ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

*Московский институт электроники и математики им. А.Н.Тихонова*

**Домашнее задание №4, вариант 1. Основы цифровой форензики.**

По направлению 10.04.01 – «Информационная безопасность»

Проверил:

преп. Сорокин А. В.

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Выполнил:

Новиков В. С. МКБ 241

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2025

# Задание «Вариант 1».

1. Каков IP-адрес зараженного узла?
2. Каков MAC-адрес зараженного узла?
3. Каково доменное имя зараженного узла?
4. Какие сайты посетил пользователь зараженного устройства по своему желанию?
5. Посещение каких сайтов зафиксировано в сетевом трафике?
6. Каково доменное имя сайта, с которого произошла загрузка вредоносного программного обеспечения?
7. Каков IP-адрес узла, с которого произошла загрузка вредоносного программного обеспечения?
8. Загружались ли пользователем или системой без ведома пользователя файлы, не являющиеся вредоносными?
9. Какие сайты (доменные имена) задействованы в заражении пользователя вредоносным программным обеспечением (имеют следы вредоносной активности, участвуют во вредоносных действиях)?
10. Каков механизм переходов (перенаправлений) пользователя с посещенных сайтов на сайт, с которого было загружено вредоносное программное обеспечение?

# Решение

## Каков IP-адрес зараженного узла?

Statistics → Endpoints → IPv4 → сортировка по Packets

Абсолютный лидер среди внутренних адресов — 172.16.165.165

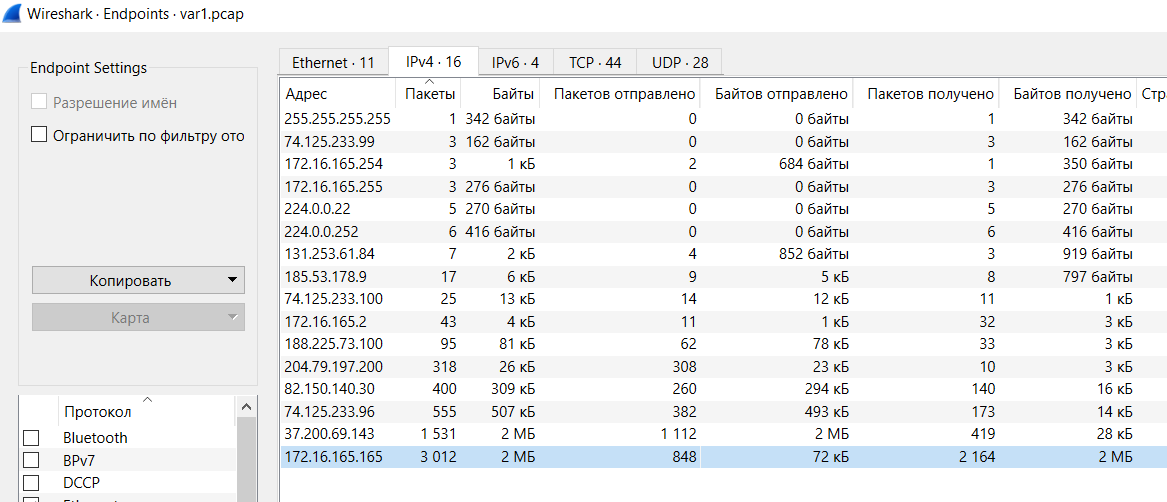


Рисунок 1 «сортировка IP по Packets»

# Каков MAC-адрес зараженного узла?

У IP-адреса 172.16.165.165 число входящих пакетов 2 МБ и исходящих ≈ 848 пакетов / 72 КБ.

Это почти совпадает со строкой f0:19:af:02:9b:f1 (разница в десяток пакетов объясняется тем, что IP-и Ethernet-таблицы считаются в разное время/фильтрации).

