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».

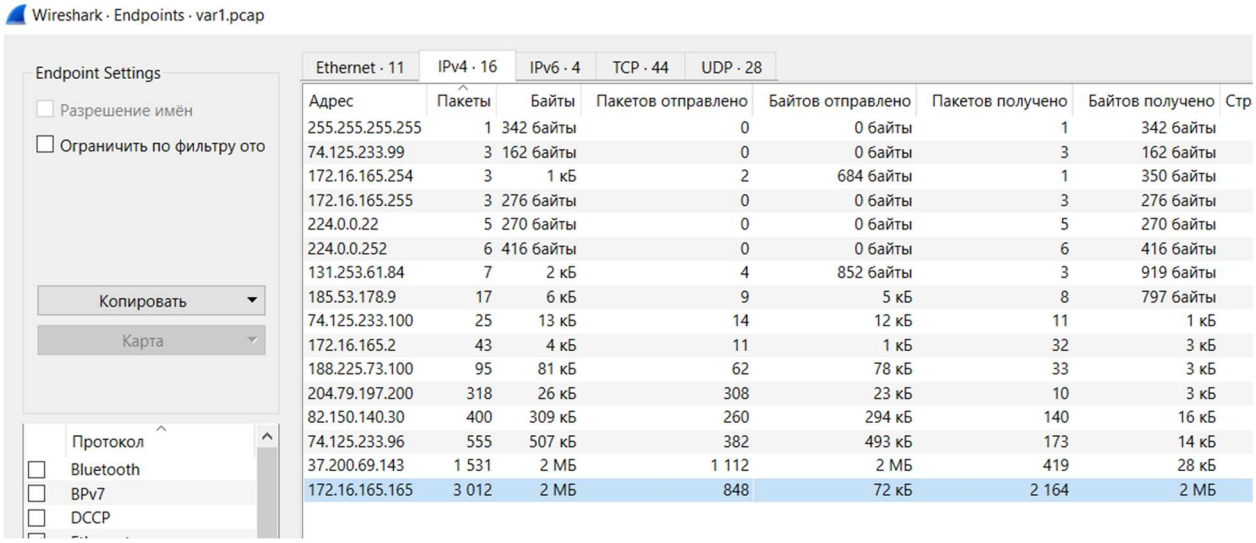
1. Каков IP-адрес зараженного узла?
2. Каков MAC-адрес зараженного узла?
3. Каково доменное имя зараженного узла?
4. Какие сайты посетил пользователь зараженного устройства по своему желанию?
5. Посещение каких сайтов зафиксировано в сетевом трафике?
6. Каково доменное имя сайта, с которого произошла 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

1. Каков IP-адрес зараженного узла?

Statistics → Endpoints → IPv4 → сортировка по Packets

Абсолютный лидер среди внутренних адресов — 172.16.165.165



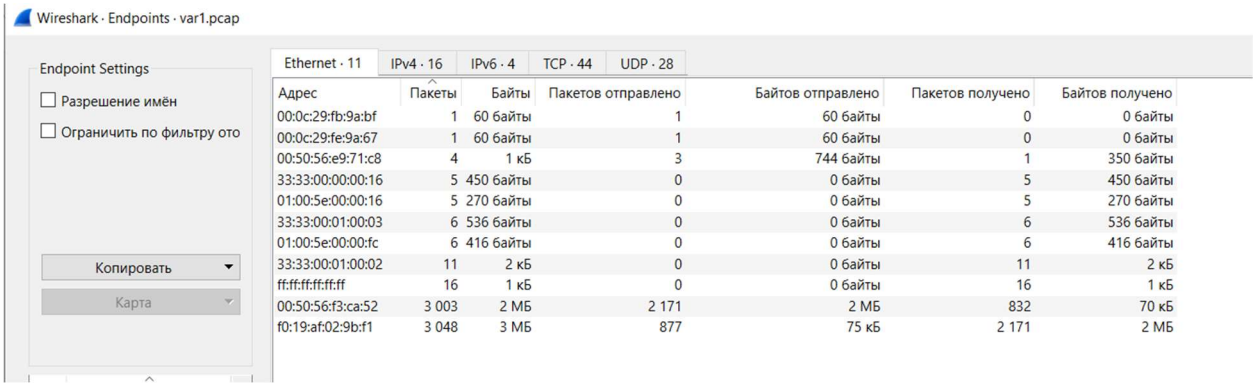
Адрес	Пакеты	Байты	Пакетов отправлено	Байтов отправлено	Пакетов получено	Байтов получено	Стр
255.255.255.255	1	342 байты	0	0 байты	1	342 байты	
74.125.233.99	3	162 байты	0	0 байты	3	162 байты	
172.16.165.254	3	1 кБ	2	684 байты	1	350 байты	
172.16.165.255	3	276 байты	0	0 байты	3	276 байты	
224.0.0.22	5	270 байты	0	0 байты	5	270 байты	
224.0.0.252	6	416 байты	0	0 байты	6	416 байты	
131.253.61.84	7	2 кБ	4	852 байты	3	919 байты	
185.53.178.9	17	6 кБ	9	5 кБ	8	797 байты	
74.125.233.100	25	13 кБ	14	12 кБ	11	1 кБ	
172.16.165.2	43	4 кБ	11	1 кБ	32	3 кБ	
188.225.73.100	95	81 кБ	62	78 кБ	33	3 кБ	
204.79.197.200	318	26 кБ	308	23 кБ	10	3 кБ	
82.150.140.30	400	309 кБ	260	294 кБ	140	16 кБ	
74.125.233.96	555	507 кБ	382	493 кБ	173	14 кБ	
37.200.69.143	1 531	2 МБ	1 112	2 МБ	419	28 кБ	
172.16.165.165	3 012	2 МБ	848	72 кБ	2 164	2 МБ	

