

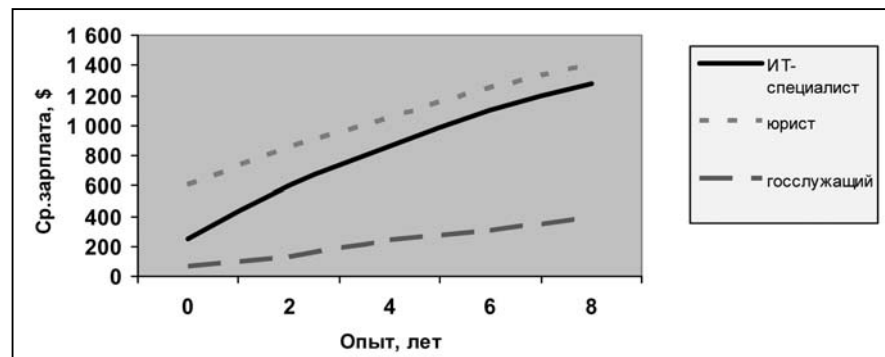
## 2. Оперативно-розыскные мероприятия

### Взаимодействие

При раскрытии компьютерных преступлений на вероятность успеха сильно влияет взаимодействие с двумя видами субъектов: специалистами и операторами связи. Настолько сильной корреляции между содействием с их стороны и успехом раскрытия нет, пожалуй, ни для каких других типов преступлений.

Специальные знания в области ИТ, телекоммуникаций, программирования и защиты информации требуются буквально на каждом этапе — от обнаружения признаков преступления до поддержания обвинения в суде. Источником специальных знаний является специалист. Со стороны следователя или оперуполномоченного было бы слишком самонадеянно рассчитывать на собственные знания в этих областях.

Настоящим ИТ-профессионалом становятся после обучения в вузе и нескольких лет работы по соответствующей специальности. Получить эквивалентные знания, прочитав книги, побеседовав со специалистами и расследовав десяток-другой компьютерных преступлений, никак не возможно. Хотя иллюзия всезнания может возникнуть. Ею часто страдают начинающие. Для таких даже существует особый термин «ламер\*», то есть дилетант, «чайник\*», который считает себя знающим. Видимо, специфика нашей отрасли такова, что в процессе обучения довольно трудно увидеть свой «горизонт незнания», чтобы адекватно оценить собственный уровень.



*Зависимость средней заработной платы от опыта работы (на 2000 год).  
Для специалистов в области информационных технологий и связи рост  
быстрее, то есть опыт ценится выше*

Как бы сами себя ни оценивали служащие правоохранительных органов, но, как говорится, со стороны виднее. Специалиста с должным уровнем квалификации в области ИТ и телекоммуникаций в штате МВД или ФСБ иметь невозможно. Зато получить помощь стороннего специалиста не слишком сложно.

Было бы ошибкой привлекать специалиста только лишь тогда, когда дело дойдет до экспертизы или до изъятия компьютерной техники. Специальные знания нужны на самой ранней стадии расследования — при первичной проверке материала, а также при проведении оперативно-розыскных мероприятий.

Содействие провайдера\* (оператора связи) также обязательный элемент расследования, если только в деле что-то связано с публичной компьютерной сетью.

Роль провайдера в деле получения информации о сетях, клиентах и их активности трудно переоценить. Так сложилось исторически, что Интернет возник как чисто техническое устройство. В те начальные времена его можно было рассматривать как сеть, связывающую компьютеры. Соответственно с этим управлялся Интернет техническими специалистами при помощи доступных и понятных им технических методов. С течением времени, с приходом в Сеть массового пользователя, с развитием сетевых форм общения, с возникновением сетевого бизнеса Интернет превратился из технического устройства в среду, где взаимодействуют не устройства, а люди. На Интернет сейчас завязаны многочисленные финансовые, политические, личные интересы множества людей и организаций. Уже даже говорят о целом виртуальном мире. Но методы управления Интернетом пока остаются старыми. Им управляют в основном технические специалисты, не имеющие гуманитарного образования, зачастую не понимающие, что они взаимодействуют с людьми, а не с техникой. Автор даже предлагает рассматривать диалектическое противоречие — противоречие между новыми общественными отношениями в Сети и старыми методами управления Сетью [98].

Возможно, что в скором времени «сетевая власть» от технарей перейдет в руки профессиональных управленцев. Такие тенденции уже отчетливо заметны на всех уровнях — от домашней сети до международных организаций. Но пока в лице провайдера мы имеем все четыре власти в одном лице. Ныне интернет-провайдер выступает в роли полновластного хозяина своего участка, всемогущего и всеведущего.

Внедрение во всех странах комплексов, аналогичных российскому СОРМУ, призвано, в частности, исключить взаимодействие с оператором связи, когда требуется получить информацию о работе пользователя в сети, его трафике и так далее. К сожалению, несмотря на отчеты о внедрении таких комплексов, полностью решить эту задачу не удалось. Ни в России,

ни в других странах. Без содействия со стороны оператора связи пока невозможно проводить полноценные ОРМ или следственные действия.

Именно поэтому взаимодействие с работниками операторов связи столь важно на всех этапах — от первичной проверки материала до показаний в суде.

## Перехват и исследование трафика

### Значение

В перечне видов оперативно-розыскной деятельности присутствует «снятие информации с технических каналов связи». Эта универсальная формулировка включает, в частности, и перехват сетевого трафика\*.

В российской судебной практике трафик (результаты его экспертизы) почти не использовался в качестве доказательства. Для ведения ОРД трафик также используется крайне редко. Автор полагает, что его следует использовать шире. В криминальной деятельности перехват и анализ трафика (снифинг\*) является основой чуть ли не половины всех методов совершения преступлений. В работе ИТ-специалистов анализ сетевого трафика — один из основных методов диагностики и поиска неисправностей. Возможности этого метода велики. Поэтому и в правоохранительной деятельности он должен использоваться как можно шире.

На основе анализа содержимого, а также статистики сетевого трафика можно определить и доказать совершение пользователем многих действий в сети, а также получить информацию об устройстве программ, информационных систем и сетей.

Сбор и анализ сетевого трафика определенного компьютера может заменить изъятие и экспертизу самого этого компьютера, поскольку даст такую же информацию, а именно содержимое электронной почты, свидетельства о просмотре веб-сайтов, о размещении информации в Сети, о несанкционированном доступе к удаленным узлам, об использовании контрафактных программ. И в то же время перехватить трафик бывает проще, чем найти и изъять в исправном состоянии компьютер.

### Пример

В качестве примера приведем образец перехваченного веб-трафика, то есть трафика при доступе пользователя к веб-сайту. Перехват осуществлен программой «tcpdump», которая относится к классу сниферов\* и входит в состав любой операционной системы (кроме Windows). Параметры команды таковы: «-n» означает приводить IP-адреса в цифровой нотации, то есть не переводить их в доменные имена; «-i fxp0» указывает интерфейс, с которого снимать трафик; «-v» включает режим более подробного вывода сведений о пакетах; «-xX» означает приводить также символьное представление всех байтов пакета; «-s 1024» указывает,

сколько байтов из каждого пакета показывать; параметр «tcp and port 80» определяет фильтр, то есть критерии, по которым пакеты включаются или не включаются в выдачу, в данном случае мы перехватываем пакеты протокола TCP, относящиеся к порту 80, то есть к веб-трафику.

Здесь и далее содержимое трафика приводится в одном из вариантов общепринятого формата «hex dump» [49, W18]. Бинарное содержимое каждого пакета показано в шестнадцатеричной системе счисления по 16 байт в строке. Слева указан порядковый номер первого байта строки, справа — представление тех же байтов в виде ASCII-символов.

```
fnn# tcpdump -n -i fxp0 -v -xx -s 1024 'tcp and port 80'
tcpdump: listening on bge0, link-type EN10MB (Ethernet), capture size 1024 bytes
```

```
12:07:16.541938 IP (tos 0x0, ttl 64, id 21663, offset 0, flags [DF],
length: 64, bad cksum 0 (->16e3)!) 10.0.4.31.65406 > 81.16.112.7.80: S [bad
tcp cksum cf68 (->c6d1)!] 11159565:11159565(0) win 65535 <mss
1460,nop,nop,sackOK,nop,wscale 1,nop,nop,timestamp 39474456 0>
 0x0000: 000e a6a4 b3cf 0002 a5e7 4133 0800 4500 .....A3..E.
 0x0010: 0040 549f 4000 4006 0000 0a00 041f 5110 .@T.@.@.....Q.
 0x0020: 7007 ff7e 0050 00aa 480d 0000 0000 b002 p...~.P..H.....
 0x0030: ffff cf68 0000 0204 05b4 0101 0402 0103 ...h.....
 0x0040: 0301 0101 080a 025a 5518 0000 0000 .....ZU.....
```

```
12:07:16.617508 IP (tos 0x0, ttl 58, id 40598, offset 0, flags [DF],
length: 64) 81.16.112.7.80 > 10.0.4.31.65406: S [tcp sum ok]
352447028:352447028(0) ack 11159566 win 65535 <mss 1380,nop,wscale
1,nop,nop,timestamp 913842465 39474456,nop,nop,sackOK>
 0x0000: 0002 a5e7 4133 000e a6a4 b3cf 0800 4500 ....A3.....E.
 0x0010: 0040 9e96 4000 3a06 d2eb 5110 7007 0a00 .@..@.:...Q.p...
 0x0020: 041f 0050 ff7e 1501 ea34 00aa 480e b012 ...P...~...4..H...
 0x0030: ffff 7041 0000 0204 0564 0103 0301 0101 ..pA.....d.....
 0x0040: 080a 3678 2121 025a 5518 0101 0402 ..6x!!..ZU.....
```

```
12:07:16.617558 IP (tos 0x0, ttl 64, id 21664, offset 0, flags [DF],
length: 52, bad cksum 0 (->16ee)!) 10.0.4.31.65406 > 81.16.112.7.80: . [bad
tcp cksum cf5c (->3075)!] ack 1 win 32832 <nop,nop,timestamp 39474464
913842465>
 0x0000: 000e a6a4 b3cf 0002 a5e7 4133 0800 4500 .....A3.....E.
 0x0010: 0034 54a0 4000 4006 0000 0a00 041f 5110 .4T.@.@.....Q.
 0x0020: 7007 ff7e 0050 00aa 480e 1501 ea35 8010 p...~.P..H....5...
 0x0030: 8040 cf5c 0000 0101 080a 025a 5520 3678 .@.@.....ZU.6x
 0x0040: 2121 !!
```

```
12:07:16.617940 IP (tos 0x0, ttl 64, id 21665, offset 0, flags [DF],
length: 624, bad cksum 0 (->14b1)!) 10.0.4.31.65406 > 81.16.112.7.80: P
[bad tcp cksum d198 (->3a57)!] 1:573(572) ack 1 win 32832 <nop,nop,time-
stamp 39474464 913842465>
 0x0000: 000e a6a4 b3cf 0002 a5e7 4133 0800 4500 .....A3.....E.
 0x0010: 0270 54a1 4000 4006 0000 0a00 041f 5110 .pT.@.@.....Q.
```

```
0x0020: 7007 ff7e 0050 00aa 480e 1501 ea35 8018 p...~.P..H....5...
0x0030: 8040 d198 0000 0101 080a 025a 5520 3678 .@.....ZU.6x
0x0040: 2121 4745 5420 2f63 6769 2d62 696e 2f61 !!GET../cgi-bin/a
0x0050: 6c6c 6970 5f76 6965 772e 706c 2048 5454 llip_view.pl.HTT
0x0060: 502f 312e 310d 0a48 6f73 743a 2061 6c6c P/1.1..Host:.all
0x0070: 6970 2e73 7461 7274 7465 6c65 636f 6d2e ip.starttelecom.
0x0080: 7275 0d0a 5573 6572 2d41 6765 6e74 3a20 ru..User-Agent:.
0x0090: 4d6f 7a69 6c6c 612f 352e 3020 2858 3131 Mozilla/5.0.(X11
0x00a0: 3b20 553b 2046 7265 6542 5344 2069 3338 ;.U;.FreeBSD.i38
0x00b0: 363b 2065 6e2d 5553 3b20 7276 3a31 2e38 6;.en-US;.rv:1.8
0x00c0: 2e31 2920 4765 636b 6f2f 3230 3036 3131 .1).Gecko/200611
0x00d0: 3037 2046 6972 6566 6f78 2f32 2e30 0d0a 07.Firefox/2.0..
0x00e0: 4163 6365 7074 3a20 7465 7874 2f78 6d6c Accept:.text/xml
0x00f0: 2c61 7070 6c69 6361 7469 6f6e 2f78 6d6c ,application/xml
0x0100: 2c61 7070 6c69 6361 7469 6f6e 2f78 6874 ,application/xht
0x0110: 6d6c 2b78 6d6c 2c74 6578 742f 6874 6d6c ml+xml;text/html
0x0120: 3b71 3d30 2e39 2c74 6578 742f 706c 6169 ;q=0.9;text/plai
0x0130: 6e3b 713d 302e 382c 696d 6167 652f 706e n;q=0.8,image/pn
0x0140: 672c 2a2f 2a3b 713d 302e 350d 0a41 6363 g,/*;q=0.5..Acc
0x0150: 6570 742d 4c61 6e67 7561 6765 3a20 7275 ept-Language:.ru
0x0160: 2c65 6e2d 7573 3b71 3d30 2e37 2c65 6e3b ,en-us;q=0.7,en;
0x0170: 713d 302e 330d 0a41 6363 6570 742d 456e q=0.3..Accept-En
0x0180: 636f 6469 6e67 3a20 677a 6970 2c64 6566 coding:.gzip,def
0x0190: 6c61 7465 0d0a 4163 6365 7074 2d43 6861 late..Accept-Cha
0x01a0: 7273 6574 3a20 4953 4f2d 3838 3539 2d31 rset:.ISO-8859-1
0x01b0: 2c75 7466 2d38 3b71 3d30 2e37 2c2a 3b71 ,utf-8;q=0.7,*;q
0x01c0: 3d30 2e37 0d0a 4b65 6570 2d41 6c69 7665 =0.7..Keep-Alive
0x01d0: 3a20 3330 300d 0a43 6f6e 6e65 6374 696f :.300..Connectio
0x01e0: 6e3a 206b 6565 702d 616c 6976 650d 0a52 n:.keep-alive..R
0x01f0: 6566 6572 6572 3a20 6874 7470 3a2f 2f61 eferer:.http://a
0x0200: 6c6c 6970 2e73 7461 7274 7465 6c65 636f llip.startteleco
0x0210: 6d2e 7275 2f63 6769 2d62 696e 2f61 6c6c m.ru/cgi-bin/all
0x0220: 6970 5f76 6965 772e 706c 3f73 7479 7065 ip_view.pl?stype
0x0230: 3d69 7026 7265 713d 2a0d 0a41 7574 686f =ip&req=*.Autho
0x0240: 7269 7a61 7469 6f6e 3a20 4261 7369 6320 rization:.Basic.
0x0250: 6458 4e6c 636a 6f33 4e7a 6468 4367 3d3d dXNlcjo3NzdhdCg==
0x0260: 0d0a 4361 6368 652d 436f 6e74 726f 6c3a ..Cache-Control:
0x0270: 206d 6178 2d61 6765 3d30 0d0a 0d0a .max-age=0....
```

```
12:07:16.771948 IP (tos 0x0, ttl 58, id 40614, offset 0, flags [DF],
length: 1420) 81.16.112.7.80 > 10.0.4.31.65406: . 1:1369(1368) ack 573 win
32832 <nop,nop,timestamp 913842586 39474464>
```

```
0x0000: 0002 a5e7 4133 000e a6a4 b3cf 0800 4500 ....A3.....E.
0x0010: 058c 9ea6 4000 3a06 cd8f 5110 7007 0a00 ....@.:...Q.p...
0x0020: 041f 0050 ff7e 1501 ea35 00aa 4a4a 8010 ...P...~...5..JJ..
0x0030: 8040 2142 0000 0101 080a 3678 219a 025a .@!B.....6x!..Z
0x0040: 5520 4854 5450 2f31 2e31 2032 3030 204f U.HTTTP/1.1.200.0
0x0050: 4b0d 0a44 6174 653a 2057 6564 2c20 3133 K..Date:Wed,.13
0x0060: 2044 6563 2032 3030 3620 3039 3a30 353a .Dec.2006.09:05:
0x0070: 3432 2047 4d54 0d0a 5365 7276 6572 3a20 42.GMT..Server:.
0x0080: 4170 6163 6865 2f31 2e33 2e33 3420 2855 Apache/1.3.34.(U
0x0090: 6e69 7829 206d 6f64 5f70 6572 6c2f 312e nix).mod_perl/1.
0x00a0: 3239 206d 6f64 5f73 736c 2f32 2e38 2e32 29.mod_ssl/2.8.2
```

```

0x00b0: 3520 4f70 656e 5353 4c2f 302e 392e 3863 5.OpenSSL/0.9.8c
0x00c0: 2072 7573 2f50 4c33 302e 3232 0d0a 4361 .rus/PL30.22..Ca
0x00d0: 6368 652d 436f 6e74 726f 6c3a 206e 6f2d che-Control:.no-
0x00e0: 6361 6368 650d 0a45 7870 6972 6573 3a20 cache..Expires:.
0x00f0: 4672 692c 2030 3120 4a61 6e20 3139 3830 Fri,.01.Jan.1980
0x0100: 2031 323a 3030 3a30 3020 474d 540d 0a50 .12:00:00.GMT..P
0x0110: 7261 676d 613a 206e 6f2d 6361 6368 650d ragma:.no-cache.
0x0120: 0a4b 6565 702d 416c 6976 653a 2074 696d .Keep-Alive:.tim
0x0130: 656f 7574 3d31 352c 206d 6178 3d31 3030 eout=15,.max=100
0x0140: 0d0a 436f 6e6e 6563 7469 6f6e 3a20 4b65 ..Connection:.Ke
0x0150: 6570 2d41 6c69 7665 0d0a 5472 616e 7366 ep-Alive..Transf
0x0160: 6572 2d45 6e63 6f64 696e 673a 2063 6875 er-Encoding:.chu
0x0170: 6e6b 6564 0d0a 436f 6e74 656e 742d 5479 nked..Content-Ty
0x0180: 7065 3a20 7465 7874 2f68 746d 6c3b 2063 pe:.text/html;c
0x0190: 6861 7273 6574 3d6b 6f69 382d 720d 0a0d harset=koi8-r...
0x01a0: 0a35 3261 0d0a 3c48 544d 4c3e 0a3c 4845 .52a.<HTML>.<HE
0x01b0: 4144 3e3c 7469 746c 653e 416c 6c2d 4950 AD><title>All-IP
0x01c0: 3c2f 7469 746c 653e 3c2f 4845 4144 3e0a </title></HEAD>.
0x01d0: 3c42 4f44 5920 6267 636f 6c6f 723d 2345 <BODY.bgcolor=#E
0x01e0: 3545 4345 3920 7465 7874 3d62 6c61 636b 5ECE9.text=black
0x01f0: 206c 6566 746d 6172 6769 6e3d 3136 2072 .leftmargin=16.r
0x0200: 6967 6874 6d61 7267 696e 3d31 3620 746f ightmargin=16.to
0x0210: 706d 6172 6769 6e3d 3130 2062 6f74 746f pmargin=10.botto
0x0220: 6d6d 6172 6769 6e3d 3130 206d 6172 6769 mmargin=10.margi
0x0230: 6e68 6569 6768 743d 3130 206d 6172 6769 nheight=10.margi
0x0240: 6e77 6964 7468 3d31 363e 0a20 0a3c 6365 nwidth=16>...<ce
0x0250: 6e74 6572 3e3c 4831 3e49 5020 7365 6172 nter><H1>IP.sear
0x0260: 6368 3c2f 4831 3e3c 2f63 656e 7465 723e ch</H1></center>
0x0270: 0a3c 7461 626c 6520 626f 7264 6572 3d30 .<table.border=0
0x0280: 2061 6c69 676e 3d63 656e 7465 7220 6365 .align=center.ce
0x0290: 6c6c 7061 6464 696e 673d 373e 3c74 7220 llpadding=7><tr.
0x02a0: 7661 6c69 676e 3d74 6f70 3e3c 7464 2062 valign=top><td.b
0x02b0: 6763 6f6c 6f72 3d23 3631 4332 3945 3e0a gcolor=#61C29E>.
0x02c0: 3c70 3e3c 464f 524d 206e 616d 653d 2269 <p><FORM.name="i
0x02d0: 7069 6e66 6f22 2061 6374 696f 6e3d 222f pinfo».action="/
0x02e0: 6367 692d 6269 6e2f 616c 6c69 705f 7669 cgi-bin/allip_vi
0x02f0: 6577 2e70 6c22 204d 4554 484f 443d 4745 ew.pl».METHOD=GE
0x0300: 543e 0a51 7565 7279 3a20 3c69 6e70 7574 T>.Query:.<input
0x0310: 2074 7970 653d 7465 7874 206e 616d 653d .type=text.name=
0x0320: 7265 7120 7661 6c75 653d 2727 2073 697a req.value=''.siz
0x0330: 653d 3332 206d 6178 6c65 6e67 7468 3d38 e=32.maxlength=8
0x0340: 303e 203c 696e 7075 7420 7479 7065 3d73 0>.<input.type=s
0x0350: 7562 6d69 7420 7661 6c75 653d 2720 2053 ubmit.value=''.S
0x0360: 6561 7263 6820 2027 3e3c 6272 3e0a 3c74 earch..'><br>.<t
0x0370: 6162 6c65 2062 6f72 6465 723d 303e 3c74 able.border=0><t
0x0380: 7220 7661 6c69 676e 3d74 6f70 3e3c 7464 r.valign=top><td
0x0390: 2061 6c69 676e 3d72 6967 6874 3e54 7970 .align=right>Typ
0x03a0: 6520 6f66 2074 6865 2073 6561 7263 683a e.of.the.search:
0x03b0: 3c2f 7464 3e0a 3c74 6420 616c 6967 6e3d </td>.<td.align=
0x03c0: 6c65 6674 3e3c 696e 7075 7420 7479 7065 left><input.type
0x03d0: 3d72 6164 696f 206e 616d 653d 7374 7970 =radio.name=styp
0x03e0: 6520 7661 6c75 653d 6970 2063 6865 636b e.value=ip.check
0x03f0: 6564 3e20 4950 2061 6464 7265 7373 3c62 ed>.IP.address<b

```

Из анализа этого трафика эксперт может сделать следующие выводы:

- Наблюдаемый компьютер использовал IP-адрес 10.0.0.31.
- Пользователь использовал браузер «Firefox» версии 2.0 (см. строку «0x00d0» четвертого пакета) английской версии, но с поддержкой русского языка (см. строку «0x0150» четвертого пакета).
- Пользователь использовал ОС «FreeBSD» для процессора типа Intel (см. строку «0x00a0» четвертого пакета).
- Пользователь в 12 часов 7 минут обращался к веб-сайту «allip.starttelecom.ru» и просматривал содержимое веб-страницы «/cgi-bin/allip\_view.pl».
- На указанную веб-страницу пользователь перешел по ссылке со страницы «allip.starttelecom.ru/cgi-bin/allip\_view.pl?stype=ip&req=» (см. поле «Referer» в строке «0x01f0» четвертого пакета).
- При доступе к указанному веб-сайту использовался логин «user» и пароль «777a» (см. четвертый пакет, строка «0x0250», параметр «Authorization: Basic» и далее логин и пароль в кодировке base64).

На взгляд автора, такая экспертиза перехваченного трафика в ряде случаев может заменить экспертизу компьютера пользователя и сервера, к которому он обращался. А если и не заменить совсем, то дополнить, значительно усилив доказательную базу.

### Организация перехвата

Ясно, что трафик, относящийся к определенному узлу, проще всего перехватывать вблизи этого узла. По мере удаления от него возрастает техническая сложность перехвата, но зато снижается организационная сложность. По мере удаления от узла падает надежность и, возможно, полнота перехвата трафика, но зато повышается скрытность. Место перехвата трафика в значительной мере определяется наличием возможностей у органа, ведущего ОРД. Для определения мест и методов возможного перехвата обязательно привлечение технического специалиста.

При этом распространенной ошибкой является привлечение специалиста по аппаратуре телефонной связи. Такой специалист, конечно, доступнее, чем ИТ-специалист того же уровня. «Телефонист» лучше разбирается в оборудовании, технологиях и протоколах связи 1-го и 2-го уровня (физический и канальный). Но работать на более высоких уровнях сетевых протоколов (3-7) он не способен. А как раз на этих уровнях лежит большинство возможностей перехвата трафика.

Различных мест и методов для перехвата сетевого трафика слишком много, чтобы перечислить их здесь. Выделим лишь организационные варианты:

- перехват при помощи имеющейся аппаратуры СОРМ;
- перехват средствами оператора связи;

- перехват собственными средствами.

В подавляющем большинстве случаев в перехватываемом трафике может содержаться тайна связи или тайна частной жизни. Поэтому необходимо получать судебное решение. Без судебной санкции возможен перехват своего собственного трафика потерпевшим либо с его письменного разрешения.

Перехват трафика может быть реализован на разных уровнях.

