

# Deep Dive in Packet Analysis - Using Wireshark and Network Miner

## OBJECTIVE:

### CompTIA Security+ Domain:

Domain 3: Threats and Vulnerabilities

### CompTIA Security+ Objective Mapping:

Objective 3.7: Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.

## OVERVIEW:

Packet Analysis is the process of sifting through network traffic and finding relevant artifacts. Analyzing network traffic is critical to the protection of information systems.

## OUTCOMES:

In this lab, you will learn to:

1. Use Wireshark to view protocol traffic.
2. View protocols using Wireshark.
3. Parse objects from network traffic.
4. Use NetworkMiner.

### Key Term Description

FTP	File Transfer Protocol is a clear text protocol used to transfer files between systems.
TELNET	TELNET is a clear text protocol that is used to remotely administer a machine.
ping	uses internet control message protocol to check for connectivity between two systems
SSH	Secure shell is used to securely transfer files between two systems.
DNS	The Domain Name System converts IP addresses to names and names to IP addresses.

## Reading Assignment

### Introduction

Packet analysis is the process of sifting through network traffic and finding relevant artifacts. Analyzing network traffic is critical to the protection of information systems. Figure 1 shows the lab topology for this lab. You will be using a pcap file with previously captured network activity in Wireshark to explore that

network traffic.



## Windows 8.1 Attack Machine

**FIGURE 1 - LAB TOPOLOGY**

### Overview of TCP/IP

Recall, the Transmission Control Protocol/Internet Protocol (TCP/IP) networking model consists of four layers: application, transport, network, and data link. Figure 2 shows the different TCP/IP layers. Services run at the application layer and interact with the transport layer using ports. Port numbers are assigned to different services on the operation system. Services, such as File Transfer Protocol (FTP), Telnet, Hypertext Transport Protocol (HTTP), and others, use unique port numbers assigned to them by the operating system. FTP has a port number of 21, Telnet uses the port number of 23, and HTTP has a port number of 80. Port numbers are assigned to a particular protocol and service by the operating system. These port numbers are how TCP/IP knows how to communicate from the transport layer to the application layer. TCP/IP was not initially designed with security in mind so these applications are configured by default to send traffic over the network in plaintext. There are newer services the use encryption like Secure Shell (SSH) and Hypertext Transport Protocol Secure (HTTPS) that are used in place of these older, less secure protocols.

Application (FTP, Telnet, HTTP, etc.)
Transport (TCP/UDP)
Network (IP)
Data Link

**FIGURE 2 - TCP/IP NETWORKING MODEL**

There are several protocols used in this lab which will have an image of the header format to assist in analyzing network traffic when you are using Wireshark.

### Address Resolution Protocol (ARP)

ARP is a protocol used for discovering Media Access Control (MAC) addresses associated with an IP address. When the TCP/IP stack using ARP to determine the MAC address for an Internet Protocol (IP) address, the mappings are stored in an ARP cache and can be manipulated with the arp command. (Note: arp is both a protocol as well as a command).

Hardware Type (16 bits)		Protocol Type (16 bits)
HA Length (8 bits)	PA Length (8 bits)	Operation (16 bits)
Sender Hardware Address (Octets 0-3)		
Sender Hardware Address (Octets 4-5)		Sender Protocol Address (Octets 0-1)
Sender Protocol Address (Octets 2-3)		Target Hardware Address (Octets 0-1)
Target Hardware Address (Octets 2-5)		
Target Protocol Address (Octets 0-3)		

FIGURE 3 - ARP PROTOCOL (SOURCE: ARP)

## Internet Protocol (IP)

IP is a connectionless network layer protocol that transmits packets from a source host to a destination host. It uses a 32-bit address space and usually represented in decimal dotted notation (192.153.10.1). One of the functions of the IP protocol is a routing function that allows for communications between hosts on a local area network (LAN) and a wide area network (WAN). The successor to IP is IPv6. Figure 4 shows the IP protocol.

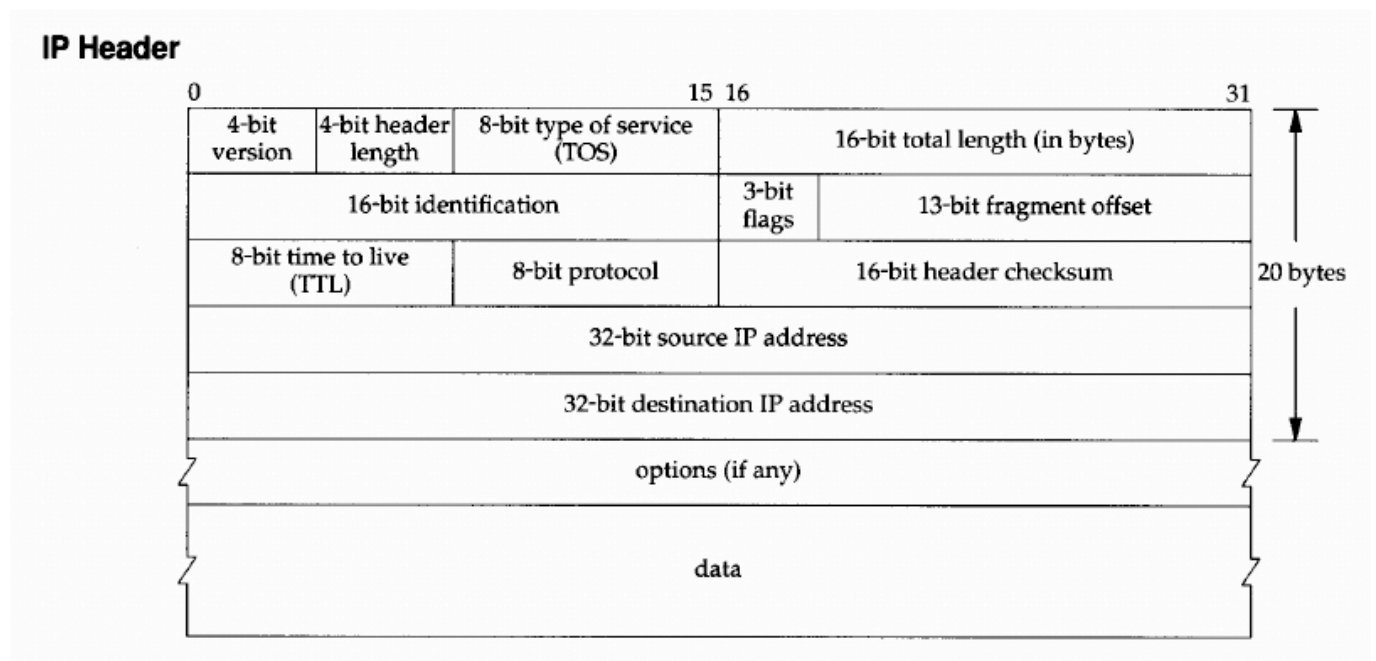
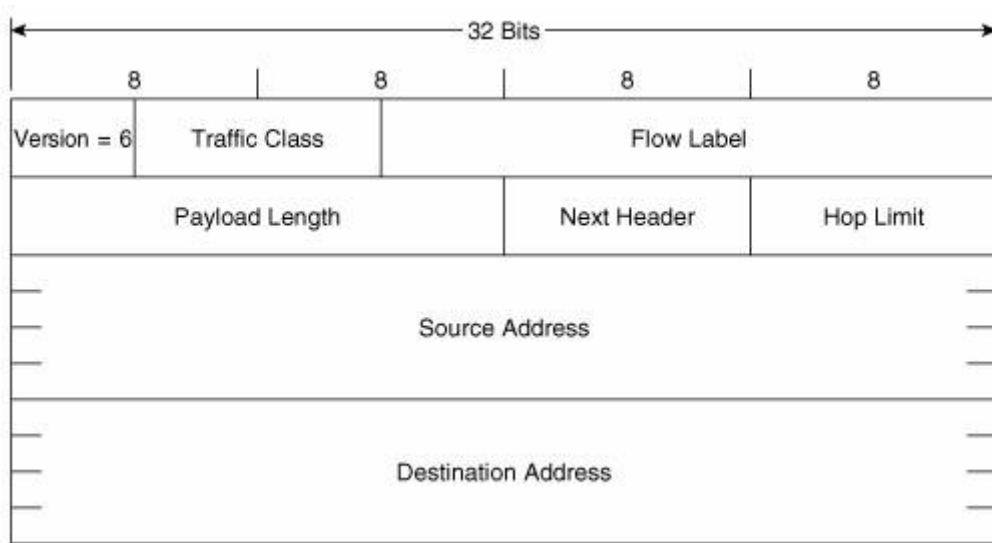


FIGURE 4 - IP PROTOCOL (SOURCE: IP)

## Internet Protocol (IPV6)

IPv6 is the successor to IP, which is also known as IPv4. It is an upgrade to IPv4 to allow for more

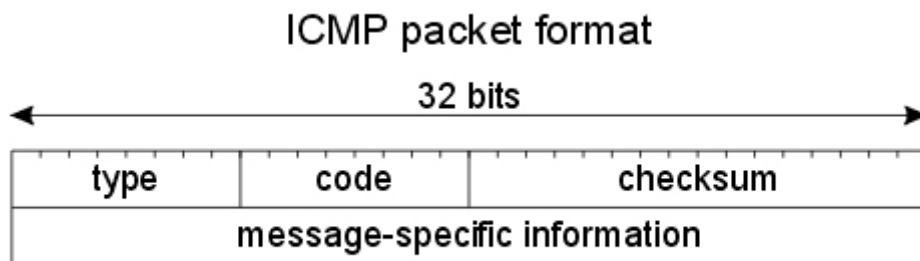
addressing, and its addresses include both numbers and hexadecimal letters. IPv6 also allows for a much larger 128-bit address space. Notice the difference in the size of the IP address. Figure 5 shows IPv6 protocol.



**FIGURE 5 - IPV6 (SOURCE: IPV6)**

### Internet Control Message Protocol (ICMP)

ICMP is a supporting protocol. ICMP is typically used with the ping and traceroute (tracert in Linux) commands. It allows network devices to send error messages and other diagnostic information. Figure 6 shows the ICMP protocol.

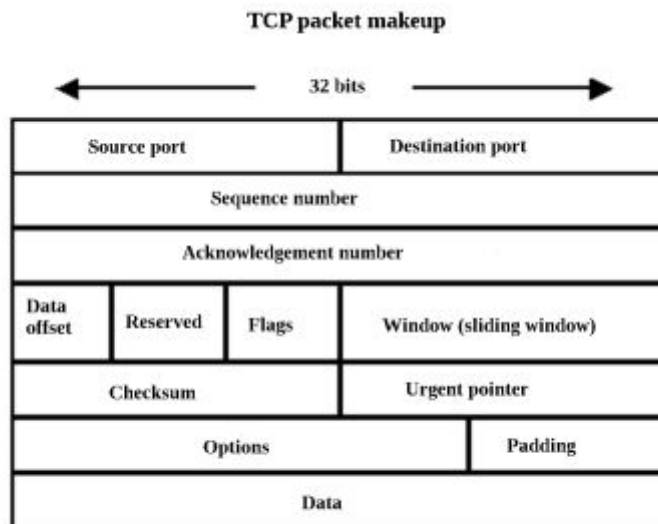


**FIGURE 6 - ICMP PROTOCOL (SOURCE: ICMP)**

### Transport Control Protocol (TCP)

TCP is a protocol that sits at the transport layer of the TCP/IP stack. It is a reliable, ordered, connection oriented, and error checked. TCP's job is to make sure that a connection is created between the source and destination host and reliably send packets over the network. TCP works in three phases: connection setup, data transmission, and connection termination. Port numbers are assigned to particular application layer protocols to allow for applications to talk to each other from source to destination. Figure 7 shows the TCP protocol.

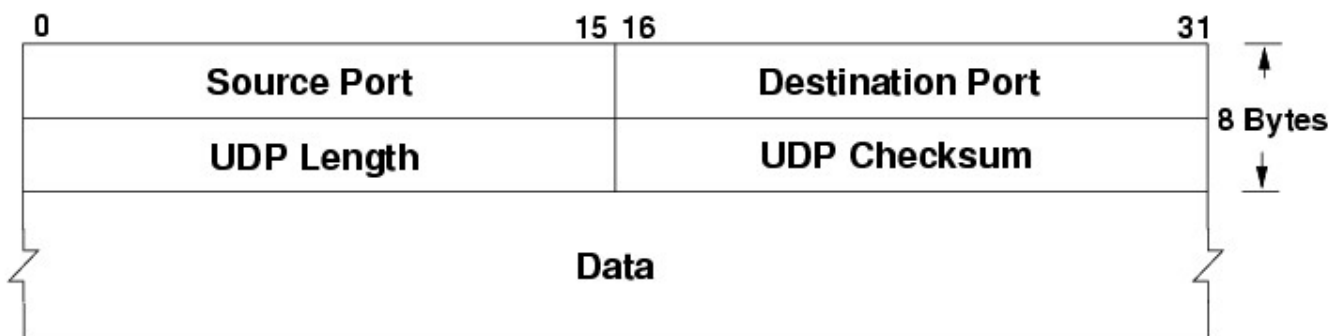




**FIGURE 7 - TCP PROTOCOL (SOURCE: TCP)**

### User Datagram Protocol (UDP)

UDP is a protocol that sits at the transport layer of the TCP/IP stack. It is a connectionless protocol. It provides minimal error checking unlike TCP. It also allows for port numbers to communicate with application layer protocols. Figure 8 shows the UDP protocol.



**FIGURE 8 - UDP PROTOCOL (SOURCE: UDP)**

### File Transfer Protocol (FTP) (Port 20/21)

FTP, which uses TCP, is a protocol that allows for transfer of files between systems and runs on top of TCP. The different layers and protocols that run FTP are shown in Figure 9. All data and credentials are transmitted over the network in clear text. It is a very insecure protocol. FTP can be secured in different ways using the Secure Sockets Layer (SSL) as one example, but Secure Copy (SCP) can be used as the secure alternative also and it is easier to configure because it comes with SSH. In this lab, the Kali machine will act as the FTP client and the Windows Server will host the FTP server.

<b>Application</b>	<b>FTP</b>
<b>Transport</b>	<b>TCP</b>
<b>Network</b>	<b>IP</b>
<b>Data Link</b>	<b>Ethernet</b>

**FIGURE 9 - FTP PROTOCOL STACK**

## Post Office Protocol (POP3) (Port 110)

POP3, which uses TCP, is an application layer protocol that provides a way for users to read e-mail from an e-mail server. Figure 10 shows the protocol stack for POP.

<b>Application</b>	<b>POP</b>
<b>Transport</b>	<b>TCP</b>
<b>Network</b>	<b>IP</b>
<b>Data Link</b>	<b>Ethernet</b>

FIGURE 10 - POP PROTOCOL STACK

## Simple Mail Transfer Protocol (SMTP)

SMTP, which uses TCP, is an application layer protocol that provides a way for users to send e-mail from an e-mail server. Figure 11 shows the protocol stack for SMTP.

<b>Application</b>	<b>SMTP</b>
<b>Transport</b>	<b>TCP</b>
<b>Network</b>	<b>IP</b>
<b>Data Link</b>	<b>Ethernet</b>

FIGURE 11 - SMTP PROTOCOL STACK

## Domain Name System (DNS)

DNS, which uses UDP and TCP, is a hierarchical naming system for network devices on a network called a domain. DNS uses UDP for lookups and TCP for zone transfers. Each network device can have a domain name associated with it. DNS allows for translation between a fully qualified domain name (F.Q.D.N) and an IP address on a network. Users will use the domain name at the application layer, and the TCP/IP translates that into an IP address to be transmitted onto a network.

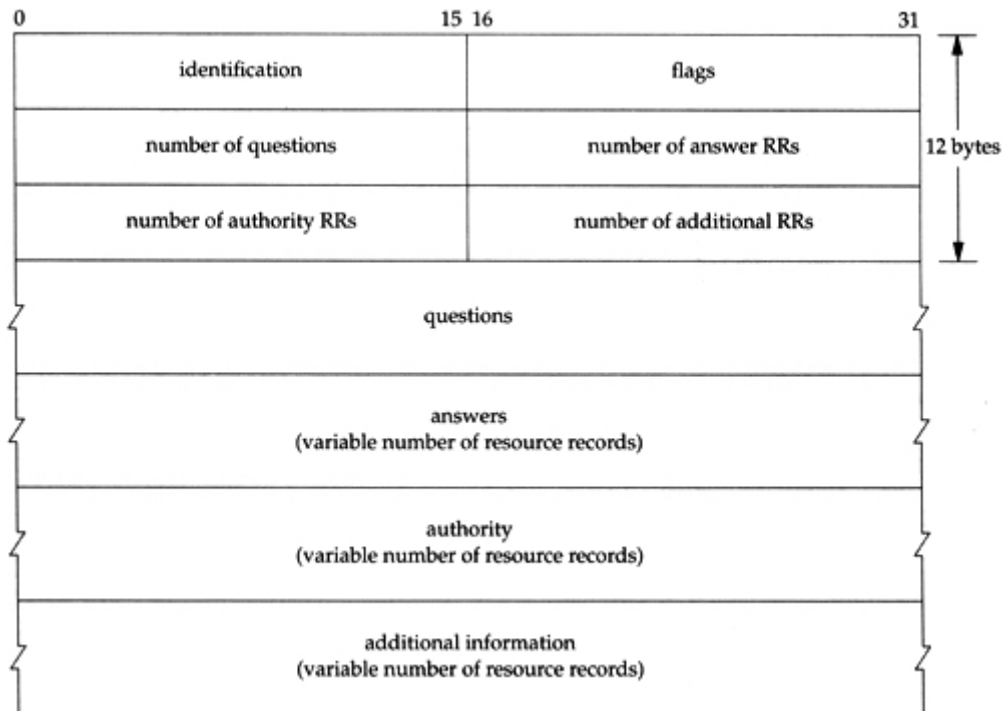


FIGURE 12 - DNS PROTOCOL (SOURCE: DNS)

Figure 13 shows the protocol stack for DNS.

<b>Application</b>	<b>DNS</b>
<b>Transport</b>	<b>UDP</b>

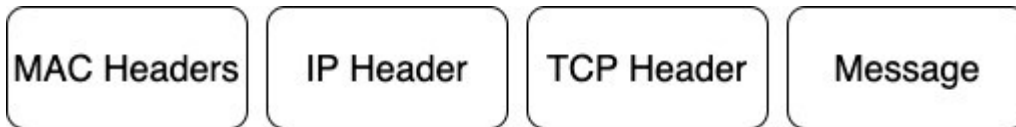
<b>Network</b>	<b>IP</b>
<b>Data Link</b>	<b>Ethernet</b>

**FIGURE 13 - DNS PROTOCOL STACK**

## Examining Protocol Traffic in Wireshark

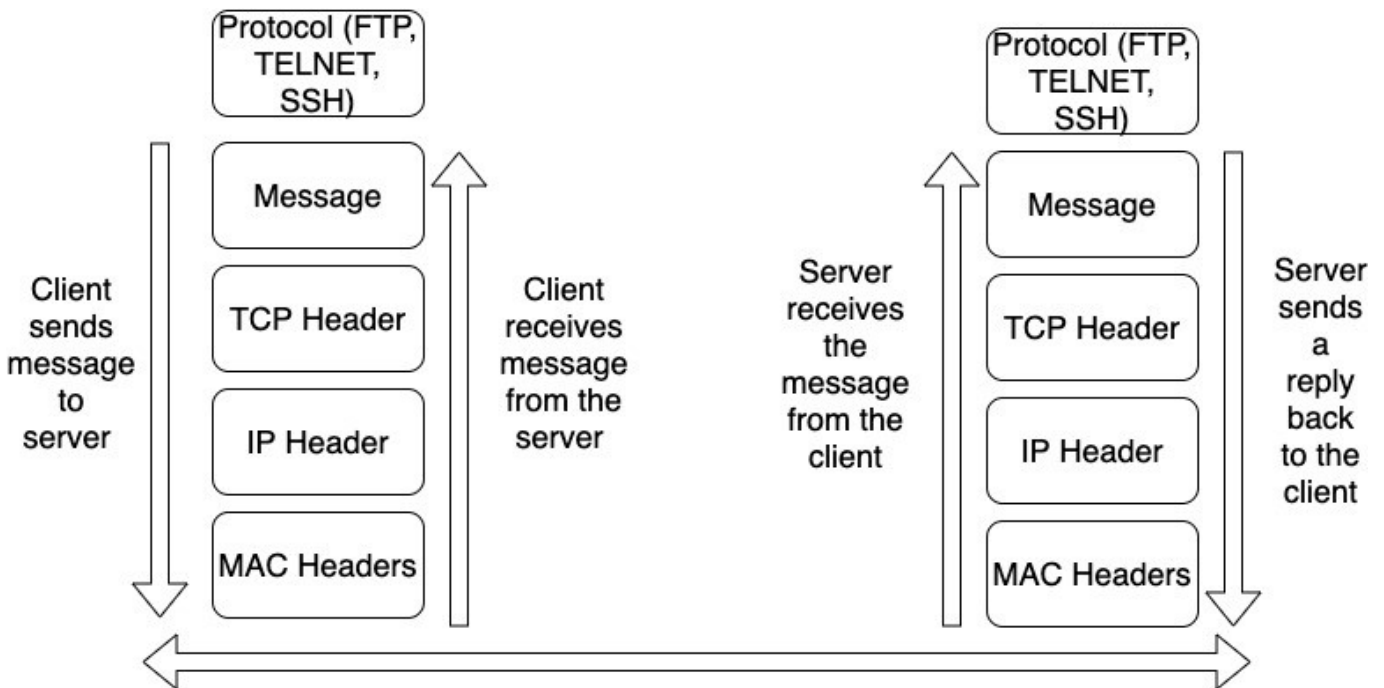
Wireshark is a network protocol analyzer. It allows you to inspect and capture packets on your network. It allows you to inspect the traffic that is transmitting on your network.