Рисунок 1 «сортировка IP по Packets»

2. 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).



Адрес	Пакеты	Байты	Пакетов отправлено	Байтов отправлено	Пакетов получено	Байтов получено
00:0c:29:fb:9a:bf	1	60 байты	1	60 байты	0	0 байты
00:0c:29:fe:9a:67	1	60 байты	1	60 байты	0	0 байты
00:50:56:e9:71:c8	4	1 кБ	3	744 байты	1	350 байты
33:33:00:00:00:16	5	450 байты	0	0 байты	5	450 байты
01:00:5e:00:00:16	5	270 байты	0	0 байты	5	270 байты
33:33:00:01:00:03	6	536 байты	0	0 байты	6	536 байты
01:00:5e:00:00:fc	6	416 байты	0	0 байты	6	416 байты
33:33:00:01:00:02	11	2 кБ	0	0 байты	11	2 кБ
ff:ff:ff:ff:ff:ff	16	1 кБ	0	0 байты	16	1 кБ
00:50:56:f3:ca:52	3 003	2 МБ	2 171	2 МБ	832	70 кБ
f0:19:af:02:9b:f1	3 048	3 МБ	877	75 кБ	2 171	2 МБ

Рисунок 2 «сортировка Ethernet по Packets»

3. 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»).

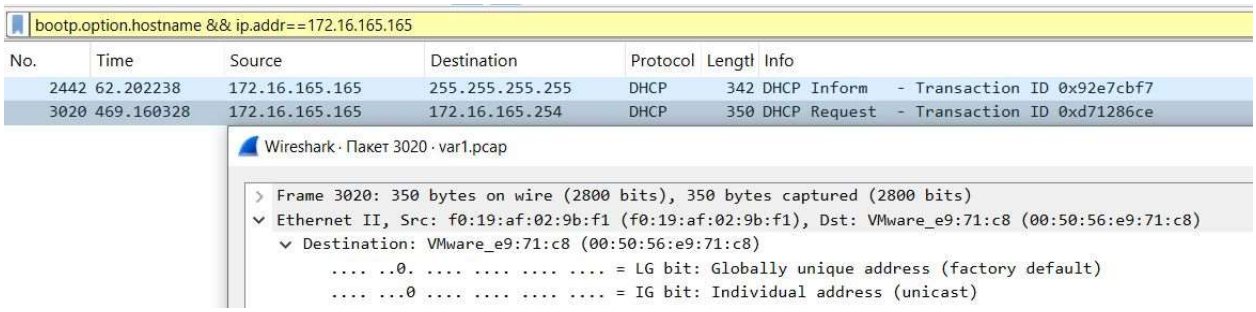


Рисунок 3 «bootp.option.hostname && ip.addr==172.16.165.165»

4. 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))

