КОМПЬЮТЕРНАЯ РАЗВЕДКА

Тема № 6 Трассировка и идентификация в компьютерной сети

Вопросы:

1. Исследование IP-адресов;
2. Исследование динамических IP-адресов;
3. Исследование адресов MAC;
4. Трассировка электронной почты.

1. ИССЛЕДОВАНИЕ IP-АДРЕСОВ.

ПРОБЛЕМЫ ИДЕНТИФИКАЦИИ ПО IP-АДРЕСУ

1. IP-адрес источника может быть подделан;
2. IP-адрес источника атаки может находиться на расстоянии множества транзитных участков от истинного источника атаки;
3. IP-адрес принадлежит машине (а не человеку), и соответствует определенной системе в определенное время (динамические адреса).

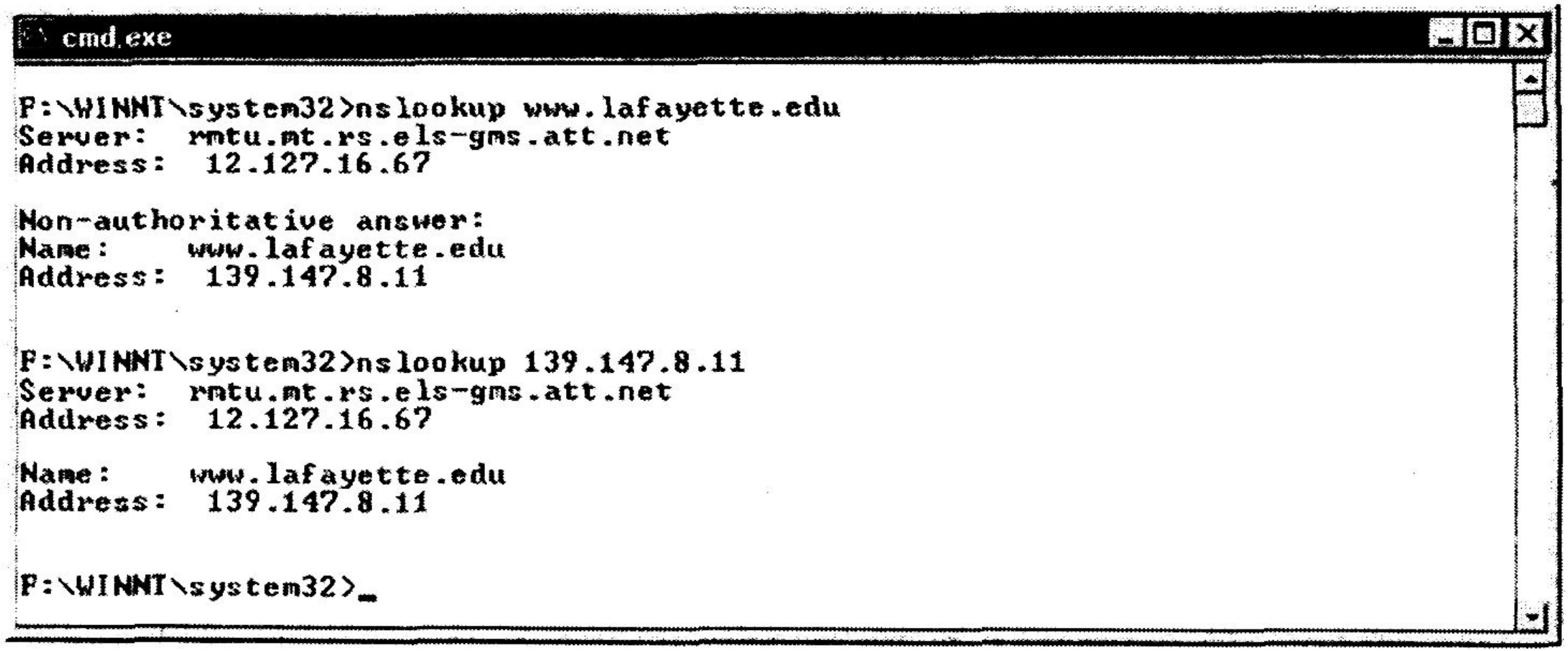
Использование nslookup для идентификации IP-адреса сети

FQDN (fully qualified domain name, полностью квалифицированное имя домена*)* имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS.

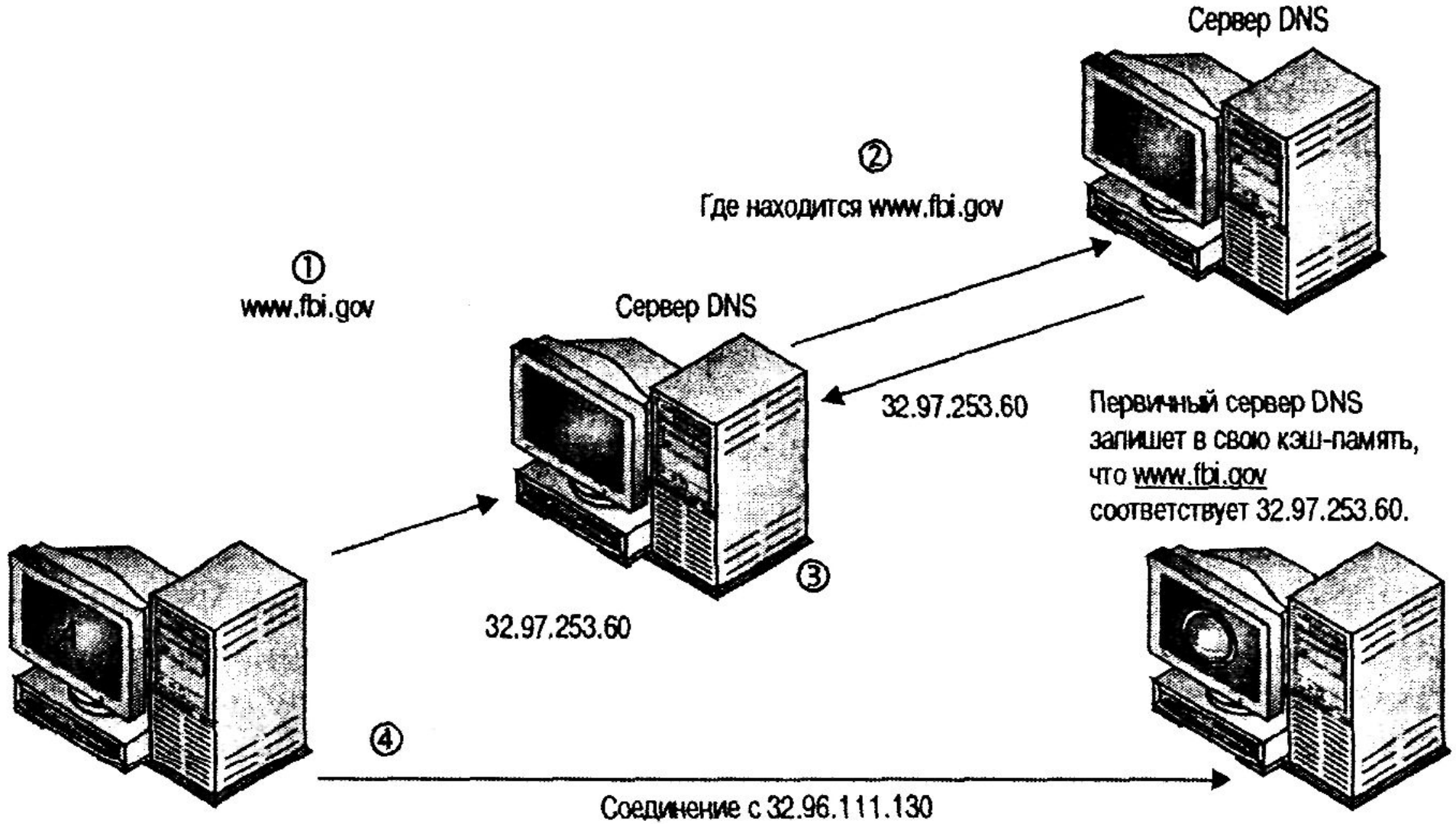
DNS (Domain Name System, система доменных имён) компьютерная распределенная система для получения информации о доменах.

Команда **nslookup** (поиск на сервере имен) используется для получения IP-адреса или FQDN, если известно одна из этих ссылок на системе. **nslookup** просто запрашивает сервер DNS (систему имен доменов), чтобы отобразить IP-адрес в FQDN.

