Laboratorium - Używanie programu Wireshark do obserwacji mechanizmu uzgodnienia trójetapowego TCP

Topologia



Cele

Część 1: Przygotowanie Wireshark do przechwytywania pakietów

• Wybór odpowiedniego interfejsu karty sieciowej do przechwytywania pakietów.

Część 2: Przechwytywanie, lokalizowanie i badanie pakietów

- Przechwytywanie sesji internetowej dla adresu www.google.com.
- Znajdowanie odpowiednich pakietów dla sesji internetowej.
- Sprawdzanie informacji zawartych w pakietach: adresy IP, numery portów TCP oraz flagi TCP.

Scenariusz

W tym laboratorium używany jest program Wireshark w celu przechwytywania i sprawdzania pakietów generowanych pomiędzy przeglądarką PC używającą protokołu HyperText Transfer Protocol (HTTP) i serwerem www, takim jak www.google.com. Jeżeli aplikacja, taka jak HTTP lub File Transfer Protocol (FTP) zostanie uruchomiona, to protokół TCP użyje mechanizmu uzgodnienia trójetapowego w celu ustanowienia wiarygodnej sesji TCP pomiędzy dwoma hostami. Na przykład, gdy komputer korzysta z przeglądarki internetowej, aby przeglądać Internet, uzgadnianie trójetapowe jest inicjowane i sesja jest ustalona pomiędzy hostem PC i serwerem WWW. Komputer PC może obsługiwać wiele równoczesnych aktywnych sesji TCP do różnych stron internetowych.

Uwaga: To ćwiczenie nie może być przeprowadzone przy użyciu środowiska Netlab. To ćwiczenie zakłada, że masz dostęp do Internetu.

Wymagane wyposażenie

1 PC (Windows 7, Vista, lub XP z dostępem do wiersza poleceń, dostępem do Internetu i zainstalowanym programem Wireshark)

Część 1. Przygotowanie Wireshark do przechwytywania pakietów

W części 1 należy uruchomić program Wireshark i wybrać odpowiedni interfejs, aby rozpocząć przechwytywanie pakietów.

Krok 1. Pobieranie adresów interfejsu PC.

W tym laboratorium, musisz znać adres IP twojego komputera oraz adres fizyczny karty sieciowej(NIC), nazywany adresem MAC.

a. W oknie poleceń wpisz ipconfig /all i naciśnij Enter.

Physical Address.						=	C8-0A-A9-FA-DE-0D
DHCP Enabled						:	Yes
Autoconfiguration 1	Enab	ble	:d			-	Yes
IPv4 Address						=	192.168.1.130(Preferred)
Subnet Mask						=	255.255.255.0
Lease Obtained						=	Saturday, December 01, 2012 1:43:35 PM
Lease Expires						=	Sunday, December 02, 2012 1:43:35 PM
Default Gateway						=	192.168.1.1
DHCP Server			-	-	-	=	192.168.1.1
DNS Servers						=	192.168.1.1
NetBIOS over Tcpip.						:	Enabled

b. Zapisz adres IP i adres MAC dla wybranej karty Ethernet, ponieważ te adresy źródłowy będą używane do przechwytywania pakietów.

Adres hosta PC:	
Adres MAC dla hosta:	

Krok 2. Uruchom program Wireshark i wybierz odpowiedni interfejs.

- a. Kliknij przycisk Windows Start i rozwiń menu za pomocą podwójnego kliknięcia Wireshark.
- b. Po uruchomieniu Wireshark kliknij Interface List.

