

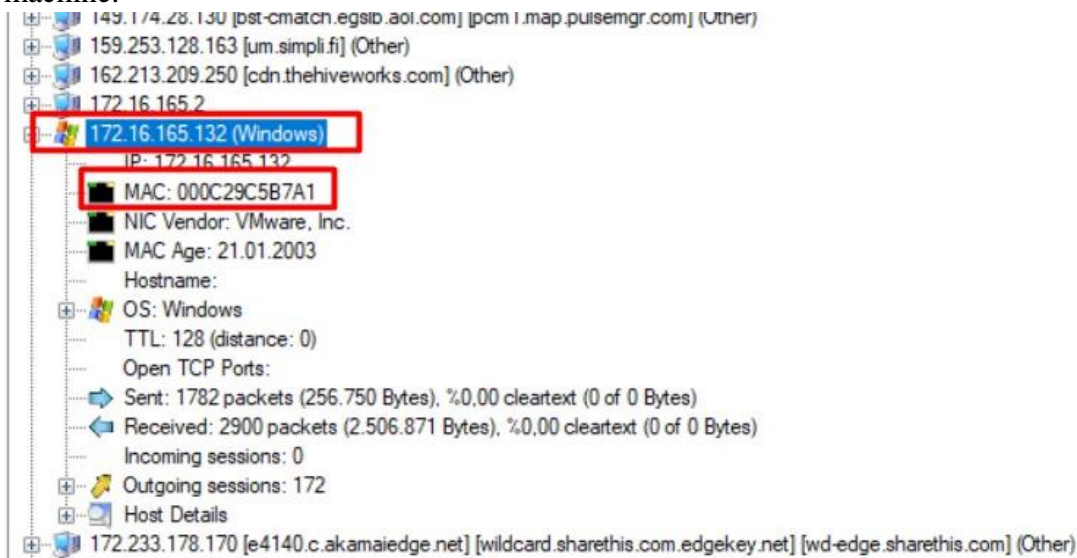
'Malware Traffic Analysis 2' challenge at cyberdefenders.org

Tools used for this challenge:

- NetworkMiner
- Wireshark
- VirusTotal
- PacketTotal
- Brim

Q.1) What is the IP address of the Windows VM that gets infected?

I load the pcap file to Networkminer and we can see the information about infected Windows machine.



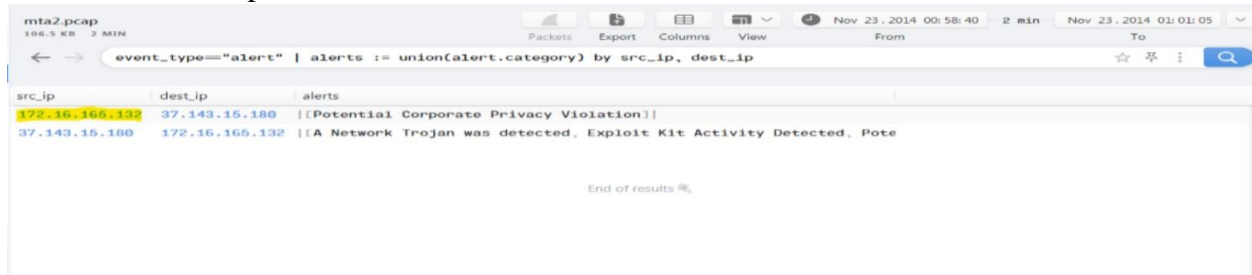
Answer :172.16.165.132

Q.2) What is the MAC address of the infected VM?

We can the answer in the previous picture. We get the MAC address of the infected VM as 00:0c:29:c5:b7:a1.

Q.3) What are the IP address and port number that delivered the exploit kit and malware?

When we look at the alerts in Brim we can see the Ip address that matches our infected host and Ip address of the compromised website.



The screenshot shows the Brim interface with a search query `event_type="alert" | alerts := union(alert.category) by src_ip, dest_ip`. The results table has three columns: `src_ip`, `dest_ip`, and `alerts`. Two rows are visible:

src_ip	dest_ip	alerts
172.16.166.132	37.143.15.180	[[Potential Corporate Privacy Violation]]
37.143.15.180	172.16.166.132	[[A Network Trojan was detected, Exploit Kit Activity Detected, Pote

And when I check the IP in Networkminer I can see the port number.



