Laboratorium - Używanie programu Wireshark do badania ruchu sieciowego

Topologia



Cele

Część 1: Użycie programu Wireshark do przechwycenia i analizy lokalnych danych ICMP.

- Przechwycenie danych generowanych w sieci poleceniem ping między hostami lokalnymi.
- Zlokalizowanie adresu IP i MAC w przechwyconych PDU.

Część 2: Użycie programu Wireshark do przechwycenia i analizy zdalnych danych ICMP.

- Przechwycenie danych generowanych w sieci poleceniem ping między hostami zdalnymi.
- Zlokalizowanie adresu IP i MAC w przechwyconych PDU.
- Wyjaśnienie dlaczego adresy MAC zdalnych hostów są inne, niż adresy MAC lokalnych hostów.

Scenariusz

Wireshark jest programowym analizatorem protokołów sieciowych, czasem zwany bywa snifferem pakietów. Używany jest do analizy sieci, diagnozowania problemów, wspierania rozwoju różnego rodzaju oprogramowania i nowych protokołów. Jego głównym zastosowaniem jest również edukacja. W momencie gdy strumienie danych podróżują poprzez sieć, analizator przechwytuje i zapamiętuje każdą jednostkę PDU. Następnie dekoduje informacje w nich zawarte do postaci przejrzystej struktury odzwierciedlającej zalecenia RFC i umożliwiającej obserwatorowi bardzo wygodną ich analizę.

Wireshark jest bardzo użytecznym narzędziem dla każdego, kto w swej pracy ma do czynienia z sieciami komputerowymi. Może być z powodzeniem wykorzystywany w większości laboratoriów kursu CCNA w celu analizy przesyłanych danych oraz rozwiązywania napotkanych problemów. To laboratorium zawiera instrukcję dotyczącą pobierania i instalacji programu Wireshark, aczkolwiek może on już być zainstalowany. W tym laboratorium użyjesz programu Wireshark do przechwytywania danych ICMP w celu wyłuskiwania z nich adresów IP i adresów MAC.

Wymagane wyposażenie

- 1 PC (Windows 7, Vista lub XP z dostępem do Internetu)
- Dodatkowy komputer(y) PC w sieci lokalnej (LAN), którego zadaniem będzie odpowiadać na przychodzące żądania ping.

Część 1: Użycie programu Wireshark do przechwycenia i analizy lokalnych danych ICMP.

W 2 części tego ćwiczenia będziesz wysyłać pakiety ping do innego komputera w sieci lokalnej i przechwycisz żądania i odpowiedzi ICMP w programie Wireshark. Ponadto zajrzysz do wnętrza przechwyconych ramek w celu znalezienia konkretnych informacji. Analiza ta powinna przyczynić się do wyjaśnienia, w jaki sposób nagłówki pakietów są używane do transportu danych w miejsce przeznaczenia.

Krok 1: Pobieranie adresów interfejsu twojego PC.

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

- a. Otwórz okno wiersza poleceń, wpisz ipconfig /all i naciśnij Enter.
- b. Zanotuj adres IP i adres MAC (fizyczny) twojego komputera.



c. Poproś innych uczestników o ich adresy IP oraz przekaż im swój. Nie podawaj im swojego adresu MAC.

Krok 2: Uruchomienie programu Wireshark i rozpoczęcie przechwytywania pakietów danych.

- a. Na swoim komputerze, kliknij przycisk **Start** systemu Windows i w menu podręcznym znajdź program Wireshark. Kliknij dwukrotnie **Wireshark**.
- b. Po uruchomieniu Wireshark, kliknij Interface List.

In the Wireshark Network Analyzer (Wireshark 18.3) (SVN Rev 45256 from /trunk-1.8)) File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help Image: Statistic Telephony Ioons Image: Statistic Telephony Ioons Image: Statistic Telephony Ioons Image: Statistic Telephony Ioons Image: Statistic Telephony Ioons <								
Capture Interface List Use sits of the capture interfaces Start Choose one or more interfaces to capture from, then Start Operice/NPF_(DBEC4325-FFF4-4E82-BCLS-9:036F4946680) Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_(6179E093-A447-4E Image: Capture Options Start a capture with detailed options Capture Options Start a capture with detailed options Capture Help Image: Provide Capture Start b capture Media Spatic information for capturing on: Device information for capturing on:	Files Open Open Recent: Image: Sample Captures Arich assonment of example capture files on the wild	Website Wat the project's website With the project's website						
Ready to load or capture	No Packets	Profile: Default						

Uwaga: Kliknięcie na pierwszą ikonę z lewej strony w pasku narzędzi również otworzy Interface List.

c. W oknie Wireshark: Capture Interfaces, kliknij pole wyboru (zaznacz je) odpowiadające interfejsowi podłączonemu do twojej sieci LAN.