The Wireshark Network Analyzer [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)] Elle Edit Virew Go Capture Analyze Statistics Telephony Iools Internals	Help Dia a a minar og ør wing	
Filter:	sion Clear Apply Save	
WIRESHARK The World's Most Popular Netwo Version 1.8.3 (SVN Rev 45256 from /trunk-	rk Protocol Analyzer L®	
Capture	Files	Online
Interface List Use is of the capture interfaces Image: Start Choose one or more interfaces to capture from, then Start Sur: Ubwice: NUPF_(IDECG325-FF46-4822-BC18-9636F4946680) Image: Ima	 Per a previously captured fite Cpen Recent: Parallel Captures Arch assortment of example capture files on the wild 	Website Via the property website Via the Wreehark as securely as possible
Ready to load or capture	No Packets	Profile: Default

c. W oknie **Wireshark: Capture Interfaces** kliknij opcję (zaznacz ją) odpowiadającą Twojemu interfejsowi podłączonego do sieci LAN.

Wireshark: Capture Interfaces										
	Description	IP	Packets	Packets/s						
	Intel(R) PRO/1000 MT Network Connection		19	0	<u>D</u> etails					
	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	Details					
<u>H</u> elp		Start	Stop	<u>O</u> ptions	<u>C</u> lose					

Uwaga: W przypadku wielu interfejsów gdy nie masz pewności, który interfejs sprawdzić, to kliknij przycisk **Details**. Kliknij zakładkę **802.3 (Ethernet)** i sprawdź czy adres MAC zgadza się z adresem zapisanym w kroku 1b. Zamknij okno Interface Details.

Część 2. Przechwytywanie, lokalizowanie i badanie pakietów

Krok 1. Kliknij przycisk Start aby rozpocząć przechwytywanie.

a. Wybierz www.google.com Zminimalizuj okno przeglądarki i wróć do Wireshark. Zatrzymaj proces przechwytywania. Powinieneś zobaczyć przechwycony ruch podobny do tego poniżej w kroku b.

Uwaga: Twój instruktor może podać Ci inną stronę. Jeżeli tak, to wpisz nazwę lub adres strony tutaj:

<u>File</u> Edit <u>V</u> iew <u>G</u>	o <u>C</u> apture <u>A</u> nalyze <u>S</u> ta	itistics Telephon <u>y T</u> ool	s <u>I</u> nternals <u>H</u> elp	
	(E 🔲 🗙 😂 占) 🔍 🗢 🛸 🍛 7		0,0,0,11 🖼 🗹 畅 % 💢
Filter:			 Expression 	Clear Apply Save
Time	Source	Destination	Protocol Length	Info
1 0.00000000	192.168.1.130	157.55.130.157	тср 54	49166 > 40013 [ACK] Seq=1 Ack=1 Win=255 Len=0
2 0.033696000	157.55.130.157	192.168.1.130	тср 144	40013 > 49166 [PSH, ACK] Seq=1 Ack=1 Win=83 Len=9
3 0.034064000	192.168.1.130	157.55.130.157	TCP 58	3 49166 > 40013 [PSH, ACK] Seq=1 Ack=91 Win=255 Len
4 0.069409000	157.55.130.157	192.168.1.130	TCP 60)40013 > 49166 [ACK] Seq=91 Ack=5 Win=83 Len=0
5 0.069469000	192.168.1.130	157.55.130.157	TCP 66	549166 > 40013 [PSH, ACK] Seq=5 Ack=91 Win=255 Len
6 0.120203000	157.55.130.157	192.168.1.130	TCP 60) 40013 > 49166 [АСК] Seq=91 Ack=17 Win=83 Len=0
7 0.120559000	157.55.130.157	192.168.1.130	TCP 60)40013 > 49166 [P5H, ACK] Seq=91 Ack=17 Win=83 Len
8 0.327738000	192.168.1.130	157.55.130.157	тср 54	49166 > 40013 [ACK] Seq=17 Ack=95 Win=255 Len=0
9 0.360199000	157.55.130.157	192.168.1.130	тср 326	540013 > 49166 [P5H, ACK] 5eq=95 Ack=17 Win=83 Len
10 0.561615000	192.168.1.130	157.55.130.157	тср 54	49166 > 40013 [ACK] Seq=17 Ack=367 Win=254 Len=0
11 1.140459000	192.168.1.130	192.168.1.1	DNS 74	Standard query Oxded2 A www.google.com
12 1.155247000	192.168.1.1	192.168.1.130	DNS 154	Standard query response 0xded2 A 74.125.225.209
13 1.232568000	192.168.1.130	172.17.0.254	SNMP 119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.
14 1.576595000	192.168.1.130	74.125.225.209	TCP 66	5 49522 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460
15 1.576754000	192.168.1.130	74.125.225.209	TCP 66	549523 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460
16 1.611218000	74.125.225.209	192.168.1.130	тср 66	5 http > 49523 [SYN, ACK] Seq=0 Ack=1 Win=14300 Len
17 1.611293000	192.168.1.130	74.125.225.209	тср 54	49523 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
18 1.611553000	74.125.225.209	192.168.1.130	TCP 66	6 http > 49522 [SYN, ACK] Seq=0 Ack=1 Win=14300 Len
•		III		•
⊕ Frame 4: 60 k	oytes on wire (480	bits), 60 bytes c	aptured (480 k	oits) on interface 0
∃ Ethernet II.	Src: Cisco-Li_f6:8	34:6e (58:6d:8f:f6	:84:6e), Dst:	QuantaCo_fa:de:Od (c8:0a:a9:fa:de:Od)
Internet Prot	tocol Version 4, Sr	c: 157.55.130.157	(157.55.130.1	L57), Dst: 192.168.1.130 (192.168.1.130)
Transmission	Control Protocol,	Src Port: 40013 (4	40013), Dst Po	ort: 49166 (49166), Seq: 91, Ack: 5, Len: 0