Пример использование консольной утилиты nslookup для идентификации IP-адреса сети



Принцип работы DNS

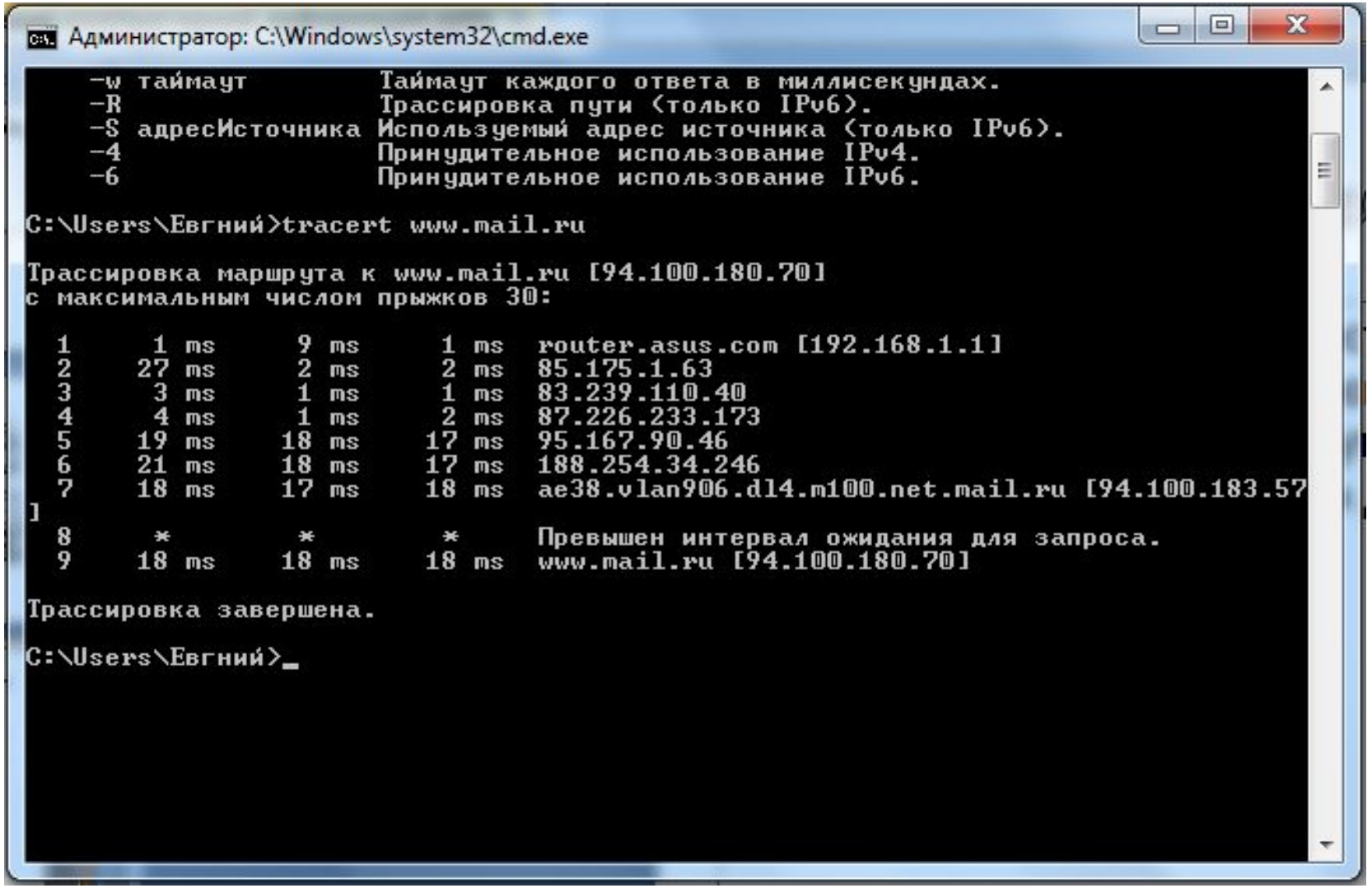


Трассировка IP-адреса компьютерной сети

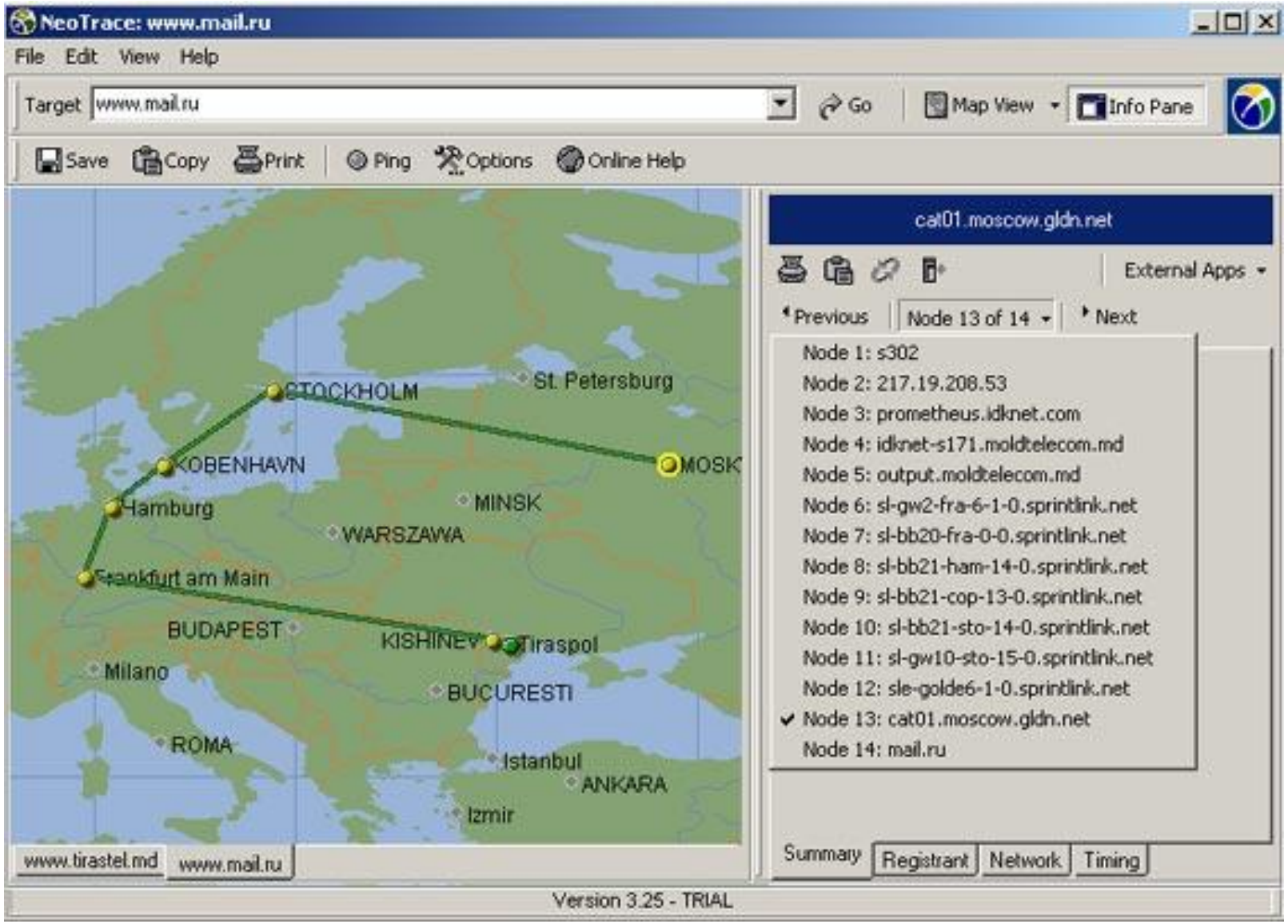
Traceroute, или tracert в системах Windows, является системной командой, которая определяет маршрут, которым следует пакет, чтобы дойти до системы назначения.

Traceroute использует поле TTL (Time To Live — время жизни) протокола Интернета (IP) для получения ответа Time-Excee- ded (превышение времени) протокола контроля сообщений Интернета (ICMP) от каждого маршрутизатора на пути доступа к хосту назначения. Traceroute посылает пакеты протокола датаграмм пользователя (UDP) с небольшим TTL и ожидает возвращения сообщений Time-Exceeded ICMP. Первый пакет, который посылает traceroute, имеет значение TTL, равное 1, и traceroute увеличивает TTL на единицу, пока не будет получен пакет ICMP Port Unreachable (порт недоступен) от выбранного хоста назначения.