- На физическом уровне:
  - при помощи электрических и оптических разветвителей;
  - при помощи бесконтактных датчиков;
  - при помощи перехвата радиосигнала (для Wi-Fi и других беспроводных протоколов).
- На канальном уровне:
  - при помощи подключения к концентратору\* (хабу);
  - при помощи функции зеркалирования порта на коммутаторе\* (свиче);
  - при помощи ARP-атак и проксирования трафика;
  - при помощи установки снифера\* на целевом или транзитном узле.
- На сетевом уровне:
  - при помощи изменения маршрутизации и проксирования трафика;
  - при помощи встроенных функций межсетевого экрана или системы обнаружения атак (IDS).
- На прикладном уровне:
  - анализом трафика на прокси-сервере (для HTTP-трафика);
  - анализом трафика на сервере электронной почты (для SMTP-трафика).

Формулируя техническое задание для перехвата трафика, следует непременно прикинуть объем информации. При слишком широких условиях соответствующий трафик может достигнуть астрономических величин. Большой объем не уместится на носителе и поэтому не поддастся последующему анализу.

Например, нас интересуют действия пользователя, работающего за домашним компьютером, который подключен к Интернету через местную домовую сеть. В его трафике мы хотели бы найти доказательства неправомерного доступа к удаленным узлам. Было бы ошибкой ставить задачу так: «перехват исходящего и входящего трафика компьютера с IP-адресом 10.0.0.6». Помимо неправомерного доступа подозреваемый также занимается и другой деятельностью. На его компьютере стоит клиент файлообменных сетей\* со средним суммарным трафиком 6 кбайт/с (500 Мбайт за сутки, 50 входящего и 450 исходящего). Кроме того, в домашней сети расположен файловый сервер с набором музыки и фильмов. Пос-

кольку внутренний трафик для пользователей бесплатен и не ограничен, подозреваемый скачивает 1-2 фильма в день и немного музыки (1 Гбайт за сутки). Внутрисетевой служебный трафик составляет за сутки еще порядка 2 Мбайт. Причем все перечисленное — в автоматическом режиме, независимо от присутствия подозреваемого дома. На этом фоне суточные 10 Мбайт веб-трафика, 0,5 Мбайт электронной почты и 0,2 Мбайт по протоколу ICQ просто теряются. А доказательства неправомерного доступа содержатся лишь в последнем пункте. Перехват всего перечисленного трафика (1,5 Гбайт в сутки) за несколько дней потребует диска очень большой емкости, которого может и не оказаться в распоряжении специалиста. И потом найти в этой куче полезные 0,013% будет нелегко.

Если же мы, чтобы исключить внутрисетевой трафик, велим специалисту перехватывать информацию за пределами домашней сети, на выходе из нее, то допустим иную ошибку. Поскольку домашняя сеть подключена к Интернету не напрямую, а через устройство, осуществляющее трансляцию IP-адресов (NAT\*), то в этой точке мы не сможем отличить трафик подозреваемого от трафика всех других пользователей той же домашней сети.

В описанной ситуации правильная формулировка задания должна выглядеть примерно так: «перехват исходящего и входящего трафика компьютера с MAC-адресом 00:15:f2:20:96:54, относящегося к протоколам HTTP, telnet, SMTP, POP, IMAP, ICQ и имеющего в качестве IP-адреса назначения (destination) или происхождения (source) какие-либо внешние IP-адреса, то есть, IP-адреса кроме 10.0.0.0/8».

Анализ и интерпретация перехваченного трафика должны производиться экспертом в ходе КТЭ. Вместо экспертизы можно оформить это как очередное ОРМ, но тогда доказательством в суде перехваченный трафик не будет.

К перехваченному трафику для его анализа необходимо приложить некоторую информацию о конфигурации и состоянии коммуникационного оборудования, чтобы в ходе КТЭ содержимое трафика можно было интерпретировать уверенно, без предположений. Например, в вышеописанном случае для интерпретации понадобится конфигурация коммутатора домашней сети, MAC-таблица на соответствующем его порту, а также конфигурация устройства, производящего трансляцию адресов (NAT).

### **Шифрованный трафик**

Некоторая часть трафика может оказаться зашифрованной. Это касается таких протоколов, как HTTPS, SSH, SMTP/TLS, IPSec и других. В некоторых случаях весь трафик между определенными узлами или сетями подвергается шифрованию — это называется VPN-туннель. Во всех протоколах, даже простейших, сейчас используются стойкие алгоритмы шифрования, дешифровать которые без знания ключа не стоит даже пытаться.

Столкнувшись с зашифрованным трафиком, можно узнать немного: установить сам факт сетевой активности, ее приблизительный объем, а также установить IP-адреса взаимодействующих узлов (кроме случая VPN-туннеля).

Для решения указанной задачи следует установить, где именно производится шифрование, и перехватывать трафик в том месте, где он идет открытым.

Например, производя перехват трафика на внешнем интерфейсе «vr0» сервера доступа, мы увидели следующую картину:

```
# tcpdump -n -i vr0 -xX -s 256 -c 4
```

```
18:15:04.958167 IP 213.148.4.178.5000 > 80.94.84.25.5000: UDP, length: 212
0x0000: 0040 f435 d7c3 0040 63da 3cda 0800 4500 .@.5...@c.<...E.
0x0010: 00f0 7bef 0000 4011 7f50 d594 04b2 505e ..{...@.P....P^
0x0020: 5419 1388 1388 00dc 659d 423e 673d 2225 T.....e.B>g=%
0x0030: 3d3e f779 4fb3 ba35 806f b861 cae4 abbb =>.yO...5.o.a....
0x0040: 23ca c65c faf7 8950 2fdb 01e4 9eb7 e105 #.\\.\\P/.....
0x0050: 4601 58f4 e981 2507 7585 2ab0 0002 0bbb F.X...%.u.*.....
0x0060: 5246 54e0 0c8e f849 5772 c879 52e1 8373 RFT....IWr.yR..s
0x0070: cb25 9815 0e1e 240a fd7a 5e62 bc7e 75a9 .%....$.z^b~.u.
0x0080: d13d d834 ac32 79ff ce43 e744 75a7 1d74 .=.4.2y..C.Du..t
0x0090: d958 4f1b 82bf 66e5 25ed 3a7d 20e4 3c80 .XO...f.%.:}.<.
0x00a0: a747 0a87 f919 0c8e 4d06 610f 4956 f01d .G.....M.a.IV..
0x00b0: 333f 4921 630d cde8 cd73 4538 1e41 8187 3?I!c.....sE8.A..
0x00c0: fae6 658d e7be ebf2 68f0 3bb1 3e0d f5ff .e.....h.;>...
0x00d0: 908e fb90 6c76 1735 c2d6 5874 96b1 1af5 ....lv.5..Xt....
0x00e0: 45b7 0562 6446 1848 1218 42ad 1e99 39b9 E..bdf.H..B...9.
0x00f0: 28aa d7e2 7699 4482 499b 0990 a5ee (...v.D.I.....

18:15:04.958639 IP 213.148.4.178.5000 > 80.94.84.25.5000: UDP, length: 212
0x0000: 0040 f435 d7c3 0040 63da 3cda 0800 4500 .@.5...@c.<...E.
0x0010: 00f0 7bf1 0000 4011 7f4e d594 04b2 505e ..{...@.N....P^
0x0020: 5419 1388 1388 00dc d69a 654c 24ab 2841 T.....eL$. (A
0x0030: 8a74 b88b 110b 7d78 ee9d a54b c274 f704 .t....}x...K.t..
0x0040: 685a 6100 c3a5 d689 cab9 2e04 bcca d4ea hZa.....
0x0050: ede9 c6a2 a8c3 141a d052 cc56 0b90 2018 .....R.V....
0x0060: 1325 442c 20fb 0a08 a1cd 7592 5926 573b .%D,.....u.Y&W;
0x0070: a4ee 17b3 6b37 7a11 fc03 3847 952a 83da ....k7z...8G.*..
0x0080: a825 eaf9 a4d4 2e91 4b5f f2ca ef96 c18d .%.....K_.....
0x0090: 1801 39f4 20d3 117a b57a a5b1 a23c ddf7 ..9.....z.z...<.
0x00a0: 9247 4cd7 d573 1a06 c42d dab0 e64c 7760 .GL.s.....Lw`
0x00b0: 7f3f 3a99 8bb2 2c29 f537 a6ce 86dc eb96 .?:....).7.....
0x00c0: 7897 87e8 4158 78b2 4cd2 736f 9a27 262c x...AXx.L.so.'&,
0x00d0: 6541 785e 69ac 46f1 8a4b 5b0a c409 4923 eAx^i.F..K[...I#
0x00e0: 023b 69a4 b2f0 f2d8 b579 060d 6027 a115 .;i.....y...`'..
0x00f0: a5fe 0f61 860d aa2d 1c6b ceb6 f3cc ...a....-k....

18:15:05.259010 IP 80.94.84.25.5000 > 213.148.4.178.5000: UDP, length: 100
0x0000: 0040 63da 3cda 0040 f435 d7c3 0800 4500 .@c.<...@.5....E.
```

```
0x0010: 0080 b734 0000 3611 4e7b 505e 5419 d594 ...4..6.N{P^T...
0x0020: 04b2 1388 1388 006c 21db 38f8 3e20 65eb .....1!1.8.>.e.
0x0030: dfbc 20ba 5e0a 137e 9ade 447b 0579 0636 ....^...~..D{.y.6
0x0040: 37e5 43d5 3991 7424 44ee b635 b222 d454 7.C.9.t$D..5.».T
0x0050: acee c0a0 2d3b 078d 5e42 aa83 747e 4cfc .....;..^B..t~L.
0x0060: c577 76d4 785d d27b 553a 2f2b d7de 0d29 .wv.x].{U:/+...)
0x0070: 985f 1743 3744 ca4a 470d 4097 ec2a 3d0f _..C7D.JG@...*=.
0x0080: 8eb4 cba6 1854 d08a 18f2 8292 b45a .....T.....Z
```

```
18:15:05.263016 IP 80.94.84.25.5000 > 213.148.4.178.5000: UDP, length: 148
0x0000: 0040 63da 3cda 0040 f435 d7c3 0800 4500 .@c.<...@.5....E.
0x0010: 00b0 b735 0000 3611 4e4a 505e 5419 d594 ...5..6.NJP^T...
0x0020: 04b2 1388 1388 009c de31 9a0d 4907 1e0d .....1..I...
0x0030: 0eb6 1425 6892 7903 b778 f0bc 701a be8b ...%h.y..x..p...
0x0040: 8416 9337 7019 144a 5270 b623 0037 49c0 ...7p..JRp.#.7I.
0x0050: 768b 53d8 471c 589f 80fd b48c 21e3 0cf5 v.S.G.X.....!...
0x0060: 9d27 95ba fb36 6c89 d0ac 9b02 13a1 a170 .'...6l.....P
0x0070: aaea 9c20 0a30 e192 2773 842b c6f7 f85f .....0..'s.+..._
0x0080: a765 f720 24fd be29 849d 3b3c 206f 528e (.e.$..)..

```

По контенту пакетов очевидно, что мы имеем дело с зашифрованным трафиком. Это подтверждается характерным номером порта (5000), который часто используется для организации VPN-туннелей. Перехватывать такой VPN-трафик бессмысленно. Нужно перехватывать его до входа в туннель или после выхода из него. В данном случае, поскольку туннель terminates на этом же компьютере, достаточно изменить интерфейс перехвата — вместо физического интерфейса «vr0» взять виртуальный интерфейс «tun0», соответствующий программному VPN-туннелю. То есть запустить снифер\* «tcpdump» с параметром «-i tun0».

```
# tcpdump -n -i tun0 -xX -s 256 -c 6
```

```
18:24:58.503902 IP 80.94.84.26.22 > 83.222.198.130.64106: P
954349589:954349781(192) ack 1245249879 win 33000 <nop,nop,timestamp
1169732958 3836952>
0x0000: 0200 0000 4510 00f4 7e8a 4000 4006 fc90 ....E...~.@.@...
0x0010: 505e 541a 53de c682 0016 fa6a 38e2 3815 P^T.S.....j8.8.
0x0020: 4a39 0157 8018 80e8 9b06 0000 0101 080a J9.W.....
0x0030: 45b8 b55e 003a 8c18 812c b31d 3e7a 12a3 E..^.:...>z...
0x0040: 90d6 db8b c515 f6fb c344 7b0c 4527 6950 .....D{.E'iP
0x0050: f7da 74ef 2653 e64e bbd4 35f1 1c7b f23b .t.&S.N..5..{.;
0x0060: 049f d235 2907 65e5 1cce ea52 5480 e4c6 (...5).e....RT...
0x0070: 6a73 bf84 8d44 b90b 0bd1 3182 2d17 4014 js....D....1.-.@
0x0080: d0ef e13b ecf0 8635 8670 d620 d31c 6249 ...;...5.p....bI
0x0090: 031a 4e9f b267 0ea7 8325 f85b e9e6 8aab ..N..g...%.[....
0x00a0: f843 1722 b71e bf45 7664 cccb 3de9 3bd7 .C.»...Evd..=;.
```

```

0x00b0: 579a 33f2 24d6 6a0f 763b 4033 db8b 23c3 W.3.$j.v;@3..#.
0x00c0: dd57 e1f2 e903 a93a 1cdd 6a0c d27e 4390 .W.....j...~C.
0x00d0: 4523 c955 c5ec e8ee 0899 1d0b 1e91 b52b E#.U.....+
0x00e0: 4af6 31a4 28c3 34e5 d890 3966 bdb3 17f8 J.1.(.4...9f....
0x00f0: a1f1 cddb 2504 bf3c ....%.<

18:24:58.672890 IP 83.222.198.130.64106 > 80.94.84.26.22: . ack 192 win
32904 <nop,nop,timestamp 3836981 1169732957>
0x0000: 0200 0000 4500 0034 6936 4000 3606 1cb5 ....E..4i6e.6...
0x0010: 53de c682 505e 541a fa6a 0016 4a39 0157 S...P^T...j...J9.W
0x0020: 38e2 38d5 8010 8088 f80d 0000 0101 080a 8.8.....
0x0030: 003a 8c35 45b8 b55d ...5E..]

18:24:58.763472 IP 80.94.110.110.3727 > 80.94.84.26.445: S
3023694823:3023694823(0) win 16384 <mss 1212,nop,nop,sackOK>
0x0000: 0200 0000 4500 0030 bd5f 4000 7406 e623 ....E..0._@.t..#
0x0010: 505e 6e6e 505e 541a 0e8f 01bd b439 ebe7 P^nnP^T.....9..
0x0020: 0000 0000 7002 4000 3065 0000 0204 04bc ....p@.0e.....
0x0030: 0101 0402 ....

18:24:58.889058 IP 83.222.198.130 > 80.94.84.26: icmp 64: echo request seq
927
0x0000: 0200 0000 4500 0054 6937 0000 3601 5c99 ....E..Ti7..6.\.
0x0010: 53de c682 505e 541a 0800 1c73 4e39 039f S...P^T....sN9..
0x0020: 45b6 298a 000e 2f63 0809 0a0b 0c0d 0e0f E.).../c.....
0x0030: 1011 1213 1415 1617 1819 1a1b 1c1d 1e1f .....
0x0040: 2021 2223 2425 2627 2829 2a2b 2c2d 2e2f .!"$%&'()*+,-./
0x0050: 3031 3233 3435 3637 01234567

18:24:58.894094 IP 80.94.84.26.25 > 10.5.0.1.59816: P 1:86(85) ack 1 win
33000 <nop,nop,timestamp 1169744268 483531548>
0x0000: 0200 0000 4500 0089 7ee2 4000 4006 0d0f ....E...~.@.@...
0x0010: 505e 541a 0a05 0001 0019 e9a8 6640 b1dc P^T.....f@...
0x0020: 791d 6448 8018 80e8 3420 0000 0101 080a y.dH....4.....
0x0030: 45b8 e18c 1cd2 1b1c 3232 3020 686f 6d65 E.....220.home
0x0040: 2e66 6e6e 2e72 7520 4553 4d54 5020 5365 .fnn.ru.ESMTP.Se
0x0050: 6e64 6d61 696c 2038 2e31 332e 312f 382e ndmail.8.13.1/8.
0x0060: 3133 2e31 3b20 5475 652c 2032 3320 4a61 13.1;.Tue,.23.Ja
0x0070: 6e20 3230 3037 2031 383a 3236 3a35 3120 n.2007.18:26:51.
0x0080: 2b30 3330 3020 284d 534b 290d 0a +0300.(MSK)..

18:24:58.984199 IP 10.5.0.1.59816 > 80.94.84.26.25: P 1:19(18) ack 86 win
33000 <nop,nop,timestamp 483531595 1169744268>
0x0000: 0200 0000 4500 0046 dac3 4000 4006 b170 ....E..F..@..p
0x0010: 0a05 0001 505e 541a e9a8 0019 791d 6448 ....P^T.....y.dH
0x0020: 6640 b231 8018 80e8 2595 0000 0101 080a f@.1.....
0x0030: 1cd2 1b4b 45b8 e18c 4548 4c4f 2061 6968 ...KE...EHL0.aih
0x0040: 732e 666e 6e2e 7275 0d0a s.fnn.ru..

```

И мы увидим тот же трафик, но уже вне VPN-туннеля. Из шести видимых пакетов 3-й относится к протоколу NETBIOS, 4-й — к протоколу ICMP, 5-й и 6-й пакеты — к протоколу SMTP. А контент первых двух па-

кетов по-прежнему зашифрован: эти пакеты относятся к протоколу SSH со встроенным шифрованием. Получить их в открытом виде перехватом трафика в ином месте нельзя, поскольку шифрование здесь происходит на более высоком уровне (6).

Кстати, этот пример еще раз подтверждает высказанный ранее тезис, что при перехвате сетевого трафика необходимо знать сопутствующую конфигурацию оборудования. В данном примере — конфигурацию интерфейсов сервера доступа. Только благодаря знанию этой конфигурации мы определили, где следует перехватывать трафик, чтобы получить его в нешифрованном состоянии.

## Исследование статистики трафика

Статистика прошедшего трафика собирается на многих устройствах. Все без исключения маршрутизаторы, а также многие иные коммуникационные устройства имеют встроенные функции для сбора разнообразной статистики.

Статистика — это, конечно, не перехват трафика, она не дает доступа к его содержимому. Но и из статистики можно немало почерпнуть для расследования и для доказательства компьютерных преступлений.

В простейших случаях на каждом интерфейсе подсчитывается лишь общее количество полученных и отправленных байтов и пакетов. Настройки по умолчанию предполагают более подробную статистику. Полное архивирование всего трафика ведется лишь в редких случаях и не для всех протоколов.

### Netflow

Часто статистика ведется по формату «netflow». Он предусматривает запись сведений о каждом «потоке» (flow), то есть серии пакетов, объединенных совокупностью IP-адресов, портов и номером протокола [45, 46]. По такой статистике можно установить:

- факт обращения определенного узла (компьютера, идентифицированного IP-адресом) к другому узлу;
- время обращения с точностью до интервала дискретизации (от 5 минут до 1 часа);
- количество переданного и полученного трафика;
- протокол;
- номера портов с обеих сторон (для TCP и UDP).

### Пример

Приведем пример, как при помощи статистики трафика можно получить ценную оперативную информацию.

Потерпевшим было получено сообщение электронной почты, отправленное злоумышленником через анонимайзер «**remailer@aarg.net**». Анонимайзер — это сервер электронной почты, который специально предназначен для сокрытия отправителя (подробнее об анонимайзерах — ниже, в параграфе «Анонимные ремейлеры»). Служебные заголовки сообщения не содержали никакой полезной информации. Логи анонимайзером не ведутся из принципа.

Для вычисления отправителя можно воспользоваться статистикой трафика.

Для начала сделаем следующие предположения: отправитель находится в России, и он отправил свое сообщение на этот анонимайзер непосредственно, а не через другой анонимайзер. При таких условиях можно попытаться вычислить отправителя.

IP-адрес анонимайзера «**remailer@aarg.net**» — **206.132.3.41**. Письмо к потерпевшему пришло 20 января вечером. Значит, отправлено было, скорее всего, в этот же день, поскольку, хотя анонимайзер предусматривает задержку в доставке сообщений, но вводить слишком большую задержку бессмысленно. Будем искать в статистике российских магистральных операторов связи все обращения на IP-адрес **206.132.3.41**, совершенные в течение суток 20.01.07 по протоколу SMTP. Для просмотра статистики используем набор утилит «flow tools».

Итак, для начала, проверим, на какие IP-адреса были обращения за нужную дату по протоколу TCP, на порт 25 (SMTP). Нижеприведенная команда берёт хранящуюся на сервере статистику (**flow-cat**), отфильтровывает из нее протокол TCP (**flow-filter -r6**), отфильтровывает трафик, направленный на порт 25 (**flow-filter -P 25**), и агрегирует данные по IP-адресу назначения (**flow-stat -f8**).

```
fnn@statserver$>flow-cat /data/flows/moscow-bbn/2007/2007-01/2007-01-20/* |
flow-filter -r6 | flow-filter -P 25 | flow-stat -f8 -S3
```

```
# --- ---- ---- Report Information --- ----
#
# Fields:      Total
# Symbols:     Disabled
# Sorting:     Descending Field 3
# Name:        Destination IP
#
# Args:        flow-stat -f8 -S3
#
#
# IPAddr      flows      octets      packets
#
212.12.0.5    100206    3074015739  3155006
195.98.64.73  172775    473707543   947041
213.177.96.24 66199    553528589   838639
```

195.98.64.65	85655	270256429	748457
82.208.117.5	7989	837433907	630376
83.221.165.2	615	872160671	606258
...			
85.113.144.109	19	2036	38
12.40.224.88	1	27848	38
204.136.64.90	1	28001	38
213.140.7.76	1	28447	38
169.253.4.31	1	28395	38
170.148.48.177	1	28425	38
193.120.46.86	1	27824	38
203.63.58.213	1	28017	38
66.151.183.153	1	28503	38
12.7.175.31	1	33541	38
208.148.192.202	2	27997	38
209.47.66.10	1	28437	38
85.10.215.4	1	28365	38
204.58.248.20	1	28425	38
12.4.27.60	1	28401	38
12.47.209.186	1	28413	38
66.150.143.146	1	27860	38
148.235.52.9	1	27977	38
128.83.32.61	1	28431	38
211.76.152.8	1	28431	38
206.132.3.41	2	27995	38
203.77.177.12	1	28485	38
192.44.63.50	1	28449	38
204.64.38.10	1	27864	38
202.57.99.9	1	29005	38
...			

В списке DST-адресов (адресов назначения) мы видим интересующий нас адрес **206.132.3.41** (пятая строка снизу), причем на него зафиксировано 2 обращения (flow), всего 38 пакетов, 27995 байт. Такое небольшое количество пакетов за целые сутки неудивительно. Анонимайзерами пользуются нечасто, поскольку это хоть и относительно безопасно, но не слишком удобно.

Выше мы запрашивали статистику за сутки. Поскольку статистика собирается с интервалом в 15 минут, поинтересуемся, в какой именно интервал времени в течение суток были зафиксированы эти обращения. Поищем их в каждом из четвертьчасовых файлов. То есть произведем поиск, аналогичный предыдущему, но не для всей суточной статистики, а для каждого из 15-минутных интервалов (команда «**for f in ... do**»).

```
fnn@statserver$>for f in /data/flows/moscow-bbn/2007/2007-01/2007-01-20/*;
do ls ${f}; flow-cat ${f} | flow-filter -r6 | flow-filter -P 25 | flow-stat
-f8 -S3 | grep "206.132.3.41"; done
```



[illegible][illegible]

Упоминание искомого IP-адреса нашлось в 2 из 96 файлов. Оказалось, что обращения происходили в интервале 9:30-9:45 и 14:30-14:45, причем во втором случае было передано лишь 2 пакета, а этого недостаточно для полноценной SMTP-сессии. Таким образом, все данные следует искать в файле, содержащем статистику за 9:30-9:45.

```
fnn@statserver$>flow-cat /data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-
v05.2007-01-20.093000+0300 | flow-filter -r6 | flow-filter -P 25 | flow-stat
-f8 -S3 | grep "206.132.3.41"
206.132.3.41      1                27899                36
fnn@statserver$>
```

Выберем из полной статистики за указанный интервал те пакеты, которые относятся к интересующему нас анонимайзеру. Для этого вместо упорядочивания данных по IP-адресу назначения, как в предыдущих случаях (`flow-stat -f8`), запросим полную статистику (`flow-print`) и выделим из нее утилитой «`grep`» те потоки, которые относятся к адресу анонимайзера 206.132.3.41.

```
fnn@statserver$>flow-cat /data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-
v05.2007-01-20.093000+0300 | flow-filter -r6 | flow-filter -P 25 | flow-
print | egrep "IP|206.132.3.41"

srcIP      dstIP      prot  srcPort  dstPort  octets  packets
81.16.118.238 206.132.3.41 6      4453     25       27899   36
fnn@statserver$>
```

Мы видим, что у всех относящихся к делу пакетов один и тот же source-адрес — 81.16.118.238. Это, скорее всего, и есть IP-адрес отправителя. Переданный объем информации, 27899 байт, примерно соответствует (с учетом служебных заголовков и шифрования) длине сообщения, полученного потерпевшим, что косвенно подтверждает правильность нашего вывода.

