

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).

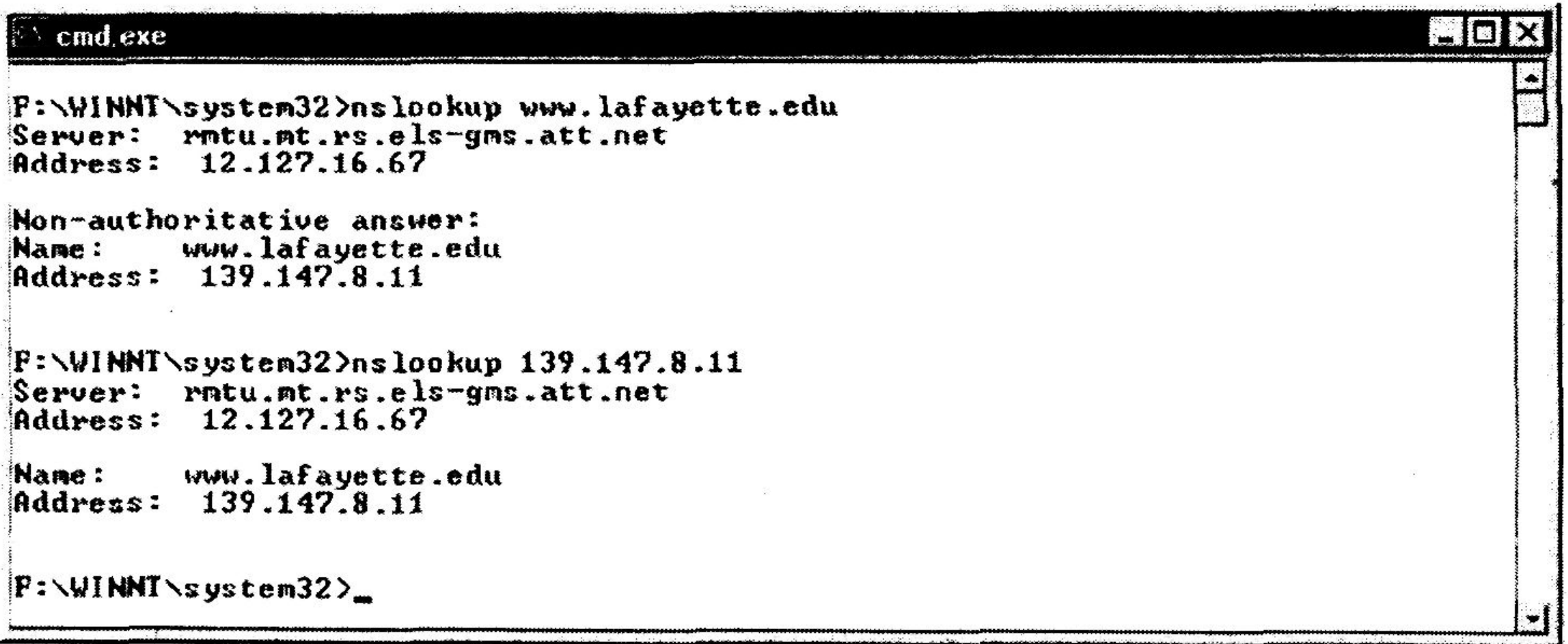
Использование `nslookup` для идентификации IP-адреса сети

