# Использование программы Wireshark для просмотра сетевого трафика Топология



### Задачи

Часть 1. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в локальной сети

Часть 2. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в удаленную сеть

# Общие сведения/сценарий

Wireshark – это программа для анализа протоколов (анализатор пакетов), которая используется для поиска и устранения неполадок в сети, анализа, разработки программного обеспечения и протоколов, а также обучения. По мере движения потоков данных по сети анализатор «захватывает» каждую единицу данных протокола (PDU), после чего расшифровывает или анализирует ее содержание согласно соответствующему документу RFC или другим спецификациям.

Wireshark – полезный инструмент для всех, кто работает с сетями. Его можно использовать для анализа данных, а также для поиска и устранения неполадок при выполнении большинства лабораторных работ в рамках курсов CCNA. В ходе лабораторной работы вы научитесь пользоваться программой Wireshark для захвата IP-адресов пакетов данных ICMP и MAC-адресов Ethernet-кадров.

# Часть 1. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в локальной сети

В части 1 необходимо отправить эхо-запрос с помощью команды ping на другой ПК в локальной сети и перехватить ICMP-запросы и отклики в программе Wireshark. Кроме того, вам нужно найти необходимую информацию в собранных кадрах. Этот анализ поможет понять, как заголовки пакетов позволяют доставлять данные адресатам.

### Шаг 1: Определите адреса интерфейсов вашего ПК.

Вам необходимо узнать IP-адрес компьютера и физический адрес сетевой платы, который называется МАСадресом.

- а. Откройте окно командной строки, введите команду ipconfig /all и нажмите клавишу ввода.
- b. Запишите IP-адрес интерфейса ПК и МАС-адрес.

C:\Windows\system32\cmd.exe	X
C:∖>ipconfig ∕all	*
Windows IP Configuration	
Host Name PC-A	
Primary Dns Suffix	
IP Routing Enabled.	
WINS Proxy Enabled : No	Ξ
Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix .:	
Description : Lasting The Mark Connection	
Physical Hodress	
Autoconfiguration Enabled Yes	
Link-local IPv6 Address : المح <del>ادة 1960، 24م</del> وني Link-local IPv6 Address	
IPv4 Address	
Subnet Mask	
$\frac{1}{2} \frac{1}{2} \frac{1}$	

с. Обменяйтесь ІР-адресами ПК с другими учащимися, но пока что не сообщайте им свой МАС-адрес.

#### Шаг 2: Запустите программу Wireshark и начните сбор данных.

а. После запуска программы Wireshark нажмите на Interface List (Список интерфейсов).

The Wireshark Network Analyzer [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]												
<u>File Edit View Go Capture Analyze Statistics Telephony</u> <u>Iools</u> Internals	Help											
(3) ₩ 월 월 월   ▷ 🖫 🗙 🕾 占   < + + + + 7 ±   [=]	🗐 0, 0, 0, 11   🕷 🗹 🍢 💢											
Filter: Express	sion Clear Apply Save											
WIRESHARK Version 1.8.3 (SVN Rev 45256 from /trunk-1	rk Protocol Analyzer .8)	Osline										
Capture	Files	Omine										
Interface List         Up the of the capture interfaces         Image: Start         Choose one or more interfaces to capture from them Start         Sum: \Device\NPF_(D9EC4325-FF46-4E82-BC18-9636F4946680)         Image: Image	<ul> <li>Open Byoen a previously captured fite</li> <li>Open Recent:</li> <li>Sample Captures</li> <li>A rich assortment of example capture files on the wild</li> </ul>	Website           Vati the project's website										
Ready to load or capture	No Packets	Profile: Default										

Примечание. Список интерфейсов можно также открыть, нажав на значок первого интерфейса в ряду значков.

b. В окне Capture Interfaces (Захват интерфейсов) программы Wireshark установите флажок рядом с интерфейсом, подключенным к вашей локальной сети.

