

Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ярославский государственный технический университет»
Кафедра «Информационные системы и технологии»

Отчет защищен
с оценкой _____
Преподаватель
А.Н. Вологин
«28» октября 2022

WIRESHARK

Отчет о лабораторной работе №4
по дисциплине «Компьютерные сети»

ЯГТУ 09.03.04 – 004 ЛР

Отчет выполнил
студент группы ЦПИ-21
Д.В. Аристов
«24» октября 2022

Цель работы: ознакомиться с работой программы Wireshark, найти и проанализировать посылаемые запросы. Научиться составлять фильтры.

Задание: найти протоколы ARP, HTTP, DNS, TCP, UDP, Telnet, ICMP

Wireshark – программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. Это приложение, которое «знает» структуру самых различных сетевых протоколов, и поэтому позволяет разобрать сетевой пакет, отображая значение каждого поля протокола любого уровня.

1) ARP

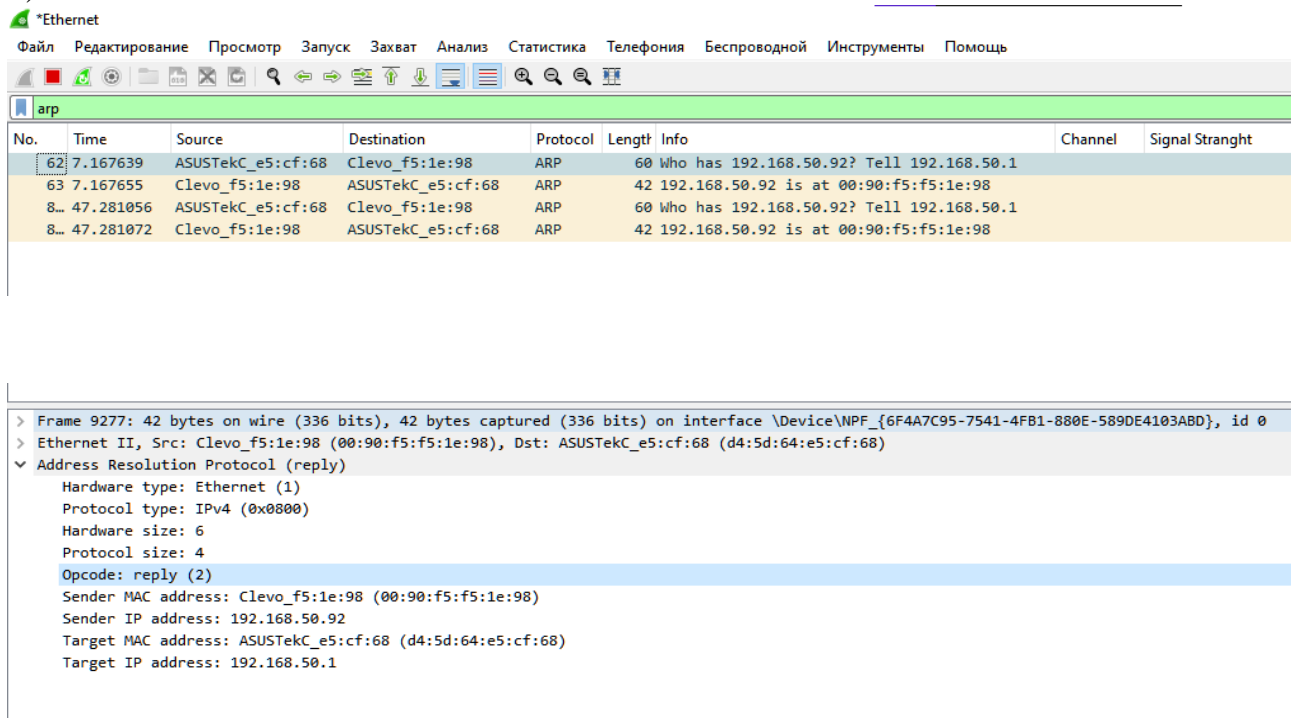


Рисунок 1 – протокол ARP

2) HTTP

HTTP — это протокол, позволяющий получать различные ресурсы, например HTML-документы. Протокол HTTP лежит в основе обмена данными в Интернете. HTTP является протоколом клиент-серверного взаимодействия, что означает инициирование запросов к серверу самим получателем, обычно веб-браузером.

