Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Московский государственный технический университет им. Н. Э. Баумана

23 0102

Согласовано

_____ *Антонов А.И.*

“____” _____ _____

Утверждаю

_____ *Антонов А.И.*

“____” _____ _____

Лабораторная работа 1-3 по курсу «Системы передачи данных»

Студент группы ИУ5-92

_____ *Гуща А. В*

“____” _____ _____

2014

Содержание

1 Задание **3**

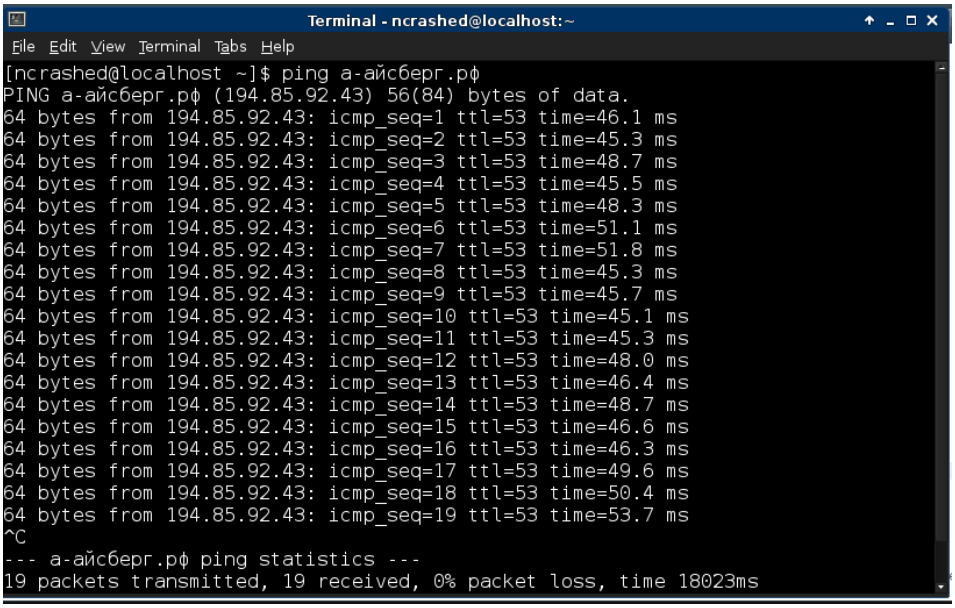
2 Выполнение **3**

1 Задание

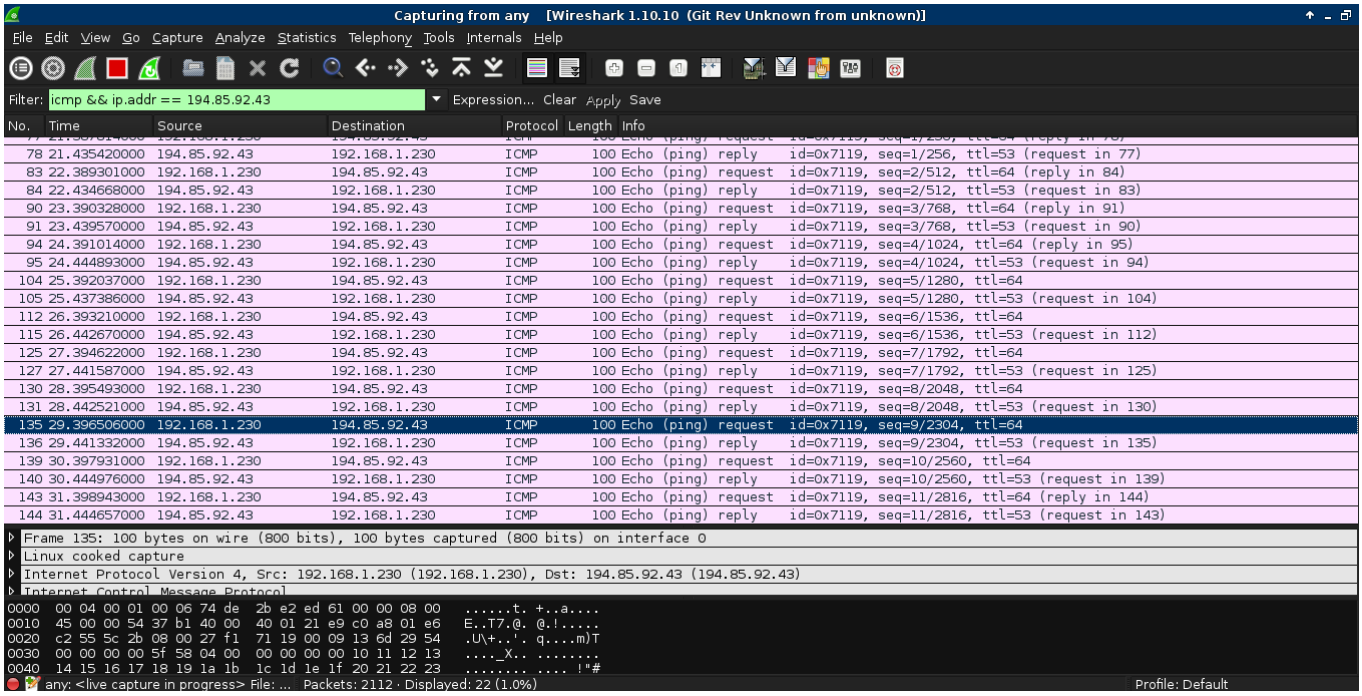
Вариант	Удаленный хост	Ping	Traceroute	Проверка сервисов	Запрос
7	а-айсберг.рф	+		+	whois, lookup

