МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
“БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ”
КАФЕДРА ИИТ

ОТЧЁТ

по лабораторной работе №6

«Анализ сетевого трафика и протоколов на базе WireShark»

Выполнил:

Студент 2 курса
группы ПО-9
Харитонович Захар Сергеевич

Проверил:

Савицкий Ю. В.

Брест 2023

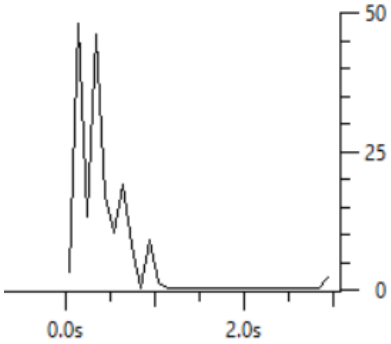
Вариант 1

Цель работы: приобретение навыков анализа сетевого трафика компьютерных сетей; изучение структуры сетевых протоколов различных уровней.

Ход работы

1. Изучить краткие теоретические сведения по возможностям, приемам работы с программой Wireshark (файл netWS.pdf).
2. Изучить: типы фильтрации трафика, правила построения фильтров, приемы статистической обработки сетевого трафика в Wireshark.
3. Запустив Wireshark на захват, выполнить загрузку страницы https://www.google.ru
4. Остановить и сохранить захват. Для захваченных пакетов определить статистические данные:

- процентное соотношение трафика разных протоколов в сети;
  UDP – 97.73% пакетов
  DNS – 2.27% пакетов
- среднюю скорость - 59.964 пакетов/сек;
- среднюю скорость – 34243.594 байт/сек;
- минимальный, максимальный и средний размеры пакета;
  минимальный – 24 байта
  максимальный – 1357 байт
  средний – 571.068 байт
- степень использования полосы пропускания канала (загрузку сети)



5. На примере третьего захваченного IP-пакета указать структуры протокола канального уровня (протокола Ethernet 802.3, Wi-Fi 802.11, либо другого, используемого в вашей конфигурации) и протокола IPv4.