The format for a packet that is transmitted over a network usually looks like in Figure 14.



**FIGURE 14 - PACKET FORMAT**

This relates to the layers in the TCP/IP protocol stack. Media Access Control (MAC) header is Ethernet, Internet Protocol (IP) header is the network/Internet layer, TCP header is the transport layer, and the message is the application layer. When a message is transmitted over the network, it encapsulates the header from each of the layers before it transmits onto the network. When the message is received, the headers are stripped off as it works its way up the protocol stack to the application. Figure 15 illustrates how a message flows from the client to the server.



**FIGURE 15 - MESSAGE FLOW FROM CLIENT TO SERVER AND BACK**

Wireshark provides a user interface that allows you to filter your network traffic and analyze that traffic. A system administrator can use Wireshark if he or she suspects there might be nefarious traffic that the firewall and intrusion detection system is not detecting. A system administrator needs to know the protocols in depth to grasp the information being transmitted on the network. Figure 16 shows the user interface for Wireshark. You open a captured network traffic file and the first step is to filter the traffic which is called a DisplayFilter.

A DisplayFilter allows you to only see traffic that you want to see. You can filter on items like the tcp.port number, the protocol type, IP addresses, etc. For more information on DisplayFilter, see this [link](#). To fully

appreciate the details of the headers of the different protocols at the different layers, you need to review the header information. Wikipedia is a good source of header information for the different protocols used on a network. Once the filter is set, the results appear in #2. As you change the DisplayFilter, you can zero in on what you want to see. When you click on a packet, the packet info appears in #3. Details about the selected link is in the second part of the window. You can examine the details of that particular part of the captured data. The #4 of the screenshot shows the file in hexadecimal format on the left side of the pane.

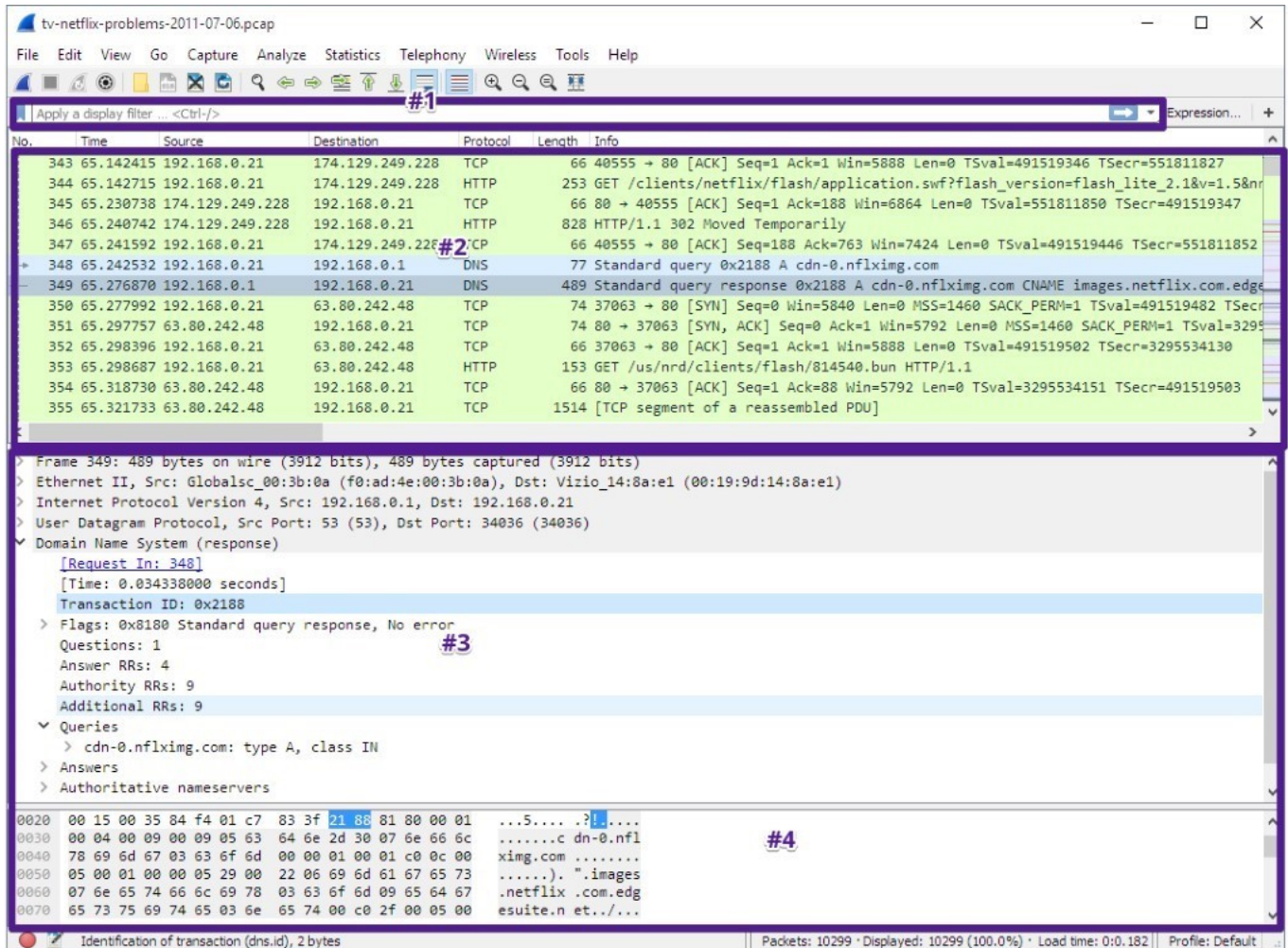


FIGURE 16 - WIRESHARK INTERFACE

## Network Miner

Network miner is Network Forensic Analysis tool (NFAT) that runs on Windows, Linux, MacOS X, and FreeBSD. It can be used as a passive packet sniffer or a network analysis tools using PCAP files. Network Miner can extract images, files, e-mails, certificates, credentials, cookies, passwords, and others artifacts using a PCAP file or by directly sniffing network traffic. Figure 17 shows the user interface for Network Miner.

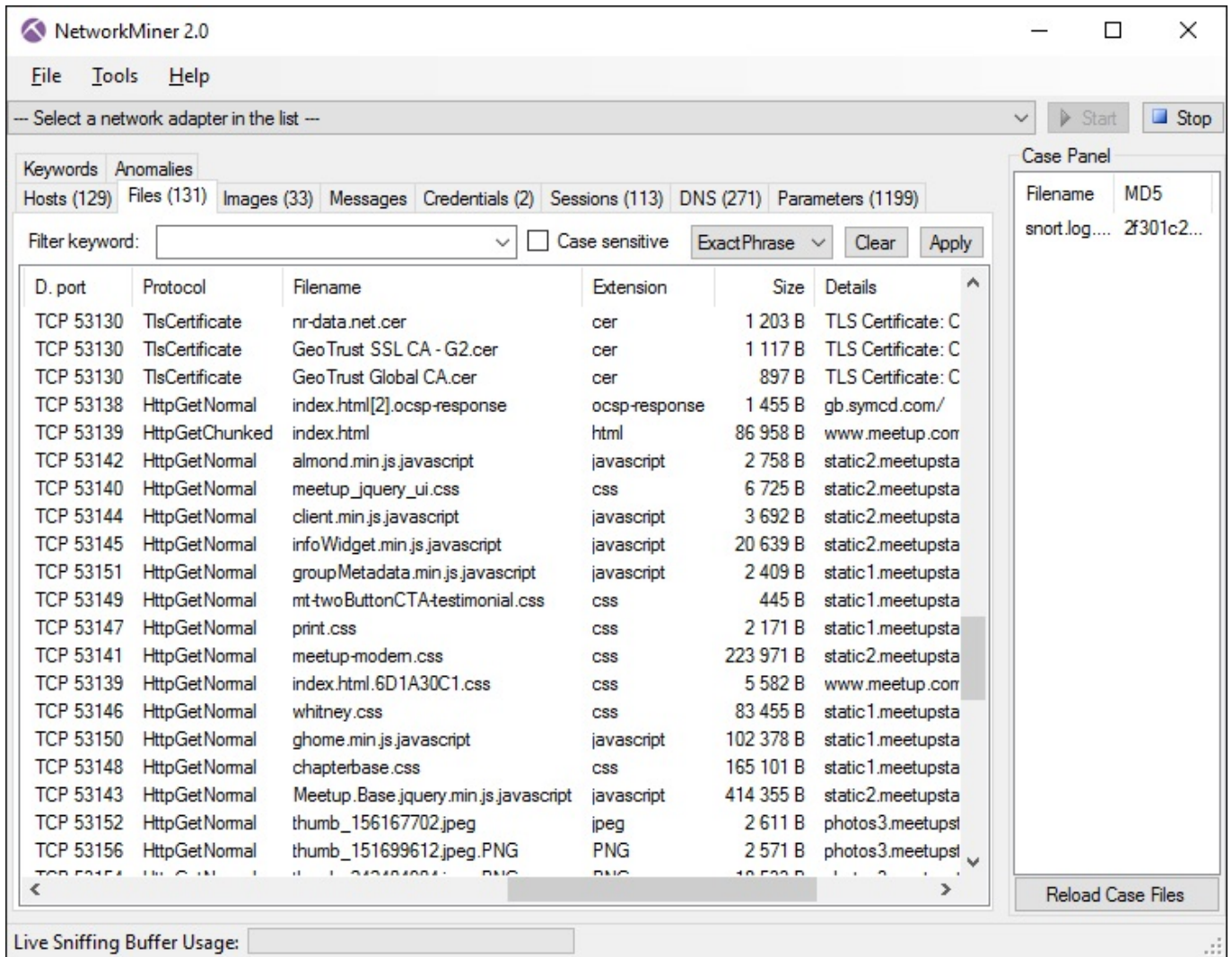


FIGURE 17 - NETWORK MINER INTERFACE (SOURCE: NETWORKMINER)

## CONCLUSION:

In this lab, you will be using Wireshark to analyze different protocols at different layers. You will also use Network Miner to extract images and files.

## Viewing Protocols With Wireshark

1. **Click** on the external [Windows 8.1 icon](#) on the topology.

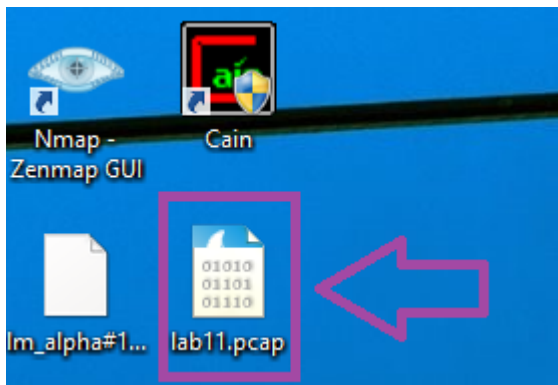




Windows 8.1 Attack Machine

## WINDOWS 8.1 MACHINE

2. **Double-click** on the `lab11.pcap` Wireshark file in the list.



## CAPTURE FILE

3. **Type** `ipv6` in the Wireshark filter pane and then **click** `Apply` to view `IPv6` traffic.

No.	Time	Source	Destination	Protocol	Length	Info
593	52.853953	fe80::78d5:d63:3ede:ff02::1:3		LLMNR	94	Standard query 0x4ed4 A METASPLOITABLE
595	52.959123	fe80::78d5:d63:3ede:ff02::1:3		LLMNR	94	Standard query 0x4ed4 A METASPLOITABLE
622	77.415018	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
624	78.412214	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
625	80.412283	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
626	84.412245	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
627	92.412302	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
680	108.412424	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
831	140.412547	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
5084	433.781238	fe80::78d5:d63:3ede:ff02::1:3		LLMNR	84	Standard query 0x6385 A wpad
5086	433.880572	fe80::78d5:d63:3ede:ff02::1:3		LLMNR	84	Standard query 0x6385 A wpad
5187	504.414508	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
5188	505.411983	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
5189	507.411999	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
5190	511.412020	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
5191	519.412001	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
5192	535.412099	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
5271	567.428199	fe80::78d5:d63:3ede:ff02::1:2		DHCPv6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
19550	825.880090	fe80::78d5:d63:3ede:ff02::1:3		LLMNR	86	Standard query 0x61a2 A server
19552	825.975150	fe80::78d5:d63:3ede:ff02::1:3		LLMNR	86	Standard query 0x61a2 A server
19576	833.892281	fe80::78d5:d63:3ede:ff02::1:3		LLMNR	84	Standard query 0x6e4a A wpad
19578	833.990496	fe80::78d5:d63:3ede:ff02::1:3		LLMNR	84	Standard query 0x6e4a A wpad
19584	836.445026	fe80::78d5:d63:3ede:ff02::1:3		LLMNR	86	Standard query 0xb670 A server

## WIRESHARK FILTER

4. Type `ip and !ipv6` in the Wireshark filter pane and then click **Apply** to view IPv4 traffic.

No.	Time	Source	Destination	Protocol	Length	Info
19585	836.445163	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0xb670 A server
19587	836.552534	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0xb670 A server
19588	836.755678	172.16.200.200	172.16.200.255	NBNS	92	Name query NB SERVER<00>
19589	836.755753	172.16.200.100	172.16.200.200	NBNS	104	Name query response NB 172.16.200.100
19591	836.756206	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x0a4f A server
19593	836.865581	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x0a4f A server
19594	837.068805	172.16.200.200	172.16.200.100	TCP	66	1255-80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
19595	837.068886	172.16.200.100	172.16.200.200	TCP	66	80-1255 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 WS=1 SACK_PERM=1
19596	837.068960	172.16.200.200	172.16.200.100	TCP	54	1255-80 [ACK] Seq=1 Ack=1 win=65536 Len=0
19597	837.069065	172.16.200.200	172.16.200.100	HTTP	149	OPTIONS / HTTP/1.1
19598	837.203652	172.16.200.100	172.16.200.200	HTTP	460	HTTP/1.1 200 OK
19599	837.412421	172.16.200.200	172.16.200.100	TCP	54	1255-80 [ACK] Seq=96 Ack=407 win=65280 Len=0
19601	840.199281	172.16.200.200	224.0.0.252	LLMNR	64	Standard query 0xa98f A wpad
19603	840.302589	172.16.200.200	224.0.0.252	LLMNR	64	Standard query 0xa98f A wpad
19604	840.506206	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19605	841.255473	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19606	842.005596	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19608	842.758863	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x9b28 A server
19610	842.865587	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x9b28 A server
19612	843.069116	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x7600 A server
19614	843.177555	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x7600 A server
19615	843.380884	172.16.200.200	172.16.200.100	TCP	66	1256-80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
19616	843.380952	172.16.200.100	172.16.200.200	TCP	66	80-1256 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 WS=1 SACK_PERM=1

## WIRESHARK FILTER

5. Type `ip.addr == 224.0.0.0/8` in the filter pane and then click **Apply** to view multicast traffic.

No.	Time	Source	Destination	Protocol	Length	Info
594	52.854161	172.16.200.200	224.0.0.252	LLMNR	74	Standard query 0x4ed4 A METASPLOITABLE
596	52.959186	172.16.200.200	224.0.0.252	LLMNR	74	Standard query 0x4ed4 A METASPLOITABLE
5085	433.781349	172.16.200.200	224.0.0.252	LLMNR	64	Standard query 0x6385 A wpad
5087	433.880633	172.16.200.200	224.0.0.252	LLMNR	64	Standard query 0x6385 A wpad
19551	825.880200	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x61a2 A server
19553	825.975251	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x61a2 A server
19577	833.892405	172.16.200.200	224.0.0.252	LLMNR	64	Standard query 0x6e4a A wpad
19579	833.990558	172.16.200.200	224.0.0.252	LLMNR	64	Standard query 0x6e4a A wpad
19585	836.445163	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0xbe70 A server
19587	836.552534	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0xbe70 A server
19591	836.756206	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x0a4f A server
19593	836.865581	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x0a4f A server
19601	840.199281	172.16.200.200	224.0.0.252	LLMNR	64	Standard query 0xa98f A wpad
19603	840.302589	172.16.200.200	224.0.0.252	LLMNR	64	Standard query 0xa98f A wpad
19608	842.758863	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x9b28 A server
19610	842.865587	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x9b28 A server
19612	843.069116	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x7600 A server

## WIRESHARK FILTER

6. Type `ip.addr == 172.16.200.255` in the filter pane and then **click Apply** to view broadcast traffic.

No.	Time	Source	Destination	Protocol	Length	Info
19604	840.506206	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19605	841.255473	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19606	842.005596	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19625	843.694679	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19626	844.443542	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19627	845.193512	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19668	866.615769	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19674	867.365565	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19792	868.115540	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
20469	869.256212	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
20968	870.005540	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
21421	870.755597	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
22081	940.505928	172.16.200.100	172.16.200.255	BROWSEF	243	Local Master Announcement SERVER, Workstation, Server, SQL Server, Domain
27846	1132.34164	172.16.200.30	172.16.200.255	BROWSEF	286	Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue
27847	1132.34167	172.16.200.30	172.16.200.255	BROWSEF	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
27926	1132.90909	172.16.200.100	172.16.200.255	NBNS	92	Name query NB TSCLIENT<00>
27927	1132.90928	172.16.200.100	172.16.200.255	NBNS	92	Name query NB TSCLIENT<20>
27956	1133.64663	172.16.200.100	172.16.200.255	NBNS	92	Name query NB TSCLIENT<00>
27957	1133.64678	172.16.200.100	172.16.200.255	NBNS	92	Name query NB TSCLIENT<20>
28055	1134.39658	172.16.200.100	172.16.200.255	NBNS	92	Name query NB TSCLIENT<00>
28056	1134.39663	172.16.200.100	172.16.200.255	NBNS	92	Name query NB TSCLIENT<20>
28199	1135.14703	172.16.200.100	172.16.200.255	NBNS	92	Name query NB TSCLIENT<00>