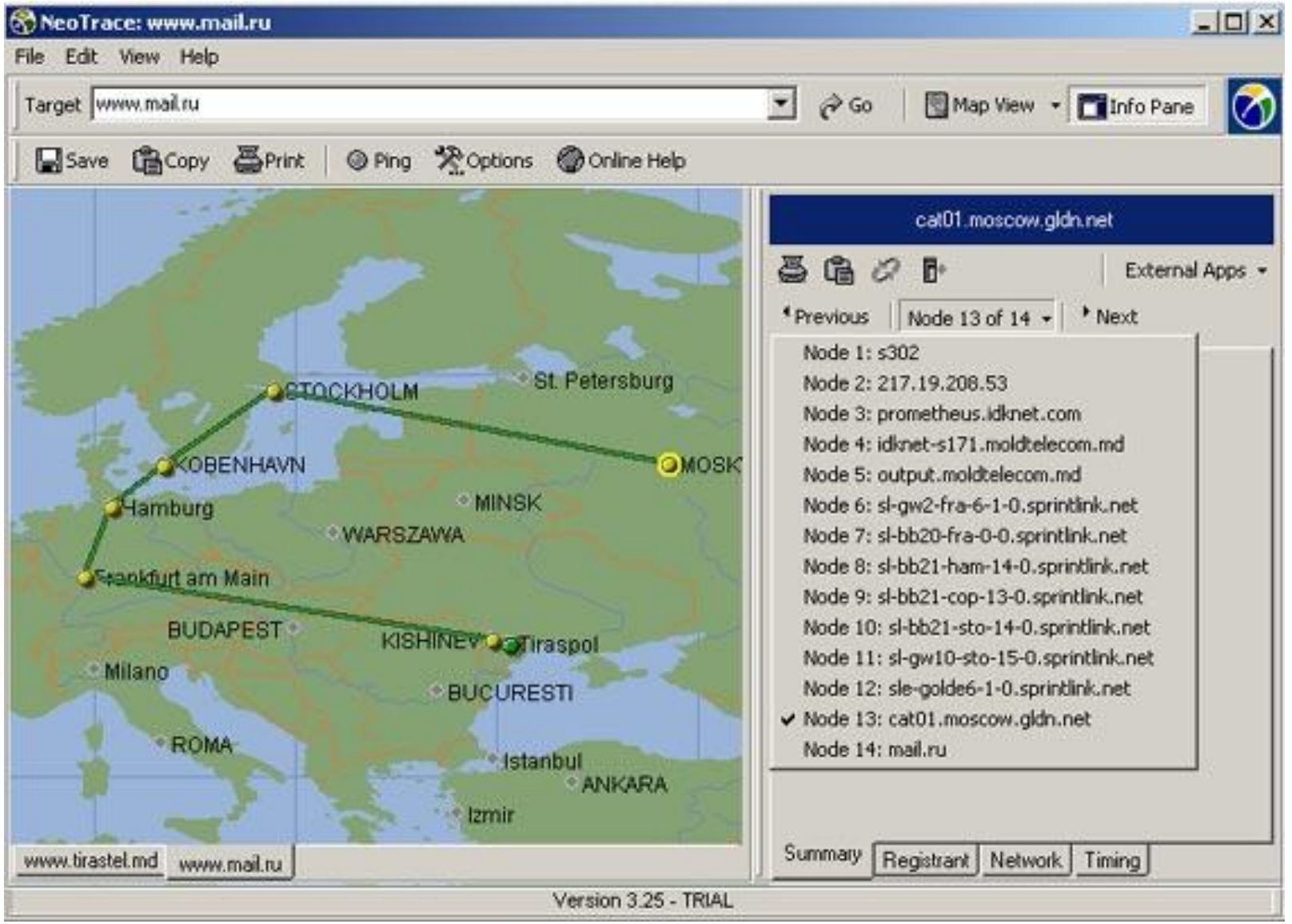
Пример использования команды tracert в системе Windows



Пример графической утилиты, выполняющей функцию трассировки



Пример удаленного сервиса, выполняющей функцию трассировки



Базы данных Whois

База данных Whois является центральным репозиторием, который содержит информацию для каждого домена, зарегистрированного в Интернете. Является своего рода «телефонной книгой».

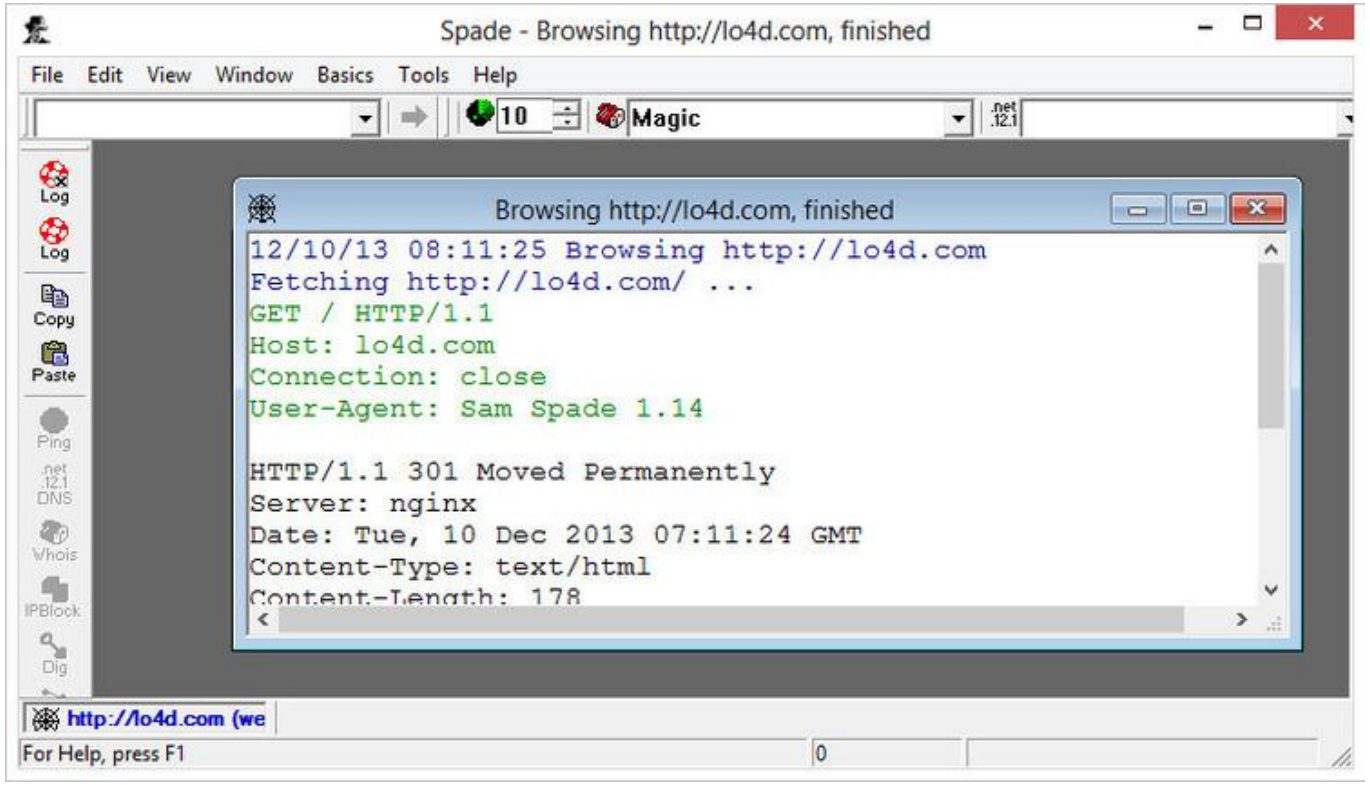
ARIN управляет IP-номерами для Северной Америки, Южной Америки, Карибских островов и Африки, южнее Сахары. ARIN является одним из трех мировых Региональных реестров Интернета (RIR), которые совместно предоставляют службы регистрации IP для всех регионов на земном шаре.

RIPE NCC (Reseaux IP Europeans) обслуживает Европу, Средний Восток и часть Африки.

APNIC (Asia Pacific Network Information Center) обслуживает Азиатско-Тихоокеанский регион.

Выполнение запросов Whois в системах Windows

Системы Windows не имеют утилиты командной строки whois. Поэтому необходимо использовать приложения независимых поставщиков или соответствующие Web-сайты, такие как ARIN или RIPE, для запроса баз данных Whois.



Интерфейс утилиты Sam Spade

ИНФОРМАЦИОННЫЕ РЕСУРСЫ В ИНТЕРНЕТЕ

- Запросы к базе данных Whois ARIN: http://www.arin.net/
- Запросы к базе данных Whois армии США: http://www.nic.mil/dodnic/
- Запросы американских точек контакта: http://www.internic.net/whois.html
- Запросы базы данных Whois RIPE: http://www.ripe.net/cgi-bin/whois
- Запросы базы данных Whois APNIC: http://www.apnic.net/

2. ИССЛЕДОВАНИЕ ДИНАМИЧЕСКИХ IP-АДРЕСОВ.

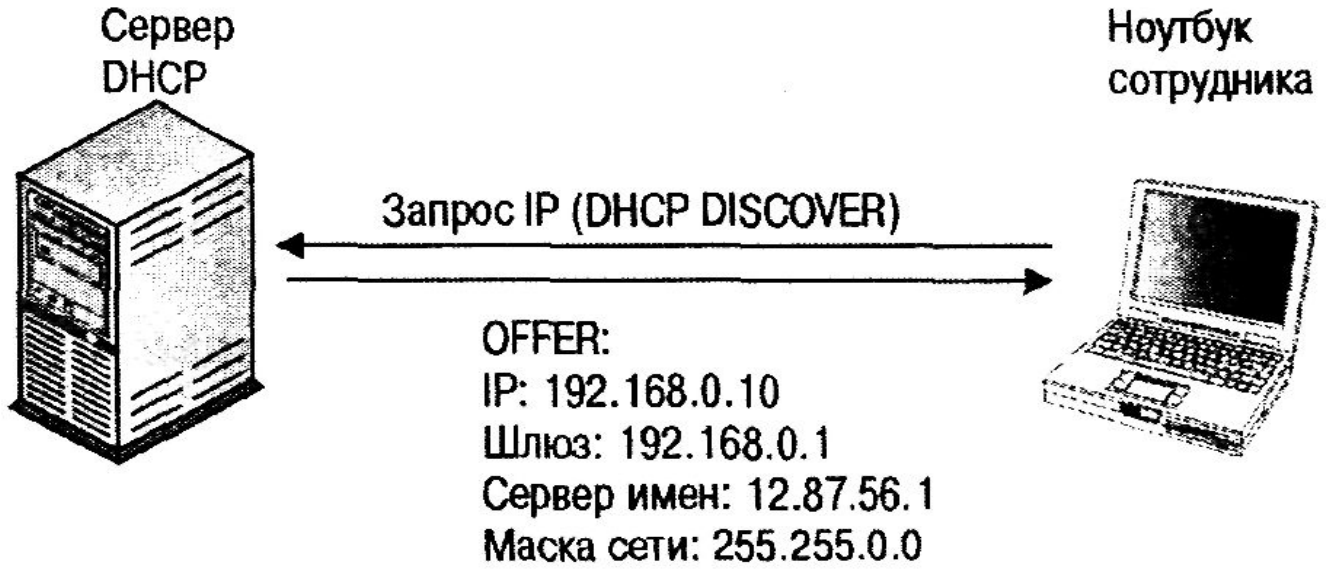
Динамические IP-адреса чаще всего используются для экономии пула IP-адресов *(все современные роутеры позволяют реализовать оба варианта)*. Наиболее распространенные способы сбережения IP-адресов:

- ***трансляция сетевых адресов (NAT);***
- ***протокол динамической конфигурации хоста (DHCP).***

Оба метода обеспечивают распределение IP-адресов, которое может быть динамическим.

Исследование IP-адреса в среде DHCP

DHCP предоставляет динамические IP-адреса хостам, обращающимся к сети. Рабочие станции конфигурируются для получения своих IP-адресов (вместе с другой сетевой информацией) от централизованного сервера DHCP.



Работа начального запроса

log сервера DHCP фиксирует время аренды IP-адреса

Microsoft DHCP Service Activity Log

Event ID	Meaning
00	The log was started.
01	The log was stopped.
02	The log was temporarily paused due to low disk space.
10	A new IP address was leased to a client.
11	A lease was renewed by a client.
12	A lease was released by a client.
13	An IP address was found to be in use on the network.
14	A lease request could not be satisfied because the scope's address pool was exhausted.
15	A lease was denied.
16	A lease was deleted.
17	A lease was expired.
20	A BOOTP address was leased to a client.
21	A dynamic BOOTP address was leased to a client.
22	A BOOTP request could not be satisfied because the scope's address pool for BOOTP was exhausted.
23	A BOOTP IP address was deleted after checking to see it was not in use.
50+	Codes above 50 are used for Rogue Server Detection information.

ID Date,Time,Description,IP Address,Host Name,MAC Address

1) 11,12/05/00,18:35:38,Renew,10.0.2.8,lappie-XX.,00104BDF3720

2)11,12/05/00,18:35:40,Renew,10.0.2.78,TEST2.company.com,006097CC6172

3)11,12/05/00,18:35:40,Renew,10.0.2.8,lappie-XX.,00104BDF3720

4)11,12/05/00,18:39:33,Renew,10.0.2.78,TEST2.company.com,006097CC6172

5) 10,12/05/00,18:39:43,Assign,10.0.2.94,,005056AC0208

6) 17,12/05/00,18:47:55,Expired,10.0.2.21,

Исследование IP-адресов при трансляции сетевых адресов

Трансляция сетевых адресов **(NAT)** позволяет одному устройству с одним реальным, зарегистрированным IP-адресом представлять целую сеть систем в Интернете.

Существуют три диапазона IP-адресов, которые зарезервированы для частного использования:

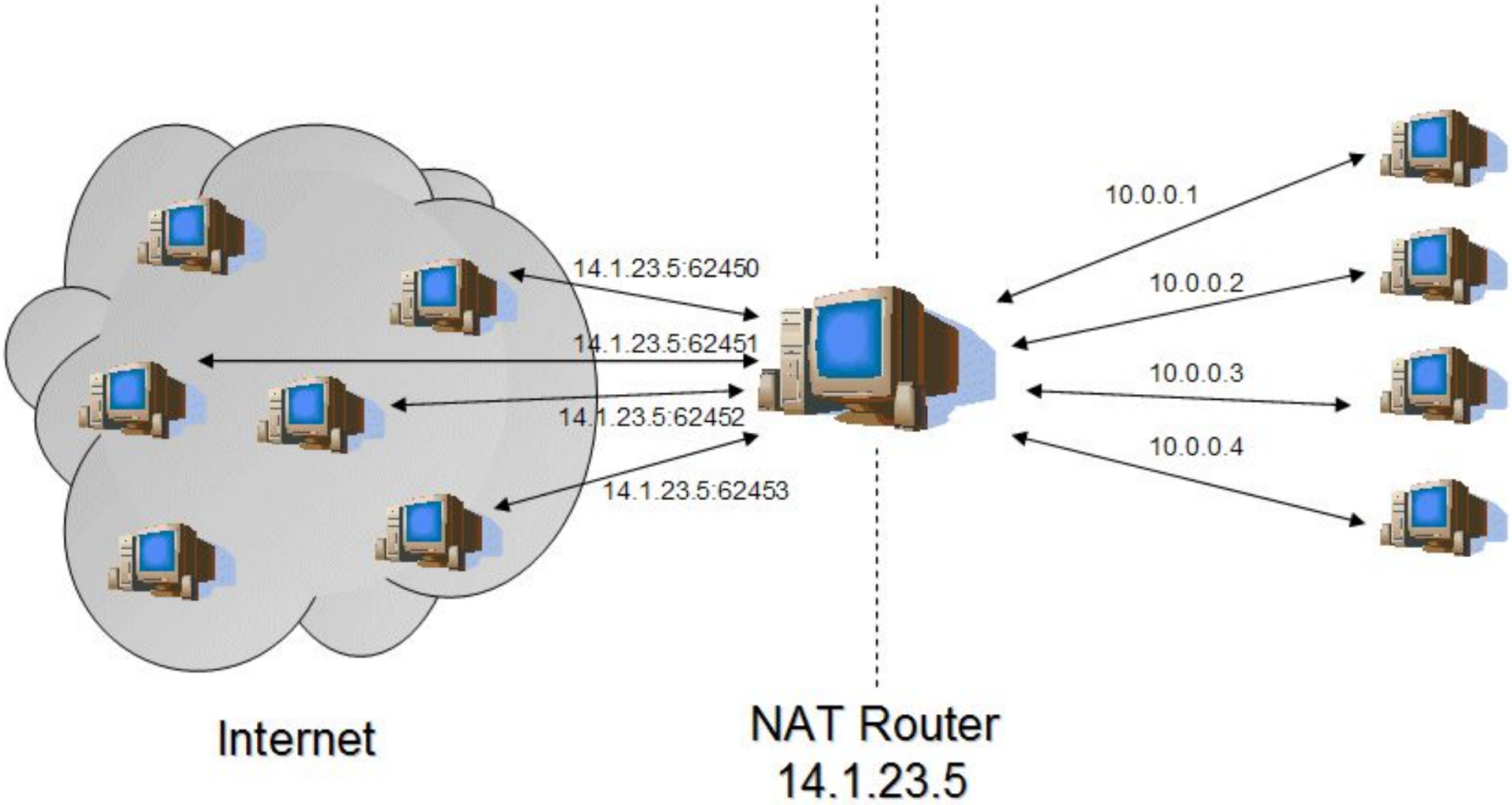
от **10.0.0.0** до **10.255.255.255**,

от **172.16.0.0** до **172.31.255.255**

от **192.168.0.0** до **192.168.255.255**.

Подобные адреса никогда не будут распределены публично и являются *незарегистрированными* номерами.

Принцип работы NAT



2009.03.14 22:48:07 **Smurf** 221.13.14.0, 14150->> 192.168.1.2, 15000 (from ATM1 Inbound)
2009.03.14 22:41:40 ADSL Media Up !
2009.03.14 22:31:03 NTP Date/Time updated.
2009.03.14 22:25:39 ADSL Media Up !
2009.03.14 21:52:55 ADSL Media Up !
2009.03.14 21:34:04 ADSL Media Up !
2009.03.14 21:29:24 ADSL Media Up !
2009.03.14 20:50:29 ADSL Media Up !
2009.03.14 19:49:53 ADSL Media Up !
2009.03.14 19:36:49 ADSL Media Up !
2009.03.14 19:16:24 **Smurf** **221.13.14.0, 14150->> 192.168.1.2**, 15000 (from ATM1 Inbound)
2009.03.14 19:03:07 ADSL Media Up !
2009.03.14 17:49:07 **Smurf** **196.206.196.0, 27844->> 192.168.1.2,** 15000 (from ATM1 Inbound)
2009.03.14 17:27:13 ADSL Media Up !
2009.03.14 16:26:17 ADSL Media Up !
2009.03.14 16:25:12 ADSL Media Up !
2009.03.14 16:22:47 **192.168.1.7** login success
2009.03.14 16:22:40 User from 192.168.1.7 timed out
2009.03.14 16:12:48 ADSL Media Up !
2009.03.14 16:07:46 **192.168.1.7** login success
2009.03.14 16:07:39 **192.168.1.7** login fail
2009.03.14 16:00:47 **Smurf** 192.168.0.255->> 192.168.0.7, Type:3, Code:3 (from ATM1 Outbound)
2009.03.14 16:00:45 **Smurf** 192.168.0.255->> 192.168.0.7, Type:3, Code:3 (from ATM1 Outbound)
2009.03.14 16:00:19 **Smurf** 192.168.0.255->> 192.168.0.7, Type:3, Code:3 (from ATM1 Outbound)
2009.03.14 16:00:11 **Smurf** 192.168.0.255->> 192.168.0.7, Type:3, Code:3 (from ATM1 Outbound)
2009.03.14 16:00:10 **Smurf** 192.168.0.255->> 192.168.0.7, Type:3, Code:3 (from ATM1 Outbound)
2009.03.14 16:00:08 **Smurf** 192.168.0.255->> 192.168.0.7, Type:3, Code:3 (from ATM1 Outbound)
2009.03.14 16:00:07 **Smurf** 192.168.0.255->> 192.168.0.7, Type:3, Code:3 (from ATM1 Outbound)
2009.03.14 16:00:05 **Smurf** 192.168.0.255->> 192.168.0.7, Type:3, Code:3 (from ATM1 Outbound)