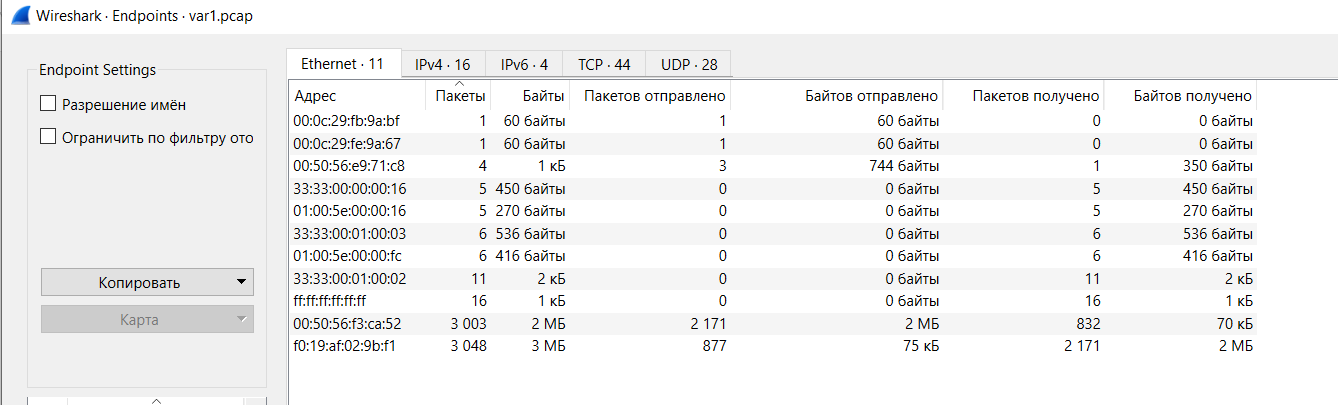


Рисунок 2 «сортировка Ethernet по Packets»

## Каково доменное имя зараженного узла?

Введем команду для вывода имени с учетом IP 172.16.165.165:

*bootp.option.hostname && ip.addr==172.16.165.165*

DHCP hostname не передавался, NBNS тоже пустой → имя не определяется («N/A»).

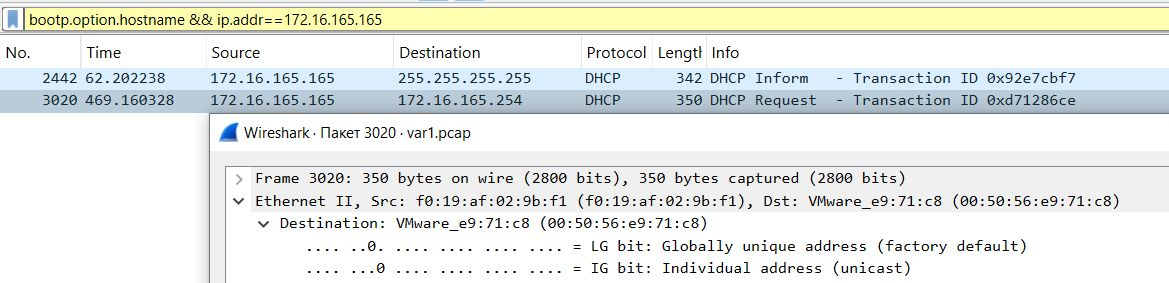


Рисунок 3 «bootp.option.hostname && ip.addr==172.16.165.165»

## Какие сайты посетил пользователь зараженного устройства по своему желанию?

Введем фильтр, который выведет все HTTP-запросы и первый пакет любой HTTPS-сессии IP 172.16.165.165:

*ip.src == 172.16.165.165 && (http.request || tls.handshake.type == 1)*

http.request || tls.handshake.type == 1 означает, что есть начало HTTPS-сеанса со стороны клиента (поле Handshake Type = 1 (Client Hello))