📶 Wireshark: Cap	ture Interfaces				- • <b>×</b>
	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
Help		Start	Stop	<u>O</u> ptions	<u>C</u> lose

**Примечание**. Если перечислено несколько интерфейсов и вы не уверены в том, какой из них нужно выбрать, нажмите кнопку **Details** (Подробнее) и откройте вкладку **802.3 (Ethernet)**. Убедитесь в том, что МАС-адрес соответствует результату, который вы получили в шаге 1б. Убедившись в правильности интерфейса, закройте окно информации об интерфейсе.

Wireshark: Interface Details	
Characteristics Statistics (802.3 (Ethernet)	802.11 (WLAN) Task Offload
Characteristics Permanent station address Current station address	00:50:56:BE:76:8C 00:50:56:BE:76:8C
Statistics	

с. После этого нажмите кнопку Start (Начать), чтобы начать захват данных.

📶 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	<u>D</u> etails
<u>H</u> elp		Start	Stop	<u>O</u> ptions	<u>C</u> lose

В верхней части окна программы Wireshark начнет прокручиваться информация. Строки данных выделяются различными цветами в зависимости от протокола.

📶 Cap	oturing from Intel(R) 82577LM Gigabit Network Cor	nection: \Device\NPF_{6179E093-A	47-4EC8-81	DF-5E22D08A6F63} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]	
Eile	Edit View Go Capture Analyze Statistics	Telephony Iools Internals H	elp		
D( ä		💩 📦 🧔 🐺 🔮 🗐 🗐	∎ ⊕ ∈	2 😟 📅 🛙 🎬 🕅 🕵 💥 🛛 🛱	
Filter:		<ul> <li>Expression</li> </ul>	n Clear	Apply Save	
No.	Time Source	Destination	Protocol	Length Info	
	21 2.451962000 cisco_7a:ec:84	Spanning-tree-(for-b	r'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 [ACK] Seq=1 Ack=38 Win=1002 Len=0	
	24 4.451700000 cisco_7a:ec:84	Spanning-tree-(for-b	r'STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84	
	25 6.451326000 Cisco_7a:ec:84	Spanning-tree-(for-b	r'STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	26 8.451225000 Cisco_7a:ec:84	Spanning-tree-(for-b	IT'STP	60 Conf. Root = 32768/0/30:†7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	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(1/3. 36.12. /2	10.20.164.21	TCP	66 10846 > 53964 [ACK] Seq=1 ACK=2 Win=513 Len=0 SLE=1 SRE=2	
	29 10.45232500(C15C0_7a;ec:84	spanning-cree-(ror-c	NDNG	60 CONT. ROOT = 32/68/0/3017/1001/a1ec184 COST = 0 POPT = 0X8001	
	30 10.94920600(10.20.164.21	1/1.00.3/.33	NBNS	92 Name query NB UNICS<20>	
	32 10 00758500(10 20 164 21	172 27 115 101	NDND	90 Name query response, requested name does not exist	
	33 11 08046600(173 37 115 191	10 20 164 21	NENS	92 Name query response. Requested name does not exist	
	34 11 09043000(10 20 164 21	10 20 164 31	NBNS	92 Name query NB LINDC3/205	
	35 11 84043400(10 20 164 21	10.20.164.31	NBNS	92 Name query NB UNDC3-20>	
	36 12,45071000(cisco 7a:ec:84	Spanning-tree-(for-h	IT'STP	60  cont = 32768/0/30:f7:0d:7a:ec:84  cost = 0  Port = 0x8001	
	37 12.59048100(10.20.164.21	10.20.164.31	NBNS	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	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(cisco_7a:ec:84	Spanning-tree-(for-b	IT'STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84	
	45 14.69467200(10.20.164.21	192.168.87.9	SRVLOC	86 Attribute Request, V1 Transaction ID - 49289	
٠				m	•
E Enz	ame 1: 66 bytes on wire (528 bits)	. 66 bytes captured (52	8 bits)	on interface 0	
E Et	hernet II. Src: Dell 24:2a:60 (5c:	26:0a:24:2a:60). Dst: C	isco 7a:	ec:84 (30:f7:0d:7a:ec:84)	
In Int	ternet Protocol Version 4. Src: 10	.20.164.21 (10.20.164.2	1). Dst:	204,236,230,45 (204,236,230,45)	
E Tra	ansmission Control Protocol. Src P	ort: 54996 (54996), Dst	Port: h	ttps (443). Seg: 0. Len: 0	
0000	20 f7 0d 72 oc 84 5c 26 02 24 2	- 60 08 00 45 00 0 7	\ P. \$#		
0010	00 34 4f 78 40 00 80 06 4a 08 0	a 14 a4 15 cc ec .40x0	·\α)"		*
0020	e6 2d d6 d4 01 bb dc b2 af 4e 0	0 00 00 00 80 02	N		=
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	vice\NPF_{6179E093-A447-4EC8-81	DF Packe	ts: 45 Displayed: 45 Marked: 0 Profile: Default	