Таблица трансляции адресов содержит такую информацию:

- Компьютер-источник
- IP-адрес компьютера-источника
- Номер порта компьютера-источника
- IP-адрес системы NAT
- Присвоенный номер порта системы NAT

3. ИССЛЕДОВАНИЕ АДРЕСОВ MAC

Адрес протокола управления доступом к среде (MAC) компьютера.

Протокол разрешения адреса **(ARP)** является протоколом на основе TCP/IP (другие пакеты протоколов также могут использовать ARP), кото рый отображает логический IP-адрес в физический MAC-адрес.

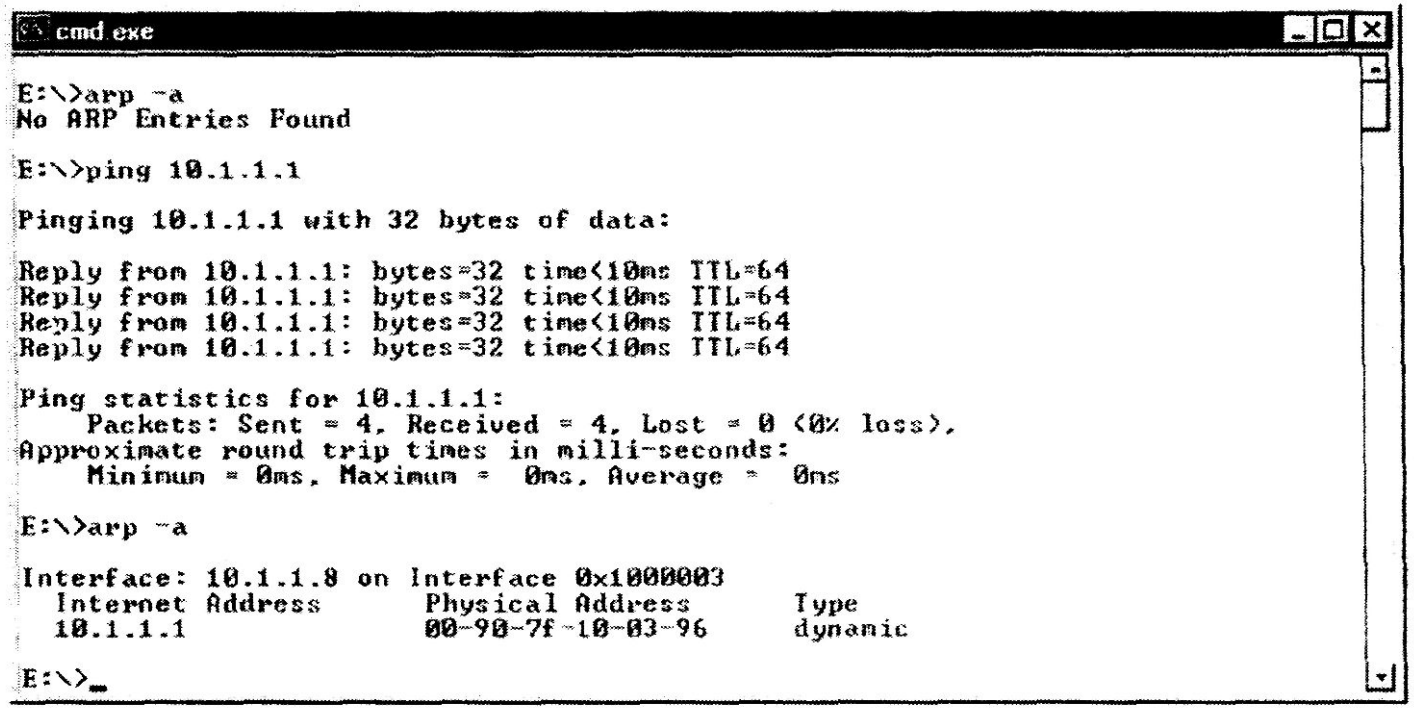
ARP-таблица для адреса 198.150.11.36

MAC-адрес	IP-адрес
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:AB:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35
FE:ED:F9:23:44:EF	198.150.11.36

Просмотр таблицы ARP

Каждая машина поддерживает таблицу ARP, которая отображает адреса MAC в соответствующие IP-адреса. Эта таблица обновляется примерно каждые 30 с на большинстве систем при условии, что не существует исходящих соединений с удаленной машиной, которые находятся в таблице ARP.

Можно использовать команду ***arp -a*** для перечисления содержимого таблицы ARP системы (называемой обычно *кэш-памятью arp).*

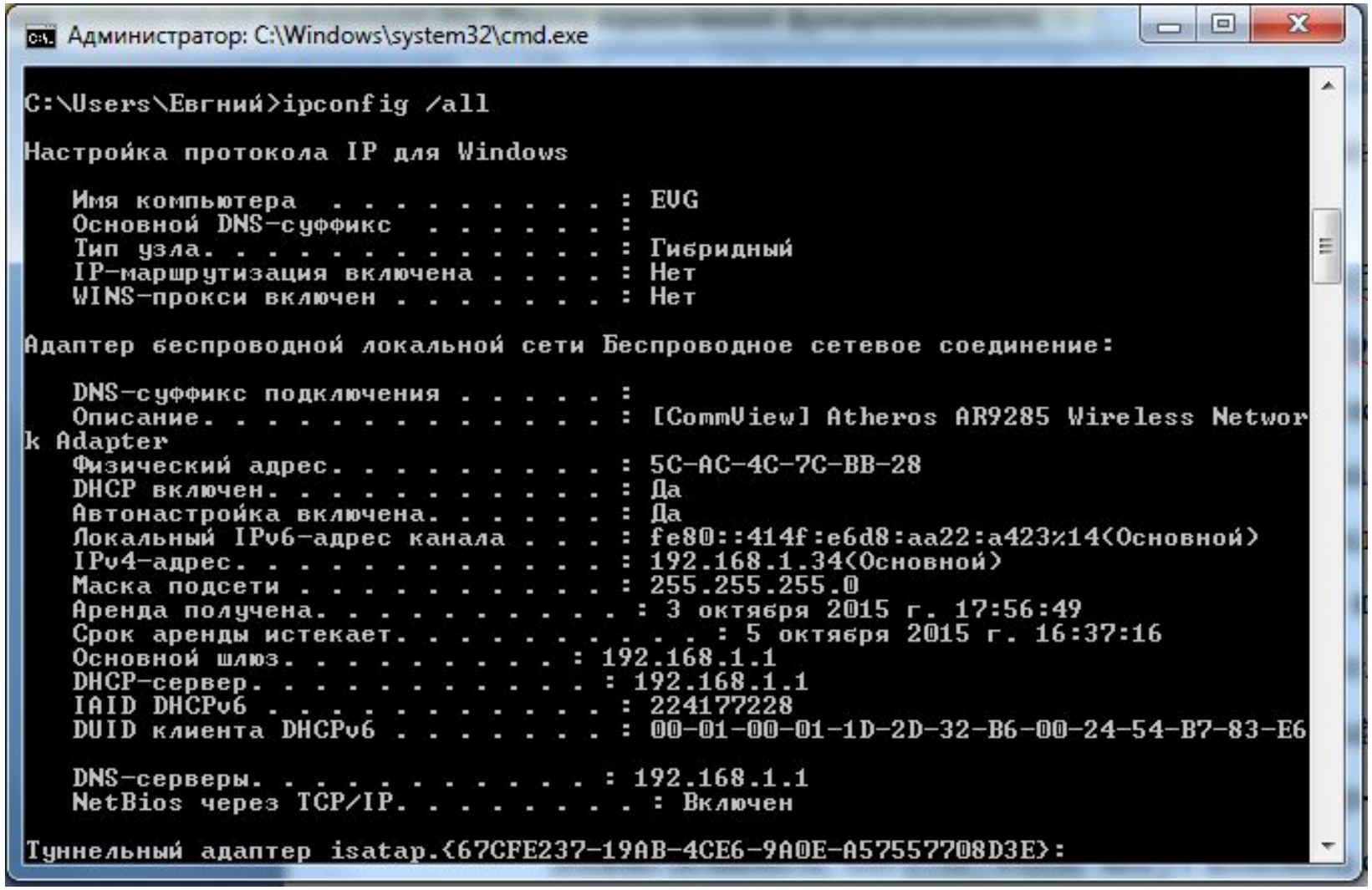


Получение MAC-адреса системы

Если требуется узнать MAC-адрес системы, можно использовать одну из следующих команд:

- На машинах с Windows 9x используйте **winipcfg.**
- На системах с Windows NT/2000 применяйте **ipconfig /all.**
- На системах UNIX, таких как Linux и Solaris, используйте **ifconfog -a**.