## WIRESHARK FILTER

7. Type `icmp` in the filter pane and then **click Apply** to view ICMP traffic.

No.	Time	Source	Destination	Protocol	Length	Info
565	34.955034	172.16.200.100	172.16.200.50	ICMP	98	Echo (ping) reply id=0x072d, seq=16/4096, ttl=128 (request in 564)
566	35.954026	172.16.200.50	172.16.200.100	ICMP	98	Echo (ping) request id=0x072d, seq=17/4352, ttl=64 (reply in 567)
567	35.954110	172.16.200.100	172.16.200.50	ICMP	98	Echo (ping) reply id=0x072d, seq=17/4352, ttl=128 (request in 566)
568	36.954058	172.16.200.50	172.16.200.100	ICMP	98	Echo (ping) request id=0x072d, seq=18/4608, ttl=64 (reply in 569)
569	36.954156	172.16.200.100	172.16.200.50	ICMP	98	Echo (ping) reply id=0x072d, seq=18/4608, ttl=128 (request in 568)
570	37.954008	172.16.200.50	172.16.200.100	ICMP	98	Echo (ping) request id=0x072d, seq=19/4864, ttl=64 (reply in 571)
571	37.954107	172.16.200.100	172.16.200.50	ICMP	98	Echo (ping) reply id=0x072d, seq=19/4864, ttl=128 (request in 570)
572	38.953051	172.16.200.50	172.16.200.100	ICMP	98	Echo (ping) request id=0x072d, seq=20/5120, ttl=64 (reply in 573)
573	38.953162	172.16.200.100	172.16.200.50	ICMP	98	Echo (ping) reply id=0x072d, seq=20/5120, ttl=128 (request in 572)
574	39.953034	172.16.200.50	172.16.200.100	ICMP	98	Echo (ping) request id=0x072d, seq=21/5376, ttl=64 (reply in 575)
575	39.953125	172.16.200.100	172.16.200.50	ICMP	98	Echo (ping) reply id=0x072d, seq=21/5376, ttl=128 (request in 574)
576	40.953027	172.16.200.50	172.16.200.100	ICMP	98	Echo (ping) request id=0x072d, seq=22/5632, ttl=64 (reply in 577)
577	40.953121	172.16.200.100	172.16.200.50	ICMP	98	Echo (ping) reply id=0x072d, seq=22/5632, ttl=128 (request in 576)
578	41.953038	172.16.200.50	172.16.200.100	ICMP	98	Echo (ping) request id=0x072d, seq=23/5888, ttl=64 (reply in 579)
579	41.953129	172.16.200.100	172.16.200.50	ICMP	98	Echo (ping) reply id=0x072d, seq=23/5888, ttl=128 (request in 578)
580	42.953048	172.16.200.50	172.16.200.100	ICMP	98	Echo (ping) request id=0x072d, seq=24/6144, ttl=64 (reply in 581)
581	42.953140	172.16.200.100	172.16.200.50	ICMP	98	Echo (ping) reply id=0x072d, seq=24/6144, ttl=128 (request in 580)
582	43.953072	172.16.200.50	172.16.200.100	ICMP	98	Echo (ping) request id=0x072d, seq=25/6400, ttl=64 (reply in 583)
583	43.953153	172.16.200.100	172.16.200.50	ICMP	98	Echo (ping) reply id=0x072d, seq=25/6400, ttl=128 (request in 582)
584	44.953062	172.16.200.50	172.16.200.100	ICMP	98	Echo (ping) request id=0x072d, seq=26/6656, ttl=64 (reply in 585)

## WIRESHARK FILTER

8. Type `arp` in the filter pane and then **click Apply** to view ARP traffic.



No.	Time	Source	Destination	Protocol	Length	Info
5194	566.587001	Vmware_f3:68:90	Vmware_98:00:1a	ARP	42	172.16.200.2 is at 00:50:56:f3:68:90
18087	717.046052	Vmware_98:00:1a	Broadcast	ARP	42	who has 172.16.200.100? Tell 172.16.200.200
18088	717.046133	Vmware_43:c9:0d	Vmware_98:00:1a	ARP	42	172.16.200.100 is at 00:0c:29:43:c9:0d
19669	866.870242	Vmware_f3:68:90	Broadcast	ARP	42	who has 172.16.200.200? Tell 172.16.200.2
19670	866.870321	Vmware_98:00:1a	Vmware_f3:68:90	ARP	42	172.16.200.200 is at 00:50:56:98:00:1a
21998	921.974873	Vmware_98:00:1a	Vmware_f3:68:90	ARP	42	who has 172.16.200.2? Tell 172.16.200.200
21999	921.974893	Vmware_f3:68:90	Vmware_98:00:1a	ARP	42	172.16.200.2 is at 00:50:56:f3:68:90
22068	936.474805	Vmware_98:00:1a	Vmware_43:c9:0d	ARP	42	who has 172.16.200.100? Tell 172.16.200.200
22069	936.474873	Vmware_43:c9:0d	Vmware_98:00:1a	ARP	42	172.16.200.100 is at 00:0c:29:43:c9:0d
22082	945.671060	Vmware_98:00:1a	Broadcast	ARP	42	who has 172.16.200.30? Tell 172.16.200.200
22083	945.671137	Vmware_fa:dd:2a	Vmware_98:00:1a	ARP	42	172.16.200.30 is at 00:0c:29:fa:dd:2a
24344	1022.53769	Vmware_98:00:1a	Broadcast	ARP	42	who has 172.16.200.50? Tell 172.16.200.200
24345	1022.53783	Vmware_9a:be:c1	Vmware_98:00:1a	ARP	60	172.16.200.50 is at 00:0c:29:9a:be:c1
24425	1026.21676	Vmware_f3:68:90	Broadcast	ARP	42	who has 172.16.200.50? Tell 172.16.200.2
24426	1026.21690	Vmware_9a:be:c1	Vmware_f3:68:90	ARP	60	172.16.200.50 is at 00:0c:29:9a:be:c1
24461	1027.42744	Vmware_98:00:1a	Broadcast	ARP	42	who has 172.16.200.100? Tell 172.16.200.200
24462	1027.42750	Vmware_43:c9:0d	Vmware_98:00:1a	ARP	42	172.16.200.100 is at 00:0c:29:43:c9:0d
25986	1067.78329	Vmware_fa:dd:2a	Vmware_98:00:1a	ARP	42	who has 172.16.200.200? Tell 172.16.200.30
25987	1067.78338	Vmware_98:00:1a	Vmware_fa:dd:2a	ARP	42	172.16.200.200 is at 00:50:56:98:00:1a
27332	1111.97451	Vmware_98:00:1a	Vmware_f3:68:90	ARP	42	who has 172.16.200.2? Tell 172.16.200.200
27333	1111.97453	Vmware_f3:68:90	Vmware_98:00:1a	ARP	42	172.16.200.2 is at 00:50:56:f3:68:90
27859	1132.73412	Vmware_43:c9:0d	Broadcast	ARP	42	who has 172.16.200.50? Tell 172.16.200.100

## WIRESHARK FILTER

9. Type **tcp** in the filter pane and then **click Apply** to view **TCP** traffic. In the bottom pane, **expand Transmission Control Protocol** and then **expand flags** to view **TCP flags**.

lab11.pcap [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from m

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
599	53.165537	172.16.200.200	172.16.200.30	TCP	66	1050-139 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK
600	53.165622	172.16.200.30	172.16.200.200	TCP	66	139-1050 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460
601	53.165708	172.16.200.200	172.16.200.30	NBSS	126	Session request, to METASPLOITABLE<20> from STUDENT-PC<
602	53.165822	172.16.200.30	172.16.200.200	TCP	54	139-1050 [ACK] Seq=1 Ack=73 win=5856 Len=0
603	53.168737	172.16.200.30	172.16.200.200	NBSS	58	Positive session response
604	53.169045	172.16.200.200	172.16.200.30	SMB	213	Negotiate Protocol Request
605	53.169954	172.16.200.30	172.16.200.200	SMB	185	Negotiate Protocol Response
606	53.170481	172.16.200.200	172.16.200.30	SMB	196	Session Setup AndX Request, NTLMSSP_NEGOTIATE
607	53.171335	172.16.200.30	172.16.200.200	SMB	354	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error:
608	53.172052	172.16.200.200	172.16.200.30	SMB	256	Session Setup AndX Request, NTLMSSP_AUTH, User: \
609	53.172615	172.16.200.30	172.16.200.200	SMB	180	Session Setup AndX Response
610	53.172793	172.16.200.200	172.16.200.30	SMB	152	Tree Connect AndX Request, Path: \\METASPLOITABLE\IPC\$
611	53.173783	172.16.200.30	172.16.200.200	SMB	106	Tree Connect AndX Response
612	53.173940	172.16.200.200	172.16.200.30	LANMAN	176	NetServerEnum2 Request, Workstation, Server, SQL Server
613	53.174218	172.16.200.30	172.16.200.200	LANMAN	219	NetServerEnum2 Response
614	53.381075	172.16.200.200	172.16.200.30	TCP	54	1050-139 [ACK] Seq=796 Ack=779 win=64768 Len=0
615	65.678391	172.16.200.200	172.16.200.30	SMB	93	Tree Disconnect Request
616	65.678558	172.16.200.30	172.16.200.200	SMB	93	Tree Disconnect Response
617	65.678655	172.16.200.200	172.16.200.30	SMB	97	Logoff AndX Request
618	65.678720	172.16.200.30	172.16.200.200	SMB	97	Logoff AndX Response
619	65.678892	172.16.200.200	172.16.200.30	TCP	54	1050-139 [FIN, ACK] Seq=878 Ack=861 win=64768 Len=0
620	65.682403	172.16.200.30	172.16.200.200	TCP	54	139-1050 [FIN, ACK] Seq=861 Ack=879 win=9056 Len=0
621	65.682516	172.16.200.200	172.16.200.30	TCP	54	1050-139 [ACK] Seq=879 Ack=862 win=64768 Len=0
630	99.623642	172.16.200.200	172.16.200.100	TCP	66	1051-23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK
631	99.623704	172.16.200.100	172.16.200.200	TCP	66	23-1051 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460

Frame 605: 185 bytes on wire (1480 bits), 185 bytes captured (1480 bits)

Ethernet II, Src: Vmware\_fa:dd:2a (00:0c:29:fa:dd:2a), Dst: Vmware\_98:00:1a (00:50:56:98:00:1a)

Internet Protocol Version 4, Src: 172.16.200.30 (172.16.200.30), Dst: 172.16.200.200 (172.16.200.200)

Transmission Control Protocol, Src Port: 139 (139), Dst Port: 1050 (1050), Seq: 5, Ack: 232, Len: 131

Source Port: 139 (139)  
 Destination Port: 1050 (1050)  
 [Stream index: 0]  
 [TCP Segment Len: 131]  
 Sequence number: 5 (relative sequence number)  
 [Next sequence number: 136 (relative sequence number)]  
 Acknowledgment number: 232 (relative ack number)  
 Header Length: 20 bytes

... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)

000. .... = Reserved: Not set  
 ...0 .... = Nonce: Not set  
 .... 0... = Congestion window Reduced (CWR): Not set  
 .... .0.. = ECN-Echo: Not set  
 .... ..0. = Urgent: Not set  
 .... ...1 = Acknowledgment: Set  
 .... .... 1... = Push: Set  
 .... ..0. = Reset: Not set  
 .... .... ..0. = Syn: Not set  
 .... .... ...0 = Fin: Not set



## TCP FLAGS

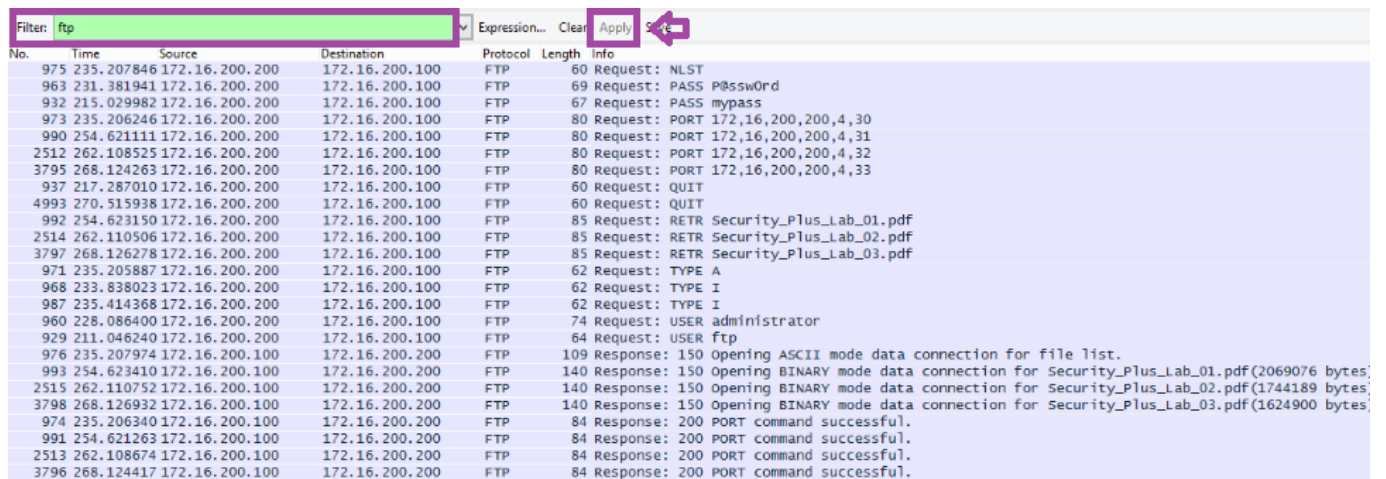
10. Type **udp** in the filter pane and then **click Apply** to view **UDP** traffic.

Filter: udp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
22114	946.427929	fe80::78d5:db3:edeff02::1:2	fe80::78d5:db3:edeff02::1:2	DHCPv6	152	Solicit XID: 0x7ffd83 CID: 00010001162e8/42000c29166864
22555	962.427996	fe80::78d5:d63:edeff02::1:2	8.8.8.8	DHCPv6	152	Solicit XID: 0x7ffd83 CID: 00010001162e8742000c29166864
22700	968.943458	172.16.200.200	8.8.8.8	DNS	76	Standard query 0x2bfc A dns.msftncsi.com
22701	968.960298	8.8.8.8	172.16.200.200	DNS	92	Standard query response 0x2bfc A 131.107.255.255
22702	968.960558	172.16.200.200	8.8.8.8	DNS	76	Standard query 0x3bc8 AAAA dns.msftncsi.com
22703	968.978583	8.8.8.8	172.16.200.200	DNS	104	Standard query response 0x3bc8 AAAA fd3e:4f5a:5b81::1
23495	994.428106	fe80::78d5:d63:edeff02::1:2	fe80::78d5:d63:edeff02::1:2	DHCPv6	152	Solicit XID: 0x7ffd83 CID: 00010001162e8742000c29166864
24424	1026.19597	172.16.200.50	8.8.8.8	DNS	87	Standard query 0x1bf5 PTR 200.200.16.172.in-addr.arpa
24427	1026.21692	8.8.8.8	172.16.200.50	DNS	87	Standard query response 0x1bf5 No such name
25038	1046.32344	172.16.200.200	8.8.8.8	DNS	76	Standard query 0x8f96 A aus3.mozilla.org
25039	1046.34162	8.8.8.8	172.16.200.200	DNS	140	Standard query response 0x8f96 CNAME aus3.external.zlb.s
25049	1046.49664	172.16.200.200	8.8.8.8	DNS	75	Standard query 0xb156 A oosp.thawte.com
25050	1046.58356	8.8.8.8	172.16.200.200	DNS	177	Standard query response 0xb156 CNAME oosp-ds.ws.symanted
25065	1046.78512	172.16.200.200	8.8.8.8	DNS	80	Standard query 0xf05b A download.mozilla.org
25066	1046.80526	8.8.8.8	172.16.200.200	DNS	145	Standard query response 0xf05b CNAME bouncer-bouncer-e1l
25093	1046.84482	172.16.200.200	8.8.8.8	DNS	84	Standard query 0xc402 A download.cdn.mozilla.net
25096	1046.88790	8.8.8.8	172.16.200.200	DNS	235	Standard query response 0xc402 CNAME 2-01-2967-001b.cdx.
27846	1132.34164	172.16.200.30	172.16.200.255	BROWSEF	286	Local Master Announcement METASPLOITABLE, Workstation, S
27847	1132.34167	172.16.200.30	172.16.200.255	BROWSEF	257	Domain/workgroup Announcement WORKGROUP, NT workstation,
27926	1132.90909	172.16.200.100	172.16.200.255	NBNS	92	Name query NB TSCLIENT<00>
27927	1132.90928	172.16.200.100	172.16.200.255	NBNS	92	Name query NB TSCLIENT<20>
27956	1133.64663	172.16.200.100	172.16.200.255	NBNS	92	Name query NB TSCLIENT<00>
27957	1133.64678	172.16.200.100	172.16.200.255	NBNS	92	Name query NB TSCLIENT<20>
28055	1134.39658	172.16.200.100	172.16.200.255	NBNS	92	Name query NB TSCLIENT<00>

## WIRESHARK FILTER

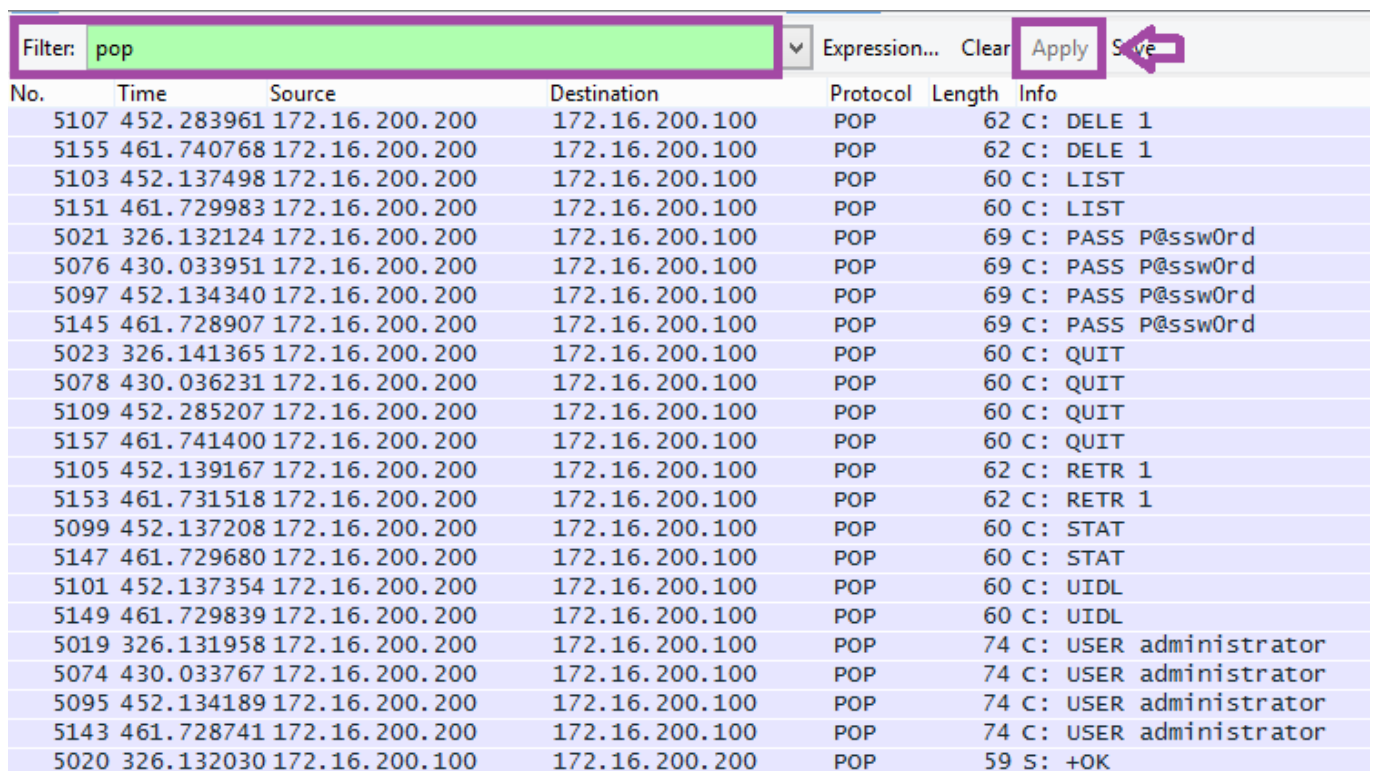
11. Type **ftp** in the filter pane and then **click Apply** to view **FTP** traffic.