The screenshot shows the Networkminer interface with details for IP 37.143.15.180. The IP is associated with `g.trinketking.com` and `h.trinketking.com`. The details include:

- IP: 37.143.15.180
- MAC: 005056F3CA52
- NIC Vendor: VMware, Inc.
- MAC Age: 4 01 2000
- Hostname: g.trinketking.com, h.trinketking.com
- OS: Other
- TTL: 128 (distance: 0)
- Open TCP Ports: 51439
- Sent: 322 packets (422.382 Bytes), %0,00 cleartext (0 of 0 Bytes)
- Received: 125 packets (5.947 Bytes), %0,00 cleartext (0 of 0 Bytes)
- Incoming sessions: 2
- Outgoing sessions: 0

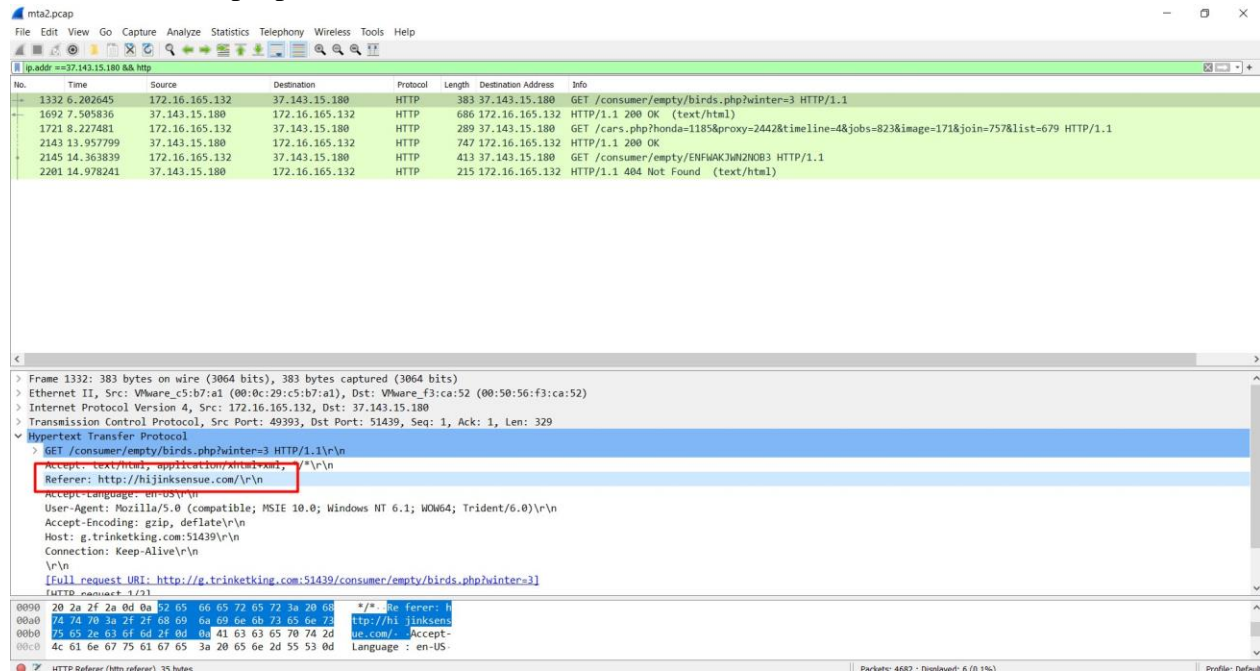
Answer : 37.143.15.180:51439

Q.4) What are the two FQDN's that delivered the exploit kit? comma-separated in alphabetical order.

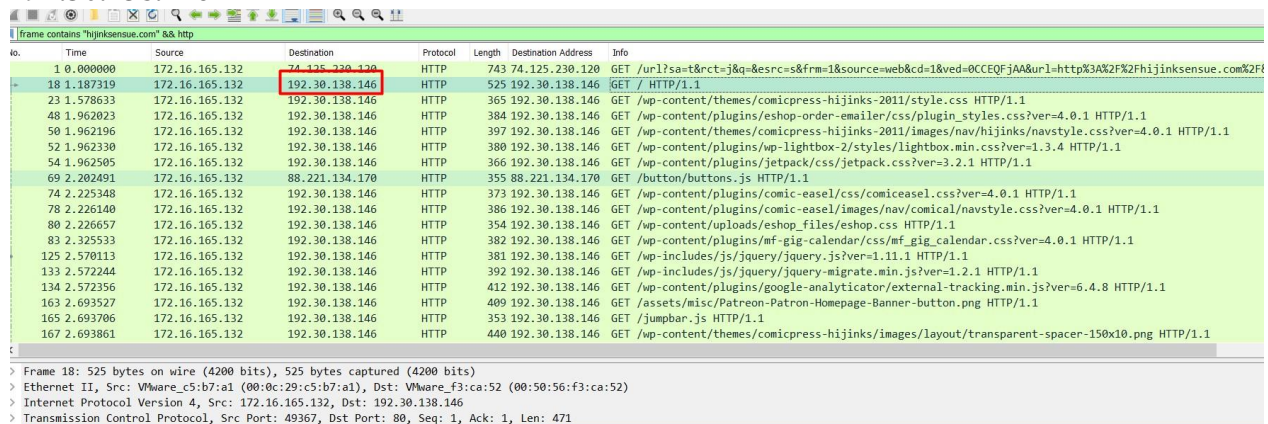
From the above Networkminer result, we also get the two FQDN that delivered the exploit kit.
g.trinketking.com,h.trinketking.com