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



```
F:\WINNT\system32>nslookup www.lafayette.edu
Server:  rntu.mt.rs.els-gms.att.net
Address:  12.127.16.67

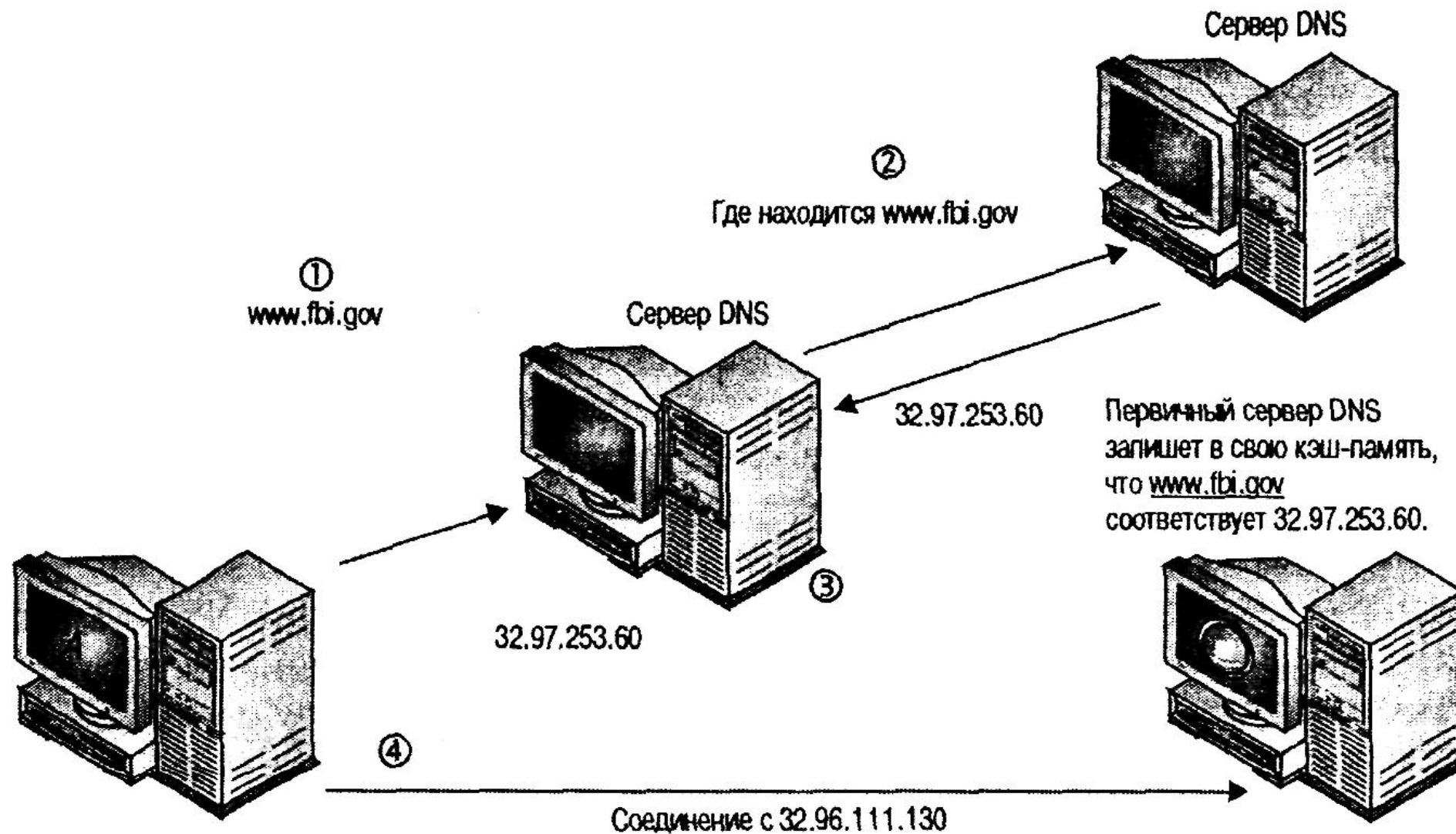
Non-authoritative answer:
Name:    www.lafayette.edu
Address:  139.147.8.11

F:\WINNT\system32>nslookup 139.147.8.11
Server:  rntu.mt.rs.els-gms.att.net
Address:  12.127.16.67

Name:    www.lafayette.edu
Address:  139.147.8.11

F:\WINNT\system32>_
```

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-Exceeded (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

```
Администратор: C:\Windows\system32\cmd.exe
-w таймаут          Таймаут каждого ответа в миллисекундах.
-R                Трассировка пути (только IPv6).
-S адресИсточника  Используемый адрес источника (только IPv6).
-4                Принудительное использование IPv4.
-6                Принудительное использование IPv6.

C:\Users\Евгний>tracert www.mail.ru

Трассировка маршрута к www.mail.ru [94.100.180.70]
с максимальным числом прыжков 30:

 1      1 ms      9 ms      1 ms  router.asus.com [192.168.1.1]
 2     27 ms     2 ms     2 ms  85.175.1.63
 3      3 ms     1 ms     1 ms  83.239.110.40
 4      4 ms     1 ms     2 ms  87.226.233.173
 5     19 ms    18 ms    17 ms  95.167.90.46
 6     21 ms    18 ms    17 ms  188.254.34.246
 7     18 ms    17 ms    18 ms  ae38.vlan906.d14.m100.net.mail.ru [94.100.183.57]
]
 8      *        *        *     Превышен интервал ожидания для запроса.
 9     18 ms    18 ms    18 ms  www.mail.ru [94.100.180.70]

Трассировка завершена.

C:\Users\Евгний>_
```

Пример графической утилиты, выполняющей функцию трассировки

The screenshot displays the NeoTrace application window. The title bar reads "NeoTrace: www.mail.ru". The menu bar includes "File", "Edit", "View", and "Help". The "Target" field contains "www.mail.ru". The toolbar features icons for "Save", "Copy", "Print", "Ping", "Options", and "Online Help".

The main area shows a map of Europe with a green line representing the network path. The path starts at Frankfurt am Main, goes to Hamburg, then to Kobenhavn, Stockholm, and finally to Moscow. Other cities labeled on the map include St. Petersburg, Minsk, Warszawa, Budapest, Kishinev, Tiraspol, Milano, Roma, Bucuresti, Istanbul, Ankara, and Izmir.

On the right side, there is a panel titled "cat01.moscow.gldn.net". It includes navigation buttons for "Previous" and "Next", and a "Node 13 of 14" indicator. The list of nodes is as follows:

- Node 1: s302
- Node 2: 217.19.208.53
- Node 3: prometheus.idknet.com
- Node 4: idknet-s171.moldtelecom.md
- Node 5: output.moldtelecom.md
- Node 6: sl-gw2-fra-6-1-0.sprintlink.net
- Node 7: sl-bb20-fra-0-0.sprintlink.net
- Node 8: sl-bb21-ham-14-0.sprintlink.net
- Node 9: sl-bb21-cop-13-0.sprintlink.net
- Node 10: sl-bb21-sto-14-0.sprintlink.net
- Node 11: sl-gw10-sto-15-0.sprintlink.net
- Node 12: sle-golde6-1-0.sprintlink.net
- ✓ Node 13: cat01.moscow.gldn.net
- Node 14: mail.ru

At the bottom of the right panel, there are buttons for "Summary", "Registrant", "Network", and "Timing". The status bar at the bottom of the window indicates "Version 3.25 - TRIAL".