No.	Time	Source	Destination	Protocol	Length	Info
975	235.207846	172.16.200.200	172.16.200.100	FTP	60	Request: NLST
963	231.381941	172.16.200.200	172.16.200.100	FTP	69	Request: PASS P@ssw0rd
932	215.029982	172.16.200.200	172.16.200.100	FTP	67	Request: PASS mypass
973	235.206246	172.16.200.200	172.16.200.100	FTP	80	Request: PORT 172,16,200,200,4,30
990	254.621111	172.16.200.200	172.16.200.100	FTP	80	Request: PORT 172,16,200,200,4,31
2512	262.108525	172.16.200.200	172.16.200.100	FTP	80	Request: PORT 172,16,200,200,4,32
3795	268.124263	172.16.200.200	172.16.200.100	FTP	80	Request: PORT 172,16,200,200,4,33
937	217.287010	172.16.200.200	172.16.200.100	FTP	60	Request: QUIT
4993	270.515938	172.16.200.200	172.16.200.100	FTP	60	Request: QUIT
992	254.623150	172.16.200.200	172.16.200.100	FTP	85	Request: RETR Security_Plus_Lab_01.pdf
2514	262.110506	172.16.200.200	172.16.200.100	FTP	85	Request: RETR Security_Plus_Lab_02.pdf
3797	268.126278	172.16.200.200	172.16.200.100	FTP	85	Request: RETR Security_Plus_Lab_03.pdf
971	235.205887	172.16.200.200	172.16.200.100	FTP	62	Request: TYPE A
968	233.838023	172.16.200.200	172.16.200.100	FTP	62	Request: TYPE I
987	235.414368	172.16.200.200	172.16.200.100	FTP	62	Request: TYPE I
960	228.086400	172.16.200.200	172.16.200.100	FTP	74	Request: USER administrator
929	211.046240	172.16.200.200	172.16.200.100	FTP	64	Request: USER ftp
976	235.207974	172.16.200.100	172.16.200.200	FTP	109	Response: 150 Opening ASCII mode data connection for file list.
993	254.623410	172.16.200.100	172.16.200.200	FTP	140	Response: 150 Opening BINARY mode data connection for Security_Plus_Lab_01.pdf(2069076 bytes;
2515	262.110752	172.16.200.100	172.16.200.200	FTP	140	Response: 150 Opening BINARY mode data connection for Security_Plus_Lab_02.pdf(1744189 bytes;
3798	268.126932	172.16.200.100	172.16.200.200	FTP	140	Response: 150 Opening BINARY mode data connection for Security_Plus_Lab_03.pdf(1624900 bytes;
974	235.206340	172.16.200.100	172.16.200.200	FTP	84	Response: 200 PORT command successful.
991	254.621263	172.16.200.100	172.16.200.200	FTP	84	Response: 200 PORT command successful.
2513	262.108674	172.16.200.100	172.16.200.200	FTP	84	Response: 200 PORT command successful.
3796	268.124417	172.16.200.100	172.16.200.200	FTP	84	Response: 200 PORT command successful.

## WIRESHARK FILTER

12. Type **pop** in the filter pane and then **click Apply** to view **POP** traffic.



No.	Time	Source	Destination	Protocol	Length	Info
5107	452.283961	172.16.200.200	172.16.200.100	POP	62	C: DELE 1
5155	461.740768	172.16.200.200	172.16.200.100	POP	62	C: DELE 1
5103	452.137498	172.16.200.200	172.16.200.100	POP	60	C: LIST
5151	461.729983	172.16.200.200	172.16.200.100	POP	60	C: LIST
5021	326.132124	172.16.200.200	172.16.200.100	POP	69	C: PASS P@ssw0rd
5076	430.033951	172.16.200.200	172.16.200.100	POP	69	C: PASS P@ssw0rd
5097	452.134340	172.16.200.200	172.16.200.100	POP	69	C: PASS P@ssw0rd
5145	461.728907	172.16.200.200	172.16.200.100	POP	69	C: PASS P@ssw0rd
5023	326.141365	172.16.200.200	172.16.200.100	POP	60	C: QUIT
5078	430.036231	172.16.200.200	172.16.200.100	POP	60	C: QUIT
5109	452.285207	172.16.200.200	172.16.200.100	POP	60	C: QUIT
5157	461.741400	172.16.200.200	172.16.200.100	POP	60	C: QUIT
5105	452.139167	172.16.200.200	172.16.200.100	POP	62	C: RETR 1
5153	461.731518	172.16.200.200	172.16.200.100	POP	62	C: RETR 1
5099	452.137208	172.16.200.200	172.16.200.100	POP	60	C: STAT
5147	461.729680	172.16.200.200	172.16.200.100	POP	60	C: STAT
5101	452.137354	172.16.200.200	172.16.200.100	POP	60	C: UIDL
5149	461.729839	172.16.200.200	172.16.200.100	POP	60	C: UIDL
5019	326.131958	172.16.200.200	172.16.200.100	POP	74	C: USER administrator
5074	430.033767	172.16.200.200	172.16.200.100	POP	74	C: USER administrator
5095	452.134189	172.16.200.200	172.16.200.100	POP	74	C: USER administrator
5143	461.728741	172.16.200.200	172.16.200.100	POP	74	C: USER administrator
5020	326.132030	172.16.200.100	172.16.200.200	POP	59	S: +OK

## WIRESHARK FILTER

13. Type **smtp** in the filter pane and then **click Apply** to view **SMTP** traffic.



No.	Time	Source	Destination	Protocol	Length	Info
5058	429.802368	172.16.200.200	172.16.200.100	SMTP	60	C: DATA
5125	457.657742	172.16.200.200	172.16.200.100	SMTP	60	C: DATA
5173	470.686202	172.16.200.200	172.16.200.100	SMTP	60	C: DATA
5175	470.687924	172.16.200.200	172.16.200.100	SMTP	1199	C: DATA fragment, 1145 bytes
5060	429.803191	172.16.200.200	172.16.200.100	SMTP	447	C: DATA fragment, 393 bytes
5127	457.660210	172.16.200.200	172.16.200.100	SMTP	944	C: DATA fragment, 890 bytes
5119	457.651467	172.16.200.200	172.16.200.100	SMTP	70	C: EHLO studentPC
5167	470.683761	172.16.200.200	172.16.200.100	SMTP	70	C: EHLO studentPC
5003	326.101977	172.16.200.200	172.16.200.100	SMTP	70	C: HELO studentPC
5033	326.142700	172.16.200.200	172.16.200.100	SMTP	70	C: HELO studentPC
5052	429.801480	172.16.200.200	172.16.200.100	SMTP	70	C: HELO studentPC
5054	429.801901	172.16.200.200	172.16.200.100	SMTP	97	C: MAIL FROM: <administrator@XYZcompany.com>
5121	457.657271	172.16.200.200	172.16.200.100	SMTP	97	C: MAIL FROM: <administrator@XYZcompany.com>
5169	470.684752	172.16.200.200	172.16.200.100	SMTP	97	C: MAIL FROM: <administrator@XYZcompany.com>
5005	326.105451	172.16.200.200	172.16.200.100	SMTP	97	C: MAIL FROM: <administrator@university.edu>
5035	326.143139	172.16.200.200	172.16.200.100	SMTP	97	C: MAIL FROM: <administrator@university.edu>
5009	326.129395	172.16.200.200	172.16.200.100	SMTP	60	C: QUIT
5039	326.144856	172.16.200.200	172.16.200.100	SMTP	60	C: QUIT
5064	430.031416	172.16.200.200	172.16.200.100	SMTP	60	C: QUIT
5132	460.302696	172.16.200.200	172.16.200.100	SMTP	60	C: QUIT
5180	473.318764	172.16.200.200	172.16.200.100	SMTP	60	C: QUIT
5056	429.802130	172.16.200.200	172.16.200.100	SMTP	95	C: RCPT TO: <administrator@XYZcompany.com>
5123	457.657525	172.16.200.200	172.16.200.100	SMTP	95	C: RCPT TO: <administrator@XYZcompany.com>
5171	470.685744	172.16.200.200	172.16.200.100	SMTP	95	C: RCPT TO: <administrator@XYZcompany.com>
5007	326.128880	172.16.200.200	172.16.200.100	SMTP	95	C: RCPT TO: <administrator@university.edu>
5037	326.143406	172.16.200.200	172.16.200.100	SMTP	95	C: RCPT TO: <administrator@university.edu>

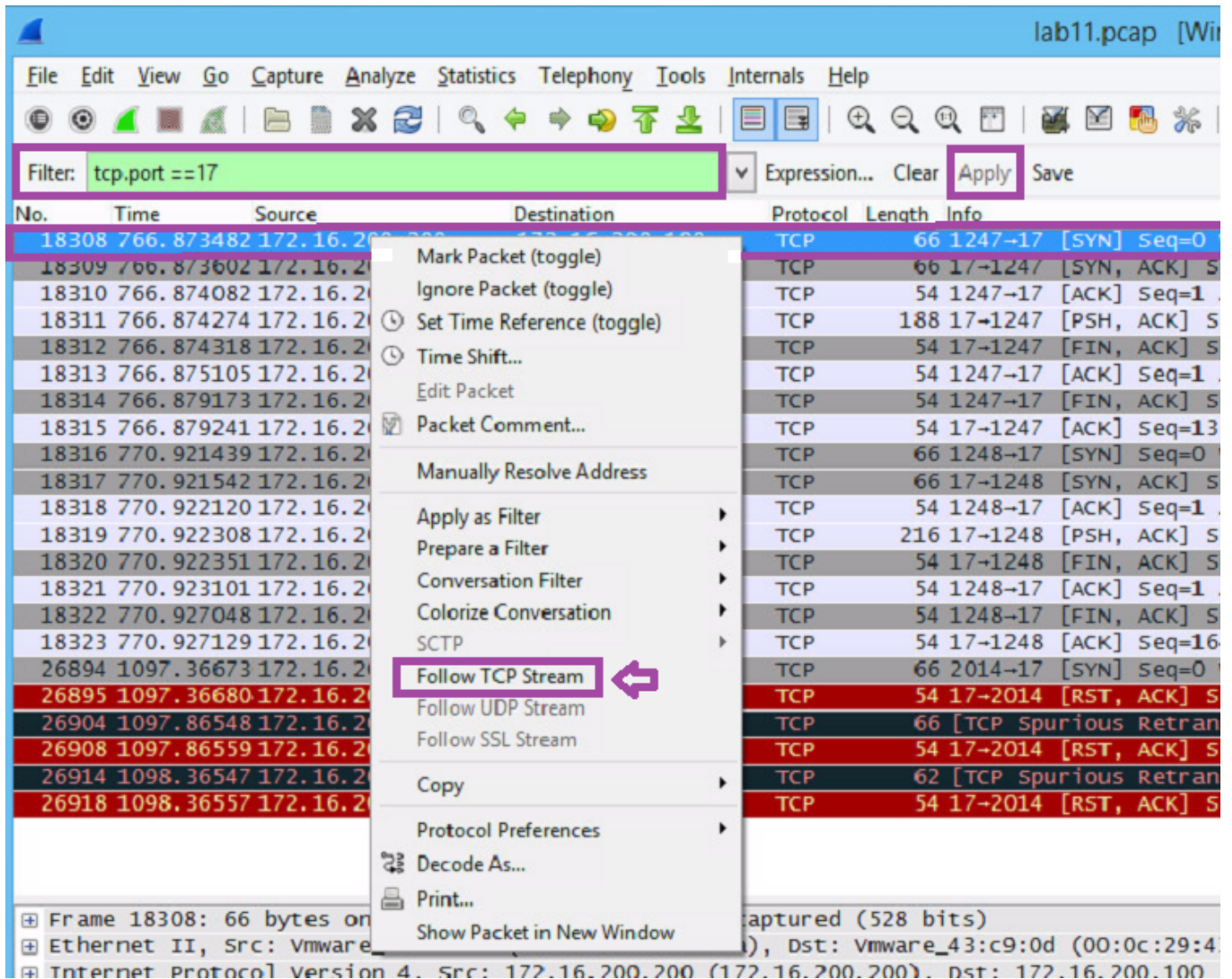
## WIRESHARK FILTER

14. Type **dns** in the filter pane and then **click Apply** to view **DNS** traffic.

No.	Time	Source	Destination	Protocol	Length	Info
18045	692.988897	172.16.200.200	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
18047	693.011736	172.16.200.200	8.8.8.8	DNS	72	Standard query 0x0002 A www.espn.com
18049	693.032206	172.16.200.200	8.8.8.8	DNS	72	Standard query 0x0003 AAAA www.espn.com
10438	594.513171	172.16.200.200	8.8.8.8	DNS	75	Standard query 0x0085 A ssl.gstatic.com
19686	868.005717	172.16.200.200	8.8.8.8	DNS	89	Standard query 0x0110 A safebrowsing-cache.google.com
12265	631.593297	172.16.200.200	8.8.8.8	DNS	72	Standard query 0x0185 A www.sway.com
5313	571.526837	172.16.200.200	8.8.8.8	DNS	79	Standard query 0x02af A fxfeeds.mozilla.com
531	2.053271	172.16.200.50	8.8.8.8	DNS	86	Standard query 0x03ef PTR 50.200.16.172.in-addr.arpa
14057	637.175999	172.16.200.200	8.8.8.8	DNS	87	Standard query 0x0470 A www.thefemalecelebrity.info
5382	572.746128	172.16.200.200	8.8.8.8	DNS	73	Standard query 0x04b1 A a.espn.com
5685	573.740244	172.16.200.200	8.8.8.8	DNS	73	Standard query 0x04b1 A a.espn.com
19620	843.388449	fe80::78d5:d63:3ede:ff02::1:3	224.0.0.252	LLMNR	84	Standard query 0x04c6 A wpad
19621	843.388569	172.16.200.200	224.0.0.252	LLMNR	64	Standard query 0x04c6 A wpad
19622	843.490539	fe80::78d5:d63:3ede:ff02::1:3	224.0.0.252	LLMNR	84	Standard query 0x04c6 A wpad
19623	843.490602	172.16.200.200	224.0.0.252	LLMNR	64	Standard query 0x04c6 A wpad
9421	576.375279	172.16.200.200	8.8.8.8	DNS	73	Standard query 0x04f2 A s.adzmath.com
5272	568.481043	172.16.200.200	8.8.8.8	DNS	77	Standard query 0x08f8 A sb-ssl.google.com
19590	836.756108	fe80::78d5:d63:3ede:ff02::1:3	224.0.0.252	LLMNR	86	Standard query 0x0a4f A server
19591	836.756206	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x0a4f A server
19592	836.865484	fe80::78d5:d63:3ede:ff02::1:3	224.0.0.252	LLMNR	86	Standard query 0x0a4f A server
19593	836.865581	172.16.200.200	224.0.0.252	LLMNR	66	Standard query 0x0a4f A server
14123	637.612323	172.16.200.200	8.8.8.8	DNS	77	Standard query 0x0cc0 A www.ecenglish.com
14105	637.417673	172.16.200.200	8.8.8.8	DNS	76	Standard query 0x0cd2 A www.popsugar.com
9379	576.281849	172.16.200.200	8.8.8.8	DNS	70	Standard query 0x0d39 A log.go.com
12173	631.422907	172.16.200.200	8.8.8.8	DNS	72	Standard query 0x107d A www.bing.com
5195	566.587097	172.16.200.200	8.8.8.8	DNS	80	Standard query 0x12d6 A snippets.mozilla.com

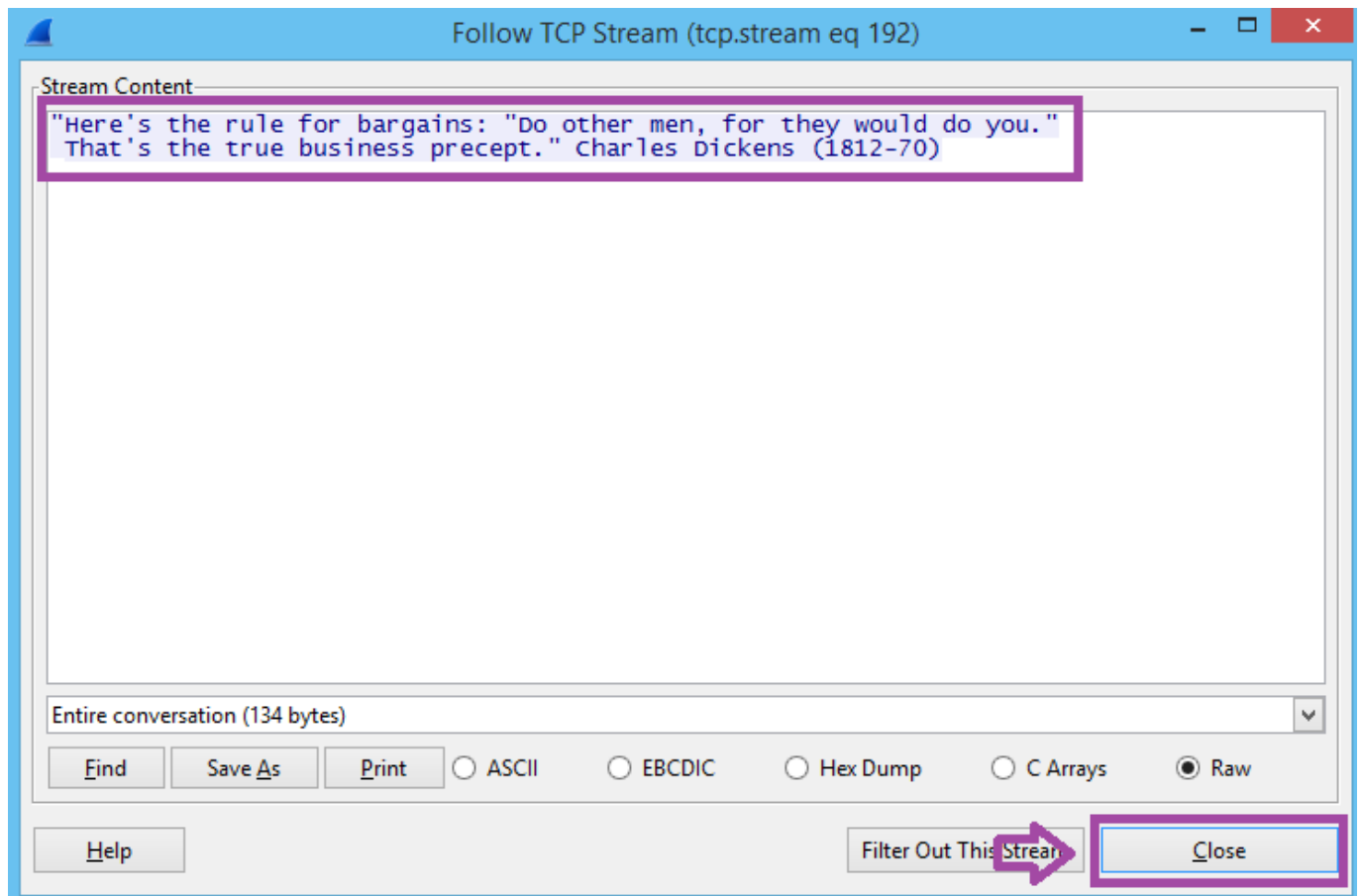
## WIRESHARK FILTER

15. Type **tcp.port == 17** in the Wireshark filter pane and then **click Apply** to view **QOTD** traffic. **Right-click** the first frame and then **select Follow TCP Stream**.