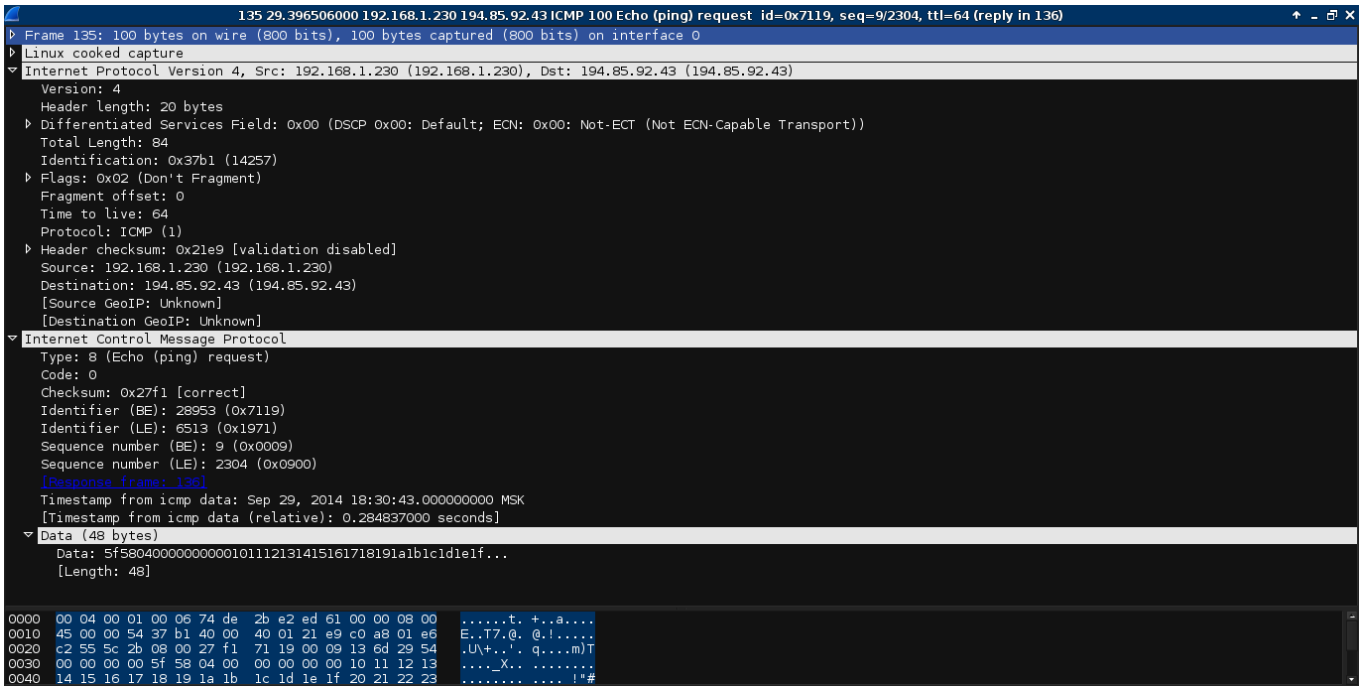
2 Выполнение

Выполним команду ping на хост а-айсберг.рф:



Отловим все ICMP сообщения по адресу 194.85.92.43 через wireshark:
Проведем подробный анализ содержимого пакета:


