Topic: Using Wireshark to Perform File Carving

Objectives: After completing this activity the student will be able to:  
 1. Perform file carving using Wireshark to export the object   
 2. Perform file carving based on the magic number of a file and a hex editor  
 3. Identify OSI layer 3 information of sending and receiving hosts

4. Identify OSI layer 4 information of sending and receiving hosts  
 5. Identify OSI layer 7 information of sending and receiving hosts

Watch the “File Carving Using Wireshark” video (11:21). In this video there is a host machine accessing a web page from a web server using Internet Explorer. An image is transferred from the server to the client which is captured using Wireshark. This video will explain the process of obtaining the actual picture transferred using the packets captured by Wireshark. Open Wireshark and download the .PCAPNG file used in the video (name here). Follow along the steps in the video pausing where necessary and completing the steps demonstrated and answer the following questions.

1. How many total packets are in the packet capture file? \_\_\_\_\_\_\_\_\_\_\_\_
2. Which packet number initiates the TCP 3-way handshake? \_\_\_\_\_\_\_\_\_\_
3. What is the value of the Acknowledgement number for the packet in question 2? \_\_\_\_\_\_\_\_\_\_
4. Which TCP flags are set in the packet in question 2? \_\_\_\_\_\_\_\_\_\_
5. Which packet number is the response to the packet in question 2? \_\_\_\_\_\_\_\_\_\_
6. What is the value of the Sequence number for the responding packet? \_\_\_\_\_\_\_\_\_\_
7. What is the value of the Acknowledgement number for the responding packet? \_\_\_\_\_\_\_\_\_\_
8. Which TCP flags are set in the responding packet? \_\_\_\_\_\_\_\_\_\_
9. Which packet represents the third phase of the TCP 3-way handshake? \_\_\_\_\_\_\_
10. What is the value of the Sequence number for the third phase? \_\_\_\_\_\_\_\_\_\_
11. What is the value of the Acknowledgement number for the third phase? \_\_\_\_\_\_\_\_\_\_
12. What is the MAC address of the host sending the web page request?  
    \_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_
13. Who is the vendor of the host NIC sending the request? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
14. What is the MAC address of the MAC address of the web server?  
    \_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_
15. Who is the vendor of the web server NIC? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
16. What is the IP ID for the first packet that contains the penguins.png image? \_\_\_\_\_\_\_\_\_\_\_
17. What is the IP ID for the last packet that contains the penguins.png image? \_\_\_\_\_\_\_\_\_\_\_

Download the “challenge.pcapng” file and use Wireshark to analyze the file and answer the following questions.

1. How many total packets are in the packet capture file? \_\_\_\_\_\_\_\_\_\_\_\_
2. Which packet number initiates the TCP 3-way handshake? \_\_\_\_\_\_\_\_\_\_
3. What is the value of the Acknowledgement number for the packet in question 2? \_\_\_\_\_\_\_\_\_\_
4. Which TCP flags are set in the packet in question 2? \_\_\_\_\_\_\_\_\_\_
5. Which packet number is the response to the packet in question 2? \_\_\_\_\_\_\_\_\_\_
6. What is the value of the Sequence number for the responding packet? \_\_\_\_\_\_\_\_\_\_
7. What is the value of the Acknowledgement number for the responding packet? \_\_\_\_\_\_\_\_\_\_
8. Which TCP flags are set in the responding packet? \_\_\_\_\_\_\_\_\_\_
9. Which packet represents the third phase of the TCP 3-way handshake? \_\_\_\_\_\_\_
10. What is the value of the Sequence number for the third phase? \_\_\_\_\_\_\_\_\_\_
11. What is the value of the Acknowledgement number for the third phase? \_\_\_\_\_\_\_\_\_\_
12. What is the MAC address of the host sending the request?  
    \_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_
13. Who is the vendor of the host NIC sending the request? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
14. What is the MAC address of the MAC address of the server?  
    \_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_:\_\_\_\_\_\_
15. Who is the vendor of the web server NIC? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
16. What service is the server running? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
17. What protocol is being used to transfer the data? \_\_\_\_\_\_\_\_\_\_\_\_\_\_
18. What is the user name of the account accessing the server? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
19. What is the password of the user account being used? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
20. What is the file that is being transferred? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
21. What is the size of the file being transferred? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
22. What is the IP ID for the first packet that contains the file transferred? \_\_\_\_\_\_\_\_\_\_\_
23. What is the IP ID for the last packet that contains the file transferred? \_\_\_\_\_\_\_\_\_\_\_
24. What is the picture of that is transferred? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
25. Answer the following questions regarding the image (use Phil Harvey’s EXIF tool for best results)  
    1. What is the make and model of the device that took the picture? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
    2. What software was used to edit the picture? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
    3. Who is the author (artist) of the picture? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
    4. When was the picture taken? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
    5. What is the physical address of where the picture was taken?