

# 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



#### 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

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).

FIGURE 2 - TCP/IP NETWORKING MODEL

Hardwa	re Type	Protocol Type				
(16	bits)	(16 bits)				
HA Length	PA Length	Operation				
(8 bits)	(8 bits)	(16 bits)				
Sender Hardware Address (Octets 0-3)						
Sender Hardy	ware Address	Sender Protocol Address				
(Octer	is 4-5)	(Octets 0-1)				
Sender Proto	ocol Address	Target Hardware Address				
(Octer	(s 2-3)	(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.

#### **IP Header**



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.

<		3	2 Bits	······,	
8		8	8	8	
Version = 6	n = 6 Traffic Class Flow Label				
	Payload Length	Ú.	Next Header	Hop Limit	
		Sourc	e Address	-	
		Destina	tion Address	-	

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.

# ICMP packet format <u>32 bits</u> type code checksum message-specific information

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.

#### TCP packet makeup



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.





#### 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.

Application	FTP
Transport	ТСР
Network	IP
Data Link	Ethernet

**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.

Application	POP
Transport	ТСР
Network	IP
Data Link	Ethernet

**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.

Application	SMTP
Transport	ТСР
Network	IP
Data Link	Ethernet

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.

Application	DNS
Transport	UDP

Network	IP		
Data Link	Ethernet		
	FICURE 13		CTAC

**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 <u>link</u>. 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.

4	v-netf	lix-proble	ms-2011-07-0	)6.pcap					– 🗆 X
File	Edit	View	Go Captur	e Analyz	e Statistics	Telephor	ny Wirele	ss Tools	Help
1				Q @	e 🕾 🖗		=	9 1	
					~ = 0	#1			
	ppiy a	display filte	sr <ctri-></ctri->						E Pression +
No.		lime	Source		Destination		Protocol	Length	Info
	343 6	55.14241	5 192.168.	0.21	174.129.	249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
	344 8	5 23073	192.100.	240 228	102 168	249.220 0 21	тср	255	001 / Clients/netTlix/flash/application.swf?tlash_version=Tlash_lite_2.lav=1.5ann
	346 6	55.24074	2 174.129.	249.228	192.168.	0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
	347 (	55.24159	2 192.168.	0.21	174.129.	249.228#	2.CP	66	40555 → 80 [ACK] Seg=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
	348 (	55.24253	2 192.168.	0.21	192.168.	0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
	349 6	55.27687	0 192.168.	0.1	192.168.	0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
	350 6	55.27799	2 192.168.	0.21	63.80.24	2.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
	351 6	55.29775	7 63.80.24	2.48	192.168.	0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
	352 (	55.29839	6 192.168.	0.21	63.80.24	2.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
	353 (	55.29868	7 192.168.	0.21	63.80.24	2.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
	354 6	55.31873	0 63.80.24	2.48	192.168.	0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
	355 6	5.3217:	13 63.80.24	2.48	192.168.	0.21	TCP	1514	[TCP segment of a reassembled PDU]
E.									>
	Intern ser D omain [Ti Tra [Ti Tra Que Ans Aut Add Que Ans Aut Add Add Ans Aut	<pre>int if, int prot latagram in Name S quest I me: 0.0 nsactio gs: 0x8 stions: wer RRs hority itional ries cdn-0.n wers horitat</pre>	src: Globa ocol Versi Protocol, ystem (res <u>n: 348]</u> 34338000 s n ID: 0x21 180 Standa 1 : 4 RRs: 9 RRs: 9 RRs: 9 flximg.com	Isc_e00:sc on 4, Src Src Port ponse) econds] 88 rd query : type A, rvers	:: 192.168 :: 53 (53) response, class IN	No error	:: 192.16 t: 34036	(34036)	D_1+:04:E1 (A0:13:20:14:04:E1)
002		15 00	25 94 f4 0	1 -7 02	2£ 21 00	01 00 00	01	- 3	
003	00	04 00	09 00 09 0	5 63 64	6e 2d 30	07 6e 66	6c	c dn	-0.nfl #4
004	78	69 6d	67 03 63 6	f 6d 00	00 01 00	01 c0 0c	00 xim	g.com	
005	05	00 01	00 00 05 2	9 00 22	06 69 6d	61 67 65	73	). ".	images
005	0 07 0 65	73 75	69 74 65 0	3 6e 65	74 00 c0	2f 00 05	00 esu	ite.n et	
-	7 1	dentificati	on of transactiv	an (dos id)	bytes				Darkete: 10299 - Dienlaveri: 10299 (100 0%) - Load time: 0:0-193 Decilia: Dafait
	Line .	activitedu	an or u di isdicul	in (unanu), a	L Dytes				Provers, 10239 Displayed, 10239 (100.0 %) Load dife, 0(0.102 Profile; Default

**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.

🔇 NetworkMi	iner 2.0					- 0	×
<u>File</u> <u>T</u> ools	<u>H</u> elp						
Select a networ	urk adapter in the li	et				V & Start	Ston
Science a networ	and adapter in the i	51				- Oton	- Stop
Keywords Anor	malies					Case Panel	
Hosts (129) File	es (131) Images	(33) Messages Credentials (2) Ses	sions (113) DNS	(271) Para	meters (1199)	Filename ME	)5
-				_		snort.log 2f3	01c2
Filter keyword:			se sensitive Ex	actPhrase	<ul> <li>Clear Apply</li> </ul>		
D. port F	Protocol	Filename	Extension	Size	Details ^		
TCP 53130 T	TIsCertificate	nr-data.net.cer	cer	1 203 B	TLS Certificate: C		
TCP 53130 T	TIsCertificate	GeoTrust SSL CA - G2.cer	cer	1 117 B	TLS Certificate: C		
TCP 53130 T	TIsCertificate	GeoTrust Global CA.cer	cer	897 B	TLS Certificate: C		
TCP 53138 H	HttpGetNormal	index.html[2].ocsp-response	ocsp-response	1 455 B	gb.symcd.com/		
TCP 53139 H	HttpGetChunked	index.html	html	86 958 B	www.meetup.com		
TCP 53142 H	HttpGetNormal	almond.min.js.javascript	javascript	2 758 B	static2.meetupsta		
TCP 53140 H	HttpGetNormal	meetup_jquery_ui.css	CSS	6 725 B	static2.meetupsta		
TCP 53144 H	HttpGetNormal	client.min.js.javascript	javascript	3 692 B	static2.meetupsta		
TCP 53145 H	HttpGetNormal	infoWidget.min.js.javascript	javascript	20 639 B	static2.meetupsta		
TCP 53151 H	HttpGetNormal	groupMetadata.min.js.javascript	javascript	2 409 B	static1.meetupsta		
TCP 53149 H	HttpGetNormal	mt-twoButtonCTA-testimonial.css	CSS	445 B	static1.meetupsta		
TCP 53147 H	HttpGetNormal	print.css	CSS	2 171 B	static1.meetupsta		
TCP 53141 H	HttpGetNormal	meetup-modem.css	CSS	223 971 B	static2.meetupsta		
TCP 53139 H	HttpGetNormal	index.html.6D1A30C1.css	CSS	5 582 B	www.meetup.com		
TCP 53146 H	HttpGetNormal	whitney.css	CSS	83 455 B	static1.meetupsta		
TCP 53150 H	HttpGetNormal	ghome.min.js.javascript	javascript	102 378 B	static1.meetupsta		
TCP 53148 H	HttpGetNormal	chapterbase.css	CSS	165 101 B	static1.meetupsta		
TCP 53143 H	HttpGetNormal	Meetup.Base.jquery.min.js.javascript	javascript	414 355 B	static2.meetupsta		
TCP 53152 H	HttpGetNormal	thumb_156167702.jpeg	ipeg	2 611 B	photos3.meetupst		
TCP 53156 H	HttpGetNormal	thumb_151699612.jpeg.PNG	PNG	2 571 B	photos3.meetupst		
<		I L MANAGAN DNC	DNC	10 COO D	>	Reload Case	Files
Live Sniffing But	ffer Usage:						

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 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.

Filter:	іруб			V Expression	Clear	Apply Sve
lo.	Time	Source	Destination	Protocol L	.ength	Info
5	93 52.853	953 fe80::78d5	5:d63:3edeff02::1:3	LLMNR	94	Standard query 0x4ed4 A METASPLOITABLE
5	95 52.959	123 fe80::78d5	5:d63:3edeff02::1:3	LLMNR	94	Standard query 0x4ed4 A METASPLOITABLE
6	22 77.415	018 fe80::78d	5:d63:3edeff02::1:2	DHCPv6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
6	24 78.412	214 fe80::78d5	5:d63:3edeff02::1:2	DHCPV6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
6	25 80.412	283 fe80::78d5	5:d63:3edeff02::1:2	DHCPv6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
6	26 84.412	245 fe80::78d5	5:d63:3edeff02::1:2	DHCPV6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
6	27 92.412	302 fe80::78d	5:d63:3edeff02::1:2	DHCPv6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
6	80 108.41	2424 fe80::78d	5:d63:3edeff02::1:2	DHCPv6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
8	31 140.41	2547 fe80::78d5	5:d63:3edeff02::1:2	DHCPV6	152	Solicit XID: 0xf42084 CID: 00010001162e8742000c29166864
50	84 433.78	1238 fe80::78d5	5:d63:3edeff02::1:3	LLMNR	84	Standard query 0x6385 A wpad
50	86 433.88	0572 fe80::78d	5:d63:3edeff02::1:3	LLMNR	84	Standard query 0x6385 A wpad
51	87 504.41	4508 fe80::78d	5:d63:3edeff02::1:2	DHCPV6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
51	88 505.41	1983 fe80::78d5	5:d63:3edeff02::1:2	DHCPV6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
51	89 507.41	1999 fe80::78d	5:d63:3edeff02::1:2	DHCPv6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
51	90 511.41	2020 fe80::78d	5:d63:3edeff02::1:2	DHCPv6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
51	91 519.41	2001 fe80::78d	5:d63:3edeff02::1:2	DHCPV6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
51	92 535.41	2099 fe80::78d5	5:d63:3edeff02::1:2	DHCPV6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
52	71 567.42	8199 fe80::78d	5:d63:3edeff02::1:2	DHCPv6	152	Solicit XID: 0x258b3 CID: 00010001162e8742000c29166864
195	50 825.88	0090 fe80::78d	5:d63:3edeff02::1:3	LLMNR	86	Standard query 0x61a2 A server
195	52 825.97	5150 fe80::78d5	5:d63:3edeff02::1:3	LLMNR	86	Standard query 0x61a2 A server
195	76 833.89	2281 fe80::78d5	5:d63:3edeff02::1:3	LLMNR	84	Standard query 0x6e4a A wpad
195	78 833.99	0496 fe80::78d	5:d63:3edeff02::1:3	LLMNR	84	Standard query 0x6e4a A wpad
195	84 836.44	5026 fe80::78d	5:d63:3edeff02::1:3	LLMNR	86	Standard guery Oxbe70 A server

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

<b>A</b>		lab11.pcap [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
<u>File Edit View Go Capture Analyze Statis</u>	tics Telephony <u>T</u> ools <u>I</u> ntern	als <u>H</u> elp
● ● 🖌 🖩 🖉   🖻 🗎 🗶 🤪   🥄	. 🗢 🗇 🖗 生   📃	🗐   Q, Q, Q, 🖭   🐺 🔟 🥵 %   💢
Filten ip and lipv6	✓ E	rpression Clear Apply Ste
No. Time Source	Destination P	Protocol Length Info
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
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 837.068805172.16.200.200	172.16.200.100	FCP 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 837.069065172.16.200.200	172.16.200.100	ATTP 149 OPTIONS / HTTP/1.1
19598 837.203652 172.16.200.100	172.16.200.200	АТТР 460 НТТР/1.1 200 ОК
19599 837.412421 172.16.200.200	172.16.200.100	FCP 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 840.302589172.16.200.200	224.0.0.252	LLMNR 64 Standard query 0xa98f A wpad
19604 840.506206172.16.200.200	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 843.069116172.16.200.200	224.0.0.252	LLMNR 66 Standard query 0x7600 A server
19614 843.177555172.16.200.200	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.