Вот таким образом заурядная статистика провайдера позволила нам раскрыть инкогнито злоумышленника, понадеявшегося на анонимный ремейлер.

Другая задача, выполняемая при помощи статистики трафика, это обнаружение источника DoS-атаки или иной атаки с подделанными адресами источника (source IP). По статистике видно, из какого интерфейса пришел на маршрутизатор такой пакет, то есть каков был предыдущий узел в его пути. Обратившись к статистике этого предыдущего узла, мы можем узнать предпредыдущий узел и так далее. К сожалению, это задача непростая, придется устанавливать контакт с несколькими провайдерами. Если один из них откажется сотрудничать или не сохранит статистику, то цепочка оборвется.

### Другие данные о трафике

Кроме полного перехвата сетевого трафика и анализа его статистики имеют право на существование промежуточные варианты ОРМ. Полное содержимое трафика может оказаться чересчур объемным, что затрудня-

ет анализ или делает его невозможным в реальном времени. Статистика, напротив, слишком скупа. Промежуточные варианты — это перехват сведений о сетевых соединениях (сессиях) или перехват трафика на основе сигнатур.

### Анализ заголовков пакетов

Сведения о сетевых соединениях или о заголовках пакетов — это то ли урезанный перехват трафика (без сохранения сведений о содержимом пакетов, но лишь об их заголовках), то ли развернутый вариант статистики (когда записывается не агрегированная по времени информация о переданных пакетах).

Например, что можно сказать о компьютере 10.0.4.224, получив следующую информацию о переданных пакетах? Перехват заголовков осуществлялся той же программой «`tcpdump`», что и в примере для главы «Перехват и исследование трафика», но без опций «`-v -x`». Использованный в этот раз фильтр «`tcp and (net 64.12.0.0/16 or net 205.188.0.0/16)`» выделяет из общего потока те пакеты, которые относятся к сетям 64.12.0.0/16 и 205.188.0.0/16 — это сети, где стоят сервера, обслуживающие ICQ.

```
-bash-2.05b$ sudo tcpdump -i fxp0 -n 'tcp and (net 64.12.0.0/16 or net
205.188.0.0/16)'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on fxp0, link-type EN10MB (Ethernet), capture size 96 bytes

15:53:53.968123 IP 205.188.165.249.80 > 10.0.4.224.1728: . ack 2482877808 win
16384
15:53:54.462314 IP 205.188.165.249.80 > 10.0.4.224.1728: P 0:1122(1122) ack 1 win
16384
15:53:54.514242 IP 10.0.4.224.1728 > 205.188.165.249.80: P 1:617(616) ack 1122
win 64413
15:53:54.521192 IP 10.0.4.224.1729 > 205.188.165.249.80: S
3173139757:3173139757(0) win 65535 <mss 1460,nop,nop,sackOK>
15:53:54.866705 IP 205.188.165.249.80 > 10.0.4.224.1729: S
1561008869:1561008869(0) ack 3173139758 win 16384 <mss 1360>
15:53:54.866882 IP 10.0.4.224.1729 > 205.188.165.249.80: . ack 1 win 65535
15:53:54.867122 IP 10.0.4.224.1729 > 205.188.165.249.80: P 1:261(260) ack 1 win
65535
15:53:55.252895 IP 205.188.165.249.80 > 10.0.4.224.1728: . 1122:2482(1360) ack
617 win 16384
15:53:55.259856 IP 205.188.165.249.80 > 10.0.4.224.1728: . 2482:3842(1360) ack
617 win 16384
15:53:55.260369 IP 10.0.4.224.1728 > 205.188.165.249.80: . ack 3842 win 65535
15:53:55.261250 IP 205.188.165.249.80 > 10.0.4.224.1728: . 3842:5202(1360) ack
617 win 16384
15:53:55.462175 IP 10.0.4.224.1728 > 205.188.165.249.80: . ack 5202 win 65535
15:53:55.656819 IP 205.188.165.249.80 > 10.0.4.224.1729: . 1:1361(1360) ack 261
win 16384
```

```
15:53:55.763942 IP 10.0.4.224.1729 > 205.188.165.249.80: . ack 1361 win 65535
15:53:55.911588 IP 205.188.165.249.80 > 10.0.4.224.1728: . 5202:6562(1360) ack
617 win 16384
15:53:55.918786 IP 205.188.165.249.80 > 10.0.4.224.1728: . 6562:7922(1360) ack
617 win 16384
15:53:55.919324 IP 10.0.4.224.1728 > 205.188.165.249.80: . ack 7922 win 65535
15:53:56.349446 IP 205.188.165.249.80 > 10.0.4.224.1729: P 1361:1770(409) ack 261
win 16384
15:53:56.468076 IP 10.0.4.224.1729 > 205.188.165.249.80: . ack 1770 win 65126
15:53:56.698139 IP 205.188.165.249.80 > 10.0.4.224.1728: . 7922:9282(1360) ack
617 win 16384
15:53:56.699544 IP 205.188.165.249.80 > 10.0.4.224.1728: . 9282:10642(1360) ack
617 win 16384
15:53:56.700065 IP 10.0.4.224.1728 > 205.188.165.249.80: . ack 10642 win 65535
15:53:56.705243 IP 205.188.165.249.80 > 10.0.4.224.1728: . 10642:12002(1360) ack
617 win 16384
15:53:56.706685 IP 205.188.165.249.80 > 10.0.4.224.1728: . 12002:13362(1360) ack
617 win 16384
15:53:56.707210 IP 10.0.4.224.1728 > 205.188.165.249.80: . ack 13362 win 65535
15:53:57.429094 IP 205.188.165.249.80 > 10.0.4.224.1728: P 13362:13835(473) ack
617 win 16384
15:53:57.574583 IP 10.0.4.224.1728 > 205.188.165.249.80: . ack 13835 win 65062
```

Можно сказать, что на компьютере с адресом 10.0.4.224 установлена программа ICQ, которая достаточно активно используется. Причем установлена бесплатная версия этой программы, поскольку наряду с приемом и отправкой сообщений (порт 5190) наблюдается прием рекламных баннеров (порт 80). Содержание передаваемых сообщений из перехваченных заголовков пакетов не видно.

### Избирательный перехват

Перехват по сигнатурам используется для защиты информации в таком техническом средстве, как система обнаружения атак (IDS\*). Она ищет в передаваемых пакетах заранее предопределенные последовательности байтов, соответствующие попыткам несанкционированного доступа, активности вредоносных программ, иным неразрешенным или подозрительным действиям.

Аналогично можно построить и анализ трафика подозреваемого — предопределить характерные последовательности (сигнатуры), соответствующие подозрительным действиям. И ловить только сессии, в которых встречаются эти сигнатуры. Например, подозреваемый пользуется услугами провайдера коммутируемого доступа и, следовательно, соединяется с Интернетом с использованием динамического\* IP-адреса. Наряду с ним IP-адреса из той же сети используют еще несколько сотен пользователей. Требуется проконтролировать переписку подозреваемого по электронной почте. Для этого достаточно записывать все SMTP-сессии, исходящие из сети, где расположен компьютер подозреваемого, в кото-

рых встречается последовательность символов «From: <info@e38.biz>», чтобы выделить письма, направленные от подозреваемого любым адресатам через любые промежуточные узлы.

Для такого избирательного перехвата можно использовать почти любую IDS. Многие из них поддерживают довольно сложные сигнатуры со многими условиями.

## Исследование логов веб-сервера

### Значение логов

Автор подметил интересную особенность. Выражения «лог-файлы» или просто «логи\*» легко употребляются оперативниками, следователями всеми участниками процесса, однако мало кто из них четко представляет себе, что это такое. Чиновники Минсвязи норовят заставить операторов «хранить логи в течение трех лет», однако затрудняются сказать, какие именно логи и вообще, что это такое. Государственный обвинитель во время процесса лихо ссылается на «логи провайдера», однако когда ему эти логи показывают, в упор их не узнает, удивляясь, что это за невразумительная цифирь.

Технические же специалисты, которые с лог-файлами сталкиваются ежедневно, для которых это неотъемлемая составляющая каждодневной работы, приходят в недоумение от такого вопроса следователя: «Какая информация записывается в лог-файл?» Да любая! Какую вы пожелаете, такая и записывается.

Поэтому автор считает нужным здесь объяснить, что же такое лог-файл или лог.

Лог — это журнал автоматической регистрации событий, которые фиксируются в рамках какой-либо программы. Обычно каждому событию соответствует одна запись в логге. Обычно запись вносится сразу же после события (его начала или окончания). Записи эти складываются в назначенный файл самой программой либо пересылаются ею другой, специализированной программе, предназначенной для ведения и хранения логов.

Как понятно из определения, в логах могут регистрироваться абсолютно любые события — от прихода единичного ethernet-фрейма до результатов голосования на выборах президента. Форма записи о событии также целиком остается на усмотрение автора программы. Формат лога может быть машинно-ориентированным, а может быть приспособлен для чтения человеком.

Иногда логи ориентированы на цели безопасности и расследования инцидентов. В таких случаях стараются по возможности изолировать логи от системы, события в которой они фиксируют. Если злоумышленник

преодолеет средства защиты и получит доступ в систему, он, возможно, не сможет одновременно получить доступ к логам, чтобы скрыть свои следы.

Почти каждое действие, производимое человеком при взаимодействии с информационной системой, может отражаться в логе прямо или косвенно, иногда даже в нескольких логах одновременно. И логи эти могут быть разбросаны по различным местам, о которых неспециалист даже не догадается.

Чтобы узнать о действиях злоумышленника, получить какие-либо данные о нем при помощи логов, необходимо:

- узнать, какие компьютеры и их программы вовлечены во взаимодействие;
- установить, какие события логируются в каждой из вовлеченных программ;
- получить все указанные логи за соответствующие промежутки времени;
- исследовать записи этих логов, сопоставить их друг с другом.

Вот, например, такое обыденное действие, как просмотр одним пользователем одной веб-страницы. Перечислим вовлеченные в это действие системы, которые в принципе могут вести логи событий:

- браузер пользователя;
- персональный межсетевой экран на компьютере пользователя;
- антивирусная программа на компьютере пользователя;
- операционная система пользователя;
- DNS-сервер (резолвер\*), к которому обращался браузер пользователя перед запросом веб-страницы, а также DNS-сервера (держатели зон), к которым рекурсивно обращался этот резолвер;
- все маршрутизаторы по пути от компьютера пользователя до веб-сервера и до DNS-серверов, а также билинговые системы, на которые эти маршрутизаторы пересылают свою статистику;
- средства защиты (межсетевой экран, система обнаружения атак, антивирус), стоящие перед веб-сервером и вовлеченными DNS-серверами;
- веб-сервер;
- CGI-скрипты, запускаемые веб-сервером;
- веб-сервера всех счетчиков и рекламных баннеров, расположенных на просматриваемой пользователем веб-странице (как правило, они поддерживаются независимыми провайдерами);
- веб-сервер, на который пользователь уходит по гиперссылке с просматриваемой страницы;
- прокси-сервер (если используется);
- АТС пользователя (при коммутируемом соединении с Интернетом —

по телефонной линии) или иное оборудование последней мили (xDSL, Wi-Fi, GPRS и т.д.);

- оборудование COPM со стороны пользователя и со стороны веб-сервера.

Итого может набраться два-три десятка мест, где откладываются взаимно скоррелированные записи, относящиеся к одному-единственному действию пользователя — просмотру веб-страницы.

При более сложных видах взаимодействия появляется еще больше мест, в которых могут остаться следы действий пользователя [72]. Определить все эти места и указать, к кому именно следует обращаться за соответствующими логами, — это задача для ИТ-специалиста. Даже самый продвинутый следователь не в состоянии его заменить. Поэтому привлечение специалиста в таких случаях обязательно.

### Содержание

Логи веб-сервера, как понятно из предыдущего, являются далеко не единственным источником информации о действиях пользователя. Автор даже не станет называть этот источник главным. Один из основных — вот так правильно.

Какие же данные можно найти в логах веб-сервера? Набор таких данных различается в зависимости от типа веб-сервера и его настроек. Чаще всего в логах присутствуют следующие данные:

- IP-адрес клиента;
- время запроса, включая часовой пояс;
- поля HTTP-запроса клиента:
  - идентификатор (логин) пользователя, если присутствует аутентификация,
  - метод,
  - URL запрашиваемой веб-страницы и отдельные его элементы (домен, путь, параметры),
  - версия протокола,
  - истинный IP (при доступе через неанонимный прокси-сервер),
  - идентификационная строка браузера клиента (включая язык и ОС),
  - реферер (referrer), то есть адрес веб-страницы, с которой был осуществлен переход на данную страницу,
  - тип контента ответа веб-сервера (MIME type),
  - любые другие поля;
- код ответа веб-сервера [30] (status code);
- размер ответа веб-сервера (без учета HTTP-заголовка);
- ошибки, происшедшие при доступе к веб-страницам;
- ошибки при запуске CGI-программ.

### Можно ли доверять логам?

Какие данные в логах веб-сервера возможно фальсифицировать, не имея доступа к самому веб-серверу?

Только поля HTTP-запроса. Этот запрос полностью формируется на стороне клиента, поэтому при желании злоумышленник может подставить в него любые поля с любыми значениями.

Зафиксированному в логе IP-адресу можно доверять. Конечно, при этом следует помнить, что это может оказаться IP прокси-сервера или сокс-сервера или иного посредника.

Прочие поля — это внутренние данные веб-сервера (код ответа, размер страницы и т.п.), которым также можно доверять.

Для проверки достоверности данных логов веб-сервера применяется сопоставление записей между собой, а также с иными логами.

Приведем пример из практики, иллюстрирующий полезность сопоставления различных логов. Сотрудник службы информационной безопасности интернет-казино, анализируя логи веб-сервера, заметил, что браузер одного из игроков, согласно полям его HTTP-запросов, поддерживает русский язык. При этом IP-адрес числился за Кореей. Указания же на корейский язык не было. Это возбудило подозрения. Сотрудник проверил, с каких еще адресов обращался пользователь под этим аккаунтом. Оказалось, что с единственного IP. Тогда он проверил, какие еще пользователи обращались с этого же IP. Оказалось, что больше никто этот корейский IP-адрес не использовал. Но сотрудник службы безопасности не успокоился и проверил, какие еще были обращения от браузера с таким же набором настроек (язык, версия браузера, версия ОС, разрешение экрана, принимаемые типы данных). Оказалось, что с такого же браузера было зарегистрировано больше 10 аккаунтов. Все эти пользователи приходили с IP-адресов разных стран, причем страна соответствовала имени пользователя, то есть, например, Джон Смит с IP-адресом США, Ву Пак с IP-адресом Кореи, Ганс Мюллер с IP-адресом Германии и так далее. Но идентичный набор настроек браузера всех этих пользователей (включая поддержку русского языка) вызывал большие подозрения. Когда же сотрудник сопоставил периоды активности всех подозрительных пользователей, он увидел, что они не пересекаются и более того — примыкают один к другому. Он понял, что имеет дело с кардером\*, который регистрирует аккаунты по краденым карточкам, пользуясь сокс-серверами в разных странах. Дальнейшая проверка это подтвердила.

### Исследование системных логов

Логирование событий в операционной системе является одной из трех составляющих безопасности. Имеется в виду модель «AAA» — authentica-

tion, authorization, accounting — аутентификация, авторизация, аудит. Запись всех событий, связанных прямо или косвенно с безопасностью системы, и составляет сущность аудита. Логирование само по себе не препятствует злоумышленнику получить несанкционированный доступ к информационной системе. Однако оно повышает вероятность его выявления, а также последующего нахождения и изобличения злоумышленника. Также логирование способствует выявлению уязвимостей защищаемой системы.

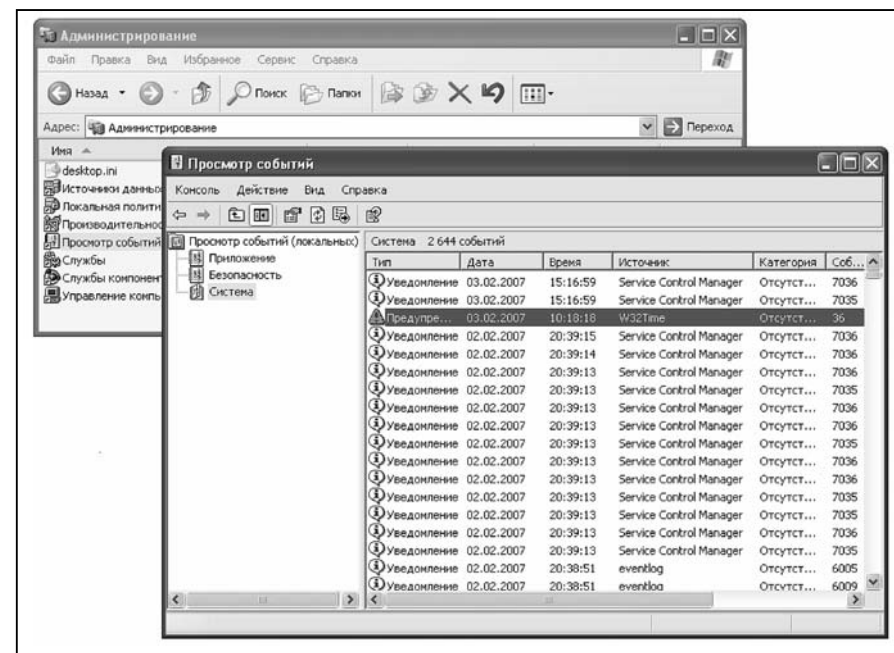
Чем более полон аудит, тем проще расследовать компьютерное преступление. Пользуясь записанными данными, специалист или эксперт может извлечь много полезной для дела информации.

Рассмотрим устройство системного аудита событий для различных классов операционных систем.

### Системные логи Windows

В операционных системах линейки «Windows-NT» — «Windows-2000» — «Windows-XP» предусмотрено три лога — прикладных программ (application log), системы (system log) и безопасности (security log).

В application log пишутся сообщения и события, генерируемые прикладными программами, а также некоторыми сервисами (службами). В system log помещаются события ядра ОС и важнейших сервисов. В security log



Программа «Event Viewer» для просмотра логов в Windows

записываются также события, генерируемые системными сервисами, относящиеся к отслеживаемой активности пользователей, их аутентификации и авторизации. К этим трем могут добавляться иные логи, если на компьютере работают дополнительные программы, такие как DNS-сервер.

По умолчанию логируются очень немногие события, а в security log — вообще никаких. Чтобы в логах осаждалась более полная информация, администратор должен явно включить аудит и настроить политики аудита.

Все логи Windows просматриваются специальной программой «Event Viewer», которую можно найти в меню «Administrative Tools» или «Management Console».

В зависимости от того, что именно мы ищем, следы «взлома» исследуемого компьютера или следы противоправной деятельности пользователя, может оказаться полезной разная информация из разных логов.

### **Системные логи UNIX и Linux**

Несмотря на разнообразие UNIX-подобных операционных систем, у всех у них имеется схожая система сбора и хранения системных логов. Логирование событий в операционной системе «MacOS-X» устроено точно таким же образом.

Специальный демон (процесс), называемый **syslogd**, принимает сообщения о событиях от различных программ и процессов и раскладывает их по соответствующим файлам. Сообщения из одного источника можно направить в разные файлы, сообщения от разных источников можно направить в один и тот же файл — система настраивается довольно гибко. Сообщения о событиях можно принимать как локально, так и через сеть; оба способа используют один и тот же протокол [55].

Каждое сообщение при его генерации снабжается двумя идентифицирующими признаками — приоритет (priority) и ресурс (facility). Их сочетание служит для последующей сортировки полученных сообщений по файлам.

Принятые **syslogd** сообщения снабжаются временной меткой и записываются в обычный текстовый файл по принципу одно сообщение — одна строка. Просмотреть эти сообщения можно в любом текстовом редакторе или иной программой, умеющей работать с текстовыми файлами.

### **Системные логи IOS**

Значительная часть (если не большинство) коммутаторов и маршрутизаторов сети Интернет работают под управлением операционной системы IOS. Другие ОС для коммуникационного оборудования схожи с IOS своими чертами, в частности, ведут логи аналогичным образом. К таким типичным устройствам относится коммуникационное оборудование, выпущенное под марками «Cisco», «Juniper», «Huawei» и некоторыми другими. Оно составляет подавляющее большинство.

В системе IOS логируются следующие события:

- изменение статуса интерфейса или порта;
- авторизация администратора или устройства;
- изменение и сохранение конфигурации устройства;
- прием транзитного пакета, если такой пакет подпадает под правило (ACL entry), отмеченное флагом логирования;
- некоторые другие.

Сообщения о событиях обычно отсылаются на внешний логирующий сервер по протоколу syslog [55] или SNMP. Также несколько последних сообщений хранятся в буфере, в оперативной памяти и могут быть просмотрены соответствующей командой (show logging).

Когда требуется ознакомиться с логами коммуникационного оборудования, следует проделать такие действия:

- получить доступ к текущей конфигурации устройства (конфигурационному файлу), чтобы определить, куда именно отсылаются логи с данного устройства (команда show running-config); сохранить и задокументировать вышеуказанную конфигурацию (или только ее часть, касающуюся логов);
- (опционально) просмотреть содержимое буфера устройства с последними сообщениями;
- определить местоположение логирующего сервера, то есть сервера, принимающего и сохраняющего логи;
- получить доступ к логирующему серверу и ознакомиться с конфигурацией его syslog-демона, чтобы определить, в какой файл складываются логи, принятые от интересующего нас устройства; сохранить и задокументировать вышеуказанную конфигурацию syslog-демона;
- осмотреть или изъять файл (файлы), в котором сохраняются логи с нужного устройства.

Некоторые коммуникационные устройства, относящиеся к меньшинству, не используют ОС IOS или схожую. В таких нетипичных устройствах логирование может быть устроено иначе. В частности, логи могут храниться локально или передаваться на логирующий сервер по нестандартному протоколу.

## **Исследование логов мейл-сервера и заголовков электронной почты**

### **Как устроено**

Сообщение электронной почты обычно создается на компьютере отправителя в специализированной программе, называемой клиентом электронной почты (MUA — mail user agent). Затем оно отправляется на сервер электронной почты (MTA — mail transfer agent) отправителя. Отту-

да — на сервер электронной почты получателя, возможно, через промежуточный сервер электронной почты (релей). На сервере получателя сообщение помещается в почтовый ящик соответствующего пользователя. Из этого ящика при посредстве сервера доставки (MDA) пользователь забирает сообщение при помощи своей программы-клиента электронной почты (MUA).

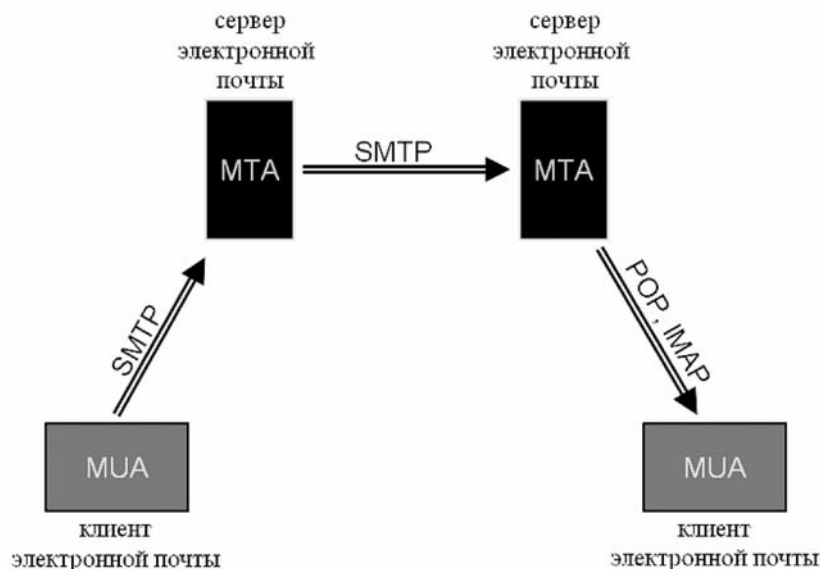


Схема организации передачи электронной почты

Сообщение обычно сохраняется в клиенте (MUA) отправителя и получателя. При прохождении через сервер (MTA) копия сообщения не сохраняется, однако делается запись в логе о его получении и отправке. Также при этом в сообщение вставляется служебный заголовок «Received» — так называемый маршрутный заголовок.

Вместо программы-клиента электронной почты (MUA) отправитель и получатель могут использовать веб-интерфейс сервера электронной почты. Он выполняет те же функции, что и клиент, но работает обычно «вблизи» соответствующего MTA (на том же компьютере или на соседнем). Связь отправителя или получателя с веб-интерфейсом происходит при посредстве браузера.

### Следы

Таким образом, при прохождении сообщения от отправителя к получателю остаются следующие основные следы:

- копия сообщения на компьютере отправителя;
- запись в логе каждого MTA\*, через который сообщение прошло;
- копия сообщения на компьютере получателя с добавленными по пути заголовками.