Capturing from any [Wireshark 1.10.10 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: icmp && ip.addr == 194.85.92.43
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
78 21.435420000 194.85.92.43 192.168.1.230 ICMP 100 Echo (ping) reply id=0x7119, seq=1/256, ttl=53 (request in 77)
83 22.389301000 192.168.1.230 194.85.92.43 ICMP 100 Echo (ping) request id=0x7119, seq=2/512, ttl=64 (reply in 84)
84 22.434668000 194.85.92.43 192.168.1.230 ICMP 100 Echo (ping) reply id=0x7119, seq=2/512, ttl=53 (request in 83)
90 23.390328000 192.168.1.230 194.85.92.43 ICMP 100 Echo (ping) request id=0x7119, seq=3/768, ttl=64 (reply in 91)
91 23.439570000 194.85.92.43 192.168.1.230 ICMP 100 Echo (ping) reply id=0x7119, seq=3/768, ttl=53 (request in 90)
94 24.391014000 192.168.1.230 194.85.92.43 ICMP 100 Echo (ping) request id=0x7119, seq=4/1024, ttl=64 (reply in 95)
95 24.444893000 194.85.92.43 192.168.1.230 ICMP 100 Echo (ping) reply id=0x7119, seq=4/1024, ttl=53 (request in 94)
104 25.392037000 192.168.1.230 194.85.92.43 ICMP 100 Echo (ping) request id=0x7119, seq=5/1280, ttl=64
105 25.437386000 194.85.92.43 192.168.1.230 ICMP 100 Echo (ping) reply id=0x7119, seq=5/1280, ttl=53 (request in 104)
112 26.393210000 192.168.1.230 194.85.92.43 ICMP 100 Echo (ping) request id=0x7119, seq=6/1536, ttl=64
115 26.442670000 194.85.92.43 192.168.1.230 ICMP 100 Echo (ping) reply id=0x7119, seq=6/1536, ttl=53 (request in 112)
125 27.394622000 192.168.1.230 194.85.92.43 ICMP 100 Echo (ping) request id=0x7119, seq=7/1792, ttl=64
127 27.441587000 194.85.92.43 192.168.1.230 ICMP 100 Echo (ping) reply id=0x7119, seq=7/1792, ttl=53 (request in 125)
130 28.395493000 192.168.1.230 194.85.92.43 ICMP 100 Echo (ping) request id=0x7119, seq=8/2048, ttl=64
131 28.442521000 194.85.92.43 192.168.1.230 ICMP 100 Echo (ping) reply id=0x7119, seq=8/2048, ttl=53 (request in 130)
135 29.396506000 192.168.1.230 194.85.92.43 ICMP 100 Echo (ping) request id=0x7119, seq=9/2304, ttl=64
136 29.441332000 194.85.92.43 192.168.1.230 ICMP 100 Echo (ping) reply id=0x7119, seq=9/2304, ttl=53 (request in 135)
139 30.397931000 192.168.1.230 194.85.92.43 ICMP 100 Echo (ping) request id=0x7119, seq=10/2560, ttl=64
140 30.444976000 194.85.92.43 192.168.1.230 ICMP 100 Echo (ping) reply id=0x7119, seq=10/2560, ttl=53 (request in 139)
143 31.398943000 192.168.1.230 194.85.92.43 ICMP 100 Echo (ping) request id=0x7119, seq=11/2816, ttl=64 (reply in 144)
144 31.444657000 194.85.92.43 192.168.1.230 ICMP 100 Echo (ping) reply id=0x7119, seq=11/2816, ttl=53 (request in 143)
Frame 135: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.1.230 (192.168.1.230), Dst: 194.85.92.43 (194.85.92.43)
Internet Control Message Protocol
0000 00 04 00 01 00 06 74 de 2b e2 ed 61 00 00 08 00 ......t. +..a....
0010 45 00 00 54 37 b1 40 00 40 01 21 e9 c0 a8 01 e6 E..T7.@. @.!.....
0020 c2 55 5c 2b 08 00 27 f1 71 19 00 09 13 6d 29 54 .U\+..'. q....m)T
0030 00 00 00 00 5f 58 04 00 00 00 00 00 10 11 12 13 ...._X.. ....
0040 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 .... !"#
any: <live capture in progress> File: ... Packets: 2112 · Displayed: 22 (1.0%)
Profile: Default

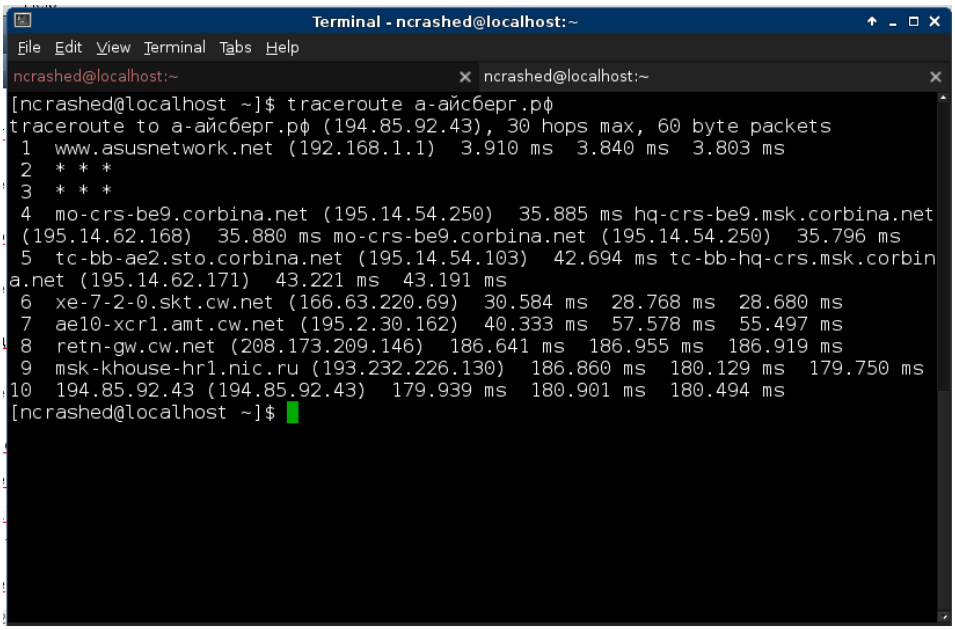

135 29.396506000 192.168.1.230 194.85.92.43 ICMP 100 Echo (ping) request id=0x7119, seq=9/2304, ttl=64 (reply in 136)
Frame 135: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.1.230 (192.168.1.230), Dst: 194.85.92.43 (194.85.92.43)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 84
Identification: 0x37b1 (14257)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0x21e9 [validation disabled]
Source: 192.168.1.230 (192.168.1.230)
Destination: 194.85.92.43 (194.85.92.43)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x27f1 [correct]
Identifier (BE): 28953 (0x7119)
Identifier (LE): 6513 (0x1971)
Sequence number (BE): 9 (0x0009)
Sequence number (LE): 2304 (0x0900)
[Response frame: 136]
Timestamp from icmp data: Sep 29, 2014 18:30:43.000000000 MSK
[Timestamp from icmp data (relative): 0.284837000 seconds]
Data (48 bytes)
Data: 5f5804000000000010111213141516171819 1a1b1c1d1e1f...
[Length: 48]
0000 00 04 00 01 00 06 74 de 2b e2 ed 61 00 00 08 00 ......t. +..a....
0010 45 00 00 54 37 b1 40 00 40 01 21 e9 c0 a8 01 e6 E..T7.@. @.!.....
0020 c2 55 5c 2b 08 00 27 f1 71 19 00 09 13 6d 29 54 .U\+..'. q....m)T
0030 00 00 00 00 5f 58 04 00 00 00 00 00 10 11 12 13 ...._X.. ....
0040 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 .... !"#