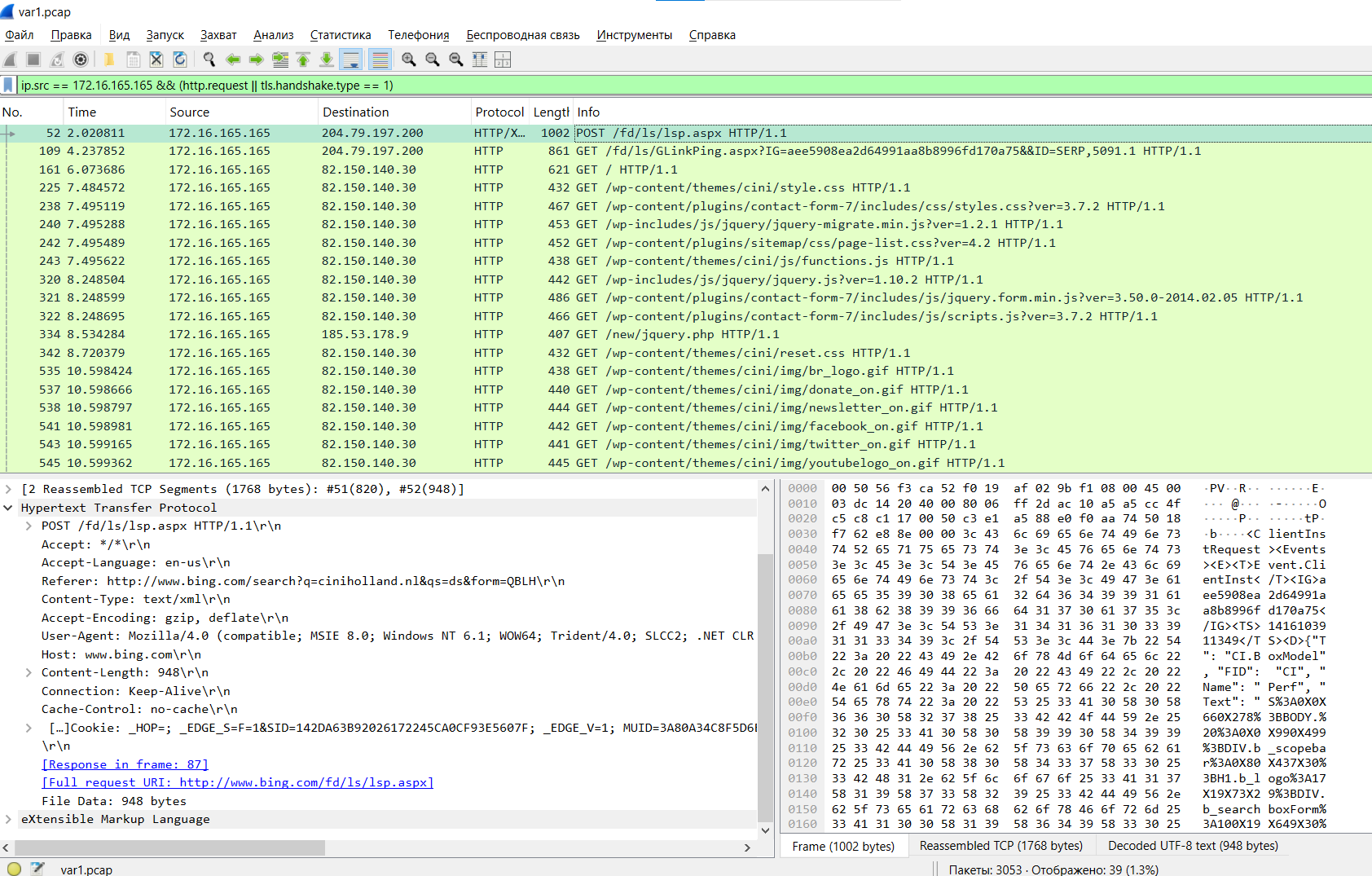


Рисунок 4 «ip.src == 172.16.165.165 && (http.request || tls.handshake.type == 1)»

Ответ (пользователь зараженного устройства посетил по своему желанию):

* www.bing.com поиск
* www.ciniholland.nl клик по выдаче

## Посещение каких сайтов зафиксировано в сетевом трафике?

В Wireshark перейти по Statistics → HTTP → Requests.