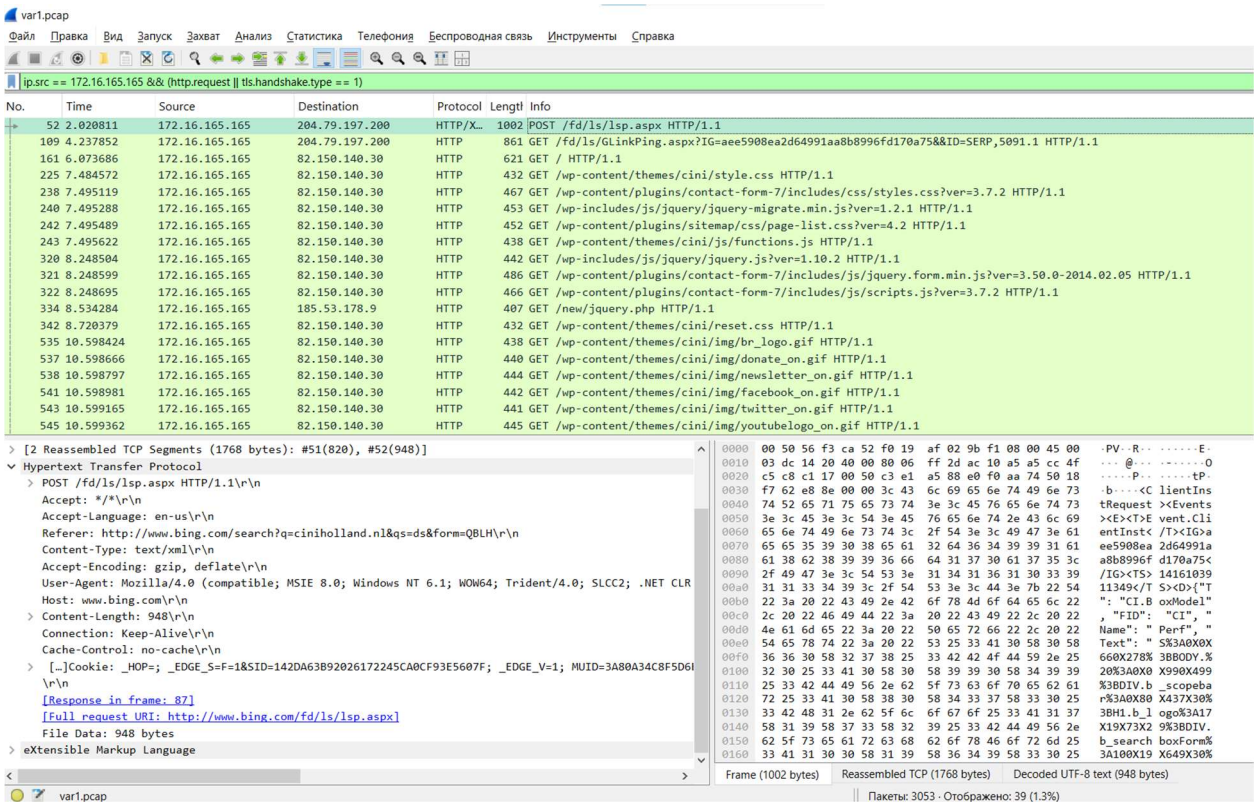


Рисунок 4 «ip.src == 172.16.165.165 && (http.request || tls.handshake.type == 1)»

Ответ (пользователь зараженного устройства посетил по своему желанию):

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

5. 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/…`)

