Collins College of Professional Studies
Division of Computer Science, Mathematics, and Science

Shamar Roberts, William Lentini, Daniel Lake
CSS 1005 Wireless Security

Week 4 Lab: Deep packet inspection with Wireshark

Description of activity: The goal of this lab is to introduce Wireshark, a tool which might be very useful to you during your development as Cybersecurity professionals. It will give you a glimpse on the theoretical aspect of network layers. You will be able to see different layers such as Application, Transport, Network, Link layer (layers 5,4,3,2) with some different protocols that reside on those layers.

Please download the Wireshark Introduction Lab manual located in the link here:

Assessment of the activity: Please answer questions 1-4 of the What to hand in section (last page) to the best of your abilities.

Special notes: You may utilize a Word document to write up your response and upload any appropriate screen shots along your steps. Your Wireshark interface might look a little bit different from what the Lab manual shows, however the functionality should stay fairly the same.

Please upload the document as **Group-X-CSS-1005-wireshark** either in Word or PDF format in the proper Blackboard section. Remember, this is a group lab, hence collaboration is highly suggested.

The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you've been able to get Wireshark up and running, and have explored some of its capabilities. Answer the following questions, based on yourWireshark experimentation:

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

HTTP, TCP, DHCP, DNS, ARP

2.How long did it take from when the HTTP GET message was sent until the HTTPOK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began.To display the Time field in time-of-day format, select the Wireshark*View*pulldown menu, then select Time*Display Format*, then select*Time-of-day*.)
15:53:59.838232951(OK) - 15:53:59.805922118(GET) = 0.032310841 Seconds

3.What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?
Gaia: 128.119.245.12
My Computer: 192.168.5.4

4.Print the two HTTP messages(GET and OK) referred to in question 2 above. Todo so, select*Print*from the Wireshark*File*command menu, and select the"*Selected Packet Only"*and*"Print as displayed"*radial buttons,and then clickOK.

/home/kali/Downloads/Lab4.pcapng 400 total packets, 12 shown

```
No.     Time               Source                Destination           Protocol Length Info
    389 15:53:59.805922118 192.168.5.4           128.119.245.12        HTTP     412    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 389: 412 bytes on wire (3296 bits), 412 bytes captured (3296 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_5c:65:26 (08:00:27:5c:65:26), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
    Destination: RealtekU_12:35:00 (52:54:00:12:35:00)
    Source: PcsCompu_5c:65:26 (08:00:27:5c:65:26)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.5.4, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55400, Dst Port: 80, Seq: 1, Ack: 1, Len: 358
Hypertext Transfer Protocol
```