📶 Wireshark: C	apture 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: Jeżeli w wykazie znajduje się wiele interfejsów, a nie jesteś pewien, który z nich zaznaczyć, kliknij przycisk **Details** oraz otwórz zakładkę **802.3 (Ethernet)**. Sprawdź czy adres MAC jest taki sam jak ten, który zapisałeś w kroku 1b. Po pomyślnej weryfikacji zamknij okno Interface Details.

📶 Wireshark: Interfa	ace Details		
Characteristics S	Statistics 802.3 (Ethernet)	802,11 (WLAN)	ask Offload
Characteristics Permanent sta	ition address	00:50:50	5:BE:76:8C
Statistics	1 address	00:50:50	DE:/0:0C

d. Po wybraniu właściwego interfejsu, kliknij Start by rozpocząć przechwytywanie danych.

📶 Wireshark: Cap	ture 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
1					
<u>H</u> elp		Start	Stop	<u>O</u> ptions	<u>C</u> lose
		\sim			

Informacje zaczną pojawiać się w górnej sekcji programu Wireshark. W zależności od typu protokołu, linie z danymi będą pojawiać się w różnych kolorach.

🗖 Cap	turing from Intel(R) 82577LM Gigabit Network Cor	nnection: \Device\NPF_{6179E093-A447-4EC8	-81DF-5E22D08A6F63) [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]	
Eile	Edit View Go Capture Analyze Statistics	Telephony <u>T</u> ools Internals <u>H</u> elp		
EV a				
Filter:		 Expression Cle 	ar Apply Save	
No.	Time Source	Destination Proto	col Length Info	*
	21 2.451962000 cisco_7a:ec:84	Spanning-tree-(for-br:STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	22 3.497376000 10.20.164.21	173.194.79.125 TCP	91 [TCP segment of a reassembled PDU]	
	23 3.567094000 173.194.79.125	10.20.164.21 TCP	60 xmpp-client > 53588 [Аск] seq=1 Ack=38 Win=1002 Len=0	
	24 4.451700000 cisco_7a:ec:84	Spanning-tree-(for-br:STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	25 6.451326000 cisco_7a:ec:84	Spanning-tree-(for-br:STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84	
	26 8.451225000 cisco_7a:ec:84	Spanning-tree-(for-br:STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84	
	27 10.27736800(10.20.164.21	173.36.12.72 TCP	55 53964 > 10846 [ACK] seq=1 Ack=1 win=63974 Len=1	
	28 10.35963200(173.36.12.72	10.20.164.21 TCP	66 10846 > 53964 [ACK] Seq=1 Ack=2 win=513 Len=0 SLE=1 SRE=2	
	29 10.45232500(cisco_7a:ec:84	Spanning-tree-(for-br:STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84	