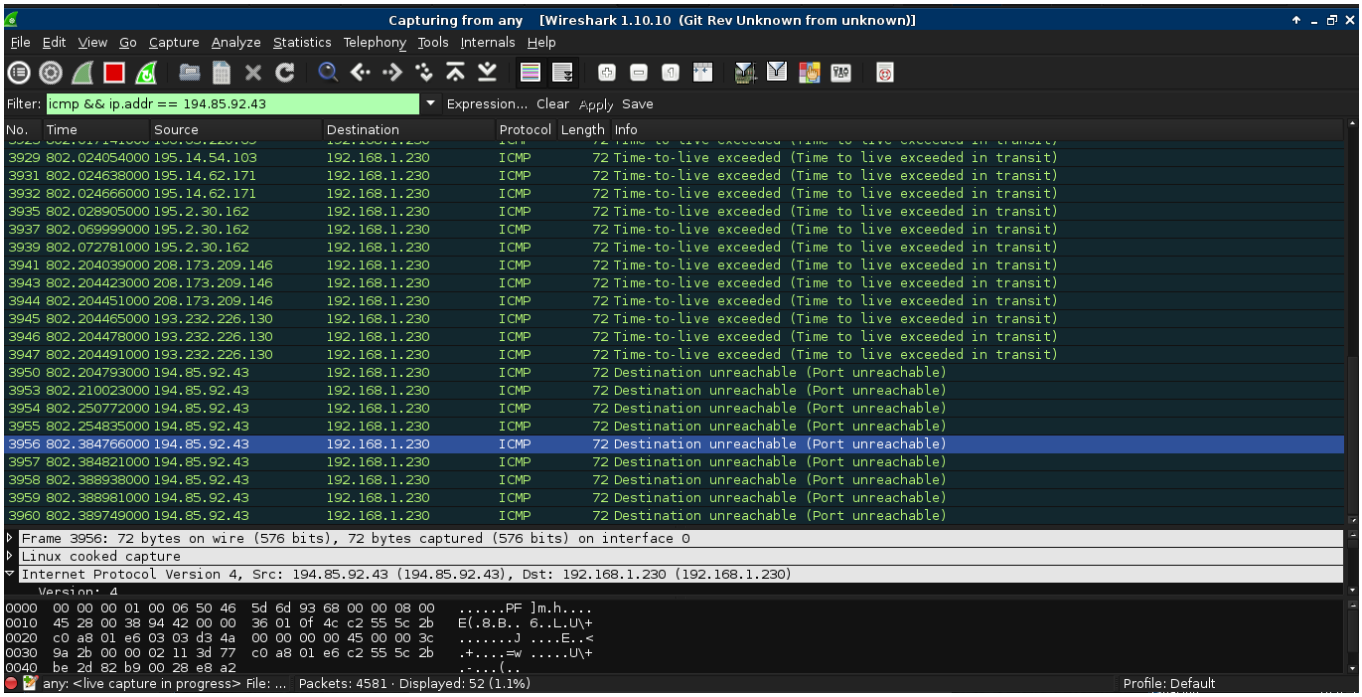
Исходя из данной информации можно сделать выводы:

– Использовался ICMP поверх IPv4. В сообщении есть все поля из IP (адрес назначения и источника, время жизни, контрольная сумма и т.д.)

– Тип ICMP сообщения 8, который означает эхо-запрос. Просмотр аналогичного сообщения ответа показывает Type равным 0, что означает ответ на полученное сообщение.

Используем команду traceroute:

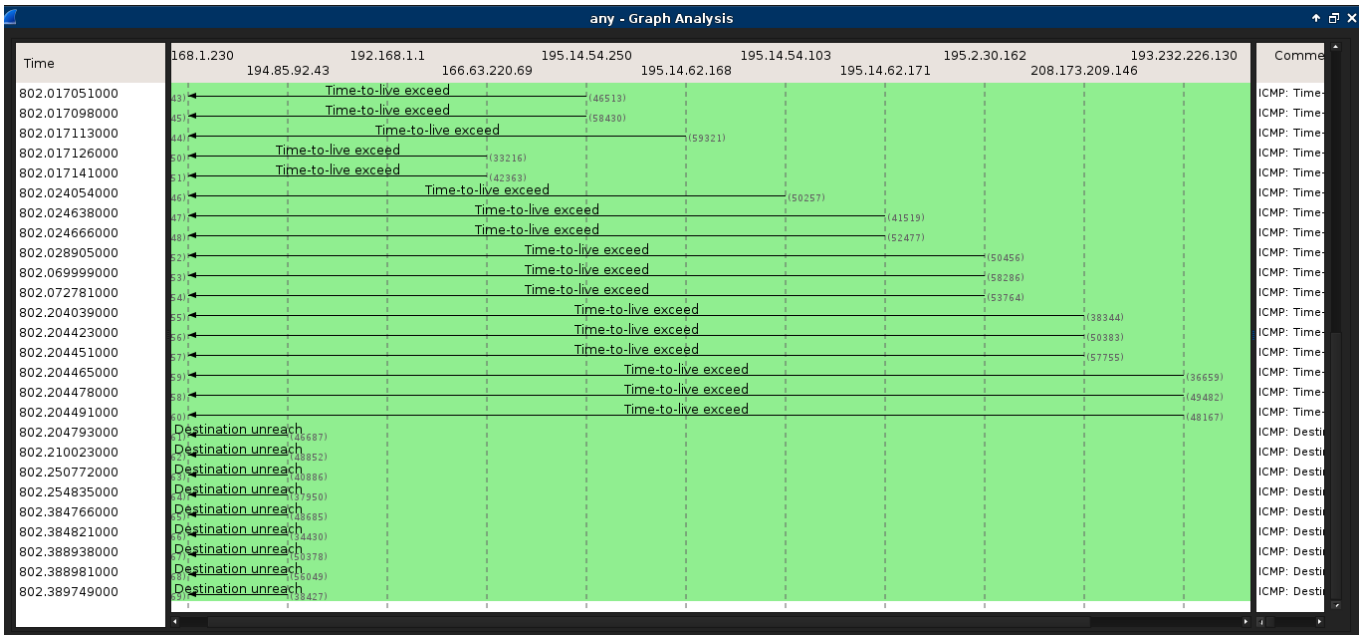




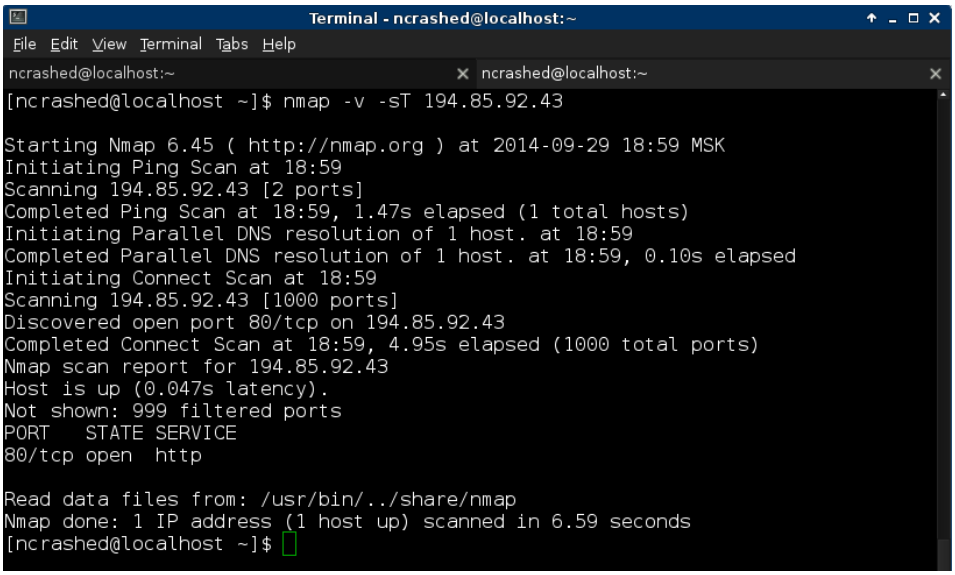
Traceroute отправляет пакеты с заранее малым значением TTL, которое постепенно увеличивается, что позволяет получать статистику о узлах, через ко-

торые проходят пакеты. При уменьшении значения поля TTL до 0, отправителю отправляется сообщение-ошибка.

Это подтверждается на packet-flow графике:



Проверим все сервисы и порты на хосте а-айсберг.рф с помощью утилиты nmap: Открыт только порт с номером 80 - HTTP порт.