*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

http

No.	Time	Source	Destination	Protocol	Length	Info	Channel	Signal Strength
1..	201.951997	192.168.50.92	91.105.192.100	HTTP	122	POST /api HTTP/1.1 (application/x-www-for...		
1..	206.368904	192.168.50.92	91.105.192.100	HTTP	246	POST /api HTTP/1.1 (application/x-www-for...		
1..	211.733878	192.168.50.92	91.105.192.100	HTTP	110	POST /api HTTP/1.1 (application/x-www-for...		
1..	215.280190	192.168.50.92	149.154.167.151	HTTP	110	POST /api HTTP/1.1 (application/x-www-for...		
1..	215.301004	192.168.50.92	149.154.167.151	HTTP	118	POST /api HTTP/1.1 (application/x-www-for...		
1..	215.309640	192.168.50.92	149.154.167.151	HTTP	230	POST /api HTTP/1.1 (application/x-www-for...		
1..	240.423964	192.168.50.92	149.154.167.151	HTTP	286	POST /api HTTP/1.1 (application/x-www-for...		
1..	245.693151	192.168.50.92	52.5.38.83	HTTP	427	GET /pulse?authon&user=3680991C6848BCC5D6C...		
1..	245.821901	52.5.38.83	192.168.50.92	HTTP	194	HTTP/1.1 200 OK		
1..	263.516772	192.168.50.92	149.154.167.151	HTTP	142	POST /api HTTP/1.1 (application/x-www-for...		
1..	278.801111	192.168.50.92	2.23.167.113	HTTP	341	GET /msdownload/update/v3/static/trustedr/...		
1..	278.809077	2.23.167.113	192.168.50.92	HTTP	321	HTTP/1.1 304 Not Modified		
1..	292.205818	192.168.50.92	91.105.192.100	HTTP	130	POST /api HTTP/1.1 (application/x-www-for...		
1..	292.206233	192.168.50.92	91.105.192.100	HTTP	170	POST /api HTTP/1.1 (application/x-www-for...		
1..	292.271258	192.168.50.92	91.105.192.100	HTTP	202	POST /api HTTP/1.1 (application/x-www-for...		
1..	298.814390	192.168.50.92	149.154.167.51	HTTP	134	POST /api HTTP/1.1 (application/x-www-for...		
1..	298.814446	192.168.50.92	149.154.167.41	HTTP	146	POST /api HTTP/1.1 (application/x-www-for...		
1..	305.685574	192.168.50.92	52.5.38.83	HTTP	427	GET /pulse?authon&user=3680991C6848BCC5D6C...		
1..	305.814240	52.5.38.83	192.168.50.92	HTTP	194	HTTP/1.1 200 OK		
1..	312.150532	192.168.50.92	91.105.192.100	HTTP	162	POST /api HTTP/1.1 (application/x-www-for...		
1..	312.166489	192.168.50.92	91.105.192.100	HTTP	98	POST /api HTTP/1.1 (application/x-www-for...		

> Frame 15391: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{6F4A7C95-7541-4FB1-880E-589DE4103ABD}, id 0
 > Ethernet II, Src: Clevo_f5:1e:98 (00:90:f5:f5:1e:98), Dst: ASUSTek_e5:cf:68 (d4:5d:64:e5:cf:68)
 > Internet Protocol Version 4, Src: 192.168.50.92, Dst: 149.154.167.151
 > Transmission Control Protocol, Src Port: 53066, Dst Port: 80, Seq: 228, Ack: 1, Len: 56
 > [2 Reassembled TCP Segments (283 bytes): #15389(227), #15391(56)]
 > Hypertext Transfer Protocol
 > POST /api HTTP/1.1\r\n
 Host: 149.154.167.151:80\r\n
 Content-Type: application/x-www-form-urlencoded\r\n
 > Content-Length: 56\r\n
 Connection: Keep-Alive\r\n
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: ru-RU,en,*\r\n
 User-Agent: Mozilla/5.0\r\n
 \r\n
 [Full request URI: http://149.154.167.151:80/api]
 [HTTP request 1/1]
 File Data: 56 bytes
 > HTML Form URL Encoded: application/x-www-form-urlencoded