b. Mając aktywne okno Capture, znajdź kolumny: Source, Destination, Protocol.

Krok 2. Znajdź odpowiednie pakiety dla sesji internetowej.

Jeżeli komputer został dopiero dołączony do sieci i nie było żadnej jego aktywności dotyczącej dostępu do Internetu, to możesz zobaczyć cały proces przechwytywanych komunikatów: Address Resolution Protocol (ARP),Domain Name System (DNS) i uzgadnianie 3-etapowe TCP. Ekran przechwytywania w kroku 1 w części 2 pokazuje wszystkie pakiety wymagane, aby komputer musiał pobrać stronę www.google.com. W tym przypadku komputer PC ma już wpis w tabeli ARP dla bramy domyślnej; w związku z tym, komputer żąda odwzorowania adresu DNS www.google.com.

Laboratorium - Używanie programu Wireshark do obserwacji mechanizmu uzgodnienia trójetapowego TCP

a. Ramka 11 przedstawia zapytanie DNS z komputera do serwera DNS, próbując odwzorować nazwę domeny www.google.com na adres IP serwera www. Komputer musi mieć adres IP, zanim wyśle pierwszy pakiet do serwera www.

Jaki jest adres IP serwera DNS?

- b. Ramka 12 to odpowiedź z serwera DNS (zawiera adres IP strony www.google.com).
- c. Znajdź odpowiedni pakiet w początkowej fazie procesu uzgadniania trójetapowego. W tym przykładzie ramka 15 jest początkiem procesu uzgadniania trójetapowego TCP.

Jaki jest adres serwera Google?_

d. Jeżeli masz dużo pakietów, które nie są powiązane z sesją TCP to może być konieczne aby użyć opcji filtrowania. W programie Wireshark wpisz **tcp** w obszarze filtru i naciśnij Enter.