Filter:	ip.addr == 224.0.	0.0/8		✓ Expression	. Clear	Apply	3		
No.	Time	Source	Destination	Protocol I	Length	Info			
59	4 52.854161	172.16.200.200	224.0.0.252	LLMNR	74	Standard q	uery (	0x4ed4	A METASPLOITABLE
59	6 52.959186	172.16.200.200	224.0.0.252	LLMNR	74	Standard q	uery (	0x4ed4	A METASPLOITABLE
508	5 433.781349	9172.16.200.200	224.0.0.252	LLMNR	64	Standard q	uery (	0x6385	A wpad
508	7 433.880633	3 172.16.200.200	224.0.0.252	LLMNR	64	Standard q	uery (	0x6385	A wpad
1955	1 825.880200	0 172.16.200.200	224.0.0.252	LLMNR	66	Standard q	uery (	0x61a2	A server
1955	3 825.975251	L 172.16.200.200	224.0.0.252	LLMNR	66	Standard q	uery (	0x61a2	A server
1957	7 833.89240	5 172.16.200.200	224.0.0.252	LLMNR	64	Standard q	uery (	0x6e4a	A wpad
1957	9 833.990558	8 172.16.200.200	224.0.0.252	LLMNR	64	Standard q	uery (	0x6e4a	A wpad
1958	5 836.445163	3 172.16.200.200	224.0.0.252	LLMNR	66	Standard q	uery (	0xbe70	A server
1958	7 836.552534	172.16.200.200	224.0.0.252	LLMNR	66	Standard q	uery (	0xbe70	A server
1959	1 836.756200	5172.16.200.200	224.0.0.252	LLMNR	66	Standard q	uery (	0x0a4f	A server
1959	3 836.865581	L 172.16.200.200	224.0.0.252	LLMNR	66	Standard q	uery (	0x0a4f	A server
1960	1 840.199281	L 172.16.200.200	224.0.0.252	LLMNR	64	Standard q	uery (	0xa98f	A wpad
1960	3 840.302589	9172.16.200.200	224.0.0.252	LLMNR	64	Standard q	uery (	0xa98f	A wpad
1960	8 842.758863	3 172.16.200.200	224.0.0.252	LLMNR	66	Standard q	uery (	0x9b28	A server
1961	0 842.865587	7 172.16.200.200	224.0.0.252	LLMNR	66	Standard q	uery (	0x9b28	A server
1961	2 843.069110	5172.16.200.200	224.0.0.252	LLMNR	66	Standard q	uery (	0x7600	A server

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

							_			_							
F	ilter:	ip.ad	ldr == 172.1	6.200.255			~	Expression.	Clear	Apply	(Ne						
No	o.	Tir	me	Source		Destination		Protocol	Length	Info							
	1960	4 84	40.50620	6172.10	5.200.200	172.16.200.2	55	NBNS	92	Name	query	NB	WPAD<00>				
	1960	5 84	41.25547	3172.10	5.200.200	172.16.200.2	55	NBNS	92	Name	query	NB	WPAD<00>				
	1960	6 84	42.00559	6172.10	5.200.200	172.16.200.2	55	NBNS	92	Name	query	NB	WPAD<00>				
	1962	5 84	43.69467	9172.10	5.200.200	172.16.200.2	55	NBNS	92	Name	query	NB	WPAD<00>				
	1962	6 8	44.44354	2 172.16	5.200.200	172.16.200.2	55	NBNS	92	Name	query	NB	WPAD<00>				
	1962	7 84	45.19351	2 172.10	5.200.200	172.16.200.2	55	NBNS	92	Name	query	NB	WPAD<00>				
	1966	8 8	66.61576	9172.16	5.200.200	172.16.200.2	55	NBNS	92	Name	query	NB	WPAD<00>				
	1967	4 8	67.36556	5172.10	5.200.200	172.16.200.2	55	NBNS	92	Name	query	NB	WPAD<00>				
	1979	2 8	68.11554	0172.16	5.200.200	172.16.200.2	55	NBNS	92	Name	query	NB	WPAD<00>				
	2046	9 8	69.25621	2 172.10	5.200.200	172.16.200.2	55	NBNS	92	Name	query	NB	WPAD<00>				
	2096	8 8	70.00554	0172.16	5.200.200	172.16.200.2	55	NBNS	92	Name	query	NB	WPAD<00>				
	2142	1 8	70.75559	7 172.10	5.200.200	172.16.200.2	55	NBNS	92	Name	query	NB	WPAD<00>				
	2208	1 94	40.50592	8172.10	5.200.100	172.16.200.2	55	BROWSER	243	Loca	1 Mast	er /	nnouncement SERVER	Norkstatic	on, Server,	SQL Server	, Domain (
	2784	6 1:	132.34164	4 172.10	5.200.30	172.16.200.2	55	BROWSER	286	Loca	1 Mast	er /	nnouncement METASP	LOITABLE, WO	orkstation,	Server, Pri	int Queue
	2784	7 1	132.3416	7 172.10	5.200.30	172.16.200.2	55	BROWSER	257	Doma	in/Wor	kgro	up Announcement WO	RKGROUP, NT	Workstatio	n, Domain Er	านm
	2792	6 1	132.9090	9172.16	5.200.100	172.16.200.2	55	NBNS	92	Name	query	NB	TSCLIENT<00>				
	2792	7 1	132.9092	8172.10	5.200.100	172.16.200.2	55	NBNS	92	Name	query	NB	TSCLIENT<20>				
	2795	6 1	133.6466	3172.16	5.200.100	172.16.200.2	55	NBNS	92	Name	query	NB	TSCLIENT<00>				
	2795	7 1	133.6467	8172.10	5.200.100	172.16.200.2	55	NBNS	92	Name	query	NB	TSCLIENT<20>				
	2805	5 1	134.3965	8 172.16	5.200.100	172.16.200.2	55	NBNS	92	Name	query	NB	TSCLIENT<00>				
	2805	6 1	134.3966	3 172.10	5.200.100	172.16.200.2	55	NBNS	92	Name	query	NB	TSCLIENT<20>				
	2819	9 1	135.1470	3 172.16	5.200.100	172.16.200.2	55	NBNS	92	Name	query	NR	TSCI TENT<00>				

WIRESHARK FILTER

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

Filter	: icmp		Y	Expression	Clear Apply						
No.	Time	Source	Destination	Protocol Le	nath 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.

Filter:	arp				<ul> <li>Expression</li> </ul>	Clear	Apply
No.	Tin	ne	Source	Destination	Protocol	Length	Info
51	94 56	6.587001	Vmware_f3:68:90	Vmware_98:00:1a	ARP	42	172.16.200.2 is at 00:50:56:f3:68:90
180	87 71	7.046052	Vmware_98:00:1a	Broadcast	ARP	42	who has 172.16.200.100? Tell 172.16.200.200
180	88 71	7.046133	Vmware_43:c9:0d	Vmware_98:00:1a	ARP	42	172.16.200.100 is at 00:0c:29:43:c9:0d
196	69 86	6.870242	Vmware_f3:68:90	Broadcast	ARP	42	who has 172.16.200.200? Tell 172.16.200.2
196	70 86	6.870321	Vmware_98:00:1a	Vmware_f3:68:90	ARP	42	172.16.200.200 is at 00:50:56:98:00:1a
219	98 92	1.974873	Vmware_98:00:1a	Vmware_f3:68:90	ARP	42	who has 172.16.200.2? Tell 172.16.200.200
219	99 92	1.974893	Vmware_f3:68:90	Vmware_98:00:1a	ARP	42	172.16.200.2 is at 00:50:56:f3:68:90
220	68 93	6.474805	Vmware_98:00:1a	Vmware_43:c9:0d	ARP	42	Who has 172.16.200.100? Tell 172.16.200.200
220	69 93	6.474873	Vmware_43:c9:0d	Vmware_98:00:1a	ARP	42	172.16.200.100 is at 00:0c:29:43:c9:0d
220	82 94	5.671060	Vmware_98:00:1a	Broadcast	ARP	42	Who has 172.16.200.30? Tell 172.16.200.200
220	83 94	5.671137	Vmware_fa:dd:2a	Vmware_98:00:1a	ARP	42	172.16.200.30 is at 00:0c:29:fa:dd:2a
243	44 10	22.53769	Vmware_98:00:1a	Broadcast	ARP	42	who has 172.16.200.50? Tell 172.16.200.200
243	45 10	22.53783	Vmware_9a:be:c1	Vmware_98:00:1a	ARP	60	172.16.200.50 is at 00:0c:29:9a:be:c1
244	25 10	26.21676	Vmware_f3:68:90	Broadcast	ARP	42	who has 172.16.200.50? Tell 172.16.200.2
244	26 10	26.21690	Vmware_9a:be:c1	Vmware_f3:68:90	ARP	60	172.16.200.50 is at 00:0c:29:9a:be:c1
244	61 10	27.42744	Vmware_98:00:1a	Broadcast	ARP	42	Who has 172.16.200.100? Tell 172.16.200.200
244	62 10	27.42750	Vmware_43:c9:0d	Vmware_98:00:1a	ARP	42	172.16.200.100 is at 00:0c:29:43:c9:0d
259	86 10	67.78329	Vmware_fa:dd:2a	Vmware_98:00:1a	ARP	42	Who has 172.16.200.200? Tell 172.16.200.30
259	87 10	67.78338	Vmware_98:00:1a	Vmware_fa:dd:2a	ARP	42	172.16.200.200 is at 00:50:56:98:00:1a
273	32 11	11.97451	Vmware_98:00:1a	Vmware_f3:68:90	ARP	42	who has 172.16.200.2? Tell 172.16.200.200
273	33 11	11.97453	Vmware_f3:68:90	Vmware_98:00:1a	ARP	42	172.16.200.2 is at 00:50:56:f3:68:90
278	59 11	32.73412	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.