Рисунок 2 – протокол HTTP

3) DNS

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Length	Info	Channel	Signal Strength
2..	471.309246	192.168.50.92	192.168.50.1	DNS	70	Standard query 0x90f8 A github.com		
2..	471.310891	192.168.50.1	192.168.50.92	DNS	86	Standard query response 0x90f8 A github.co...		
2..	482.048112	192.168.50.92	192.168.50.1	DNS	79	Standard query 0x4dd1 A alert-eu.battle.net		
2..	482.050037	192.168.50.1	192.168.50.92	DNS	231	Standard query response 0x4dd1 A alert-eu...		
2..	485.665339	192.168.50.92	192.168.50.1	DNS	82	Standard query 0x0c53 A lgcps-ru-nsdb.lest...		
2..	485.667186	192.168.50.1	192.168.50.92	DNS	144	Standard query response 0x0c53 A lgcps-ru-...		
2..	486.780848	192.168.50.92	192.168.50.1	DNS	90	Standard query 0xcec4 A self.events.data.m...		
2..	486.782561	192.168.50.1	192.168.50.92	DNS	208	Standard query response 0xcec4 A self.even...		
2..	494.022363	192.168.50.92	192.168.50.1	DNS	81	Standard query 0xad6e A collections.yandex...		
2..	494.023979	192.168.50.1	192.168.50.92	DNS	253	Standard query response 0xad6e A collectio...		
2..	497.836637	192.168.50.92	192.168.50.1	DNS	74	Standard query 0x7446 A portal.mail.ru		
2..	497.838477	192.168.50.1	192.168.50.92	DNS	308	Standard query response 0x7446 A portal.ma...		
2..	498.172304	192.168.50.92	192.168.50.1	DNS	70	Standard query 0xba18 A t.kite.com		
2..	498.174125	192.168.50.1	192.168.50.92	DNS	148	Standard query response 0xba18 No such nam...		
2..	498.516921	192.168.50.92	192.168.50.1	DNS	76	Standard query 0x5851 A windows.kite.com		
2..	498.518647	192.168.50.1	192.168.50.92	DNS	154	Standard query response 0x5851 No such nam...		
2..	515.277912	192.168.50.92	192.168.50.1	DNS	80	Standard query 0xbad6 A services.gismeteo...		
2..	515.278708	192.168.50.1	192.168.50.92	DNS	176	Standard query response 0xbad6 A services...		

> Frame 24109: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{6F4A7C95-7541-4FB1-880E-589DE4103ABD},
 > Ethernet II, Src: Clevo_f5:1e:98 (00:90:f5:f5:1e:98), Dst: ASUSTek_e5:cf:68 (d4:5d:64:e5:cf:68)
 > Internet Protocol Version 4, Src: 192.168.50.92, Dst: 192.168.50.1
 > User Datagram Protocol, Src Port: 58441, Dst Port: 53
 Source Port: 58441
 Destination Port: 53
 Length: 48
 Checksum: 0xe5ef [unverified]
 [Checksum Status: Unverified]
 [Stream index: 247]
 > [Timestamps]
 UDP payload (40 bytes)
 > Domain Name System (query)
 Transaction ID: 0x0c53
 > Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 [Response In: 24110]