d. Информация может прокручиваться очень быстро, это зависит от интенсивности взаимодействия ПК с локальной сетью. Чтобы облегчить просмотр и работу с данными, собранными программой Wireshark, можно применить фильтр. В этой лабораторной работе нас интересуют только единицы данных протокола (PDU) ICMP (эхо-запрос с помощью команды ping). Чтобы вывести на экран только единицы данных протокола ICMP (эхо-запрос с помощью команды ping), в поле фильтра в верхней части окна программы Wireshark введите **icmp** и нажмите клавишу ввода или кнопку **Аpply** (Применить).

n c	apturing from	Intel(R) 82577LM Gigabit N	letwork Connection: \	Device\NP	F_{6179E093-A447-4E	EC8-81DF-5E	E22D08A6F63}	[Wireshark 1.8.3	(SVN Rev 45256 from /trunk-1.8)]
<u>F</u> ile	<u>E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u> apture <u>A</u> nalyze	Statistics Telephon	n <u>y T</u> ools	<u>I</u> nternals <u>H</u> elp				
	in di <del>ci</del>			<table-cell> 🖗</table-cell>		0, 0, 10	<b>L</b> 🖂 🛛 🖉	🖹 🍢 🎇	ġ.
Eilte	r: icmp	$\rightarrow$	)		Expression	Clear Appl	ly Save		
No.	Time	Source	Dest	ination	Pro	otocol Ler	ngth Info		

е. После этого все данные в верхнем окне исчезнут, однако захват трафика в интерфейсе продолжится. Откройте окно командной строки, которое вы открывали ранее, и отправьте эхо-запрос с помощью команды ping на IP-адрес, полученный от другого учащегося. Обратите внимание на то, что в верхней части окна программы Wireshark снова появятся данные.

Capturing from Intel(R) PRO/1000 MT Netwo	k Connection [Wireshark 1.6.1 (S)	/N Rev 38096 from /trunk-1.	6)]									
<u>File Edit View Go Capture Analyze S</u>	atistics Telephon <u>y T</u> ools <u>I</u> nter	nals <u>H</u> elp										
	] 🔍 🍬 🔿 ዥ 👱		🖭   🎬 🕅 🔂	*   🕱								
Filter: icmp	•	Expression Clear Apply										
No. Time Source	Destination	Protocol Length Info										
11 15.118840 192.168.1.11	192.168.1.12	ICMP 74 Echo	(ping) request	id=0x0001,	seq=21/5376,	tt]=12						
14 15.119602 192.168.1.12	192.168.1.11	ICMP 74 Echo	(ping) reply	id=0x0001,	seq=21/5376,	tt]=12						
16 16.127853 192.168.1.11	192.168.1.12	ICMP 74 Echo	(ping) request	id=0x0001,	seq=22/5632,	tt]=12						
17 16.128679 192.168.1.12	192.168.1.11	ICMP 74 Echo	(ping) reply	id=0x0001,	seq=22/5632,	tt]=12						
18 17.141897 192.168.1.11	192.168.1.12	ICMP 74 Echo	(ping) request	id=0x0001,	seq=23/5888,	tt1=12						
19 17.145943 192.168.1.12	192.168.1.11	ICMP 74 Echo	(ping) reply	1d=0x0001,	seq=23/5888,	tt1=12						
21 18.140246 192.168.1.11	192.168.1.12	ICMP /4 ECho	(ping) request	1d=0x0001,	seq=24/6144,	tt I=1/						
	C:\Windows\system3	2\cmd.exe				• 8						
C C:\Windows\system32\cmd.exe  C C:\\Dimensional Adapter Local Area Connection* 11:  Media State												
<ul> <li>ethernet II, Src: Vmware_be:76</li> <li>Internet Protocol Version 4, S</li> <li>Internet Control Message Proto</li> </ul>	:8c (()     DHCP Enabled.       rc: 10     Autoconfigurat       col     C:>       C:>ping 192.168.	ss	. : 00-00-00-00 . : No . : Yes	-00-00-00-E0	-Interface							