	30 10.94920600(10.20.164.21	171.68.57.53 NBNS	92 Name query NB UNIDC3<20>	
	31 10.99746700(171.68.57.53	10.20.164.21 NBNS	98 Name query response, Requested name does not exist	
	32 10.99758500(10.20.164.21	173.37.115.191 NBNS	5 92 Name query NB UNIDC3<20>	
	33 11.08046600(173.37.115.191	10.20.164.21 NBNS	98 Name query response, Requested name does not exist	
	34 11.09043000(10.20.164.21	10.20.164.31 NBNS	5 92 Name query NB UNIDC3<20>	
	35 11.84043400(10.20.164.21	10.20.164.31 NBNS	5 92 Name query NB UNIDC3<20>	
	36 12.45071000(cisco_7a:ec:84	Spanning-tree-(for-br:STP	60 Conf. Root = 32768/0/30:†7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	37 12.59048100(10.20.164.21	10.20.164.31 NBNS	5 92 Name query NB UNIDC3<20>	_
	38 13.34153600(10.20.164.21	171.68.57.53 NBNS	92 Name query NB UNIDC3<20>	-
	39 13.41142100(171.68.57.53	10.20.164.21 NBNS	98 Name query response, Requested name does not exist	
	40 13.41151700(10.20.164.21	173.37.115.191 NBNS	92 Name query NB UNIDC3<20>	
	41 13.49295400(173.37.115.191	10.20.164.21 NBNS	98 Name query response, Requested name does not exist	
	42 13.50250600(10.20.164.21	10.20.164.31 NBNS	5 92 Name query NB UNIDC3<20>	
	43 14.25256700(10.20.164.21	10.20.164.31 NBNS	92 Name query NB UNIDC3<20>	
	44 14.45045300(C1sco_7a:ec:84	Spanning-tree-(for-briSTP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	45 14.6946/200(10.20.164.21	192.168.87.9 SRVI	.OC 86 Attribute Request, VI Transaction ID - 49289	*
•			m	•
🗄 Fra	ame 1: 66 bytes on wire (528 bits)), 66 bytes captured (528 bits) on interface 0	
🗉 Etł	nernet II, Src: Dell_24:2a:60 (5c:	:26:0a:24:2a:60), Dst: Cisco_7	a:ec:84 (30:f7:0d:7a:ec:84)	
🗉 Int	ternet Protocol Version 4, Src: 10	0.20.164.21 (10.20.164.21), Ds	t: 204.236.230.45 (204.236.230.45)	
🗉 Tra	ansmission Control Protocol, Src F	Port: 54996 (54996), Dst Port:	https (443), Seq: 0, Len: 0	
0000	30 f7 0d 7a ec 84 5c 26 0a 24 2	a 60 08 00 45 00 0 z \&	\$*, E	
0010	00 34 4f 78 40 00 80 06 4a 08 0	a 14 a4 15 cc ec .40x@ J		<u>^</u>
0020	e6 2d d6 d4 01 bb dc b2 af 4e 0	0 00 00 00 80 02	N	E
0030	20 00 8a 09 00 00 02 04 04 ec 0	1 03 03 02 01 01		
0040	04 02			-
0 💅	Intel(R) 82577LM Gigabit Network Connection: \De	evice\NPF_{6179E093-A447-4EC8-81DF Pa	ckets: 45 Displayed: 45 Marked: 0 Profile: Default	
0.0				