Кроме того, можно обнаружить дополнительные следы, свидетельствующие о прохождении сообщения:

- иные следы на компьютере отправителя (в логах сетевых соединений, антивируса, персонального межсетевого экрана и т.д.);
- следы в логах провайдеров (например, статистика трафика), через которых осуществлялось соединение между MUA отправителя и MTA отправителя;
- записи в логах антивирусных и антиспамовых программ на всех MTA, через которые прошло сообщение;
- следы, образовавшиеся вследствие обращения всех MTA, через которые прошло сообщение, к соответствующим DNS-серверам как во время приема, так и передачи сообщения;
- следы в логах провайдеров, через которых осуществлялось соединение между MUA получателя и MDA/MTA получателя;
- иные следы на компьютере получателя (в логах сетевых соединений, антивируса, персонального межсетевого экрана и т.д.).

В случаях использования вместо MUA веб-интерфейса к перечисленным следам добавляются следы, характерные для просмотра веб-страниц (см. главу «Исследование логов веб-сервера»). Более подробно об оставляемых следах можно узнать в специализированной литературе [5, 31, 59].

### Примеры

Все примеры в этой главе содержат подлинные данные без изъятий, исправлений и дополнений от автора.

Сообщение электронной почты, отложившееся в архиве исходящих сообщений отправителя:

```

From: Nikolay Nikolaevich Fedotov <fnn@starttelecom.ru>
Organization: Start-Telecom
To: fnn@fnn.ru
Subject: Path test
Date: Fri, 15 Dec 2006 16:00:05 +0300
User-Agent: KMail/1.9.4
X-KMail-Transport: Corporate
MIME-Version: 1.0
Content-Type: text/plain;
    charset="koi8-r"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
Message-Id: <200612151600.05273.fnn@starttelecom.ru>
Status: RO
  
```

X-Status: RSC  
X-KMail-EncryptionState: N  
X-KMail-SignatureState: N  
X-KMail-MDN-Sent:

path test  
--

Nikolay N Fedotov  
Information Security Officer  
Start Telecom Inc. (Russia)

Два фрагмента лога МТА отправителя (прием и передача). Взяты с сервера mail.starttelecom.ru, он же mail1.wimax.ru:

```
16:00:35.57 4 SMTP-21885([83.222.198.130]) got connection on
[81.16.112.3:25](wimax.ru) from [83.222.198.130:51746]
16:00:35.71 4 SMTP-21885([83.222.198.130]) rsp: 220 mail1.wimax.ru
ESMTP CommuniGate Pro 5.0.9
16:00:35.80 4 SMTP-21885([83.222.198.130]) cmd: EHLO fnn.starttele-
com.ru
16:00:35.80 3 DNR-15700(fnn.starttelecom.ru) A:host name is unknown
16:00:35.80 3 SMTP-21885(fnn.starttelecom.ru) failed to resolve
HELO parameter: host name is unknown. Real address is
[83.222.198.130]
16:00:35.80 4 SMTP-21885([83.222.198.130]) rsp: 250-mail1.wimax.ru
host name is unknown fnn.starttelecom.ru\r\n250-DSN\r\n250-SIZE
104857600\r\n250-STARTTLS\r\n250-AUTH LOGIN PLAIN CRAM-MD5 DIGEST-
MD5 GSSAPI MSN NTLM\r\n250-ETRN\r\n250-TURN\r\n250-ATRN\r\n250-NO-
SOLICITING\r\n250-8BITMIME\r\n250-HE
16:00:35.84 4 SMTP-21885([83.222.198.130]) cmd: STARTTLS
16:00:35.84 4 SMTP-21885([83.222.198.130]) rsp: 220 please start a
TLS connection
16:00:35.90 4 SMTP-21885([83.222.198.130]) TLSv1 client hello:
method=RC4_SHA, residual=0, session=34247 < 00 00 85 C7 45 82 9C 73
42 FF 69 04 BF 61 AC 45 0F 1E 45 40 1F B0 BE 2C 72 92 44 C2 F2 55
4D 38>
16:00:35.90 4 SMTP-21885([83.222.198.130]) TLS handshake: sending
'server_hello'
16:00:35.90 4 SMTP-21885([83.222.198.130]) TLS handshake: sending
the certificate
16:00:35.90 4 SMTP-21885([83.222.198.130]) TLS handshake: sending
'hello_done'
16:00:36.07 4 SMTP-21885([83.222.198.130]) TLS client key exchange
processed
16:00:36.07 4 SMTP-21885([83.222.198.130]) security initiated
16:00:36.07 4 SMTP-21885([83.222.198.130]) TLS 'change cipher'
processed
16:00:36.07 4 SMTP-21885([83.222.198.130]) TLS 'change cipher'
sending
16:00:36.07 4 SMTP-21885([83.222.198.130]) TLS 'finish handshake'
processed
16:00:36.07 4 SMTP-21885([83.222.198.130]) TLS handshake: sending
```

```
'finished'
16:00:36.07 4 SMTP-21885([83.222.198.130]) TLS(RC4_SHA) connection
accepted for 'wimax.ru', session 34247
16:00:36.28 4 SMTP-21885([83.222.198.130]) cmd: EHLO fnn.starttele-
com.ru
16:00:36.29 3 DNR-15701(fnn.starttelecom.ru) A:host name is unknown
16:00:36.29 3 SMTP-21885(fnn.starttelecom.ru) failed to resolve
HELO parameter: host name is unknown. Real address is
[83.222.198.130]
16:00:36.29 4 SMTP-21885([83.222.198.130]) rsp: 250-mail1.wimax.ru
host name is unknown fnn.starttelecom.ru\r\n250-DSN\r\n250-SIZE
104857600\r\n250-AUTH LOGIN PLAIN CRAM-MD5 DIGEST-MD5 GSSAPI MSN
NTLM\r\n250-ETRN\r\n250-TURN\r\n250-ATRN\r\n250-NO-SOLICITING\r\n250-
8BITMIME\r\n250-HELP\r\n250-PIPELI
16:00:36.33 4 SMTP-21885([83.222.198.130]) cmd: AUTH PLAIN
bi5mZWRvdG92QHN0YXJ0dGVsZWVbS5ydQBuLmZlZG90b3ZAc3RhcnR0ZWxly29tLnJlA
DIzc2Q3c2Rr
16:00:36.46 2 SMTP-21885([83.222.198.130]) 'n.fedotov@starttele-
com.ru' connected from [83.222.198.130:51746]
16:00:36.46 2 SMTP-21885([83.222.198.130]) 'n.fedotov@starttele-
com.ru' disconnected ([83.222.198.130:51746])
16:00:37.17 4 SMTP-21885([83.222.198.130]) rsp: 235
n.fedotov@starttelecom.ru relaying authenticated
16:00:37.22 4 SMTP-21885([83.222.198.130]) cmd: MAIL
FROM:<fnn@starttelecom.ru> BODY=8BITMIME SIZE=468
16:00:37.22 4 SMTP-21885([83.222.198.130]) rsp: 250 fnn@starttele-
com.ru sender accepted
16:00:37.22 4 SMTP-21885([83.222.198.130]) cmd: RCPT
TO:<fnn@fnn.ru>
16:00:37.22 4 SMTP-21885([83.222.198.130]) rsp: 250 fnn@fnn.ru will
relay mail for an authenticated user
16:00:37.22 4 SMTP-21885([83.222.198.130]) cmd: DATA
16:00:37.22 4 SMTP-21885([83.222.198.130]) rsp: 354 Enter mail, end
with "." on a line by itself
16:00:37.30 4 QUEUE([952839]) closed, nOpen=1
...
16:00:39.69 4 SMTP-77633(fnn.ru) connected to mail.fnn.ru
[80.94.84.25:25], ESMTP
16:00:39.69 4 SMTP-77633(fnn.ru) cmd: EHLO mail1.wimax.ru
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-aihs.fnn.ru Hello
mail1.wimax.ru [81.16.112.3], pleased to meet you
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-ENHANCEDSTATUSCODES
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-PIPELINING
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-8BITMIME
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-SIZE
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-DSN
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-ETRN
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-DELIVERBY
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250 HELP
16:00:39.74 4 SMTP-77633(fnn.ru) Connected. DSN SIZE
16:00:39.74 4 SMTP-77633(fnn.ru) [952840] sending
16:00:39.74 4 SMTP-77633(fnn.ru) cmd: MAIL
FROM:<fnn@starttelecom.ru> SIZE=687
```



```

16:00:40.00 4 SMTP-77633(fnn.ru) rsp: 250 2.1.0
<fnn@starttelecom.ru>... Sender ok
16:00:40.00 4 SMTP-77633(fnn.ru) cmd: RCPT TO:<fnn@fnn.ru>
NOTIFY=FAILURE,DELAY
16:00:40.06 4 SMTP-77633(fnn.ru) rsp: 250 2.1.5 <fnn@fnn.ru>...
Recipient ok
16:00:40.06 4 SMTP-77633(fnn.ru) cmd: DATA
16:00:40.11 4 SMTP-77633(fnn.ru) rsp: 354 Enter mail, end with "."
on a line by itself
16:00:40.11 4 QUEUE([952840]) opened, nOpen=3
16:00:40.11 4 QUEUE([952840]) closed, nOpen=2
16:00:40.17 4 SMTP-77633(fnn.ru) rsp: 250 2.0.0 kBFD0bU6010332
Message accepted for delivery
16:00:40.17 2 SMTP-77633(fnn.ru) [952840] sent to [80.94.84.25:25],
got:250 2.0.0 kBFD0bU6010332 Message accepted for delivery
16:00:40.17 4 SMTP(fnn.ru) [952840] batch relayed
16:00:40.17 2 DEQUEUEER [952840] SMTP(fnn.ru)fnn@fnn.ru relayed:
relayed via mail.fnn.ru
16:00:40.17 4 QUEUE([952840]) dequeued, nTotal=2
16:00:40.17 4 SMTP-77633(fnn.ru) cmd: QUIT
16:00:40.17 2 QUEUE([952840]) deleted
16:00:40.23 4 SMTP-77633(fnn.ru) rsp: 221 2.0.0 aihs.fnn.ru closing
connection
16:00:40.23 4 SMTP-77633(fnn.ru) closing connection
16:00:40.23 4 SMTP-77633(fnn.ru) releasing stream

```

Обратите внимание на идентификатор соединения «kBFD0bU6010332». Он зафиксирован как в логе этого сервера, так и в логе следующего. Он же будет записан в маршрутном заголовке письма.

Фрагмент лога МТА получателя. Взят с сервера mail.fnn.ru:

```

Dec 15 14:00:38 aihs sm-mta[10332]: kBFD0bU6010332: from=<fnn@start-
telecom.ru>, size=661, class=0, nrcpts=1,
msgid=<200612151600.05273.fnn@starttelecom.ru>, proto=ESMTP,
daemon=IPv4, relay=mail1.wimax.ru [81.16.112.3]

```

```

Dec 15 14:00:39 aihs sm-mta[10333]: kBFD0bU6010332: to=fnn@home.fnn,
delay=00:00:01, xdelay=00:00:01, mailer=esmtpl, pri=30881,
relay=home.fnn. [80.94.84.26], dsn=2.0.0, stat=Sent (kBFD0g7M018585
Message accepted for delivery)

```

Фрагмент лога второго МТА получателя, на который предыдущий сервер (mail.fnn.ru) пересылает (forward) всю полученную почту. Взят с сервера home.fnn.ru:

```

Dec 15 16:00:43 home sm-mta[18585]: kBFD0g7M018585: from=<fnn@start-
telecom.ru>, size=877, class=0, nrcpts=1,
msgid=<200612151600.05273.fnn@starttelecom.ru>, proto=ESMTP,
daemon=IPv4, relay=aihs-tun [10.5.0.1]

```

```

Dec 15 16:00:43 home sm-mta[18586]: kBFD0g7M018585:
to=<fnn@home.fnn>, delay=00:00:01, xdelay=00:00:00, mailer=local,
pri=31086, relay=local, dsn=2.0.0, stat=Sent

```

Сообщение в почтовом ящике получателя (хранится там временно, до того как получатель заберет свою почту по протоколу POP):

```

From fnn@starttelecom.ru Fri Dec 15 16:00:43 2006
Return-Path: <fnn@starttelecom.ru>
Received: from aihs.fnn.ru (aihs-tun [10.5.0.1])
    by home.fnn.ru (8.13.1/8.13.1) with ESMTP id kBFD0g7M018585
    for <fnn@home.fnn>; Fri, 15 Dec 2006 16:00:42 +0300 (MSK)
    (envelope-from fnn@starttelecom.ru)
Received: from mail1.wimax.ru (mail1.wimax.ru [81.16.112.3])
    by aihs.fnn.ru (8.13.3/8.13.3) with ESMTP id kBFD0bU6010332
    for <fnn@fnn.ru>; Fri, 15 Dec 2006 14:00:38 +0100 (CET)
    (envelope-from fnn@starttelecom.ru)
Received: from [83.222.198.130] (account n.fedotov@starttelecom.ru
HELO fnn.starttelecom.ru)
    by mail1.wimax.ru (CommuniGate Pro SMTP 5.0.9)
    with ESMTPLSA id 952840 for fnn@fnn.ru; Fri, 15 Dec 2006 16:00:37
+0300
From: Nikolay Nikolaevich Fedotov <fnn@starttelecom.ru>
Organization: Start-Telecom
To: fnn@fnn.ru
Subject: Path test
Date: Fri, 15 Dec 2006 16:00:05 +0300
User-Agent: KMail/1.9.4
MIME-Version: 1.0
Content-Type: text/plain;
    charset="koi8-r"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
Message-Id: <200612151600.05273.fnn@starttelecom.ru>

```

```

path test
--
Nikolay N Fedotov
Information Security Officer
Start Telecom Inc. (Russia)

```

Письмо в архиве входящей почты получателя:

```

From fnn@starttelecom.ru Fri Dec 15 16:00:43 2006
Return-Path: <fnn@starttelecom.ru>
Received: from aihs.fnn.ru (aihs-tun [10.5.0.1])
    by home.fnn.ru (8.13.1/8.13.1) with ESMTP id kBFD0g7M018585
    for <fnn@home.fnn>; Fri, 15 Dec 2006 16:00:42 +0300 (MSK)
    (envelope-from fnn@starttelecom.ru)

```

```
Received: from mail1.wimax.ru (mail1.wimax.ru [81.16.112.3])
  by aihs.fnn.ru (8.13.3/8.13.3) with ESMTTP id kBFD0bU6010332
  for <fnn@fnn.ru>; Fri, 15 Dec 2006 14:00:38 +0100 (CET)
  (envelope-from fnn@starttelecom.ru)
Received: from [83.222.198.130] (account n.fedotov@starttelecom.ru
HELO fnn.starttelecom.ru)
  by mail1.wimax.ru (CommuniGate Pro SMTP 5.0.9)
  with ESMTTPSA id 952840 for fnn@fnn.ru; Fri, 15 Dec 2006 16:00:37
+0300
From: Nikolay Nikolaevich Fedotov <fnn@starttelecom.ru>
Organization: Start-Telecom
To: fnn@fnn.ru
Subject: Path test
Date: Fri, 15 Dec 2006 16:00:05 +0300
User-Agent: KMail/1.9.4
MIME-Version: 1.0
Content-Type: text/plain;
  charset="koi8-r"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
Message-Id: <200612151600.05273.fnn@starttelecom.ru>
```

path test

--

Nikolay N Fedotov  
Information Security Officer  
Start Telecom Inc. (Russia)

Дотошный читатель может самостоятельно сравнить отправленное и полученное сообщение и определить, какие именно служебные заголовки (кроме упоминавшихся маршрутных заголовков «Received») у них отличаются. Также можно сравнить указанные в логах и заголовках моменты времени и сделать из них выводы не только о «скорости» письма, но и о разнице в показаниях часов всех участвующих компьютеров.

Как видно по иллюстрациям, по пути к сообщению добавились три маршрутных заголовка «Received» соответственно трем серверам электронной почты (МТА), через которые сообщение прошло. Эти заголовки добавляются сверху, то есть нижний из них — первый, верхний — последний.

Бывает, что сервер добавляет не один, а два или даже три заголовка, если он производит какую-либо дополнительную, «внутреннюю» обработку или пересылку сообщения, например, передает его на проверку антивирусной программе. Приведем в качестве примера такого случая заголовки другого сообщения, полученного автором (тело сообщения не приводится).

```
From crackpotsaugur's@accion.org Wed Dec 13 02:25:42 2006
Return-Path: <crackpotsaugur's@accion.org>
Received: from aihs.fnn.ru (aihs-tun [10.5.0.1])
  by home.fnn.ru (8.13.1/8.13.1) with ESMTTP id kBCNPfIu006292
  for <fnn@home.fnn.ru>; Wed, 13 Dec 2006 02:25:41 +0300 (MSK)
  (envelope-from crackpotsaugur's@accion.org)
Received: from msk-m10-st01.rtcomm.ru (msk-m10-st01.rtcomm.ru
[213.59.0.34])
  by aihs.fnn.ru (8.13.3/8.13.3) with ESMTTP id kBCNPb2X094397
  for <nfn@fnn.ru>; Wed, 13 Dec 2006 00:25:38 +0100 (CET)
  (envelope-from crackpotsaugur's@accion.org)
Received: from msk-m10-st01.rtcomm.ru (localhost.rtcomm.ru
[127.0.0.1])
  by msk-m10-st01.rtcomm.ru (Postfix) with SMTP id D2E6669E19
  for <nfn@fnn.ru>; Wed, 13 Dec 2006 02:25:37 +0300 (MSK)
Received: from p54BE5FBF.dip.t-dialin.net (p54BE5FBF.dip.t-
dialin.net [84.190.95.191])
  by msk-m10-st01.rtcomm.ru (Postfix) with ESMTTP id
EB48069ED9
  for <nfn@fnn.ru>; Wed, 13 Dec 2006 02:25:35 +0300 (MSK)
Received: from 12.15.162.211 (HELO smtp2.accion.org)
  by fnn.ru with esmtpp (7(6.6-74)?F/ 4.43)
  id 58T.)?-.A-TUD-DX
  for nfn@fnn.ru; Thu, 1 Jan 1998 11:05:44 -0060
From: "Juana Deal" <crackpotsaugur's@accion.org>
To: <nfn@fnn.ru>
Subject: [!! SPAM] It ready
Date: Thu, 1 Jan 1998 11:05:44 -0060
Message-ID: <01bd16a5$34c829f0$6c822ecf@crackpotsaugur's>
MIME-Version: 1.0
Content-Type: text/plain;
  charset="iso-8859-2"
Content-Transfer-Encoding: 7bit
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Office Outlook, Build 11.0.5510
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2905
Thread-Index: Aca6Q,IL*A82<@Y=XJD'59Q+16@.***=
X-SpamTest-Envelope-From: crackpotsaugur's@accion.org
X-SpamTest-Group-ID: 00000000
X-SpamTest-Info: Profiles 597 [Dec 12 2006]
X-SpamTest-Info: {Headers: Spam A269}
X-SpamTest-Method: headers plus
X-SpamTest-Rate: 100
X-SpamTest-Status: SPAM
X-SpamTest-Status-Extended: spam
X-SpamTest-Version: SMTP-Filter Version 3.0.0 [0255], KAS30/Release
X-Anti-Virus: Kaspersky Anti-Virus for MailServers 5.5.2/RELEASE,
bases: 12122006 #236282, status:
notchecked
```

Два заголовка «Received» от одного и того же сервера (2-й и 3-й снизу) означают, что сообщение было обработано в два этапа: сначала принято, потом проверено антивирусно-антиспамовой программой и лишь после этого отослано дальше. При указанной проверке к служебным заголовкам были добавлены еще несколько заголовков, начинающиеся с «X-SpamTest».

### *Можно ли доверять заголовкам?*

Возникает резонный вопрос: насколько сложно фальсифицировать служебные заголовки письма? Например, чтобы направить следствие по ложному пути.

Понятно, что, имея доступ на запись к лог-файлам и к архиву почты, можно изменить любые данные. А что можно фальсифицировать, не имея такого доступа?

Заголовки «From», «To», «Subject», «Date» и некоторые другие представляются клиентской программой (MUA) отправителя и при дальнейшей передаче не изменяются. Поэтому отправитель может их заполнить по собственному усмотрению. Если клиентская программа этого сделать не позволяет, надо использовать другую программу или даже обойтись вовсе без нее, составив сообщение в любом текстовом редакторе и передав серверу через telnet. То есть заголовкам «From», «To», «Date» и «Reply-To» доверять нельзя.

Заголовок «Return-Path» проставляется принимающим сервером электронной почты, но его содержимое извлекается из команды «mail from», которую отдает клиентская сторона во время сеанса связи (SMTP-сессии). Соответственно, этот заголовок тоже может быть фальсифицирован.

Заголовки «Received» проставляются принимающим сервером. Поэтому передающая сторона подставить в них произвольные данные не может. Однако фальсификатор может поставить в передаваемое сообщение несколько подложных «Received», как будто сообщение уже ранее прошло через некие сервера. При получении сервер не проверяет соответствия последнего маршрутного заголовка «Received» и адреса передающего узла, поэтому такая подмена возможна. Однако последующие маршрутные заголовки будут добавляться уже вне контроля фальсификатора. Таким образом, можно доверять тому заголовку, который добавлен явно независимым, не находящимся под контролем злоумышленника сервером, а также всем последующим. Прочие заголовки «Received» следует проверять, сверяя их с записями в логах соответствующих серверов электронной почты.

Пример подложного заголовка можно увидеть на последней из иллюстраций в предыдущем параграфе. Первый (самый нижний) заго-

ловок «Received: from 12.15.162.211 (HELO smtp2.accion.org) by fnn.ru...» явно подложный, поскольку проставлен он от имени несуществующего сервера «fnn.ru» из домена, который принадлежит получателю. Это довольно распространенная уловка для рассылки спама\*.

### *Формат сообщений*

Сообщения электронной почты имеют многовариантный, неоднократно расширявшийся формат, который определяется соответствующим стандартом [31].

В качестве приложений допустимы различные типы данных, в том числе произвольные, бинарные. При отправке и получении сообщений электронной почты клиентские программы стараются кодировать и декодировать данные без участия и ведома пользователя. Хранящийся в архиве исходный текст сообщения (см. примеры выше) часто совсем не похож на то, что видно в почтовом клиенте.

Содержимое тела сообщения и приложений может кодироваться несколькими различными способами: UUENCODE, Base64, quoted-printable. Оно может быть в обычном, текстовом формате, в HTML-формате или в обоих сразу.

В рамках данной книги невозможно описать всего разнообразия контента электронной почты, поэтому отошлем читателя к соответствующей литературе [2, 23, 31].

### *Документирование прохождения сообщений*

В рамках предварительного следствия необходимо не только исследовать электронные следы с целью установления истины, но и добывать пригодные доказательства. То есть документировать действия в порядке, установленном УПК.

Предположим, в рамках расследования необходимо доказать факт направления сообщения электронной почты от подозреваемого к потерпевшему. Какие доказательства необходимо собрать для этого и как их закрепить? Автор предлагает три варианта — нестрогий, промежуточный и строгий.

### *Деревенский вариант*

Производится осмотр или экспертиза компьютера отправителя. Из архива отправленных извлекается, распечатывается и приобщается к делу интересующее нас сообщение.

Производится осмотр или экспертиза компьютера получателя. Из архива полученных извлекается, распечатывается и приобщается к делу интересующее нас сообщение.

Оба вышеуказанных сообщения сравниваются. Должны совпасть тело письма (возможно, с точностью до кодировки) и основные служебные заголовки. Из этого совпадения делается вывод о том, что сообщение реально было отправлено и получено.

### **Провинциальный вариант**

В дополнение к копиям сообщения с компьютеров отправителя и получателя к делу приобщается также документ о логах хотя бы одного сервера электронной почты (МТА), через который сообщение прошло, — протокол осмотра, заключение эксперта или, в крайнем случае, письменный ответ провайдера на запрос. Сервер должен находиться под управлением незаинтересованного лица, обычно это оператор связи. Данные из лога должны коррелировать с заголовками из полученного сообщения.

Таким образом, в лице независимого сервера появляется третья «точка опоры».

### **Столичный вариант**

В деле должно иметься не менее трех независимых друг от друга свидетельств о прохождении письма. Например, компьютер отправителя, компьютер получателя и МТА провайдера. Либо компьютер получателя и МТА двух «промежуточных» провайдеров. Каждое должно быть закреплено экспертизой. Естественно, данные должны коррелировать.

### **Анонимные ремейлеры**

Анонимизирующие транзитные сервера электронной почты — ремейлеры — предназначены для сокрытия отправителей сообщений, которые, согласно официальной политике этих серверов, «могут опасаться незаконных преследований или политических репрессий». Рассылка спама\* через такой ремейлер невозможна — для этого предприняты соответствующие технические меры.

Пользователь отправляет сообщение на специальный адрес. Ремейлер получает его, расшифровывает, обрабатывает предусмотренным образом и затем отсылает на адрес, указанный пользователем в специальной команде в теле письма.

