

< Teach
Me
Skills />

Incident response

Часть 2

Вопросы по предыдущим темам или ДЗ

Mini-quize по прошлым темам:

1. Какое ПО вы бы использовали для получения информации о файле?
2. Для чего необходим регламент реагирования?
3. Как представлен реестр в ос windows?
4. Хранит ли ОС информацию о процессах, подключениях, в течении какого-то времени?
5. Какую информацию, по вашему мнению, мы можем получить из снимка ОС?

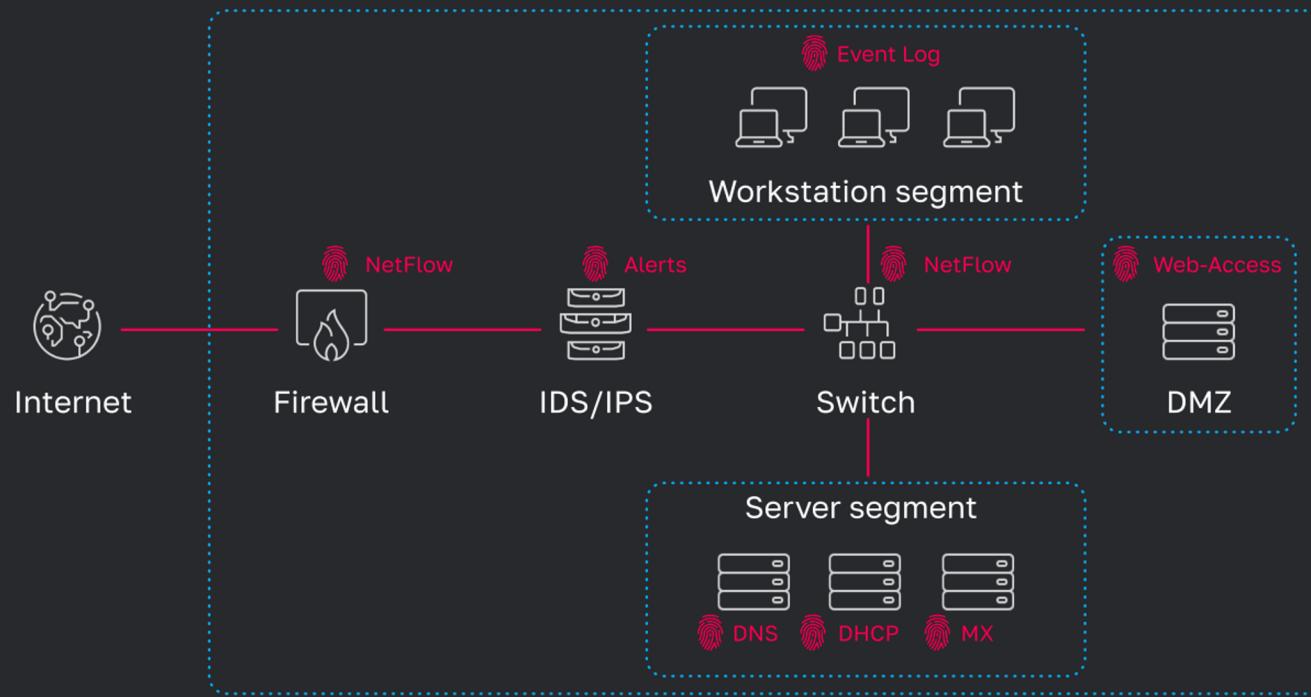
Mini-quize по новой теме:

1. Что такое дамп памяти?
2. Какую информацию мы можем из него извлечь?
3. Можем ли мы проанализировать сетевые подключения?
4. Как мы можем сделать дамп сетевого трафика?