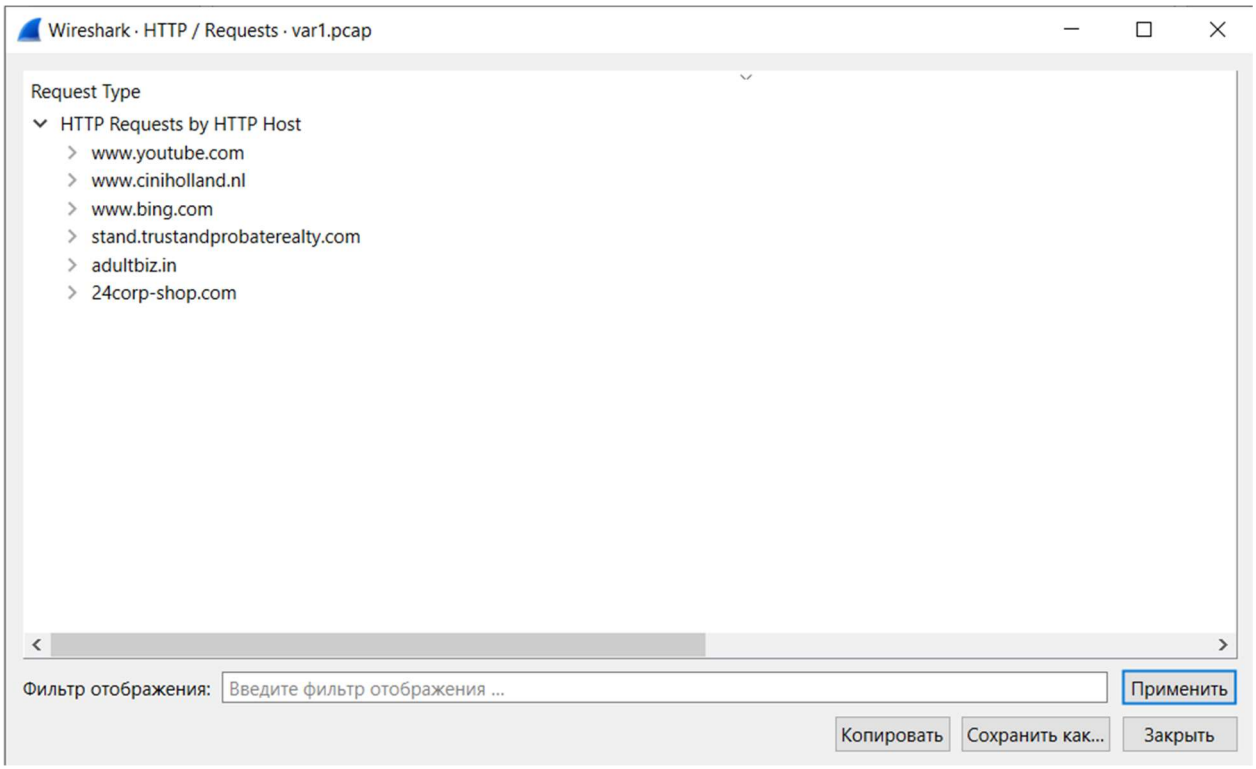


Рисунок 5 «Statistics → HTTP → Requests»

6. 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:

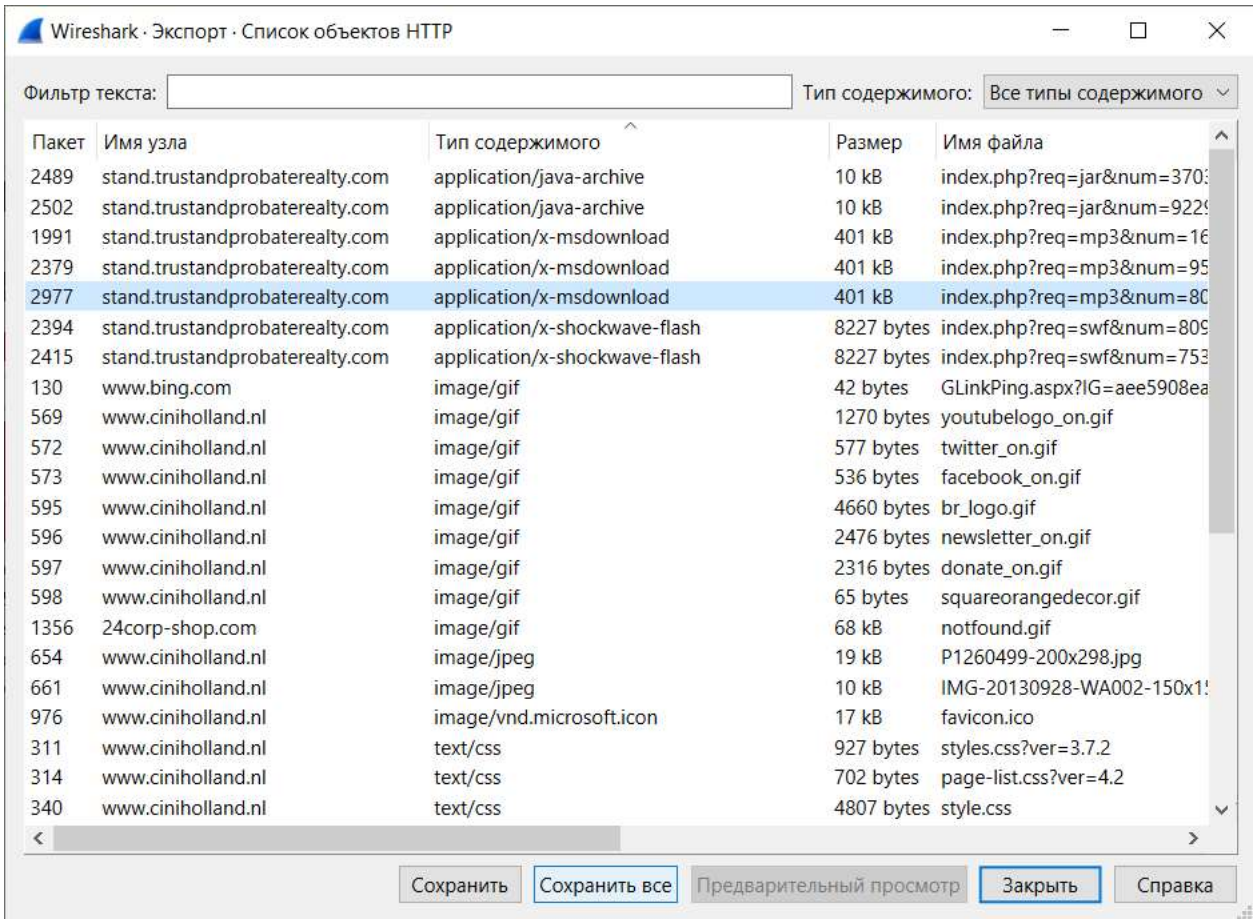


Рисунок 6 «File → Export Objects → HTTP»