**Примечание**. Если компьютеры других учащихся не отвечают на ваши эхо-запросы, это может быть вызвано тем, что межсетевые экраны их компьютеров блокируют эти запросы. Информацию о том, как обеспечить пропуск трафика ICMP через межсетевой экран на ПК с ОС Windows 7 см. в **Ошибка!** Источник ссылки не найден..

f. Остановите захват данных, нажав на значок Stop Capture (Остановить захват).

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> tat	istics	Telep			
			)			×	2	₽	Q				
Filter	: icm	р											
No.	1	lime		Sour	ce				D	estinat			
	22.1	L6.973	5362	192	.16	8.1.	. 11		1	.92.1:			

#### Шаг 3: Изучите полученные данные.

В шаге 3 необходимо проверить данные, сформированные эхо-запросами с помощью команды ping на ПК других учащихся. Программа Wireshark отображает данные в трех разделах: 1) в верхнем разделе отображается список полученных кадров PDU со сводной информацией об IP-пакетах; 2) в среднем разделе

приводится информация о PDU для кадра, выбранного в верхней части экрана, а также разделение перехваченного кадра PDU по уровням протоколов; 3) в нижнем разделе показываются необработанные данные каждого уровня. Необработанные данные отображаются как в шестнадцатеричном, так и в десятичном форматах.

🗖 Ca	pturing from In	itel(R) PR	0/1000 N	/IT Netw	ork Co	nnection	[Wiresh	ark 1.6.	1 (SVI	N Rev 38096	from /	trunk-1	.6)]						- 6	
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>(</u>	<u>G</u> o <u>C</u> ap	oture <u>A</u> r	nalyze	<u>S</u> tatisti	cs Telep	hony ]	<u>T</u> ools	Intern	nals <u>H</u> elp										
	in di di ei		8 🖪 🗴	8	8	् 🔅	۵	₹.	₽		⊕ (	<b>A</b> 0	++	<b>X</b> (	¥ 🖪 :	*	Ø			
Filter	: icmp								▼ E	xpression	Clear	Apply	/							
No.	Time	Sou	urce			Destina	tion			Protocol L	ength	Info								_
	11 15.1188	340 19	2.168.	1.11		192.1	68.1.1	2		ICMP	74	Echo	(ping	) re	equest	id=	=0x0001,	seq=21/5	5376,	ttl=1.
·	14 15.1196	602 19	2.168.	1.12		192.1	68.1.1	1		ICMP	74	Echo	(ping	) re	eply	id=	=0x0001,	seq=21/5	376,	tt]=12
	16 16.1278	353 19	2.168.	1.11		192.1	68.1.1	.2		ICMP	74	Echo	(ping	) re	equest	id=	=0x0001,	seq=22/5	632,	tt]=12
	17 16.1286	579 19	2.168.	1.12		192.1	68.1.1	.1		ICMP	74	Echo	(ping	) re	eply	id=	=0x0001,	seq=22/5	632,	tt]=12
	18 17.1418	897 19	2.168.	1.11		192.1	68.1.1	.2		ICMP	74	Echo	(ping	) re	equest	id=	=0x0001,	seq=23/5	5888,	tt]=12
	19 17.1459	43 19	2.168.	1.12		192.1	68.1.1	.1		ICMP	74	Echo	(ping	) re	eply	id=	=0x0001,	seq=23/5	888,	tt]=12
	21 18.1402	46 19	2.168.	1.11		192.1	68.1.1	.2		ICMP	74	Echo	(ping	) re	equest	id=	=0x0001,	seq=24/6	5144,	tt]=12
	22 18.1407	94 19	2.168.	1.12		192.1	68.1.1	.1		ICMP	74	Echo	(ping	) re	eply	id=	=0x0001,	seq=24/6	5144,	tt]=12
																		psection		
+ Fr	ame 11: 74	bytes	s on wi	ire (5	92 bi	its), 7	4 byte	es cap	ptur	ed (592	bits	)		(00.		05.0	1.40			
± Et	nernet II,	src:	Intelo	or_34	:92:J	102 16	94:60:	34:94	2:10	), DST:	Inte	1_07:9	91:48	(00:	(102.1	OT : 9	91:48)			
	ternet Con	trol N	Ver STU Assand	Drot	ocol	192.10	0.1.11	(19)	2.10	0.1.11),	DSC	. 192.	.100.1	.12	(192.1	.00.1				
. 1			essage		.0001												Mic	dle Sectior	ı	
0000 0010 0020 0030 0040	00 50 56 00 3c 01 01 0c 08 67 68 69 77 61 62	be f6 ac 00 00 4d 6a 6b 63 64	db 00 00 80 46 00 6c 6d 65 66	50 01 01 6e 67	56 be b5 ad 00 15 6f 70 68 69	76 8c c0 a8 61 62 71 72	08 00 01 0b 63 64 73 74	45 0 c0 a 65 6 75 7	00 48 56 76	.PV . <mf. ghijklm wabcdef</mf. 	P V.V a n opc g hi	bcdef	:				Bot	tom Secito	n	* 
O In	tel(R) PRO/1000	MT Net	work Con	nection	: Pa	ackets: 19	Display	ed: 8 M	arked:	0							Profile: Defa	ult		зá