План занятия

1. Рассмотрим на практике расследование инцидентов информационной безопасности
2. Познакомимся с инструментарием для проведения расследования
3. Потренируемся в форензике

Источники цифровых улик



Источники криминалистических улик

Сетевой трафик

- Сбор на уровне хоста
- Сбор с сетевых устройств в локальной сети
- Сбор на периметре/магистральный трафик

Журналы

- DNS, DHCP
- Журналы почтового сервера
- Журналы прокси сервера
- Журналы веб-сервера, веб-приложений
- Журналы IDS, IPS систем
- Netflow
- Журналы сетевого оборудования (syslog)
- Журналы рабочих станций

Захват сетевого трафика

На периметре



Сетевое
оборудование ЛВС

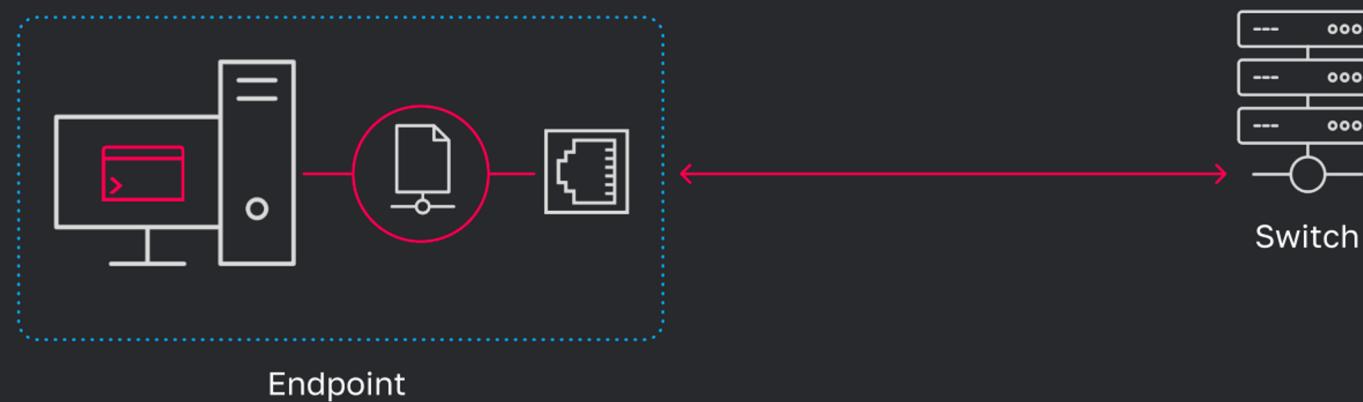


На уровне хоста

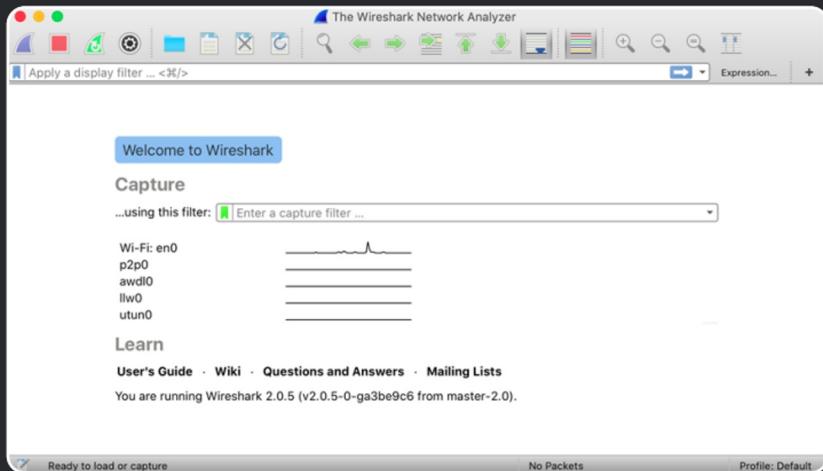


Утилиты для захвата трафика

- Cross-platform (Wireshark, Tshark)
- *nix (tcpdump)
- Windows (netsh)