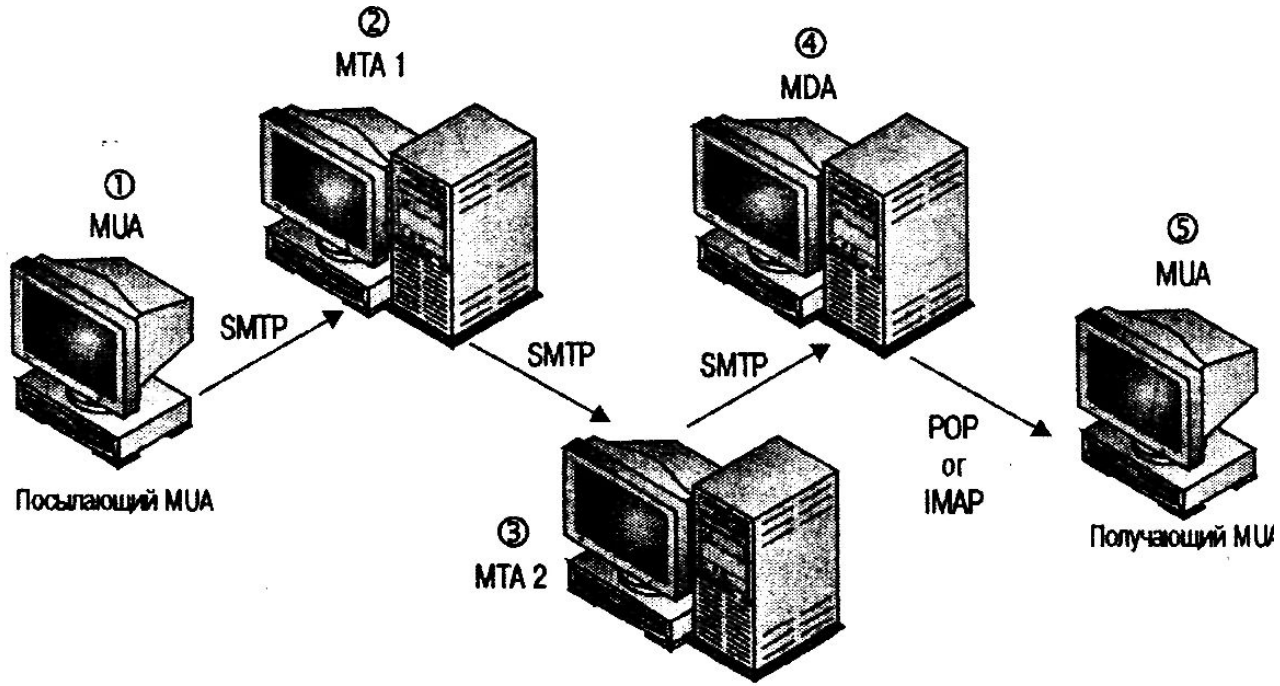
Пример использования команды ipconfig /all



4. ТРАССИРОВКА ЭЛЕКТРОННОЙ ПОЧТЫ

Существуют три компонента в системе e-mail, которые сегодня используются в Интернете:

- ***почтовые агенты пользователей*** (MUA — Mail User Agents);
- ***агенты пересылки почты*** (MTA — Mail Transfer Agents)
- ***агенты доставки почты*** (MDA — Mail Delivery Agents)



① Клиент посылает e-mail через Netscape Messenger локальному серверу SMTP

Трассировка поддельной почты

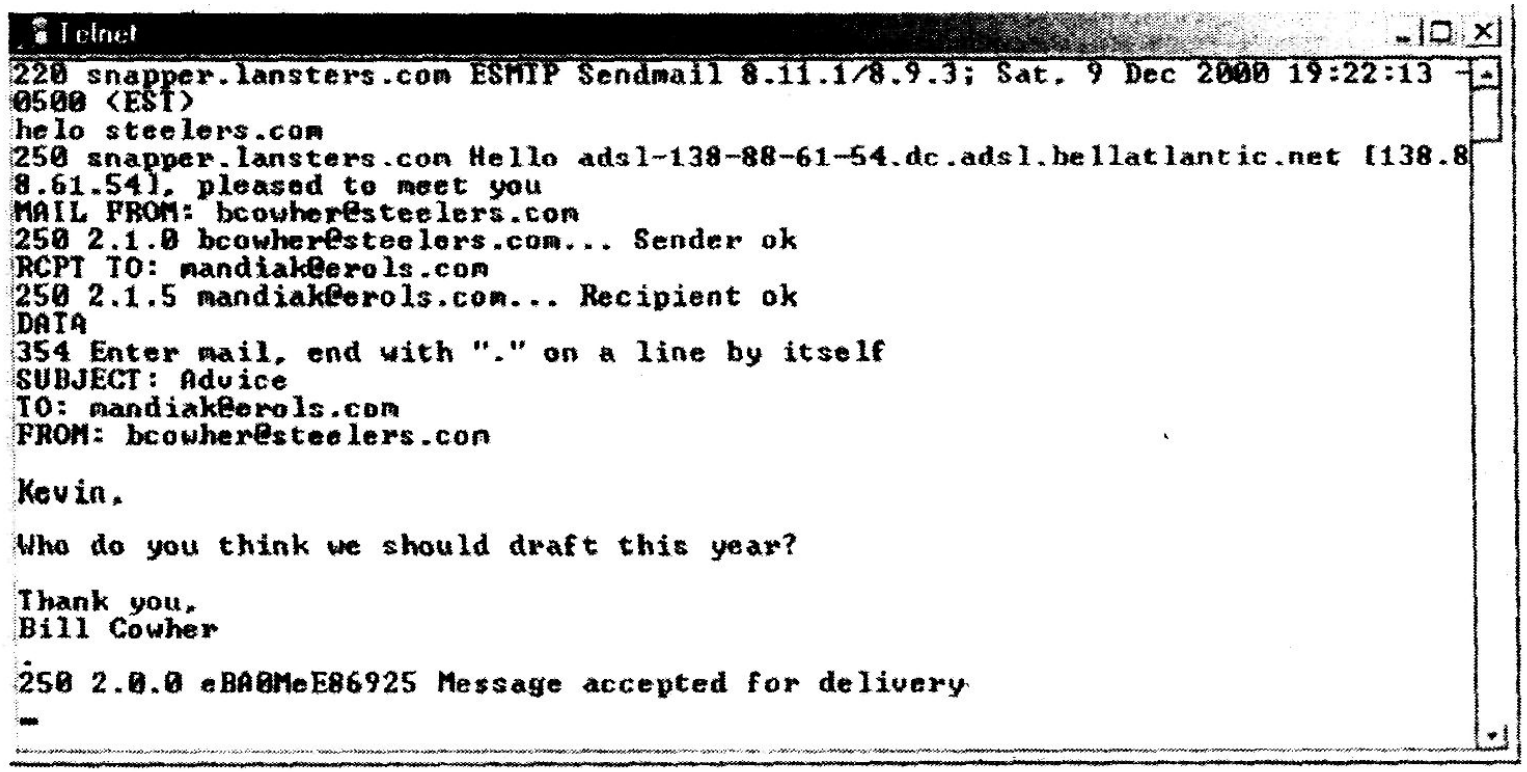
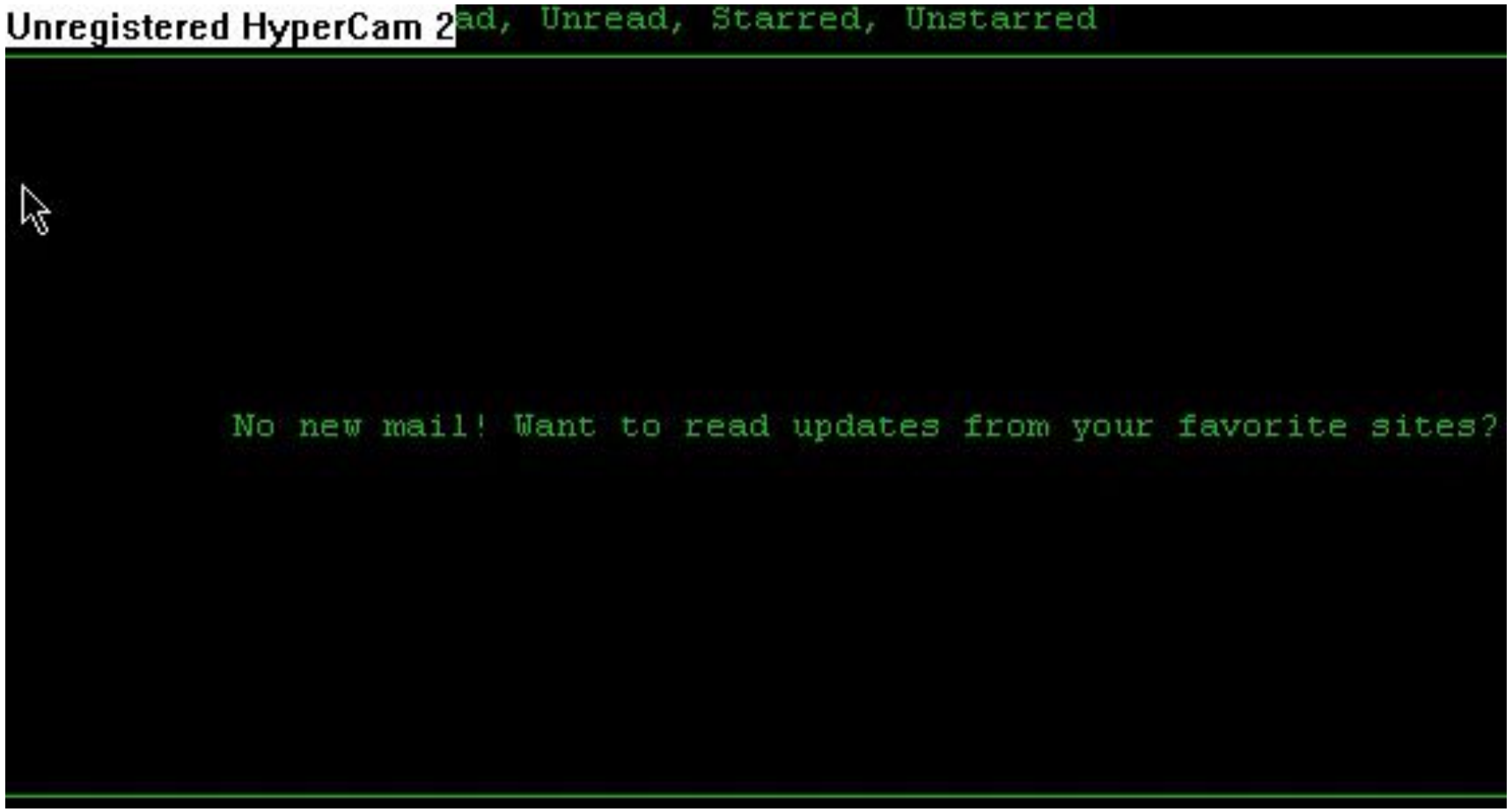