Q.5) What is the IP address of the compromised web site?

When I filter the pcap in Wireshark I can see the referrer website.



I get the name of the referrer website and when I filter the name I get the IP address which is **192.30.138.146**



Q.6) What is the FQDN of the compromised website?

From previous question, we found the FQDN of the compromised website as **hijinksensue.com**.

Q.7) What is the name exploit kit (EK) that delivered the malware? (two words)

I upload the pcap file to <http://packettotal.com>. We can see a name multiple times which is our answer. **“Sweet Orange”**.

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol
2014-11-23 00:58:46 Z	A Network Trojan was detected	ET CURRENT_EVENTS Sweet Orange CDN Gate Sept 09 2014 Method 2	1	172.16.165.132	49388	58-87-149-98	80	TCP
2014-11-23 00:58:47 Z	A Network Trojan was detected	ET CURRENT_EVENTS Sweet Orange Landing Nov 04 2013	1	37-143-15-188	51439	172.16.165.132	49393	TCP
2014-11-23 00:58:49 Z	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP	1	37-143-15-188	51439	172.16.165.132	49398	TCP
2014-11-23 00:58:55 Z	Potential Corporate Privacy Violation	ET POLICY Outdated Windows Flash Version IE	1	172.16.165.132	49393	37-143-15-188	51439	TCP
2014-11-23 00:59:51 Z	A Network Trojan was detected	ET CURRENT_EVENTS Possible Sweet Orange redirection Nov 4 2014	1	58-87-149-98	80	172.16.165.132	49388	TCP

Q.8) What is the redirect URL that points to the exploit kit landing page?

When we look again to the packettotal analysis we can see the host name of the website.

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname
2014-11-23 00:58:46 Z	A Network Trojan was detected	ET CURRENT_EVENTS Sweet Orange CDN Gate Sept 09 2014 Method 2	1	172.16.165.132	49388	58-87-149-98	80	TCP	static.charlotteretirementcommunities.com
2014-11-23 00:58:47 Z	A Network Trojan was detected	ET CURRENT_EVENTS Sweet Orange Landing Nov 04 2013	1	37-143-15-188	51439	172.16.165.132	49393	TCP	g.trinketking.com
2014-11-23 00:58:49 Z	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP	1	37-143-15-188	51439	172.16.165.132	49398	TCP	h.trinketking.com
2014-11-23 00:58:55 Z	Potential Corporate Privacy Violation	ET POLICY Outdated Windows Flash Version IE	1	172.16.165.132	49393	37-143-15-188	51439	TCP	g.trinketking.com
2014-11-23 00:59:51 Z	A Network Trojan was detected	ET CURRENT_EVENTS Possible Sweet Orange redirection Nov 4 2014	1	58-87-149-98	80	172.16.165.132	49388	TCP	static.charlotteretirementcommunities.com

And when I filter the website in Wireshark I can see the redirect URL .

static.charlotteretirementcommunities.com/k?tstmp=3701802802

No.	Time	Source	Destination	Protocol	Length	Destination Address	Info
780	4.710462	172.16.165.132	50.87.149.90	HTTP	382	50.87.149.90	GET /k?tstmp=3701802802 HTTP/1.1


```

<
> Internet Protocol Version 4, Src: 172.16.165.132, Dst: 50.87.149.90
> Transmission Control Protocol, Src Port: 49388, Dst Port: 80, Seq: 1, Ack: 1, Len: 328
> Hypertext Transfer Protocol
  GET /k?tstmp=3701802802 HTTP/1.1\r\n
  Accept: application/javascript, */*;q=0.8\r\n
  Referer: http://hijinksensue.com/\r\n
  Accept-Language: en-US\r\n
  User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: static.charlotteretirementcommunities.com\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://static.charlotteretirementcommunities.com/k?tstmp=3701802802]
  [HTTP request 1/1]
  [Response in frame: 1211]
0080 38 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 8..Refer er: http
0090 38 2f 2f 68 69 6a 69 6e 6b 73 65 6e 73 75 65 74 3///hijin ksensue
00a0 63 6f 6d 2f 0d 0a 41 63 63 65 70 74 2d 4c 61 6e com/.Ac cept-Lan
00b0 67 75 61 67 65 3a 20 65 6e 2d 55 53 0d 0a 55 73 guage: e n-US..Us

```

HTTP Referer (http.referer), 35 bytes

Q.9) What is the IP address of the redirect URL that points to the exploit kit landing page?