## WIRESHARK FILTER

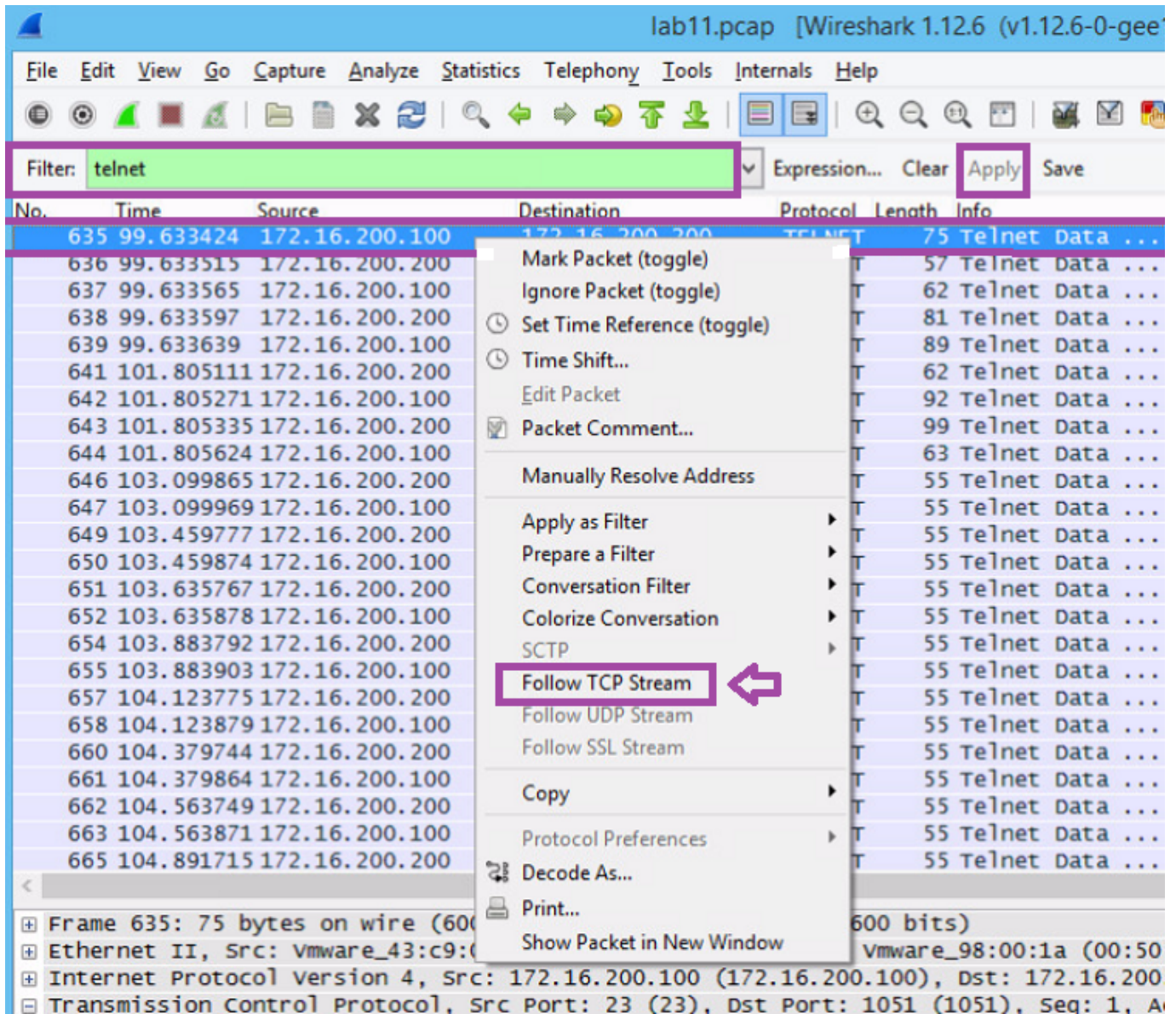
16. **Read** the Quote of the Day. **Click** the Close button to close the TCP Stream.



## TCP STREAM CONTENT

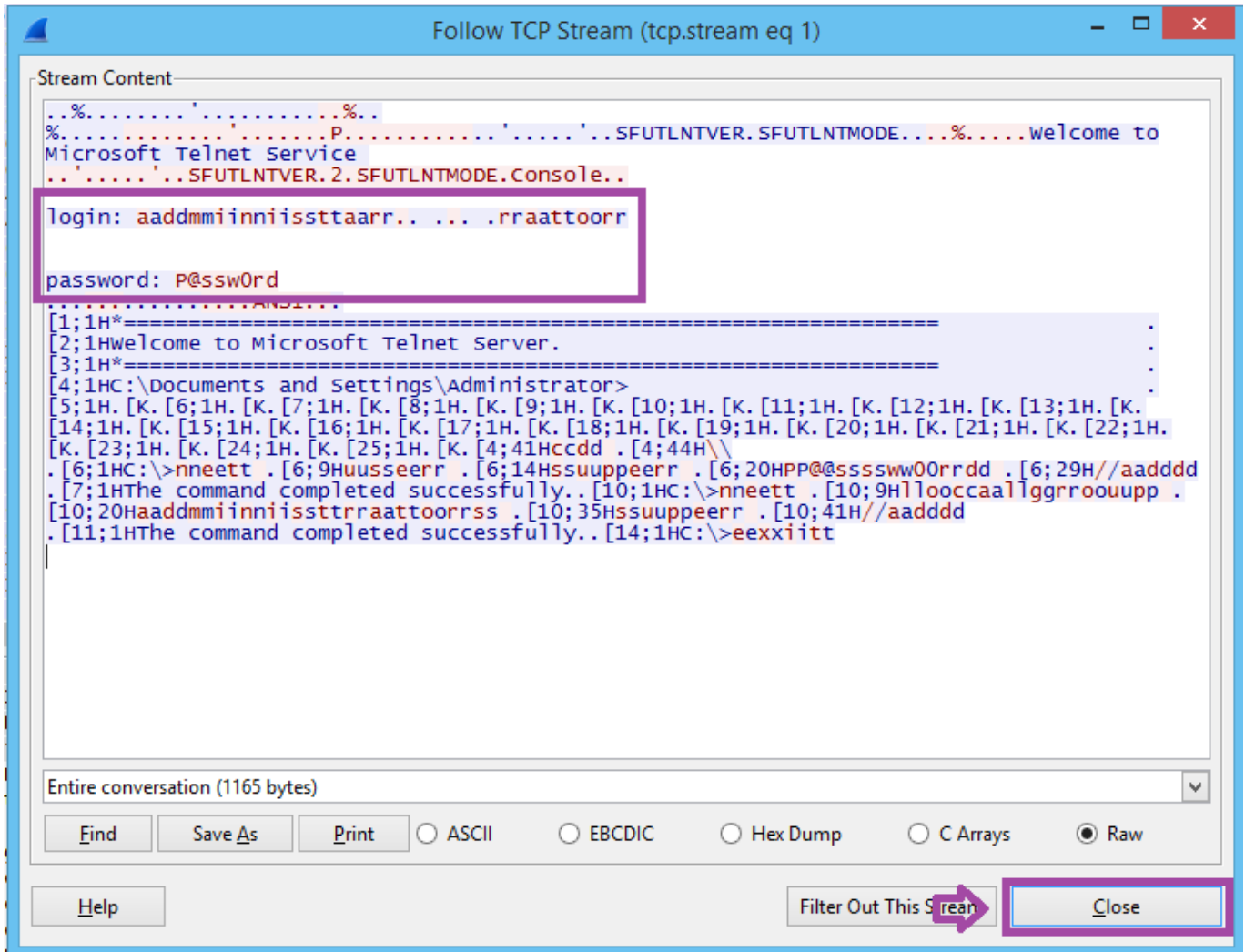
17. **Type telnet** in the Wireshark filter pane and then **click Apply** to view **TELNET** traffic. **Right-click** on the **first frame** and **select Follow TCP Stream**.





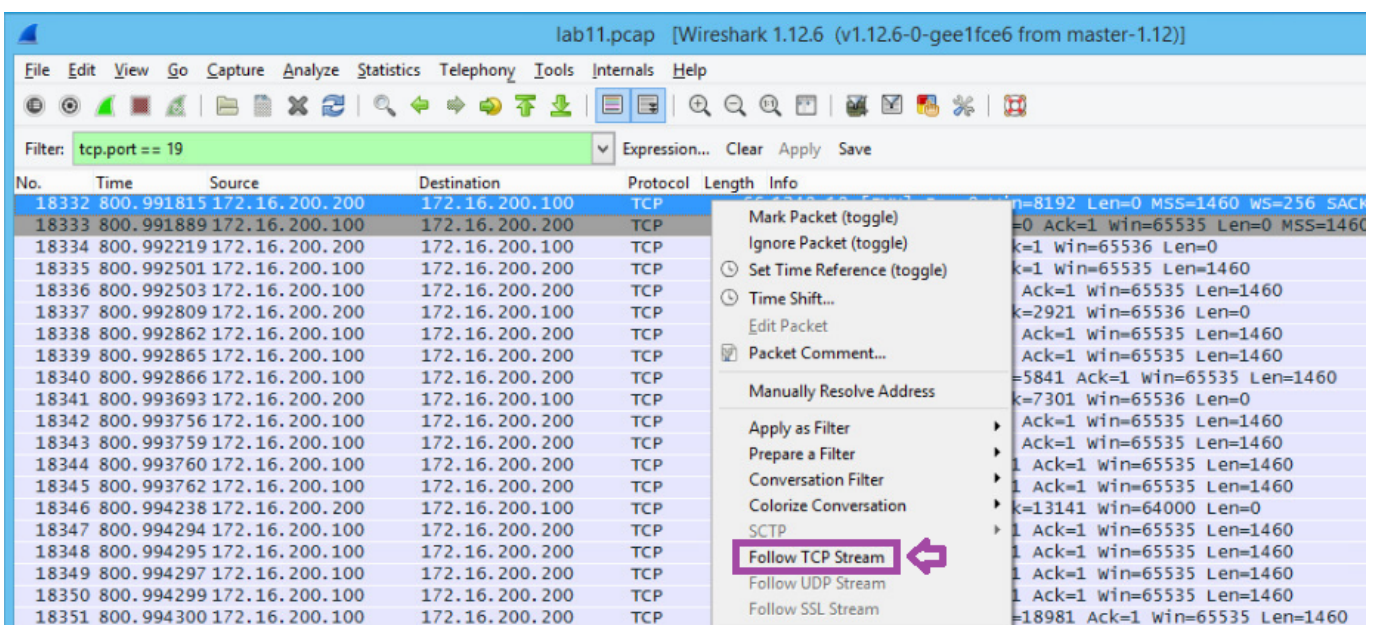
## WIRESHARK FILTER

18. **Read** the plain text credentials. **Click** the **Close** button to close the **TCP Stream**.



## WIRESHARK FILTER

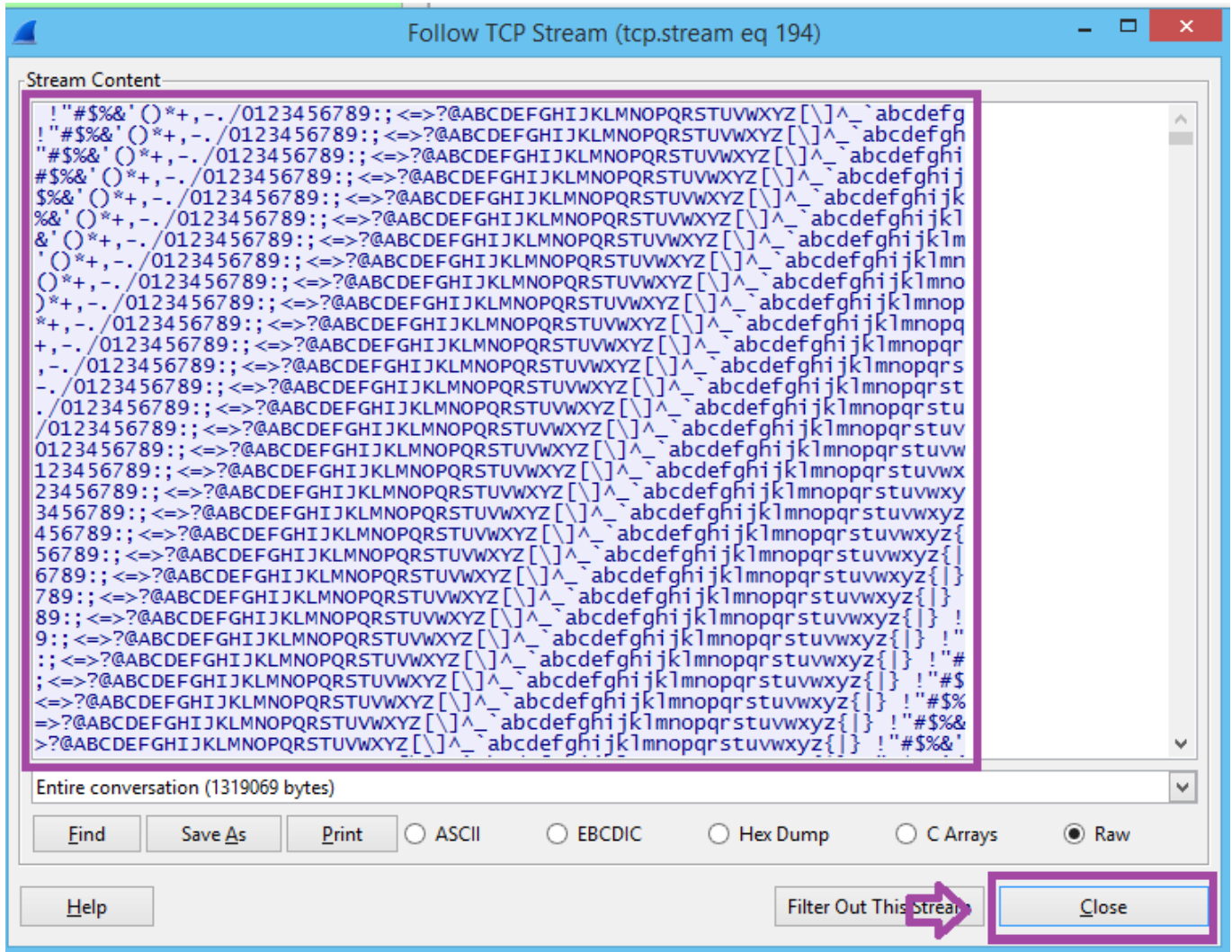
19. Type `tcp.port == 19` in the Wireshark filter pane and then click **Apply** to view **CHARGEN** traffic. **Right-click** on the first frame and **select Follow TCP Stream**.



## WIRESHARK FILTER

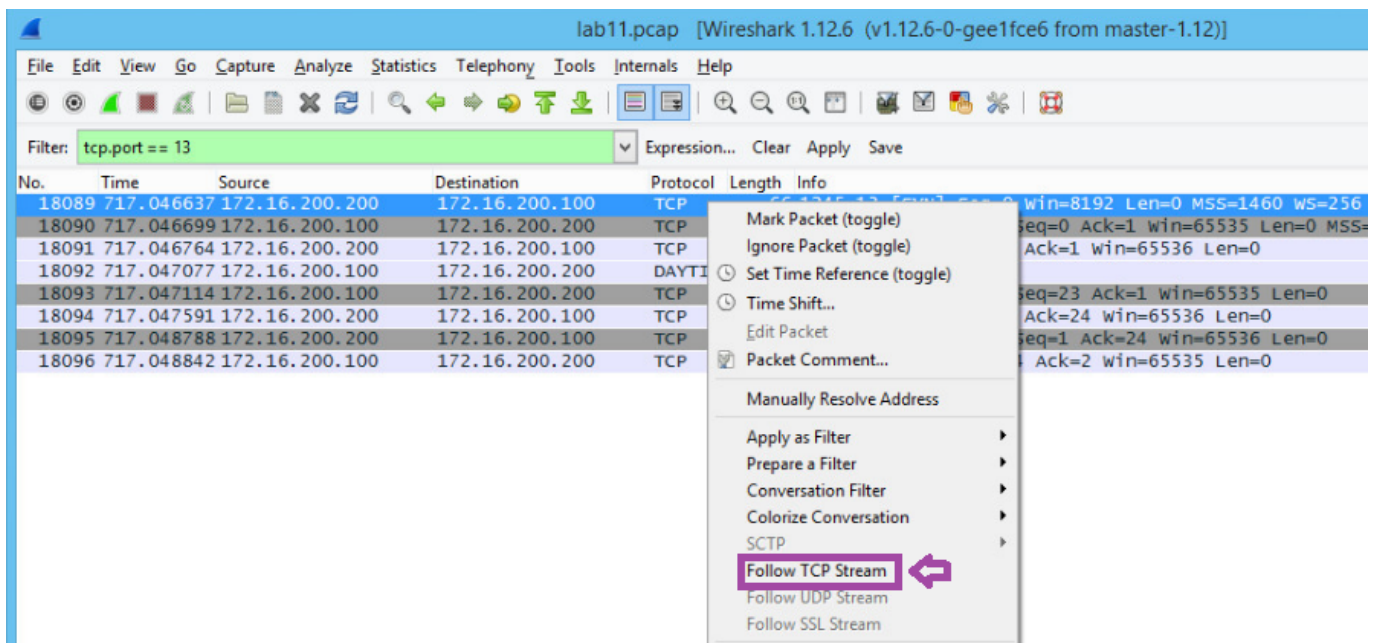


20. **Read** the generated characters. **Click** the **Close** button to close the **TCP Stream**.



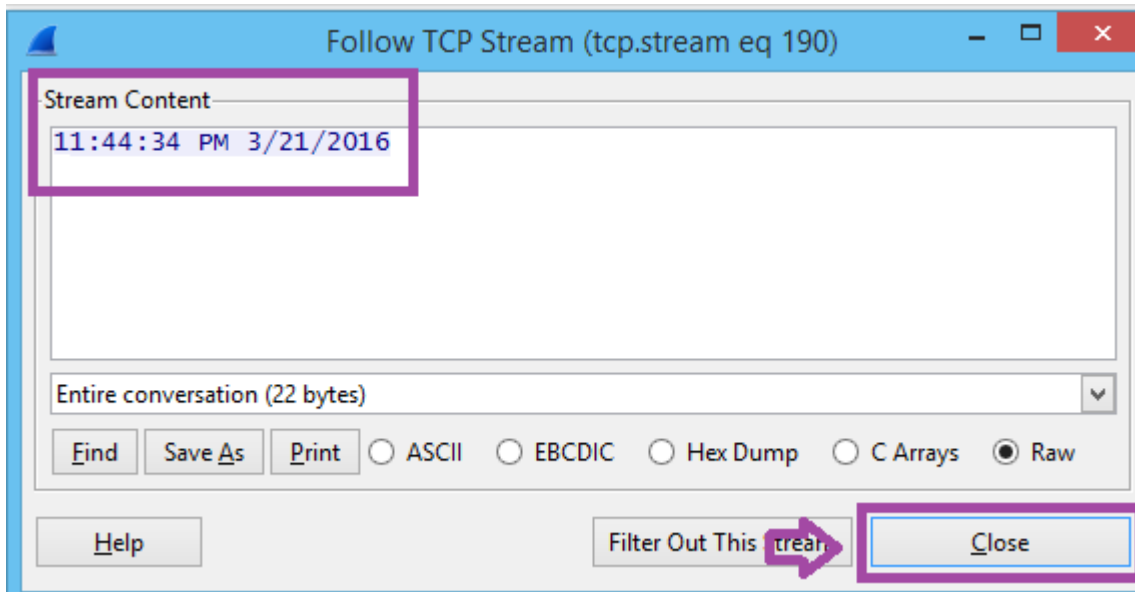
## TCP STREAM CONTENT

21. **Type** `tcp.port == 13` in the Wireshark filter pane and then **click** **Apply** to view **DAYTIME** traffic. **Right-click** on the first frame and **select** **Follow TCP Stream**.



