

Анализ трафика

Основы Веб-программирования

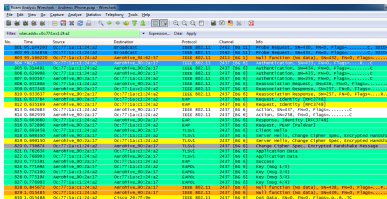
Кафедра Интеллектуальных Информационных Технологий, ИнФО, УрФУ

<http://www.tcpdump.org/>

<https://www.wireshark.org/>

<https://lecturesnet.readthedocs.org/net/sniff.html>

Классификация анализаторов



No.	Date	Source	Destination	Protocol	Channel	Info
100	06.10.2016 10:17:12.1214	192.168.1.10	192.168.1.1	TCP	100	192.168.1.10 -> 192.168.1.1 [RST] Seq=1234567890 Win=0 Len=0
101	06.10.2016 10:17:12.1214	192.168.1.1	192.168.1.10	TCP	101	192.168.1.1 -> 192.168.1.10 [ACK] Seq=9876543210 Win=0 Len=0
102	06.10.2016 10:17:12.1214	192.168.1.10	192.168.1.1	TCP	102	192.168.1.10 -> 192.168.1.1 [ACK] Seq=1234567890 Win=0 Len=0
103	06.10.2016 10:17:12.1214	192.168.1.1	192.168.1.10	TCP	103	192.168.1.1 -> 192.168.1.10 [ACK] Seq=9876543210 Win=0 Len=0
104	06.10.2016 10:17:12.1214	192.168.1.10	192.168.1.1	TCP	104	192.168.1.10 -> 192.168.1.1 [ACK] Seq=1234567890 Win=0 Len=0
105	06.10.2016 10:17:12.1214	192.168.1.1	192.168.1.10	TCP	105	192.168.1.1 -> 192.168.1.10 [ACK] Seq=9876543210 Win=0 Len=0
106	06.10.2016 10:17:12.1214	192.168.1.10	192.168.1.1	TCP	106	192.168.1.10 -> 192.168.1.1 [ACK] Seq=1234567890 Win=0 Len=0
107	06.10.2016 10:17:12.1214	192.168.1.1	192.168.1.10	TCP	107	192.168.1.1 -> 192.168.1.10 [ACK] Seq=9876543210 Win=0 Len=0
108	06.10.2016 10:17:12.1214	192.168.1.10	192.168.1.1	TCP	108	192.168.1.10 -> 192.168.1.1 [ACK] Seq=1234567890 Win=0 Len=0
109	06.10.2016 10:17:12.1214	192.168.1.1	192.168.1.10	TCP	109	192.168.1.1 -> 192.168.1.10 [ACK] Seq=9876543210 Win=0 Len=0
110	06.10.2016 10:17:12.1214	192.168.1.10	192.168.1.1	TCP	110	192.168.1.10 -> 192.168.1.1 [ACK] Seq=1234567890 Win=0 Len=0
111	06.10.2016 10:17:12.1214	192.168.1.1	192.168.1.10	TCP	111	192.168.1.1 -> 192.168.1.10 [ACK] Seq=9876543210 Win=0 Len=0
112	06.10.2016 10:17:12.1214	192.168.1.10	192.168.1.1	TCP	112	192.168.1.10 -> 192.168.1.1 [ACK] Seq=1234567890 Win=0 Len=0
113	06.10.2016 10:17:12.1214	192.168.1.1	192.168.1.10	TCP	113	192.168.1.1 -> 192.168.1.10 [ACK] Seq=9876543210 Win=0 Len=0
114	06.10.2016 10:17:12.1214	192.168.1.10	192.168.1.1	TCP	114	192.168.1.10 -> 192.168.1.1 [ACK] Seq=1234567890 Win=0 Len=0
115	06.10.2016 10:17:12.1214	192.168.1.1	192.168.1.10	TCP	115	192.168.1.1 -> 192.168.1.10 [ACK] Seq=9876543210 Win=0 Len=0
116	06.10.2016 10:17:12.1214	192.168.1.10	192.168.1.1	TCP	116	192.168.1.10 -> 192.168.1.1 [ACK] Seq=1234567890 Win=0 Len=0
117	06.10.2016 10:17:12.1214	192.168.1.1	192.168.1.10	TCP	117	192.168.1.1 -> 192.168.1.10 [ACK] Seq=9876543210 Win=0 Len=0
118	06.10.2016 10:17:12.1214	192.168.1.10	192.168.1.1	TCP	118	192.168.1.10 -> 192.168.1.1 [ACK] Seq=1234567890 Win=0 Len=0
119	06.10.2016 10:17:12.1214	192.168.1.1	192.168.1.10	TCP	119	192.168.1.1 -> 192.168.1.10 [ACK] Seq=9876543210 Win=0 Len=0
120	06.10.2016 10:17:12.1214	192.168.1.10	192.168.1.1	TCP	120	192.168.1.10 -> 192.168.1.1 [ACK] Seq=1234567890 Win=0 Len=0