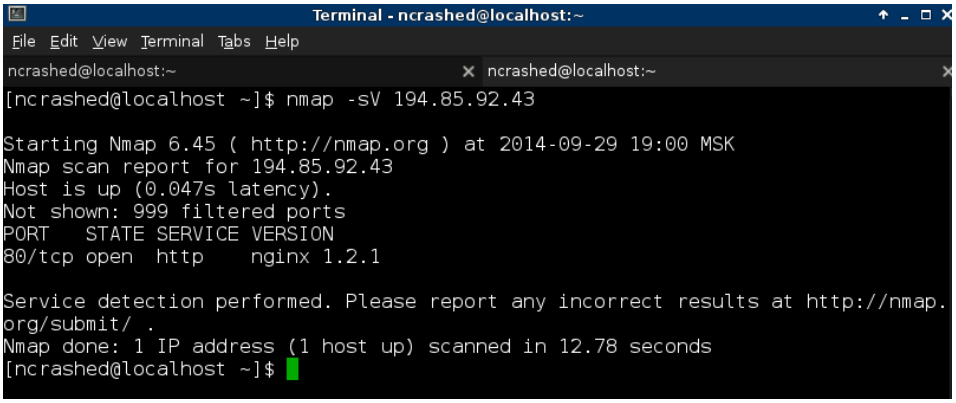


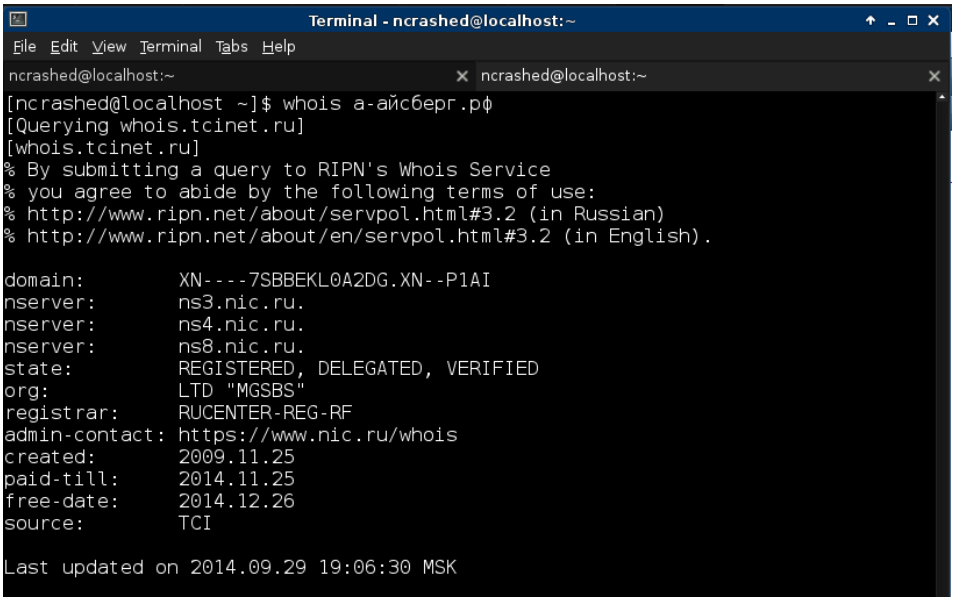
Проверим доступные службы:

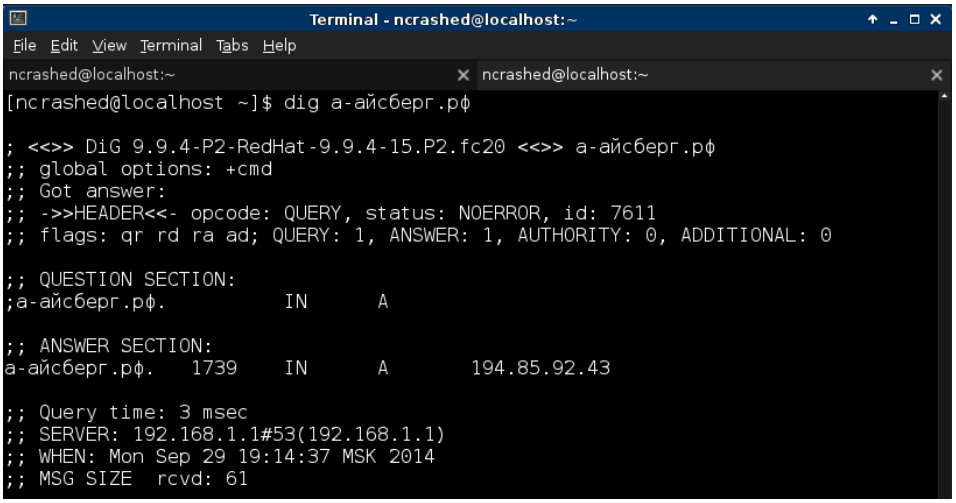
После сканирования было выявлено, что на 80-м порту запущен веб сервер nginx.

Сделаем запрос whois: Вся информация получена из базы данных Internet Network Information Center - interNIC.

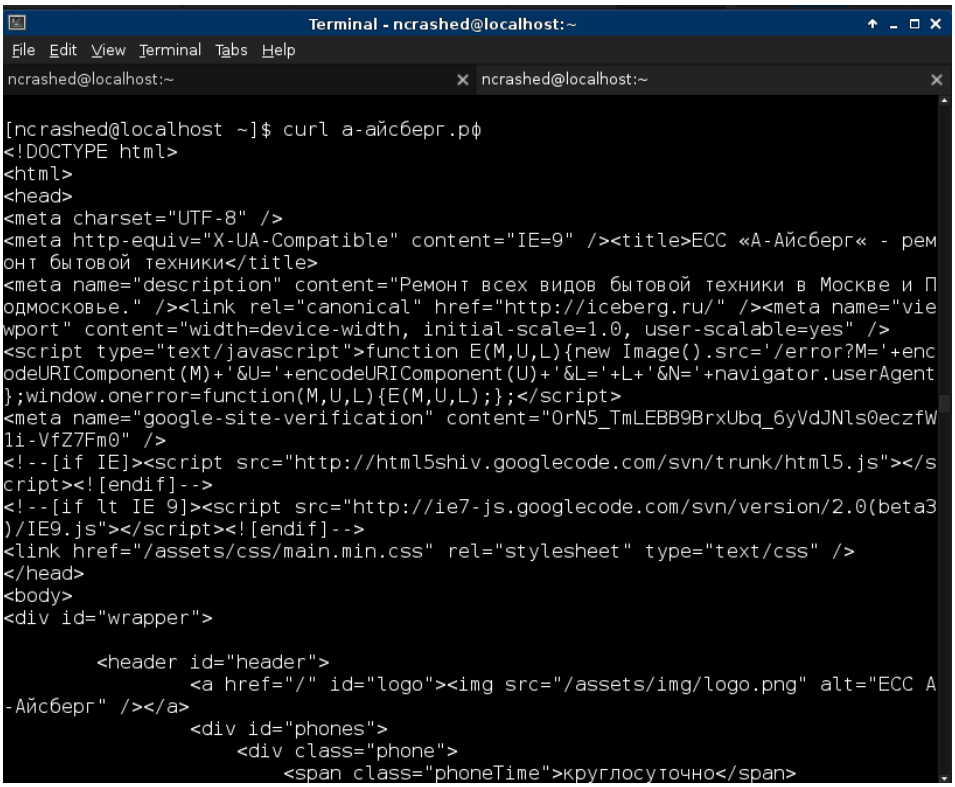
Сделаем запрос lookup: DNS сервер ответил, что домен а-айсберг.рф имеет IP адрес 194.85.92.43.