Пример удаленного сервиса, выполняющей функцию трассировки

The screenshot displays the NeoTrace application window with the target set to `www.mail.ru`. The main map shows a green path connecting several cities: Frankfurt am Main, Hamburg, Kobenhavn, Stockholm, and Moscow. A detailed information pane on the right shows the current node as `cat01.moscow.gldn.net` (Node 13 of 14). The list of nodes includes various IP addresses and domain names, with the final node being `mail.ru`. The interface includes a menu bar (File, Edit, View, Help), a toolbar with icons for Save, Copy, Print, Ping, Options, and Online Help, and a status bar at the bottom indicating 'Version 3.25 - TRIAL'.

Target: `www.mail.ru`

Map View | Info Pane

Save | Copy | Print | Ping | Options | Online Help

cat01.moscow.gldn.net

External Apps

Previous | Node 13 of 14 | Next

- Node 1: s302
- Node 2: 217.19.208.53
- Node 3: prometheus.idknet.com
- Node 4: idknet-s171.moldtelecom.md
- Node 5: output.moldtelecom.md
- Node 6: sl-gw2-fra-6-1-0.sprintlink.net
- Node 7: sl-bb20-fra-0-0.sprintlink.net
- Node 8: sl-bb21-ham-14-0.sprintlink.net
- Node 9: sl-bb21-cop-13-0.sprintlink.net
- Node 10: sl-bb21-sto-14-0.sprintlink.net
- Node 11: sl-gw10-sto-15-0.sprintlink.net
- Node 12: sle-golde6-1-0.sprintlink.net
- ✓ Node 13: cat01.moscow.gldn.net
- Node 14: mail.ru

Summary | Registrant | Network | Timing

www.tirastel.md | www.mail.ru

Version 3.25 - TRIAL

Базы данных Whois

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

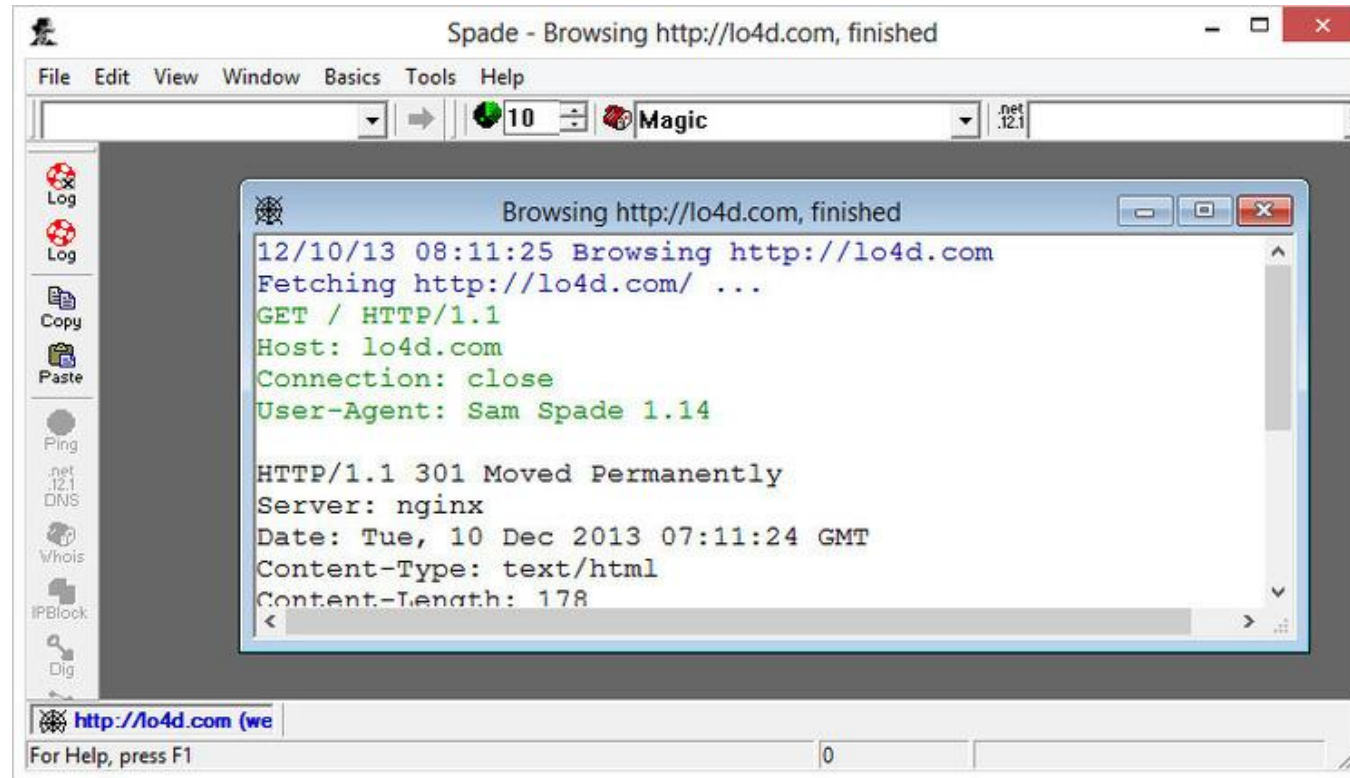
ARIN управляет IP-номерахми для Северной Америки, Южной Америки, Карибских островов и Африки, южнее Сахары. ARIN является одним из трех мировых Региональных реестров Интернета (RIR), которые совместно предоставляют службы регистрации IP для всех регионов на земном шаре.

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.