4						lab11.pcap [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from m
Eile	<u>E</u> di	it <u>V</u> iew <u>G</u> o	Capture Analyze Statis	tics Telephony Iools	Internals Help	
۰	۲	🛋 🔳 🙇	🖹 🖹 🗶 🔁 🔍	수 수 🕹 🗿 🛃		. 🔍 🔍 🔟 📓 📓 🥵 🖗   🧱
Filt	er: to	cp			✓ Expression	Clear Apply Save
No.		Time	Source	Destination	Protocol Lo	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 SAC
	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	53.165/08	1/2.16.200.200	1/2.16.200.30	NBSS	126 Session request, to METASPLOITABLE<20> from STUDENT-PC<
	603	53 168737	172.16.200.30	172.16.200.200	NRSS	54 15941030 [ACK] SEGET ACK=/5 WITH=3630 LET=0
	604	53.169045	172.16.200.200	172.16.200.30	SMB	213 Negotiate Protocol Reguest
	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	53.1/4218	1/2.16.200.30	1/2.16.200.200	LANMAN	219 NetServerEnum2 Response
	615	65 678301	172.16.200.200	172.16.200.30	SMR	03 Tree Disconnect Dequest
	61.6	65.678558	172.16.200.30	172.16.200.200	SMR	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	e 605: 185	bytes on wire (14)	80 bits), 185 bytes	s captured (	(1480 bits)
	Inter	rnet II, Sr	rc: Vmware_ra:dd:20	172 16 200 30 (1	72 16 200 30	$m_a = 98:00:14 (00:50:50:98:00:14)$
	Trans	smission Co	ontrol Protocol, S	c Port: 139 (139)	Dst Port:	1050 (1050), Seq: 5, Ack: 232, Len: 131
	500	urce Port:	139 (139)	C / 0/ C/ 255 (255)	,	1050 (1050); See 5; Kekt 151; Cent 151
	Des	stination F	Port: 1050 (1050)			
	[51	tream index	x: 0]			
	[T0	CP Segment	Len: 131]			
	Sec	quence numb	ber: 5 (relative	e sequence number)		
	[N	ext sequence	ce number: 136	(relative sequence	number)]	
	Ac	knowledgmer	nt number: 232	(relative ack numbe	er)	
	Har	adar Lanath	h: 20 but or	010 (000 100)		
		0000 000	01 1000 = Flags: 0	KOI8 (PSH, ACK)		
		0	= Nonce: Not	ot set		
		0	= Condestion	window Reduced (CW	R): Not set	
		0	= ECN-Echo: No	ot set		
		0	= Urgent: Not	set		
		1 .	= Acknowledgm	ent: Set		
		1	1 = Push: Set			
			.O = Reset: Not :	set		
				t		
			0 = Fin: Not set	t		

**TCP FLAGS** 

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

Filte	r: u	dp			<ul> <li>Expression</li> </ul>	Clear Apply Save
No.		Time	Source	Destination	Protocol Le	ength Info
- 22	114	946.	42/929 Te80::/8d5:d63:30	edett02::1:2	DHCPV6	152 Solicit XID: 0x/ffd83 CID: 00010001162e8/42000c29166864
22	555	962.	427996 fe80::78d5:d63:30	edeff02::1:2	DHCPV6	152 Solicit XID: 0x7ffd83 CID: 00010001162e8742000c29166864
22	700	968.	943458 172.16.200.200	8.8.8.8	DNS	76 Standard query 0x2bfc A dns.msftncsi.com
22	701	968.	960298 8.8.8.8	172.16.200.200	DNS	92 Standard query response 0x2bfc A 131.107.255.255
22	702	968.	960558 172.16.200.200	8.8.8.8	DNS	76 Standard query 0x3bc8 AAAA dns.msftncsi.com
22	703	968.	978583 8.8.8.8	172.16.200.200	DNS	104 Standard query response 0x3bc8 AAAA fd3e:4f5a:5b81::1
23	495	994.	428106 fe80::78d5:d63:30	edeff02::1:2	DHCPV6	152 Solicit XID: 0x7ffd83 CID: 00010001162e8742000c29166864
24	424	1026	5.19597 172.16.200.50	8.8.8.8	DNS	87 Standard query 0x1bf5 PTR 200.200.16.172.in-addr.arpa
24	427	1026	5.21692 8.8.8.8	172.16.200.50	DNS	87 Standard query response 0x1bf5 No such name
25	038	1046	5.32344 172.16.200.200	8.8.8.8	DNS	76 Standard query 0x8f96   A aus3.mozilla.org
25	039	1046	5.34162 8.8.8.8	172.16.200.200	DNS	140 Standard query response 0x8f96 CNAME aus3.external.zlb.
25	049	1046	5.49664 172.16.200.200	8.8.8.8	DNS	75 Standard query 0xb156 A ocsp.thawte.com
25	050	1046	5.58356 8.8.8.8	172.16.200.200	DNS	177 Standard query response Oxb156 CNAME ocsp-ds.ws.symante
25	065	1046	5.78512 172.16.200.200	8.8.8.8	DNS	80 Standard query 0xf05b A download.mozilla.org
25	066	1046	5.80526 8.8.8.8	172.16.200.200	DNS	145 Standard query response 0xf05b CNAME bouncer-bouncer-ell
25	093	1046	5.84482 172.16.200.200	8.8.8.8	DNS	84 Standard query 0xc402 A download.cdn.mozilla.net
25	096	1046	5.88790 8.8.8.8	172.16.200.200	DNS	235 Standard query response 0xc402 CNAME 2-01-2967-001b.cdx
27	846	1132	2.34164 172.16.200.30	172.16.200.255	BROWSEF	286 Local Master Announcement METASPLOITABLE, Workstation, Se
27	847	1132	2.34167 172.16.200.30	172.16.200.255	BROWSEF	257 Domain/Workgroup Announcement WORKGROUP, NT Workstation,
27	926	1132	2.90909172.16.200.100	172.16.200.255	NBNS	92 Name query NB TSCLIENT<00>
27	927	1132	2.90928 172.16.200.100	172.16.200.255	NBNS	92 Name query NB TSCLIENT<20>
27	956	1133	3.64663 172.16.200.100	172.16.200.255	NBNS	92 Name query NB TSCLIENT<00>
27	957	1133	3.64678 172.16.200.100	172.16.200.255	NBNS	92 Name query NB TSCLIENT<20>
28	055	1134	. 39658 172.16.200.100	172.16.200.255	NBNS	92 Name query NB TSCLIENT<00>

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

F	ilter:	fte	0											mression.		ear	Apply	-	5	
Ľ		. ap											_				- PPO			
No			Tin	ne		Sour	ce			Des	tinatio	on		Protocol	Leng	th	Info			
	97	75	23	5.20	7846	5 172	.16	5.200	.200	17	2.16	. 200.	.100	FTP		60	Reque	st:	NLST	r
	- 96	63	23	1.38	1941	172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		69	Reque	st:	PASS	i P@ssw0rd
	93	32	21	5.02	9982	2 172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		67	Reque	st:	PASS	5 mypass
	97	73	23	5.20	6246	5172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		80	Reque	st:	PORT	172,16,200,200,4,30
	99	90	25	4.62	1111	172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		80	Reque	st:	PORT	172,16,200,200,4,31
	251	12	26	2.10	8525	5 172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		80	Reque	st:	PORT	172,16,200,200,4,32
	379	95	26	8.12	4263	3 172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		80	Reque	st:	PORT	172,16,200,200,4,33
	93	37	21	7.28	7010	172	.16	5.200	.200	17	2.16	. 200.	.100	FTP		60	Reque	st:	QUIT	r
	499	93	27	0.51	5938	3 172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		60	Reque	st:	QUIT	r
	- 99	92	25	4.62	3150	172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		85	Reque	st:	RETR	<pre>&amp; Security_Plus_Lab_01.pdf</pre>
	251	14	26	2.11	0506	5172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		85	Reque	st:	RETR	<pre>Security_Plus_Lab_02.pdf</pre>
	379	97	26	8.12	6278	3172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		85	Reque	st:	RETR	<pre>&amp; Security_Plus_Lab_03.pdf</pre>
	97	71	23	5.20	5887	172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		62	Reque	st:	TYPE	E A
	96	68	23	3.83	8023	3 172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		62	Reque	st:	TYPE	: I
	98	87	23	5.41	4368	3 172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		62	Reque	st:	TYPE	: I
	- 96	60	22	8.08	6400	172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		74	Reque	st:	USER	administrator
	97	29	21	1.04	6240	172	.16	5.200	. 200	17	2.16	. 200.	.100	FTP		64	Reque	st:	USER	t ftp
	97	76	23	5.20	7974	172	.16	5.200	.100	17	2.16	. 200.	. 200	FTP	1	.09	Respo	nse:	: 150	) Opening ASCII mode data connection for file list.
	- 99	93	25	4.62	3410	172	.16	5.200	.100	17	2.16	. 200.	. 200	FTP	1	40	Respo	nse:	: 150	) Opening BINARY mode data connection for Security_Plus_Lab_01.pdf(2069076 bytes
	251	15	26	2.11	0752	2 172	.16	5.200	.100	17	2.16	. 200.	. 200	FTP	1	40	Respo	nse:	: 150	Opening BINARY mode data connection for Security_Plus_Lab_02.pdf(1744189 bytes
	379	98	26	8.12	6932	2 172	.16	5.200	.100	17	2.16	. 200.	. 200	FTP	1	40	Respo	nse:	: 150	) Opening BINARY mode data connection for Security_Plus_Lab_03.pdf(1624900 bytes
	97	74	23	5.20	6340	172	.16	5.200	.100	17	2.16	. 200.	. 200	FTP		84	Respo	nse:	: 200	) PORT command successful.
	99	91	25	4.62	1263	3 172	.16	5.200	.100	17	2.16	. 200.	. 200	FTP		84	Respo	nse:	200	) PORT command successful.
	251	13	26	2.10	8674	172	.16	5.200	.100	17	2.16	. 200.	. 200	FTP		84	Respo	nse:	200	) PORT command successful.
	379	96	26	8.12	4417	172	.16	5.200	.100	17	2.16	. 200.	. 200	FTP		84	Respo	nse:	: 200	) PORT command successful.