Утилиты для захвата трафика



wireshark

```
bash
As-MacBook-Air:~ tyvision$ tshark --help
TShark (Wireshark) 2.0.5 (v2.0.5-0-ga3be9c6 from master-2.0)
Dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: tshark [options] ...

Capture interface:
-i <interface>          name or idx of interface (def: first non-loopback)
-f <capture filter>      packet filter in libpcap filter syntax
-s <snaplen>             packet snapshot length (def: 65535)
-p                         don't capture in promiscuous mode
-I                         capture in monitor mode, if available
-B <buffer size>         size of kernel buffer (def: 2MB)
-y <link type>           link layer type (def: first appropriate)
-D                         print list of interfaces and exit
-L                         print list of link-layer types of iface and exit

Capture stop conditions:
-c <packet count>        stop after n packets (def: infinite)
-a <autostop cond.> ...  duration:NUM - stop after NUM seconds
                           filesize:NUM - stop this file after NUM KB
                           files:NUM - stop after NUM files
```

tshark

Утилиты для захвата трафика

bash

```
As-MacBook-Air:~ tyvision$ tcpdump --help
tcpdump version tcpdump version 4.9.3 -- Apple version 90.100.1
libpcap version 1.9.1
LibreSSL 2.8.3
Usage: tcpdump [-aAbdDefhHIJKllNnNOpqStuUvxX#] [ -B size ] [ -c count ]
           [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
           [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
           [ -Q inlout|inout ]
           [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
           [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
           [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
           [ -g ] [ -k ] [ -o ] [ -P ] [ -Q meta-data-expression]
           [ --apple-tzo offset] [--apple-truncate]
           [ -Z user ] [ expression ]
```