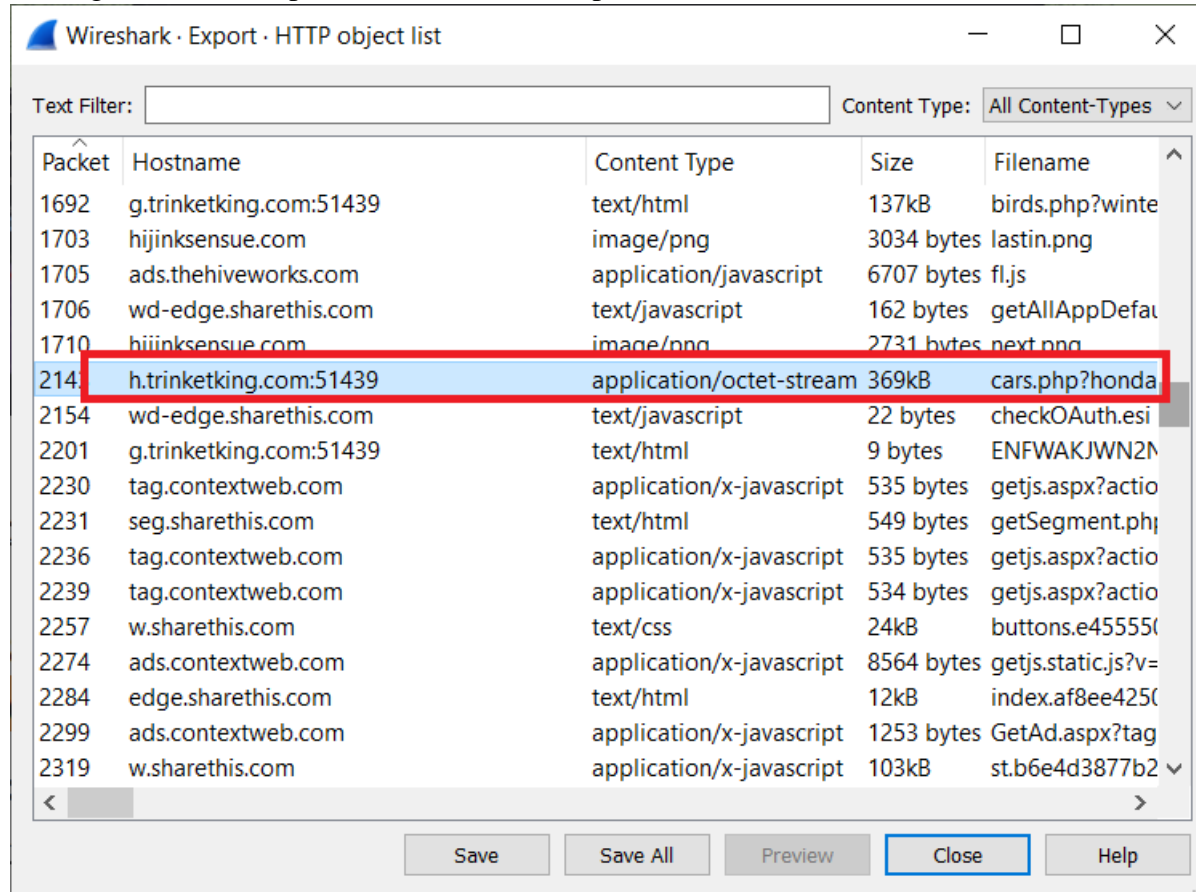
We know the name of the website from previous question, we can just look at the frame and get the IP address.**Answer**

No.	Time	Source	Destination	Protocol	Length	Destination Address	Info
780	4.710462	172.16.165.132	50.87.149.90	HTTP	382	50.87.149.90	GET /k?tstmp=3701802802 HTTP/1.1

Answer : 50.87.149.90

Q10. Extract the malware payload (PE file) from the PCAP. What is the MD5 hash?

In Wireshark, File -> Export Objects -> HTTP, select packet with application/octet-stream coming from our compromised website and upload it to VirusTotal.



I get the MD5 hash : **1408275c2e2c8fe5e83227ba371ac6b3**

Q.11) What is the CVE of the exploited vulnerability?