а. Выберите кадры PDU первого запроса ICMP в верхнем разделе окна программы Wireshark. Обратите внимание на то, что в столбце Source (Источник) указывается IP-адрес вашего компьютера, а в столбце «Destination» (Назначение) — IP-адрес ПК другого участника, на который вы отправили эхо-запрос с помощью команды ping.

🗖 In	tel(R)	PRO/100	00 MT	Network (	Connectio	n [Wiresha	rk 1.6.1 (SV	N Rev 3809	96 from /trunk-1.	6)]						
<u>F</u> ile	Edit	<u>V</u> iew	<u>G</u> o	<u>C</u> apture	<u>A</u> nalyze	<u>S</u> tatistics	Telephon	<u>/ T</u> ools	<u>I</u> nternals <u>H</u> elp	0						Sourc
8	Ë.	ok 🕷			X 2	4 Q	, 🗢 🔿	🤣 ዥ	⊻   🔳 🛢	⊕ (		<b>**</b>	ı 🗹 🚯	*		Joure
Filte	r: ic	mp							Expression.	Clear	Apply					
No.		Time		Source		D	estination		Protocol	Length	Info					
	5	2.8017	784	192.16	58.1.11	1	92.168.	1.12	ICMP	74	Echo	(ping)	request	id=0x0001,	seq=25/6400,	tt]=12
	8	2.8026	579	192.16	58.1.12	1	92.168.	1.11	ICMP	74	Echo	(ping)	reply	id=0x0001,	seq=25/6400,	tt]=12
	10	3.8168	395	192.16	58.1.11	1	92.168.	1.12	ICMP	74	Echo	(ping)	request	id=0x0001,	seq=26/6656,	tt]=12
	11	3.8175	540	192.16	58.1.12	1	92.168.	1.11	ICMP	74	Echo	(ping)	reply	id=0x0001,	seq=26/6656,	tt]=12
	13	4.831	343	192.16	58.1.11	> <	92.168.	1.12	ICMP	74	Echo	(pinc	request	<b>i</b> d=0x0001,	seq=27/6912,	tt]=12
	14	4.8320	006	192.16	58.1.12	1	92.168.	1.11	ICMP	74	Echo	(ping)	reply	id=0x0001,	seq=27/6912,	tt]=12
	15	5.8448	358	192.16	58.1.11	1	92.168.	1.12	ICMP	74	Echo	(ping)	request	id=0x0001,	seq=28/7168,	tt]=12
	16	5.8454	88	192.16	58.1.12	1	92.168.	1.11	ICMP	74	Echo	(ping)	reply	id=0x0001,	seq=28/7168,	tt]=12

b. Не меняя выбор кадра PDU в верхнем разделе окна, перейдите в средний раздел. Нажмите на символ + слева от строки «Ethernet II», чтобы увидеть MAC-адреса источника и назначения.