tcpdump

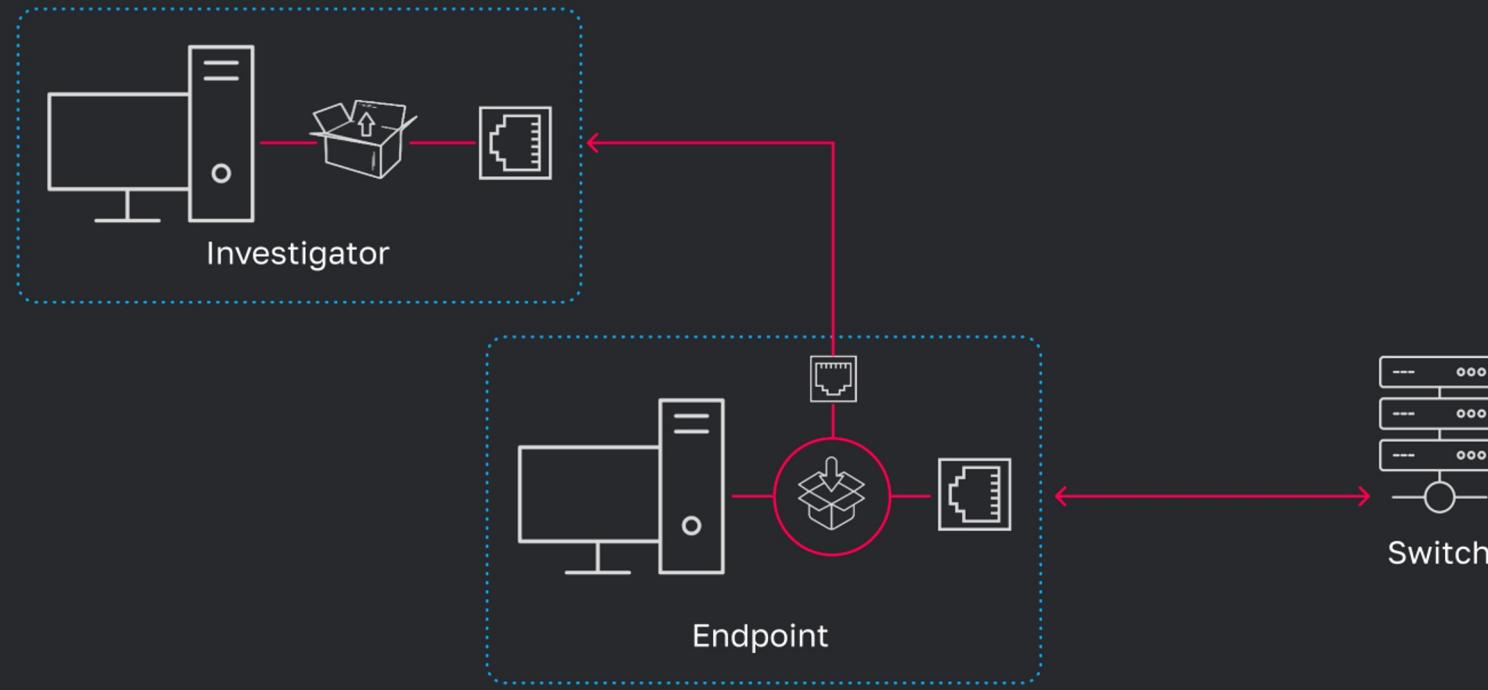


Windows PowerShell

```
PS C:\Users\tyvision> netsh
netsh>trace
netsh trace>
```

netsh

Удалённый захват трафика с хоста



Что искать?

Сетевые индикаторы

- IP-адреса
- Сетевые порты
- Сетевые протоколы
- Доменные имена

Артефакты в сетевом трафике

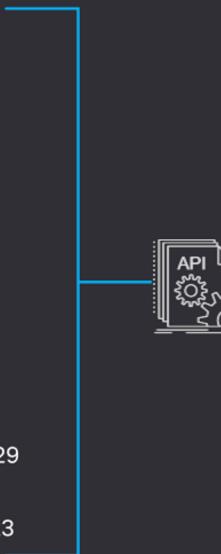
- SSL/TLS-сертификаты
- Передаваемые файлы

Как искать?

IPs
101.10.50.4
84.90.111.8
...
8.8.8.88

Domains
go0gle.com
google.com
...
facebook.com

Certificates
f32a898bc4235e9090d7429
...
f484aa8ce4725c962bb4123



The screenshot shows a threat intelligence report for the IP address 81.98.112.39. The top section displays basic information: 'No interesting sightings for this IP address', the IP address itself, and its ASN details ('AS 5089 | Virgin Media Limited'). Below this are tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY'. The 'DETECTION' tab lists several security products with 'Clean' status: 'ADMINUS Labs', 'AlienVault', 'AutoShun', and 'BADCWARE-INFO'. The 'DETAILS' tab shows the IP's location as 'London, United Kingdom'. The 'COMMUNITY' tab lists various organizations with 'Clean' status: 'AngloLab WebGuard', 'Anti-AVL', 'Avira (no cloud)', and 'Baidu-International'.

HTTP

Методы запроса

Основные:

GET, POST

Опциональные:

OPTIONS, PUT, DELETE, HEAD, TRACE, CONNECT

Строка запроса

В строке запроса также могут передаваться параметры, например:

```
1 | GET /wp-content/secure/online/thrust?auth=true&isadmin=false HTTP 1.1\r\n
```

HTTP

- **Cookie:** индекс обращения к уникальным пользовательским данным, собираемым на стороне веб-сервера (веб-приложения)
- **Accept:** предпочтаемый клиентом тип контента: text/html, application/xml+xhtml, application/xml. Смежные заголовки: Accept-Language, Accept-Encoding
- **User Agent:** <https://developers.whatismybrowser.com/useragents/explore/>
- **Authentication:** <type> -- Basic/Digest/etc – способ авторизации на HTTP-сервере
- **Referer URI:** содержит URI-адрес ресурса, с которого клиент был перенаправлен на конкретную страницу
- **X-* (X-Forwarded-For):** этот заголовок добавляется на случай reverse proxy
- **Proxy-Authorization:** <type> -- Basic/Digest/etc – способ авторизации на прокси-сервере

Пример запроса HTTP

Time	Source	Destination	Protocol	Length	Info
613 42.015401	10.2.20.101	3.121.44.244	HTTP	359	GET /wp-content/secure/online/thrust/list/aWAmxiXqfMwfMQ70EnPOc HTTP/1.1

Frame 613: 359 bytes on wire (2872 bits), 359 bytes captured (2872 bits)
Ethernet II, Src: Hewlett_P_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: 10.2.20.101, Dst: 3.121.44.244
Transmission Control Protocol, Src Port: 49195, Dst Port: 80, Seq: 1, Ack: 1, Len: 305