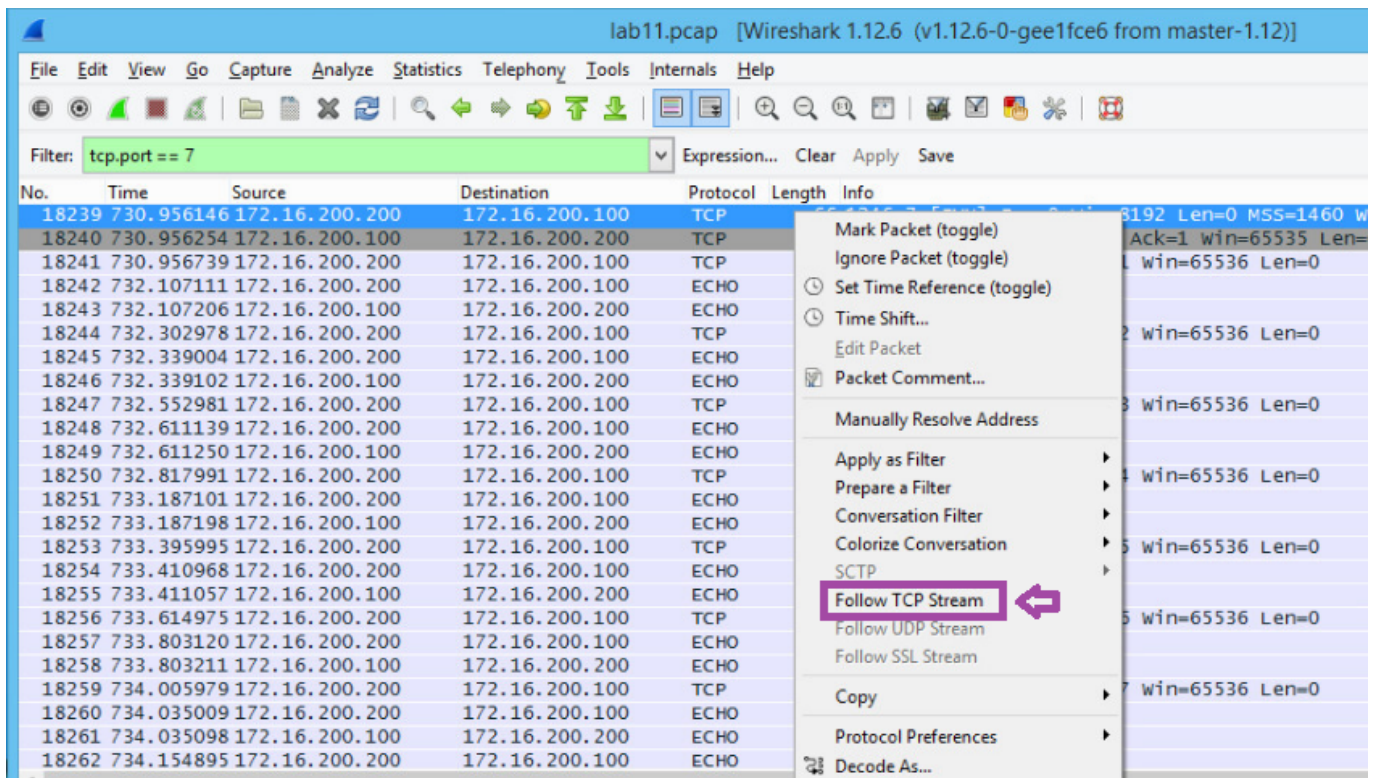
## WIRESHARK FILTER

22. **Read** the date and time. **Click** the **Close** button to close the **TCP Stream**.



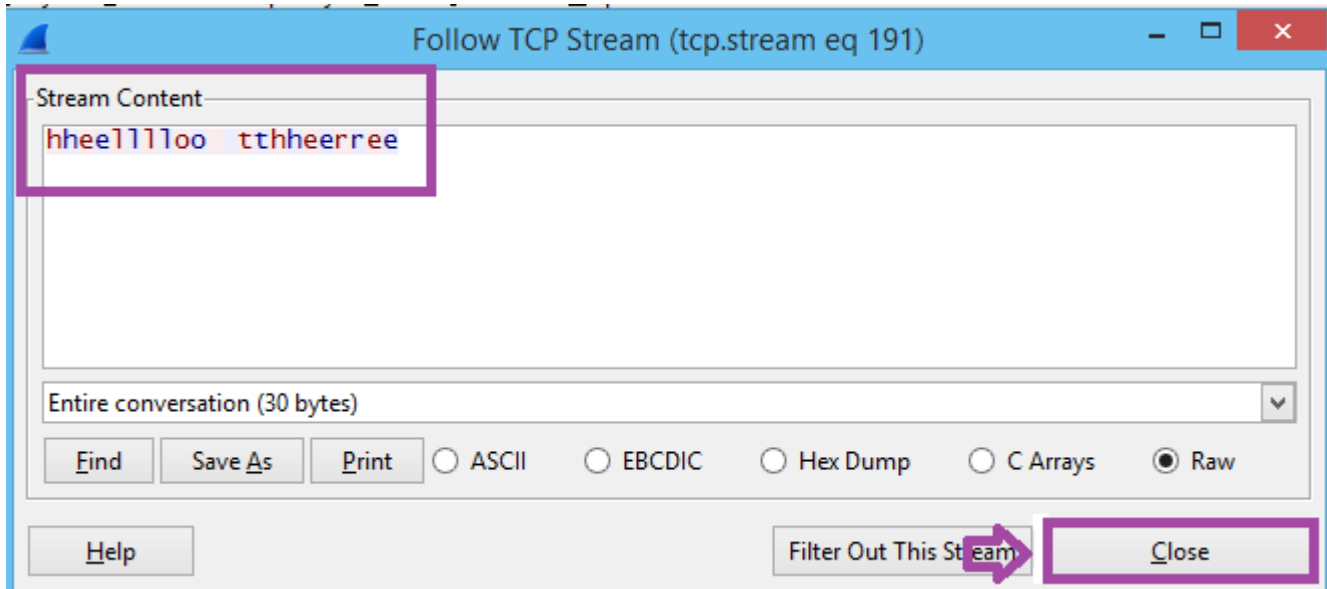
## WIRESHARK FILTER

23. Type `tcp.port == 7` in the Wireshark filter pane and then **click** **Apply** to view **ECHO** traffic. **Right-click** on the first frame and **select** **Follow TCP Stream**.



## FOLLOW TCP STREAM

24. **Read** the doubled characters. **Click** the **Close** button to close the **TCP Stream**.



### TCP STREAM CONTENT

25. Type **ssh** in the Wireshark filter pane and then **click Apply** to view **secure shell traffic**.

No.	Time	Source	Destination	Protocol	Length	Info
24360	1022.66931	172.16.200.200	172.16.200.50	SSHv2	70	Client: Diffie-Hellman Group Exchange Init
24357	1022.54568	172.16.200.200	172.16.200.50	SSHv2	70	Client: Diffie-Hellman Group Exchange Request (old)
24472	1028.11568	172.16.200.200	172.16.200.50	SSHv2	350	Client: Encrypted packet (len=296)
24628	1033.06711	172.16.200.200	172.16.200.50	SSHv2	350	Client: Encrypted packet (len=296)
24742	1036.70699	172.16.200.200	172.16.200.50	SSHv2	350	Client: Encrypted packet (len=296)
24395	1024.23097	172.16.200.200	172.16.200.50	SSHv2	106	Client: Encrypted packet (len=52)
24423	1026.19543	172.16.200.200	172.16.200.50	SSHv2	122	Client: Encrypted packet (len=68)
24353	1022.54532	172.16.200.200	172.16.200.50	SSHv2	182	Client: Key Exchange Init
24394	1024.23076	172.16.200.200	172.16.200.50	SSHv2	70	Client: New Keys
24350	1022.54499	172.16.200.200	172.16.200.50	SSHv2	82	Client: Protocol (SSH-2.0-PuTTY_release_0.61)
24358	1022.55972	172.16.200.50	172.16.200.200	SSHv2	590	Server: Diffie-Hellman Group Exchange Group
24362	1022.67417	172.16.200.50	172.16.200.200	SSHv2	1158	Server: Diffie-Hellman Group Exchange Reply, New Keys
24397	1024.23112	172.16.200.50	172.16.200.200	SSHv2	106	Server: Encrypted packet (len=52)
24428	1026.21728	172.16.200.50	172.16.200.200	SSHv2	122	Server: Encrypted packet (len=68)
24522	1029.78137	172.16.200.50	172.16.200.200	SSHv2	122	Server: Encrypted packet (len=68)
24660	1034.41631	172.16.200.50	172.16.200.200	SSHv2	122	Server: Encrypted packet (len=68)
24814	1039.27245	172.16.200.50	172.16.200.200	SSHv2	122	Server: Encrypted packet (len=68)
24356	1022.54556	172.16.200.50	172.16.200.200	SSHv2	1006	Server: Key Exchange Init
24349	1022.54394	172.16.200.50	172.16.200.200	SSHv2	86	Server: Protocol (SSH-2.0-OpenSSH_6.7p1 Debian-5)

### WIRESHARK FILTER

26. Type **rdp** in the Wireshark filter pane and then **click Apply** to view **Remote Desktop Protocol traffic**.

No.	Time	Source	Destination	Protocol	Length	Info
27866	1132.73574	172.16.200.50	172.16.200.100	RDP	512	ClientData
27867	1132.73599	172.16.200.100	172.16.200.50	RDP	399	ServerData Encryption: 128-bit RC4 (Client Compatible)

### WIRESHARK FILTER

27. Type **smb** in the Wireshark filter pane and then **click Apply** to view **Server Message Block traffic**.



No.	Time	Source	Destination	Protocol	Length	Info
533	18.115120	172.16.200.100	172.16.200.255	BROWSEF	249	Domain/workgroup Announcement XYZCOMPANY, NT
586	50.606290	172.16.200.200	172.16.200.255	BROWSEF	216	Get Backup List Request
590	50.608170	172.16.200.30	172.16.200.200	BROWSEF	231	Get Backup List Response
604	53.169045	172.16.200.200	172.16.200.30	SMB	213	Negotiate Protocol Request
605	53.169954	172.16.200.30	172.16.200.200	SMB	185	Negotiate Protocol Response
606	53.170481	172.16.200.200	172.16.200.30	SMB	196	Session Setup AndX Request, NTLMSSP_NEGOTIATI
607	53.171335	172.16.200.30	172.16.200.200	SMB	354	Session Setup AndX Response, NTLMSSP_CHALLENGE
608	53.172052	172.16.200.200	172.16.200.30	SMB	256	Session Setup AndX Request, NTLMSSP_AUTH, USI
609	53.172615	172.16.200.30	172.16.200.200	SMB	180	Session Setup AndX Response
610	53.172793	172.16.200.200	172.16.200.30	SMB	152	Tree Connect AndX Request, Path: \\METASPLOIT
611	53.173783	172.16.200.30	172.16.200.200	SMB	106	Tree Connect AndX Response
612	53.173940	172.16.200.200	172.16.200.30	LANMAN	176	NetServerEnum2 Request, workstation, Server,
613	53.174218	172.16.200.30	172.16.200.200	LANMAN	219	NetServerEnum2 Response
615	65.678391	172.16.200.200	172.16.200.30	SMB	93	Tree Disconnect Request
616	65.678558	172.16.200.30	172.16.200.200	SMB	93	Tree Disconnect Response
617	65.678655	172.16.200.200	172.16.200.30	SMB	97	Logoff AndX Request
618	65.678720	172.16.200.30	172.16.200.200	SMB	97	Logoff AndX Response
623	78.115368	172.16.200.100	172.16.200.255	BROWSEF	249	Domain/workgroup Announcement XYZCOMPANY, NT
943	218.537170	172.16.200.100	172.16.200.255	BROWSEF	225	Browser Election Request
945	218.537285	172.16.200.30	172.16.200.255	BROWSEF	286	Local Master Announcement METASPLOITABLE, WOR
946	218.537317	172.16.200.30	172.16.200.255	BROWSEF	257	Domain/workgroup Announcement WORKGROUP, NT
947	218.646824	172.16.200.100	172.16.200.255	BROWSEF	231	Browser Election Request
949	219.646831	172.16.200.100	172.16.200.255	BROWSEF	231	Browser Election Request
951	220.646845	172.16.200.100	172.16.200.255	BROWSEF	231	Browser Election Request

## WIRESHARK FILTER

28. Type **nbns** in the Wireshark filter pane and then **click Apply** to view **NetBIOS Name Service** traffic.

No.	Time	Source	Destination	Protocol	Length	Info
587	50.606393	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WORKGROUP<1b>
591	51.350114	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WORKGROUP<1b>
592	52.100090	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WORKGROUP<1b>
597	53.162375	172.16.200.200	172.16.200.255	NBNS	92	Name query NB METASPLOITABLE<20>
598	53.162505	172.16.200.30	172.16.200.200	NBNS	104	Name query response NB 172.16.200.30
633	99.632672	172.16.200.100	172.16.200.200	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><
634	99.632785	172.16.200.200	172.16.200.100	NBNS	217	Name query response NBSTAT
944	218.537277	172.16.200.100	172.16.200.255	NBNS	110	Registration NB XYZCOMPANY<1b>
948	219.286788	172.16.200.100	172.16.200.255	NBNS	110	Registration NB XYZCOMPANY<1b>
950	220.036755	172.16.200.100	172.16.200.255	NBNS	110	Registration NB XYZCOMPANY<1b>
952	220.786783	172.16.200.100	172.16.200.255	NBNS	110	Registration NB XYZCOMPANY<1b>
5088	434.083953	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
5089	434.833580	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
5090	435.583589	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
14276	642.332539	172.16.200.200	172.16.200.255	NBNS	92	Name query NB FILMVZ.COM<00>
14847	643.068663	172.16.200.200	172.16.200.255	NBNS	92	Name query NB FILMVZ.COM<00>
15273	643.818629	172.16.200.200	172.16.200.255	NBNS	92	Name query NB FILMVZ.COM<00>
19554	826.177639	172.16.200.200	172.16.200.255	NBNS	92	Name query NB SERVER<20>
19555	826.177711	172.16.200.100	172.16.200.200	NBNS	104	Name query response NB 172.16.200.100
19581	834.193661	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19582	834.943443	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19583	835.693537	172.16.200.200	172.16.200.255	NBNS	92	Name query NB WPAD<00>
19588	836.755678	172.16.200.200	172.16.200.255	NBNS	92	Name query NB SERVER<00>
19589	836.755753	172.16.200.100	172.16.200.200	NBNS	104	Name query response NB 172.16.200.100

## WIRESHARK FILTER

29. Type **http** in the Wireshark filter pane and then **click Apply** to view **Hypertext Transfer Protocol** traffic.

No.	Time	Source	Destination	Protocol	Length	Info
5213	566.817780	172.16.200.200	72.21.91.29	OCSP	565	Request
5215	566.829483	72.21.91.29	172.16.200.200	OCSP	842	Response
5216	566.831921	172.16.200.200	72.21.91.29	OCSP	565	Request
5218	566.844050	72.21.91.29	172.16.200.200	OCSP	842	Response
5222	566.943575	72.21.91.29	172.16.200.200	OCSP	842	[TCP Retransmission] Response
5238	567.094739	172.16.200.200	72.21.91.29	OCSP	565	Request
5240	567.104980	72.21.91.29	172.16.200.200	OCSP	842	Response
5267	567.204586	72.21.91.29	172.16.200.200	OCSP	842	[TCP Retransmission] Response
5288	568.579495	172.16.200.200	216.58.217.142	OCSP	563	Request
5290	568.606724	216.58.217.142	172.16.200.200	OCSP	800	Response
5292	568.707253	216.58.217.142	172.16.200.200	OCSP	800	[TCP Retransmission] Response
5298	568.727748	172.16.200.200	23.13.171.27	OCSP	546	Request
5301	568.739610	23.13.171.27	172.16.200.200	OCSP	311	Response
5318	571.628711	172.16.200.200	63.245.213.56	HTTP	439	GET /en-us/firefox/headlines.xml HTTP/1.1
5320	571.708469	63.245.213.56	172.16.200.200	HTTP	665	HTTP/1.1 302 Found (text/html)
5321	571.709352	172.16.200.200	63.245.213.56	HTTP	411	GET /firefox/headlines.xml HTTP/1.1
5326	571.786590	63.245.213.56	172.16.200.200	HTTP	735	HTTP/1.1 302 Found (text/html)
5332	571.829505	172.16.200.200	184.51.126.99	HTTP	435	GET /rss/newsonline_world_edition/front_page/rss.xml
5334	571.841919	184.51.126.99	172.16.200.200	HTTP	620	HTTP/1.1 301 Moved Permanently (text/html)
5336	571.886449	63.245.213.56	172.16.200.200	HTTP	735	[TCP Retransmission] HTTP/1.1 302 Found (text/html)
5338	571.941444	184.51.126.99	172.16.200.200	HTTP	620	[TCP Retransmission] HTTP/1.1 301 Moved Permanently
5344	571.960694	172.16.200.200	23.202.207.209	HTTP	411	GET /news/rss.xml?edition=int HTTP/1.1
5353	571.977021	23.202.207.209	172.16.200.200	HTTP/xv	1223	HTTP/1.1 200 OK
5366	572.476830	172.16.200.200	68.71.212.159	HTTP	383	GET / HTTP/1.1

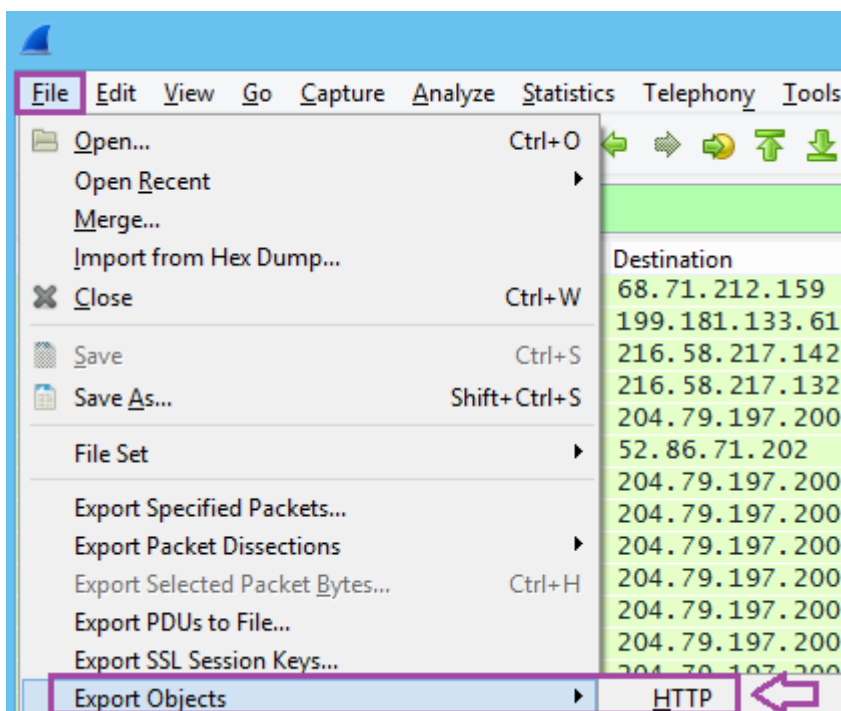
## WIRESHARK FILTER

## DISCUSSION QUESTIONS:

1. What is ICMP?
2. What is ARP?
3. What is FTP?
4. What is SMTP?

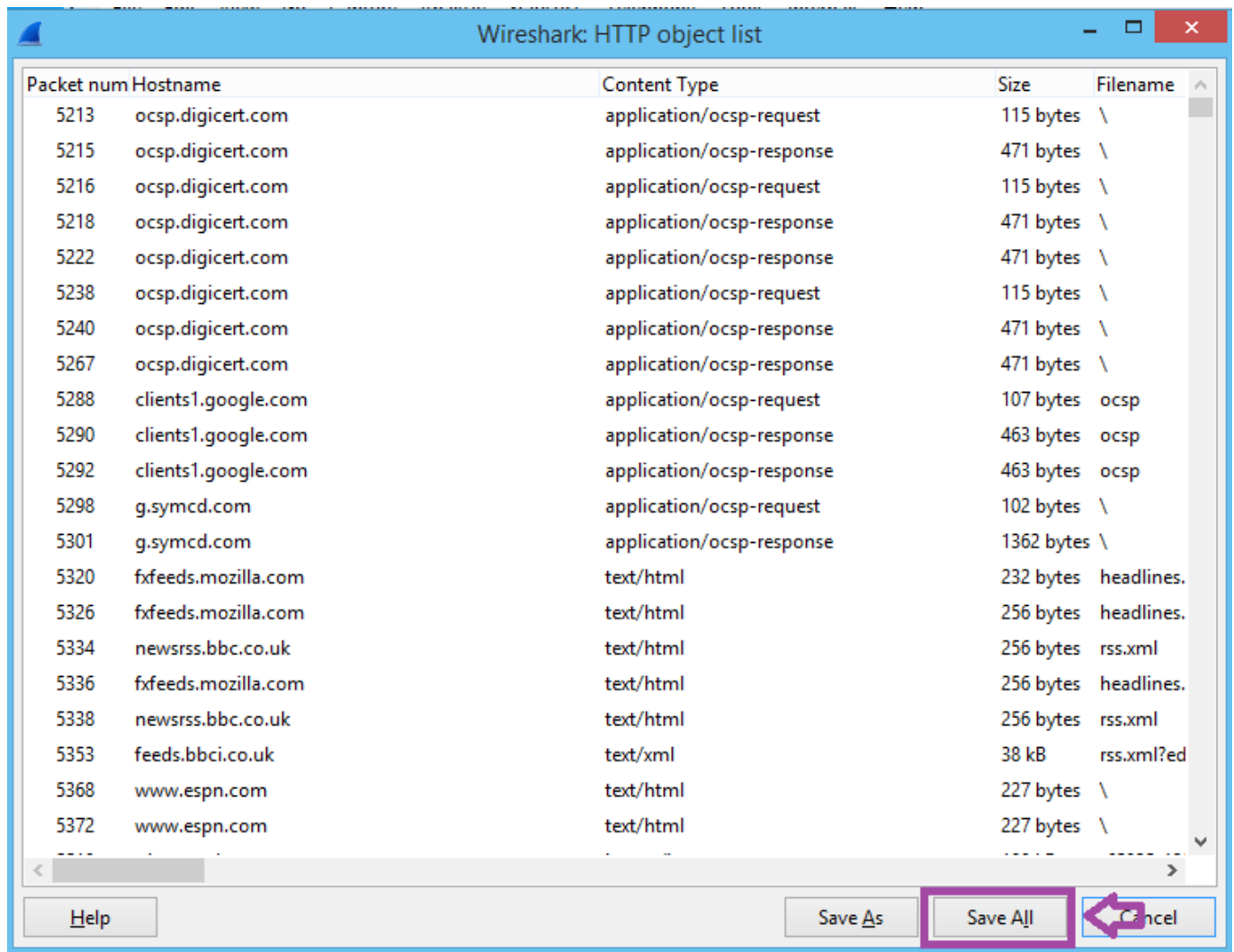
## Parsing Objects With Wireshark

1. **Right-click** File, then **select** Export Objects, then **click** HTTP.