From a google search, I find out the CVE of exploited vulnerability.

Google search results for "sweet orange cve".

Yaklaşık 398.000 sonuç bulundu (0,54 saniye)

<https://www.mcafee.com/ex...> Bu sayfanın çevirisini yap

Sweet Orange Exploit Kit - Threat Landscape Dashboard

Sweet Orange Exploit Kit, 2017-06-08 ... CVE-2014-0569 · CVE-2013-2424 · CVE-2014-6332 · CVE-2014-0497 · CVE-2013-2471 · CVE-2013-2423 · CVE-2014-0515 ...

<https://www.malware-traffic-analysis.net...> Bu sayfanın çevirisini yap

2014-04-20 - Sweet Orange EK - Malware-Traffic-Analysis.net

20 Nis 2014 — Kafeine has confirmed the Flash exploit in this example is, in fact, CVE-2014-0497. Sweet Orange has 2014-0497 Post upd.better late than ...

<https://www.malware-traffic-analysis.net...> Bu sayfanın çevirisini yap

2015-02-09 - Sweet Orange EK - Malware-Traffic-Analysis.net

9 Şub 2015 — 141.64 port 8085 - ET CURRENT_EVENTS Possible Sweet Orange CVE-2014-6332 Payload Request (sid:2019752); 91.224.141.64 port 8085 - ET ...

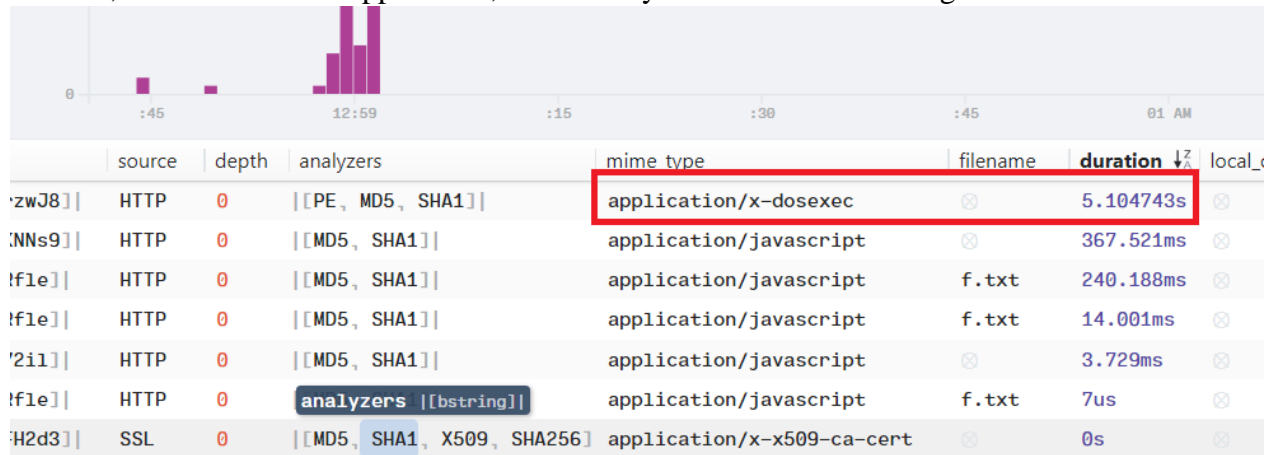
<https://malware.dontneedcoffee.com...> Bu sayfanın çevirisini yap

CVE-2014-6332 (Internet Explorer) and Exploits Kits - Blog

The first encounter was in the Sweet Orange from the actor pushing DarkShell via KR compromised website.

Q12. What is the mime-type of the file that took the longest time (duration) to be analyzed using Zeek?

In Brim, when I filter files application, then sort by duration I can see longest one.