#### WIRESHARK FILTER

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

Filte	r: po	ор				~	Expression	Clear	Арр	ly S	¢	
No.		Time	Source	D	estination		Protocol L	.ength	Info			
5	107	452.28	33961 172.16.200.2	200 1	72.16.200.10	00	POP	62	C:	DELE	1	
5	155	461.74	40768 172.16.200.2	200 1	72.16.200.10	00	POP	62	C:	DELE	1	
5	103	452.13	37498 172.16.200.2	200 1	72.16.200.10	00	POP	60	C:	LIST		
5	151	461.72	29983 172.16.200.2	200 1	72.16.200.10	00	POP	60	C:	LIST		
5	021	326.13	32124 172.16.200.3	200 1	72.16.200.10	00	POP	69	C:	PASS	P@ssw0rd	
5	076	430.03	33951 172.16.200.2	200 1	72.16.200.10	00	POP	69	C:	PASS	P@ssw0rd	
5	097	452.13	34340172.16.200.2	200 1	72.16.200.10	00	POP	69	C:	PASS	P@ssw0rd	
5	145	461.72	28907 172.16.200.2	200 1	72.16.200.10	00	POP	69	C:	PASS	P@ssw0rd	
5	023	326.14	1365 172.16.200.2	200 1	72.16.200.10	00	POP	60	C: (	QUIT		
5	078	430.03	36231 172.16.200.3	200 1	72.16.200.10	00	POP	60	C: (	QUIT		
5	109	452.28	35207 172.16.200.2	200 1	72.16.200.10	00	POP	60	C: (	QUIT		
5	157	461.74	1400 172.16.200.2	200 1	72.16.200.10	00	POP	60	C: (	QUIT		
5	105	452.13	39167 172.16.200.2	200 1	72.16.200.10	00	POP	62	C:	RETR	1	
5	153	461.73	31518 172.16.200.3	200 1	72.16.200.10	00	POP	62	C:	RETR	1	
5	099	452.13	37208 172.16.200.3	200 1	72.16.200.10	00	POP	60	C: :	STAT		
5	147	461.72	29680 172.16.200.2	200 1	72.16.200.10	00	POP	60	C: :	STAT		
5	101	452.13	37354 172.16.200.3	200 1	72.16.200.10	00	POP	60	C:	UIDL		
5	149	461.72	29839172.16.200.2	200 1	72.16.200.10	00	POP	60	C:	UIDL		
5	019	326.13	31958 172.16.200.3	200 1	72.16.200.10	00	POP	74	C:	USER	administr	ator
5	074	430.03	33767 172.16.200.3	200 1	72.16.200.10	00	POP	74	C:	USER	administr	ator
5	095	452.13	34189 172.16.200.3	200 1	72.16.200.10	00	POP	74	C:	USER	administr	ator
5	143	461.72	28741 172.16.200.2	200 1	72.16.200.10	00	POP	74	C:	USER	administr	ator
5	020	326.13	32030 172.16.200.3	100 1	72.16.200.20	00	POP	59	S: -	+OK		

#### WIRESHARK FILTER

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

Filte	r: sr	ntp									✓ E	xpression	. Clear	Ap	ply	(1	ve								
No.		Time		Sourc	e			Desti	nation			Protocol	Length	Info	,										
5	058	429.	802368	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	60	c:	DAT	Ά									
5	125	457.	657742	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	60	c:	DAT	Ά									
5	173	470.	686202	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	60	c:	DAT	Ά									
5	175	470.	687924	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	1199	с:	DAT	Ά	fragme	ent,	114	5 by	/tes				
5	060	429.	803191	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	447	с:	DAT	Ά	fragme	ent,	393	byt	tes				
5	127	457.	660210	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	944	c:	DAT	Ά	fragme	ent,	890	byt	tes				
5	119	457.	651467	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	70	c:	EHL	0	studer	ITPC							
5	167	470.	683761	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	70	с:	EHL	0	studer	ITPC							
5	003	326.	101977	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	70	с:	HEL	0	studer	ntPC							
5	033	326.	142700	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	70	c:	HEL	0	studer	ITPC							
5	052	429.	801480	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	70	c:	HEL	0	studer	ITPC							
5	054	429.	801901	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	97	с:	MAI	L	FROM:	<adn< td=""><td>nini</td><td>stra</td><td>ator@</td><td>XYZ</td><td>comp</td><td>any.</td><td><m>&gt;</m></td></adn<>	nini	stra	ator@	XYZ	comp	any.	<m>&gt;</m>
5	121	457.	657271	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	97	c:	MAI	L	FROM:	<adn< td=""><td>nini</td><td>stra</td><td>ator@</td><td>XYZ</td><td>comp</td><td>any.</td><td><pre>com&gt;</pre></td></adn<>	nini	stra	ator@	XYZ	comp	any.	<pre>com&gt;</pre>
5	169	470.	684752	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	97	c:	MAI	L	FROM:	<adn< td=""><td>nini</td><td>stra</td><td>ator@</td><td>XYZ</td><td>comp</td><td>any.</td><td><m>&lt;</m></td></adn<>	nini	stra	ator@	XYZ	comp	any.	<m>&lt;</m>
5	005	326.	105451	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	97	с:	MAI	L	FROM:	<adn< td=""><td>nini</td><td>stra</td><td>ator@</td><td>uni</td><td>vens</td><td>ity.</td><td>edu&gt;</td></adn<>	nini	stra	ator@	uni	vens	ity.	edu>
5	035	326.	143139	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	97	c:	MAI	L	FROM:	<adn< td=""><td>nini</td><td>stra</td><td>ator@</td><td>uni</td><td>vers</td><td>ity.</td><td>edu&gt;</td></adn<>	nini	stra	ator@	uni	vers	ity.	edu>
5	009	326.	129395	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	60	c:	QUI	Т									
5	039	326.	144856	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	60	с:	QUI	т									
5	064	430.	031416	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	60	c:	QUI	Т									
5	132	460.	302696	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	60	c:	QUI	Т									
5	180	473.	318764	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	60	с:	QUI	т									
5	056	429.	802130	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	95	c:	RCF	т	TO: <a< td=""><td>admir</td><td>nisti</td><td>rato</td><td>or@X\</td><td>ZCO</td><td>mpan</td><td>y.co</td><td>m&gt;</td></a<>	admir	nisti	rato	or@X\	ZCO	mpan	y.co	m>
5	123	457.	657525	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	95	с:	RCF	т	TO: <a< td=""><td>admir</td><td>nist</td><td>rate</td><td>or@X\</td><td>ZCO</td><td>mpan</td><td>y.co</td><td>m&gt;</td></a<>	admir	nist	rate	or@X\	ZCO	mpan	y.co	m>
5	171	470.	685744	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	95	c:	RCF	т	TO: <a< td=""><td>admir</td><td>nist</td><td>rate</td><td>or@x\</td><td>ZCO</td><td>mpan</td><td>y.co</td><td>m&gt;</td></a<>	admir	nist	rate	or@x\	ZCO	mpan	y.co	m>
5	007	326.	128880	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	95	c:	RCF	т	TO: <a< td=""><td>admir</td><td>nist</td><td>rate</td><td>or@ur</td><td>ive</td><td>rsit</td><td>y.ed</td><td>lu&gt;</td></a<>	admir	nist	rate	or@ur	ive	rsit	y.ed	lu>
5	037	326.	143406	172.	.16.	200.2	200	172	.16.2	00.100		SMTP	95	c:	RCF	т	TO: <a< td=""><td>admir</td><td>nist</td><td>rate</td><td>or@ur</td><td>ive</td><td>rsit</td><td>y.ed</td><td>lu&gt;</td></a<>	admir	nist	rate	or@ur	ive	rsit	y.ed	lu>

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

Filter:	dns					✓ Expression	Clear	Apply So	e l		
No.	Time		Source		Destination	Protocol L	ength	Info	Ť		
1804	5 692	.988897	172.16.20	0.200	8.8.8.8	DNS	80	Standard	query	0x0001	PTR 8.8.8.8.in-addr.arpa
1804	7 693	.011736	5172.16.20	0.200	8.8.8.8	DNS	72	Standard	query	0x0002	A www.espn.com
1804	9 693	.032206	5172.16.20	0.200	8.8.8.8	DNS	72	Standard	query	0x0003	AAAA www.espn.com
1043	8 594	. 513171	172.16.20	0.200	8.8.8.8	DNS	75	Standard	query	0x0085	A ssl.gstatic.com
1968	6 868	.005717	172.16.20	0.200	8.8.8.8	DNS	89	Standard	query	0x0110	A safebrowsing-cache.google.com
1226	5 631	. 593297	172.16.20	0.200	8.8.8.8	DNS	72	Standard	query	0x0185	A www.sway.com
531	.3 571	. 526837	172.16.20	0.200	8.8.8.8	DNS	79	Standard	query	0x02af	A fxfeeds.mozilla.com
53	1 2.0	53271	172.16.20	0.50	8.8.8.8	DNS	86	Standard	query	0x03ef	PTR 50.200.16.172.in-addr.arpa
1405	7 637	.175999	172.16.20	0.200	8.8.8.8	DNS	87	Standard	query	0x0470	A www.thefemalecelebrity.info
538	32 572	.746128	3172.16.20	0.200	8.8.8.8	DNS	73	Standard	query	0x04b1	A a.espncdn.com
568	35 573	.740244	172.16.20	0.200	8.8.8.8	DNS	73	Standard	query	0x04b1	A a.espncdn.com
1962	0 843	.388449	fe80::78d	5:d63:3ed	eff02::1:3	LLMNR	84	Standard	query	0x04c6	A wpad
1962	1 843	. 388569	172.16.20	0.200	224.0.0.252	LLMNR	64	Standard	query	0x04c6	A wpad
1962	2 843	.490539	fe80::78d fe80	5:d63:3ed	eff02::1:3	LLMNR	84	Standard	query	0x04c6	A wpad
1962	3 843	.490602	172.16.20	0.200	224.0.0.252	LLMNR	64	Standard	query	0x04c6	A wpad
942	1 576	. 375279	172.16.20	0.200	8.8.8.8	DNS	73	Standard	query	0x04f2	A s.adzmath.com
527	2 568	.481043	172.16.20	0.200	8.8.8.8	DNS	77	Standard	query	0x08f8	A sb-ssl.google.com
1959	0 836	.756108	fe80::78d	5:d63:3ed	eff02::1:3	LLMNR	86	Standard	query	0x0a4f	A server
1959	1 836	.756206	5172.16.20	0.200	224.0.0.252	LLMNR	66	Standard	query	0x0a4f	A server
1959	2 836	.865484	fe80::78d	5:d63:3ed	eff02::1:3	LLMNR	86	Standard	query	0x0a4f	A server
1959	3 836	.865581	172.16.20	0.200	224.0.0.252	LLMNR	66	Standard	query	0x0a4f	A server
1412	3 637	.612323	172.16.20	0.200	8.8.8.8	DNS	77	Standard	query	0x0cc0	A www.ecenglish.com
1410	5 637	.417673	172.16.20	0.200	8.8.8.8	DNS	76	Standard	query	0x0cd2	A www.popsugar.com
937	9 576	.281849	172.16.20	0.200	8.8.8.8	DNS	70	Standard	query	0x0d39	A log.go.com
1217	3 631	.422907	172.16.20	0.200	8.8.8.8	DNS	72	Standard	query	0x107d	A www.bing.com
519	5 566	. 587097	172.16.20	0.200	8.8.8.8	DNS	80	Standard	auerv	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.