- программные
- программно-аппаратные

Способы перехвата

- Обычным «прослушиванием» сетевого интерфейса;
- Ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер (Network tap);
- Через анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика;
- Через атаку на канальном 2-ом (MAC-spoofing) уровне;
- Через атаку на канальном сетевом 3-м (IP-spoofing) уровне.

tcpdump — утилита UNIX (есть клон для Windows), позволяющая перехватывать и анализировать сетевой трафик, проходящий через компьютер, на котором запущена данная программа.

Просмотр интерфейсов

```
$ sudo tcpdump -D
1.wlan0 [Up, Running]
2.docker0 [Up, Running]
3.vboxnet0 [Up, Running]
4.vboxnet1 [Up, Running]
5.veth283f985 [Up, Running]
6.any (Pseudo-device that captures on all interfaces) [Up, Running]
7.lo [Up, Running, Loopback]
8.eth0 [Up]
9.bluetooth-monitor (Bluetooth Linux Monitor)
10.nflog (Linux netfilter log (NFLOG) interface)
11.nfqueue (Linux netfilter queue (NFQUEUE) interface)
12.usbmon1 (USB bus number 1)
13.usbmon2 (USB bus number 2)
```

Все запросы с интерфейса

```
$ sudo tcpdump -i wlan0
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on wlan0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
19:04:24.115872 STP 802.1d, Config, Flags [none], bridge-id 8000.bc:ae:c5:88:91:28.8
```

```
19:04:24.219665 IP Arkasha-PC.local.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Req
```

```
19:04:25.118303 IP x220t.local.32371 > google-public-dns-a.google.com.domain: 29524+
```

```
19:04:25.186526 IP google-public-dns-a.google.com.domain > x220t.local.32371: 29524
```

```
19:04:25.287550 IP6 fe80::120b:a9ff:fe0c:f638.mdns > ff02::fb.mdns: 0 PTR (QM)? 255.
```

```
^C19:04:25.287614 IP x220t.local.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 255.255.255.25
```

```
6 packets captured
```

```
50 packets received by filter
```

```
0 packets dropped by kernel
```

Фильтр по хосту

```
$ sudo tcpdump host readthedocs.org
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:08:24.734572 IP x220t.local.44169 > readthedocs.org.http: Flags [S], seq 16304875
19:08:24.900671 IP readthedocs.org.http > x220t.local.44169: Flags [S.], seq 2780774
19:08:24.900718 IP x220t.local.44169 > readthedocs.org.http: Flags [.], ack 1, win 1
19:08:24.900812 IP x220t.local.44169 > readthedocs.org.http: Flags [P.], seq 1:733,
...
    19:08:28.524595 IP readthedocs.org.https > x220t.local.37282: Flags [.], ack 2254,
19:08:28.605826 IP x220t.local.37282 > readthedocs.org.https: Flags [.], ack 9767, w
^C
83 packets captured
89 packets received by filter
0 packets dropped by kernel
```