Рис. А. Посылка e-mail с помощью telnet

Посылка e-mail с помощью telnet



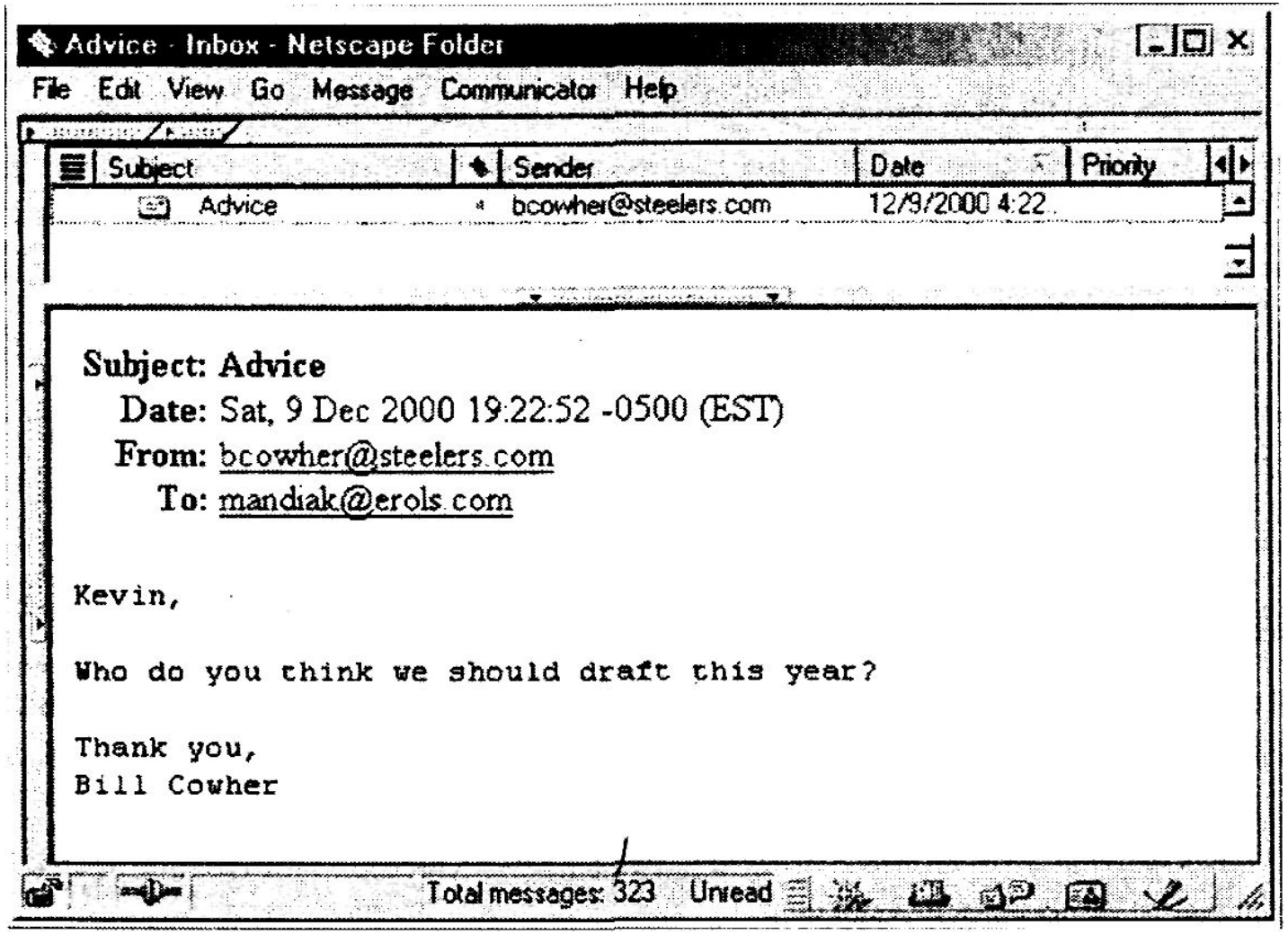
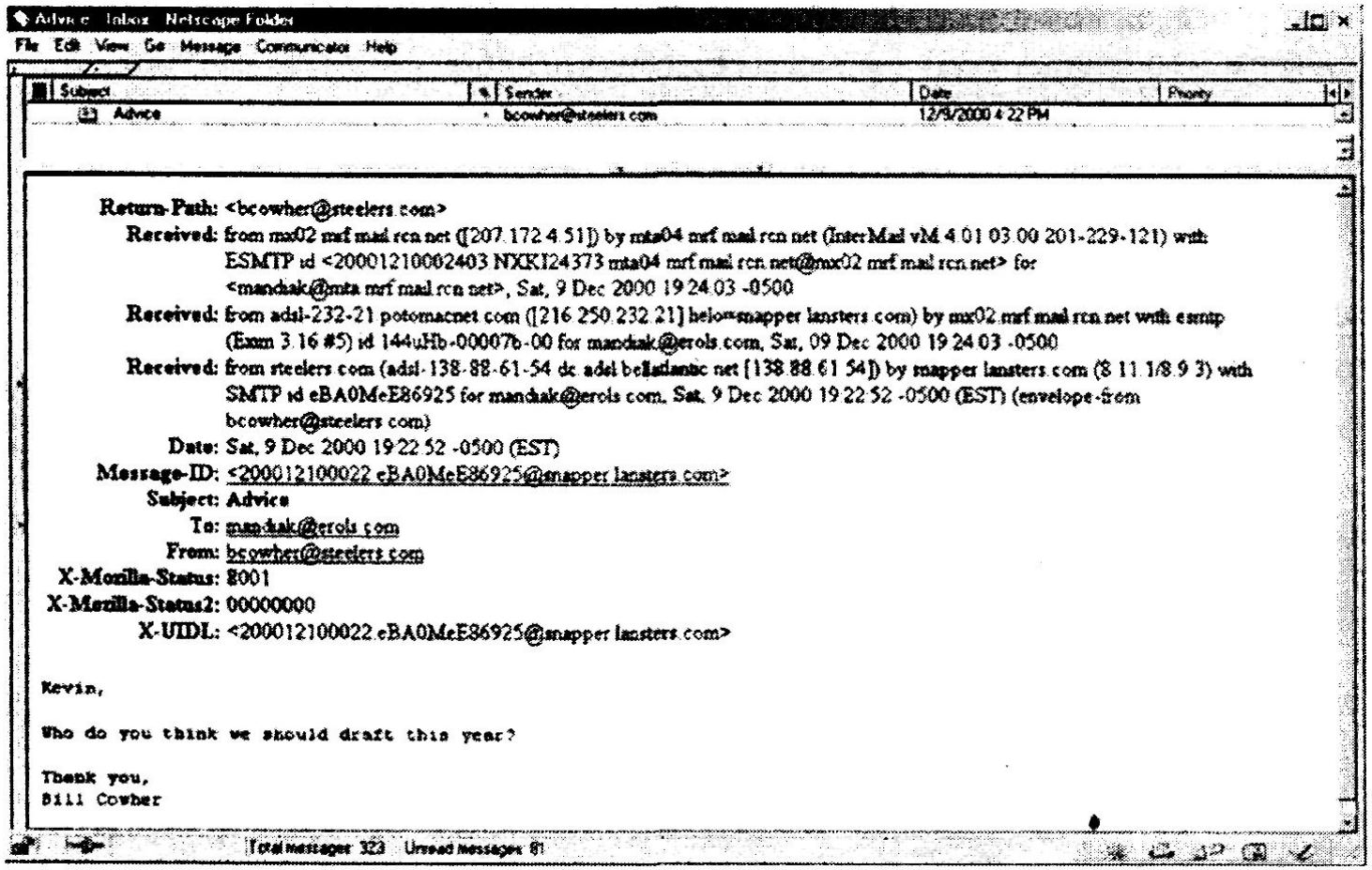
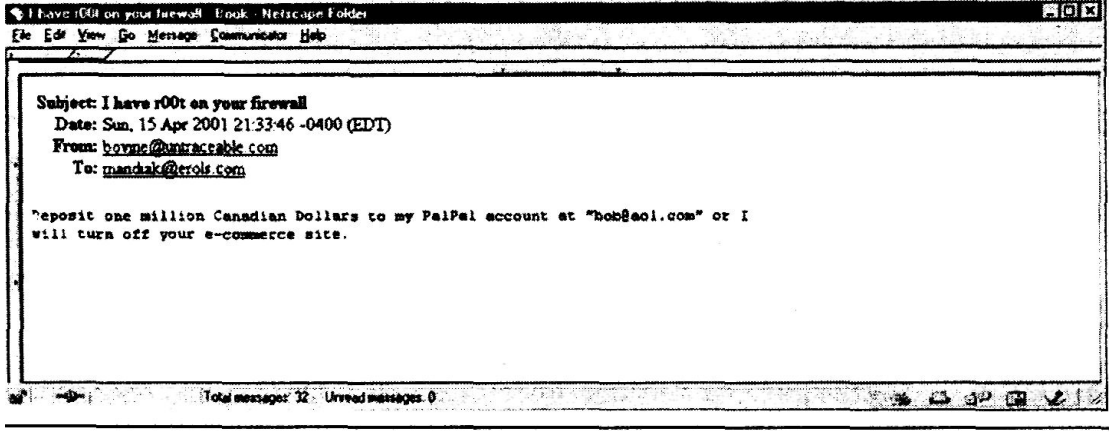