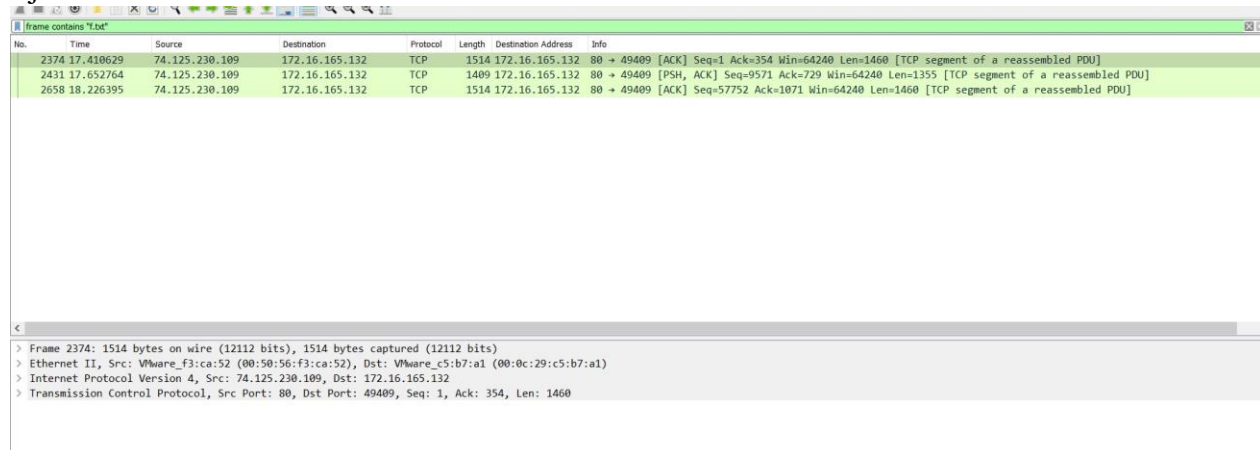
The image shows the Brim interface. At the top, there is a histogram of file durations. The x-axis represents time in seconds, with markers at 0, :45, 12:59, :15, :30, :45, and 01 AM. The y-axis represents the count of files. The histogram shows a significant peak around 12:59. Below the histogram is a table of analyzed files. The table has columns: source, depth, analyzers, mime type, filename, duration, and local. The first row is highlighted with a red box, showing a file with mime type 'application/x-dosexec' and duration '5.104743s'.

	source	depth	analyzers	mime type	filename	duration	local
zwJ8]	HTTP	0	[[PE, MD5, SHA1]]	application/x-dosexec	⊗	5.104743s	⊗
NNs9]	HTTP	0	[[MD5, SHA1]]	application/javascript	⊗	367.521ms	⊗
f1e]	HTTP	0	[[MD5, SHA1]]	application/javascript	f.txt	240.188ms	⊗
f1e]	HTTP	0	[[MD5, SHA1]]	application/javascript	f.txt	14.001ms	⊗
'2i1]	HTTP	0	[[MD5, SHA1]]	application/javascript	⊗	3.729ms	⊗
f1e]	HTTP	0	analyzers [[bstring]]	application/javascript	f.txt	7us	⊗
H2d3]	SSL	0	[[MD5, SHA1, X509, SHA256]]	application/x-x509-ca-cert	⊗	0s	⊗

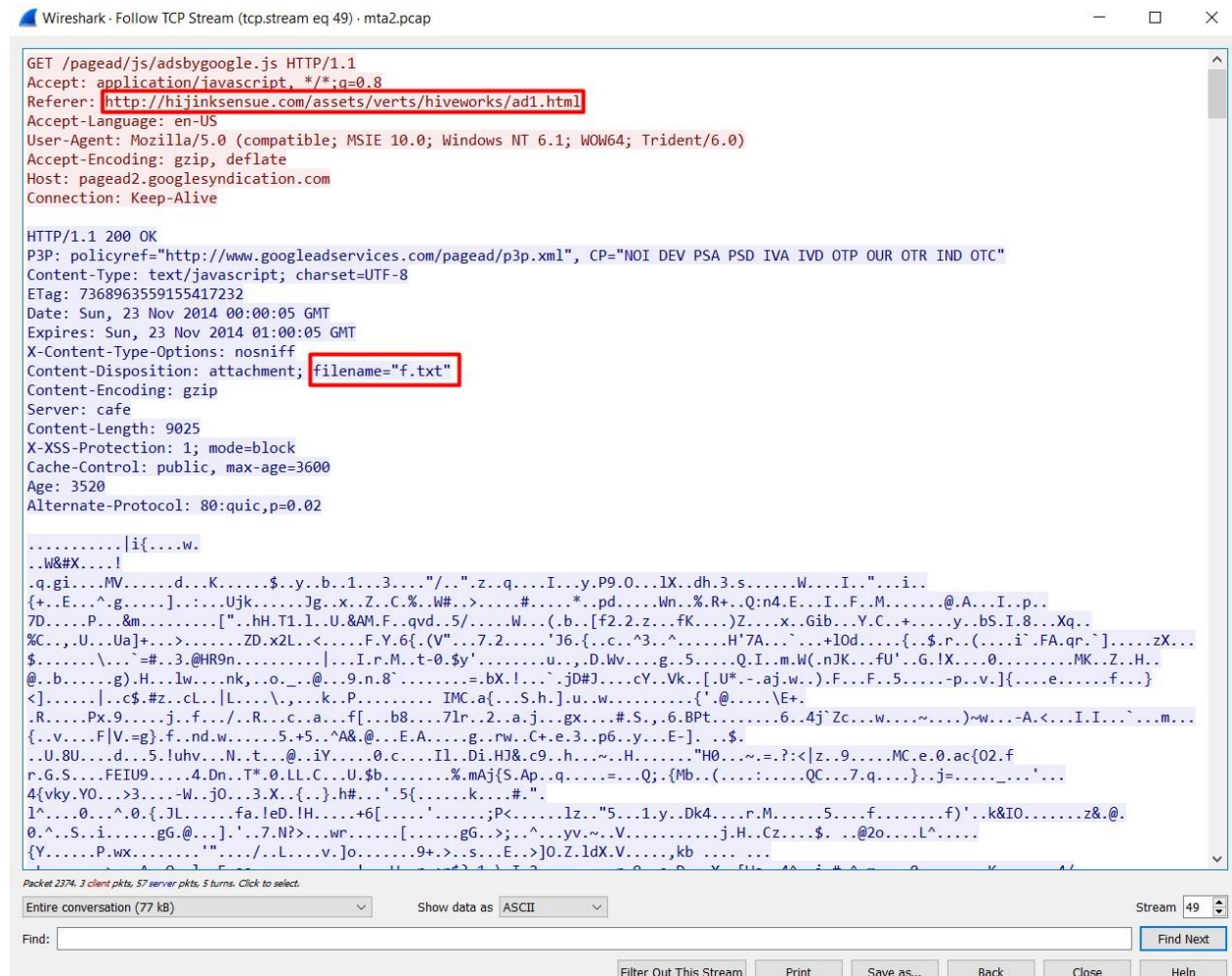
Application/x-dosexec our answer.