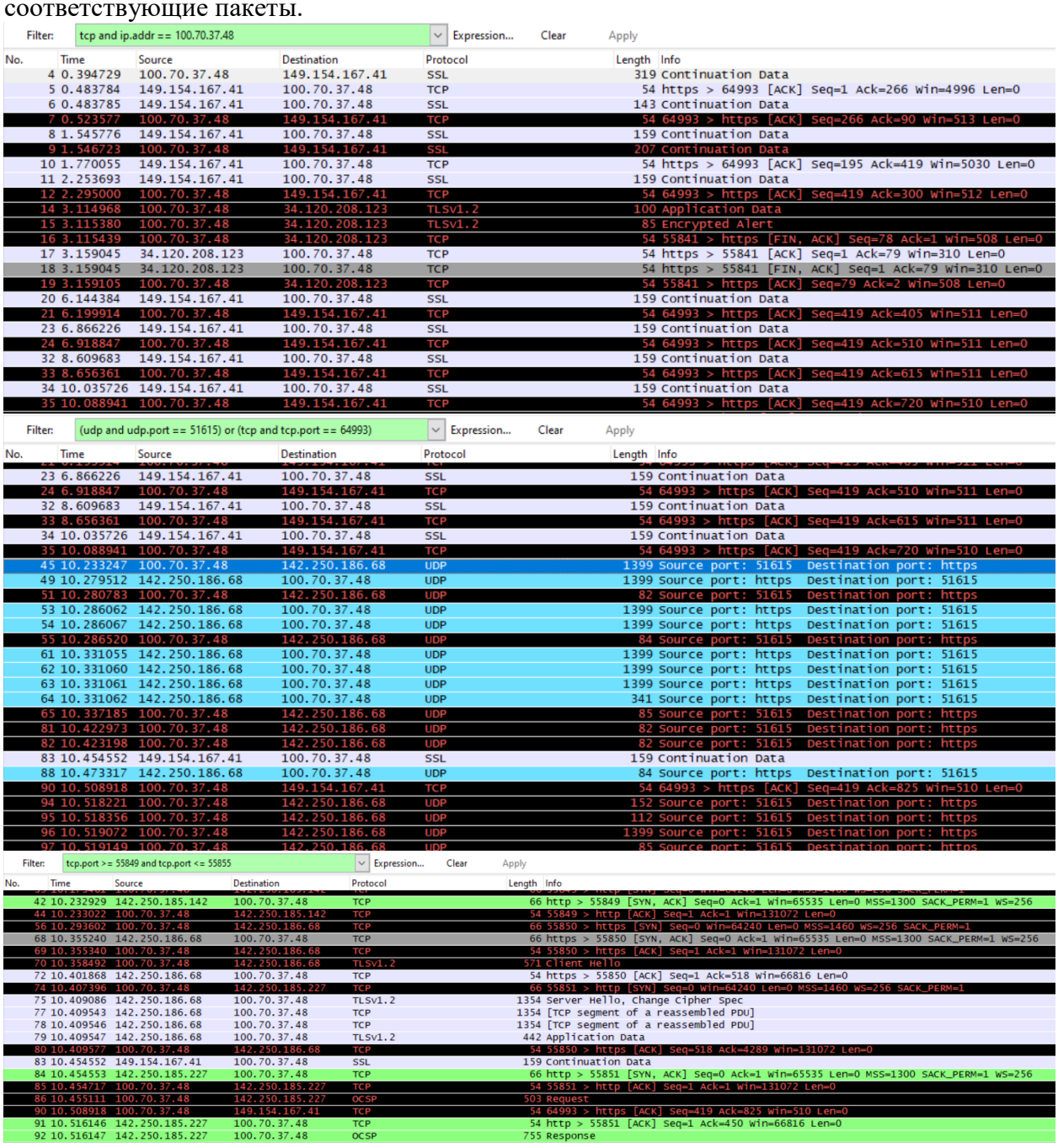
```
Ethernet II, Src: 10:51:07:57:4a:4a (10:51:07:57:4a:4a), Dst: 60:f1:8a:47:54:b2 (60:f1:8a:47:54:b2)
⊞ Destination: 60:f1:8a:47:54:b2 (60:f1:8a:47:54:b2)
⊞ Source: 10:51:07:57:4a:4a (10:51:07:57:4a:4a)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 192.168.100.44 (192.168.100.44), Dst: 142.250.75.4 (142.250.75.4)
  Version: 4
  Header length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 61
  Identification: 0xd2b4 (53940)
⊞ Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 65
  Protocol: UDP (17)
⊞ Header checksum: 0x0000 [incorrect, should be 0x6828 (maybe caused by "IP checksum offload"?)]
  Source: 192.168.100.44 (192.168.100.44)
  Destination: 142.250.75.4 (142.250.75.4)
```

6. Запустив Wireshark на захват, выполнить команду ping для IP адреса компьютера. Сохранить результат. Сформировав нужный фильтр, отфильтровать пакеты, относящиеся к выполнению команды ping.

Filter: ip.addr == 100.70.0.1 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	100.70.37.48	100.70.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=130/33280, ttl=128
2	0.013026	100.70.0.1	100.70.37.48	ICMP	74	Echo (ping) reply id=0x0001, seq=130/33280, ttl=255
4	1.006814	100.70.37.48	100.70.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=131/33536, ttl=128
5	1.019323	100.70.0.1	100.70.37.48	ICMP	74	Echo (ping) reply id=0x0001, seq=131/33536, ttl=255
6	2.026520	100.70.37.48	100.70.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=132/33792, ttl=128
7	2.038345	100.70.0.1	100.70.37.48	ICMP	74	Echo (ping) reply id=0x0001, seq=132/33792, ttl=255
10	3.032649	100.70.37.48	100.70.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=133/34048, ttl=128
11	3.045182	100.70.0.1	100.70.37.48	ICMP	74	Echo (ping) reply id=0x0001, seq=133/34048, ttl=255

7. Сформировать не менее 3-х сложных фильтров захвата с использованием полей протоколов, операторов сравнения (таблицы 1 и 2 из файла netWS.pdf) и логических операторов; каждый раз перезапуская захват, для каждого фильтра захватить соответствующие пакеты.