Hypertext Transfer Protocol

```
> GET /wp-content/secure/online/thrust/list/aWAmxiXqfMwfMQ70EnPOc HTTP/1.1\r\nAccept: text/html, application/xhtml+xml, */*\r\nAccept-Language: en-US\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\nAccept-Encoding: gzip, deflate\r\nHost: 3.121.44.244\r\nConnection: Keep-Alive\r\n\r\n[Full request URI: http://3.121.44.244/wp-content/secure/online/thrust/list/aWAmxiXqfMwfMQ70EnPOc]\n[HTTP request 1/2]\n[Response in frame: 615]\n[Next request in frame: 617]
```

Коды ответа HTTP

1xx – continue

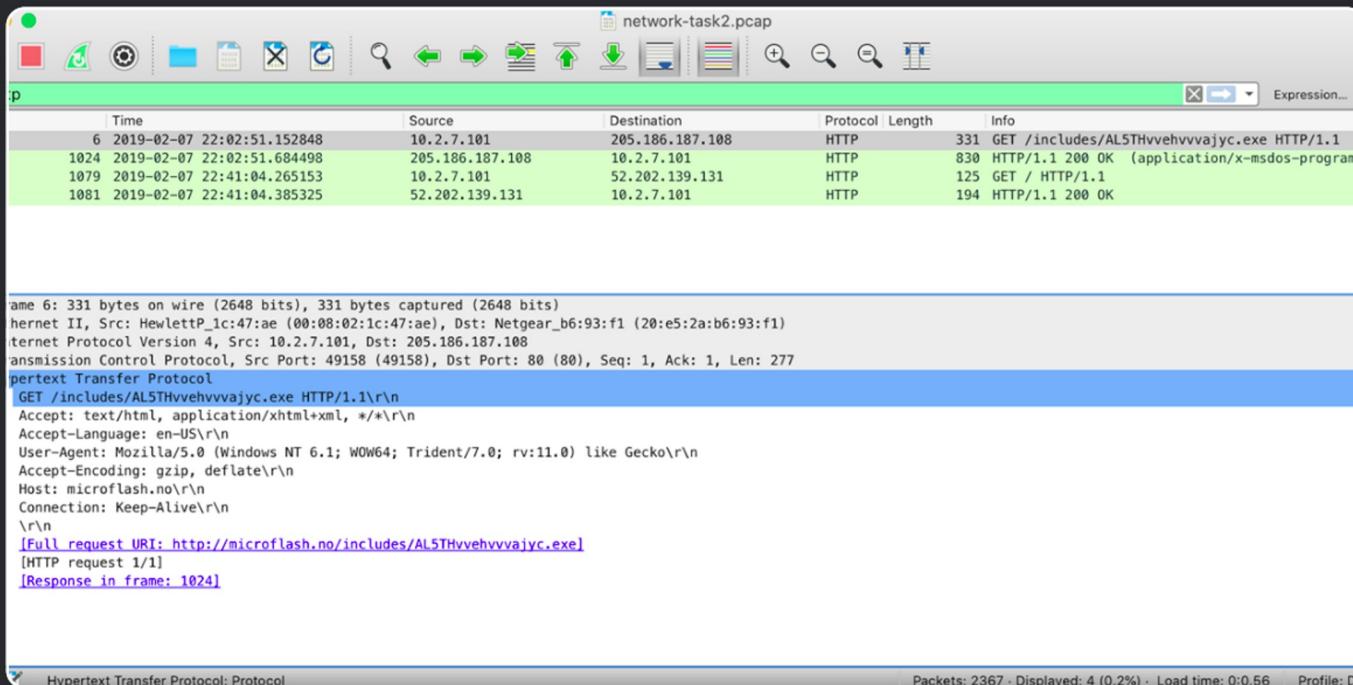
2xx – OK codes

3xx – redirection & objects

4xx – client-side errors

5xx – server-side errors

Просмотр всех пакетов HTTP



Просмотр всех пакетов HTTP

network-task2.pcap

p.request

Time	Source	Destination	Protocol	Length	Info
6 2019-02-07 22:02:51.152848	10.2.7.101	205.186.187.108	HTTP	331	GET /includes/AL5THvvehvvajyc.exe HTTP/1.1
1079 2019-02-07 22:41:04.265153	10.2.7.101	52.202.139.131	HTTP	125	GET / HTTP/1.1