4		lab11.pcap [W
<u>File Edit View Go</u> Capture Ar	alyze <u>Statistics</u> Telephony <u>T</u> ools	Internals Help
	8 😂   🔍 🗢 🔿 🐴 🛓	🗏 📑 I Q Q 🛛 🖻 🖉 🎋
Filter: tcp.port ==17		Expression Clear Apply Save
No. Time Source	Destination	Protocol Length Info
18308 766.873482 172.16.2           18309 766.873482 172.16.2           18310 766.874082 172.16.2           18311 766.874082 172.16.2           18312 766.874274 172.16.2           18313 766.874318 172.16.2           18313 766.875105 172.16.2           18314 766.879173 172.16.2           18315 766.879241 172.16.2           18316 770.921439 172.16.2           18318 770.92120 172.16.2           18319 770.922308 172.16.2           18320 770.922351 172.16.2           18321 770.923101 172.16.2           18323 770.927048 172.16.2           18323 770.927129 172.16.2           26894 1097.36673 172.16.2           26895 1097.36680 172.16.2	Mark Packet (toggle) Ignore Packet (toggle) Set Time Reference (toggle) Time Shift Edit Packet Packet Comment Manually Resolve Address Apply as Filter Prepare a Filter Conversation Filter Colorize Conversation SCTP Follow TCP Stream	TCP         66 1247-17         [SYN] Seq=0           TCP         66 1/-124/         [SYN, ACK]         S           TCP         54 1247-17         [ACK] Seq=1         TCP           TCP         188 17-1247         [PSH, ACK]         S           TCP         54 1247-17         [ACK] Seq=1         S           TCP         54 1247-17         [ACK] Seq=1         S           TCP         54 1247-17         [ACK] Seq=1         S           TCP         54 1247-17         [FIN, ACK]         S           TCP         54 1247-17         [ACK] Seq=1         S           TCP         54 17-1247         [ACK] Seq=1         S           TCP         54 17-1247         [ACK] Seq=1         S           TCP         66 17-1248         [SYN, ACK]         S           TCP         54 1248-17         [ACK] Seq=1         S           TCP         54 17-1248         [FIN, ACK]         S           TCP         54 1248-17         [ACK] Seq=1         S           TCP         54 1248-17         [ACK] Seq=1         S           TCP         54 1248-17         [ACK] Seq=1         S           TCP         54 1248-17         [ACK] Seq=1
26904 1097.86548 172.16.2 26908 1097.86559 172.16.2	Follow UDP Stream Follow SSL Stream	TCP         66 [TCP Spurious Retrain           TCP         54 17-2014 [RST, ACK]
26914 1098.36547 172.16.2 26918 1098.36557 172.16.2	Сору	
<ul> <li>➡ Frame 18308: 66 bytes or</li> <li>➡ Ethernet II, Src: Vmware</li> <li>➡ Internet Protocol Version</li> </ul>	Protocol Preferences Decode As Print Show Packet in New Window	<pre>aptured (528 bits) ), Dst: Vmware_43:c9:0d (00:0c:29:4 (172 16 200 200) pst: 172 16 200 100</pre>

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

Follow TCP Stream (tcp.stream eq 192)	-	×
Stream Content	_	
"Here's the rule for bargains: "Do other men, for they would do you That's the true business precept." Charles Dickens (1812-70)	u."	
Entire conversation (134 bytes)		¥
<u>Find</u> Save <u>As</u> <u>Print</u> O ASCII O EBCDIC O Hex Dump	C Arrays 💿	Raw
Help Filter Out This St	rear	lose

**TCP STREAM CONTENT** 

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

4											lat	o11.j	ocap	[Wi	resha	ark 1.1	2.6 (v1.1	2.6-0	-gee
Eile	Edit	t <u>V</u> ie	w <u>G</u> o	<u>C</u> aptu	re	Analyze	Stat	istics	Tele	phony	I	ools	Inter	nals	<u>H</u> elp				
	0				-	× a	6		-	-	*	л			Ð	0		57 N	2 🛤
•	۲		. ANI.		888	~ 5		•	~~~	~	Ψ	<u> </u>		-	4	4	< LL		
Filt	er: te	Inet											~ 6	xpress	ion	Clear	Apply	Save	
No.		Time		Source	e				Destina	tion				Proto	ol L	enath	Info		
	635	99.6	33424	172.	16	.200.1	00		177 -	16 20	0	200		TELN	ST.	75	Telnet	Data	
	636	99.6	33515	172.	16	.200.2	00		Mark F	acket	(tog	gle)			Г	57	Telnet	Data	
	637	99.6	33565	172.	16	.200.1	00		Ignore	Packet	t (to	ggle)			T	62	Telnet	Data	
	638	99.6	33597	172.	16	. 200. 2	00	0	Set Tin	ne Refe	eren	e (to	ggle)		T	81	Telnet	Data	
	639	99.6	33639	172.	16	.200.1	00	0	Time	hift					T	89	Telnet	Data	
	641	101.	80511	1 172.	16	. 200. 2	00	0	nine s						T	62	Telnet	Data	
	642	101.	80527	1 172.	16	.200.1	00		Edit Pa	icket					T	92	Telnet	Data	
	643	101.	80533	5 172.	16	. 200. 2	00		Packet	Comn	nent				T	99	Telnet	Data	
	644	101.	80562	4 172.	16	.200.1	00								T	63	Telnet	Data	
	646	103.	09986	5 172.	16	. 200. 2	00		Manua	ally Res	olve	Addi	ress		T	55	Telnet	Data	
	647	103.	09996	9172.	16	.200.1	00		Annly	as Filte	r			,	T I	55	Telnet	Data	
	649	103.	45977	7 172.	16	.200.2	00		- PP-9	514					T	55	Telnet	Data	
	650	103.	45987	4 172.	16	.200.1	00		Prepar	e a Flite	er				T	55	Telnet	Data	
	651	103.	63576	7 172.	16	.200.2	00		Conve	rsation	Filte	er		,	T	55	Telnet	Data	
	652	103.	63587	8 172.	16	.200.1	00		Coloria	ze Conv	versa	ation		,	T	55	Telnet	Data	
	654	103.	88379	2 172.	16	. 200. 2	00		SCTP					)	T	55	Telnet	Data	
	655	103.	88390	3 172.	16	.200.1	00		Follow	TCPS	treat		~	_	T	55	Telnet	Data	
	657	104.	12377	5 172.	16	. 200. 2	00		Follow	HOD C	treat				T	55	Telnet	Data	
	658	104.	12387	9172.	16	.200.1	00		Follow	UDP 5	trea	m			T	55	Telnet	Data	
	660	104.	37974	4 172.	16	. 200. 2	00		Follow	SSL St	rean	٦			T	55	Telnet	Data	
	661	104.	37986	4 172.	16	.200.1	00		Conv						T	55	Telnet	Data	
	662	104.	56374	9172.	16	. 200. 2	00		сору						T	55	Telnet	Data	
	663	104.	56387	1 172.	16	.200.1	00		Protoc	ol Pref	eren	ces		)	T	55	Telnet	Data	
	665	104.	89171	5 172.	16	. 200. 2	00	28	Decod	e Ar					T	55	Telnet	Data	
<								45	Decou	C AS									
	rame	635	: 75	ovtes	on	wire	(600		Print						600	bits	)		
E F	ther	net	II. S	rc: V	mwa	re 43:	c9:0		Show I	Packet	in N	ew W	indow	1	Vm	ware	98:00:1	La (0	0:50
E I	Inter	net	Proto	col v	ers	ion 4.	Sre	: 1	72.1	6.200	).1	00 (	172.	16.2	00.1	.00)	Dst: 1	72.16	. 200
01	rans	miss	ion C	ontro	1 P	rotoco	1, 9	Src	Port	: 23	(2	3),	Dst	Port	: 10	51 (1	.051), 9	Seq:	1, A

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

✓ Follow TCP Stream (tcp.stream eq 1) – □ ×
Stream Content
%% %
login: aaddmmiinniissttaarrrraattoorr
[2;1Hwelcome to Microsoft Telnet Server.
<pre>[4;1HC:\Documents and Settings\Administrator&gt; [5;1H.[K.[6;1H.[K.[7;1H.[K.[8;1H.[K.[9;1H.[K.[10;1H.[K.[11;1H.[K.[12;1H.[K.[13;1H.[K. [14;1H.[K.[15;1H.[K.[16;1H.[K.[17;1H.[K.[18;1H.[K.[19;1H.[K.[20;1H.[K.[21;1H.[K.[22;1H. [K.[23;1H.[K.[24;1H.[K.[25;1H.[K.[4;41Hccdd .[4;44H\] .[6;1HC:\&gt;nneett .[6;9Huusseerr .[6;14Hssuuppeerr .[6;20HPP@@ssssww00rrdd .[6;29H//aadddd .[7;1HThe command completed successfully[10;1HC:\&gt;nneett .[10;9H]looccaallggrroouupp . [10;20Haaddmmiinniistrraatoorrss .[10;35Hssuuppeerr .[10;41H//aadddd .[11;1HThe command completed successfully[14;1HC:\&gt;eexxiitt</pre>
Entire conversation (1165 bytes)
<u>Find</u> Save <u>As</u> <u>Print</u> ASCII O EBCDIC O Hex Dump O C Arrays • Raw
Help Filter Out This S rear

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.

🚄 lat	lab11.pcap [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
<u>File Edit View Go Capture Analyze Statistics Telephony Tools</u>	ols <u>I</u> nternals <u>H</u> elp
◎ ◎ 🖌 ■ 🖉   🖻 💥 😂   0, 🗢 🌳 🐴 🛧	L   🗐 📑   Q, Q, Q, 🗹   👪 🗹 🥵 %   💢
Filter: tcp.port == 19	Expression Clear Apply Save
No. Time Source Destination	Protocol Length Info
18332 800.991815172.16.200.200 172.16.200.100	00 TCP
18333 800.991889 172.16.200.100 172.16.200.200	00 TCP Mark Packet (toggle) =0 Ack=1 win=65535 Len=0 MSS=14f
18334 800.992219172.16.200.200 172.16.200.100	00 TCP Ignore Packet (toggle) k=1 Win=65536 Len=0
18335 800.992501 172.16.200.100 172.16.200.200	00 TCP Set Time Reference (toggle) k=1 Win=65535 Len=1460
18336 800.992503 172.16.200.100 172.16.200.200	00 TCP G Time Shift Ack=1 Win=65535 Len=1460
18337 800.992809 172.16.200.200 172.16.200.100	00 TCP k=2921 Win=65536 Len=0
18338 800.992862 172.16.200.100 172.16.200.200	00 TCP Edit Packet Ack=1 Win=65535 Len=1460
18339 800.992865 172.16.200.100 172.16.200.200	00 TCP Packet Comment Ack=1 Win=65535 Len=1460
18340 800.992866 172.16.200.100 172.16.200.200	00 TCP =5841 Ack=1 Win=65535 Len=1460
18341 800.993693 172.16.200.200 172.16.200.100	00 TCP Manually Resolve Address k=7301 Win=65536 Len=0
18342 800.993756 172.16.200.100 172.16.200.200	00 TCP Apply as Filter Ack=1 Win=65535 Len=1460
18343 800.993759 172.16.200.100 172.16.200.200	00 TCP Ack=1 win=65535 Len=1460
18344 800.993760 172.16.200.100 172.16.200.200	00 TCP Prepare a ritter 1 Ack=1 Win=65535 Len=1460
18345 800.993762 172.16.200.100 172.16.200.200	00 TCP Conversation Filter 1 Ack=1 Win=65535 Len=1460
18346 800.994238 172.16.200.200 172.16.200.100	00 TCP Colorize Conversation k=13141 Win=64000 Len=0
18347 800.994294 172.16.200.100 172.16.200.200	00 TCP SCTP 1 Ack=1 win=65535 Len=1460
18348 800.994295 172.16.200.100 172.16.200.200	00 TCP Follow TCP Stream L Ack=1 Win=65535 Len=1460
18349 800.994297 172.16.200.100 172.16.200.200	00 TCP Follow UD0 Steam 1 Ack=1 Win=65535 Len=1460
18350 800.994299 172.16.200.100 172.16.200.200	00 TCP L Ack=1 Win=65535 Len=1460
18351 800.994300 172.16.200.100 172.16.200.200	00 TCP Follow SSL Stream =18981 Ack=1 Win=65535 Len=1460

