

Лабораторная работа №3

Анализ трафика в Wireshark

Лисовская А. В.

18 декабря 2025

Российский университет дружбы народов, Москва, Россия

:::::::::::: { .columns align=center } ::: { .column width="70%" }

- Лисовская Арина Валерьевна
- Студент учебной группы
- Российский университет дружбы народов

::: ::: { .column width="30%" }

Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

1. Изучить сетевые настройки ОС (`ipconfig`, `getmac`).
2. Проанализировать работу протоколов ICMP и ARP.
3. Исследовать структуру HTTP-трафика.
4. Провести анализ процесса установления соединения (handshake) TCP.

Выполнение работы: Сетевые настройки

Изучение конфигурации IP

Команда `ipconfig /all` выводит детальную информацию о сетевых интерфейсах: имя компьютера, настройки DHCP и IPv6-адрес канала.

```
PS C:\Users\Арина> ipconfig /all
```

```
Настройка протокола IP для Windows
```

```
Имя компьютера . . . . . : LAPTOP-5GUQC0PM
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . . : Нет
WINS-прокси включен . . . . . : Нет
Порядок просмотра суффиксов DNS . : rudn.ru
```

```
Адаптер Ethernet Ethernet 2:
```

```
DNS-суффикс подключения . . . . . :
Описание. . . . . : VirtualBox Host-Only Ethernet Adapter
Физический адрес. . . . . : 0A-00-27-00-00-03
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::154b:8e54:709f:48cf
```

Определение MAC-адресов

С помощью утилиты GETMAC были определены физические адреса сетевых адаптеров и их текущее состояние (подключен/отключен).

```
C:\WINDOWS\system32> GETMAC
```

физический адрес	Имя транспорта
------------------	----------------

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

```
0-F6-0A-33-73-8B \Device\Tcpip {D4AE9452-96DB-4762-9A46-8F3DDDAC91D2}
```

```
A-00-27-00-00-03 \Device\Tcpip_{2CEC490E-8B81-4A89-8358-1B80945FC152}
```

00-FF-2F-C5-AC-F9 Носитель отключен

```
S C:\WINDOWS\system32>
```

Рис. 2: Вывод GETMAC

Сведения о подключении (GUI)

Параметры сетевого адаптера Intel Wi-Fi и адрес шлюза (192.168.192.1) подтверждены через графический интерфейс ОС Windows.

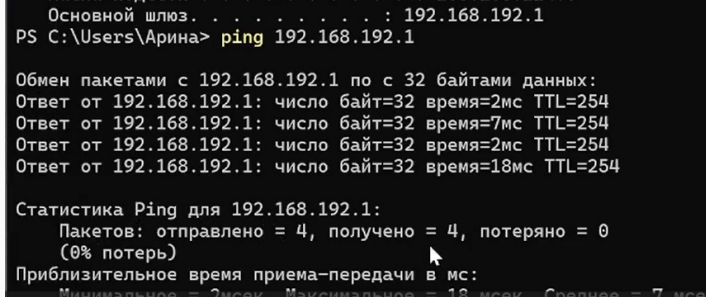
The image shows a Windows desktop environment. In the background, a black command prompt window displays the command `C:\WINDOWS\system32> GETMAC`. In the foreground, there are two windows. On the left is the 'Сведения о сетевом подключении' (Network Connection Information) window, which shows the status of the network connection as 'Подключено' (Connected) and displays the IP address '192.168.192.1'. On the right is the 'Сведения о сетевом подключении' (Network Connection Information) window, which displays the details of the network connection, including the adapter name 'Intel(R) Wi-Fi 6 AX201 160MHz', the physical address '10-F6-0A-33-73-8B', and the IP address '192.168.192.1'. The 'DHCP-сервер IPv4' (IPv4 DHCP Server) is highlighted in blue, showing the address '192.168.192.3'.

