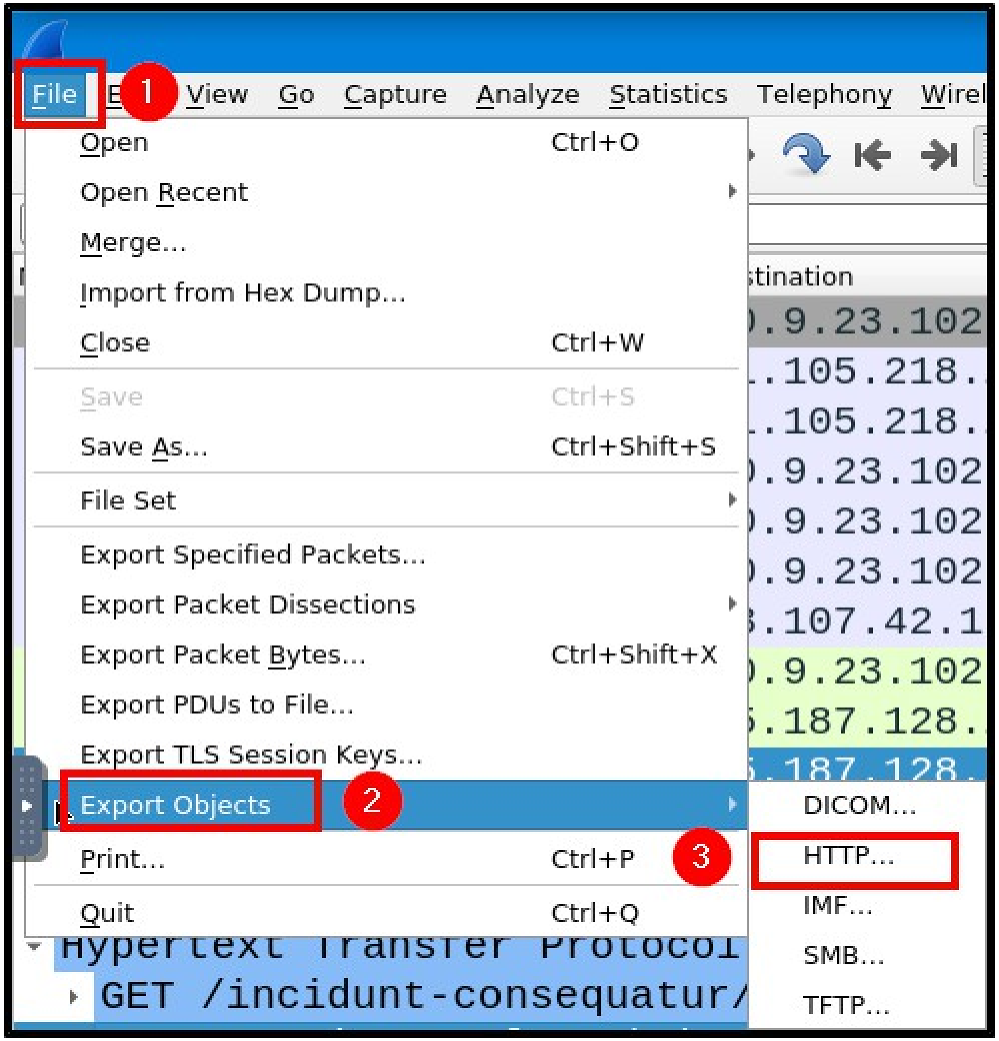
# Summary



Let's review the digital forensics concepts we learned in this workshop:

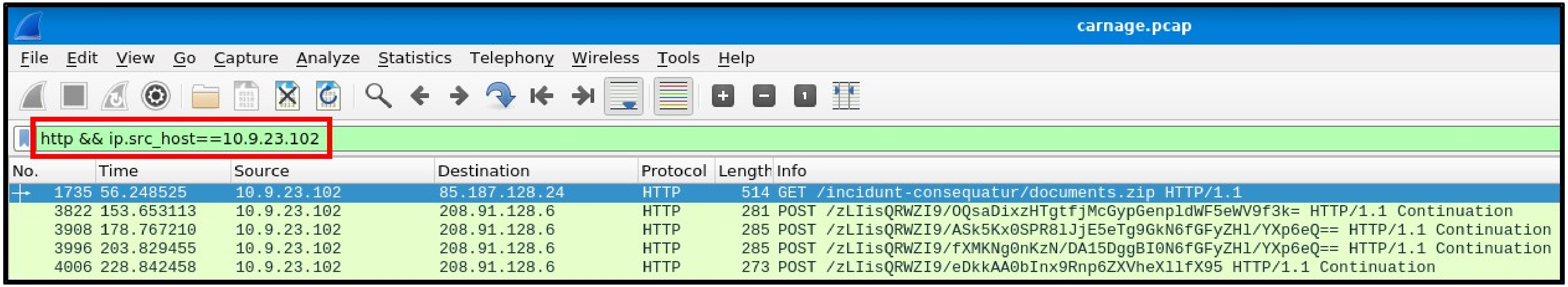
# Exporting Files From Wireshark

We can use the **Export Objects** option in Wireshark to look for files downloaded in the PCAP file, and most files are downloaded using the HTTP protocol



```
Hypertext Transfer Protocol
  GET /incidunt-consequatur/
```

# Isolating IP Addresses



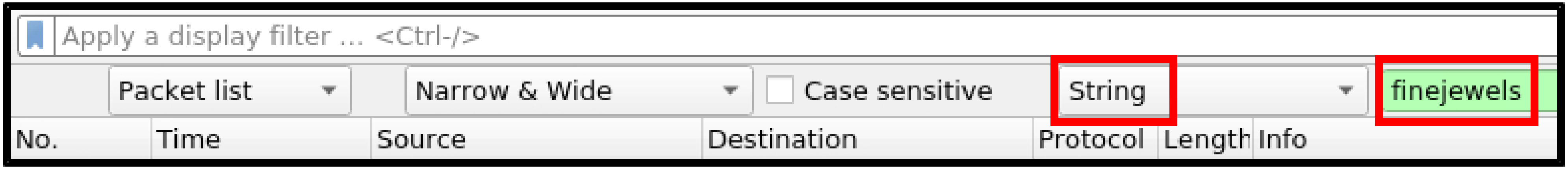
carnage.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http && ip.src_host==10.9.23.102
```

```
No.    Time        Source        Destination     Protocol  Length Info
  1735 56.248525   10.9.23.102   85.187.128.24   HTTP       514 GET /incidunt-consequatur/documents.zip HTTP/1.1
  3822 153.653113  10.9.23.102   208.91.128.6    HTTP       281 POST /zLIisQRWZI9/OQsaDixzHTgtfjMcGypGenpldWF5eWV9f3k= HTTP/1.1 Continuation
  3908 178.767210  10.9.23.102   208.91.128.6    HTTP       285 POST /zLIisQRWZI9/ASk5Kx0SPR8lJjE5eTg9GkN6fGFyZHl/YXp6eQ== HTTP/1.1 Continuation
  3996 203.829455  10.9.23.102   208.91.128.6    HTTP       285 POST /zLIisQRWZI9/fXMKNg0nKzN/DA15DggBI0N6fGFyZHl/YXp6eQ== HTTP/1.1 Continuation
  4006 228.842458  10.9.23.102   208.91.128.6    HTTP       273 POST /zLIisQRWZI9/eDkkAA0bInx9Rnp6ZXVheXllfX95 HTTP/1.1 Continuation
```

We can apply more than one display filter at once: and this is a good way to isolate traffic coming from specific IP addresses

# Searching For Strings in Packet Contents



Apply a display filter … <Ctrl-/>

Packet list ▾ | Narrow & Wide ▾ | □ Case sensitive | String ▾ | finejewels

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|

The search function in Wireshark can be very useful for searching for specific text strings in packets

# What's Next?

In the next digital forensics workshop, we'll learn about a new topic, digital disk image forensics with PicoCTF!

# Extra Credit

Looking for more study material on this workshop's topics?

See this video's description for links to supplemental documents and exercises!

# Until Next Time, HackerFrogs!