## HTTP OBJECTS

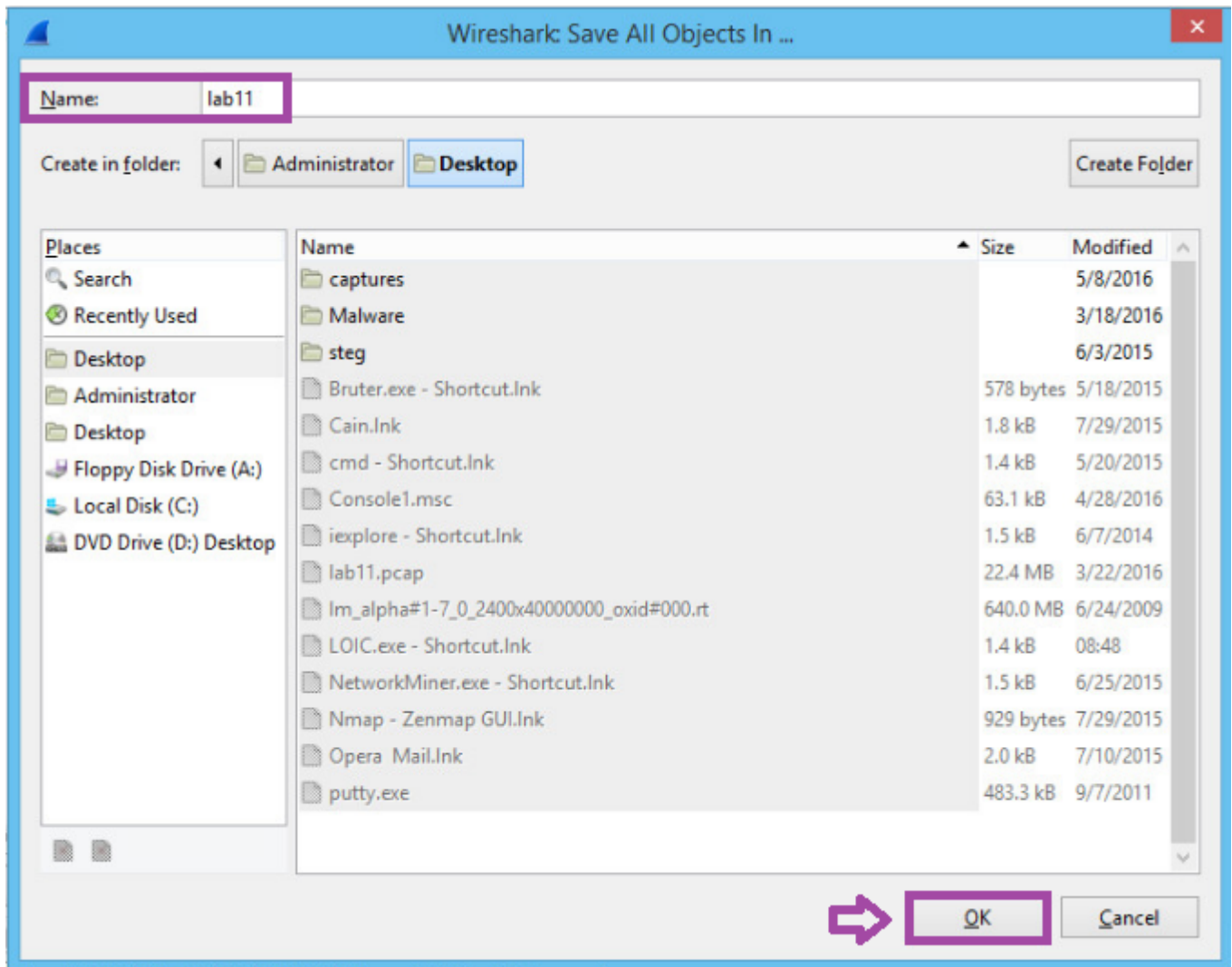
2. Click **Save All**.



## SAVE ALL

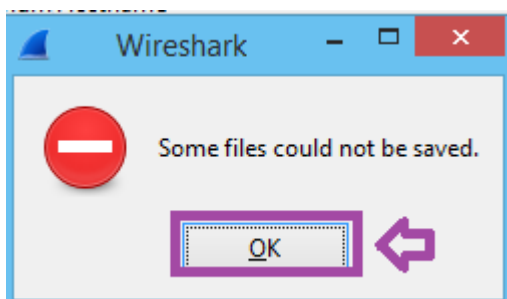
3. For the folder name, **type lab11**. Click **OK**.





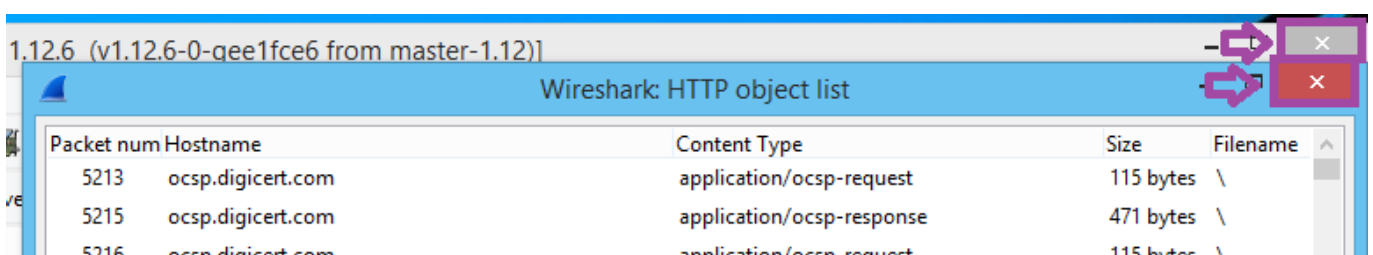
## WIRESHARK

4. Click **OK** to the message that some files cannot be saved.



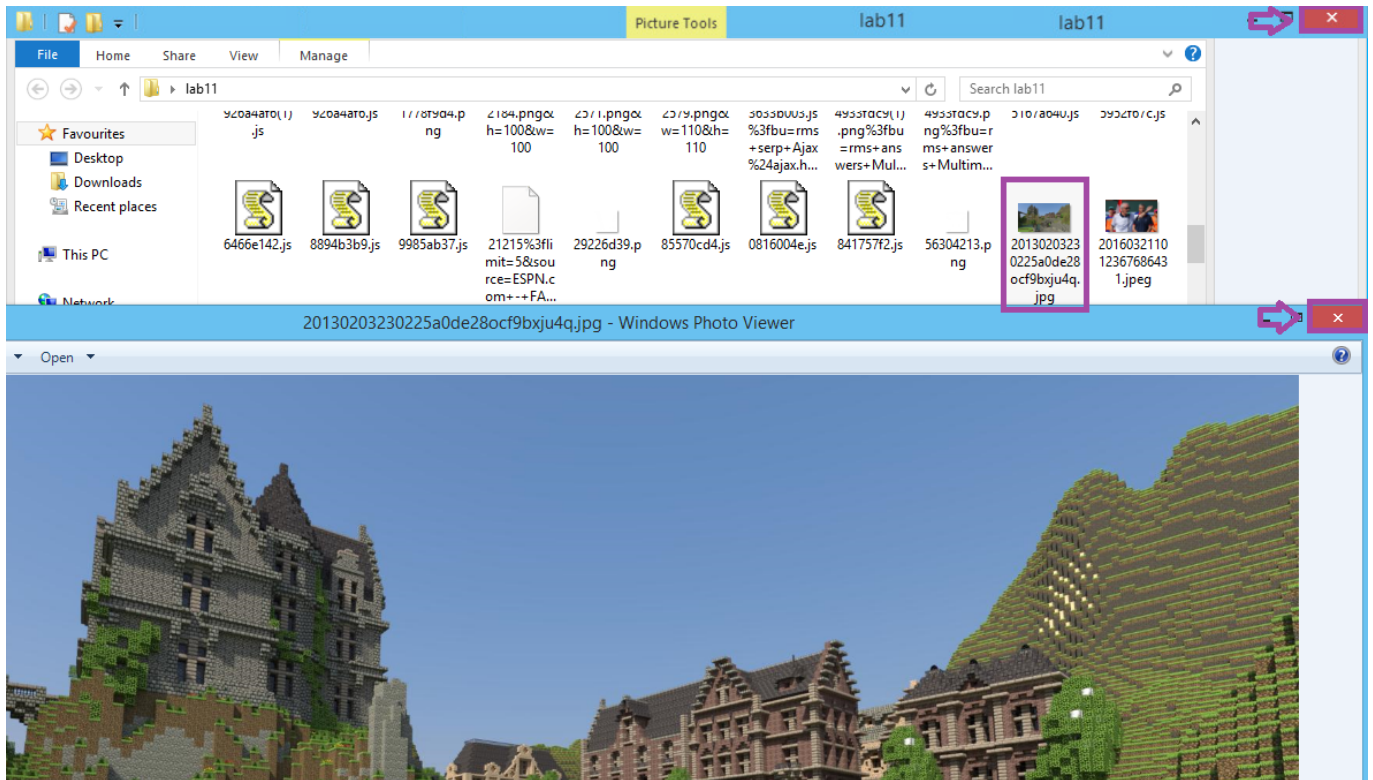
## WIRESHARK

5. Close the **HTTP** object list and **Wireshark** by clicking the two **Xs** in the top right corner.



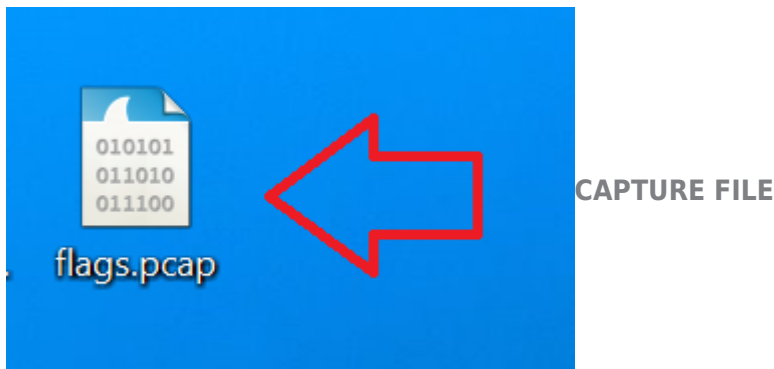




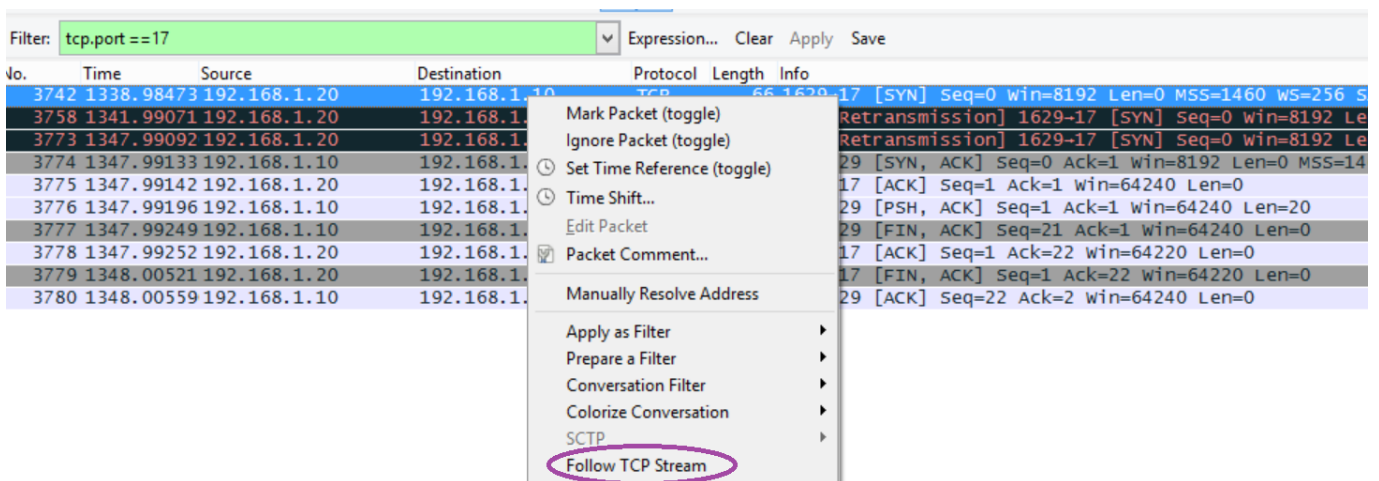


## PARSED FILES

9. **Double-click** on the `flags.pcap` Wireshark file in the list.

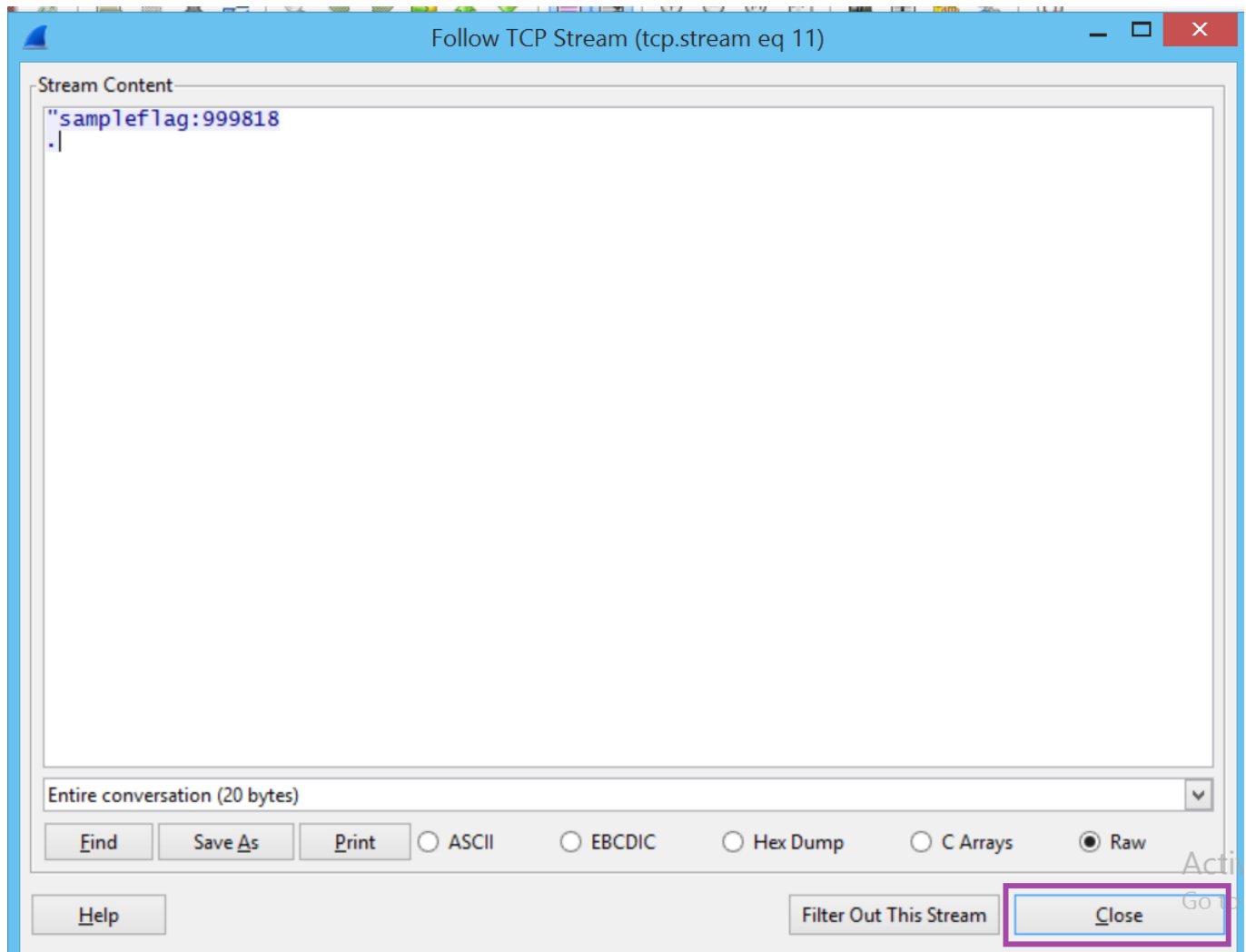


10. **Type** `tcp.port == 17` in the Wireshark filter pane and then **click Apply** to view QOTD traffic. **Right-click** the first frame and then **select Follow TCP Stream**.



## WIRESHARK FILTER

11. **Read** the Quote of the Day. **Click** the Close button to **close** the TCP Stream.



### TCP STREAM CONTENT

12. **Notice** the flag of 999818. **Click** on the Challenge icon and **type** the flag number into the left hand pane in the field for flag#1 answer box. This is just to show you how to **capture** Challenge Flags you will see throughout this lab.

Challenge Sample #

Challenge #

Challenge #

Challenge #

## DISCUSSION QUESTIONS:

1. What is HTTP?
2. What is the port of QOTD?

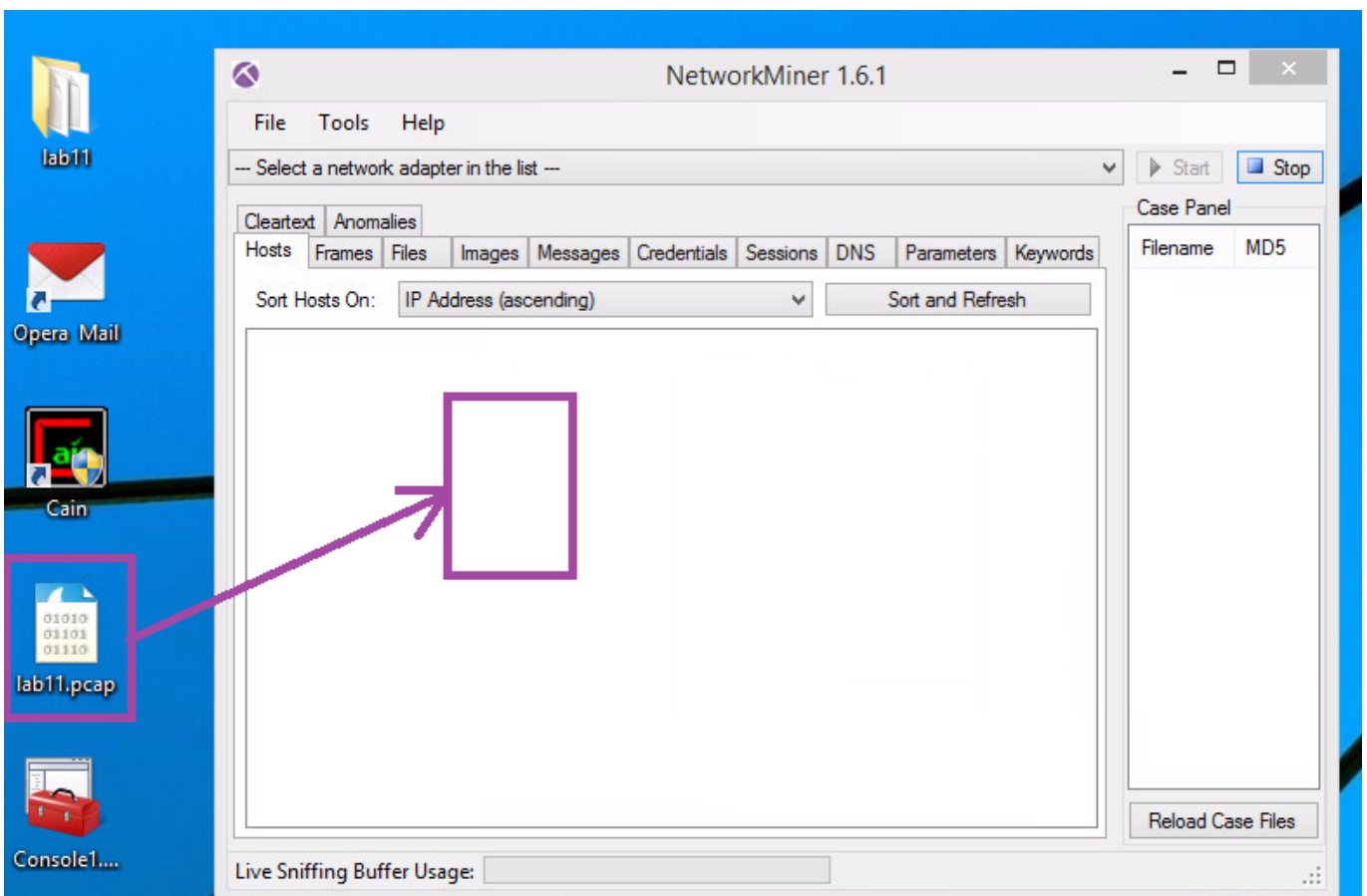
# Using Network Miner

1. **Double-click** on the **shortcut to NetworkMiner** on your desktop.