Сведения о сетевом подключении

Свойство	Значение
Определенный для по...	rudn.ru
Описание	Intel(R) Wi-Fi 6 AX201 160MHz
Физический адрес	10-F6-0A-33-73-8B
DHCP включен	Да
Адрес IPv4	192.168.192.1
Маска подсети IPv4	255.255.255.0
Аренда получена	11 октября 2025 г. 18:48:08
Аренда истекает	11 октября 2025 г. 22:27:35
Шлюз по умолчанию IPv4	192.168.192.1
DHCP-сервер IPv4	192.168.192.3
DNS серверы IPv4	192.168.80.63 37.18.92.6
WINS сервер IPv4	

Выполнение работы: Анализ трафика

В Wireshark проанализирована структура кадра Ethernet II. На скриншоте виден эхо-запрос от клиента к шлюзу и ответный пакет.



```
Основной шлюз. . . . . : 192.168.192.1
PS C:\Users\Арина> ping 192.168.192.1

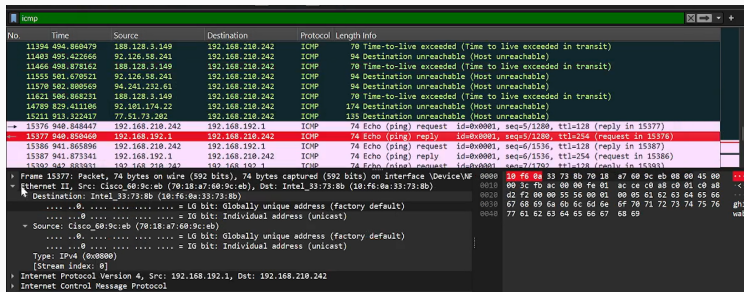
Обмен пакетами с 192.168.192.1 по 32 байтами данных:
Ответ от 192.168.192.1: число байт=32 время=2мс TTL=254
Ответ от 192.168.192.1: число байт=32 время=7мс TTL=254
Ответ от 192.168.192.1: число байт=32 время=2мс TTL=254
Ответ от 192.168.192.1: число байт=32 время=18мс TTL=254

Статистика Ping для 192.168.192.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2 мсек, Максимальное = 18 мсек, Среднее = 7 мсек
```

Рис. 4: Анализ ICMP в Wireshark

Пинг внешнего ресурса

Выполнен запрос к домену rudn.ru. IP-адрес узла — 192.168.80.63. Это действие позволило зафиксировать процесс разрешения имен.



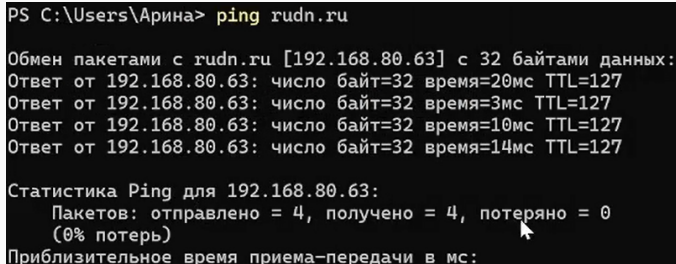
The screenshot shows a network packet capture tool window titled 'icmp'. It displays a list of ICMP packets with columns for No., Time, Source, Destination, Protocol, and Length. The list includes several 'Time-to-live exceeded' and 'Destination unreachable' messages, followed by a successful ping request and reply. The selected packet (No. 15377) is highlighted in red. Below the list, the packet details for the selected packet are shown, including the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol header.

No.	Time	Source	Destination	Protocol	Length	Info
11394	494.860479	188.128.3.149	192.168.210.242	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
11403	495.422666	92.126.58.241	192.168.210.242	ICMP	94	Destination unreachable (Host unreachable)
11466	498.876162	188.128.3.149	192.168.210.242	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
11555	501.670521	92.126.58.241	192.168.210.242	ICMP	94	Destination unreachable (Host unreachable)
11570	502.800569	94.241.232.61	192.168.210.242	ICMP	94	Destination unreachable (Host unreachable)
11621	506.868231	188.128.3.149	192.168.210.242	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14789	829.411106	92.101.174.22	192.168.210.242	ICMP	174	Destination unreachable (Host unreachable)
15211	913.322417	77.51.73.202	192.168.210.242	ICMP	135	Destination unreachable (Host unreachable)
→ 15376	940.840447	192.168.210.242	192.168.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 15377)
← 15377	940.850460	192.168.192.1	192.168.210.242	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=254 (request in 15376)
→ 15386	941.865896	192.168.210.242	192.168.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 15387)
→ 15387	941.873341	192.168.192.1	192.168.210.242	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=254 (request in 15386)
→ 15392	942.880031	192.168.210.242	192.168.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 15393)

Frame 15377: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF...
Ethernet II, Src: Cisco_60:9c:eb (70:18:a7:60:9c:eb), Dst: Intel_33:73:8b (10:f6:0e:33:73:8b)
Destination: Intel_33:73:8b (10:f6:0e:33:73:8b)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
Source: Cisco_60:9c:eb (70:18:a7:60:9c:eb)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
Type: IPv4 (0x0000)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.192.1, Dst: 192.168.210.242
Internet Control Message Protocol