e. Ilość napływających danych może być bardzo duża i zależy od intensywności komunikacji między twoim PC a siecią LAN. Możemy nałożyć filtr, by ułatwić przeglądanie i pracę z danymi przechwytywanymi przez Wireshark. Dla celów tego laboratorium interesują nas tylko PDU typu ICMP (ping). By przeglądać tylko PDU typu ICMP (ping), w polu Filter, znajdującym się w górnej części programu Wireshark wpisz icmp i kliknij przycisk Apply lub naciśnij Enter.



f. Ten filtr spowoduje zniknięcie wszystkich danych w głównym oknie aplikacji, jednak nadal są one przechwytywane na interfejsie. Przywróć okno wiersza poleceń, które wcześniej otworzyłeś i wyślij test ping na adres IP otrzymany od twojego kolegi z zajęć. Zauważ, że w głównym oknie programu Wireshark, ponownie pojawią się dane.

Capturing from Intel(R) PRO/1000 N	/T Network Connection [Wireshark 1.6	5.1 (SVN Rev 38096 from /trunk-1	6)]			
<u>File Edit View Go</u> Capture <u>A</u> r	nalyze <u>S</u> tatistics Telephon <u>y T</u> ools	<u>I</u> nternals <u>H</u> elp				
	🕻 🔁 占 🔍 🗢 💠 🌍 春		. 🖭 🕁 🗵 🕵 % (<u>B</u>		
Filter: icmp		Expression Clear Apply	ý			
No. Time Source	Destination	Protocol Length Info				
11 15.118840 192.168.	1.11 192.168.1.12	ICMP 74 Echo	(ping) request id=0	x0001, seq=21/5376, ttl=12		
14 15.119602 192.168.	1.12 192.168.1.11	ICMP 74 Echo	(ping) reply id=0	x0001, seq=21/5376, ttl=12		
16 16.127853 192.168.	1.11 192.168.1.12	ICMP 74 Echo	(ping) request id=0	x0001, seq=22/5632, ttl=12		
17 16.128679 192.168.	1.12 192.168.1.11	ICMP 74 Echo	(ping) reply id=0	x0001, seq=22/5632, ttl=12		
18 17.141897 192.168.	1.11 192.168.1.12	ICMP 74 Echo	(ping) request id=0	x0001, seq=23/5888, ttl=12		
19 17.145943 192.168.	1.12 192.168.1.11	ICMP 74 Echo	(ping) reply id=0	x0001, seq=23/5888, ttl=12		
21 18.140246 192.168.	1.11 192.168.1.12	ICMP 74 Echo	(ping) request id=0	x0001, seq=24/6144, ttl=12		
22 18.140794 192.168.	1.12 192.168.1.11	ICMP 74 Echo	(ping) reply id=0	x0001, seq=24/6144, ttl=12		
	Tunnel adapte Media Stat	stem32\cmd.exe r Local Area Connectio e	on* 11: . : Media disconnecto	n n X		
Gonnection-specific DNS Suffix .: Description Teredo Tunneling Pseudo-Interface Physical Address 80-00-00-00-00-00-00-00-E0 DHCP Enabled No Internet Protocol Version 4, Src: 19						
Thternet Control Message	Protocol G:>>					
Internet Control Message ■	Protocol C:>> C:>>ping 192.	168.1.12		Ξ		

Uwaga: Jeżeli komputer twojego kolegi z zajęć nie odpowiada na test ping, możliwe, że jego firewall blokuje twoje zapytania. Zobacz **Błąd! Nie można odnaleźć źródła odwołania.** by uzyskać więcej informacji na temat odblokowania ruchu ICMP w zaporze ogniowej systemu Windows 7.

g. Zatrzymaj proces przechwytywania danych klikając ikonę Stop Capture.

Capturing from Intel(R) PRO/1000 MT Network Connection										
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> apt	ure	<u>A</u> nal	yze	<u>S</u> tati	stics	Telep
	Ì۲.) È			×	2	₿	Q	4
Filter	r: ic	mp								
No.		Time		Sour	ce				De	estinat
	-22	16.97	5362	192	.16	8.1.	.11		1	92.1

Krok 3: Analiza przechwyconych danych.

W 3 Kroku przeanalizuj dane, wygenerowane przez żądania ping, wysyłane do komputera twojego kolegi z zajęć. W programie Wireshark, dane te są wyświetlane w trzech sekcjach: 1) Górna sekcja wyświetla listę ramek PDU wraz z podsumowaniem informacji o danym pakiecie IP, 2) środkowa sekcja wyświetla informacje na temat ramki PDU zaznaczonej w górnej części ekranu oraz dzieli ją na bazie poszczególnych warstw protokołów, i 3) dolna sekcja wyświetla nieprzetworzone dane dla poszczególnej warstwy. Nieprzetworzone dane są wyświetlane w trybie szesnastkowym (heksadecymalnym) oraz dziesiętnym.