Функциональность и особенности хороших ремейлеров на сегодняшний день таковы:

- прием почты только в зашифрованном виде (с сильной криптографией);
- удаление всех без исключения служебных заголовков исходного письма;
- удаление всех других идентифицирующих признаков исходного письма;
- возможность вставлять произвольные заголовки;
- возможность задавать произвольную задержку в отправке;

- возможность «холостых» писем;
- возможность выстраивать цепочки из ремейлеров;
- гарантии отсутствия логов;
- расположение ремейлера в стране с либеральным законодательством;
- использование SMTP/TLS с соответствующими сертификатами;
- письма с приложениями (аттачами);
- использование отправителем обычного ПО, без каких-либо добавлений;
- встроенный антивирус.

Как правило, всё взаимодействие пользователя с ремейлером производится по электронной почте при помощи сообщений. Веб-сайты есть не у всех анонимайзеров, ибо наличие веб-сайта снижает анонимность.

В основном ремейлеры построены на программном обеспечении двух типов: «Cypherpunk» и «Mixmaster». Оба кода являются открытыми проектами.

Помимо описанных «канонических» ремейлеров существует великое множество коммерческих проектов на основе проприетарного ПО для анонимизации отправки электронной почты и других действий пользователей. Подписка на такие услуги обходится пользователю от 2 до 20 долларов ежемесячно. Как правило, требуется установить на рабочей станции пользователя программное обеспечение, которое взаимодействует с сервером и обеспечивает проксирование трафика.

Довольно часто подобные сервисы представляют собой заурядный обман потребителей, то есть они как-то работают, но анонимности не обеспечивают. Владельцев таких сервисов можно понять. Кому же захочется выглядеть перед властями соучастником и укрывателем террористов, хакеров, спамеров и прочих правонарушителей, да еще за такие смешные деньги?

История знает несколько случаев, когда владельцы анонимизирующих ремейлеров, несмотря на декларации об отсутствии логов, все же предоставляли властям сведения об IP-адресах отправителей. В некоторых странах попросту запрещено не вести логов или не сохранять их в течение положенного времени, например, в США. В таких странах настоящий анонимизирующий ремейлер работать не может. Но во многих странах законодательство довольно либерально и вполне позволяет предоставлять подобный сервис и не вести логи.

Некоторые анонимизирующие провайдеры (как, впрочем, и иные провайдеры) склонны сотрудничать с правоохранительными органами в деле установления личности своих клиентов, некоторые — нет. Сказать наперед, предоставит ли информацию тот или иной оператор связи, нельзя. В одних странах операторы обязаны это делать и подлежат наказанию в случае отказа. В других странах операторы такой обязанности не имеют. Тем не менее бывает по-разному. В первом случае все равно можно получить от оператора отказ под благовидным предлогом. А во втором

случае оператор может «сдать» своего клиента, которому обещал анонимность, особенно если информацию запросит местная полиция, у которой свои собственные рычаги влияния. На что можно твердо надеяться — так это на то, что оператор прекратит предоставление услуг клиенту, замешанному в криминальной деятельности, поскольку это может отрицательно сказаться на самом операторе.

### Установление принадлежности и расположения IP-адреса

Почти в каждом уголовном деле, связанном с сетью Интернет, присутствовала такая задача: по известному IP-адресу установить использующий его компьютер и местоположение этого компьютера.

Как правило, цепочка доказательств выглядит именно таким образом:

**(преступление) — (IP-адрес) — (компьютер) — (человек)**

При помощи различных технических средств фиксируется IP-адрес, с которого осуществлялась криминальная деятельность. Затем устанавливается компьютер, который использовал данный IP-адрес, факт такого использования закрепляется экспертизой. Затем следует доказать, что этим компьютером в соответствующее время управлял подозреваемый.

Вторая из упомянутых задач — найти компьютер по его IP-адресу — и будет предметом рассмотрения в данной главе.

#### Уникальность

IP-адрес является уникальным идентификатором компьютера или иного устройства в сети Интернет. Это значит, что в пределах всей глобальной компьютерной сети в каждый момент времени только один-единственный компьютер может использовать определенный IP-адрес. Из этого правила имеется целый ряд исключений:

- приватные\*, или так называемые «серые» IP-адреса;
- коллективные, или мультикастовые (multicast) IP-адреса;
- сетевые и широковещательные (broadcast) IP-адреса;
- не выделенные или не присвоенные регистратором IP-адреса;
- IP-адреса, относящиеся к территориально распределенным кластерам компьютеров.

Если же IP-адрес относится к категории публичных\* (так называемых «белых») адресов, если он должным образом выделен одним из регистраторов, то этот адрес будет маршрутизироваться. То есть IP-пакет, отправленный на этот адрес из любой точки Интернета, найдет свою цель. Это значит, что данный IP-адрес — уникальный. И возможно установить компьютер, которому принадлежит этот IP-адрес.

Является ли тот или иной IP-адрес уникальным, не принадлежит ли он к упомянутым исключениям — это устанавливает специалист или эксперт.

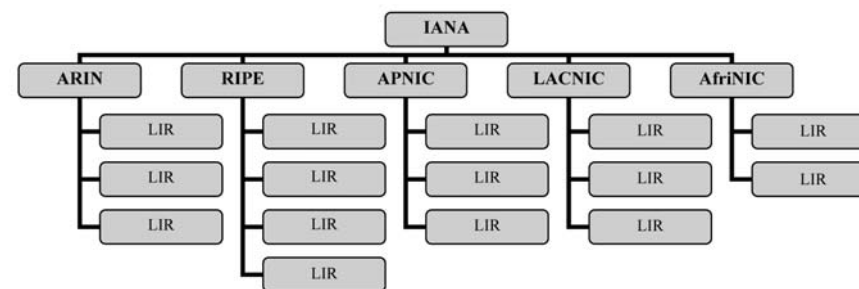
#### Регистраторы

Выделением и регистрацией IP-адресов в Интернете занимаются организации, именуемые регистраторами IP-адресов (IP Registry). Это организации, являющиеся органами самоуправления\* Интернета.

Регистраторы образуют трехуровневую иерархию: IANA — RIR — LIR.

Организация IANA является главным регистратором, она выделяет самые крупные блоки IP-адресов региональным регистраторам и большим организациям.

Региональных регистраторов (RIR) в настоящее время пять. Это ARIN (Северная Америка), RIPE (Европа и Центральная Азия), APNIC (Азиатско-Тихоокеанский регион), LACNIC (Латинская Америка), AfriNIC (Африка). Они выделяют крупные и средние блоки адресов местным регистраторам (LIR), а также ведут базу данных выделенных IP-адресов и предоставляют доступ к ней.



Местные регистраторы (LIR) выделяют мелкие блоки IP-адресов операторам связи и потребителям и регистрируют их в базе данных своего регионального регистратора. Как правило, роль местного регистратора исполняет оператор связи (интернет-провайдер). Таких регистраторов — несколько тысяч.

Все выделенные IP-адреса регистрируются в специальной базе данных, которую поддерживает региональный регистратор (RIR). Сведения из этой базы данных (за исключением некоторых полей) доступны любому лицу по протоколу whois [22]. Обратиться к этой базе достаточно просто. При наличии доступа в Интернет надо набрать в командной строке «whois <ip-адрес>». Такая команда имеется в любой операционной системе, кроме Windows. Для тех, кому она недоступна или неудобна, есть многочисленные веб-интерфейсы, то есть веб-страницы, на которых можно ввести запрашиваемый IP-адрес и получить ответ из соответствующей базы данных при помощи браузера.

**Установление принадлежности IP-адреса через whois-клиент**

Давайте для примера попробуем установить, где живет в настоящее время известный экстремистский ресурс «Кавказ-центр». Определим соответствующий ему IP-адрес и спросим об этом IP-адресе регистратора RIPE. Команда «host» разрешает доменное имя в IP-адрес, а последующая команда «whois3» связывается с whois-сервером указанного регистратора, делает запрос к его базе данных и выводит на экран всю полученную информацию.

```
$>host www.kavkazcenter.com
www.kavkazcenter.com has address 88.80.5.42

$>whois3 -B 88.80.5.42
% This is the RIPE Whois query server #1.
% The objects are in RPSL format.
%
% Note: the default output of the RIPE Whois server
% is changed. Your tools may need to be adjusted. See
% http://www.ripe.net/db/news/abuse-proposal-20050331.html
% for more details.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html

% Information related to '88.80.2.0 - 88.80.7.255'
```

```
inetnum:      88.80.2.0 - 88.80.7.255
netname:      PRQ-NET-COLO
descr:        prq Inet POP STH3
descr:        Co-located customer servers
country:      SE
admin-c:      pIN7-RIPE
tech-c:       pIN7-RIPE
status:       ASSIGNED PA
notify:       registry-ripenotify@prq.se
mnt-by:       MNT-PRQ
changed:      registry-ripe@prq.se 20051125
source:       RIPE

role:         prq Inet NOC
address:      prq Inet
              Box 1206
              SE 11479 Stockholm
              Sweden
phone:        +46 (0)8 50003150
e-mail:       noc@prq.se
e-mail:       registry-ripe@prq.se
remarks:      !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
remarks:      ! Abuse reports should ONLY be sent to abuse@prq.se !
remarks:      ! Do NOT call unless it's very urgent                !
remarks:      !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
admin-c:      PW1115-RIPE
```

```
admin-c:      AC9661-RIPE
tech-c:       PW1115-RIPE
tech-c:       AC9661-RIPE
nic-hdl:      pIN7-RIPE
mnt-by:       MNT-PRQ
changed:      registry-ripe@prq.se 20040707
changed:      registry-ripe@prq.se 20050802
changed:      registry-ripe@prq.se 20060308
changed:      registry-ripe@prq.se 20060324
changed:      registry-ripe@prq.se 20060508
source:       RIPE
abuse-mailbox: abuse@prq.se
```

```
% Information related to '88.80.0.0/19AS33837'
```

```
route:        88.80.0.0/19
descr:        prq Inet aggregated route
origin:       AS33837
notify:       registry-ripenotify@prq.se
mnt-by:       MNT-PRQ
changed:      registry-ripe@prq.se 20051124
source:       RIPE
```

Из полученного ответа усматривается, что диапазон IP-адресов с 88.80.0.0 по 88.80.31.255 выделен шведскому оператору связи «prq Inet». Из этого диапазона меньший поддиапазон с 88.80.2.0 по 88.80.7.255 используется как «Co-located customer servers», то есть для клиентских серверов на колокации\*. В их числе и интересующий нас 88.80.5.42 (www.kavkazcenter.com).

«Соседями» домена «www.kavkazcenter.com», то есть доменами, имеющими тот же IP-адрес, оказались, согласно данным проекта «IP Neighbors Domain Check» [W06], следующие:

```
kavkaz.org.uk
kavkaz.tv
kavkaz.uk.com
kavkazcenter.com
kavkazcenter.info
kavkazcenter.net
old.kavkazcenter.com
pda.kavkaz.tv
pda.kavkazcenter.com
wap.kavkaz.tv
```

Из чего можно заключить, что на этом сервере живут только проекты одного клиента. Это значит, что сервер — выделенный, принадлежит клиенту или целиком арендуется им у провайдера.

### Установление принадлежности IP-адреса через веб-форму

Тот же результат можно получить, сделав запрос через веб-форму на веб-сайте RIPE — Европейского регистратора IP-адресов или каком-либо другом веб-сайте, имеющем аналогичную функцию.

Разница между получением справки через whois-клиент и веб-форму невелика. Источник тот же. Просто во втором случае добавляется еще один технический посредник в лице чужого веб-сайта.



Запрос  
whois-сервера  
через веб-форму

### Корректность

Можно ли доверять данным, полученным таким способом? Обязанности по внесению, изменению и удалению записей лежат на местных регистраторах (LIR). Но за исполнением этих обязанностей строго не следят. Местный регистратор может несвоевременно обновить запись или же, чтобы облегчить себе работу, зарегистрировать одной записью диапазон адресов, выделенных нескольким разным клиентам. Кроме того, данные о пользователях IP-адресов заносятся, как правило, со слов клиента, без должной верификации. Всё это приводит к тому, что среди записей указанной базы данных встречаются неверные — устаревшие или с неполными, некорректными сведениями.

Поэтому всецело доверять таким сведениям не следует. Как правило, сведения о местном регистраторе (LIR) — верные, поскольку LIR является членом регионального регистратора (RIR), имеет с ним договор, платит членские взносы, постоянно взаимодействует. А сведения о клиенте LIR'a, непосредственном пользователе IP, подлежат дальнейшей проверке.

### Трассировка IP-адреса

Также некоторую помощь в установлении местоположения и принадлежности IP-адреса может оказать программа «tracert», которая имеется в составе любой операционной системы, даже Windows.

Принцип действия этой программы таков. С компьютера исследователя испускаются IP-пакеты, адресованные на целевой IP-адрес. Обычно это пакеты протокола UDP, но можно использовать и любой другой. Поле TTL каждого испущенного пакета выставляется последовательно равным 1, 2, 3 и так далее. Это поле предназначено для исключения перегрузки каналов на случай образования петель маршрутизации, то есть замкнутых маршрутов. При прохождении каждого маршрутизатора (маршрутизирующего устройства) поле TTL уменьшается на единицу. При достижении значения 0 этот IP-пакет сбрасывается, а в адрес отправителя посылается специальное уведомление — сообщение протокола ICMP [80], тип 11, код 0. Следовательно, пакет с TTL=1 будет сброшен на первом маршрутизаторе по пути следования, пакет с TTL=2 — на втором маршрутизаторе и так далее. По обратному адресу принятых ICMP-пакетов компьютер исследователя устанавливает, через какие узлы пролегает маршрут до целевого компьютера.

Вот пример работы программы «tracert». Попробуем с ее помощью определить, где располагается сервер [www.microsoft.com](http://www.microsoft.com).

```
$>tracert www.microsoft.com
tracert: Warning: www.microsoft.com has multiple addresses; using
207.46.18.30
tracert to 1b1.www.ms.akadns.net (207.46.18.30), 64 hops max, 40
byte packets
 1 gw.mkfinance.ru (10.0.4.61) 0.264 ms 0.238 ms 0.281 ms
 2 D1-MCH-gi0-2.80.rusmedia.net (83.222.194.1) 63.927 ms 48.689
ms *
 3 C1-M9-gi1-3-0.3.rusmedia.net (212.69.98.229) 26.845 ms 48.375
ms 21.793 ms
 4 msk-dsr5-v1305.rt-comm.ru (195.161.4.153) 36.798 ms 64.589 ms
79.828 ms
 5 195.50.92.1 (195.50.92.1) 111.559 ms 125.433 ms 123.118 ms
 6 ae-0-56.bbr2.London1.Level3.net (4.68.116.162) 93.407 ms ae-0-
52.bbr2.London1.Level3.net (4.68.116.34) 200.311 ms 100.872 ms
 7 as-0-0.bbr1.SanJose1.Level3.net (64.159.1.133) 253.125 ms ae-0-
0.bbr2.SanJose1.Level3.net (64.159.1.130) 258.511 ms as-0-
0.bbr1.SanJose1.Level3.net (64.159.1.133) 445.133 ms
 8 ge-4-0-0-56.gar1.SanJose1.Level3.net (4.68.123.162) 248.892 ms
ge-2-0-0-51.gar1.SanJose1.Level3.net (4.68.123.2) 348.158 ms ge-4-
0-0-52.gar1.SanJose1.Level3.net (4.68.123.34) 318.136 ms
 9 MICROSOFT-C.gar1.SanJose1.Level3.net (209.245.144.110) 229.556
ms 338.955 ms 234.984 ms
10 ge-7-3-0-45.sjc-64cb-1b.ntwk.msn.net (207.46.45.35) 289.415 ms
253.833 ms 245.386 ms
11 ten9-2.bay-76c-1b.ntwk.msn.net (207.46.37.166) 253.875 ms
383.844 ms 355.371 ms
12 ten8-3.bay-76c-1d.ntwk.msn.net (64.4.63.2) 310.604 ms 245.782
ms 273.315 ms
13 po33.bay-6nf-mcs-3b.ntwk.msn.net (64.4.63.90) 245.387 ms
```

```

260.270 ms 257.520 ms
14 * po33.bay-6nf-mcs-3b.ntwk.msn.net (64.4.63.90) 297.405 ms !X *
15 po33.bay-6nf-mcs-3b.ntwk.msn.net (64.4.63.90) 251.177 ms !X *
440.829 ms !X

```

Как видим, пакеты шли через узлы провайдера «**rusmedia.net**» (шаги 2 и 3), затем через «**rt-comm.ru**» (шаг 4), потом через «**level3.net**» (6-9). На девятом шаге пакет, очевидно, перешел в сеть «Майкрософт», потому что соответствующий маршрутизатор имеет в своем имени «**microsoft**», хотя это имя в домене «**level3.net**». Все прочие шаги — внутри корпоративной сети Майкрософта (**msn.net**). В именах транзитных маршрутизаторов мы можем заметить названия «**msk**» (Москва), «**london**» (Лондон) «**sanjose**» (Сан-Хосе) — это дает представление об их физическом расположении. Финальный сервер, скорее всего, тоже стоит в городе Сан-Хосе.

Попробуем трассировать тот же сервер из другого места Интернета.

```

fnn@home$>tracert 207.46.18.30
tracert to 207.46.18.30 (207.46.18.30), 64 hops max, 40 byte packets
 1 aihs-tun (10.5.0.1) 81.374 ms 77.511 ms 117.574 ms
 2 bg-aihs.net (80.94.80.1) 101.864 ms 106.277 ms 63.229 ms
 3 v283.mpd01.fra03.atlas.cogentco.com (149.6.81.37) 227.850 ms
267.295 ms 221.259 ms
 4 t13-0-0.core01.fra03.atlas.cogentco.com (130.117.1.221) 93.270
ms 113.874 ms 88.356 ms
 5 t4-3.mpd01.fra03.atlas.cogentco.com (130.117.0.246) 180.930 ms
188.143 ms 179.462 ms
 6 t4-1.mpd01.par02.atlas.cogentco.com (130.117.2.14) 183.689 ms
176.424 ms 167.548 ms
 7 t2-2.mpd02.par01.atlas.cogentco.com (130.117.2.81) 175.570 ms
170.390 ms 178.438 ms
 8 g5-1.mpd01.par01.atlas.cogentco.com (130.117.2.49) 205.371 ms
190.409 ms 170.393 ms
 9 p14-0.core01.jfk02.atlas.cogentco.com (130.117.1.245) 158.309
ms 164.527 ms 164.132 ms
10 p4-0.core02.dca01.atlas.cogentco.com (66.28.4.81) 163.937 ms
167.115 ms 167.780 ms
11 t4-3.mpd01.dca01.atlas.cogentco.com (154.54.5.57) 171.609 ms
174.707 ms 187.524 ms
12 v3498.mpd01.dca02.atlas.cogentco.com (154.54.7.6) 173.299 ms
172.891 ms 180.584 ms
13 t2-2.mpd01.iad01.atlas.cogentco.com (154.54.1.78) 174.717 ms
176.820 ms 244.616 ms
14 ge5-1.edge1.ash1.us.msn.net (154.54.10.102) 167.459 ms 181.929
ms 181.873 ms
15 207.46.47.92 (207.46.47.92) 179.655 ms 170.900 ms 202.355 ms
16 so-6-0-0-0.pao-64cb-1a.ntwk.msn.net (207.46.33.61) 242.773 ms
303.281 ms 326.135 ms
17 * ten9-2.bay-76c-1c.ntwk.msn.net (207.46.37.161) 272.496 ms
259.461 ms

```

```

18 po34.bay-6nf-mcs-3b.ntwk.msn.net (64.4.63.98) 247.020 ms
250.746 ms 291.349 ms
19 po34.bay-6nf-mcs-3b.ntwk.msn.net (64.4.63.98) 339.056 ms !X *
242.941 ms !X
fnn@home$>

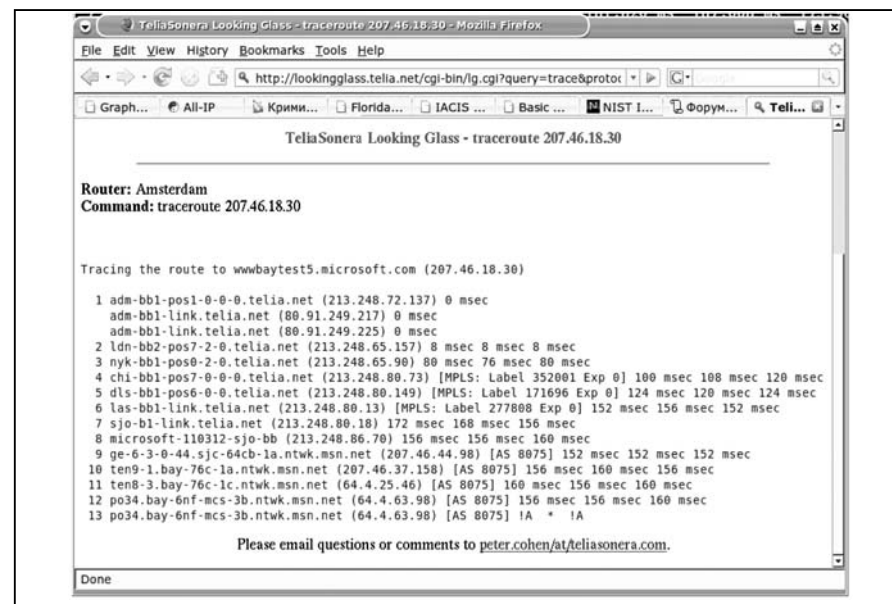
```

Путь пакетов пролегает через провайдера «**Cogent Communications, Inc.**» (**cogentco.com**), откуда непосредственно переходит в корпоративную сеть «Майкрософта» (**msn.net**).

Кроме IP-адресов установленных в ходе трассировки узлов указаны соответствующие им доменные имена. Среди операторов связи принято назначать маршрутизаторам доменные имена, говорящие об их принадлежности и географическом расположении. Поэтому можно приблизительно судить о местоположении и подключении целевого адреса. В показанном примере в именах маршрутизаторов мы видим метки городов: «**fra**» (Франкфурт-на-Майне), «**par**» (Париж), «**jfk**» (Нью-Йорк), «**dca**» (Вашингтон), «**iad**» (Вашингтон), «**ash**» (Эшбурн), «**pao**» (Пало-Альто). Эти метки-аббревиатуры взяты из кодов аэропортов соответствующих городов.

Иногда полезно трассировать искомый адрес из разных точек Сети, как бы с разных сторон, чтобы получить более надежные сведения. Для этого можно воспользоваться многочисленными публичными сервисами «**looking glass**», которые установлены у разных провайдеров и доступны через веб-формы.

Попробуем трассировать тот же адрес из третьей точки при помощи такого инструмента.



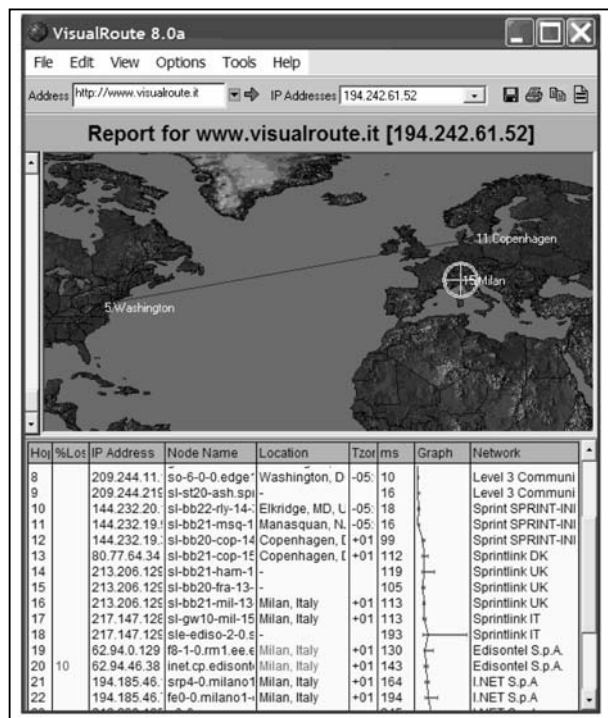
Веб-интерфейс для трассировки адреса с узла провайдера («**looking glass**»)



Путь пакета обозначается кодами: adm (Амстердам), ldn (Лондон), нук (Нью-Йорк), chi (Чикаго), dls (Даллас), las (Лос-Анджелес), sjo (Сан-Хосе).

В этом случае сети «Телии» и «Майкрософта», очевидно, стыкуются в Сан-Хосе (код «sjo», см. шаги 7-8).

У каждого провайдера свои принципы наименования маршрутизаторов и свои условные обозначения. Тем не менее все стараются придерживаться определенных правил и использовать понятные мнемоники [W25]. В случае неясности можно попробовать посмотреть whois-запись для соответствующего IP-адреса, в ней также можно найти указание на географическое расположение.



Визуальный  
трассировщик  
IP-адреса

Операции по анализу результатов трассировки IP-адреса, их сопоставлению с географией частично поддаются автоматизации. Есть несколько программ, которые с большим или меньшим успехом идентифицируют промежуточные узлы в трассировке.

К сожалению, нельзя полностью доверять доменным именам узлов, которые определяются программой «traceroute». Следить за корректностью этих имен провайдеры не обязаны. Так что результаты трассировки могут служить лишь косвенным указанием на местоположение компьютера.

Кроме того, «traceroute», работая исключительно на 3-м (сетевом) уровне, не видит туннели, VPN, MPLS и некоторые иные особенности организации сети. В качестве иллюстрации читателю предлагается самостоятельно попробовать определить при помощи трассировки географическое местоположение домашнего компьютера автора «home.fnn.ru».