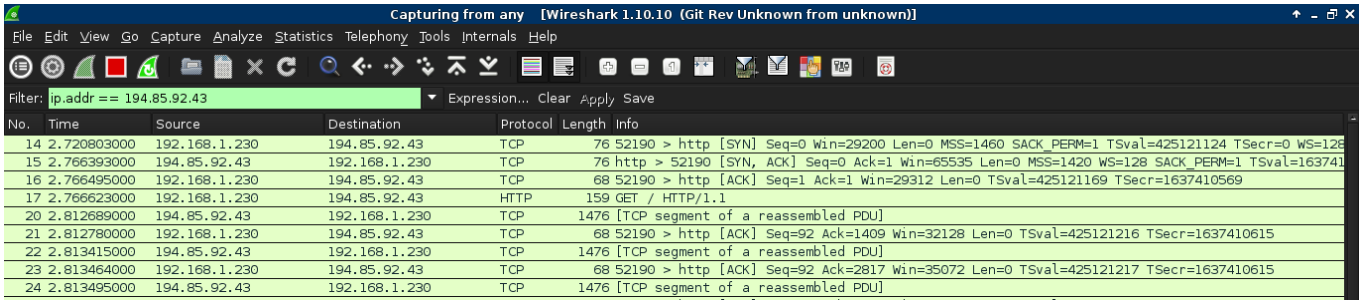
Произведем HTTP запрос на a-айсберг.рф:


Terminal - ncrashed@localhost:~
File Edit View Terminal Tabs Help
ncrashed@localhost:~
ncrashed@localhost:~
[ncrashed@localhost ~]$ curl a-айсберг.рф
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=9" /><title>ECC «А-Айсберг« - рем
онт бытовой техники</title>
<meta name="description" content="Ремонт всех видов бытовой техники в Москве и П
одмосковье." /><link rel="canonical" href="http://iceberg.ru/" /><meta name="vie
wport" content="width=device-width, initial-scale=1.0, user-scalable=yes" />
<script type="text/javascript">function E(M,U,L){new Image().src='/error?M='+enc
odeURIComponent(M)+'&U='+encodeURIComponent(U)+'&L='+L+'&N='+navigator.userAgent
};window.onerror=function(M,U,L){E(M,U,L);};</script>
<meta name="google-site-verification" content="OrN5_TmLEBB9BrxUbq_6yVdJNls0eczfW
1i-VfZ7Fm0" />
<!--[if IE]><script src="http://html5shiv.googlecode.com/svn/trunk/html5.js"></s
cript><![endif]-->
<!--[if lt IE 9]><script src="http://ie7-js.googlecode.com/svn/version/2.0(beta3
)/IE9.js"></script><![endif]-->
<link href="/assets/css/main.min.css" rel="stylesheet" type="text/css" />
</head>
<body>