Ещё фильтры

По протоколу:

```
$ sudo tcpdump -n tcp
```

По назначению:

```
$ sudo tcpdump -n 'src 192.168.1.101'
```

Только DNS пакеты:

```
$ sudo tcpdump -n 'udp and dst port 53'
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on wlan0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
19:22:52.089174 IP 192.168.1.101.17166 > 8.8.8.8.53: 44241+ A? www.google.ru. (31)
```

```
19:22:52.149972 IP 192.168.1.101.61715 > 8.8.8.8.53: 63972+ A? www.google.ru. (31)
```

```
19:22:52.157017 IP 192.168.1.101.12023 > 8.8.8.8.53: 17412+ AAAA? www.google.ru. (31)
```

```
19:22:54.062859 IP 192.168.1.101.30447 > 8.8.8.8.53: 54230+ AAAA? www.google.ru. (31)
```

ПОИСК ХОСТОВ

NetBIOS:

```
$ nbtscan 192.168.1.0/24
```

```
Doing NBT name scan for addresses from 192.168.1.0/24
```

IP address	NetBIOS Name	Server	User	MAC address
192.168.1.0	Sendto failed: Permission denied			
192.168.1.101	X220T	<server>	X220T	00:00:00:00:00:00
192.168.1.23		<server>		00:00:00:00:00:00
192.168.1.22	ARKASHA-PC	<server>	<unknown>	00:1b:fc:6c:c2:12
192.168.1.255	Sendto failed: Permission denied			

Nmap:

```
$ nmap -sP 192.168.1.*
```

```
Starting Nmap 6.46 ( http://nmap.org ) at 2015-02-02 20:56 YEKT
```

```
Nmap scan report for 192.168.1.1
```

```
Host is up (0.0068s latency).
```

```
Nmap scan report for 192.168.1.20
```

```
Host is up (0.018s latency).
```

Только ICMP пакеты (ping)

```
$ sudo tcpdump 'src 192.168.1.101 and dst 192.168.1.23 and icmp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:36:45.340321 IP x220t.local > 192.168.1.23: ICMP echo request, id 10305, seq 1, l
19:36:46.341472 IP x220t.local > 192.168.1.23: ICMP echo request, id 10305, seq 2, l
19:36:47.342180 IP x220t.local > 192.168.1.23: ICMP echo request, id 10305, seq 3, l
19:36:48.343557 IP x220t.local > 192.168.1.23: ICMP echo request, id 10305, seq 4, l
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
```

HTTP ответы со статусом 200

```
$ sudo tcpdump -n -A | grep -e '200 OK'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), capture size 262144 bytes
A)...sHTTP/1.1 200 OK
A).9...vHTTP/1.1 200 OK
```

Поиск логинов и паролей

```
$ sudo tcpdump -l -A -i lo | egrep -i 'pass=|pwd=|log=|login=|user=
|username=|pw=|passw=|passwd=|password=|pass:|user:|username:
|password:|login:|pass |user ' --color=auto --line-buffered -B20
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
Host: localhost:6543
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:35.0) Gecko/20100101 Firefox/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost:6543/login/
Cookie: csrftoken=pVVycxJs2YaTCS5vpKTob0TINGsKjAM4; _LOCALE_=ru; _ga=GA1.1.195145305
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 53

came_from=%2F&login=admin&password=123&submit=Sign+In
```

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **icmp** Expression... Clear Apply Сохранить