The screenshot displays the Sam Spade utility interface. The main window is titled "Spade - Browsing http://lo4d.com, finished". The interface includes a menu bar (File, Edit, View, Window, Basics, Tools, Help), a toolbar with icons for Log, Copy, Paste, Ping, .net, .12.1, DNS, Whois, IPBlock, and Dig, and a status bar at the bottom. The central pane shows the output of a browsing operation:

```
Browsing http://lo4d.com, finished
12/10/13 08:11:25 Browsing http://lo4d.com
Fetching http://lo4d.com/ ...
GET / HTTP/1.1
Host: lo4d.com
Connection: close
User-Agent: Sam Spade 1.14

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Tue, 10 Dec 2013 07:11:24 GMT
Content-Type: text/html
Content-Length: 178
<
```

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.

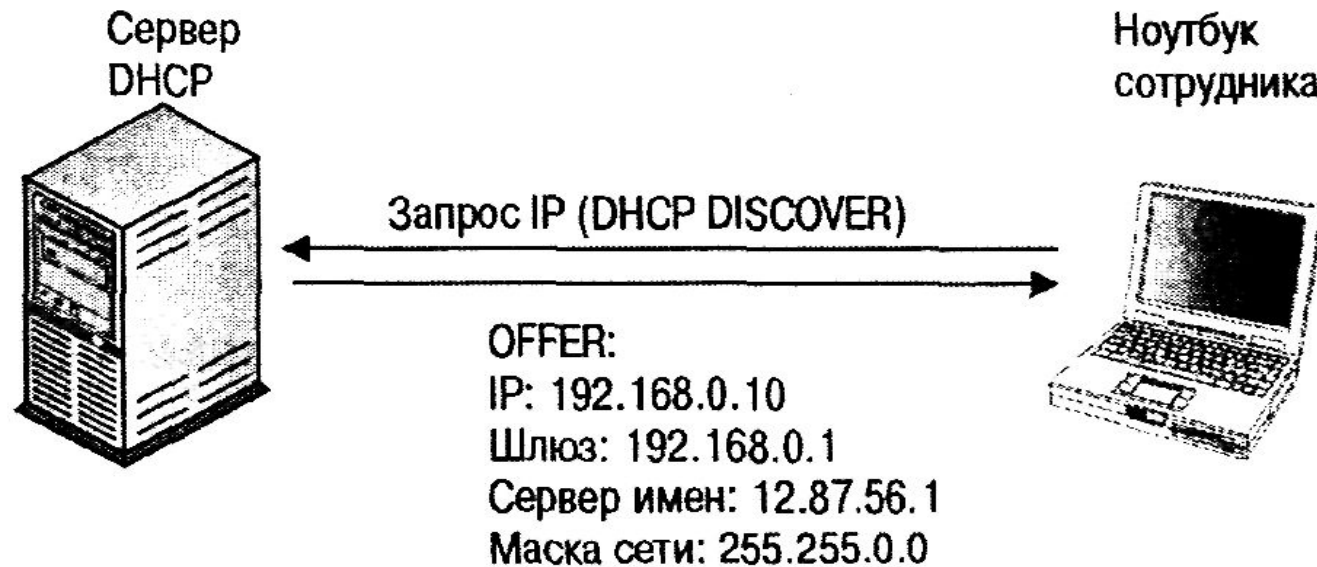
Динамические IP-адреса чаще всего используются для экономии пула IP-адресов (*все современные роутеры позволяют реализовать оба варианта*). Наиболее распространенные способы сбережения IP-адресов:

- *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

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,

log сервера DHCP фиксирует время аренды IP-адреса

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:

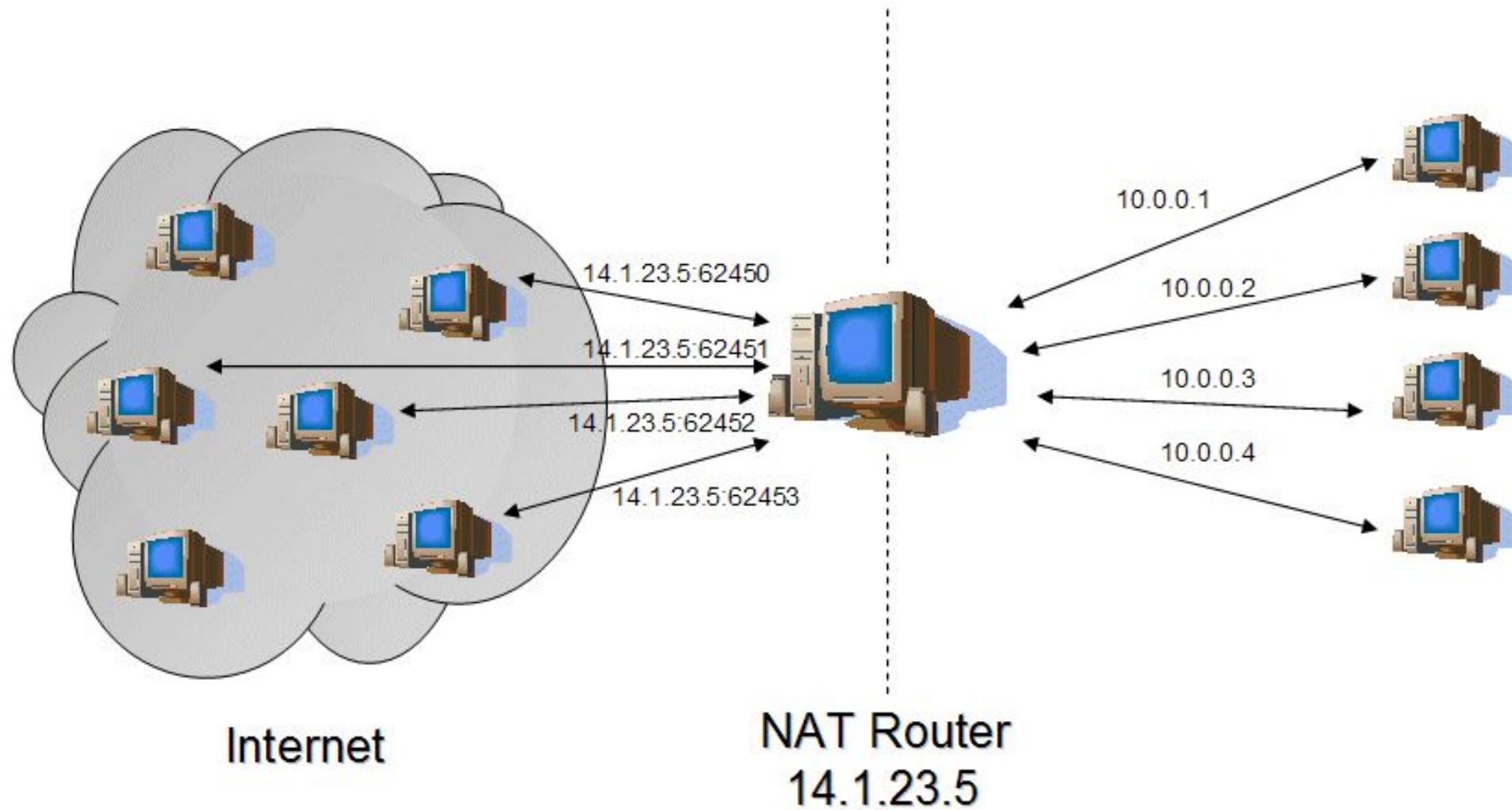
от **10.0.0.0** до **10.255.255.255**,

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), который отображает логический IP-адрес в физический MAC-адрес.

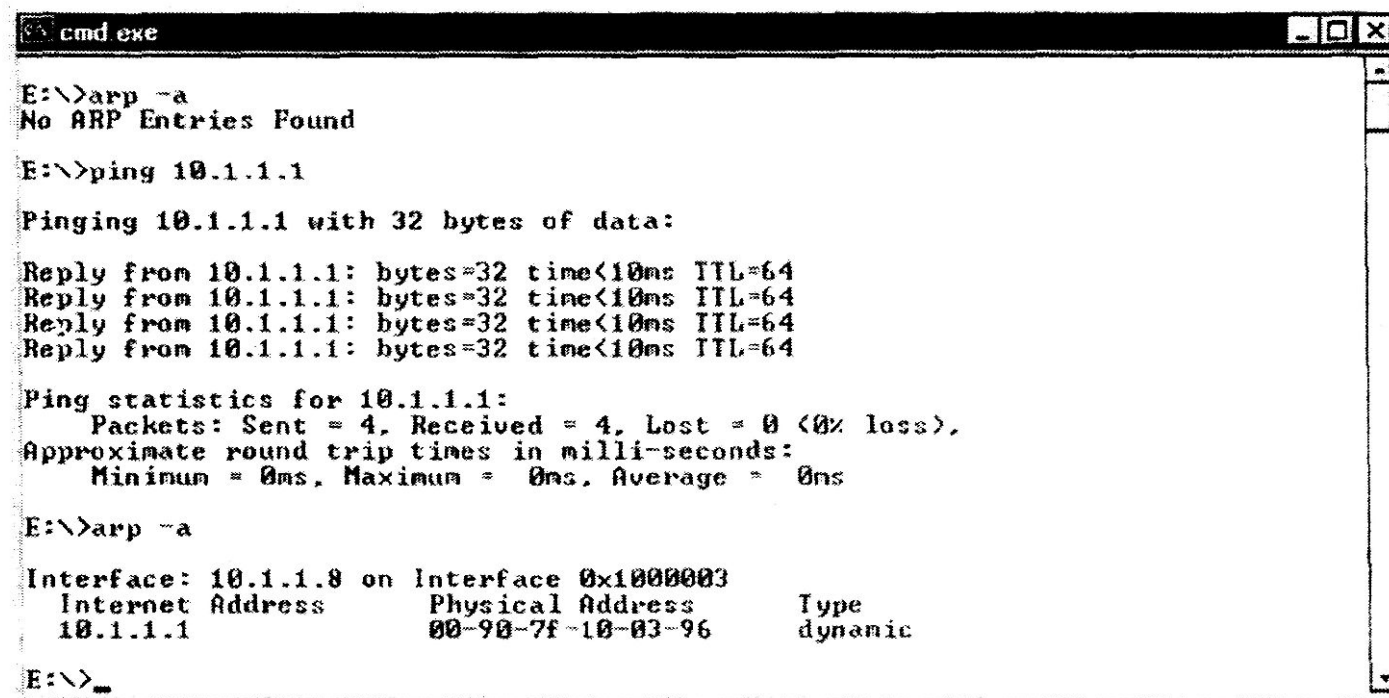
ARP-таблица для адреса 198.150.11.36

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*).



```
cmd.exe
E:\>arp -a
No ARP Entries Found

E:\>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time<10ms TTL=64
Reply from 10.1.1.1: bytes=32 time<10ms TTL=64
Reply from 10.1.1.1: bytes=32 time<10ms TTL=64
Reply from 10.1.1.1: bytes=32 time<10ms TTL=64

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

E:\>arp -a

Interface: 10.1.1.8 on Interface 0x10000003
    Internet Address      Physical Address      Type
    10.1.1.1              00-90-7f-10-03-96    dynamic

E:\>_
```


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 **ifconfig -a**.