Вывод:

www.bing.com - страница поиска

www.ciniholland.nl - «ручной» переход

stand.trustandprobaterealty.com - конечный malware-хост, отдаёт JAR/SWF/MP3

adultbiz.in - промежуточный зловредный скрипт (`/new/jquery.php`)

24corp-shop.com - redirect-вставка (+ gif «notfound»)

www.youtube.com - встраиваемый плеер (`/embed/…`)

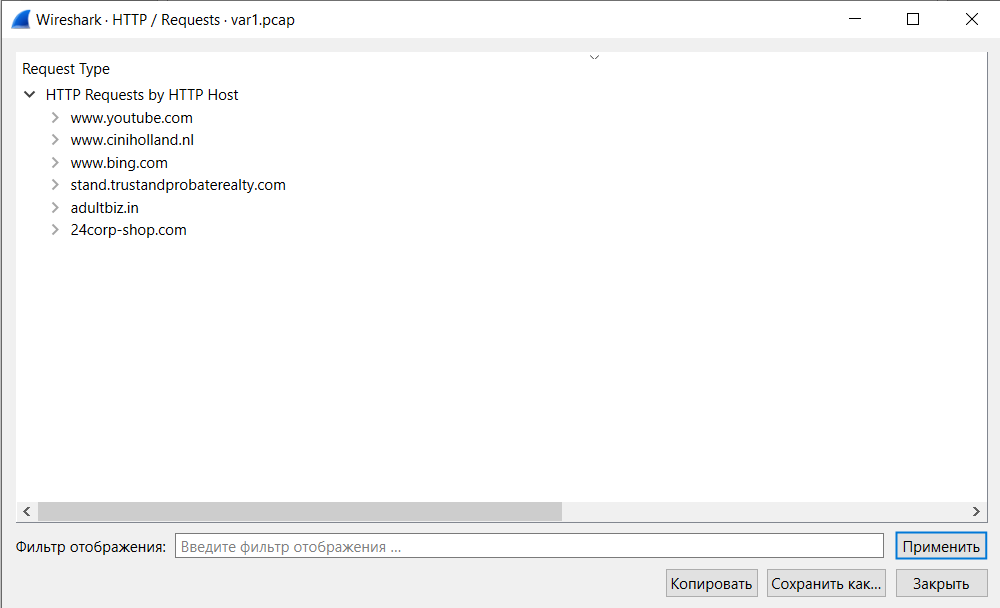


Рисунок 5 «Statistics → HTTP → Requests»

## Каково доменное имя сайта, с которого произошла загрузка вредоносного программного обеспечения?

Ответ: stand.trustandprobaterealty.com

В Wireshark откроем File → Export Objects → HTTP**.** Сортировка по Типу содержимого:

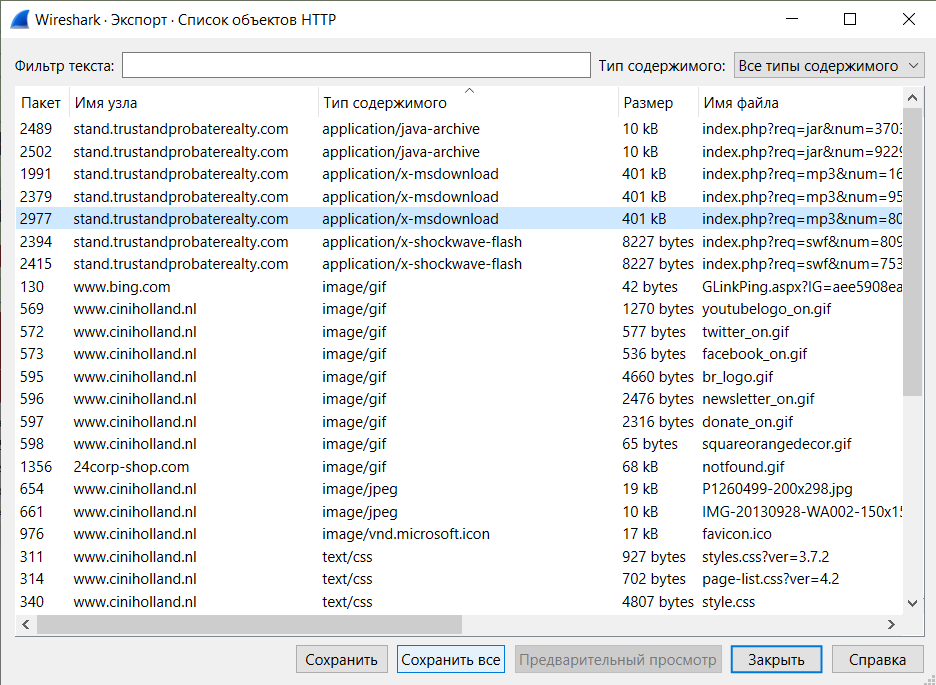


Рисунок 6 «File → Export Objects → HTTP»

## Каков IP-адрес узла, с которого произошла загрузка вредоносного программного обеспечения?

В Wireshark откроем File → Export Objects → HTTP**.** Сортировка по Типу содержимого и выбираем загрузки. В Wireshark отобразиться IP адрес с которого произошла загрузка вредоносного программного обеспечения - **37.200.69.143**

Host = stand.trustandprobaterealty.com

IP.dst = 37.200.69.143

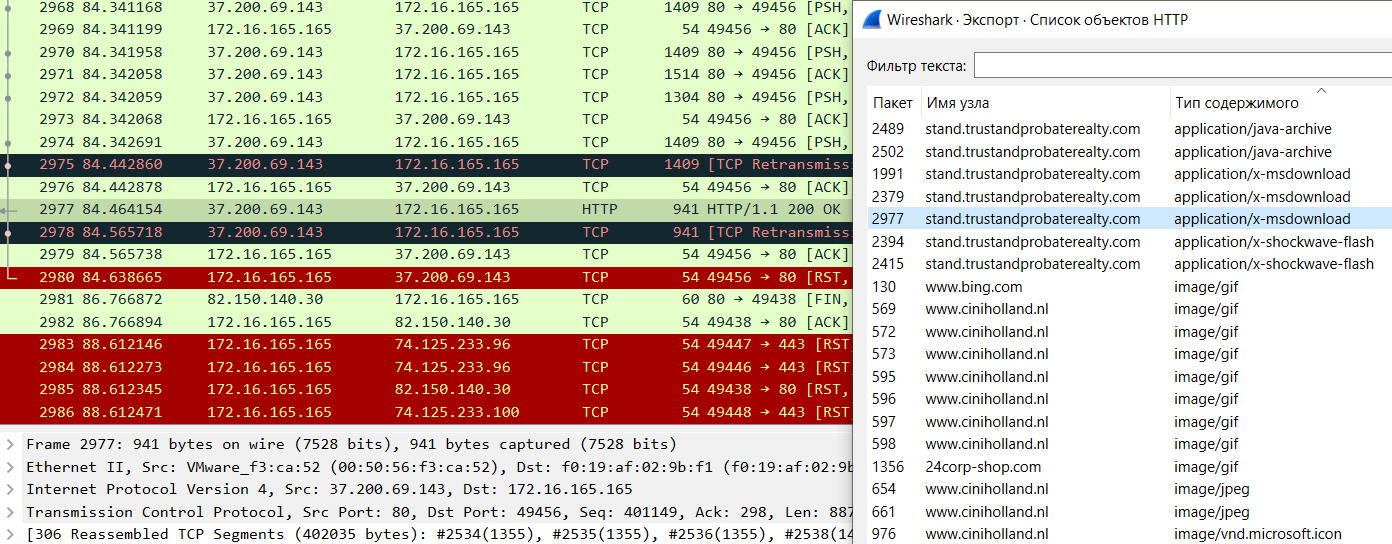


Рисунок 7 «File → Export Objects → HTTP и вывод в Wireshark IP адреса»