No.	Time	Source	Destination	Protocol	Length	Info
13190	62.528523806	192.168.1.111	192.168.0.111	ICMP	98	Echo (ping) request id=0x5981, seq=1/256, ttl=64 (no response found!)
13485	63.537046006	192.168.1.111	192.168.0.111	ICMP	98	Echo (ping) request id=0x5981, seq=2/512, ttl=64 (no response found!)
13621	64.544779006	192.168.1.111	192.168.0.111	ICMP	98	Echo (ping) request id=0x5981, seq=3/768, ttl=64 (no response found!)
13825	65.552792006	192.168.1.111	192.168.0.111	ICMP	98	Echo (ping) request id=0x5981, seq=4/1024, ttl=64 (no response found!)
14042	66.561018006	192.168.1.111	192.168.0.111	ICMP	98	Echo (ping) request id=0x5981, seq=5/1280, ttl=64 (no response found!)
19899	94.841887006	192.168.1.28	192.168.1.111	ICMP	98	Echo (ping) request id=0x1f97, seq=1/256, ttl=64 (reply in 19902)
19902	94.843420006	192.168.1.111	192.168.1.28	ICMP	98	Echo (ping) reply id=0x1f97, seq=1/256, ttl=64 (request in 19899)
20112	95.844590006	192.168.1.28	192.168.1.111	ICMP	98	Echo (ping) request id=0x1f97, seq=2/512, ttl=64 (reply in 20113)
20113	95.844666006	192.168.1.111	192.168.1.28	ICMP	98	Echo (ping) reply id=0x1f97, seq=2/512, ttl=64 (request in 20112)
20329	96.845000006	192.168.1.28	192.168.1.111	ICMP	98	Echo (ping) request id=0x1f97, seq=3/768, ttl=64 (reply in 20330)
20330	96.845116006	192.168.1.111	192.168.1.28	ICMP	98	Echo (ping) reply id=0x1f97, seq=3/768, ttl=64 (request in 20329)
20529	97.852954006	192.168.1.28	192.168.1.111	ICMP	98	Echo (ping) request id=0x1f97, seq=4/1024, ttl=64 (reply in 20530)
20530	97.853061006	192.168.1.111	192.168.1.28	ICMP	98	Echo (ping) reply id=0x1f97, seq=4/1024, ttl=64 (request in 20529)
20748	98.848354006	192.168.1.28	192.168.1.111	ICMP	98	Echo (ping) request id=0x1f97, seq=5/1280, ttl=64 (reply in 20749)
20749	98.848427006	192.168.1.111	192.168.1.28	ICMP	98	Echo (ping) reply id=0x1f97, seq=5/1280, ttl=64 (request in 20748)
20953	99.849633006	192.168.1.28	192.168.1.111	ICMP	98	Echo (ping) request id=0x1f97, seq=6/1536, ttl=64 (reply in 20954)
20954	99.849694006	192.168.1.111	192.168.1.28	ICMP	98	Echo (ping) reply id=0x1f97, seq=6/1536, ttl=64 (request in 20953)
21713	103.56984006	192.168.1.111	192.168.1.1	ICMP	98	Echo (ping) request id=0x59d8, seq=1/256, ttl=64 (reply in 21714)
21714	103.57110006	192.168.1.1	192.168.1.111	ICMP	98	Echo (ping) reply id=0x59d8, seq=1/256, ttl=64 (request in 21713)
21920	104.57080006	192.168.1.111	192.168.1.1	ICMP	98	Echo (ping) request id=0x59d8, seq=2/512, ttl=64 (reply in 21921)
21921	104.572051006	192.168.1.1	192.168.1.111	ICMP	98	Echo (ping) reply id=0x59d8, seq=2/512, ttl=64 (request in 21920)

▶ Frame 13190: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

▶ Ethernet II, Src: IntelCor_0c:f6:38 (10:0b:a9:0c:f6:38), Dst: Netgear_84:19:22 (00:24:b2:84:19:22)

▶ Internet Protocol Version 4, Src: 192.168.1.111 (192.168.1.111), Dst: 192.168.0.111 (192.168.0.111)

▶ Internet Control Message Protocol

```

0000  00 24 b2 84 19 22 10 0b a9 0c f6 38 00 00 45 00  .$.*. . . .8..E.
0010  00 54 71 07 40 00 40 01 46 73 c0 a8 01 6f c0 a8  .Tq.@.@.Fs...o.
0020  00 6f 08 00 bd 58 59 81 00 01 4e 97 cf 54 00 00  .o...XY. .N..T..
0030  00 00 fb 65 09 00 00 00 00 00 11 12 13 14 15  .e...e...e...e...

```

wlan0: <live capture in progress... Packets: 25901 - Displayed: 23 (0,1%) Profile: Default