Рисунок 3 – протокол DNS

4) TCP

tcp									
No.	Time	Source	Destination	Protocol	Length	Info	Channel	Signal	Stranght
3...	792.856035	91.105.192.100	192.168.50.92	TCP	60	443 → 53399 [ACK] Seq=328 Ack=685 Win=6876...			
3...	792.859673	91.105.192.100	192.168.50.92	TCP	66	443 → 53516 [SYN, ACK] Seq=0 Ack=1 Win=655...			
3...	792.859723	192.168.50.92	91.105.192.100	TCP	54	53516 → 443 [ACK] Seq=1 Ack=1 Win=131328 L...			
3...	792.860450	192.168.50.92	91.105.192.100	SSL	239	Continuation Data			
3...	792.861099	91.105.192.100	192.168.50.92	TCP	66	80 → 53517 [SYN, ACK] Seq=0 Ack=1 Win=6553...			
3...	792.861131	192.168.50.92	91.105.192.100	TCP	54	53517 → 80 [ACK] Seq=1 Ack=1 Win=131328 L...			
3...	792.869058	192.168.50.92	3.86.127.69	TCP	54	55166 → 9000 [ACK] Seq=1217 Ack=1027 Win=5...			
3...	792.871232	192.168.50.92	91.105.192.100	TCP	281	53517 → 80 [PSH, ACK] Seq=1 Ack=1 Win=1313...			
3...	792.882325	91.105.192.100	192.168.50.92	SSL	171	Continuation Data			
3...	792.883119	192.168.50.92	91.105.192.100	HTTP	330	POST /api HTTP/1.1 (application/x-www-for...			
3...	792.885646	192.168.50.92	91.105.192.100	SSL	351	Continuation Data			
3...	792.904715	91.105.192.100	192.168.50.92	TCP	60	80 → 53517 [RST, ACK] Seq=1 Ack=505 Win=67...			
3...	792.907697	91.105.192.100	192.168.50.92	SSL	223	Continuation Data			
3...	792.946992	192.168.50.92	91.105.192.100	TCP	54	53516 → 443 [ACK] Seq=483 Ack=287 Win=1310...			
3...	794.015180	192.168.50.92	192.168.50.72	TCP	164	51717 → 8009 [PSH, ACK] Seq=17491 Ack=1841...			
3...	794.017154	192.168.50.72	192.168.50.92	TCP	164	8009 → 51717 [PSH, ACK] Seq=18416 Ack=1760...			
3...	794.061237	192.168.50.92	192.168.50.72	TCP	54	51717 → 8009 [ACK] Seq=17601 Ack=18526 Win...			
3...	794.318691	162.159.134.234	192.168.50.92	TLSv1.2	192	Application Data			
3...	794.372135	192.168.50.92	162.159.134.234	TCP	54	63574 → 443 [ACK] Seq=1081 Ack=294071 Win=...			
3...	794.410133	162.159.134.234	192.168.50.92	TLSv1.2	276	Application Data			
3...	794.465487	192.168.50.92	162.159.134.234	TCP	54	63574 → 443 [ACK] Seq=1081 Ack=294293 Win=...			
3...	794.841950	162.159.134.234	192.168.50.92	TLSv1.2	575	Application Data			
3...	794.868807	162.159.134.234	192.168.50.92	TLSv1.2	273	Application Data			
3...	794.868855	192.168.50.92	162.159.134.234	TCP	54	63574 → 443 [ACK] Seq=1081 Ack=295033 Win=...			
3...	794.989847	192.168.50.92	91.105.192.100	SSL	159	Continuation Data			
3...	794.990042	192.168.50.92	91.105.192.100	SSL	351	Continuation Data			
3...	794.990171	192.168.50.92	91.105.192.100	SSL	191	Continuation Data			
3...	795.052504	91.105.192.100	192.168.50.92	TCP	60	443 → 53503 [ACK] Seq=371 Ack=776 Win=6876...			
3...	795.052938	91.105.192.100	192.168.50.92	TCP	60	443 → 53505 [ACK] Seq=271 Ack=560 Win=6768...			

> Frame 30995: 273 bytes on wire (2184 bits), 273 bytes captured (2184 bits) on interface \Device\NPF_{6F4A7C95-7541-4FB1-880E-589DE4103ABD}, id 0
 > Ethernet II, Src: ASUSTekC_e5:cf:68 (d4:5d:64:e5:cf:68), Dst: Clevo_f5:1e:98 (00:90:f5:f5:1e:98)
 > Internet Protocol Version 4, Src: 162.159.134.234, Dst: 192.168.50.92
 > Transmission Control Protocol, Src Port: 443, Dst Port: 63574, Seq: 294814, Ack: 1081, Len: 219
 > Transport Layer Security