Пример использования команды ipconfig /all

```
Администратор: C:\Windows\system32\cmd.exe

C:\Users\Евгний>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : EUG
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . . : Нет
WINS-прокси включен . . . . . : Нет

Адаптер беспроводной локальной сети Беспроводное сетевое соединение:

DNS-суффикс подключения . . . . . :
Описание. . . . . : [CommView] Atheros AR9285 Wireless Network Adapter
Физический адрес. . . . . : 5C-AC-4C-7C-BB-28
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::414f:e6d8:aa22:a423%14(Основной)
IPv4-адрес. . . . . : 192.168.1.34(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 3 октября 2015 г. 17:56:49
Срок аренды истекает. . . . . : 5 октября 2015 г. 16:37:16
Основной шлюз. . . . . : 192.168.1.1
DHCP-сервер. . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 224177228
DUID клиента DHCPv6 . . . . . : 00-01-00-01-1D-2D-32-B6-00-24-54-B7-83-E6

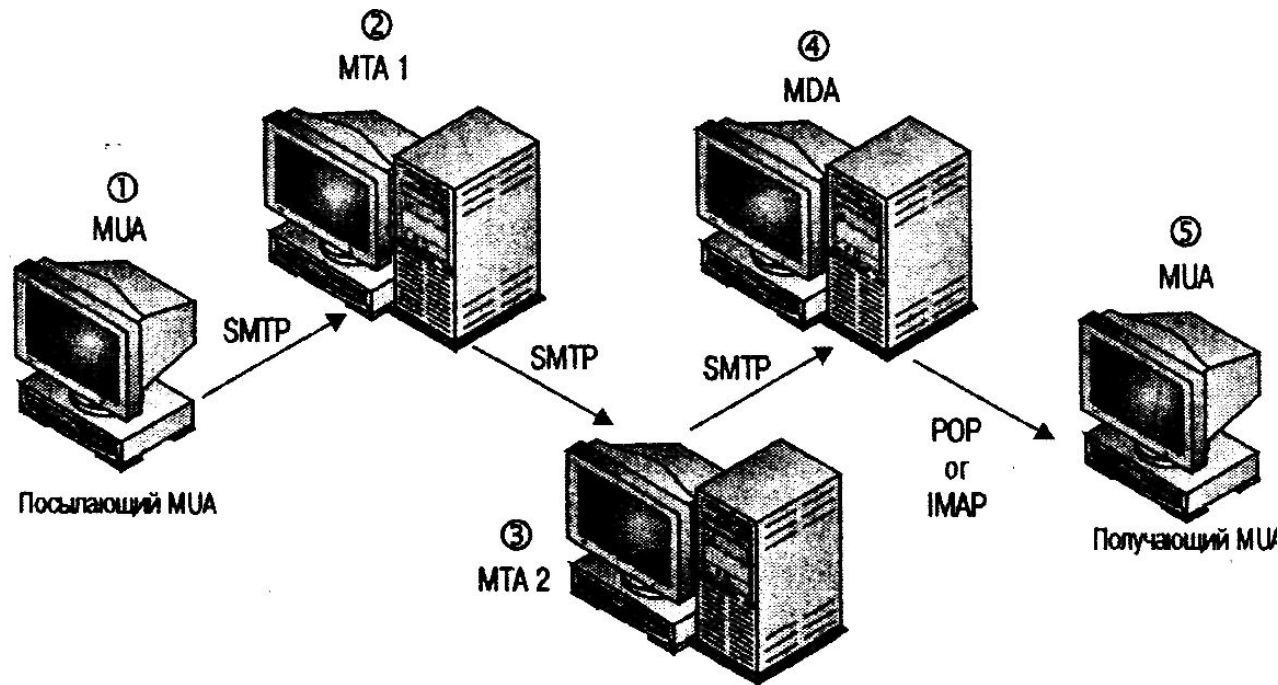
DNS-серверы. . . . . : 192.168.1.1
NetBios через TCP/IP. . . . . : Включен

Туннельный адаптер isatap.<67CFE237-19AB-4CE6-9A0E-A57557708D3E>:
```