Filter: tcp and ip.addr == 100.70.37.48 — Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
4	0.394729	100.70.37.48	149.154.167.41	SSL	319	Continuation Data
5	0.483784	149.154.167.41	100.70.37.48	TCP	54	https > 64993 [ACK] Seq=1 Ack=266 Win=4996 Len=0
6	0.483785	149.154.167.41	100.70.37.48	SSL	143	Continuation Data
7	0.523577	100.70.37.48	149.154.167.41	TCP	54	64993 > https [ACK] Seq=266 Ack=90 Win=513 Len=0
8	1.545776	149.154.167.41	100.70.37.48	SSL	159	Continuation Data
9	1.546723	100.70.37.48	149.154.167.41	SSL	207	Continuation Data
10	1.770055	149.154.167.41	100.70.37.48	TCP	54	https > 64993 [ACK] Seq=195 Ack=419 Win=5030 Len=0
11	2.253693	149.154.167.41	100.70.37.48	SSL	159	Continuation Data
12	2.295000	100.70.37.48	149.154.167.41	TCP	54	64993 > https [ACK] Seq=419 Ack=300 Win=512 Len=0
14	3.114968	100.70.37.48	34.120.208.123	TLSv1.2	100	Application Data
15	3.115380	100.70.37.48	34.120.208.123	TLSv1.2	85	Encrypted Alert
16	3.115439	100.70.37.48	34.120.208.123	TCP	54	55841 > https [FIN, ACK] Seq=78 Ack=1 Win=508 Len=0
17	3.159045	34.120.208.123	100.70.37.48	TCP	54	https > 55841 [ACK] Seq=1 Ack=79 Win=310 Len=0
18	3.159045	34.120.208.123	100.70.37.48	TCP	54	https > 55841 [FIN, ACK] Seq=1 Ack=79 Win=310 Len=0
19	3.159105	100.70.37.48	34.120.208.123	TCP	54	55841 > https [ACK] Seq=79 Ack=2 Win=508 Len=0
20	6.144384	149.154.167.41	100.70.37.48	SSL	159	Continuation Data
21	6.199914	100.70.37.48	149.154.167.41	TCP	54	64993 > https [ACK] Seq=419 Ack=405 Win=511 Len=0
23	6.866226	149.154.167.41	100.70.37.48	SSL	159	Continuation Data
24	6.918847	100.70.37.48	149.154.167.41	TCP	54	64993 > https [ACK] Seq=419 Ack=510 Win=511 Len=0
32	8.609683	149.154.167.41	100.70.37.48	SSL	159	Continuation Data
33	8.656361	100.70.37.48	149.154.167.41	TCP	54	64993 > https [ACK] Seq=419 Ack=615 Win=511 Len=0
34	10.035726	149.154.167.41	100.70.37.48	SSL	159	Continuation Data
35	10.088941	100.70.37.48	149.154.167.41	TCP	54	64993 > https [ACK] Seq=419 Ack=720 Win=510 Len=0