🗖 Cap	oturing from Int	el(R) PRO/1000	MT Network	Connection [Wireshark 1	.6.1 (SVN Rev 38096	from /trunk-1.0	5)]				
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u>	o <u>C</u> apture <u>A</u>	<u>A</u> nalyze <u>S</u> ta	atistics Telephon <u>y T</u> ools	<u>I</u> nternals <u>H</u> elp						
	M 🖾 😂 🖮		X 2 4	s °, 🐐 🔶 7	⊻ 🔳 🕞	\oplus \bigcirc \oplus	m 🛛	1	*		
Filter:	icmp				 Expression 	Clear Apply					
No.	Time	Source		Destination	Protocol L	ength Info					
	11 15.11884	0 192.168	.1.11	192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001,	seq=21/5376,	ttl=1.
	14 15.11960	2 192.168	.1.12	192.168.1.11	ICMP	74 Echo	(ping)	reply	id=0x0001,	seq=21/5376,	tt]=12
	16 16.12785	3 192.168	.1.11	192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001,	seq=22/5632,	tt]=12
	17 16.12867	9 192.168	.1.12	192.168.1.11	ICMP	74 Echo	(ping)	reply	id=0x0001,	seq=22/5632,	tt]=12
	18 17.14189	7 192.168	.1.11	192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001,	seq=23/5888,	tt]=12
	19 17.14594	3 192.168	.1.12	192.168.1.11	ICMP	74 Echo	(ping)	reply	id=0x0001,	seq=23/5888,	tt]=12
	21 18.14024	6 192.168	.1.11	192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001,	seq=24/6144,	tt1=12
	22 18.14079	4 192.168	.1.12	192.168.1.11	ICMP	74 Echo	(ping)	reply	id=0x0001,	seq=24/6144,	tt =12
+ Fra	ame 11: 74	bytes on w	vire (592	2 bits), 74 bytes c	aptured (592	bits)					
⊕ Eti	hernet II, ternet Prot	Src: Intel ocol Versi	cor_34:9	92:1c (58:94:6b:34: .c: 192.168.1.11 (1	92:1c), Dst: 92.168.1.11),	Intel_Of:9 Dst: 192.	1:48 (00 168.1.12	0:11:11 2 (192.1	:0f:91:48) L68.1.12)		
+ In	ternet Cont	roi messag	je protoc	201					Mid	dle Section	
0000 0010 0020 0030 0040	00 50 56 00 3c 01 01 0c 08 67 68 69 77 61 62	be f6 db 0 ac 00 00 8 00 4d 46 0 6a 6b 6c 6 63 64 65 6	0 50 56 0 01 b5 0 01 00 d 6e 6f 6 67 68	be 76 8c 08 00 45 ad c0 a8 01 0b c0 15 61 62 63 64 65 70 71 72 73 74 75 69	00 .PV6 a8 .< 66MF. 76 ghijklm wabcdefo	P V.VE. abcdef n opqrstuv g hi			Bot	tom Seciton	* III *
O Int	el(R) PRO/1000 I	AT Network Co	nnection:	Packets: 199 Displayed: 8	Marked: 0				Profile: Defa	ault	н

 a. Kliknij na pierwsze żądanie ICMP z listy ramek PDU w górnej sekcji programu Wireshark. Zwróć uwagę, że w kolumnie Source zapisany jest adres IP twojego komputera, a w kolumnie Destination adres IP komputera kolegi z zajęć, na który wysyłałeś żądania ping.

🗖 Ir	ntel(R) PRO/1000 M	T Network Connection	[Wireshark 1.6.1 (SVN Rev 380	96 from /trunk-1.	6)]				
<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>Statistics</u> Telephony <u>T</u> ools	Internals <u>H</u> elp)				Source
		🖻 🖥 🗶 😂	占 🔍 🗢 🔷 孩	<u>↓</u> E 🛢		1	*		Jource
Filte	r: icmp			Expression	Clear Apply				
No.	Time	Source	Destination	Protocol	Length Info				_
	5 2.801784	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping) request	id=0x0001,	seq=25/6400,	tt]=12
	8 2.802679	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping) reply	id=0x0001,	seq=25/6400,	tt]=12
	10 3.816895	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping) request	id=0x0001,	seq=26/6656,	tt]=12
	11 3.817540	192.168.1.12	192. <u>168.1</u> .11	ICMP	74 Echo	(ping) reply	id=0x0001,	seq=26/6656,	tt]=12
	13 4.831343	192.168.1.11	192.168.1.12	ICMP	74 Echo	(pinc) request	i d=0x0001,	seq=27/6912,	tt]=12
	14 4.832006	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping) reply	id=0x0001,	seq=27/6912,	tt]=12
	15 5.844858	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping) request	id=0x0001,	seq=28/7168,	tt]=12
	16 5.845488	192.168.1.12	192,168,1,11	ICMP	74 Echo	(ping) reply	id=0x0001.	seg=28/7168.	tt]=12

b. Przejdź do środkowej sekcji programu, ramka PDU w sekcji górnej nadal musi być zaznaczona. Kliknij znak plusa znajdujący się po lewej stronie wiersza Ethernet II, by zobaczyć adresy MAC urządzenia źródłowego i docelowego.

