'Malware Traffic Analysis 2' challenge at cyberdefenders.org

Tools used for this challenge:

- NetworkMiner

- Wireshark

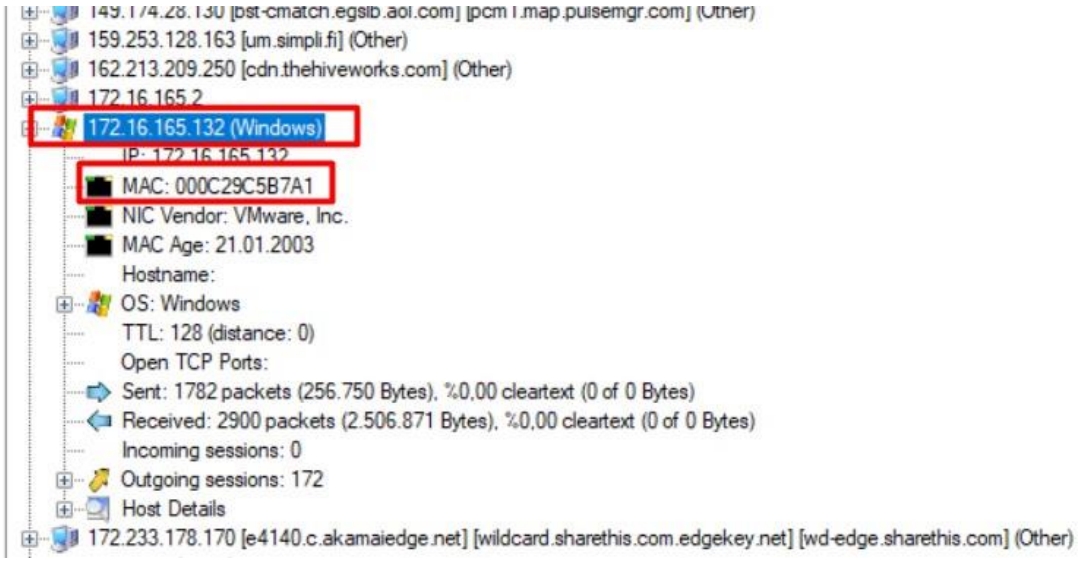
- VirusTotal

- 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.



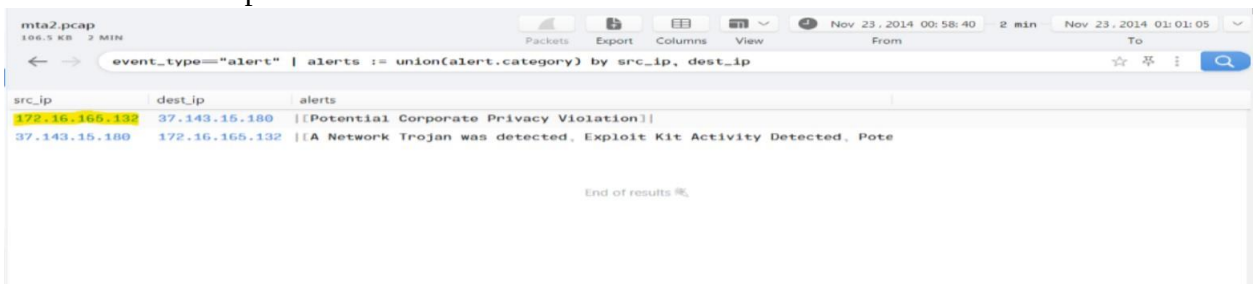
Answer :**172.16.165.132**

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 maches our infected host and Ip address of the compromised website.