🗖 In	tel(R) PRO/100	00 MT	Network C	onnectio	n [Wiresha	rk 1.6.1 (SVN	Rev 3809	96 from /1	runk-1.6	5)]		Ŷ				
<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> tatistics	Telephony	<u>T</u> ools	Internal	<u>H</u> elp							
	¥ Ø %	Ì٧		* 2		、 🗢 🛸 🖨	<b>ð</b>	<b>1</b>		⊕ (	⊇, ©,	<b>**</b>	🧸 🗹 🍋	*		
Filte	: icmp							▼ Exp	ession	. Clear	Apply					
No.	Time		Source		[	estination		Pro	tocol l	Length	Info					
	5 2.8017	784	192.16	8.1.11	1	L92.168.1	.12	IC	MP	74	Echo	(ping)	request	id=0x0001,	seq=25/6400,	tt]=12
	8 2.8026	579	192.16	8.1.12	1	192.168.1	. 11	IC	MP	74	Echo	(ping)	reply	id=0x0001,	seq=25/6400,	tt]=12
	10 3.8168	895	192.16	8.1.11	1	192.168.1	.12	IC	MP	74	Echo	(ping)	request	id=0x0001,	seq=26/6656,	tt]=12
	11 3.8175	540	192.16	8.1.12	1	192.168.1	.11	IC	MP	74	Echo	(ping)	reply	id=0x0001,	seq=26/6656,	tt]=12
	13 4.8313	343	192.16	8.1.11	1	192.168.1	.12	IC	MP	74	Echo	(ping)	request	id=0x0001,	seq=27/6912,	tt]=12
	14 4.8320	006	192.16	8.1.12	1	192.168.1	.11	IC	MP	74	Echo	(ping)	reply	id=0x0001,	seq=27/6912,	tt]=12
	15 5.8448	858	192.16	8.1.11	1	192.168.1	.12	IC	MP	74	Echo	(ping)	request	id=0x0001,	seq=28/7168,	tt]=12
	16 5.8454	188	192.16	8.1.12	1	192.168.1	.11	IC	MP	74	Echo	(ping)	reply	id=0x0001,	seq=28/7168,	tt]=12
⊞ F	ame 13: 7	74 by	/tes on	wire (	592 bit:	s), 74 by	tes ca	apturec	(592	bits	)					
OF	hernet II	E, Sr	c: Inte	elCor_3	4:92·1c	(58:94:6	h:34:9	92:1c),	Dst:	Inte	1_01:9	91:48 (	00:11:11	:0f:91:48)		
+	Destinati	ion:	Intel_(	)f:91:4	8 (00:1	1:11:0f:9	1:48)	5								
±	Source: I	Inte	ICor_34:	92:10	(58:94:	5b:34:92:	1c)									
	туре: ІР	(0x0	00800)		_					_	1.05		10 (10-			
÷Ι	nternet Pr	oto	col Vers	$10n_4$ ,	Src: 19	92.168.1.	11 (19	92.168.	1.11)	, Dst	: 192.	168.1.	12 (192.	168.1.12)		
÷I	iternet Co	ontro	DI Messa	age Pro	τοςοι											

Совпадает ли МАС-адрес источника с интерфейсом вашего компьютера?

Совпадает ли МАС-адрес назначения в программе Wireshark с МАС-адресом другого учащегося?

Как ваш ПК определил MAC-адрес другого ПК, на который был отправлен эхо-запрос с помощью команды ping?