Рисунок 4 – протокол TCP

5) UDP

udp									
No.	Time	Source	Destination	Protocol	Length	Info	Channel	Signal	Stranght
5...	11.157007	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.157184	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.157302	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.157302	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.157402	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.157546	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.157660	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.157771	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.157842	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.157986	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.158055	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.158072	192.168.50.92	109.195.121.76	UDP	75	51245 → 443 Len=33			
5...	11.158157	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.159378	192.168.50.92	109.195.121.76	UDP	76	51245 → 443 Len=34			
5...	11.159790	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.159902	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.160032	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.160118	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.160384	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.160384	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.160509	109.195.121.76	192.168.50.92	UDP	1292	443 → 51245 Len=1250			
5...	11.160509	109.195.121.76	192.168.50.92	UDP	255	443 → 51245 Len=213			
5...	11.160509	109.195.121.76	192.168.50.92	UDP	68	443 → 51245 Len=26			

> Frame 524: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF_{6F4A7C95-7541-4FB1-880E-589DE4103ABD}
 > Ethernet II, Src: ASUSTekC_e5:cf:68 (d4:5d:64:e5:cf:68), Dst: Clevo_f5:1e:98 (00:90:f5:f5:1e:98)
 > Internet Protocol Version 4, Src: 109.195.121.76, Dst: 192.168.50.92
 > User Datagram Protocol, Src Port: 443, Dst Port: 51245
 Source Port: 443
 Destination Port: 51245
 Length: 1258
 Checksum: 0x33b2 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 7]
 > [Timestamps]
 UDP payload (1250 bytes)
 > Data (1250 bytes)

Рисунок 5 – протокол UDP

6) Telnet

Telnet — это текстовый сетевой протокол, который позволяет клиенту общаться с удаленным компьютером.