### Неуловимый IP

Приведем еще один интересный пример. Это «зомби-хостинг», то есть содержание публичных сетевых ресурсов не на серверах, а на компьютерах зомби-сети\* (ботнета). Зомбированные клиентские компьютеры используются как в качестве веб-серверов, так и в качестве DNS-серверов для соответствующего домена [23]. Зомби-сервер живет недолго — от нескольких часов до нескольких дней. Однако их много. Поэтому можно поддерживать постоянную доступность.

Ниже приводятся результаты проделанного автором эксперимента. В листинге показаны результаты запросов относительно NS-серверов и IP-адреса для доменного имени «send-safe.com», это веб-сайт широко известного в узких кругах производителя программного обеспечения для рассылки спама\*. Сделаем несколько DNS-запросов с интервалом в пять минут:

```
fnn@home$>host -t ns send-safe.com
send-safe.com name server ns3.safe4net.net.
send-safe.com name server ns4.safe4net.net.
send-safe.com name server ns1.safe4net.net.
send-safe.com name server ns2.safe4net.net.
fnn@home$>host -t ns send-safe.com
send-safe.com name server ns1.london2portal.com.
send-safe.com name server ns2.london2portal.com.
fnn@home$>host send-safe.com
send-safe.com has address 89.36.47.10
send-safe.com has address 89.78.70.224
send-safe.com has address 68.37.246.232
send-safe.com has address 69.155.132.152
send-safe.com has address 71.155.241.20
fnn@home$>host send-safe.com
send-safe.com has address 86.20.204.169
send-safe.com has address 213.85.5.23
send-safe.com has address 66.61.23.171
send-safe.com has address 81.106.163.50
send-safe.com has address 82.138.37.213
fnn@home$>host send-safe.com
send-safe.com has address 24.9.184.225
send-safe.com has address 71.60.68.225
send-safe.com has address 71.155.241.20
send-safe.com has address 212.1.227.1
send-safe.com has address 217.173.174.237
fnn@home$>host send-safe.com
send-safe.com has address 24.9.184.225
```

```
send-safe.com has address 71.60.68.225
send-safe.com has address 82.246.189.246
send-safe.com has address 87.240.24.61
send-safe.com has address 212.1.227.1
fnn@home$>host send-safe.com
send-safe.com has address 66.61.23.171
send-safe.com has address 71.155.241.20
send-safe.com has address 82.138.37.213
send-safe.com has address 86.20.204.169
send-safe.com has address 213.85.5.23
```

Как видно, NS-сервера довольно часто меняются. Меняются и IP-адреса веб-сайта, причем в каждый момент их доступно несколько. То есть веб-сайт и обслуживающие его DNS-сервера рассредоточены и постоянно мигрируют. Если начать наводить справки о принадлежности и географическом положении всех выявленных IP-адресов, то окажется, что они равномерно разбросаны по всему Интернету. На самом деле это адреса зомбированных компьютеров, пригодных для размещения веб-сайтов. То есть веб-сайт как бы «размазан» по большой зомби-сети\*. Благодаря такой технологии веб-сайт «send-safe.com» виден пользователям с очень высокой вероятностью, однако прекратить его работу весьма затруднительно.

Зафиксировать положение такого сайта невозможно, обнаружить его владельца довольно трудно, доказать факт управления таким сайтом-призраком тоже нелегко.

Описанная технология применяется довольно редко. Подавляющее же большинство веб-сайтов живут на фиксированных IP-адресах, операторы-владельцы которых знают если не о личности владельца сайта, то, по крайней мере, о самом факте размещения.

### *Пространство и время*

IP-адреса могут переходить от одного пользователя к другому. Некоторые из них выделяются на постоянной основе — они именуются статическими. Другие же IP-адреса выделяются только на конкретный сеанс связи и называются динамическими. Для статических IP-адресов период жизни исчисляется месяцами и годами, а для динамических — минутами.

В записях для тех диапазонов IP-адресов, которые используются для динамического выделения, обычно это указывается. Там можно увидеть слова «dynamic», «dialup» или «NAT».

В обоих случаях при установлении принадлежности IP-адресов следует учитывать момент времени, по состоянию на который мы хотим установить пользователя этого адреса. Для динамических IP-адресов этот момент надо указывать с точностью до секунды, поскольку бывают совсем короткие сеансы связи. Кроме времени следует указать часовой пояс и возможную погрешность часов, по которым фиксировалось время.

### *Документирование*

Для уголовного дела, скорее всего, будет недостаточно простой распечатки ответа whois-сервера. Получить же официальную справку от европейского регионального регистратора RIPE будет весьма затруднительно, поскольку офис его находится в Амстердаме. Офисы других региональных регистраторов — еще дальше.

Нынешняя практика предусматривает два способа документирования ответа whois-сервера. Первый вариант: распечатка такого ответа может быть заверена каким-либо местным оператором связи, являющимся одновременно местным регистратором (LIR). В таком качестве часто выбирают РОСНИИРОС как старую и авторитетную организацию. Второй вариант: получение сведений о принадлежности IP-адреса оформляется рапортом оперуполномоченного; сведения из базы данных регистратора приводятся прямо в тексте рапорта. Иные варианты документирования (экспертиза, нотариальное заверение, справка от RIR) возможны, но до сих пор не применялись на практике.

Принадлежность IP-адреса к конкретному компьютеру все равно должна подтверждаться экспертизой этого компьютера и показаниями сотрудников оператора связи. Поэтому описанная нестрогость в документировании ответа whois-сервера вполне допустима.

### *Физическое расположение*

Из данных регистратора мы узнаем, за кем закреплена соответствующая подсеть или диапазон IP-адресов. Обычно таковым субъектом является оператор связи или его клиент. Очень редко в базе данных регистратора значится непосредственный пользователь IP-адреса.

Получить или уточнить данные о непосредственном пользователе, а также установить его географическое расположение можно у оператора связи, на которого зарегистрирован соответствующий диапазон IP. Бывает, что этот оператор не знает точного местоположения клиента, поскольку между ним и клиентом находится оператор-посредник или оператор последней мили. Бывает, что посредник не единственный. В таком случае придется пройти по всей цепочке операторов.

В принципе, функция определения местоположения конечного оборудования (компьютера пользователя) предусмотрена в СОРМе. Однако очень мало надежды, что такая функция в действительности работает в силу того, что операторы связи учитывают своих клиентов по-разному, держат эти данные в самых различных форматах и редко организуют к ним онлайн-доступ для ФСБ. Привести весь клиентский учет всех операторов к единому знаменателю — задача на сегодняшний день невыполнимая.

### Пример

Приведем характерный пример из практики.

Установлено, что неправомерный доступ к компьютерной информации был осуществлен 31.12.06, 21:01:30 по московскому времени с IP-адреса 217.107.0.58. Данный адрес зафиксирован техническими средствами потерпевшего и его провайдера и закреплён протоколами осмотра и актом экспертизы.

Запрашиваем whois и выясняем, что сеть 217.107.0.0–217.107.255.255 зарегистрирована за провайдером «Главтелеком», а подсеть 217.107.0.0–217.107.0.255 — за провайдером «Урюпинский хостинг». Первой части этих данных можно верить, поскольку «Главтелеком» является LIR'ом и данные о нем заносятся в базу самым региональным регистратором (RIR). Вторая же часть данных вызывает немного меньше доверия, поскольку здесь выше вероятность ошибки, да и времени с момента последнего обновления записи прошло немало.

Соответствующую распечатку ответа whois-сервера оформляем рапортом оперативного сотрудника. А в «Главтелеком» направляем официальный запрос с требованием предоставить информацию о клиенте.

Получаем ответ, в котором ОАО «Главтелеком» подтверждает, что диапазон 217.107.0.0–217.107.0.255 на интересующий момент времени был выделен в пользование его клиенту — ЗАО «Урюпинский хостинг». О дальнейшем распределении и использовании этих IP-адресов знают только в Урюпинске.

Предполагая, что злоумышленником является не сотрудник этого провайдера, а его клиент, и считая провайдера лицом незаинтересованным, запрашиваем ЗАО «Урюпинский хостинг» об интересующем нас адресе 217.107.0.58, указав точный момент времени, когда имел место неправомерный доступ.

Получаем ответ из Урюпинска, что поддиапазон адресов 217.107.0.2–217.107.0.63 используется для динамического выделения клиентам услуги коммутируемого доступа (dial-up), а в указанный момент (31.12.06, 18:01:30 по Гринвичу) этот адрес использовался клиентом, авторизованным по логину «pupkin». Этот логин, в свою очередь, закреплён за договором №163/2006 на имя Пупкиной Ирины Васильевны.

Для закрепления доказательств следует изъять и отправить на экспертизу компьютер, на котором функционировали технические средства, производившие авторизацию пользователя, выделение динамического IP-адреса и ведение соответствующих лог-файлов. Вместо изъятия и экспертизы можно ограничиться осмотром указанных компьютеров и лог-файлов (подробнее см. главу «Осмотр места происшествия»). Также следует изъять клиентский договор.

Окончательное закрепление доказательств производится в ходе экспертизы компьютера из квартиры Пупкина.

Итак, цепочка доказательств, привязывающая IP-адрес к компьютеру конечного пользователя, у нас сложилась такая:

- рапорт оперуполномоченного Иванова о выделении сети 217.107.0.0–217.107.255.255 российскому провайдеру «Главтелеком»;
- справка из «Главтелекома» о выделении сети 217.107.0.0–217.107.0.255 провайдеру «Урюпинский хостинг»;
- справка из ЗАО «У.Х.» об использовании подсети 217.107.0.2–217.107.0.63 для динамического выделения клиентам;
- протокол осмотра сервера «У.Х.», где в логах значится выделение адреса 217.107.0.58 пользователю «pupkin» в период 31.12.06, 22:45:31–23:20:12 по местному времени;
- клиентский договор, из которого следует принадлежность логина «pupkin»;
- акт экспертизы компьютера, изъятых при обыске в квартире Пупкина, где зафиксирован факт выхода в Интернет в период 31.12.06, 22:46:31–23:21:12 через модемный пул провайдера «У.Х.».

Цепочка замкнулась и защелкнулась. Некоторые особенности этой цепочки (вхождение одного диапазона IP в другой диапазон, особенности авторизации, разница и регулярное смещение временных интервалов и т.п.) может пояснить эксперт или специалист в ходе его допроса.

### Прочее

Понятно, что невозможно не только изложить в данной книге, но даже просто упомянуть все возможные особенности и трудности в задаче установления принадлежности IP-адресов. Например, использование протокола IP версии 6 (все вышесказанное относится только к версии 4), трансляция IP-адресов, туннелирование, несимметричная маршрутизация, провайдер, не учитывающий или не знающий своих клиентов, использование прокси-серверов и иных посредников для сокрытия истинного IP-адреса и т.д.

Подобные препятствия встречаются сплошь и рядом. Описать все возможные случаи — означает изложить полное содержание нескольких учебных курсов. На освоение соответствующих знаний ИТ-специалист тратит годы, и было бы наивно полагать, что все это можно объяснить оперу, следователю или судье простыми словами за несколько часов.

Поэтому при установлении принадлежности и местоположения IP-адреса в ходе ОРМ или предварительного следствия участие технического специалиста обязательно.

## Установление принадлежности доменного имени

Домен — область (ветвь) иерархического пространства доменных имен сети Интернет, которая обозначается уникальным доменным именем [L03].

Подробнее о доменных именах и их правовой природе можно прочесть в популярной книге А. Серго [25]. Здесь автор будет исходить из того, что читателю в общих чертах, то есть на уровне пользователя, известно, для чего предназначены и как используются доменные имена.

Некоторые юристы относят доменное имя к средствам индивидуализации (ст. 138 ГК). Другие не склонны считать его таковым и говорят, что юридическая природа доменного имени пока четко не определена. Есть даже экзотическое мнение, что доменные имена — это ресурс нумерации электросвязи (ст. 2 и 26 ФЗ «О связи»).

В отличие от юридической, техническая природа доменных имен известна хорошо и четко описана в соответствующих технических стандартах [26-29].

Для справедливого распределения пространства доменных имен и обеспечения их глобальной уникальности действует система регистрации доменных имен. Подлежат регистрации все доменные имена первого уровня (например, **org**, **info**, **ru**, **ua**), все доменные имена второго уровня (например, **gprf.info**, **fnn.ru**) и некоторые, выделенные доменные имена третьего уровня (например, **provider.net.ru**, **london.co.uk**). Прочие доменные имена регистрации не подлежат и распределяются по усмотрению владельца соответствующего домена более высокого уровня (например, домены **www.fnn.ru** и **mail.fnn.ru** создаются и используются исключительно по воле владельца домена второго уровня **fnn.ru**).

Для каждого домена, где предусмотрена обязательная регистрация, назначен регистратор или несколько регистраторов. В последнем случае все регистраторы обязаны использовать единую базу данных (централизованную или распределенную) для обеспечения уникальности регистрируемых доменных имен.

Все базы данных всех регистраторов являются публично доступными по протоколу **whois**, аналогично регистраторам IP-адресов.

Для домена **ru** регистраторов существует несколько (по состоянию на сегодня — 14). Они имеют централизованную базу данных, а кроме того — индивидуальные базы данных, являющиеся подмножеством центральной.

Таким образом, чтобы установить владельца какого-либо доменного имени из числа подлежащих регистрации, следует обратиться к базе данных соответствующего регистратора. Для не подлежащих регистрации доменных имен обращаться нужно к владельцу соответствующего домена более высокого уровня.

Например, нам требуется установить владельца доменного имени 3-го уровня **«www.internet-law.ru»**. (Не путать с веб-сайтом, живущим на этом домене! Домен и веб-сайт иногда могут иметь разных владельцев.)

Очевидно, что данный домен 3-го уровня не относится к числу регистрируемых. Он находится в полном распоряжении владельца соответствующего домена 2-го уровня, то есть домена **«internet-law.ru»**, который уже зарегистрирован.

Здесь придется сделать допущение (впоследствии, если понадобится, это надо будет подкрепить соответствующими доказательствами), а именно предположить, что указанный домен 3-го уровня в силу стандартности его имени (**www**) принадлежит тому же владельцу, что и домен 2-го уровня.

Чтобы узнать владельца доменного имени **«internet-law.ru»**, обращаемся к базе данных российских регистраторов доменов. Для этого используем команду **«whois»**, имеющуюся в любой ОС (кроме Windows). В качестве аргумента мы задаем искомое доменное имя, а параметр определяет, какой реестр запрашивать. Параметр **«-c ru»** указывает реестр доменных имен для России.

```
$>whois -c ru internet-law.ru
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).
```

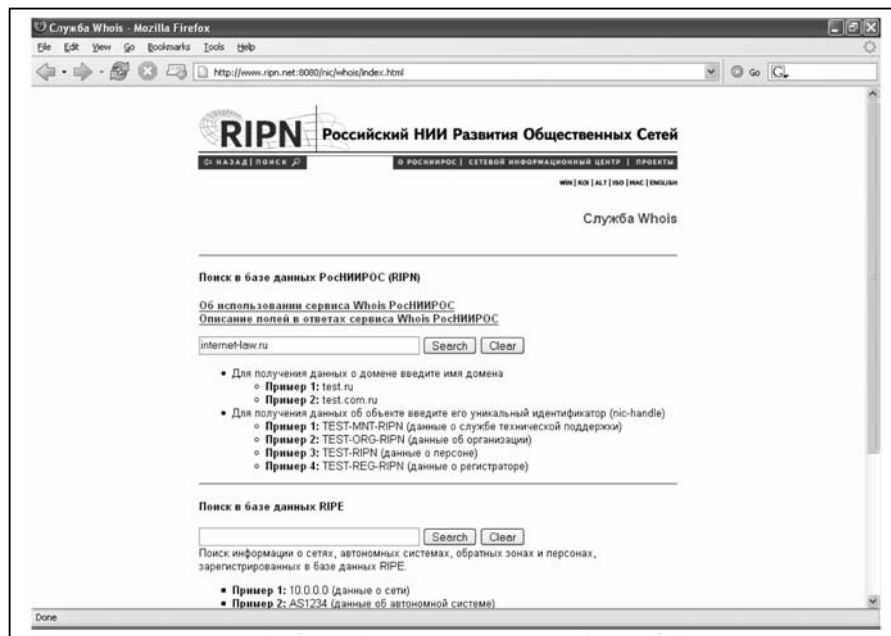
```
domain:      INTERNET-LAW.RU
type:        CORPORATE
nserver:     ns.masterhost.ru.
nserver:     ns1.masterhost.ru.
nserver:     ns2.masterhost.ru.
state:       REGISTERED, DELEGATED
org:         ANO "Internet & Law"
phone:       +7 495 7860130
e-mail:      mail@internet-law.ru
registrar:   RUCENTER-REG-RIPN
created:     2001.10.30
paid-till:   2007.10.30
source:      TC-RIPN
```

Last updated on 2006.12.16 14:02:58 MSK/MSD

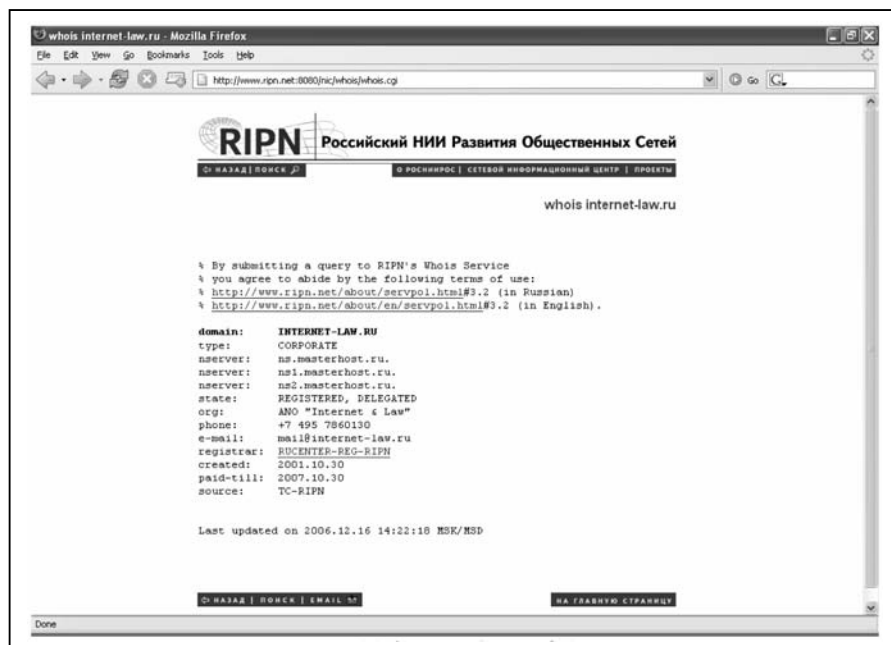
Нам отвечает **whois**-сервер технического центра РОСНИИРОСа (ТС-RIPN) — именно он поддерживает единую базу данных всех регистраторов в домене **ru**.

Ровно ту же самую информацию можно получить через веб-интерфейс, расположенный на веб-сайте РОСНИИРОСа

(<http://www.ripn.net:8080/nic/whois/index.html>) или на многих других веб-сайтах.



Запрос доменного имени через веб-интерфейс



Ответ веб-интерфейса

### Изучение ответа

Формат ответа устанавливается владельцем соответствующей базы данных. Он не регламентируется стандартами, и у других регистраторов может быть другим.

Для российского реестра доменов значения полей ответа таково:

domain: запрашиваемое доменное имя;  
 type: тип домена (GEOGRAPHICAL — географический, GENERIC — общего назначения, CORPORATE — все прочие);  
 descr: комментарий;  
 nserver: DNS-сервера, держащие записи об этом домене;  
 state: состояние домена;  
 org: имя владельца (для юридических лиц);  
 person: имя владельца (для физических лиц);  
 nic-hdl: идентификатор владельца в БД регистратора;  
 phone: номер телефона владельца;  
 fax-no: номер факса владельца;  
 e-mail: адрес электронной почты владельца;  
 p\_addr: почтовый адрес владельца;  
 registrar: идентификатор регистратора, зарегистрировавшего этот домен;  
 created: дата первичной регистрации;  
 paid-till: дата окончания действия регистрации;  
 changed: дата последнего изменения записи;  
 source: отвечающий whois-сервер.

Проведем еще один опыт по установлению владельца домена. Запросим, например, кто владеет доменом «fsb.ru»:

```
%>whois -c ru fsb.ru
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).
```

```
domain:      FSB.RU
type:        CORPORATE
nserver:     ns1.fsb.ru. 213.24.76.2
nserver:     ns2.fsb.ru. 194.226.94.138
state:       REGISTERED, DELEGATED
org:         Federal Security Service of Russian Federation
phone:       +7 095 9149084
fax-no:      +7 095 9149084
e-mail:      admin@fsb.ru
registrar:   RTCOMM-REG-RIPN
created:     1998.07.06
paid-till:   2007.08.01
source:      TC-RIPN
```

Last updated on 2006.12.16 14:36:46 MSK/MSD

В качестве регистратора выступает организация, обозначенная идентификатором «RTCOMM-REG-RIPN». Попробуем узнать об этом регистраторе больше. Для этого запросим тот же whois-сервер (ведь все российские регистраторы тоже должны быть зарегистрированы):

```
$>whois -c ru RTCOMM-REG-RIPN
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).
```

```
nic-hdl:      RTCOMM-REG-RIPN
org:          RTCOMM.RU Open Joint Stock Company
phone:        +7 095 980-01-70
fax-no:       +7 095 980-01-71
e-mail:       osp@rtcomm.ru
www:          www.rtcomm.ru
whois:        whois.rtcomm.ru
source:       TC-RIPN
```

Last updated on 2006.12.16 14:51:13 MSK/MSD

В ответе присутствует указание на собственный whois-сервер регистратора. Как указывалось выше, база данных каждого регистратора является подмножеством общей базы данных и не может ей противоречить. Однако whois-сервер конкретного регистратора может быть настроен иначе и выдаст нам более подробную информацию. Сделаем запрос к whois-серверу регистратора. Для этого используем в команде ключ «-h», после которого стоит имя whois-сервера.

```
$>whois -h whois.rtcomm.ru fsb.ru
```

```
domain:       FSB.RU
type:         CORPORATE
descr:        Corporate domain for Federal Security Service
nserver:      ns1.fsb.ru. 213.24.76.2
nserver:      ns2.fsb.ru. 194.226.94.138
state:        REGISTERED, DELEGATED
nic-hdl:      ORG_44-ORG-RTCOMM
org:          Federal Security Service of Russian Federation
p_addr:       103045, Москва
p_addr:       Лубянский проезд, 3/6,
p_addr:       Федеральная Служба Везопасности РФ
p_addr:       Дмитрий Левыкин
p_addr:       Голушко Александр
phone:        +7 095 9149084
fax_no:       +7 095 9149084
e-mail:       admin@fsb.ru
reg-till:     01-08-2007
```

```
created:      06-07-1998
changed:      09-08-2006
registrar:    RTCOMM-REG-RIPN
```

% Queries frequency limited by 60 per minute.

Здесь информации чуть больше. Однако возможности whois себя исчерпали. Для дальнейшей информации следует контактировать с регистратором.

### *Достоверность данных регистратора*

Следует помнить, что данные о владельце домена заносит в базу регистратор. Как для домена RU, так и для других доменов установлен порядок занесения и изменения записей. Разумеется, присутствуют требования об актуальности и достоверности данных. Однако регистраторы не всегда имеют возможности проводить проверку сообщенных им данных. И не всегда вовремя обновляют устаревшие.

Какие же данные о владельце домена можно считать достоверными?

Те, от которых зависит его право распоряжаться доменным именем.

Согласно условиям типового договора большинства регистраторов, указание недостоверных данных о владельце доменного имени может повлечь отмену регистрации. Невозможность связаться по указанным контактными данным также может привести к потере права на доменное имя. Многие регистраторы не позволяют передавать доменные имена иному лицу, пока прежний владелец не представит соответствующие документы. Следовательно, указание неверных контактных данных (телефона, почтового адреса, адреса электронной почты) с немалой вероятностью приводит к потере доменного имени. Указание неверного имени (названия) владельца приводит к тому, что домен нельзя будет передать другому владельцу (продать).

Отсюда можно сделать вывод о том, какие из указанных данных о владельце более достоверны, а какие — менее.

### *Анонимизация владельцев*

Ситуация с регистрацией доменов меняется. В России вступил в силу Федеральный закон «О персональных данных», согласно которому физическое лицо вправе потребовать убрать свои данные из общедоступного источника, каковым является whois-сервис регистратора. ICANN также планирует в ближайшее время внести поправки в правила регистрации доменов, предусматривающие квазианонимность. Владелец сможет указать вместо своих данных контактную информацию третьего лица, например, адвоката или интернет-провайдера, через которых теоретически можно будет выйти на реального владельца.

Тем не менее реальные данные владельца доменного имени должны храниться у регистратора. Для целей уголовного расследования их можно получить, опираясь на закон «О милиции». Для гражданских дел истцам, видимо, придется назначать ответчиком регистратора, затем в ходе судебного разбирательства получать от него персональные данные истинного владельца и затем менять ответчика.