Eile	<u>E</u> dit	<u>V</u> iew	<u> </u>	<u>Capture</u>	<u>A</u> nalyze	Statistics	: Telephon	<u>y T</u> ools	Internals	<u>H</u> elp							
	Ц.				X 🔁	8 0	ζ 🗢 🔿	4) 🖗	1	₽ ⊕	⊖ 10	T è	¥ 🗹	8 %	Ø		
Fi	er: tc	p							Express	ion Clea	r Apply	Save					
No.				Source		Destinat	ion	Protoco	ol Length	Info							
	1 0.	00000	0000	192.16	8.1.130	157.5	5.130.15	7 ТСР	5	49166	> 40013	[ACK]	Seq=	1 Ack=1	. Win=2	55 Len=	0
	2 0.	03369	6000	157.55	.130.15	7 192.1	68.1.130	TCP	14	4 40013	> 49166	5 [PSH,	ACK]	Seq=1	Ack=1	Win=83	Len=90
	30.	03406	64000	192.16	8.1.130	157.5	5.130.15	7 ТСР	5	8 49166	> 40013	B [PSH,	ACK]	Seq=1	Ack=91	. Win=25	5 Len=4
	4 0.	06940	9000	157.55	.130.15	7 192.1	68.1.130	TCP	6	0 40013	> 49166	5 [ACK]	Seq=	91 Ack=	∶5 Win=	83 Len=	0
	50.	06946	9000	192.16	8.1.130	157.5	5.130.15	7 ТСР	6	5 49166	> 40013	B [PSH,	ACK]	Seq=5	Ack=91	. Win=25	5 Len=12
	60.	12020	3000	157.55	.130.15	7 192.1	68.1.130	TCP	6	0 40013	> 49166	5 [ACK]	Seq=	91 Ack=	∶17 Win	=83 Len	=0
	7 0.	12055	9000	157.55	.130.15	7 192.1	68.1.130	TCP	6	0 40013	> 49166	5 [PSH,	ACK]	Seq=91	. Ack=1	7 Win=8	3 Len=4
	80.	32773	8000	192.16	8.1.130	157.5	5.130.15	7 ТСР	54	49166	> 40013] [ACK]	Seq=	17 Ack=	⊧95 Win	1=255 Lei	n=0
	90.	36019	9000	157.55	.130.15	7 192.1	68.1.130	TCP	32	5 40013	> 49166	5 [PSH,	ACK]	Seq=95	i Ack=1	7 Win=8	3 Len=272
	10 0.	56161	5000	192.16	8.1.130	157.5	5.130.15	7 ТСР	54	4 49166	> 40013	3 [ACK]	Seq=	17 Ack=	=367 Wi	n=254 L	en=0
	14 1.	57659	5000	192.16	8.1.130	74.12	5.225.20	9 ТСР	6	5 49522	> http	[SYN]	Seq=0	Win=81	.92 Len	=0 MSS=	1460 W5=4 S
	151.	57675	4000	192.16	8.1.130	74.12	5.225.20	9 ТСР	6	5 49523	> http	[SYN]	Seq=0	Win=81	.92 Len	=0 MSS=	1460 WS=4 S
1	161.	61121	8000	74.125	.225.20	9 192.1	68.1.130	TCP	6	5 http >	49523	[SYN,	ACK] :	5eq=0 A	∖ck=1 W	in=1430	0 Len=0 MSS
	171.	61129	3000	192.16	8.1.130	74.12	5.225.20	9 ТСР	5	49523	> http	[ACK]	Seq=1	Ack=1	Win=65	780 Len	=0
	181.	61155	3000	74.125	.225.20	9 192.1	68.1.130	TCP	6	5 http >	49522	[SYN,	ACK]	5eq=0 A	∖ck=1 W	in=1430	0 Len=0 MSS
	191.	61161	4000	192.16	8.1.130	74.12	5.225.20	9 ТСР	5	49522	> http	[ACK]	Seq=1	Ack=1	Win=65	780 Len	=0
	201.	61364	6000	192.16	8.1.130	74.12	5.225.20	9 HTTP	61	GET /	НТТР/1.	1					
	21 1.	65166	2000	74.125	.225.20	9 192.1	68.1.130	TCP	6) http >	49523	[ACK]	Seq=1	Ack=56	6 Win=	15488 L	en=0
۰.									III								
+	Frame	4: 6	i0 by	tes on	wire (4	80 bits	s), 60 by	tes cap	otured (4	80 bits)	on in	terfac	e 0				
+ [Ether	net I	II, S	rc: Cis	co-Li_f	6:84:66	e (58:6d:	8f:f6:8	84:6e), D	st: Quar	taCo_fa	a:de:0	d (c8:	0a:a9:1	Fa:de:0)d)	
+ :	Inter	net F	roto	col Ver	sion 4,	Src: 1	157.55.13	0.157 ((157.55.1	30.157),	Dst: 1	192.16	8.1.13	0 (192.	.168.1.	130)	
+	Frans	missi	ion c	ontrol	Protoco	l, src	Port: 40	013 (40	0013), Ds	t Port:	49166	(49166)), Seq	: 91, /	Ack: 5,	Len: 0	