<header id="header">
<img src="/assets/img/logo.png" alt="ECC A
-Айсберг" />

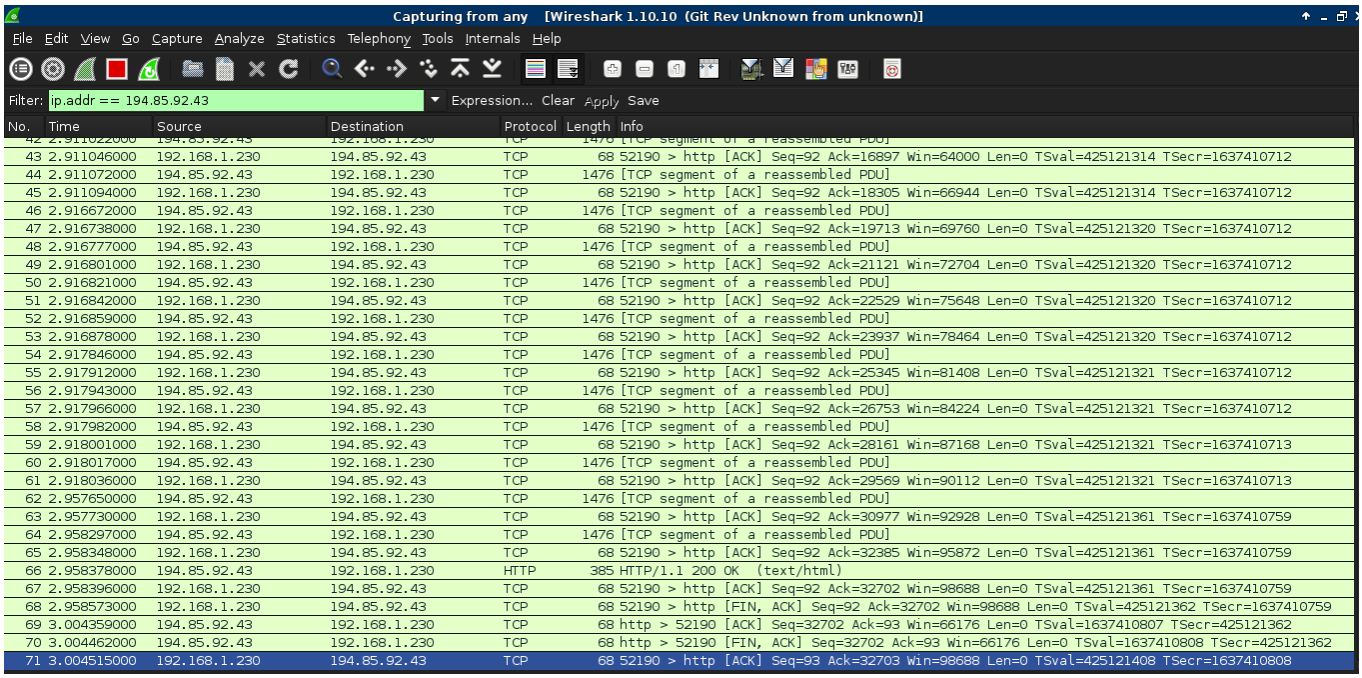
круглосуточно

Проанализируем запрос в пакетном анализаторе:



No.	Time	Source	Destination	Protocol	Length	Info
14	2.720803000	192.168.1.230	194.85.92.43	TCP	76	52190 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=425121124 TSecr=0 WS=128
15	2.766393000	194.85.92.43	192.168.1.230	TCP	76	http > 52190 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1420 WS=128 SACK_PERM=1 TSval=163741
16	2.766495000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=425121169 TSecr=1637410569
17	2.766623000	192.168.1.230	194.85.92.43	HTTP	159	GET / HTTP/1.1
20	2.812689000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]
21	2.812780000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=1409 Win=32128 Len=0 TSval=425121216 TSecr=1637410615
22	2.813415000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]
23	2.813464000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=2817 Win=35072 Len=0 TSval=425121217 TSecr=1637410615
24	2.813495000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]

Соединение производится по трехэтапной процедуре (SYN-SYN-ACK-ACK), называемой three-way handshake. Далее идет передача данных страницы с подтверждением на каждую часть.



No.	Time	Source	Destination	Protocol	Length	Info
43	2.911046000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=16897 Win=64000 Len=0 TSval=425121314 TSecr=1637410712
44	2.911072000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]
45	2.911094000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=18305 Win=66944 Len=0 TSval=425121314 TSecr=1637410712
46	2.916672000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]
47	2.916738000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=19713 Win=69760 Len=0 TSval=425121320 TSecr=1637410712
48	2.916777000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]
49	2.916801000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=21121 Win=72704 Len=0 TSval=425121320 TSecr=1637410712
50	2.916821000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]
51	2.916842000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=22529 Win=75648 Len=0 TSval=425121320 TSecr=1637410712
52	2.916859000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]
53	2.916878000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=23937 Win=78464 Len=0 TSval=425121320 TSecr=1637410712
54	2.917846000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]
55	2.917912000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=25345 Win=81408 Len=0 TSval=425121321 TSecr=1637410712
56	2.917943000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]
57	2.917966000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=26753 Win=84224 Len=0 TSval=425121321 TSecr=1637410712
58	2.917982000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]
59	2.918001000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=28161 Win=87168 Len=0 TSval=425121321 TSecr=1637410713
60	2.918017000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]
61	2.918036000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=29569 Win=90112 Len=0 TSval=425121321 TSecr=1637410713
62	2.957650000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]
63	2.957730000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=30977 Win=92928 Len=0 TSval=425121361 TSecr=1637410759
64	2.958297000	194.85.92.43	192.168.1.230	TCP	1476	[TCP segment of a reassembled PDU]
65	2.958348000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=32385 Win=95872 Len=0 TSval=425121361 TSecr=1637410759
66	2.958378000	194.85.92.43	192.168.1.230	HTTP	385	HTTP/1.1 200 OK (text/html)
67	2.958396000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=92 Ack=32702 Win=98688 Len=0 TSval=425121361 TSecr=1637410759
68	2.958573000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [FIN, ACK] Seq=92 Ack=32702 Win=98688 Len=0 TSval=425121362 TSecr=1637410759
69	3.004359000	194.85.92.43	192.168.1.230	TCP	68	http > 52190 [ACK] Seq=32702 Ack=93 Win=66176 Len=0 TSval=1637410807 TSecr=425121362
70	3.004462000	194.85.92.43	192.168.1.230	TCP	68	http > 52190 [FIN, ACK] Seq=32702 Ack=93 Win=66176 Len=0 TSval=1637410808 TSecr=425121362
71	3.004515000	192.168.1.230	194.85.92.43	TCP	68	52190 > http [ACK] Seq=93 Ack=32703 Win=98688 Len=0 TSval=425121408 TSecr=1637410808

Завершение соединения производится в четыре этапа (по два на каждое направление передачи, так как виртуальный канал полнодуплексный). Последовательность сообщений: FIN, ACK-ACK-FIN, ACK-ACK.