### Документирование

Немного сложнее обстоит дело с документированием принадлежности домена.

Как для уголовного, так и для гражданского процесса необходимо доказать, что такое-то доменное имя принадлежит такому-то лицу.

На практике применяются следующие методы (упорядочены от наименее к наиболее предпочтительному):

- Оформить получение справки от whois-сервера рапортом оперуполномоченного. Совсем не безупречный способ. Годится только если обвиняемый (ответчик) не намерен отрицать принадлежность доменного имени.
- Заверить у нотариуса содержимое веб-страницы, представляющей собой веб-интерфейс к команде whois, например, такой, как изображена на последней иллюстрации. Применяется для гражданских дел. Далеко не все нотариусы соглашаются заверять содержимое веб-страниц. Но уж если такого нотариуса удалось найти, то нотариальное заверение производит на суд положительное впечатление. Но для специалиста такой способ — почти профанация, ведь нотариус не видит, к какой именно базе данных подключен веб-интерфейс. Следовательно, его заверение — не более чем заверение надписи на заборе, сделанной неизвестно кем неизвестно для каких целей.
- Получить официальный ответ оператора связи (провайдера), который имел отношение к обслуживанию этого доменного имени, например, поддерживал для него DNS-сервер или веб-сайт. Вместо письма провайдера можно взять показания у соответствующего технического сотрудника этого провайдера.
- Получить показания свидетелей. Например, о том, что интересующее нас лицо совершало определенные действия с доменным именем, доступные только его владельцу.
- Доказать факт оплаты соответствующим лицом услуг по регистрации или продлению домена. Хотя оплачивать можно и чужой домен, но тем не менее это хорошее косвенное доказательство.
- Назначить компьютерно-техническую экспертизу, в ходе которой эксперт запросит нужный whois-сервер и о результатах напишет в своем заключении. Способ несложный, но далеко не безупречный. Сом-

нительна сама возможность проведения компьютерно-технической экспертизы, когда объект исследования (whois-сервер, база данных регистратора) находится не в распоряжении эксперта, а неизвестно где, на другом конце мира.

- Обнаружить в ходе экспертизы на компьютере соответствующего лица свидетельства соединения и успешной авторизации на интерфейсе регистратора доменов. Практически все регистраторы предоставляют владельцам доменных имен возможность удаленно управлять своими доменами через веб-интерфейс на веб-сайте регистратора. На последней иллюстрации приводится одна из страниц такого веб-интерфейса регистратора АНО «РСИЦ» (товарный знак «РУ-Центр»). Сам факт успешного доступа к этой странице говорит о прохождении авторизации. Значит, лицо, на компьютере которого обнаружена такая веб-страница, знало верный пароль. А это, скорее всего, означает, что оно и было владельцем домена.
- Получить справку о регистрации доменного имени у соответствующего регистратора или в техническом центре РОСНИИРОС, который поддерживает единую базу данных регистраторов зон RU и SU. Очень хороший способ, но годится только для тех случаев, когда регистратор находится в России, в крайнем случае, в Белоруссии или на Украине. У иностранного регистратора получить такую справку труднее, придется задействовать Интерпол.



*Клиентский веб-интерфейс регистратора доменных имен. Обнаружение подобной страницы на диске пользователя свидетельствует о наличии у него договора с регистратором*

## Принадлежность адреса электронной почты

Сообщения электронной почты фигурируют во многих уголовных и гражданских делах. В некоторых они даже являются центральным доказательством. При помощи электронной почты заключаются сделки, происходит сговор о совершении преступления, совершается вымогательство, передаются существенные для дела сведения. Во всех подобных случаях встает вопрос: кому принадлежит или кем используется тот или иной адрес электронной почты.

### Почтовый ящик

В большинстве случаев адрес электронной почты однозначно связан с почтовым ящиком. И все письма, адресованные на этот адрес, попадают в этот ящик, откуда потом пользователь может их забрать.

Однако есть исключения:

- групповые или коллективные адреса, которые представляют собой адрес списка рассылки\*; все поступающие на этот адрес письма рассылаются определенной группе адресатов; таковыми часто бывают ролевые адреса, например, `info@company.ru` или `noc@provider.net`;
- технические адреса, за которыми не стоит ни пользователь, ни почтовый ящик; все поступающие на такой адрес письма обрабатываются программой; например, иногда в качестве обратного адреса указывается нечто вроде `noreply@domain.com` — все, что поступает на такой адрес, отправляется почтовым сервером на устройство `/dev/null`;
- адреса для пересылки (forward) сообщений; все поступающие на такой адрес сообщения не складываются в почтовый ящик, а перенаправляются на другой, заранее заданный адрес.

### Передача сообщений

В сообщении электронной почты адрес может быть указан в следующих полях. Адрес получателя — в полях «To», «Cc» и «Bcc». Адрес отправителя — в полях «From», «Reply-to» и «Return-path». Парадокс в том, что все эти поля могут не содержать истинного адреса. Все шесть адресов могут быть подложными, но, несмотря на это, сообщение дойдет по назначению. Чтобы пояснить, как такое может быть, рассмотрим процесс передачи сообщения электронной почты по протоколу SMTP.

Ниже приводится образец трафика (снят командой «`tcpdump -i r10 -s 1024 -n -xX 'tcp and port 25'`»), в котором зафиксирован процесс передачи одного сообщения.

```
21:27:09.265031 IP 190.49.202.78.33594 > 80.94.84.25.25: S
3705705427:3705705427(0) win 64240 <mss 1452,nop,nop,sackOK>
0x0000: 0050 22ee 207d 0013 7f8d f11a 0800 4500 .P>..}.....E.
```

## Оперативно-розыскные мероприятия

```
0x0010: 0030 50d0 4000 6906 9400 be31 ca4e 505e .0P.@.i....1.NP^
0x0020: 5419 833a 0019 dce0 93d3 0000 0000 7002 T.....p.
0x0030: faf0 6737 0000 0204 05ac 0101 0402 ..g7.....

21:27:09.265117 IP 80.94.84.25.25 > 190.49.202.78.33594: S
440205854:440205854(0) ack 3705705428 win 65535 <mss 1460,nop,nop,sackOK>
0x0000: 0013 7f8d f11a 0050 22ee 207d 0800 4500 .....P>..}..E.
0x0010: 0030 dab6 4000 4006 331a 505e 5419 be31 .0..@.@.3.P^T..1
0x0020: ca4e 0019 833a 1a3d 021e dce0 93d4 7012 .N...i.=.....p.
0x0030: ffff 45b4 0000 0204 05b4 0101 0402 ..E.....

21:27:09.549685 IP 190.49.202.78.33594 > 80.94.84.25.25: . ack 1 win 65340
0x0000: 0050 22ee 207d 0013 7f8d f11a 0800 4500 .P>..}.....E.
0x0010: 0028 50d9 4000 6906 93ff be31 ca4e 505e .(P.@.i....1.NP^
0x0020: 5419 833a 0019 dce0 93d4 1a3d 021f 5010 T.....=..P.
0x0030: ff3c 733b 0000 0000 0000 0000 0000 .<s>.....

21:27:10.177674 IP 80.94.84.25.25 > 190.49.202.78.33594: P 1:86(85) ack 1
win 65535
0x0000: 0013 7f8d f11a 0050 22ee 207d 0800 4500 .....P>..}..E.
0x0010: 007d dac7 4000 4006 32bc 505e 5419 be31 .}..@.@.2.P^T..1
0x0020: ca4e 0019 833a 1a3d 021f dce0 93d4 5018 .N...i.=.....P.
0x0030: ffff b6b3 0000 3232 3020 6169 6873 2e66 .....220.aihs.f
0x0040: 6e6e 2e72 7520 4553 4d54 5020 5365 6e64 nn.ru.ESMTP.Send
0x0050: 6d61 696c 2038 2e31 332e 332f 382e 3133 mail.8.13.3/8.13
0x0060: 2e33 3b20 5375 6e2c 2031 3420 4a61 6e20 .3;.Sun,.14.Jan.
0x0070: 3230 3037 2032 313a 3237 3a31 3020 2b30 2007.21:27:10.+0
0x0080: 3130 3020 2843 4554 290d 0a 100.(CET)..

5
21:27:10.465809 IP 190.49.202.78.33594 > 80.94.84.25.25: P 1:35(34) ack 86
win 65255
0x0000: 0050 22ee 207d 0013 7f8d f11a 0800 4500 .P>..}.....E.
0x0010: 004a 50e9 4000 6906 93cd be31 ca4e 505e .JP.@.i....1.NP^
0x0020: 5419 833a 0019 dce0 93d4 1a3d 0274 5018 T.....=.tP.
0x0030: fee7 895b 0000 6568 6c6f 2031 3930 2d34 ...[.ehlo.190-4
0x0040: 392d 3230 322d 3738 2e73 7065 6564 792e 9-202-78.speedy.
0x0050: 636f 6d2e 6172 0d0a com.ar..

6
21:27:10.466320 IP 80.94.84.25.25 > 190.49.202.78.33594: P 86:299(213) ack
35 win 65535
0x0000: 0013 7f8d f11a 0050 22ee 207d 0800 4500 .....P>..}..E.
0x0010: 00fd dacf 4000 4006 3234 505e 5419 be31 ....@.@.24P^T..1
0x0020: ca4e 0019 833a 1a3d 0274 dce0 93f6 5018 .N...i.=.t....P.
0x0030: ffff dcd0 0000 3235 302d 6169 6873 2e66 .....250-aihs.f
0x0040: 6e6e 2e72 7520 4865 6c6c 6f20 3139 302d nn.ru.Hello.190-
0x0050: 3439 2d32 3032 2d37 382e 7370 6565 6479 49-202-78.speedy
0x0060: 2e63 6f6d 2e61 7220 5b31 3930 2e34 392e .com.ar.[190.49.
0x0070: 3230 322e 3738 5d20 286d 6179 2062 6520 202.78].(may.be.
0x0080: 666f 7267 6564 292c 2070 6c65 6173 6564 forged),.pleased
0x0090: 2074 6f20 6d65 6574 2079 6f75 0d0a 3235 .to.meet.you..25
0x00a0: 302d 454e 4841 4e43 4544 5354 4154 5553 0-ENHANCEDSTATUS
0x00b0: 434f 4445 530d 0a32 3530 2d50 4950 454c CODES..250-PIPEL
0x00c0: 494e 494e 470d 0a32 3530 2d38 4249 544d INING..250-8BITM
```



```

0x00d0: 494d 450d 0a32 3530 2d53 495a 450d 0a32 IME..250-SIZE..2
0x00e0: 3530 2d44 534e 0d0a 3235 302d 4554 524e 50-DSN..250-ETRN
0x00f0: 0d0a 3235 302d 4445 4c49 5645 5242 590d ..250-DELIVERBY.
0x0100: 0a32 3530 2048 454c 500d 0a .250.HELP..

```

7  
21:27:10.754272 IP 190.49.202.78.33594 > 80.94.84.25.25: P 35:68(33) ack 299  
win 65042

```

0x0000: 0050 22ee 207d 0013 7f8d f11a 0800 4500 .P>..}.....E.
0x0010: 0049 50f0 4000 6906 93c7 be31 ca4e 505e .IP.@.i....1.NP^
0x0020: 5419 833a 0019 dce0 93f6 1a3d 0349 5018 T...:.....=.IP.
0x0030: fe12 8283 0000 4d41 494c 2046 524f 4d3a .....MAIL.FROM:
0x0040: 203c 6164 616d 4073 6263 676c 6f62 616c .<adam@sbcglobal
0x0050: 2e6e 6574 3e0d 0a .net>..

```

8  
21:27:10.764846 IP 80.94.84.25.25 > 190.49.202.78.33594: P 299:344(45) ack  
68 win 65535

```

0x0000: 0013 7f8d f11a 0050 22ee 207d 0800 4500 .....P>..}..E.
0x0010: 0055 dad6 4000 4006 32d5 505e 5419 be31 .U..@.@.2.P^T..1
0x0020: ca4e 0019 833a 1a3d 0349 dce0 9417 5018 .N....=.I....P.
0x0030: ffff 5f8d 0000 3235 3020 322e 312e 3020 .._...250.2.1.0.
0x0040: 3c61 6461 6d40 7362 6367 6c6f 6261 6c2e <adam@sbcglobal.
0x0050: 6e65 743e 2e2e 2e20 5365 6e64 6572 206f net>....Sender.o
0x0060: 6b0d 0a k..

```

9  
21:27:11.052039 IP 190.49.202.78.33594 > 80.94.84.25.25: P 68:93(25) ack 344  
win 64997

```

0x0000: 0050 22ee 207d 0013 7f8d f11a 0800 4500 .P>..}.....E.
0x0010: 0041 50f7 4000 6906 93c8 be31 ca4e 505e .AP.@.i....1.NP^
0x0020: 5419 833a 0019 dce0 9417 1a3d 0376 5018 T...:.....=.vP.
0x0030: fde5 753f 0000 5243 5054 2054 4f3a 203c .u?..RCPT.TO:<
0x0040: 6162 7573 6540 666e 6e2e 7275 3e0d 0a abuse@fnn.ru>..

```

10  
21:27:11.062441 IP 80.94.84.25.25 > 190.49.202.78.33594: P 344:386(42) ack  
93 win 65535

```

0x0000: 0013 7f8d f11a 0050 22ee 207d 0800 4500 .....P>..}..E.
0x0010: 0052 dae1 4000 4006 32cd 505e 5419 be31 .R..@.@.2.P^T..1
0x0020: ca4e 0019 833a 1a3d 0376 dce0 9430 5018 .N....=.v....0P.
0x0030: ffff 3875 0000 3235 3020 322e 312e 3520 ..8u..250.2.1.5.
0x0040: 3c61 6275 7365 4066 6e6e 2e72 753e 2e2e <abuse@fnn.ru>..
0x0050: 2e20 5265 6369 7069 656e 7420 6f6b 0d0a ..Recipient.ok..

```

11  
21:27:11.408007 IP 190.49.202.78.33594 > 80.94.84.25.25: P 93:99(6) ack 386  
win 64955

```

0x0000: 0050 22ee 207d 0013 7f8d f11a 0800 4500 .P>..}.....E.
0x0010: 002e 50fe 4000 6906 93d4 be31 ca4e 505e ..P.@.i....1.NP^
0x0020: 5419 833a 0019 dce0 9430 1a3d 03a0 5018 T...:.....0.=.P.
0x0030: fdbb cd44 0000 4441 5441 0d0a ...D..DATA..

```

12  
21:27:11.408641 IP 80.94.84.25.25 > 190.49.202.78.33594: P 386:436(50) ack  
99 win 65535

```

0x0000: 0013 7f8d f11a 0050 22ee 207d 0800 4500 .....P>..}..E.
0x0010: 005a dae8 4000 4006 32be 505e 5419 be31 .Z..@.@.2.P^T..1
0x0020: ca4e 0019 833a 1a3d 03a0 dce0 9436 5018 .N....=.6P.

```

```

0x0030: ffff 1c33 0000 3335 3420 456e 7465 7220 ...3..354.Enter.
0x0040: 6d61 696c 2c20 656e 6420 7769 7468 2022 mail,.end.with."
0x0050: 2e22 206f 6e20 6120 6c69 6e65 2062 7920 .>.on.a.line.by.
0x0060: 6974 7365 6c66 0d0a itself..

```

13  
21:27:11.745391 IP 190.49.202.78.33594 > 80.94.84.25.25: . 99:1551(1452) ack  
436 win 64905

```

0x0000: 0050 22ee 207d 0013 7f8d f11a 0800 4500 .P>..}.....E.
0x0010: 05d4 5107 4000 6906 8e25 be31 ca4e 505e ..Q.@.i..%.1.NP^
0x0020: 5419 833a 0019 dce0 9436 1a3d 03d2 5010 T...:.....6.=.P.
0x0030: fd89 7b52 0000 4d65 7373 6167 652d 4944 ..{R..Message-ID
0x0040: 3a20 3c30 3030 3030 3163 3733 3831 6124 :.<000001c7381a$
0x0050: 3661 3739 3762 3830 2434 6563 6133 3162 6a797b80$4eca31b
0x0060: 6540 4752 4146 4943 4f53 3e0a 4672 6f6d e@GRAFICOS>.From
0x0070: 3a20 224a 6f68 6e22 203c 6164 616d 4073 :."John>.<adam@s
0x0080: 6263 676c 6f62 616c 2e6e 6574 3e0a 546f bcgglobal.net>.To
0x0090: 3a20 3c61 6275 7365 4066 6e6e 2e72 753e :.<abuse@fnn.ru>
0x00a0: 0a53 7562 6a65 6374 3a20 4265 7374 2055 .Subject:.Best.U
0x00b0: 5320 6472 7567 732e 0a44 6174 653a 2053 S.drugs..Date:.S
0x00c0: 756e 2c20 3134 204a 616e 2032 3030 3720 un,.14.Jan.2007.
0x00d0: 3137 3a32 373a 3331 202b 3031 3030 0a4d 17:27:31.+0100.M
0x00e0: 494d 452d 5665 7273 696f 6e3a 2031 2e30 IME-Version:.1.0
0x00f0: 0a43 6f6e 7465 6e74 2d54 7970 653a 206d .Content-Type:.m
0x0100: 756c 7469 7061 7274 2f72 656c 6174 6564 ultipart/related
0x0110: 3b0a 0974 7970 653d 226d 756c 7469 7061 ;..type="multipa
0x0120: 7274 2f61 6c74 6572 6e61 7469 7665 223b rt/alternative";
0x0130: 0a09 626f 756e 6461 7279 3d22 2d2d 2d2d ..boundary="----
0x0140: 2d2d 2d2d 2d2d 2d2d 6d73 3030 3033 3030 -----ms000300
0x0150: 3037 3034 3039 3030 3035 3036 3039 3034 0704090005060904
0x0160: 3039 220a 582d 5072 696f 7269 7479 3a20 09>.X-Priority:.
0x0170: 330a 582d 4d53 4d61 696c 2d50 7269 6f72 3.X-MSMail-Prior
0x0180: 6974 793a 204e 6f72 6d61 6c0a 582d 4d61 ity:.Normal.X-Ma
0x0190: 696c 6572 3a20 4d69 6372 6f73 6f66 7420 iler:.Microsoft.
0x01a0: 4f75 746c 6f6f 6b20 4578 7072 6573 7320 Outlook.Express.
0x01b0: 362e 3030 2e32 3930 302e 3238 3639 0a58 6.00.2900.2869.X
0x01c0: 2d4d 696d 654f 4c45 3a20 5072 6f64 7563 -MimeOLE:.Produc
0x01d0: 6564 2042 7920 4d69 6372 6f73 6f66 7420 ed.By.Microsoft.
0x01e0: 4d69 6d65 4f4c 4520 5636 2e30 302e 3239 MimeOLE.V6.00.29
0x01f0: 3030 2e32 3936 320a 0a54 6869 7320 6973 00.2962..This.is
0x0200: 2061 206d 756c 7469 2d70 6172 7420 6d65 .a.multi-part.me
0x0210: 7373 6167 6520 696e 204d 494d 4520 666f ssage.in.MIME.fo
0x0220: 726d 6174 2e0a 0a2d 2d2d 2d2d 2d2d 2d2d rmat.....
0x0230: 2d2d 2d2d 2d6d 7330 3030 3330 3030 3730 -----ms000300070
0x0240: 3430 3930 3030 3530 3630 3930 3430 390a 409000506090409.
0x0250: 436f 6e74 656e 742d 5479 7065 3a20 6d75 Content-Type:.mu
0x0260: 6c74 6970 6172 742f 616c 7465 726e 6174 ltipart/alternat
0x0270: 6976 653b 0a09 626f 756e 6461 7279 3d22 ive;..boundary="
0x0280: 2d2d 2d2d 2d2d 2d2d 2d2d 2d2d 6d73 3034 -----ms04
0x0290: 3035 3036 3031 3030 3035 3032 3037 3030 0506010005020700
0x02a0: 3035 3036 3031 220a 0a0a 2d2d 2d2d 2d2d 050601>.....
0x02b0: 2d2d 2d2d 2d2d 2d2d 6d73 3034 3035 3036 -----ms040506
0x02c0: 3031 3030 3035 3032 3037 3030 3035 3036 0100050207000506
0x02d0: 3031 0a43 6f6e 7465 6e74 2d54 7970 653a 01.Content-Type:

```

```

0x02e0: 2074 6578 742f 6874 6d6c 3b0a 0963 6861 .text/html;..cha
0x02f0: 7273 6574 3d22 6973 6f2d 3838 3539 2d31 rset="iso-8859-1
0x0300: 220a 436f 6e74 656e 742d 5472 616e 7366 <.Content-Transf
0x0310: 6572 2d45 6e63 6f64 696e 673a 2071 756f er-Encoding:.quo
0x0320: 7465 642d 7072 696e 7461 626c 650a 0a3c ted-printable..<
0x0330: 2144 4f43 5459 5045 2048 544d 4c20 5055 !DOCTYPE.HTML.PU
0x0340: 424c 4943 2022 2d2f 2f57 3343 2f2f 4454 BLIC."-//W3C//DT
0x0350: 4420 4854 4d4c 2034 2e30 2054 7261 6e73 D.HTML.4.0.Trans
0x0360: 6974 696f 6e61 6c2f 2f45 4e22 3e0a 3c48 itional//EN">.<H
0x0370: 544d 4c3e 3c48 4541 443e 0a3c 4d45 5441 TML><HEAD>.<META
0x0380: 2068 7474 702d 6571 7569 763d 3344 436f .http-equiv=3DCo
0x0390: 6e74 656e 742d 5479 7065 2063 6f6e 7465 ntent-Type.conte
0x03a0: 6e74 3d33 4422 7465 7874 2f68 746d 6c3b nt=3D"text/html;
0x03b0: 2063 6861 7273 6574 3d33 4469 736f 2d38 .charset=3Diso-8
0x03c0: 3835 392d 3122 3e0a 3c4d 4554 4120 636f 859-1">.<META.co
0x03d0: 6e74 656e 743d 3344 224d 5348 544d 4c20 ntent=3D"MSHTML.
0x03e0: 362e 3030 2e32 3930 302e 3239 3935 2220 6.00.2900.2995>.
0x03f0: 6e61 6d65 3d33 4447 454e 4552 4154 4f52 name=3DGENERATOR

```

14

```

21:27:11.750983 IP 190.49.202.78.33594 > 80.94.84.25.25: P 1551:1635(84) ack
436 win 64905

```

```

0x0000: 0050 22ee 207d 0013 7f8d f11a 0800 4500 .P>..}.....E.
0x0010: 007c 5108 4000 6906 937c be31 ca4e 505e .|Q.@.i...|.NP^
0x0020: 5419 833a 0019 dce0 99e2 1a3d 03d2 5018 T.:.....=.P.
0x0030: fd89 b6e2 0000 3034 3033 3036 3035 3034 .....0403060504
0x0040: 3035 3030 3037 3032 3031 3032 3031 404a 05000702010201@J
0x0050: 6f68 6e3e 0a0a 0a0a 2d2d 2d2d 2d2d 2d2d ohn>.....
0x0060: 2d2d 2d2d 2d2d 6d73 3030 3033 3030 3037 -----ms00030007
0x0070: 3034 3039 3030 3035 3036 3039 3034 3039 0409000506090409
0x0080: 2d2d 0a0a 0a0a 0a0a 0a0a 0a0a 0a0a 0a0a --.....

```

15

```

21:27:11.751073 IP 80.94.84.25.25 > 190.49.202.78.33594: . ack 1635 win
65535

```

```

0x0000: 0013 7f8d f11a 0050 22ee 207d 0800 4500 .....P>..}..E.
0x0010: 0028 daeb 4000 4006 32ed 505e 5419 be31 .(.@.@.2.P^T..1
0x0020: ca4e 0019 833a 1a3d 03d2 dce0 9a36 5010 .N.....=.6P.
0x0030: ffff 6a63 0000 0000 0000 0000 0000 ..jC.....

```

16

```

21:27:12.035765 IP 190.49.202.78.33594 > 80.94.84.25.25: P 1635:1640(5) ack
436 win 64905

```

```

0x0000: 0050 22ee 207d 0013 7f8d f11a 0800 4500 .P>..}.....E.
0x0010: 002d 5115 4000 6906 93be be31 ca4e 505e .-Q.@.i....|.NP^
0x0020: 5419 833a 0019 dce0 9a36 1a3d 03d2 5018 T.:.....6.=.P.
0x0030: fd89 27b5 0000 0d0a 2e0d 0a00 ..'.....

```

17

```

21:27:12.042413 IP 80.94.84.25.25 > 190.49.202.78.33594: P 436:492(56) ack
1640 win 65535

```

```

0x0000: 0013 7f8d f11a 0050 22ee 207d 0800 4500 .....P>..}..E.
0x0010: 0060 daf4 4000 4006 32ac 505e 5419 be31 .`.@.@.2.P^T..1
0x0020: ca4e 0019 833a 1a3d 03d2 dce0 9a3b 5018 .N.....=.....P.
0x0030: ffff d11e 0000 3235 3020 322e 302e 3020 .....250.2.0.0.
0x0040: 6c30 454b 5241 4647 3033 3434 3438 204d 10EKRAF034448.M
0x0050: 6573 7361 6765 2061 6363 6570 7465 6420 essage.accepted.