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

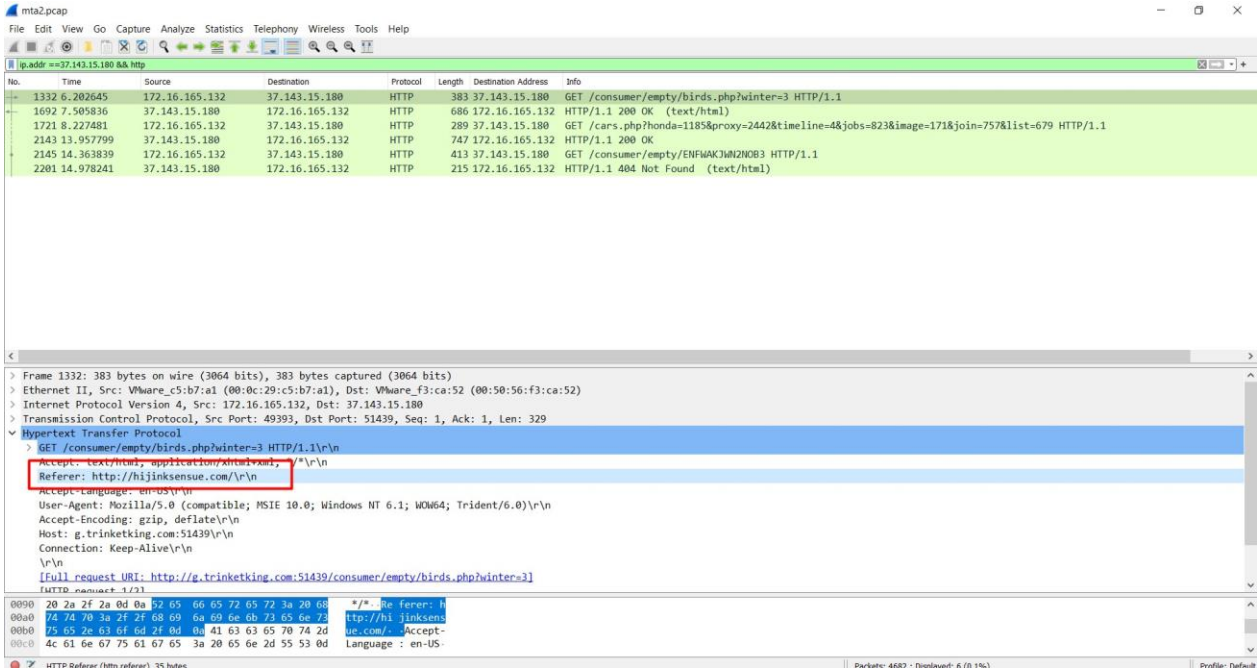
Answer : 37.143.15.180:51439

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

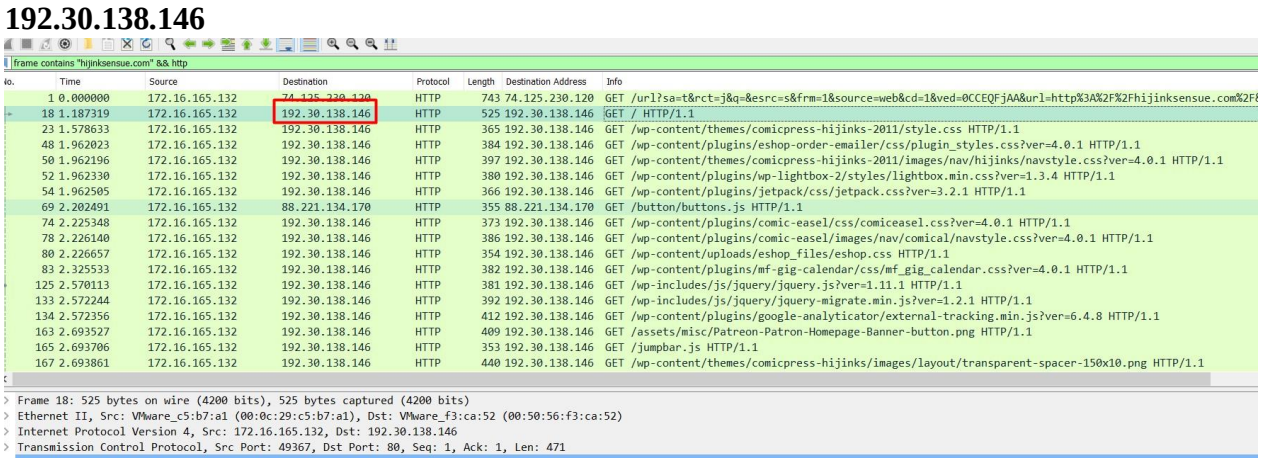
From the above Networkminer result, we also get the two FQDN that delivered the exploit kit.
g.trinketking.com,h.trinketking.com