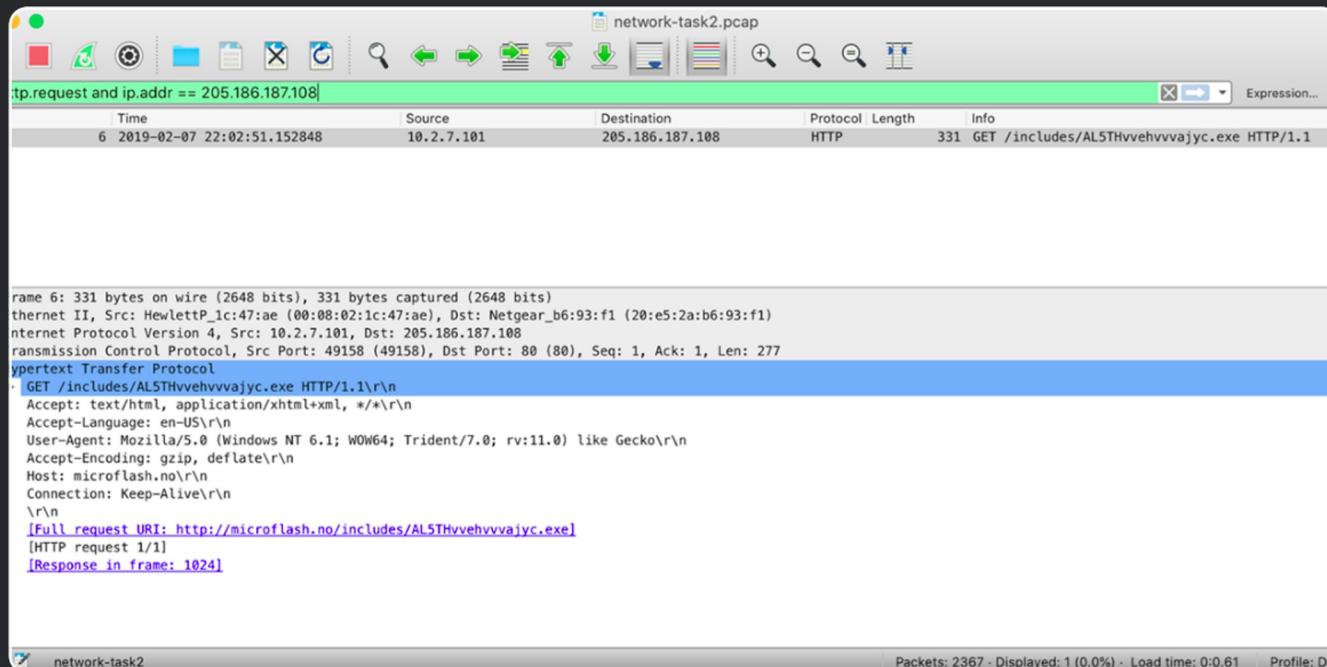
ame 6: 331 bytes on wire (2648 bits), 331 bytes captured (2648 bits)
ernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
ternet Protocol Version 4, Src: 10.2.7.101, Dst: 205.186.187.108
transmission Control Protocol, Src Port: 49158 (49158), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 277
pertext Transfer Protocol
GET /includes/AL5THvvehvvajyc.exe HTTP/1.1\r\nAccept: text/html, application/xhtml+xml, */*\r\nAccept-Language: en-US\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\nAccept-Encoding: gzip, deflate\r\nHost: microflash.no\r\nConnection: Keep-Alive\r\n\r\n[Full request URI: http://microflash.no/includes/AL5THvvehvvajyc.exe]
[HTTP request 1/1]
[Response in frame: 1024]