7. 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

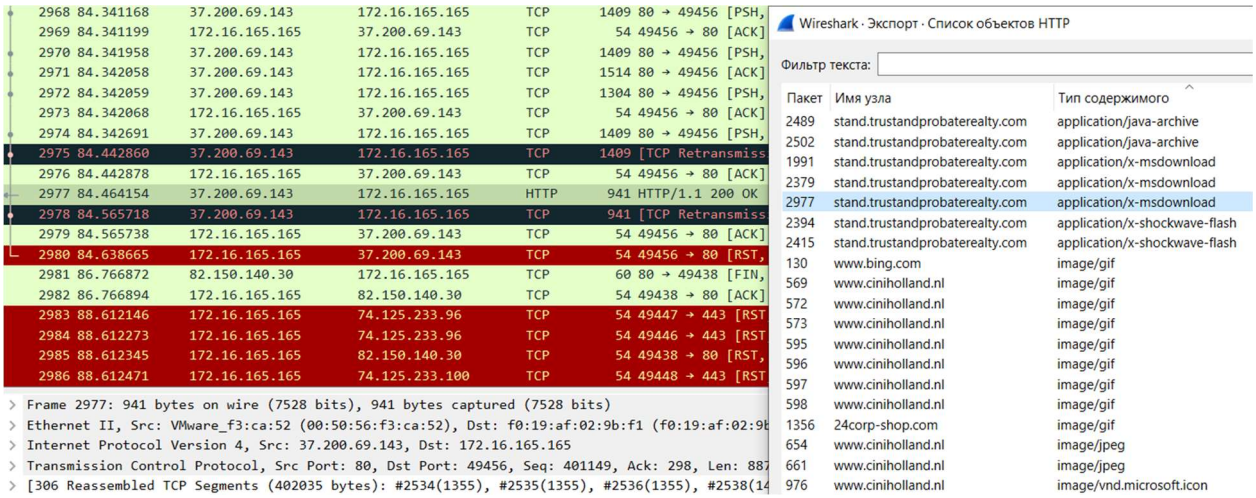


Рисунок 7 «File → Export Objects → HTTP и вывод в Wireshark IP адреса»

8. 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

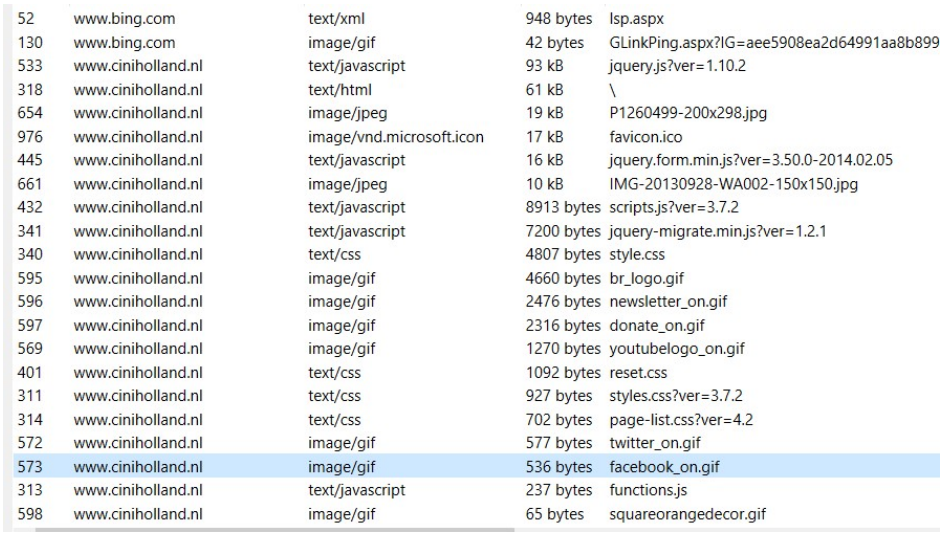


Рисунок 8 «File → Export Objects → HTTP»

9. 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.

10. 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