**Примечание**. В предыдущем примере захваченного ICMP-запроса данные протокола ICMP инкапсулируются внутри PDU пакета IPv4 (заголовка IPv4), который затем инкапсулируется в PDU кадра Ethernet II (заголовок Ethernet II) для передачи по локальной сети.

# Часть 2: Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в удаленную сеть

В части 2 вы должны будете отправить эхо-запросы с помощью команды ping на удаленные узлы (расположенные за пределами локальной сети) и изучить данные, сформированные этими запросами. Затем вам нужно будет определить различия между этими данными и данными, которые вы изучали в части 1.

#### Шаг 1: Запустите захват данных в интерфейсе.

а. Нажмите на значок Interface List (Список интерфейсов), чтобы снова открыть список интерфейсов ПК.

Intel(R) PRO/1000 MT Network Connection [Wireshark 1.										
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> aptu	ure	<u>A</u> nal	yze	<u>S</u> tat	istics	Te
		1				×	Z	₿		. 4
Filter:	icm	р								
No.	Т	ime		Sour	ce				D	esti

b. Убедитесь, что напротив интерфейса локальной сети установлен флажок, и нажмите кнопку Start (Начать).

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	<u>D</u> etails		
-							
<u>H</u> elp		Start	Stop	<u>O</u> ptions	<u>C</u> lose		

с. Появится окно с предложением сохранить полученные ранее данные перед началом нового захвата. Сохранять эти данные необязательно. Нажмите Continue without Saving (Продолжить без сохранения).



- d. Активировав захват данных, отправьте эхо-запрос с помощью команды ping на следующие три URLадреса веб-сайтов:
  - 1) www.yahoo.com
  - 2) www.cisco.com
  - 3) www.google.com

```
- - -
C:\Windows\system32\cmd.exe
   :\>ping www.yahoo.com
   tinging www.yahoo.com [72.30.38.140] with 32 bytes of data:
eply from 72.30.38.140: bytes=32 time=1ms TTL=255
eply from 72.30.38.140: bytes=32 time(1ms TTL=255
eply from 72.30.38.140: bytes=32 time(1ms TTL=255
eply from 72.30.38.140: bytes=32 time(1ms TTL=255
                                                                                                                                   TTL=255
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 = 0ms, Maximum = 1ms, Average = 0ms
   >>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
                                                                                                                                         TTL=255
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 = 0ms, Maximum = 0ms, Average = 0ms
   :\>ping www.google.com
                                                                    [74.125.129.99] with 32 bytes of data:
99: bytes=32 time=1ms TTL=255
99: bytes=32 time(1ms TTL=255
99: bytes=32 time(1ms TTL=255
99: bytes=32 time(1ms TTL=255
  Pinging www.google.com [74
Reply from 74.125.129.99:
Reply from 74.125.129.99:
Reply from 74.125.129.99:
                  from
                                 74
                                           125
  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 = Ims, Average = Oms
   :\>_
```

**Примечание**. При отправке эхо-запросов с помощью команды ping на указанные URL-адреса обратите внимание на то, что служба доменных имен (DNS) преобразует адрес URL в IP-адрес. Запишите IP-адреса, полученные для каждого URL-адреса.

е. Остановите захват данных, нажав на значок Stop Capture (Остановить захват).



# Шаг 2: Изучите и проанализируйте данные, полученные от удаленных узлов.

а. Просмотрите собранные данные в программе Wireshark и изучите IP- и MAC-адреса трех веб-сайтов, на которые вы отправили эхо-запросы. Ниже в оставленном месте укажите IP- и MAC-адреса назначения для всех трех веб-сайтов.

1⁻й адрес:	IP:	_MAC:	_:	_:	_:	_:	_:
2 <sup>-й</sup> адрес:	IP:	_ MAC:	_:	_:	_:	_:	
З⁻й адрес:	IP:	_MAC:	_:	_:	_:	:	:

- b. Какова существенная особенность этих данных?
- с. Как эта информация отличается от данных, полученных в результате эхо-запросов локальных узлов в части 1?

# Вопросы для повторения

Почему программа Wireshark показывает фактические MAC-адреса локальных узлов, но не показывает фактические MAC-адреса удаленных узлов?