```

```

0x0060: 666f 7220 6465 6c69 7665 7279 0d0a for.delivery..
18
21:27:12.327003 IP 190.49.202.78.33594 > 80.94.84.25.25: P 1640:1646(6) ack
492 win 64849

```

```

0x0000: 0050 22ee 207d 0013 7f8d f11a 0800 4500 .P>..}.....E.
0x0010: 002e 511d 4000 6906 93b5 be31 ca4e 505e .Q.@.i....|.NP^
0x0020: 5419 833a 0019 dce0 9a3b 1a3d 040a 5018 T.:.....;.=.P.
0x0030: fd51 84d2 0000 7175 6974 0d0a .Q....quit..

```

19

```

21:27:12.327578 IP 80.94.84.25.25 > 190.49.202.78.33594: P 492:534(42) ack
1646 win 65535

```

```

0x0000: 0013 7f8d f11a 0050 22ee 207d 0800 4500 .....P>..}..E.
0x0010: 0052 db09 4000 4006 32a5 505e 5419 be31 .R..@.@.2.P^T..1
0x0020: ca4e 0019 833a 1a3d 040a dce0 9a41 5018 .N.....=.AP.
0x0030: ffff 9e49 0000 3232 3120 322e 302e 3020 ...I..221.2.0.0.
0x0040: 6169 6873 2e66 6e6e 2e72 7520 636c 6f73 aihs.fnn.ru.clos
0x0050: 696e 6720 636f 6e6e 6563 7469 6f6e 0d0a ing.connection..

```

```

21:27:12.328061 IP 80.94.84.25.25 > 190.49.202.78.33594: F 534:534(0) ack
1646 win 65535

```

```

0x0000: 0013 7f8d f11a 0050 22ee 207d 0800 4500 .....P>..}..E.
0x0010: 0028 db0a 4000 4006 32ce 505e 5419 be31 .(.@.@.2.P^T..1
0x0020: ca4e 0019 833a 1a3d 0434 dce0 9a41 5011 .N.....=.4AP.
0x0030: ffff 69f5 0000 0000 0000 0000 0000 ..i.....

```

```

21:27:12.613806 IP 190.49.202.78.33594 > 80.94.84.25.25: F 1646:1646(0) ack
534 win 64807

```

```

0x0000: 0050 22ee 207d 0013 7f8d f11a 0800 4500 .P>..}.....E.
0x0010: 0028 5126 4000 6906 93b2 be31 ca4e 505e .(Q&@.i....|.NP^
0x0020: 5419 833a 0019 dce0 9a41 1a3d 0434 5011 T.:.....A.=.4P.
0x0030: fd27 6ccd 0000 0000 0000 0000 0000 .'l.....

```

```

21:27:12.613974 IP 80.94.84.25.25 > 190.49.202.78.33594: F 534:534(0) ack
1647 win 65535

```

```

0x0000: 0013 7f8d f11a 0050 22ee 207d 0800 4500 .....P>..}..E.
0x0010: 0028 db0e 4000 4006 32ca 505e 5419 be31 .(.@.@.2.P^T..1
0x0020: ca4e 0019 833a 1a3d 0434 dce0 9a42 5011 .N.....=.4AP.
0x0030: ffff 69f4 0000 0000 0000 0000 0000 ..i.....

```

```

21:27:12.617338 IP 190.49.202.78.33594 > 80.94.84.25.25: . ack 535 win 64807

```

```

0x0000: 0050 22ee 207d 0013 7f8d f11a 0800 4500 .P>..}.....E.
0x0010: 0028 5127 4000 6906 93b1 be31 ca4e 505e .Q'@.i....|.NP^
0x0020: 5419 833a 0019 dce0 9a42 1a3d 0435 5010 T.:.....B.=.5P.
0x0030: fd27 6ccc 0000 0000 0000 0000 0000 .'l.....

```

После установления соединения (первые три пакета) принимающий сервер дает код 220 и некоторые данные о себе (4-й пакет). Передающий сервер дает команду «EHLO» и свой идентификатор (5-й пакет). Принимающий сервер дает код 250 и некоторые свои параметры (6-й пакет). Передающий сервер дает команду «MAIL FROM» (7-й пакет), затем команду «RCPT TO» (9-й пакет). Принимающий подтверждает допустимость этих команд

кодом 250 (8-й и 10-й пакеты). Затем передающий сервер дает команду «**DATA**» (11-й пакет), а принимающий подтверждает кодом 354 готовность принимать текст письма (12-й пакет). Передающий сервер отправляет текст сообщения, включая все заголовки (пакеты 13, 14 и 16). Принимающий подтверждает прием кодом 250 (17-й пакет). Затем передающий дает команду «**QUIT**» (18-й пакет), на что получает код 221 (19-й пакет). Остальные пакеты завершают TCP-соединение. Так работает протокол SMTP.

Передающий МТА	Принимающий МТА
	220
HELO или EHLO	250
MAIL FROM: <адрес>	250
RCPT TO: <адрес>	250
DATA	354
текст сообщения	
.	250
QUIT	221

### Достоверность

Как видно, все заголовки сообщения («**From**», «**To**» и другие) передаются в тексте письма, они могут не анализироваться принимающей стороной. Куда именно следует доставить сообщение, принимающий сервер узнает из команды «**RCPT TO**», адрес в которой не обязан совпадать с адресом в заголовке «**To**».

Наличие какого-либо адреса в поле «**From**» или «**Reply-to**» означает лишь то, что отправитель счел нужным вписать туда этот адрес. Каких-либо достоверных выводов об источнике или отправителе письма при этом сделать невозможно. Источник и отправитель могут быть вычислены из анализа заголовков «**Received**» и соответствующих логов серверов электронной почты, как это описано в предыдущей главе.

Но если подтверждено, что адрес действующий, то есть некое лицо получает отправленные на него письма, то можно браться за установление владельца этого адреса.

### Установление

Для начала следует установить почтовый ящик, с которым связан адрес. Затем выяснить, кто пользуется этим почтовым ящиком. Так будет установлен владелец адреса.

Для установки места расположения почтового ящика исследователь устанавливает первичный MX домена. Во многих случаях ящик находится на этом же сервере. В других случаях сервер пересылает почту на иной сервер, указанный в его настройках. В обоих случаях требуется узнать эти настройки, чтобы определить местоположение почтового ящика. Для этого потребуется содействие провайдера, обслуживающего сервер. Расположение почтового ящика документируется протоколом осмотра нужного сервера (серверов) или заключением эксперта. В крайнем случае, можно ограничиться получением письменного ответа провайдера на соответствующий запрос, но этот способ доказательства нельзя назвать безупречным.

Доказательствами факта использования почтового ящика определенным лицом могут служить:

- наличие на компьютере этого лица настроек для доступа к этому ящику (включая пароль);
- наличие на компьютере этого лица полученных сообщений электронной почты со служебными заголовками, свидетельствующими о прохождении сообщений через этот почтовый ящик;
- наличие на сервере, где расположен ящик, логов об успешном соединении и аутентификации пользователя данного почтового ящика;
- наличие у других абонентов сообщений от этого лица, написанных в ответ на сообщения, отправленные на этот почтовый ящик (в ответе часто цитируется исходное сообщение, а также среди служебных заголовков присутствует заголовок со ссылками на предыдущие сообщения).

### Примеры

Три примера на тему установления владельца адреса электронной почты и доказывания этого факта.

В ходе расследования преступления было установлено, что обнаруженная на компьютере потерпевшего вредоносная программа пытается отослать некоторые данные по электронной почте. Эксперт запустил эту программу на своем компьютере, маршрутизировал весь исходящий трафик с него на другой компьютер, на котором запустил эмулятор внешнего SMTP-сервера. В результате эксперимента обнаружилось, что неизвестная вредоносная программа отправляет по электронной почте письмо на адрес user0001@pnzhost.ru. В этом письме содержалась конфиденциальная информация с компьютера потерпевшего.

Соответствующая DNS-запись (запись типа MX) указывает, что сервер входящей электронной почты для домена pnzhost.ru имеет IP-адрес 133.245.254.110. Этот IP-адрес, согласно данным регистратора, используется провайдером\* «Заречный телеком» из города Пензы. Все эти данные были установлены привлеченным специалистом в ходе ОРМ «иссле-

дование предметов и документов». По данным из whois, можно было предположить, что указанный IP-адрес используется не самим провайдером для собственных нужд, а сервером одного из клиентов этого провайдера.

Сделан запрос в ЗАО «Заречный телеком». Официальный ответ пришел по почте лишь через три недели, но оперуполномоченный, пользуясь личными контактами с работником провайдера, получил быстрый неофициальный ответ, что упомянутый IP-адрес 133.245.254.110 действительно используется сервером одного из клиентов по фамилии Семенов; на этом сервере оказываются услуги хостинга\*. Кроме того, присутствует услуга бесплатного хостинга: каждый желающий может получить место для веб-сайта и ящик электронной почты. Предположительно, именно такой бесплатный анонимный ящик и соответствует адресу user0001@pnzhost.ru

Проведен осмотр указанного сервера. В логах обнаружены несколько записей о доступе к почтовому ящику по протоколу POP3 с IP-адресов 220.12.122.3, 220.12.122.16, 220.12.122.55. Эти адреса относятся к одному пулу, который, как установлено, используется провайдером «МСК-Антен» для оказания услуги коммутируемого доступа.

Далее последовал запрос к этому провайдеру. Очень хорошо, что при осмотре логов сервера были зафиксированы не только адреса, но и точное время каждого обращения, а также погрешность внутренних часов сервера, поскольку IP-адреса оказались динамическими\*. По ним был установлен номер телефона абонента.

Итак, доказательствами принадлежности адреса электронной почты явились:

- протокол ОРМ об исследовании документов с указанием на «Заречный телеком», за которым зарегистрирован адрес 133.245.254.110, являющийся MX для домена электронной почты **pnzhost.ru**;
- ответ от ЗАО «Заречный телеком», подтверждающий использование ими IP-адреса 133.245.254.110 для сервера клиента Семенова;
- протокол выемки документов и изъятый договор с бланк-заказом клиента Семенова;
- показания Семенова, владельца сервера, на котором живет домен электронной почты **pnzhost.ru**;
- протокол осмотра сервера Семенова с фрагментами логов об осуществлении доступа к почтовому аккаунту\* **user0001** с IP-адресов из подсети 220.12.122.0;
- ответ от ЗАО «МСК-Антен» о том, что запрошенные 3 IP-адреса в указанные моменты времени динамически выделялись одному и тому же пользователю с идентификатором «av00387205» и номером телефона 4580445;
- ответ от телефонного узла, что указанный номер закреплен за абонентом Кучеровым, проживающим по адресу: Москва, Правобережная улица, д. 1, кв. 2;

- заключение эксперта по компьютеру, изъятому при обыске в квартире Кучерова по указанному адресу, о том, что с этого компьютера осуществлялся доступ по протоколу POP3 к серверу 133.245.254.110, а также о том, что для доступа в Интернет использовался логин «av00387205» и 3 IP-адреса из пула провайдера «МСК-Антен».

Конечно же, не все перечисленные доказательства безупречны. Конечно, вместо осмотра логов предпочтительно было бы сделать экспертизу. А кроме ответов на запросы было бы полезно сделать выемку документов у этих операторов связи или хотя бы допросить их технических специалистов. Однако для нашей российской практики и такая цепочка доказательств выглядит достижением. Безупречная, зато замкнутая.

Во втором примере злоумышленник воспользовался иностранным мейл-сервером.

В ходе расследования дела о вымогательстве было установлено, что потерпевший получил предложение вымогателя по электронной почте. Сообщение пришло с адреса **vera3456@yahoo.com** (этот адрес был указан в поле **From**). Потерпевший вступил в переписку, пользуясь указанным адресом, и получил несколько ответов на свои письма.

Потерпевший передал на экспертизу свой компьютер, где хранились сообщения, полученные и отправленные им. В одном из сообщений вымогателя в заголовках имелся IP-адрес его домашнего компьютера 217.225.194.202 (прочие сообщения он отправлял с использованием анонимизирующего прокси-сервера\*).

При получении денег вымогатель был задержан. При обыске у него изъят компьютер. Экспертиза обнаружила на нем фрагменты архива полученных и отправленных сообщений электронной почты, среди которых нашлись и сообщения от потерпевшего, адресованные на **vera3456@yahoo.com**, с которого они автоматически перенаправлялись на адрес вымогателя.

Получить информацию от зарубежного оператора связи, поддерживающего почтовый ящик в домене yahoo.com, оказалось невозможно.

Привлеченный судом специалист сопоставил сообщения, найденные экспертами на двух компьютерах (потерпевшего и подсудимого), и сделал вывод, что пользователь второго компьютера действительно получал те сообщения, которые отправлялись пользователем первого компьютера на адрес **vera3456@yahoo.com**.

Итак, доказательствами принадлежности адреса электронной почты явились:

- показания потерпевшего об отправлении и получении писем;
- заключение эксперта по компьютеру потерпевшего;
- заключение эксперта по компьютеру подозреваемого;
- заключение специалиста о сопоставлении данных из этих двух экспертиз;

- комплекс доказательств, установивший принадлежность IP-адреса 217.225.194.202 к компьютеру подозреваемого.

Здесь была опущена третья «точка опоры» в лице почтового сервера провайдера. Дело опиралось на совпадение сообщений на компьютерах отправителя и получателя. Возможно, при отсутствии иных доказательств вины двух «опор» и не хватило бы. Но задержание вымогателя при передаче денег не оставляло у следствия и суда никаких сомнений.

Третий пример будет, так сказать, негативным.

При расследовании сбыта номеров банковских карт и поддельных банковских карт было установлено, что подозреваемый осуществлял контакты с покупателями при помощи электронной почты. При этом он использовал адрес **bigbuyer@123card.com** — принимал сообщения на этот адрес и отправлял ответы с него.

Специалист установил, что сервер электронной почты (MX\*), соответствующий почтовому домену **123card.com**, имеет IP-адрес **80.12.254.4**, и этот адрес используется провайдером «Condor-Net GmbH» из Германии. Тот же IP-адрес присутствовал в заголовках сообщений, полученных от подозреваемого.

Оперативники посчитали, что позже, когда будет возбуждено уголовное дело, у провайдера можно будет получить сведения о клиенте и логи доступа к аккаунту и связать таким образом адрес **bigbuyer@123card.com** с подозреваемым.

Однако когда дело дошло до получения сведений о клиенте провайдера «Condor-Net GmbH», обнаружилось, что данный клиент воспользовался услугой аренды виртуального сервера. Все настройки такого сервера клиент делает самостоятельно. Все логи, относящиеся к электронной почте, могут лежать только на сервере клиента. Провайдер же не логирует сетевую активность клиентов, кроме учета общего объема трафика. К моменту, когда немецкая полиция провела по поручению российской стороны следственные действия, все содержимое виртуального сервера было уже клиентом (или кем-то другим) вычищено. Никаких логов (если они вообще велись) не осталось.

Договор между провайдером и клиентом заключался через акцепт публичной оферты, размещенной на веб-сайте, а оплата производилась кредитной картой. Указанные клиентом данные оказались вымышленными, а использованная карта — чужой. Таким образом, не было даже доказательств того, что подозреваемый пользовался арендованным сервером **80.12.254.4**.

На компьютере у подозреваемого эксперт не обнаружил следов взаимодействия с сервером **80.12.254.4** или сообщений с адресом **bigbuyer@123card.com**.

Домен **123card.com** был зарегистрирован на имя одного из сообщников подозреваемого, однако этого недостаточно, чтобы доказать использование подозреваемым указанного адреса электронной почты.

В результате из-за невозможности доказать получение и отправку подозреваемым сообщений электронной почты пришлось уголовное дело прекратить.

## Кейлогеры

Кейлогерами (keyloggers) называют устройства (программные или аппаратные) для перехвата сигналов с клавиатуры, то есть для записи последовательности нажатых пользователем клавиш.

Большинство паролей набирается с клавиатуры. С нее же вводится большая часть переписки, персональных данных и иной информации, которая может интересовать злоумышленников. Поэтому сбор информации о нажатых клавишах является эффективным способом совершения различных компьютерных преступлений.

Наряду с этим кейлогер может служить инструментом для проведения ОРМ.

Кейлогер можно отнести к устройствам двойного назначения. У него есть ряд легальных применений: отслеживание владельцем случаев несанкционированного использования его собственного компьютера, архивирование информации пользователя на случай ее утраты при сбоях. Тем не менее очевидно, что основным предназначением кейлогеров является скрытное (негласное) получение информации.

### Аппаратные кейлогеры

Они выполнены в виде переходника, который вставляется в разрыв клавиатурного кабеля. Бывают аппаратные устройства, которые встроены непосредственно в клавиатуру.



*Аппаратные кейлогеры. Вставляются в разрыв между клавиатурой и системным блоком. Не могут быть детектированы программным способом, зато легко обнаруживаются визуально*

Современный кейлогер имеет встроенную память на сотни килобайт или несколько мегабайт, собранную информацию хранит в зашифрованном виде. Взаимодействие с «хозяином» обычно строится на том же самом интерфейсе, то есть при помощи клавиатуры, в которую он включен.

Любой желающий может без формальностей приобрести аппаратный кейлогер по цене 150-200 долларов.

### **Программные кейлогеры**

Такие программы доступны как за деньги, так и бесплатно. Как правило, они выполнены по технологиям, используемым в троянских программах, каковыми, по сути, и являются.

Большинство программных кейлогеров будут признаны вредоносными программами, поскольку приспособлены для скрытного внедрения и незаметной для пользователя работы. Однако некоторые из них, имеющие «открытый» режим, добросовестный эксперт вредоносной программой не признает.

Многие программные кейлогеры имеют дополнительные функции — запись движений мыши и снятие скриншотов\*.

## **Интернет-поиск как метод ОРД**

Для начала несколько примеров.

Потерпевшим было получено по электронной почте письмо с предложением перевести некую сумму через систему «WebMoney» под угрозой разглашения данных об уязвимости его веб-сервера. Выкуп предлагалось перевести на счет (кошелек) номер **z18364577**. Пока один оперативник выяснял у сотрудников платежной системы, кем использовался этот счет, другой ввел строку «**z18364577**» в поисковой системе. Оказалось, что этот номер кошелька уже засвечен в Интернете. Один пользователь жаловался, что перевел на него деньги в оплату за некую услугу, но обещанной услуги не получил. Таким образом нашелся второй потерпевший, в деле появился второй эпизод и дополнительные доказательства.

Поступило заявление о клевете. Неизвестный злоумышленник разместил на веб-форуме информацию, порочащую деловую репутацию потерпевшего. К сожалению, не удалось установить, с какого IP-адреса происходило размещение информации, поскольку злоумышленник воспользовался анонимным прокси-сервером. Тогда оперативник предположил, что преступник мог разместить ту же информацию и на иных интернет-ресурсах. Он ввел характерную фразу из размещенной статьи в поисковую систему и нашел два других веб-форума, на которых, по-видимому, тот же злоумышленник разместил ту же информацию. Во всех случаях он воспользовался анонимизирующим прокси-сервером. Одна-

ко на одном из найденных форумов, кроме вышеописанного клеветнического материала, было обнаружено еще несколько постингов (статей), судя по их содержанию, размещенных тем же человеком. Размещенных уже без использования прокси. По ним-то оперативники и вышли на исполнителя.

Подозреваемый в мошенничестве кардер\*, задержанный в Москве, был отпущен под подписку о невыезде и немедленно скрылся. Оперуполномоченный для розыска подозреваемого нашел в деле несколько адресов электронной почты, которыми тот пользовался в разное время. Поиск в Интернете по этим адресам среди прочих результатов принес одно объявление о продаже номеров кредитных карт. Объявление было размещено давно и явно неактуально. Однако кроме адреса электронной почты в объявлении был указан для контактов также номер ICQ\*. Оперативник предположил, что подозреваемый может до сих пор пользоваться этим номером. Он ввел номер в контакт-лист своего ICQ-клиента и стал ждать, когда абонент «выйдет в эфир», то есть будет обозначен как «online». Через несколько недель это случилось. Подозреваемый стал пользоваться своим номером ICQ почти ежедневно. Оперативник пытался определить IP-адрес, с которого подозреваемый соединяется, но без прямого контакта с ним это оказалось невозможным. Тогда оперуполномоченный вторично обратился к поисковой системе и стал искать, где еще упоминается номер ICQ подозреваемого. И нашел относительно свежее объявление, касающееся организации DoS-атак на сервер. Это дало повод для контакта. Оперативник по ICQ вышел на контакт с подозреваемым и ежедневно общался с ним, пользуясь найденным предложением. При обмене сообщениями по ICQ есть возможность определить IP собеседника (правда, не во всех случаях). В течение нескольких дней общения в качестве IP подозреваемого детектировался адрес socks-сервера\*. Но однажды высветился IP-адрес, похожий на реальный. Он числился за германским провайдером из города Франкфурт-на-Майне. Согласно материалам дела, у подозреваемого в этом городе жил родственник. Дальнейшее было делом техники. Через провайдера установили адрес, и через несколько дней немецкая полиция подозреваемого арестовала. Не прошло и года, как он был экстрадирован в Россию.

Поисковые системы в Интернете стали не только основной «дорогой в сеть» для обычных пользователей, они также широко используются злоумышленниками. При помощи поисковых систем привлекаются жертвы на веб-сайты мошенников. При помощи поисковых систем находятся как сведения об уязвимостях, так и сервера, имеющие эти уязвимости. При помощи поисковых систем маскируется местоположение веб-сайтов. При помощи поисковых систем определяются перспективные слова для киберсквоттинга\*. И так далее. В работе специалистов по защите ин-

формации поисковые системы также используются широко. Почему бы не использовать их и в оперативной работе?

Для криминалистики поисковые системы представляют большой интерес, поскольку в них также можно обнаружить следы. Очень многие виды сетевой активности оставляют след в поисковых системах. И этот след не только проще найти, но в ряде случаев он держится в базе данных поисковика дольше, чем в оригинальном расположении.

Например, в ходе одного гражданского дела о нарушении авторских прав истец смог доказать факт размещения ответчиком произведения в сети, хотя ответчик к тому моменту уже успел убрать его с веб-сайта. Но в базе данных двух поисковых систем первоначальная версия сайта ответчика осталась. Заверенные нотариусом распечатки страниц поисковых систем с кэшированным содержимым сайта ответчика признаны судом достаточным доказательством того факта, что в прошлом произведение размещалось в Сети и было общедоступно.

Также поисковик полезен для других задач. Например, для декомпиляции программ. С целью исследования программ для ЭВМ, доступных исследователю только в виде исполняемого (объектного\*) кода, можно воспользоваться декомпилятором. Но проблема в том, что восстановленный таким образом исходный текст\* малопонятен для человека и не соответствует исходному тексту, из которого был сделан объектный код. Говорят, что операция компиляции исходного текста необратима. Вместо декомпиляции можно провести поиск в Интернете на предмет исходного кода этой же программы [57]. Злоумышленник, скорее всего, не написал свою программу с нуля, а позаимствовал ее целиком или немного модифицировал чужую программу, взяв ее из того же источника — из Сети. Невозможно по исполняемому коду восстановить исходный код\* программы на алгоритмическом языке высокого уровня, но возможно доказать, что найденный исходный код соответствует имеющемуся исполняемому коду.

С другой стороны, со стороны поисковой системы тоже можно вести оперативно-розыскную деятельность. Или получать данные в ходе следственных действий. Поисковая система может протоколировать и сохранять все действия пользователя. Объем этой информации относительно невелик, поэтому хранить ее можно без особых затрат на протяжении нескольких лет. Судя по всему, поисковики так и делают.

Когда и какие поисковые запросы отправлял пользователь, по каким из показанных ему ссылок переходил — эти сведения могут быть полезны в ОРД и послужить косвенными доказательствами по уголовному делу.

Поисковая система идентифицирует пользователя по cookie-файлу, а также другим доступным через протокол HTTP параметрам (IP-адрес, версия браузера и ОС, язык, местное время и т.д.).

По некоторым уголовным делам, обнаружив на компьютере подозреваемого cookie от поисковой системы, имеет смысл затребовать протокол действий этого пользователя у администрации поисковика. При этом нужно будет предоставить содержимое cookie и параметры браузера. Разумеется, потребуется судебная санкция.

## Заключение к разделу 2

Мы рассмотрели некоторые, наиболее часто употребляемые виды оперативно-розыскных мероприятий по компьютерным преступлениям и методы их проведения.

В подавляющем большинстве случаев для проведения таких мероприятий не требуется специального оборудования или специальных программных средств. Вполне достаточно обычных средств, имеющихся в распоряжении любого оператора связи. Зато специальные знания необходимы всегда.

Автор еще раз хотел бы обратить внимание, что специальные знания требуются не только, чтобы правильно собирать и документировать доказательства. Специальные знания нужны, чтобы знать, где именно эти доказательства искать. Устройство современных ЭВМ и компьютерных сетей настолько сложно, что следы различных действий остаются в самых неожиданных местах. Неожиданных — для обычного пользователя. А для специалиста, глубоко знающего устройство сетей, — вполне очевидных. И чем глубже его знания, тем больше цифровых доказательств он может обнаружить.