SELECTED STADIUM
SOLUTIONS

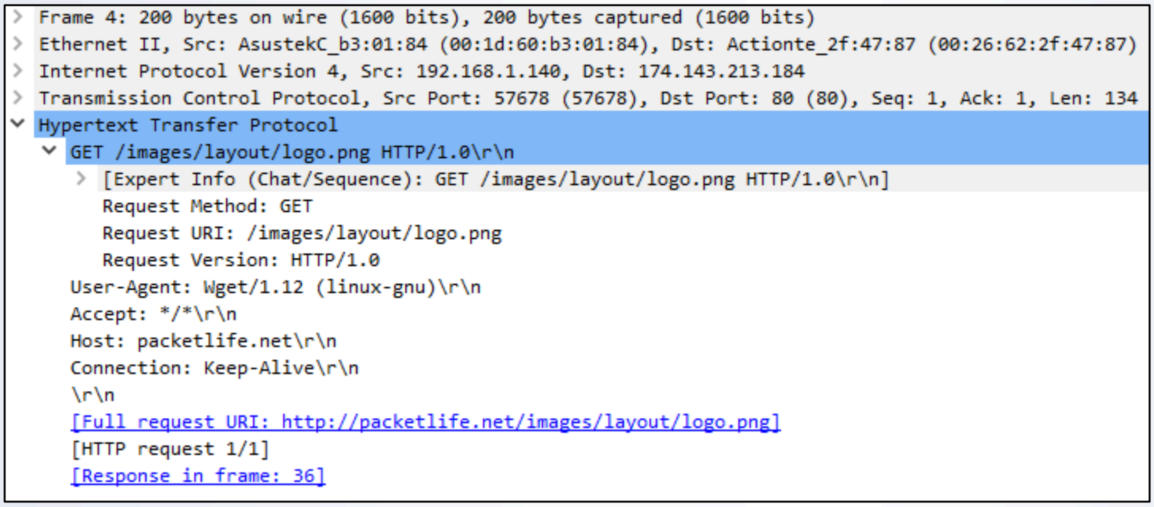
Category: Network Traffic Analysis
Bracket: Bronze
Title: HTTP Challenge **SOLUTION**

This challenge evaluates the participant's ability to understand a packet capture containing Hypertext Transfer Protocol (HTTP) traffic - https://www.dropbox.com/s/e6akwxnsun8bipb/NCL-2015-HTTP2.pcap?dl=0. During the game, it was suggested to use the Wireshark program to solve the challenge.

1. What Linux tool was used to execute a file download?	**wget**
2. What is the name of the web server software that handled the request?	**nginx**
3. What IP address initiated request?	**192.168.1.140**
4. What is the IP address of the server?	**174.143.213.184**
5. What is the MD5 sum of the file downloaded?	**966007c476e0c200fba8b28b250a6379**

Question 1 can be solved by applying the filter below and looking at the Wireshark dissection:

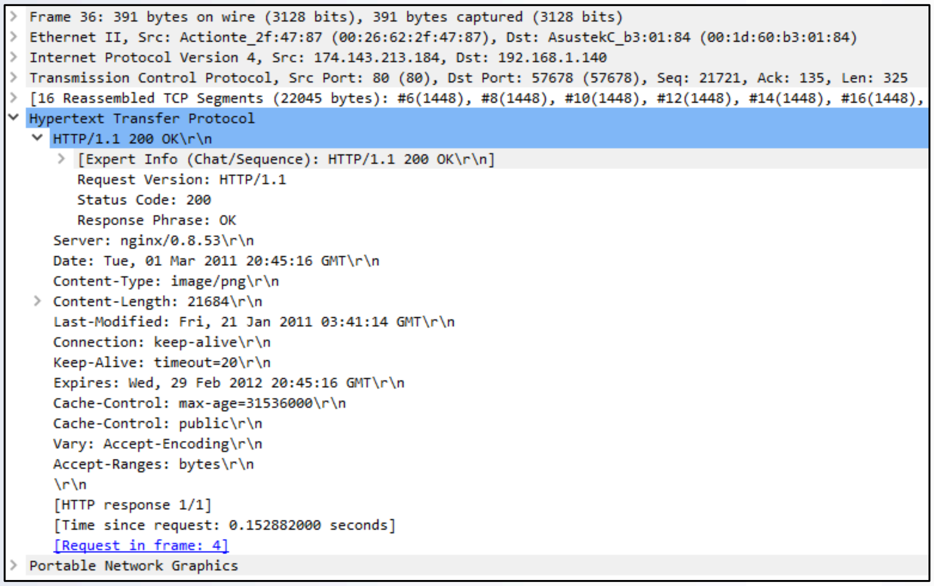
```
http.request
```



```
> Frame 4: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits)
> Ethernet II, Src: AsustekC_b3:01:84 (00:1d:60:b3:01:84), Dst: Actionte_2f:47:87 (00:26:62:2f:47:87)
> Internet Protocol Version 4, Src: 192.168.1.140, Dst: 174.143.213.184
> Transmission Control Protocol, Src Port: 57678 (57678), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 134
v Hypertext Transfer Protocol
  v GET /images/layout/logo.png HTTP/1.0\r\n
    > [Expert Info (Chat/Sequence): GET /images/layout/logo.png HTTP/1.0\r\n]
      Request Method: GET
      Request URI: /images/layout/logo.png
      Request Version: HTTP/1.0
    User-Agent: Wget/1.12 (linux-gnu)\r\n
    Accept: */*\r\n
    Host: packetlife.net\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://packetlife.net/images/layout/logo.png]
    [HTTP request 1/1]
    [Response in frame: 36]
```