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

```
Telnet
220 snapper.lansters.com ESMTP Sendmail 8.11.1/8.9.3; Sat, 9 Dec 2000 19:22:13
0500 <EST>
helo steelers.com
250 snapper.lansters.com Hello adsl-138-88-61-54.dc.adsl.bellatlantic.net [138.8
8.61.54], pleased to meet you
MAIL FROM: bcowher@steelers.com
250 2.1.0 bcowher@steelers.com... Sender ok
RCPT TO: mandiak@erols.com
250 2.1.5 mandiak@erols.com... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
SUBJECT: Advice
TO: mandiak@erols.com
FROM: bcowher@steelers.com

Kevin,

Who do you think we should draft this year?

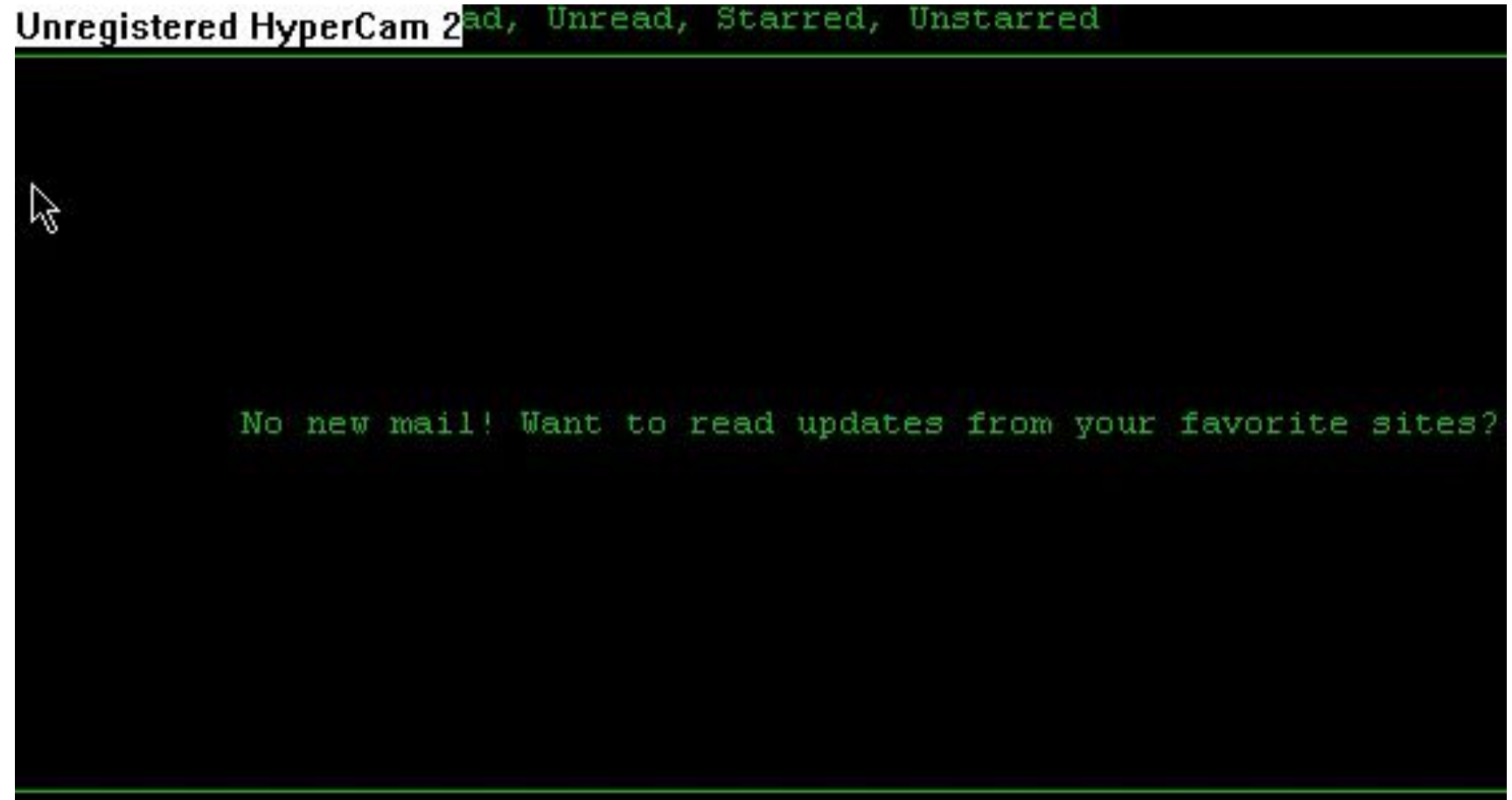
Thank you,
Bill Cowher

250 2.0.0 eBA8MeE86925 Message accepted for delivery
-
```

Рис. А. Посылка e-mail с помощью telnet

Посылка e-mail с помощью telnet

```
Unregistered HyperCam 2 ad, Unread, Starred, Unstarred
```



```
No new mail! Want to read updates from your favorite sites?
```