Q.13) What was the referrer for the visited URI that returned the file “f.txt”?

I just search for all the frames which contain f.txt in Wireshark. I followed the TCP stream.



No.	Time	Source	Destination	Protocol	Length	Destination Address	Info
2374	17.410629	74.125.230.109	172.16.165.132	TCP	1514	172.16.165.132	80 → 49409 [ACK] Seq=1 Ack=354 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
2431	17.652764	74.125.230.109	172.16.165.132	TCP	1409	172.16.165.132	80 → 49409 [PSH, ACK] Seq=9571 Ack=729 Win=64240 Len=1355 [TCP segment of a reassembled PDU]
2658	18.226395	74.125.230.109	172.16.165.132	TCP	1514	172.16.165.132	80 → 49409 [ACK] Seq=57752 Ack=1071 Win=64240 Len=1460 [TCP segment of a reassembled PDU]



Wireshark · Follow TCP Stream (tcp.stream eq 49) · mta2.pcap

GET /pagead/js/adsbygoogle.js HTTP/1.1
Accept: application/javascript, */*;q=0.8
Referer: **http://hijinksensue.com/assets/verts/hiveworks/ad1.html**
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Accept-Encoding: gzip, deflate
Host: pagead2.googlesyndication.com
Connection: Keep-Alive

HTTP/1.1 200 OK
P3P: policyref="http://www.googleadservices.com/pagead/p3p.xml", CP="NOI DEV PSA PSD IVA IVD OTP OUR OTR IND OTC"
Content-Type: text/javascript; charset=UTF-8
ETag: 7368963559155417232
Date: Sun, 23 Nov 2014 00:00:05 GMT
Expires: Sun, 23 Nov 2014 01:00:05 GMT
X-Content-Type-Options: nosniff
Content-Disposition: attachment; **filename="f.txt"**
Content-Encoding: gzip
Server: cafe
Content-Length: 9025
X-XSS-Protection: 1; mode=block
Cache-Control: public, max-age=3600
Age: 3520
Alternate-Protocol: 80:quic,p=0.02

Packet 2374: 3 client pkts, 57 server pkts, 5 turns. Click to select.

Entire conversation (77 kB) Show data as ASCII Stream 49

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

We can get the referrer of the visited URI :
http://hijinksensue.com/assets/verts/hiveworks/ad1.html

Q.14) When was this PCAP captured?