## Загружались ли пользователем или системой без ведома пользователя файлы, не являющиеся вредоносными?

Да, загружались «мирные» файлы фоном (не вредоносные)

В Wireshark откроем File → Export Objects → HTTP**.**

* IMG-20130928-WA002-150x150.jpg
* newsletter\_on.gif
* P1260499-200x298.jpg
* squareorangedecor.gif
* twitter\_on.gif
* youtubelogo\_on.gif
* и скрипты JS

Эти объекты загружались **автоматически** для отображения страницы и сбора аналитики; пользователь о них не заботился, и они не несут вредоносного кода

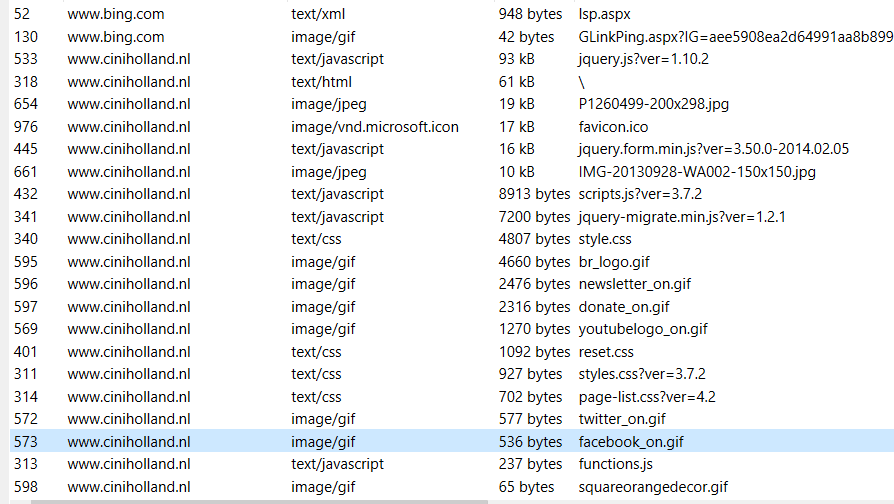


Рисунок 8 «File → Export Objects → HTTP»

## Какие сайты (доменные имена) задействованы в заражении пользователя вредоносным программным обеспечением (имеют следы вредоносной активности, участвуют во вредоносных действиях)?

Собираем цепочку по полю **Referer**:

www.ciniholland.nl

**24corp-shop.com**

**stand.trustandprobaterealty.com**

adultbiz.in есть в DNS, но HTTP-трафика не было, значит не задействован.

## Каков механизм переходов (перенаправлений) пользователя с посещенных сайтов на сайт, с которого было загружено вредоносное программное обеспечение?

Пользователь открыл www.ciniholland.nl из поиска Bing. Страница незаметно вставила iframe на 24corp-shop.com, который вернул HTTP 302 на stand.trustandprobaterealty.com. Последний отдал несколько файлов, среди которых находилось вредоносное ПО (Exploit:JS/Meadgive.P, Trojan:Win32/Ceevee, Exploit:Java/CVE-2012-0507).

|  |  |  |
| --- | --- | --- |
| **Переход** | **Техника** | **Как видно в пакете** |
| *ciniholland* → 24corp | Iframe | в HTML ответа www.ciniholland.nl - строка <iframe src="http://24corp-shop.com/"> |
| 24corp → stand.trustandprobaterealty | HTTP 302 | ответ HTTP/1.1 302 Found с Location: http://stand.trustandprobaterealty.com/... |
| stand.trustandprobaterealty → payload | многократные GET (…req=jar, …req=swf, …req=mp3) | обычные HTTP 200 и скачивание бинарей |