HTTP Accept Language (http.accept_language), 24 bytes

Packets: 2367 - Displayed: 2 (0.1%) - Load time: 0:0.33 Profile: De

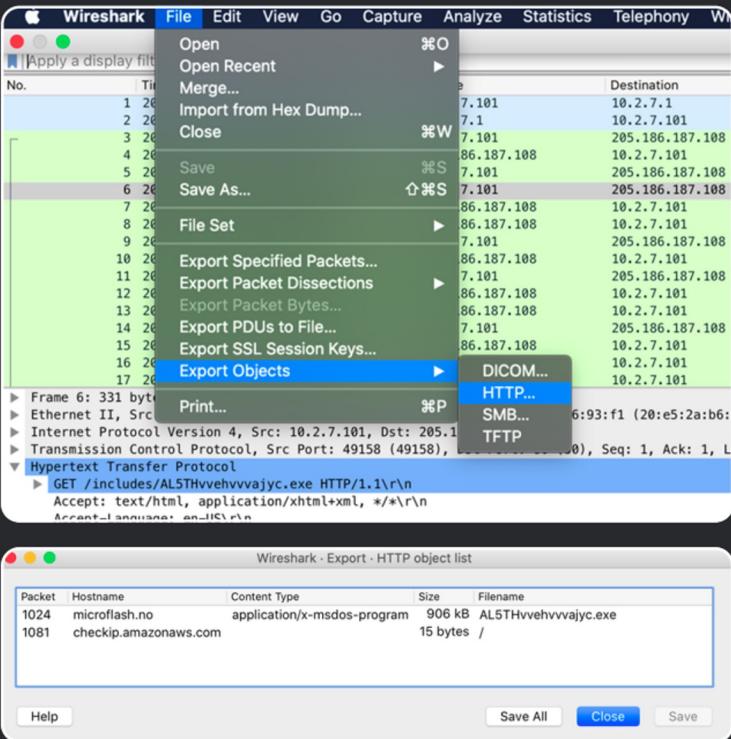
http.request or http.request.method == GET

HTTP-запросы на определённый IP-адрес

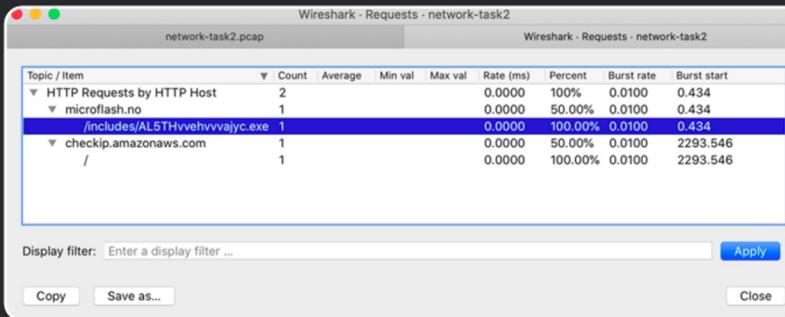
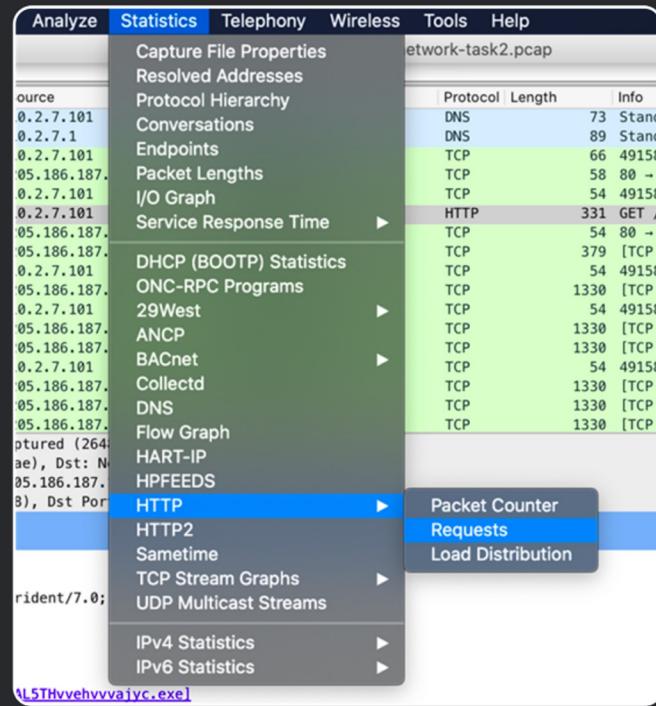


http.request and ip.addr == 205.186.187.108

Экспорт объектов, переданных по HTTP



Полезные фичи (1)