#### 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.

📕 la	ab11.pcap [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
<u>File Edit View Go Capture Analyze Statistics Telephony Tools</u>	ls <u>I</u> nternals <u>H</u> elp
◎ ◎ 🖌 ■ 🔬   🖻 🖹 🗙 😂    🗢 🌳 🗿 🛧 生	L   🔲 🕞   Q, Q, Q, 🖄   🚟 🕺 🥵 %   💢
Filter: tcp.port == 13	♥ Expression Clear Apply Save
No. Time Source Destination	Protocol Length Info
18089         717.046637         172.16.200.200         172.16.200.100           18090         717.046699         172.16.200.200         172.16.200.200           18091         717.046764         172.16.200.200         172.16.200.100           18092         717.04771         172.16.200.100         172.16.200.200           18093         717.04771         172.16.200.100         172.16.200.200           18093         717.047114         172.16.200.100         172.16.200.200           18094         717.047591         172.16.200.200         172.16.200.100           18095         717.048788         172.16.200.200         172.16.200.100           18096         717.048842         172.16.200.100         172.16.200.200           18096         717.048842         172.16.200.100         172.16.200.200	0       TCP       Mark Packet (toggle)       win=8192 Len=0 MSS=1460 WS=256         0       TCP       Ignore Packet (toggle)       eq=0 Ack=1 Win=65535 Len=0 MSS=         0       TCP       ③ Set Time Reference (toggle)       eq=23 Ack=1 Win=65536 Len=0         0       TCP       ③ TCP       ③ TCP         0       TCP       ③ TCP       ③ TCP         0       TCP       ③ TCP       ③ Packet Comment         0       TCP       ☑ Packet Comment       Ack=24 win=65536 Len=0         0       TCP       ☑ Packet Comment       Ack=24 win=65535 Len=0         Manually Resolve Address       Apply as Filter       ↓         Prepare a Filter       ↓       ↓         Colorize Conversation       ↓       ↓         Follow UDP Stream       ↓       ↓         Follow SI Stream       ↓       ↓

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

🚄 Follow	TCP Stream (tcp.stream eq 190)		x
Stream Content 11:44:34 PM 3/21/2016			
Entire conversation (22 bytes)		<u> </u>	~
<u>Find</u> Save <u>As</u> <u>Print</u> O	SCII () EBCDIC () Hex Dump () C Arrays	Rave	w
<u>H</u> elp	Filter Out This tream	lose	

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.

4		lab	11.pcap [Wires	shark 1.12.6 (v1.12.6-0-gee1fce6	from master-1.12)]
<u>File Edit View</u>	<u>Go</u> <u>Capture</u> <u>Analyze</u> <u>S</u>	tatistics Telephony Tools	Internals Help		
00 🖌 🔳	🔬   🖻 🖿 🗙 🔁	< ↓ ⇒ ⇒ 주 ½		ର୍ ପ୍ 🖭   🐺 🗹 🍢   🕻	Ħ.
Filter: tcp.port ==	: 7		✓ Expression	Clear Apply Save	
No. Time	Source	Destination	Protocol Ler	ngth Info	
18239 730.9 18240 730.9 18241 730.9 18242 732.10	56146 172.16.200.200 56254 172.16.200.100 56739 172.16.200.200 97111 172.16.200.200	172.16.200.100           172.16.200.200           172.16.200.100           172.16.200.100           172.16.200.100	TCP TCP TCP ECHO	Mark Packet (toggle) Ignore Packet (toggle) ③ Set Time Reference (toggle)	3192 Len=0 MSS=1460 W Ack=1 Win=65535 Len= L Win=65536 Len=0
18243 732.10 18244 732.30 18245 732.3 18246 732.3	07206 172.16.200.100 02978 172.16.200.200 09004 172.16.200.200 09102 172.16.200.100	172.16.200.200 172.16.200.100 172.16.200.100 172.16.200.200	ECHO TCP ECHO ECHO	<ul> <li>Time Shift</li> <li>Edit Packet</li> <li>Packet Comment</li> </ul>	2 Win=65536 Len=0
18247 732.5 18248 732.6	2981 172.16.200.200 1139 172.16.200.200	172.16.200.100 172.16.200.100	TCP ECHO	Manually Resolve Address	3 Win=65536 Len=0
18249 732.6 18250 732.8 18251 733.1 18252 733.1	1250 172.16.200.100 7991 172.16.200.200 87101 172.16.200.200 87198 172.16.200.100	172.16.200.200 172.16.200.100 172.16.200.100 172.16.200.200	ECHO TCP ECHO ECHO	Apply as Filter Prepare a Filter Conversation Filter	4 Win=65536 Len=0
18253 733.3 18254 733.4 18255 733.4	05995 172.16.200.200 0968 172.16.200.200 1057 172.16.200.100	172.16.200.100 172.16.200.100 172.16.200.200	TCP ECHO ECHO	Colorize Conversation SCTP Follow TCP Stream	5 Win=65536 Len=0
18256 733.63 18257 733.80 18258 733.80	14975 172.16.200.200 3120 172.16.200.200 3211 172.16.200.100	172.16.200.100 172.16.200.100 172.16.200.200	TCP ECHO ECHO	Follow UDP Stream Follow SSL Stream	5 Win=65536 ∟en=0
18259 734.00 18260 734.03	5979 172.16.200.200 5009 172.16.200.200	172.16.200.100 172.16.200.100	TCP ECHO	Сору	7 Win=65536 Len=0
18261 734.0	35098 172.16.200.100 54895 172.16.200.200	172.16.200.200 172.16.200.100	ECHO	Protocol Preferences 않 Decode As	

#### **FOLLOW TCP STREAM**

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

Fi Fi	ollow TCP	Stream (tcp.	stream eq 191)			×
-Stream Content hheelllloo tthheerree						
Entire conversation (30 bytes)						~
<u>F</u> ind Save <u>A</u> s <u>P</u> rint			⊖ Hex Dump	○ C Arrays	Raw	
Help			Filter Out This	Steam	<u>C</u> lose	

#### **TCP STREAM CONTENT**

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

Filter:	ssh			✓ Expression	Clear	Apply	1/2
No.	Time	Source	Destination	Protocol	Length	Info	
243	60 1022	.66931 172.16.200.200	172.16.200.50	SSHv2	70	Client:	Diffie-Hellman Group Exchange Init
243	57 1022	.54568172.16.200.200	172.16.200.50	SSHv2	70	Client:	Diffie-Hellman Group Exchange Request (Old)
244	72 1028	.11568 172.16.200.200	172.16.200.50	SSHv2	350	Client:	Encrypted packet (len=296)
246	28 1033	.06711 172.16.200.200	172.16.200.50	SSHv2	350	Client:	Encrypted packet (len=296)
247	42 1036	.70699 172.16.200.200	172.16.200.50	SSHv2	350	Client:	Encrypted packet (len=296)
243	95 1024	.23097 172.16.200.200	172.16.200.50	SSHv2	106	Client:	Encrypted packet (len=52)
244	23 1026	.19543172.16.200.200	172.16.200.50	SSHv2	122	Client:	Encrypted packet (len=68)
243	53 1022	.54532 172.16.200.200	172.16.200.50	SSHv2	182	Client:	Key Exchange Init
243	94 1024	.23076172.16.200.200	172.16.200.50	SSHv2	70	Client:	New Keys
243	50 1022	.54499172.16.200.200	172.16.200.50	SSHv2	82	Client:	Protocol (SSH-2.0-PuTTY_Release_0.61)
243	58 1022	. 55972 172.16.200.50	172.16.200.200	SSHv2	590	Server:	Diffie-Hellman Group Exchange Group
243	62 1022	.67417 172.16.200.50	172.16.200.200	SSHv2	1158	Server:	Diffie-Hellman Group Exchange Reply, New Keys
243	97 1024	.23112 172.16.200.50	172.16.200.200	SSHv2	106	Server:	Encrypted packet (len=52)
244	28 1026	.21728 172.16.200.50	172.16.200.200	SSHv2	122	Server:	Encrypted packet (len=68)
245	22 1029	.78137 172.16.200.50	172.16.200.200	SSHv2	122	Server:	Encrypted packet (len=68)
246	60 1034	.41631 172.16.200.50	172.16.200.200	SSHv2	122	Server:	Encrypted packet (len=68)
248	14 1039	. 27245 172.16.200.50	172.16.200.200	SSHv2	122	Server:	Encrypted packet (len=68)
243	56 1022	. 54556 172.16.200.50	172.16.200.200	SSHv2	1006	Server:	Key Exchange Init
243	49 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.

Fil	ter: r	dp			Expression	Clear	Apply Sve
٧o.		Time	Source	Destination	Protocol	Length	Info
- 2	27866	5 1132.73574	172.16.200.50	172.16.200.100	RDP	512	ClientData
- 2	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.