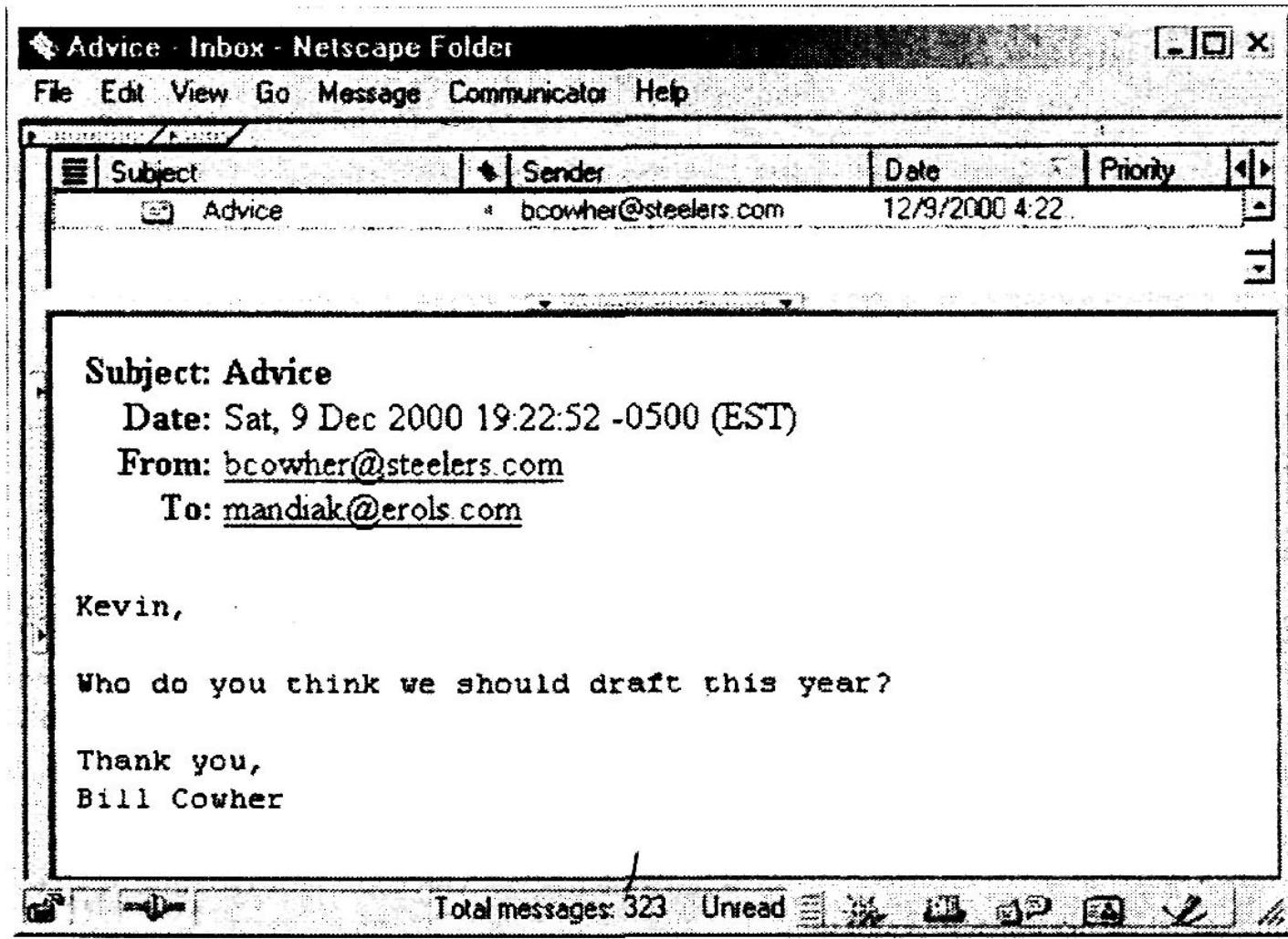


Рис. Б. Получение поддельной почты

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.mai.rcn.net ([207.172.4.51]) by mta04.mrf.mai.rcn.net (InterMail vM 4.01.03.00 201-229-121) with ESMTP id <20001210002403.NXKI24373.mta04.mrf.mai.rcn.net@mx02.mrf.mai.rcn.net> for <mandak@mta.mrf.mai.rcn.net>, Sat, 9 Dec 2000 19:24:03 -0500

Received: from adsl-232-21.potomacnet.com ([216.250.232.21]) by mx02.mrf.mai.rcn.net with esmtp (Exam 3.16 #5) id 144uHb-00007b-00 for mandak@erols.com, Sat, 09 Dec 2000 19:24:03 -0500

Received: from steelers.com (adsl-138-88-61-54.de.adel.bellatlantic.net [138.88.61.54]) by snapper.lansters.com (8.11.1/8.9.3) with SMTP id eBA0McE86925 for mandak@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.eBA0McE86925@snapper.lansters.com>

Subject: Advice

To: mandak@erols.com

From: bcowher@steelers.com

X-Mozilla-Status: 8001

X-Mozilla-Status2: 00000000

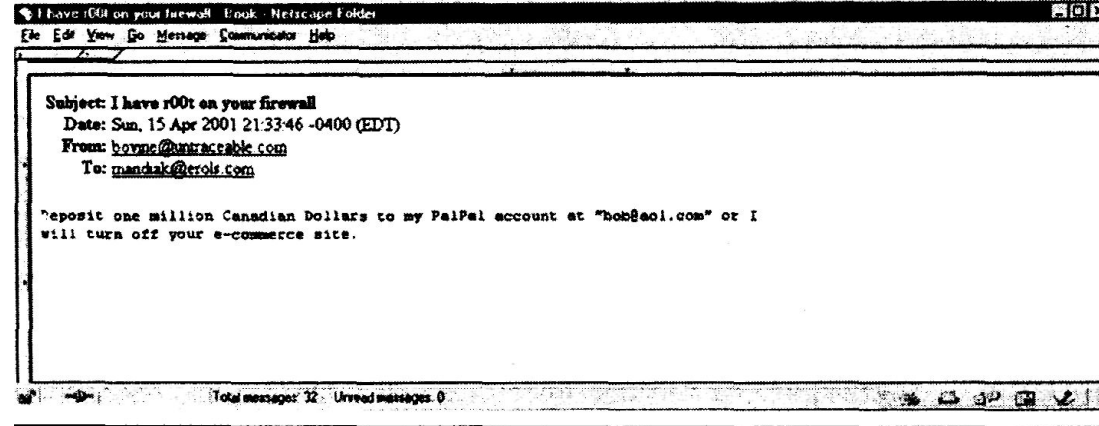
X-UIDL: <200012100022.eBA0McE86925@snapper.lansters.com>

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 r00t 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=esmtplib, 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](mailto: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 HTTP/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>