Рис. Б. Получение поддельной почты


Advice - Inbox - Netscape Folder
File Edit View Go Message Communicator Help
Subject
Sender
Date
Priority
Advice
bcowher@steelers.com
12/9/2000 4:22 PM
Return-Path: <bcowher@steelers.com>
Received: from mx02.mrf.mail.rcn.net ([207.172.4.51]) by mta04.mrf.mail.rcn.net (InterMail vM.4.01.03.00.201-229-121) with ESMTP id <20001210002403.NXKI24373.mta04.mrf.mail.rcn.net@mx02.mrf.mail.rcn.net> for <manchak@mta.mrf.mail.rcn.net>, Sat, 9 Dec 2000 19:24:03 -0500
Received: from adsl-232-21.potomacnet.com ([216.250.232.21] helo=mapper.lansters.com) by mx02.mrf.mail.rcn.net with esmtp (Exim 3.16 #5) id 144uHb-00007b-00 for manchak@erols.com, Sat, 09 Dec 2000 19:24:03 -0500
Received: from steelers.com (adsl-138-88-61-54.dc.adel.bellatlantic.net [138.88.61.54]) by mapper.lansters.com (8.11.1/8.9.3) with SMTP id eBA0MeE86925 for manchak@erols.com, Sat, 9 Dec 2000 19:22:52 -0500 (EST) (envelope-from bcowher@steelers.com)
Date: Sat, 9 Dec 2000 19:22:52 -0500 (EST)
Message-ID: <200012100022.eBA0MeE86925@mapper.lansters.com>
Subject: Advice
To: manchak@erols.com
From: bcowher@steelers.com
X-Mozilla-Status: 8001
X-Mozilla-Status2: 00000000
X-UIDL: <200012100022.eBA0MeE86925@mapper.lansters.com>
Kevin,
Who do you think we should draft this year?
Thank you,
Bill Cowher
Total messages: 323 Unread messages: 81



1) Return-Path : <bovine@untraceable.com>

2) Received: from mx02.mrf.mail.rcn.net ([207.172.4.51]) by mta04.mrf.mail.rcn.net(InterMail vM.4.01.03.14 201

3) -229-121-114-20001227) with ESMTP
id<20010416013359.SDEZ22651.mta04.mrf.mail.rcn.net@mx02.mrf.mail.rcn.net> for
<mandiak@mta.mrf.mail.rcn.net>;
Sun, 15 Apr 2001 21:33:59 - 0400

3) Received: from 21-155-124-64.dsl.lan2wan.com ([64.124.155.21]) helo=snapper.lansters.com) by mx02.

4) mrf.mail.rcn.net with esmtp
(Exim 3.16 #5) id 14oxtv-0002jQ-00 for mandiak@erols.com; Sun, 15 Apr 2001 21:33:59 - 0400

4) Received:from nobody@localhost) by snapper.lansters.com (8.11.3/8.9.3) id f3G1Xkq11863 for
mandiak@erols.com;

5) Sun, 15 Apr 2001 21:33:46 - 0400 (EOT) (envelope-from, bovine@untraceable.com)

5) X-Authentication-Warning: snapper.lansters.com: nobody set sender to bcvine@untraceable.com using -f

6) To: mandiak@erols.com

7) Subject: I have rOOt on your firewall

8) Message-ID: <987384826.3ada4bfa10b99@secure.code-monks.com>

9) Date: Sun, 15 Apr 2001 21:33:46 -0400 (EOT)

10) From: bovine@untraceable.com

11) MIME-Version: 1.0

12) Content-Type: text/plain; cha/-set=ISO-88,59-1

13) Content-Transfer-Encoding: 8bit

14) User-Agent: IMP/PHP IMAP webmail program 2.2.3

15) X-Mozilla-Status: 8001

16) X-Mozilla-Status2: 00000000 X-UIDL: 987384826.3ada4bfa10b99@secure.code-monks.com

1) Apr 15 21:33:46 snapper sendmail[11863]: f3G1Xkq11863: from=bovine@untraceable.com, size=453, class=0, nrcpts=1, msgid=<**987384826.3ada4bfa10b99**@secure.code-monks. com>, relay=nobody@localhost

2) Apr 15 21:33:47 snapper imapd[11861]: Logout user=mtpepe host=localhost.lansters.com [127.0.0.1] -

3) Apr 15 21:33:47 snapper imapd[11866]: Authenticated user=mtpepe host=localhost.lansters.com [127.0.0.1]

4) Apr 15 21:33:56 snapper imapd[11866]: Logout user=mtpepe host=localhost.lansters.com [127.0.0.1]

5) Apr 15 21:33:57 snapper sendmail[11865]: f3G1Xkq11863:

to=mandiak@erols.com,ctladdr=bovine@untraceable.com (65534/65533),

delay=00:00:11,xdelay=00:00:11, mailer=esmtp,

pri=30453,relay=mx.mail.rcn.net.

[207.172.4.98], dsn=2.0.0, stat=Sent

(OK id=14oxtv-0002jQ-00@mx02.mrf.mail.rcn.net)

1) 12.38.29.235 - - [15/Apr/2001:21:32:35 -0400] "GET

/webmail/imp/compose.php3?uniq=987384510169 НИР/1.1" 200 15364

2) 12.38.29.235 - - [15/Apr/2001:21:32:46 -0400] "GET

/webmail/imp/status.php3?language=en&message=Message+Composition &status=green HTTP/1.1" 200 1027

3) 12.38.29.235 - - [15/Apr/2001:21:33:46 - - 0400] "POST

/webmail/imp/compose.php3?uniq=5439335813ada4bb339f76 HTTP/1.1" 200 628

4) 12.38.29.235 - - [15/Apr/2001:21:33:56 - - 0400] "GET /webmail/imp/status. php3?language=en&message=Mes'sage+sent+successfully. &status=green HTTP/1.1" 200 1034

ИНФОРМАЦИОННЫЕ РЕСУРСЫ В ИНТЕРНЕТЕ

- Поиск адресов e-mail: http://www.deafworldweb.org/net/dir
- Поиск адресов e-mail: http://www.emailchange.com
- Поиск сообщений в конференциях (по определенному адресу e-mail): http://www.dejanews.com
- Поиск по любым критериям идентификации: http://www.dogpile.com
- Поиск по любым критериям идентификации: http://www.google.com