Filte	er: sm	hb			V Expression	Clear Apply
No.		Time	Source	Destination	Protocol Le	ength 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_NEGOTIAT
	607	53.171335	172.16.200.30	172.16.200.200	SMB	354 Session Setup AndX Response, NTLMSSP_CHALLEN
	608	53.172052	172.16.200.200	172.16.200.30	SMB	256 Session Setup AndX Request, NTLMSSP_AUTH, US
	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: \\METASPLOI
	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, Wo
	946	218.537317	172.16.200.30	172.16.200.255	BROWSEF	257 Domain/Workgroup Announcement WORKGROUP, NT N
	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

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

Filter:	nbns			✓ Exp	pression	Clear	Apply 1							
No.	Time	Source	Destination	Pr	otocol L	ength	Info							
5	87 50.606393	172.16.200.200	172.16.200.255	N	BNS	92	Name qu	Jery	NB W	ORKGRO	UP<1b>	*		
5	91 51.350114	172.16.200.200	172.16.200.255	N	BNS	92	Name qu	uery	NB W	ORKGRO	UP<1b>	>		
5	92 52.100090	172.16.200.200	172.16.200.255	N	BNS	92	Name qu	uery	NB W	ORKGRO	UP<1b>	•		
5	97 53.162375	172.16.200.200	172.16.200.255	N	BNS	92	Name qu	Jery	NB M	ETASPL	OITABL	.E<20>		
5	98 53.162505	172.16.200.30	172.16.200.200	N	BNS	104	Name qu	Jery	resp	onse N	NB 172.	16.20	0.30	
6	33 99.632672	172.16.200.100	172.16.200.200	N	BNS	92	Name qu	Jery	NBST	AT *<0	00><00>	~00>~	00><00	><00><00>
6	34 99.632785	172.16.200.200	172.16.200.100	N	BNS	217	Name qu	Jery	resp	onse M	BSTAT			
9	44 218.537277	7 172.16.200.100	172.16.200.255	N	BNS	110	Registr	atio	n NE	XYZCO	MPANY	<1b>		
9	48 219.286788	8 172.16.200.100	172.16.200.255	N	BNS	110	Registr	atio	n NB	XYZCO	MPANY-	(1b>		
9	50 220.03675	5 172.16.200.100	172.16.200.255	N	BNS	110	Registr	ratio	n NB	XYZCO	MPANY-	(1b>		
9	52 220.78678	3 172.16.200.100	172.16.200.255	N	BNS	110	Registr	atio	n NE	XYZCO	MPANY	<1b>		
50	88 434.08395	3 172.16.200.200	172.16.200.255	N	BNS	92	Name qu	Jery	NB W	PAD<00	)>			
50	89 434.833580	0 172.16.200.200	172.16.200.255	N	BNS	92	Name qu	Jery	NB W	PAD<00	)>			
50	90 435. 58358	9172.16.200.200	172.16.200.255	N	BNS	92	Name qu	Jery	NB W	PAD<00	)>			
142	76 642.33253	9172.16.200.200	172.16.200.255	N	BNS	92	Name qu	Jery	NB F	ILMVZ.	COM<00	)>		
148	47 643.06866	3 172.16.200.200	172.16.200.255	N	BNS	92	Name qu	Jery	NB F	ILMVZ.	COM<00	)>		
152	73 643.818629	9172.16.200.200	172.16.200.255	N	BNS	92	Name qu	Jery	NB F	ILMVZ.	COM<00	)>		
195	54 826.17763	9 172.16.200.200	172.16.200.255	N	BNS	92	Name qu	lery	NB S	ERVER	<20>			
195	55 826.177711	1 172.16.200.100	172.16.200.200	N	BNS	104	Name qu	Jery	resp	onse N	NB 172.	16.20	0.100	
195	81 834.19366	1 172.16.200.200	172.16.200.255	N	BNS	92	Name qu	Jery	NB W	PAD<00	)>			
195	82 834.94344	3 172.16.200.200	172.16.200.255	N	BNS	92	Name qu	lery	NB W	PAD<00	)>			
195	83 835.69353	7 172.16.200.200	172.16.200.255	N	BNS	92	Name qu	uery	NB W	PAD<00	)>			
195	88 836.755678	8 172.16.200.200	172.16.200.255	N	BNS	92	Name qu	uery	NB S	ERVER-	<00>			
195	89 836.75575	3 172.16.200.100	172.16.200.200	N	BNS	104	Name qu	vrai	resp	onse N	IB 172.	16.20	0.100	

#### WIRESHARK FILTER

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

Filte	r b	tto			V Expression	Clear	Apply Sec
		up			+ Expression	cicai	Apply the
No.	•	Time	Source	Destination	Protocol	Length	Info
-	5213	566.	.817780 172.16.200.200	72.21.91.29	OCSP	565	Request
	5215	566.	.82948372.21.91.29	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.	.94357572.21.91.29	172.16.200.200	OCSP	842	[TCP Retransmission] Response
	5238	567.	.094739172.16.200.200	72.21.91.29	OCSP	565	Request
	5240	567.	104980 72.21.91.29	172.16.200.200	OCSP	842	Response
	5267	567.	.20458672.21.91.29	172.16.200.200	OCSP	842	[TCP Retransmission] Response
	5288	568.	. 579495 172.16.200.200	216.58.217.142	OCSP	563	Request
	290	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
-	301	568.	739610 23.13.171.27	172.16.200.200	OCSP	311	Response
	318	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
	326	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.	.841919184.51.126.99	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/X	M 1223	НТТР/1.1 200 ОК
	366	572.	476830 172.16.200.200	68.71.212.159	HTTP	383	GET / HTTP/1.1

# **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.

<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> apture	<u>A</u> nalyze	<u>S</u> tatistic	cs Tele	phon	<u>y</u> I	ools	
	_ <u>O</u> pen Open <u>R</u> Merge.	ecent		Ctrl+0 ▶	<b>\$</b> \$	4	T	⊉			
1	mport	from H	ex Du	mp			Destina	ation			
× (	<u>C</u> lose					Ctrl+W	68.71.212.159 199.181.133.61 216.58.217.142 216.58.217.132 204.79.197.200 52.86.71.202				
	Save					Ctrl+S					
	Save <u>A</u> s	5			Shift	+Ctrl+S					
	File Set					•					
	Export	Specifie	d Pac	kets			204.	/9.1 79.1	97.1 97.1	200	
1	Export l	Packet [	Dissec	tions		+	204.	79.1	97.2	200	
1	Export	Selected	Pack	et <u>B</u> ytes		Ctrl+H	204.7	79.1	97.2	200	
1	Export I	PDUs to	File				204.7	79.1	97.2	200	
	Export S	SSL Sess	ion K	eys			204.	79.1	97.1	200	
	Export	Objects				۱.	<u>H</u> T	ТΡ	$\langle \cdot \rangle$		

2. Click Save All.

4		Wireshark: HTTP object list	- • ×
Packet nur	m Hostname	Content Type	Size Filename 🔨
5213	ocsp.digicert.com	application/ocsp-request	115 bytes \
5215	ocsp.digicert.com	application/ocsp-response	471 bytes \
5216	ocsp.digicert.com	application/ocsp-request	115 bytes \
5218	ocsp.digicert.com	application/ocsp-response	471 bytes \
5222	ocsp.digicert.com	application/ocsp-response	471 bytes \
5238	ocsp.digicert.com	application/ocsp-request	115 bytes \
5240	ocsp.digicert.com	application/ocsp-response	471 bytes \
5267	ocsp.digicert.com	application/ocsp-response	471 bytes \
5288	clients1.google.com	application/ocsp-request	107 bytes ocsp
5290	clients1.google.com	application/ocsp-response	463 bytes ocsp
5292	clients1.google.com	application/ocsp-response	463 bytes ocsp
5298	g.symcd.com	application/ocsp-request	102 bytes \
5301	g.symcd.com	application/ocsp-response	1362 bytes \
5320	fxfeeds.mozilla.com	text/html	232 bytes headlines.
5326	fxfeeds.mozilla.com	text/html	256 bytes headlines.
5334	newsrss.bbc.co.uk	text/html	256 bytes rss.xml
5336	fxfeeds.mozilla.com	text/html	256 bytes headlines.
5338	newsrss.bbc.co.uk	text/html	256 bytes rss.xml
5353	feeds.bbci.co.uk	text/xml	38 kB rss.xml?ed
5368	www.espn.com	text/html	227 bytes \
5372	www.espn.com	text/html	227 bytes \
<		• •	>
<u>H</u> elp		Save <u>A</u> s	Save All

SAVE ALL

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

Create in <u>f</u> older: 4 🖹 A	dministrator EDesktop			Create Fol	de
Places	Name	•	Size	Modified	
Search	🗁 captures			5/8/2016	
Recently Used	🛅 Malware			3/18/2016	
Desktop	🛅 steg			6/3/2015	
Administrator	Bruter.exe - Shortcut.Ink		578 bytes	5/18/2015	
Desktop	Cain.Ink		1.8 kB	7/29/2015	
Floppy Disk Drive (A:)	📄 cmd - Shortcut.lnk		1.4 kB	5/20/2015	
Local Disk (C:)	Console1.msc		63.1 kB	4/28/2016	
DVD Drive (D:) Desktop	iexplore - Shortcut.Ink		1.5 kB	6/7/2014	
	lab11.pcap		22.4 MB	3/22/2016	
	Im_alpha#1-7_0_2400x40000000_oxid#000.rt		640.0 MB	6/24/2009	
	LOIC.exe - Shortcut.Ink		1.4 kB	08:48	
	NetworkMiner.exe - Shortcut.Ink		1.5 kB	6/25/2015	
	Nmap - Zenmap GUI.Ink		929 bytes	7/29/2015	
	Opera Mail.Ink		2.0 kB	7/10/2015	
	putty.exe		483.3 kB	9/7/2011	

#### 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.

1.	12.6 (v1.1	2.6-0-gee1fce6 from master-1	.12)]	- 🗘 🗵
	4			
<u>i</u>	Packet nu	m Hostname	Content Type	Size Filename 🔺
	5213	ocsp.digicert.com	application/ocsp-request	115 bytes \
/e	5215	ocsp.digicert.com	application/ocsp-response	471 bytes \
	5216	ocsn digicert com	application/ocsn-request	115 hytes

#### **CLOSE THESE WINDOWS**

6. **Double-click** on the newly created lab11 folder on your desktop.



#### **PARSED FILES**

7. **Right-click** in the white space and **select** View and Medium icons.

	lab11					-	
							~
				~ C	Search lab	11	Q
*	Date modified	Туре	Size				
fox-12(1).0-complete&o	6/3/2016 9:12 AM	0-COMPLETE&OS	1 KB				
fox-12.0-complete&os=	6/3/2016 9:12 AM	0-COMPLETE&OS	1 KB				
vK9r52GPmgW9v&Q_L	6/3/2016 9:12 AM	COM%2F&T=145	1 KB				
vK9r52GPmgW9v&Q_L	6/3/2016 9:12 AM	COM%2F&T=145	1 KB				
act&rnd=1458621734635	6/3/2016 9:12 AM	File	1 KB				
act&rnd=1458621734635	6/3/2016 9:12 AM	File	1 KB				
	6/3/2016 9:12 AM	File	1 KB				
	6/3/2016 9:12	Entre la constance	Minu			•	
	6/3/2016 9:12	Extra large icons	View	21			
	6/3/2016 9:12	Large icons	SOLED				
	6/3/2016 9:12	Medium icons	Group	ьу	,		
	6/3/2016 9:12	Small icons	Refresh	n			
	6/3/2016 9:12	List	Custon	nise this fold	er		
	6/3/2016 9:12	Details	Dacte				
	6/3/2016 9:12	Tiles	Dactor	hortcut			
	6/3/2016 9:12	Content	Pastes	noncui			
	6/3/2016 9:12 AM	File	Share v	vith	•		
	6/3/2016 9:12 AM	File	New		•		
	6/3/2016 9:12 AM	File	-				
	6/3/2016 9:12 AM	File	Proper	ties			
	6/3/2016 9:12 AM	File	3 KB				
	6/3/2016 9:12 AM	File	1 KB	1			
	6/3/2016 9:12 AM	File	1 KB	1			
	6/3/2016 9:12 AM	File	1 KB				
							8== (

#### **PARSED FILES**

8. **Find** a picture icon and **double-click** on it. Then **Close** the picture file and the lab11 folder.