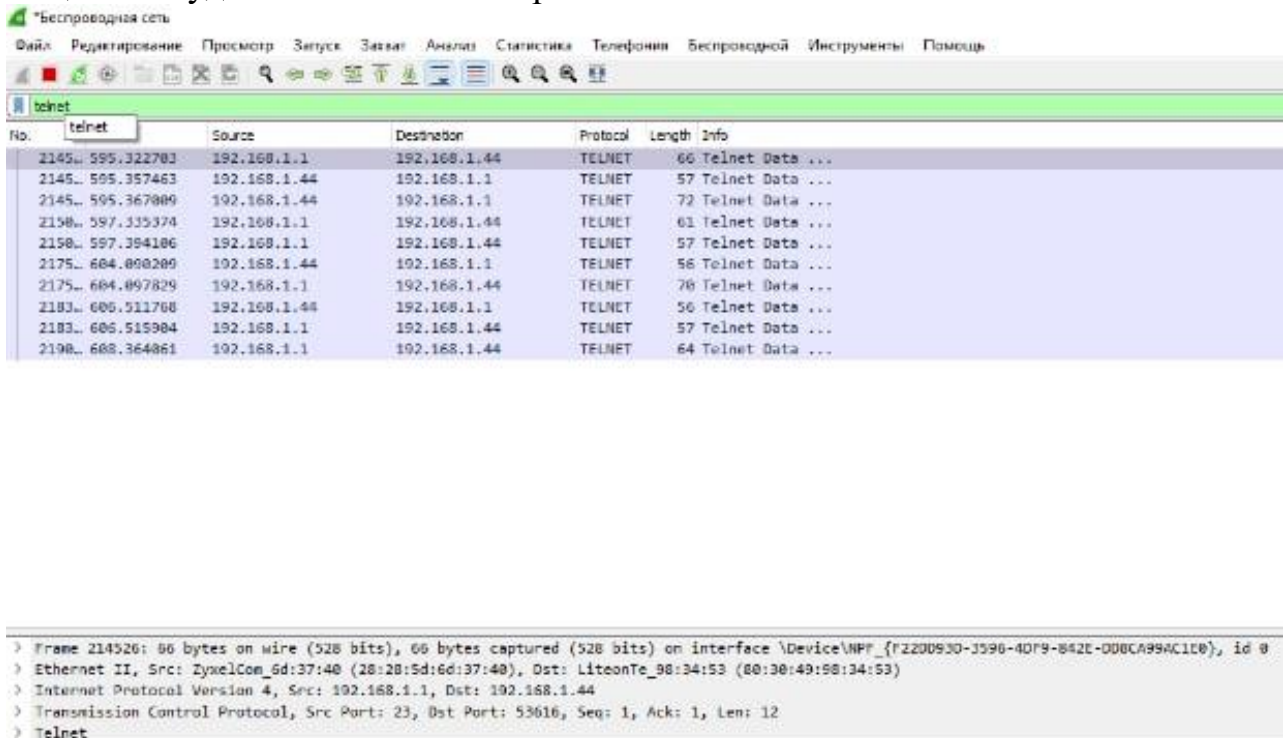


Рисунок 6 – протокол Telnet

7) ICMP

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

icmp

No.	Time	Source	Destination	Protocol	Length	Info	Channel	Si
1...	172.496841	212.33.255.84	192.168.50.92	ICMP	135	Destination unreachable (Port unreachable)		
1...	202.792633	222.189.206.2	192.168.50.92	ICMP	135	Destination unreachable (Port unreachable)		
1...	207.667152	199.36.223.180	192.168.50.92	ICMP	174	Destination unreachable (Port unreachable)		
1...	232.732191	92.43.185.50	192.168.50.92	ICMP	174	Destination unreachable (Host unreachable)		
1...	242.875675	39.184.78.95	192.168.50.92	ICMP	174	Destination unreachable (Port unreachable)		
1...	287.938543	113.88.230.125	192.168.50.92	ICMP	174	Destination unreachable (Port unreachable)		
1...	317.729844	94.75.27.48	192.168.50.92	ICMP	174	Destination unreachable (Port unreachable)		
2...	483.157671	27.4.194.177	192.168.50.92	ICMP	135	Destination unreachable (Port unreachable)		
2...	505.120883	192.168.50.92	5.167.85.250	ICMP	422	Echo (ping) request id=0x0001, seq=154/39...		
2...	505.133350	5.167.85.250	192.168.50.92	ICMP	422	Echo (ping) reply id=0x0001, seq=154/39...		
2...	506.137387	192.168.50.92	5.167.85.250	ICMP	422	Echo (ping) request id=0x0001, seq=155/39...		
2...	506.149860	5.167.85.250	192.168.50.92	ICMP	422	Echo (ping) reply id=0x0001, seq=155/39...		
2...	507.147514	192.168.50.92	5.167.85.250	ICMP	422	Echo (ping) request id=0x0001, seq=156/39...		
2...	507.160010	5.167.85.250	192.168.50.92	ICMP	422	Echo (ping) reply id=0x0001, seq=156/39...		
2...	508.157896	192.168.50.92	5.167.85.250	ICMP	422	Echo (ping) request id=0x0001, seq=157/40...		
2...	508.170329	5.167.85.250	192.168.50.92	ICMP	422	Echo (ping) reply id=0x0001, seq=157/40...		
2...	509.168422	192.168.50.92	5.167.85.250	ICMP	422	Echo (ping) request id=0x0001, seq=158/40...		
2...	509.180845	5.167.85.250	192.168.50.92	ICMP	422	Echo (ping) reply id=0x0001, seq=158/40...		

> Frame 25329: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface \Device\NPF_{6F4A7C95-7541-4FB1-880E-5...}

> Ethernet II, Src: ASUSTekC_e5:cf:68 (d4:5d:64:e5:cf:68), Dst: Clevo_f5:1e:98 (00:90:f5:f5:1e:98)

> Internet Protocol Version 4, Src: 5.167.85.250, Dst: 192.168.50.92

Internet Control Message Protocol

- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0x7ae1 [correct]
- [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 155 (0x009b)
- Sequence Number (LE): 39680 (0x9b00)
- [\[Request frame: 25284\]](#)
- [Response time: 12,473 ms]

> Data (65500 bytes)

Рисунок 7 – протокол ICMP

Вывод: в ходе данной лабораторной работы я ознакомился с программой Wireshark, нашел и проанализировал посылаемые запросы, научился составлять и работать с фильтрами.