🗖 Ir	tel(R) PRO/100	0 MT Ne	etwork C	onnectior	n [Wiresh	ark 1.6.1	L (SVN R	ev 38096	5 from ,	trunk-1.6	5)]		Ŷ							
File	<u>E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u>	apture	<u>A</u> nalyze	Statistics	: Telep	phony	<u>T</u> ools	Interna	ls <u>H</u> elp										
	iii () ()) 1	-	X 2	8 0)	۵) T	⊈ [Ð,	Q (1		è	i 🗹	6 %	6 🔯			
Filte	r: icmp								▼ Exp	ression	. Clear	Арр	у							
No.	Time	S	ource			Destina	tion		P	otocol	Length	Info								_
	5 2.8017	84 1	.92.16	8.1.11		192.1	.68.1.1	12	I	CMP	74	Echo) (pi	ng)	r eque:	st	id=0x0001,	seq=25	/6400,	tt]=12
	8 2.8026	79 1	.92.16	8.1.12		192.1	.68.1.1	11	I	CMP	74	Echo) (pi	ng)	reply		id=0x0001,	seq=25	/6400,	tt]=12
	10 3.8168	95 1	.92.16	8.1.11		192.1	.68.1.1	12	I	CMP	74	Echo) (pi	ng)	reque	st	id=0x0001,	seq=26	/6656,	tt]=12
	11 3.8175	40 1	.92.16	8.1.12		192.1	.68.1.1	11	I	CMP	74	Echo) (pi	ng)	reply		id=0x0001,	seq=26	/6656,	tt]=12
	13 4.8313	43 1	92.16	8.1.11		192.1	.68.1.1	12	I	CMP	74	Echo) (pi	ng)	reque	st	id=0x0001,	seq=27	/6912,	tt]=12
	14 4.8320	06 1	.92.16	8.1.12		192.1	.68.1.1	11	I	CMP	74	Echo) (pi	ng)	reply		id=0x0001,	seq=27	/6912,	tt]=12
	15 5.8448	58 1	.92.16	8.1.11		192.1	.68.1.1	12	I	CMP	74	Echo) (pi	ng)	reque	st	id=0x0001,	seq=28	/7168,	tt]=12
	16 5.8454	88 1	.92.16	8.1.12		192.1	.68.1.1	11	I	CMP	74	Echo) (pi	ng)	reply		id=0x0001,	seq=28	/7168,	tt]=12
⊞ F	rame 13: 7	4 byt	es on	wire (592 bit	:s), 7	'4 byt	es cap	pture	d (592	bits)								
OF	thernet II	, Src	: Inte	lcor_3	4:92:10	- (58)	94:6h	:34:92	2:1c)	, Dst:	Inte	1_0f:	91:4	B ((0:11:1	1:0	f:91:48)			
•	Destinati	on: I	ntel_0	f:91:/	8 (00:1	1:11:	0f:91	:48)												
+	Source: I	ntelC	or_34:	92:10	(58:94:	6b:34	1:92:10	c)												
	Туре: ІР	(0x08	00)																	
+ I	nternet Pr	otoco	l Vers	ion 4,	Src: 1	92.16	i8.1.1	1 (192	2.168	(1.11)	, Dst	: 192	.168	1.1	.2 (192	2.16	8.1.12)			
÷I	nternet Co	ntrol	Messa	ge Pro	tocol															

Czy adres MAC urządzenia źródłowego pasuje do interfejsu twojego PC?

Czy adres MAC urządzenia docelowego w programie Wireshark, pasuje do adresu MAC komputera twojego kolegi z zajęć?_____

W jaki sposób twój PC uzyskał MAC adres komputera PC, na który wysyłałeś żądania ping?

Uwaga: W powyższym przykładzie ilustrującym przechwytywanie żądania ICMP, dane ICMP enkapsulowane są wewnątrz PDU pakietu IPv4 (nagłówek IPv4), który następnie enkapsulowany jest w PDU ramki Ethernet II (nagłówek Ethernet II) i przygotowany do transmisji w sieci LAN.

Część 2: Użycie programu Wireshark do przechwycenia i analizy zdalnych danych ICMP.

W części 3, wykonasz test ping do zdalnych komputerów (komputerów nie będących w sieci LAN) oraz zbadasz dane wygenerowane przez test ping. Następnie ustalisz, jaka jest różnica między tymi danymi, a danymi zbadanymi w Części 2.