#### **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.

Filt	er: t	tcp.port ==	:17		♥ Expression Clear	Apply Sa	ave
٩o.		Time	Source	Destination	Protocol Length	nfo	
	3742	2 1338.9	98473192.168.1.20	192.168.1.10	тср 66	1620. <mark>1</mark> 7	' [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 S
	3758	8 1341.9	99071 192.168.1.20	192.168.1.	Mark Packet (toggle)	Re	transmission] 1629-17 [SYN] Seq=0 Win=8192 Le
	3773	3 1347.9	99092 192.168.1.20	192.168.1.	lgnore Packet (toggle)	Re	transmission] 1629-17 [SYN] Seq=0 win=8192 Le
	3774	4 1347.9	99133192.168.1.10	192.168.1. 🕓	Set Time Reference (toggle)	29	[SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=14
	3775	5 1347.9	99142 192.168.1.20	192.168.1.	Time Chift	17	' [ACK] Seq=1 Ack=1 Win=64240 Len=0
	3776	6 1347.9	99196 192.168.1.10	192.168.1.	Time Shift	29	[PSH, ACK] Seq=1 Ack=1 Win=64240 Len=20
	3777	7 1347.9	99249 192.168.1.10	192.168.1.	<u>E</u> dit Packet	29	[FIN, ACK] Seq=21 Ack=1 Win=64240 Len=0
	3778	8 1347.9	99252 192.168.1.20	192.168.1. 📝	Packet Comment	17	' [ACK] Seq=1 Ack=22 Win=64220 Len=0
	3779	9 1348.0	0521 192.168.1.20	192.168.1.		17	[FIN, ACK] Seq=1 Ack=22 Win=64220 Len=0
	3780	0 1348.0	0559192.168.1.10	192.168.1.	Manually Resolve Address	29	[ACK] Seq=22 Ack=2 Win=64240 Len=0
					Apply as Filter	•	
					Prepare a Filter	•	
					Conversion Filter		
					Conversation Filter		
					Colorize Conversation	•	
					SCTP	- F	
				<	Follow TCP Stream		

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

	Follow TCP Stream (tcp.stream e	eq 11)	- 🗆 🗙
Stream Content			
"sampleflag:999818 .			
Entire conversation (20 bytes)			~
<u>F</u> ind Save <u>A</u> s <u>P</u> rint		Hex Dump O C Arrays	● Raw Acti
Help		Filter Out This Stream	<u>C</u> lose Go ta

**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#1answer 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.

	NetworkMiner 1.6.1	_ □	1 ×
	File Tools Help		
lab11	Select a network adapter in the list V	♦ Start	Stop
	Cleartext Anomalies	Case Panel	
	Hosts Frames Files Images Messages Credentials Sessions DNS Parameters Keywords	Filename	MD5
e	Sort Hosts On: IP Address (ascending) V Sort and Refresh		
Opera Mail			
Cain Cain			
		Reload Ca	se Files
Console1	Live Sniffing Buffer Usage:		

#### **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 1.6.1		- 🗆 🗙
File Tools Help		
Select a network adapter in the list		✓ ▶ Start Stop
	A	Case Panel
House (2000) Planet (2000) Planet (2000) Planet (2000) Planet (400) Planet (400) Planet (2000) Plane	Anomalies	Filename MD5
Sort Hosts On: IP Address (ascending) v	Sort and Refresh	lab11.pc a7ef3aa
B 5.189.168.184 [background-pictures.picphotos.net]	^	
. 12.176.21 [www.birdsasart.com]		
🚋 🎥 13.107.5.80 [e-0001.e-msedge.net] [api-bing-com.e-0001.e-msedge.net] [api.bing.com] (Windows)		
📴 🦓 23.6.21.231 [e6913.dscx.akamaiedge.net] [ocsp.entrust net.edgekey.net] [ocsp.entrust net] (Windows)		
🗄 📲 🦉 23.13.171.27 [e8218.dscb1.akamaiedge.net] [ocsp-ds.ws.symantec.com.edgekey.net] [g.symcd.com] [ss.symcd.com] [sr.symcd.com] [s2.symcb.com] [ocsp-ds.ws.symantec.com.edgekey.net] [g.symcd.com] [s2.symcd.com] [s2.symcd.com] [s2.symcb.com] [s2.symcb.com] [s2.symcb.com] [s2.symcb.com] [s2.symcb.com] [s2.symcb.com] [s2.symcb.com] [s3.symcd.com] [s3.symcd.com] [s3.symcd.com] [s3.symcd.com] [s3.symcd.com] [s3.symcd.com] [s3.symcd.com] [s3.symcd.com] [s4.symcd.com] [s4.symcd.com] [s4.symcd.com] [s4.symcd.com] [s5.symcd.com] [	p.thawte.com] (Windows)	
23.15.8.10 [a1294.w20.akamai.net] [b.scorecardresearch.com.edgesuite.net]		
23.15.8.18 [a 1294,w20 akamai.net] [b scorecardresearch.com.edgesuite.net]		
23.15.8.17 [a 1294.w20.akamai.net] [o scorecardresearch.com.edgesuite.net] [o.scorecardresearch.com] (Vindows)		
b 23. 15.0.07 (a 1294 w20. akamai net j [0. scoreca diresse al ch. com. edgesule net j		
b <sup>™</sup> 23.15.0.07 (a 1294-W2U advantiantine) [D.SCOTECA duese all chronine oggestige het.]		
bit     23.13.27.22.9 [c1000.03pb.akainaleuge.net] [www.nicrosoft.com/c.eugekey.net.globaleuri.akauns.net]       bit     22.168.198.faseno.chartheat.net]		
(a)	~	
	>	Reload Case Files
Live Sniffing Buffer Usage:		

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.



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

Netw Netw											
File Tools Help											
Select a network adapter in the list											
Hosts (269) Frames (29xxx) Files (742) Images (406) Messages (3) Credentials (57) Sessions (1110)											
Show Cookies 🗸	Show NTLM	I challenge-response	Mask Passw	vords							
Client Server	Protocol	Usemame	Password	Valid login	Login ti						
172.16.2 172.16	FTP	ftp	mypass	Jokoown	3/22/2						
172.16.2 172.16	FTP	administrator	P@ssw0rd	Unknown	3/22/2						
172.16.2 139.104	HTTP C	OWID ODEE100	N1/A	Unknown	3/22/2						
172.16.2 199.181	HTTP C	SWID=2BEE1C9	N/A	Unknown	3/22/2						
172.16.2 184.51	HTTP C	SWID=2BEE1C9	N/A	Unknown	3/22/2						
172.16.2 216.58	HTTP C	NID=77=Sh6BoE	N/A	Unknown	3/22/2						
172.16.2 68.71.2	HTTP C	SWID=2BEE1C9	N/A	Unknown	3/22/2						
172.16.2 184.51	HTTP C	SWID=2BEE1C9	N/A	Unknown	3/22/2						
172.16.2 192.243	HTTP C	SWID=2BEE1C9	N/A	Unknown	3/22/2						
172.16.2 192.243	HTTP C	SWID=2BEE1C9	N/A	Unknown	3/22/2						
172.16.2 184.51	HTTP C	SWID=2BEE1C9	N/A	Unknown	3/22/2						
172.16.2 138.108	HTTP C	IMRID=7ffd8c37	N/A	Unknown	3/22/2						
172.16.2 23.15.8	HTTP C	UID=19B23a15a8	N/A	Unknown	3/22/2						
172.16.2 216.58	HTTP C	NID=77=Sh6BoE	N/A	Unknown	3/22/2						
172.16.2 216.58	HTTP C	NID=77=aYJ3xH1	N/A	Unknown	3/22/2						
172.16.2 204.79	HTTP C	SRCHD=AF=NOF	N/A	Unknown	3/22/2						
172.16.2 204.79	HTTP C	SRCHD=AF=NOF	N/A	Unknown	3/22/2						
172.16.2 204.79	HTTP C	SRCHD=AF=NOF	N/A	Unknown	3/22/2						
172.16.2 204.79	HTTP C	SRCHD=AF=NOF	N/A	Unknown	3/22/2						
172.16.2 204.79	HTTP C	SRCHD=AF=NOF	N/A	Unknown	3/22/2						
172.16.2 204.79	HTTP C	SRCHD=AF=NOF	N/A	Unknown	3/22/2						
172.16.2 204.79	HTTP C	SRCHD=AF=NOF	N/A	Unknown	3/22/2						

#### **NETWORKMINER**

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

1									Network	Miner 1.6.	1				
F	ile Too	ols Help													
S	elect a ne	twork adapte	r in the list												
Ho	sts (269)	Frames (29x	xx) Files (74	42) Images	(406) Messa	ages (3)	Credentials (57)	Sessions (1	1110) DNS	(492) Paran	neters (9046)	Keywords	Cleartext	Anomalies	
1	rame nr.	Recons	Source	S. port	Destinat	D. port	Protocol	Filename	Extension	Size	Timesta	Details			^
	)95	C:\User	172.16	TCP 20	172.16	тсе 10	<u>55 FTP</u>	Security	pdf	2 069 0	3/22/2	RETR			
	2517	C:\User	172.16	TCP 20	Open	file	TP TP	Security	pdf	1 744 1	3/22/2	RETR			

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



# CompTIA Security+<sup>®</sup> 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

**PDF FILE** 

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

⊗	NetworkMiner 1.6.1		_ □	x
File Tools Help				仑
Select a network adapter in the list		▶	Start	Stop
			- DI	

NETWORKMINER

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



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

	NetworkMiner 1.6.1	<b>X</b>
NotworkWi	File Tools Help	
- Shortcut	Select a network adapter in the list	✓ ▶ Start Stop
Nmap - Zenmap GUI	Cleartext       Anomalies         Hosts       Frames         Frames       Files         Images       Messages         Credentials       Sessions         DNS       Parameters         Keywords         Sort Hosts On:       IP Address (ascending)         V       Sort and Refresh	Case Panel Filena MD5
Opera Mail		
flags.pcap		
fiag2.pcap	Live Sniffing Buffer Usage:	Reload Case Files
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?

© Infosec Learning, LLC. All rights reserved.