Krok 3. Sprawdź informacje zawarte w pakietach: adresy IP, numery portów TCP oraz flagi TCP.

- a. W tym przykładzie ramka 15 jest początkiem procesu uzgadniania trójetapowego pomiędzy komputerem PC i serwerem Google. W panelu listy pakietów (górna część okna głównego), zaznacz ramkę. Po zaznaczeniu linii pokażą się dodatkowe zdekodowane informacje o zawartości pakietu w dwóch dolnych panelach. Sprawdź informacje dotyczące TCP w okienku szczegółów pakietu (środkowa część okna głównego).
- b. W panelu dotyczącym szczegółów pakietu kliknij ikonę + znajdującą się po lewej stronie pozycji Transmission Control Protocol aby rozwinąć informacje o TCP.
- c. Kliknij ikonę + znajdującą się po lewej stronie słowa Flags. Przeczytaj numery portów źródłowych i docelowych oraz flagi, które są ustawione.

Uwaga: Możesz dostosować rozmiary oraz położenie okien programu Wireshark tak aby wyświetlać potrzebne informacje.

le Edit View Go	Canture Analyze Statistics	Telephony Tools Inter	nals Heln								
it ind ind ind ind						× 188					
			Evoression Cle	ar Apply Save		v					
Time	Source	Dectination	Protocol Le	nath Info							
10 0.5616150	000 192.168.1.130	157.55.130.157	TCP	54 49166 > 4	0013 [AC	(] Seq=17 A	ck=367 Win=	254 Len=0			
14 1.5/65950	000 192.168.1.130 000 192.168.1.130	74.125.225.209	TCP	66 49522 > h 66 49523 > h	ttp [SYN] ttp [SYN]	Seq=0 Win Seq=0 Win	=8192 Len=0 =8192 Len=0	MSS=1460 WS=4 MSS=1460 WS=4	SACK_PERM SACK_PERM SACK_PERM	1=1	
16 1.6112180	000 74.125.225.209	192.168.1.130	TCP	66 http > 49	523 [SYN	ACK] Seq=	0 Ack=1 Win	=14300 Len=0 M	455=1430 SA	ACK_PERM=1 WS=	•64
18 1.6112930	000 192.168.1.130 000 74.125.225.209	74.125.225.209 192.168.1.130	TCP	54 49523 > r 66 http > 49	522 [SYN	ACK] Seq=1	=1 W1N=65/8 0 Ack=1 Win	0 Len=0 ≔14300 Len=0 M	455=1430 SA	ACK_PERM=1 WS=	=64
						· · · · ·					Þ
Fransmission Co	ontrol Protocol. Src F	Port: 49523 (49523)	. Dst Port:	http (80), 50	a: 0, Le	n: 0	,				
Source port:	49523 (49523)		,								
Destination p	port: http (80) x: 2]										
Sequence numb	ber: 0 (relative se	equence number)									
Header length	h: 32 bytes (SYN)										
000	= Reserved: Not s	et									
0	= Nonce: Not set	low Roducod (CWR):	Not set								
	= ECN-Echo: Not s	iet	NOU SEL								
0	= Urgent: Not set										
0 .	= Acknowledgment:	Not set									
	.O = Reset: Not set										
• • • • • • • • • • •	1. = Syn: Set										
Window cize)	0 = Fin: Not set										
[Calculated w	window size: 8192]										
Checksum: 0xe	ee9f [validation disal	led]									
0 58 6d 8f f6	84 6e c8 0a a9 fa d	e 0d 08 00 45 00	Xmn	E.							
LO 00 34 20 37	40 00 80 06 00 00 c	0 a8 01 82 4a 7d	.4 7@								
0 20 00 ee 9f	00 00 02 04 05 b4 0	1 03 03 02 01 01	····								
0 <u>04 02</u>	i hu hua	a aluata 170 Diaglaca di 170 b	•••	0.00.046			Des Clas De Ca				
≥ Frame (frame), 66	b bytes F	ackets: 178 Displayed: 170 N	narked: U Load tin	ne: 0:00.046			Profile: Defa	uit			
aki iest ni	umer portu źr	ódłowego T	CP?								
and joot in		cale nogo i	···-								
ak można	a eklaevfikow	ać nort źród	l_{0}	lakiego	typui	act nor	t źródk				
	a shiasyiikuwa	ας μοιτ Ζίθα	10 vv y f (Janiegu	ւյքսյ	esi pui	1 21 0010	Uvvy)			