Krok 1: Rozpoczęcie przechwytywania danych z interfejsu.

a. Kliknij ikonę Interface List, by ponownie przywołać listę interfejsów twojego PC.



b. Upewnij się, że pole wyboru obok interfejsu LAN jest zaznaczone, a następnie kliknij Start.

📶 Wireshark: Capt	ture 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	<u>D</u> etails
<u>H</u> elp		Start	Stop	<u>O</u> ptions	<u>C</u> lose

c. Przed rozpoczęciem nowego procesu przechwytywania, pojawi się okno informujące o możliwości zapisania wcześniej przechwyconych danych. Nie ma potrzeby ich zapisywać. Kliknij **Continue without Saving**.

📶 Wireshark	
	Save capture file before starting a new capture?
	If you start a new capture without saving, your current capture data will
	be discarded.
Save	Continue without Saving Cancel

- d. Kiedy już proces przechwytywania jest aktywny, wykonaj test ping dla trzech poniższych stron internetowych:
 - 1. www.yahoo.com
 - 2. www.cisco.com
 - 3. www.google.com

C:\Windows\system32\cmd.exe	- • •
C:\>ping www.yahoo.com	*
Pinging www.yahoo.com [72.30.38.140] with 32 bytes of data: Reply from 72.30.38.140: bytes=32 time=1ms TTL=255 Reply from 72.30.38.140: bytes=32 time<1ms TTL=255 Reply from 72.30.38.140: bytes=32 time<1ms TTL=255 Reply from 72.30.38.140: bytes=32 time<1ms TTL=255	
Ping statistics for 72.30.38.140: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = 1ms, Average = Oms	E
C:∖>ping www.cisco.com	
Pinging www.cisco.com [198.133.219.25] with 32 bytes of data: Reply from 198.133.219.25: bytes=32 time<1ms TTL=255 Reply from 198.133.219.25: bytes=32 time<1ms TTL=255 Reply from 198.133.219.25: bytes=32 time<1ms TTL=255 Reply from 198.133.219.25: bytes=32 time<1ms TTL=255	
Ping statistics for 198.133.219.25: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms	
C:∖>ping www.google.com	
Pinging www.google.com [74.125.129.99] with 32 bytes of data: Reply from 74.125.129.99: bytes=32 time=1ms ITL=255 Reply from 74.125.129.99: bytes=32 time<1ms ITL=255 Reply from 74.125.129.99: bytes=32 time<1ms ITL=255 Reply from 74.125.129.99: bytes=32 time<1ms ITL=255	
Ping statistics for 74.125.129.99: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = 1ms, Average = Oms	
C:\>_	

Uwaga: Kiedy wykonujesz test ping kolejnych URL zwróć uwagę, że DNS (ang. Domain Name Server) tłumaczy URL na adres IP. Zanotuj adres IP dla każdego URL.

e. Zatrzymaj proces przechwytywania danych klikając ikonę Stop Capture.



Krok 2: Badanie i analiza danych otrzymanych z hostów zdalnych.

a. Przejrzyj przechwycone dane w programie Wireshark, sprawdź adresy IP i MAC trzech stron internetowych dla których wykonałeś polecenie ping. Poniżej wpisz, docelowy adres IP i MAC dla wszystkich trzech stron internetowych.

1 st Lokalizacja:	IP:	-•	•	·	MAC:	_:	<u>:</u>	<u>:</u>	:	<u>:</u>	
2 nd Lokalizacja:	IP:				MAC:	_:	:		:	:	
3 rd Lokalizacja:	IP:				MAC:	_:	_:	:	:	:	

- b. Co jest istotne w tej informacji?
- c. Czym różni się ta informacja od informacji uzyskanej w części 2, dotyczącej używania polecenia ping w sieci lokalnej?

Do przemyślenia

Dlaczego Wireshark pokazuje aktualny adres MAC dla hostów lokalnych, ale już nie pokazuje aktualnego MAC dla hostów zdalnych?

it iven	All	INU	Allow		пер
I Cach	All	No	Allow		TCLUD D
iscove	All	No	Allow	Allo	bw ICMP Requests
Proje	Domain	No	Allow	۰	Disable Rule
Proje	Private	No	Allow	X	Cut
Proje	Private	No	Allow		Comu
Proje	Domain	No	Allow		сору
Proje	Domain	No	Allow 🔍	×	Delete
Proie	Private	No	Allow	F	Properties