Filter: (udp and udp.port == 51615) or (tcp and tcp.port == 64993) — Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
23	6.866226	149.154.167.41	100.70.37.48	SSL	159	Continuation Data
24	6.918847	100.70.37.48	149.154.167.41	TCP	54	64993 > https [ACK] Seq=419 Ack=510 Win=511 Len=0
32	8.609683	149.154.167.41	100.70.37.48	SSL	159	Continuation Data
33	8.656361	100.70.37.48	149.154.167.41	TCP	54	64993 > https [ACK] Seq=419 Ack=615 Win=511 Len=0
34	10.035726	149.154.167.41	100.70.37.48	SSL	159	Continuation Data
35	10.088941	100.70.37.48	149.154.167.41	TCP	54	64993 > https [ACK] Seq=419 Ack=720 Win=510 Len=0
45	10.233247	100.70.37.48	142.250.186.68	UDP	1399	Source port: 51615 Destination port: https
49	10.279512	142.250.186.68	100.70.37.48	UDP	1399	Source port: https Destination port: 51615
51	10.280783	100.70.37.48	142.250.186.68	UDP	82	Source port: 51615 Destination port: https
53	10.286062	142.250.186.68	100.70.37.48	UDP	1399	Source port: https Destination port: 51615
54	10.286067	142.250.186.68	100.70.37.48	UDP	1399	Source port: https Destination port: 51615
55	10.286520	100.70.37.48	142.250.186.68	UDP	84	Source port: 51615 Destination port: https
61	10.331055	142.250.186.68	100.70.37.48	UDP	1399	Source port: https Destination port: 51615
62	10.331060	142.250.186.68	100.70.37.48	UDP	1399	Source port: https Destination port: 51615
63	10.331061	142.250.186.68	100.70.37.48	UDP	1399	Source port: https Destination port: 51615
64	10.331062	142.250.186.68	100.70.37.48	UDP	341	Source port: https Destination port: 51615
65	10.337185	100.70.37.48	142.250.186.68	UDP	85	Source port: 51615 Destination port: https
81	10.422973	100.70.37.48	142.250.186.68	UDP	82	Source port: 51615 Destination port: https
82	10.423198	100.70.37.48	142.250.186.68	UDP	82	Source port: 51615 Destination port: https
83	10.454552	149.154.167.41	100.70.37.48	SSL	159	Continuation Data
88	10.473317	142.250.186.68	100.70.37.48	UDP	84	Source port: https Destination port: 51615
90	10.508918	100.70.37.48	149.154.167.41	TCP	54	64993 > https [ACK] Seq=419 Ack=825 Win=510 Len=0
94	10.518221	100.70.37.48	142.250.186.68	UDP	152	Source port: 51615 Destination port: https
95	10.518356	100.70.37.48	142.250.186.68	UDP	112	Source port: 51615 Destination port: https
96	10.519072	100.70.37.48	142.250.186.68	UDP	1399	Source port: 51615 Destination port: https
97	10.519149	100.70.37.48	142.250.186.68	UDP	85	Source port: 51615 Destination port: https

Filter: tcp.port >= 55849 and tcp.port <= 55855 — Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
42	10.232929	142.250.185.142	100.70.37.48	TCP	66	http > 55849 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 SACK_PERM=1 WS=256
44	10.233022	100.70.37.48	142.250.185.142	TCP	54	55849 > http [ACK] Seq=1 Ack=1 Win=131072 Len=0
56	10.293602	100.70.37.48	142.250.186.68	TCP	66	55850 > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
68	10.355240	142.250.186.68	100.70.37.48	TCP	66	https > 55850 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 SACK_PERM=1 WS=256
69	10.355340	100.70.37.48	142.250.186.68	TCP	54	55850 > https [ACK] Seq=1 Ack=1 Win=131072 Len=0
70	10.358492	100.70.37.48	142.250.186.68	TLSv1.2	571	Client Hello
72	10.401868	142.250.186.68	100.70.37.48	TCP	54	https > 55850 [ACK] Seq=1 Ack=518 Win=66816 Len=0
74	10.407396	100.70.37.48	142.250.185.227	TCP	66	55851 > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
75	10.409086	142.250.186.68	100.70.37.48	TLSv1.2	1354	Server Hello, Change Cipher Spec
77	10.409543	142.250.186.68	100.70.37.48	TCP	1354	[TCP segment of a reassembled PDU]
78	10.409546	142.250.186.68	100.70.37.48	TCP	1354	[TCP segment of a reassembled PDU]
79	10.409547	142.250.186.68	100.70.37.48	TLSv1.2	442	Application Data
80	10.409577	100.70.37.48	142.250.186.68	TCP	54	55850 > https [ACK] Seq=518 Ack=4289 Win=131072 Len=0
83	10.454552	149.154.167.41	100.70.37.48	SSL	159	Continuation Data
84	10.454553	142.250.185.227	100.70.37.48	TCP	66	http > 55851 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 SACK_PERM=1 WS=256
85	10.454717	100.70.37.48	142.250.185.227	TCP	54	55851 > http [ACK] Seq=1 Ack=1 Win=131072 Len=0
86	10.455111	100.70.37.48	142.250.185.227	OCSP	503	Request
90	10.508918	100.70.37.48	149.154.167.41	TCP	54	64993 > https [ACK] Seq=419 Ack=825 Win=510 Len=0
91	10.516146	142.250.185.227	100.70.37.48	TCP	54	http > 55851 [ACK] Seq=1 Ack=450 Win=66816 Len=0
92	10.516147	142.250.185.227	100.70.37.48	OCSP	755	Response