Jaki jest numer portu docelowego TCP? _____

Jak można sklasyfikować port docelowy? (Jakiego typu jest port docelowy) ______

Która flaga (lub flagi) są ustawione (1)? _____

Jaka jest wartość numeru sekwencyjnego? _____

d. Aby wybrać następną ramkę w procesie uzgadniania trójetapowego, w menu programu Wireshark wybierz Go a potem wybierz Next Packet In Conversation. W tym przykładzie jest to ramka 16. To jest odpowiedź serwera Google dla rozpoczęcia sesji.

<u>Eile Edit View Go Capture Analyze Statistics Telephony</u> Iools Internals <u>H</u> elp	
$\blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \square X \textcircled + \Rightarrow \Rightarrow 7 \ ! \square \blacksquare \square Q Q Q \square I \blacksquare \blacksquare \blacksquare X \square = = = = = = = = = = = = = = = = = =$	
Filter: tcp Expression Clear Apply Save	
vo. Time Source Destination Protocol Length Info	
10 0.301013000 192.108.1.130 137.33.130.137 (LP 34 49106 > 40115 [ACK] Seq=1/ACK=307 WH=234 Left=0 14 1 576585000 192 168 1 130 74 125 252 209 TCP 66 4952 > bttp [Style] Seq=0 win=8192 [Acm_BMS_4160 wS=4 SarK PERM=1	
15 1.576754000 192.168.1.130 74.125.225.209 TCP 66 49523 > http [Sty] Seq=0 win=8192 Len=0 W55=1460 W55=1400000000000000000000000000000000000	
16 1.611218000 74.125.225.209 192.168.1.130 TCP 66 http > 49523 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64	
17 1.611293000 192.168.1.130 74.125.225.209 TCP 54 49523 > http [ACK] Seq=1 ACk=1 win=65780 Len=0	
18 1.611553000 74.125.225.209 192.168.1.130 TCP 66 http > 49522 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64	
< III	۴
□ Transmission Control Protocol, Src Port: http (80), Dst Port: 49523 (49523), Seq: 0, Ack: 1, Len: 0	
Source port: http (80)	
Destination port: 49523 (49523)	
[Stream index: 2]	
sequence number: 0 (relative sequence number)	
Acknowledgment humber: 1 (relative ack humber)	
neader rengen 22 bytes	
000 = Reserved: Not set	
0 = Nonce: Not set	
0 = Congestion Window Reduced (CWR): Not set	
0 = Urgent: Not set	
1 = Acknowledgment: Set	
0 = Push: Not set	
b1. = Syn: Set	
Window size value: 14300	
[Calculated window size: 14300]	
🗄 Checksum: Oxbae5 [validation disabled]	
2000 c8 0a a9 fa de 0d 58 6d 8f f6 84 6e 08 00 45 20Xmp. F	
0010 00 34 49 cc 00 00 33 06 4f 5f 4a 7d e1 d1 c0 a8 .4I3. 0_3}	
0020 01 82 00 50 C1 73 82 65 5b 91 3b 89 92 21 80 12P.S L;!.	