Получение статистики по исследуемому дампу (HTTP-запросы)

Полезные фичи (2)

The screenshot shows the NetworkMiner interface with the 'Endpoints' section selected in the left sidebar. The main pane contains two tables of network traffic statistics.

Top Table (Selected):

Ethernet - 2 IPv4 - 5 IPv6 TCP - 23 UDP - 9									
Address	A	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Latitude	Longitude
10.2.7.1		16	1552	8	918	8	634	—	—
10.2.7.101		2,367	1784 k	946	798 k	1421	986 k	—	—
52.202.139.131		11	821	5	414	6	407	—	—
89.46.222.42		1,312	819 k	687	38 k	625	780 k	—	—
205.186.187.108		1,028	963 k	721	946 k	307	16 k	—	—

Bottom Table:

Ethernet - 2 IPv4 - 5 IPv6 TCP - 23 UDP - 9										
Address	A	Port	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Latitude	Longitude
10.2.7.101		49158	1,028	963 k	307	16 k	721	946 k	—	—
10.2.7.101		49163	36	2384	15	971	21	1413	—	—
10.2.7.101		49164	9	1058	5	838	4	220	—	—
10.2.7.101		49165	11	821	6	407	5	414	—	—
10.2.7.101		49168	36	2381	15	968	21	1413	—	—
10.2.7.101		49169	219	160 k	106	154 k	113	6106	—	—
10.2.7.101		49170	36	2381	15	968	21	1413	—	—
10.2.7.101		49171	217	160 k	106	154 k	111	5998	—	—
10.2.7.101		49172	36	2382	15	968	21	1414	—	—
10.2.7.101		49173	216	160 k	106	154 k	110	5944	—	—
10.2.7.101		49174	36	2381	15	968	21	1413	—	—
10.2.7.101		49175	218	160 k	106	154 k	112	6052	—	—
10.2.7.101		49176	36	2382	15	968	21	1414	—	—
10.2.7.101		49177	217	160 k	106	154 k	111	5998	—	—
52.202.139.131		80	11	821	5	414	6	407	—	—
89.46.222.42		21	216	14 k	126	8480	90	5811	—	—
89.46.222.42		12043	9	1058	4	220	5	838	—	—
89.46.222.42		12050	219	160 k	113	6106	106	154 k	—	—
89.46.222.42		12087	217	160 k	111	5998	106	154 k	—	—
89.46.222.42		12028	216	160 k	110	5944	106	154 k	—	—
89.46.222.42		12049	218	160 k	112	6052	106	154 k	—	—
89.46.222.42		12002	217	160 k	111	5998	106	154 k	—	—
205.186.187.108		80	1,028	963 k	721	946 k	307	16 k	—	—

Получение статистики по исследуемому дампу – сведения об объёме трафика для конечных узлов

Volatility framework

Volatility – это набор Python-инструментов для извлечения цифровых артефактов из энергонезависимой памяти RAM

Поддерживаемые форматы снимков:

- Raw (dd)
- Hibernation file (для Windows 7 и менее)
- Crash dump file
- VirtualBox ELF64 core dump
- VMware saved state and snapshot files
- EWF format (E01)
- LiME format
- Mach-O file format
- QEMU virtual machine dumps
- Firewire
- HPAK (FDPro)



Основные модули:

imageinfo
pslist
procdump
memdump
handles
dlls
cmdline

volatilityfoundation.org

[github](https://github.com/volatilityfoundation/volatility)

Спасибо за внимание!