HTTP Get

/home/kali/Downloads/Lab4.pcapng 400 total packets, 12 shown

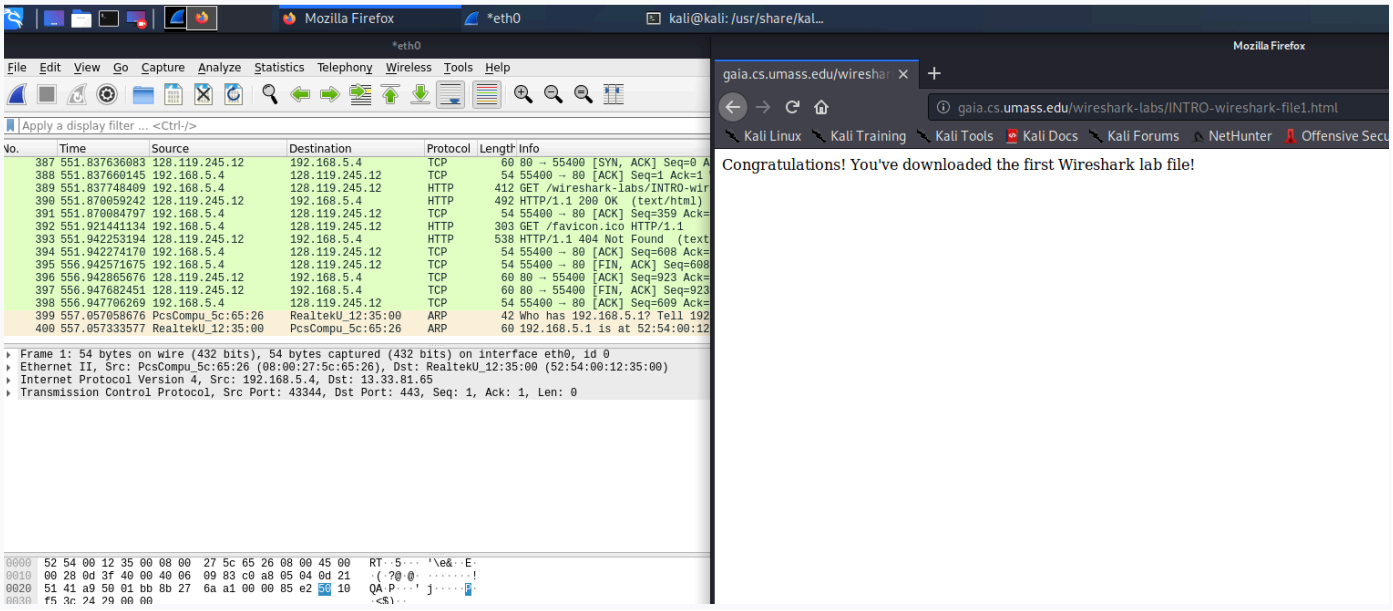
```
No.     Time               Source                Destination           Protocol Length Info
    390 15:53:59.838232951 128.119.245.12        192.168.5.4           HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 390: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface eth0, id 0
Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_5c:65:26 (08:00:27:5c:65:26)
    Destination: PcsCompu_5c:65:26 (08:00:27:5c:65:26)
    Source: RealtekU_12:35:00 (52:54:00:12:35:00)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.5.4
Transmission Control Protocol, Src Port: 80, Dst Port: 55400, Seq: 1, Ack: 359, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```

HTTP Ok

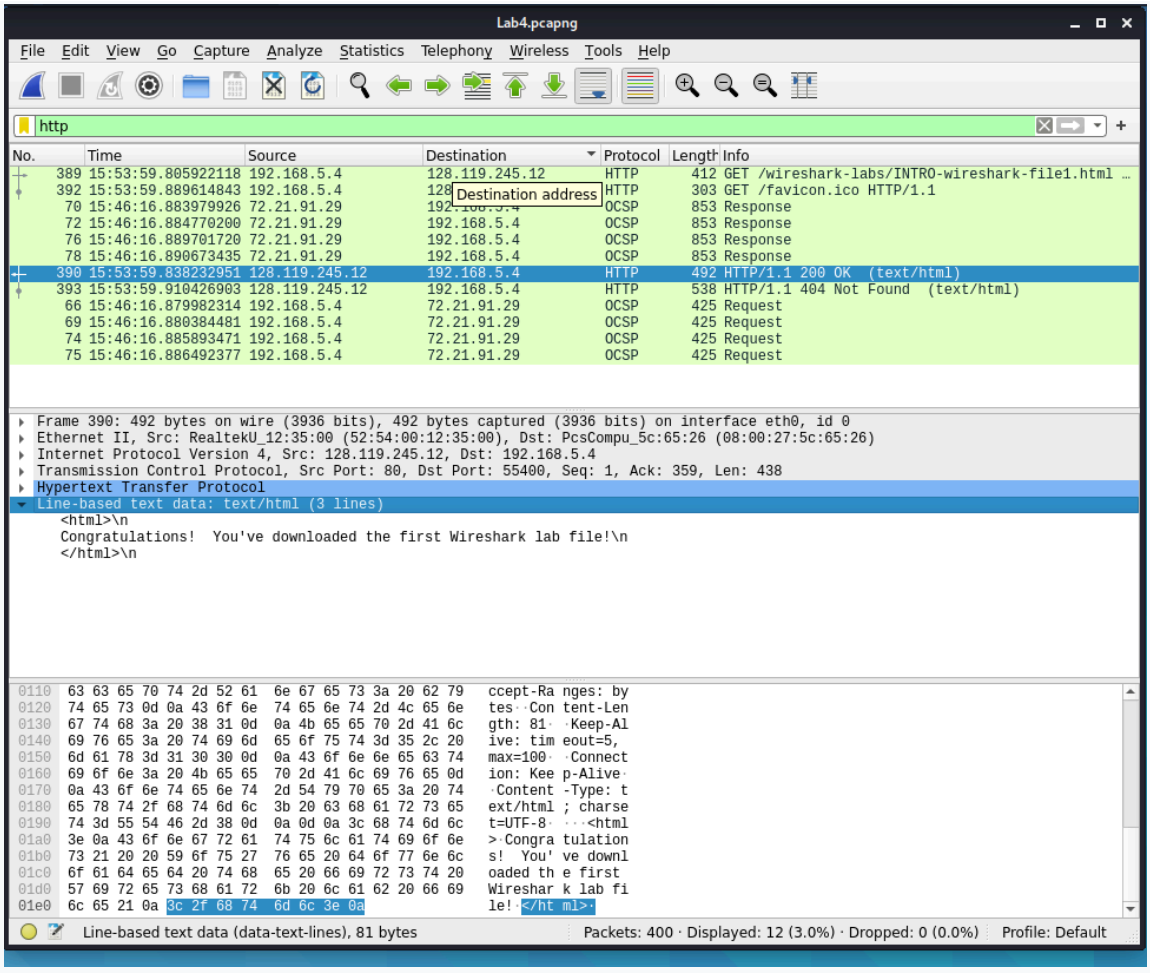
Collins College of Professional Studies
Division of Computer Science, Mathematics, and Science

```
File  Actions  Edit  View  Help

kali@kali:~$ sudo ifconfig
[sudo] password for kali:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.5.4  netmask 255.255.255.0  broadcast 192.168.5.255
        inet6 fe80::a00:27ff:fe5c:6526  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5c:65:26  txqueuelen 1000  (Ethernet)
        RX packets 4700  bytes 6407511 (6.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1450  bytes 123793 (120.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 60  bytes 2956 (2.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 60  bytes 2956 (2.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kali@kali:~$ ping gaia.cs.umass.edu
PING gaia.cs.umass.edu (128.119.245.12) 56(84) bytes of data.
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=1 ttl=48 time=14
.5 ms
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=2 ttl=48 time=14
.1 ms
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=3 ttl=48 time=14
.4 ms
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=4 ttl=48 time=14
.4 ms
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=5 ttl=48 time=14
.4 ms
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=6 ttl=48 time=14
.6 ms
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=7 ttl=48 time=13
.6 ms
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=8 ttl=48 time=14
.2 ms
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=9 ttl=48 time=13
.8 ms
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=10 ttl=48 time=1
3.5 ms
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=11 ttl=48 time=1
4.3 ms
^Z
[1]+  Stopped                 ping gaia.cs.umass.edu
kali@kali:~$
```

IP Address of my Computer and IP address of the website



Result of address and packets captured from wireshark



The HTTPOK message the same as what was produced from link of website