Jakie są wartości portów źródłowych i docelowych? _____

Które flagi są ustawione?

Jakie są względne numery sekwencyjne i potwierdzenia?

e. Na koniec zbadaj trzeci pakiet procesu uzgadniania trójetapowego tego przykładu. Kliknięcie ramki 17 w górnym oknie powoduje wyświetlenie następujących informacji:

<u>File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help</u>	
루 북 북 북 북 특 등 등 % 운동이 속 수 수 주 두 ! [2] 등 이 수 수 전 한 ! 북 전 🗞 % ! [2]	
Filter Expression Clear Apply Save	
No. Time Source Destination Protocol Length Info	
12 1.155247000 192.168.1.1 192.168.1.130 DNS 154 Standard query response 0xded2 A 74.125.225.209 A 74.125.225.210 A 74.1	.25.225.212 A
13 1.222568000 192.168.1.130 172.17.0.254 SNMP 119 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.	1.25.3.5.1.2.
14 1. 576595000 192.168.1.130 74.125.225.209 TCP 66 49522 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1	
151.576/54000 1921168.11.130 /4.125.225.209 TCP 66 49523 > http [SYN] Seg=0 Win=8192 Len=0 MSS=1460 WS=4 58.4K, PERMEI	WE 64
10 1.011218000 (4.125.22).209 192.100.1.130 ICP 00 NTEP > 49523 [SYN, ACK] SEQ=0 ACK=1 WIN=14300 LEN=0 MSS=1430 SACK_PERM=1	. W5=04
18.1.011253000 74.125.100 14.125.125.00 10 14.125.125.00 10 14.125.125 10 14.125 1001 14.125 1001 14.125 1001 14.125 1001 14.125 1	WS=64
<pre>□ Transmission control Protocol, Src Port: 49523 (49523), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0 Source port: 49523 (49523) Destination port: http (80) [Stream index: 2] Sequence number: 1 (relative sequence number) Acknowledgment number: 1 (relative ack number) Header length: 20 bytes □ Flags: 0x010 (Ack) 000 = Reserved: Not set = Reserved: Not set = Reserved: Not set = Congestion window Reduced (CwR): Not set 0 = ECN-Echo: Not set 0 = Urgent: Not set 0 = Push: Not set 0 = Push: Not set </pre>	
0000 58 6d 8f f6 84 6e c6 7.0	

Zbadaj trzeciego czyli ostatni pakiet uzgadniania trójetapowego.

Która flaga (lub flagi) jest ustawiona?

Względne numery sekwencyjne oraz potwierdzenie są ustawione na 1. Dopiero teraz jest ustanowione połączenie TCP i możliwa jest komunikacja pomiędzy komputerem a serwerem.

f. Zamknij program Wireshark.

Do przemyślenia

- 1. W Wireshark wstępnie zdefiniowane jest wiele filtrów. W dużej sieci może być użytych wiele filtrów, które będą pokazywać różnego rodzaju ruch sieciowy. Które trzy filtry z listy mogą być najbardziej przydatne dla administratora sieci?
- 2. W jaki inny sposób można użyć programu Wireshark w sieci produkcyjnej?