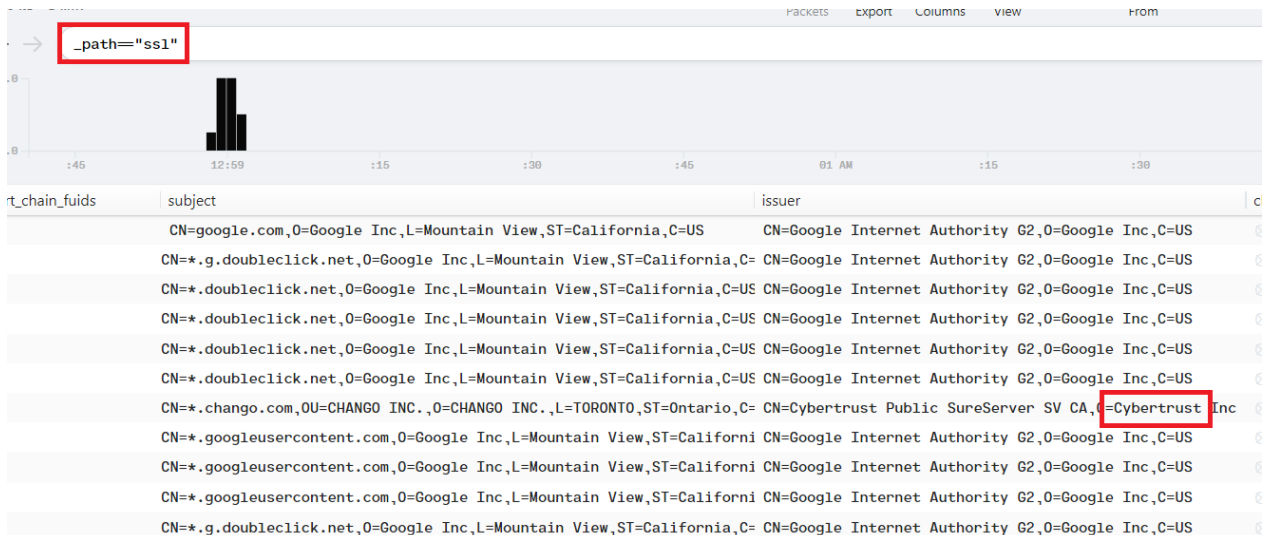
In the properties in the wireshark of the pcap file I get the time when the PCAP was captured.
23/11/2014

Q.15) When was the PE file compiled?

In VirusTotal we can see the date. **Answer: 21/11/2014**

Q.16) What is the name of the SSL certificate issuer that appeared only once? (one word)

From BrimSecurity we search for ssl & on seeing the issuer column we find out that **Cybertrust** only appears once.



t_chain_fuids	subject	issuer
	CN=google.com,O=Google Inc,L=Mountain View,ST=California,C=US	CN=Google Internet Authority G2,O=Google Inc,C=US
	CN=*.g.doubleclick.net,O=Google Inc,L=Mountain View,ST=California,C=US	CN=Google Internet Authority G2,O=Google Inc,C=US
	CN=*.doubleclick.net,O=Google Inc,L=Mountain View,ST=California,C=US	CN=Google Internet Authority G2,O=Google Inc,C=US
	CN=*.doubleclick.net,O=Google Inc,L=Mountain View,ST=California,C=US	CN=Google Internet Authority G2,O=Google Inc,C=US
	CN=*.doubleclick.net,O=Google Inc,L=Mountain View,ST=California,C=US	CN=Google Internet Authority G2,O=Google Inc,C=US
	CN=*.doubleclick.net,O=Google Inc,L=Mountain View,ST=California,C=US	CN=Google Internet Authority G2,O=Google Inc,C=US
	CN=*.chango.com,O=CHANGO INC.,L=TORONTO,ST=Ontario,C=US	CN=Cybertrust Public SureServer SV CA, Cybertrust Inc
	CN=*.googleusercontent.com,O=Google Inc,L=Mountain View,ST=California,C=US	CN=Google Internet Authority G2,O=Google Inc,C=US
	CN=*.googleusercontent.com,O=Google Inc,L=Mountain View,ST=California,C=US	CN=Google Internet Authority G2,O=Google Inc,C=US
	CN=*.googleusercontent.com,O=Google Inc,L=Mountain View,ST=California,C=US	CN=Google Internet Authority G2,O=Google Inc,C=US
	CN=*.g.doubleclick.net,O=Google Inc,L=Mountain View,ST=California,C=US	CN=Google Internet Authority G2,O=Google Inc,C=US

Q.17) What were the two protection methods enabled during the compilation of the present PE file? Format: comma-separated in alphabetical order

I used checksec (<https://github.com/Wenzel/checksec.py/releases/tag/v0.6.2>) I find out the protection methods.

Processing ... 1/1 • 100.0%

Checksec Results: PE

File	NX	Canary	ASLR	Dynamic Base	High Entropy VA	SEH	SafeSEH	Force Integrity	Control Flow Guard	Isolation	Authent...
malware	Yes	No	No	No	/	Yes	No	No	No	Yes	No

Answer: DEP,SEH