Рис. 5: Пинг rudn.ru

Пример широковещательного ARP-пакета (Gratuitous ARP). Использовался для обновления информации о физическом адресе в локальной сети.



```
PS C:\Users\Арина> ping rudn.ru

Обмен пакетами с rudn.ru [192.168.80.63] с 32 байтами данных:
Ответ от 192.168.80.63: число байт=32 время=20мс TTL=127
Ответ от 192.168.80.63: число байт=32 время=3мс TTL=127
Ответ от 192.168.80.63: число байт=32 время=10мс TTL=127
Ответ от 192.168.80.63: число байт=32 время=14мс TTL=127

Статистика Ping для 192.168.80.63:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
```

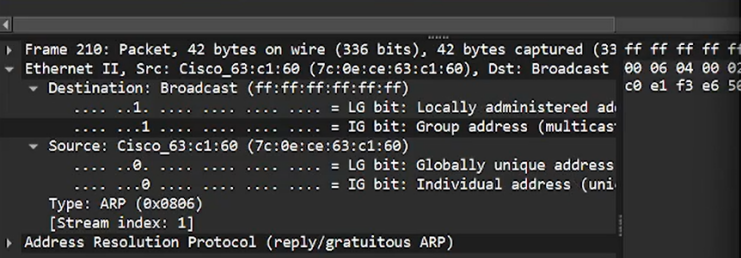
Рис. 6: Захват ARP

Выполнение работы: TCP и HTTP

Работа с протоколом НТТР

Для генерации трафика прикладного уровня осуществлен переход на сайт `info.cern.ch`. Зафиксированы GET-запросы и ответы сервера.

No.	Time	Source	Destination	Protocol	Length	Info
210	2.546276	Cisco_63:c1:60	Broadcast	ARP	42	Gratui
395	6.824311	Cisco_63:c1:60	Broadcast	ARP	42	Gratui
747	21.873208	Cisco_63:c1:60	Broadcast	ARP	42	Gratui
779	27.848223	Intel_33:73:8b	Cisco_60:9c:eb	ARP	42	Who ha
780	27.850702	Cisco_60:9c:eb	Intel_33:73:8b	ARP	60	192.16
848	45.267253	Cisco_63:c1:60	Broadcast	ARP	42	Gratui



```
Frame 210: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: Cisco_63:c1:60 (7c:0e:ce:63:c1:60), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    .... 1. .... = LG bit: Locally administered address (this is only for interfaces without permanent addresses)
    .... 1. .... = IG bit: Group address (multicast/broadcast only)
  Source: Cisco_63:c1:60 (7c:0e:ce:63:c1:60)
    .... 0. .... = LG bit: Globally unique address (reserved for IEEE 802.11)
    .... 0. .... = IG bit: Individual address (unicast only)
  Type: ARP (0x0806)
  [Stream index: 1]
Address Resolution Protocol (reply/gratuitous ARP)
```

Рис. 7: Сайт `info.cern.ch`

Анализ TCP Handshake

Наглядная иллюстрация установления соединения. Видны флаги SYN от клиента, SYN-ACK от сервера и завершающий ACK от клиента.

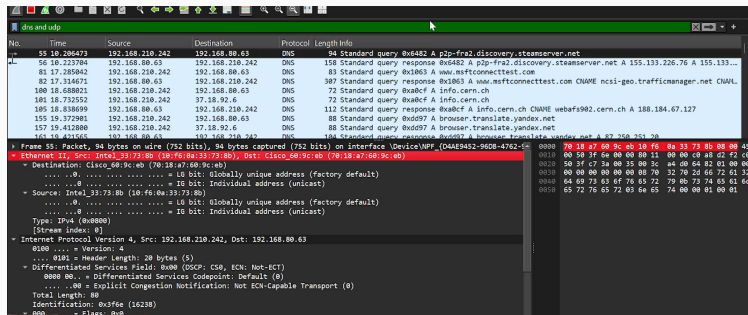


Рис. 8: TCP Handshake

- Освоены практические навыки работы в Wireshark.
- Изучена структура кадров канального и пакетов сетевого уровней.
- Проанализирован процесс «трехступенчатого рукопожатия» TCP.
- Научился определять OUI производителя по MAC-адресу.