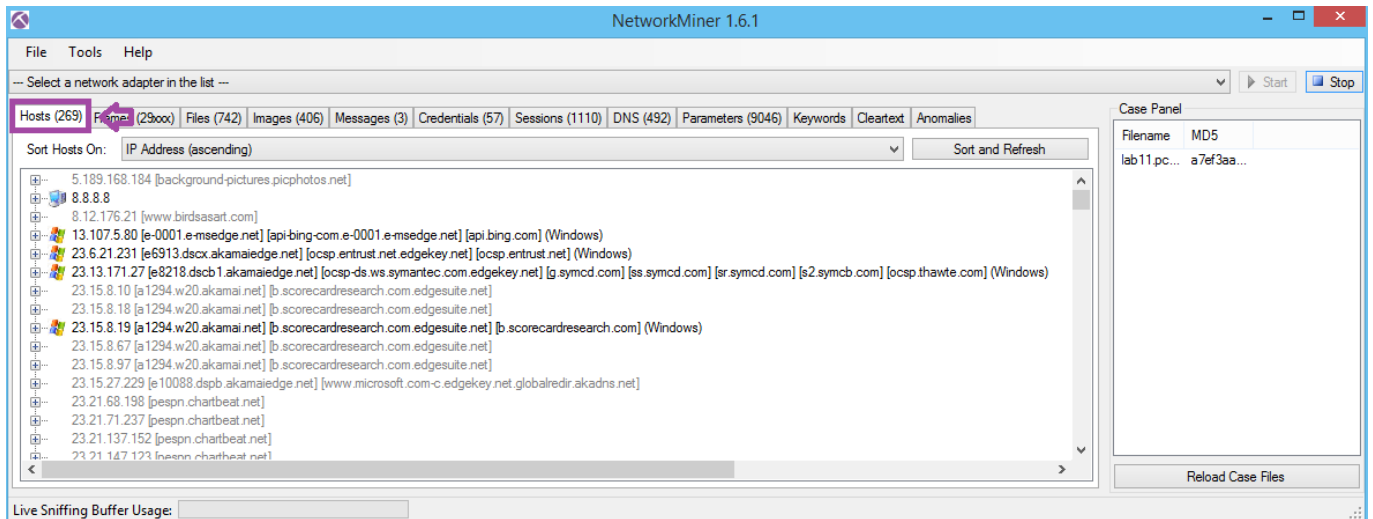
## NETWORKMINER

2. **Drag** the **lab11.pcap** file into the **NetworkMiner** window.



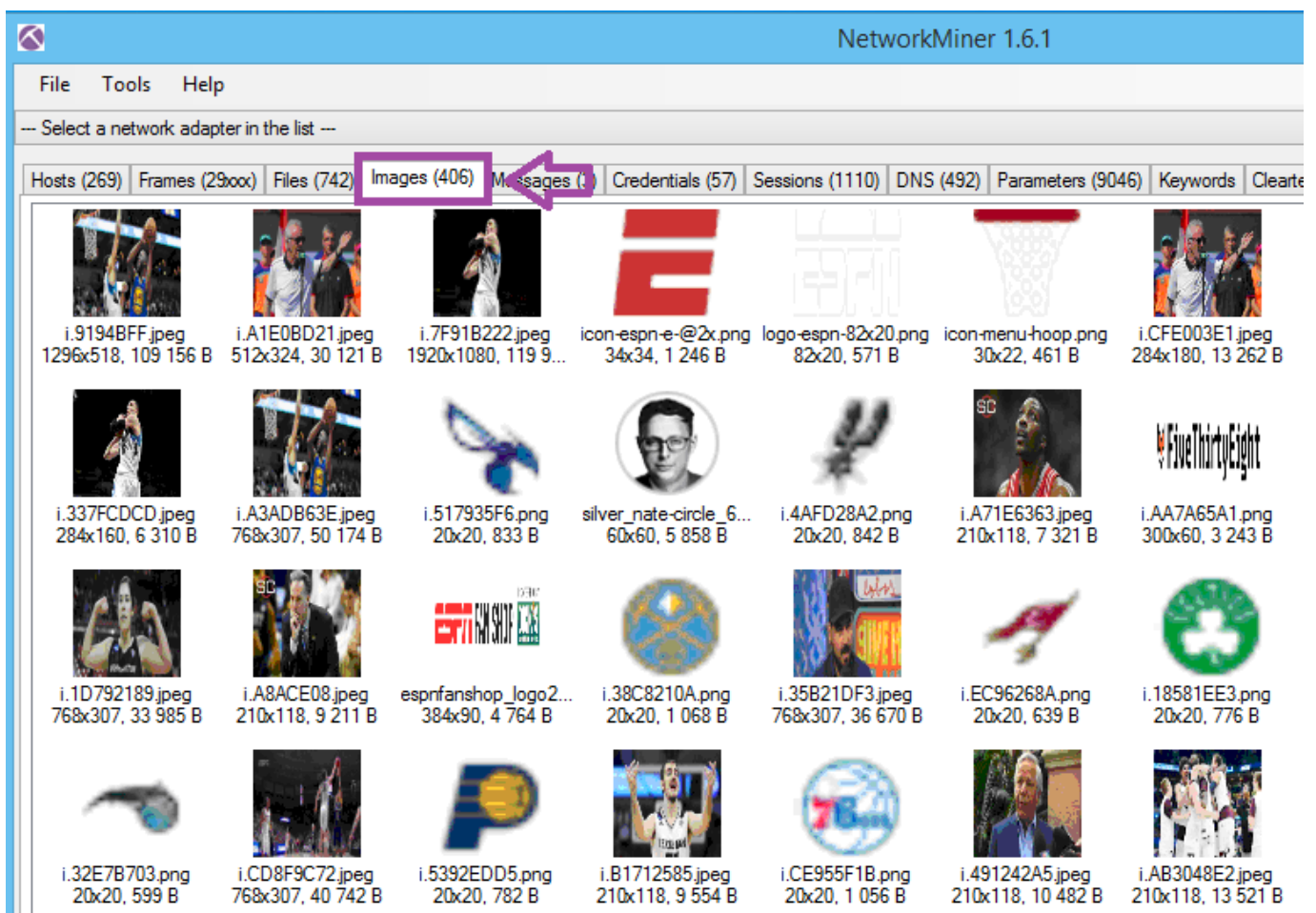
## NETWORK MINER

3. **Wait** for the **lab11.pcap** file to fully transfer. Then **click** on the **Hosts** tab and **view** the hosts running the **Microsoft** operating systems.



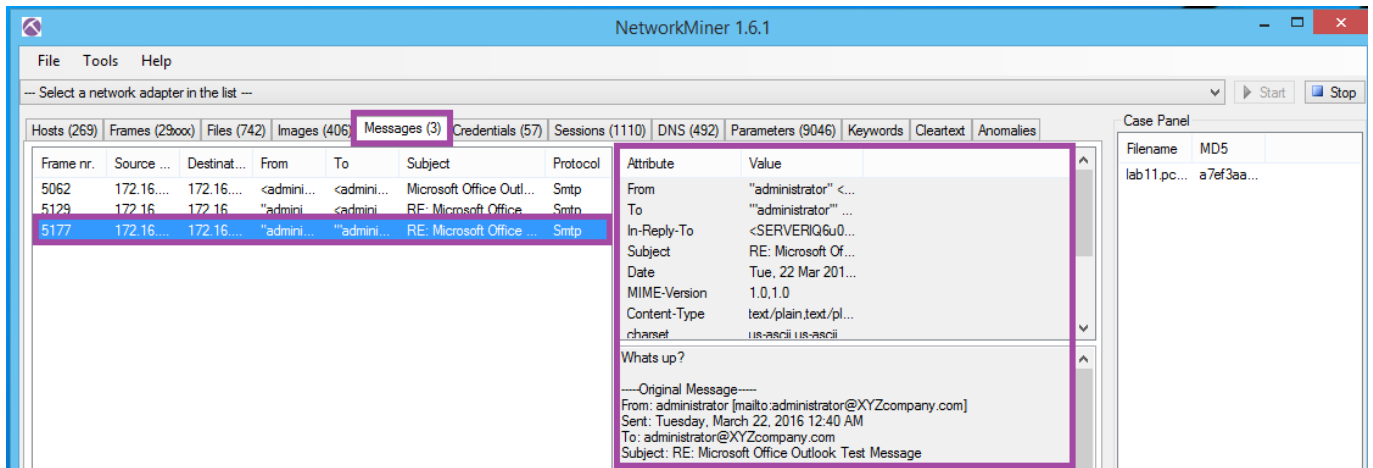
## NETWORKMINER

4. Click on the **Images** tab and **view** some of the images pared from the capture file.



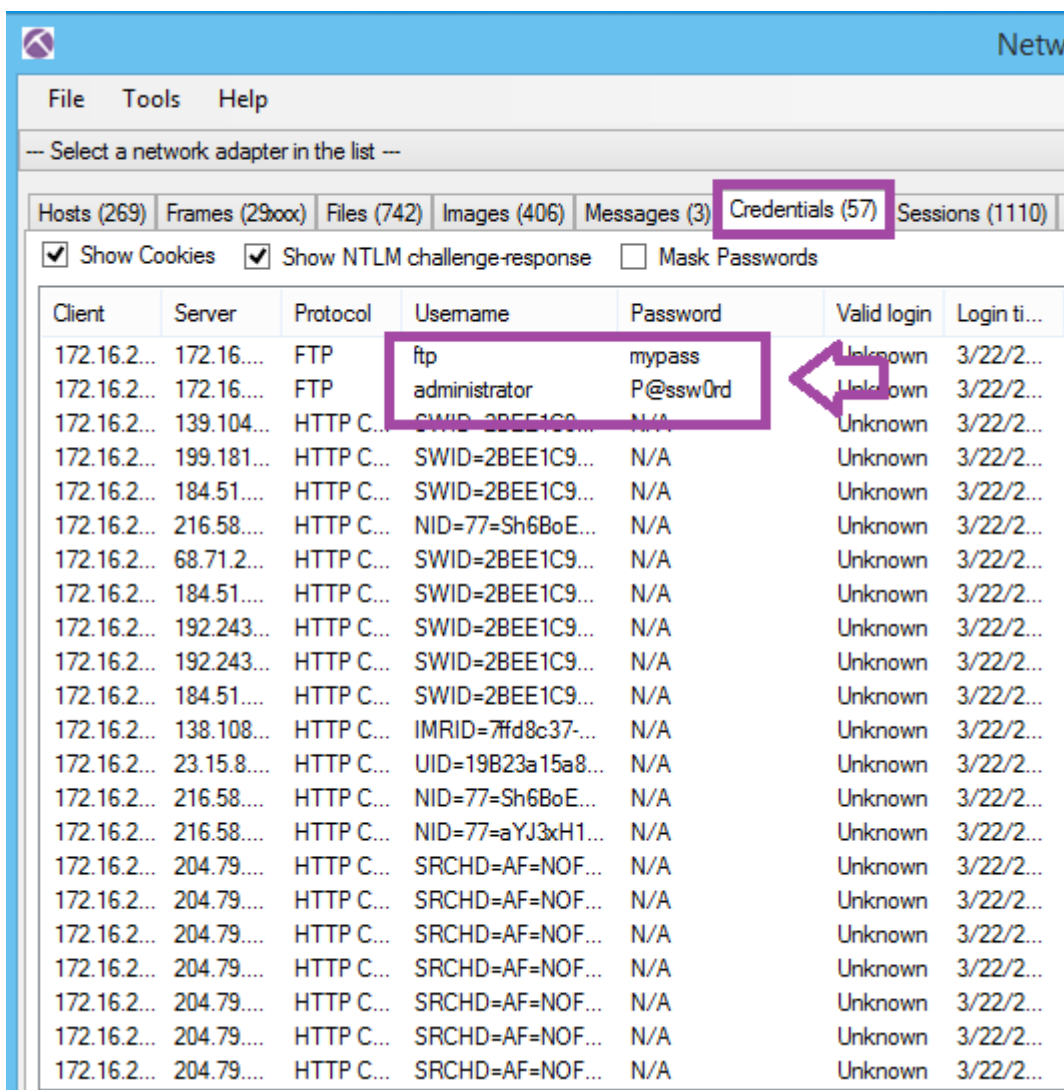
## NETWORKMINER

5. Click on the **Messages** tab. Then **click** on the **bottom email message** and **view** it in the pane.



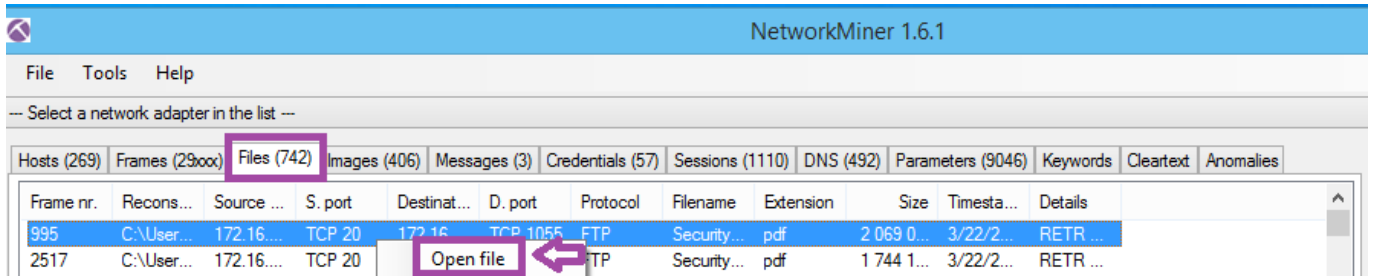
## NETWORKMINER

6. Click on the **Credentials** tab. **View** the parsed usernames and passwords.



## NETWORKMINER

7. Click on the **Files** tab, and **right-click** on the **first file**, and then **select Open file**. **View** the PDF.



**NETWORKMINER**

8. **View** the opened PDF file.



## CompTIA Security+® Lab Series

### Lab 1: Network Devices and Technologies - Capturing Network Traffic

CompTIA Security+® Domain 1 - Network Security

**Objective 1.1: Explain the security function and purpose of network devices and technologies**

**Document Version: 2012-08-15 (Beta)**

**Lab Author: Jesse Varsalone**  
Assistant Professor

**PDF FILE**

9. **Click** on the Red X in the coren to close network miner.



**NETWORKMINER**

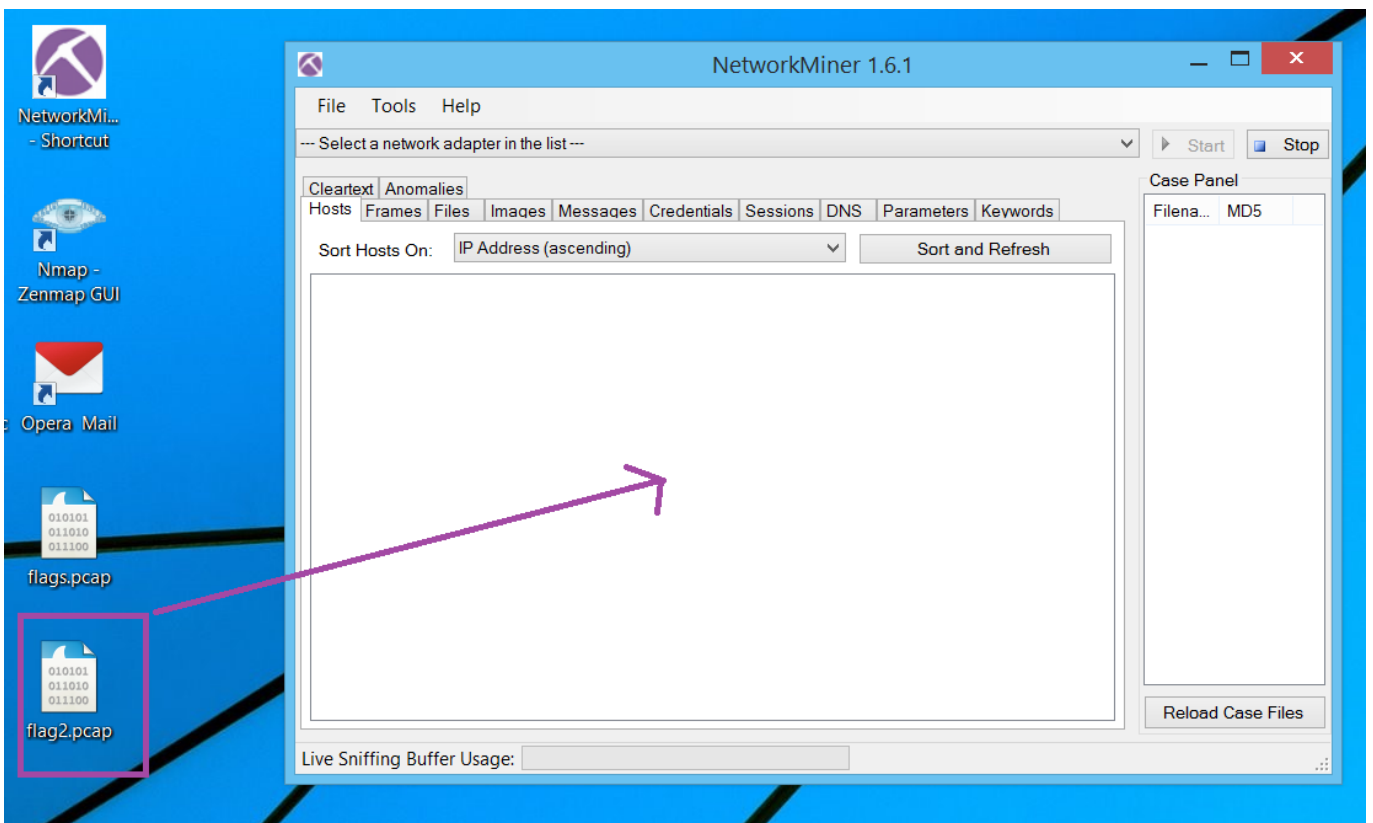
10. **Double-click** on the shortcut to NetworkMiner on your desktop.





NETWORKMINER

10. **Drag** the `flag2.pcap` file into the NetworkMiner window.



NETWORK MINER

Challenge #

Challenge #

Note: Press the STOP button to complete the lab.

## DISCUSSION QUESTIONS:

1. What is NetworkMiner?
2. What is the messages tab?
3. What is the credentials tab?
4. What is the images tab?