8. Выполнить анализ ARP-протокола по примеру из методических указаний.

Запрос

```
Sender MAC address: 10:51:07:57:4a:4a (10:51:07:57:4a:4a)
Sender IP address: 100.70.37.48 (100.70.37.48)
Target MAC address: UscInfor_00:52:13 (00:00:5e:00:52:13)
Target IP address: 100.70.0.1 (100.70.0.1)
```

Ответ

```
Sender MAC address: UscInfor_00:52:13 (00:00:5e:00:52:13)
Sender IP address: 100.70.0.1 (100.70.0.1)
Target MAC address: 10:51:07:57:4a:4a (10:51:07:57:4a:4a)
Target IP address: 100.70.37.48 (100.70.37.48)
```

9. Выполнить анализ TCP-сеансов по примеру из методических указаний

TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	bps A→B	bps A←B
100.70.37.48	64993	149.154.167.41	https	147	24 880	68	8 691	79	16 189	0.394729000	165.1353	421.04	784.28
100.70.37.48	55841	34.120.208.123	https	6	401	4	293	2	108	3.114968000	0.0441	53107.37	19575.41
100.70.37.48	55849	142.250.185.142	http	6	348	4	228	2	120	10.173461000	5.1167	356.48	187.62
100.70.37.48	55843	35.241.9.150	https	13	963	8	601	5	362	10.259657000	112.7817	42.63	25.68
100.70.37.48	55850	142.250.186.68	https	25	7 245	12	1 520	13	5 725	10.293602000	117.9795	103.07	388.20
100.70.37.48	55851	142.250.185.227	http	55	11 191	28	4 680	27	6 511	10.407396000	118.6377	315.58	439.05
100.70.37.48	55852	142.250.185.227	http	32	3 045	17	1 390	15	1 655	10.543510000	118.5014	93.84	111.73
100.70.37.48	55853	34.120.208.123	https	19	5 419	10	1 081	9	4 338	10.776501000	0.1980	43667.50	175235.56
100.70.37.48	55854	34.120.208.123	https	37	7 122	18	3 884	19	3 238	10.781114000	117.4919	264.46	220.47
100.70.37.48	55855	142.250.184.225	https	27	11 343	12	1 520	15	9 823	11.049624000	117.2233	103.73	670.38
100.70.37.48	55856	142.250.186.67	https	24	7 223	12	1 520	12	5 703	11.218745000	117.0544	103.88	389.77
100.70.37.48	55857	142.250.186.46	https	24	7 214	12	1 520	12	5 694	11.638315000	117.6301	103.37	387.25

Вывод: приобретены навыки анализа сетевого трафика компьютерных сетей; изучены структуры сетевых протоколов различных уровней.