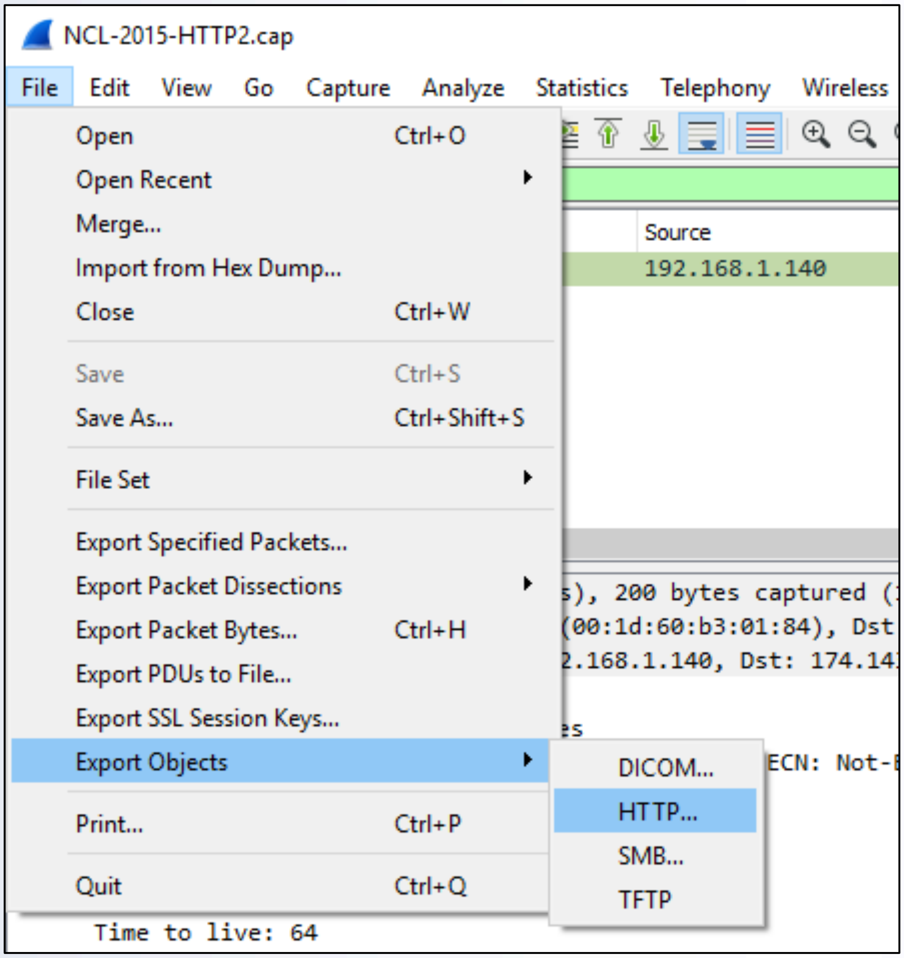
Questions 2-4 can be solved by applying the filter below and looking at the Wireshark dissection:

http.response



```
> Frame 36: 391 bytes on wire (3128 bits), 391 bytes captured (3128 bits)
> Ethernet II, Src: Actionte_2f:47:87 (00:26:62:2f:47:87), Dst: AsustekC_b3:01:84 (00:1d:60:b3:01:84)
> Internet Protocol Version 4, Src: 174.143.213.184, Dst: 192.168.1.140
> Transmission Control Protocol, Src Port: 80 (80), Dst Port: 57678 (57678), Seq: 21721, Ack: 135, Len: 325
> [16 Reassembled TCP Segments (22045 bytes): #6(1448), #8(1448), #10(1448), #12(1448), #14(1448), #16(1448),
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Server: nginx/0.8.53\r\n
    Date: Tue, 01 Mar 2011 20:45:16 GMT\r\n
    Content-Type: image/png\r\n
  > Content-Length: 21684\r\n
    Last-Modified: Fri, 21 Jan 2011 03:41:14 GMT\r\n
    Connection: keep-alive\r\n
    Keep-Alive: timeout=20\r\n
    Expires: Wed, 29 Feb 2012 20:45:16 GMT\r\n
    Cache-Control: max-age=31536000\r\n
    Cache-Control: public\r\n
    Vary: Accept-Encoding\r\n
    Accept-Ranges: bytes\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.152882000 seconds]
    [Request in frame: 4]
> Portable Network Graphics
```

Question 5 can be solved by selecting the Wireshark option, “File > Export Objects > HTTP” and then using the Linux “md5sum” program to calculate the MD5 sum:


NCL-2015-HTTP2.cap
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+H
Export PDUs to File...
Export SSL Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
HTTP...
SMB...
TFTP
Source
192.168.1.140
s), 200 bytes captured (
(00:1d:60:b3:01:84), Dst
2.168.1.140, Dst: 174.14
es
ECN: Not-
Time to live: 64