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 Protoco
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	50.87.149.90	80	TCP
2014-11-23 00:58:47 Z	A Network Trojan was detected	ET CURRENT_EVENTS Sweet Orange Landing Nov 04 2013	1	37.143.15.180	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	37.143.15.180	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	37.143.15.180	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	50.87.149.90	80	172.16.165.132	49388	TCP

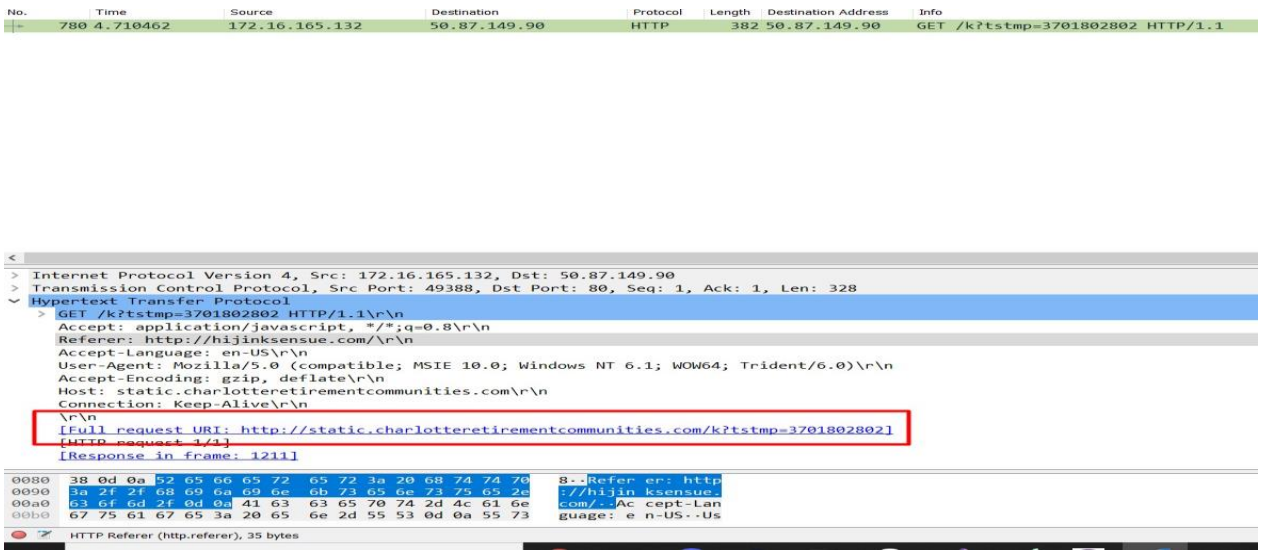
Q.8) What is the redirect URL that points to the exploit kit landing page?

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	50.87.149.90	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	37.143.15.180	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	37.143.15.180	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	37.143.15.180	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	50.87.149.90	80	172.16.165.132	49388	TCP	static.charlotteretirementcommunities.com

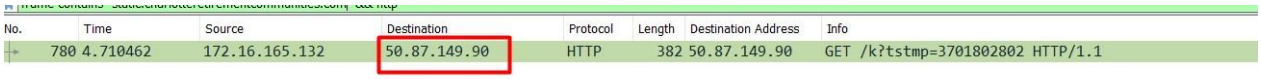
And when I filter the website in Wireshark I can see the redirect URL .

static.charlotteretirementcommunities.com/k?tstmp=3701802802



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

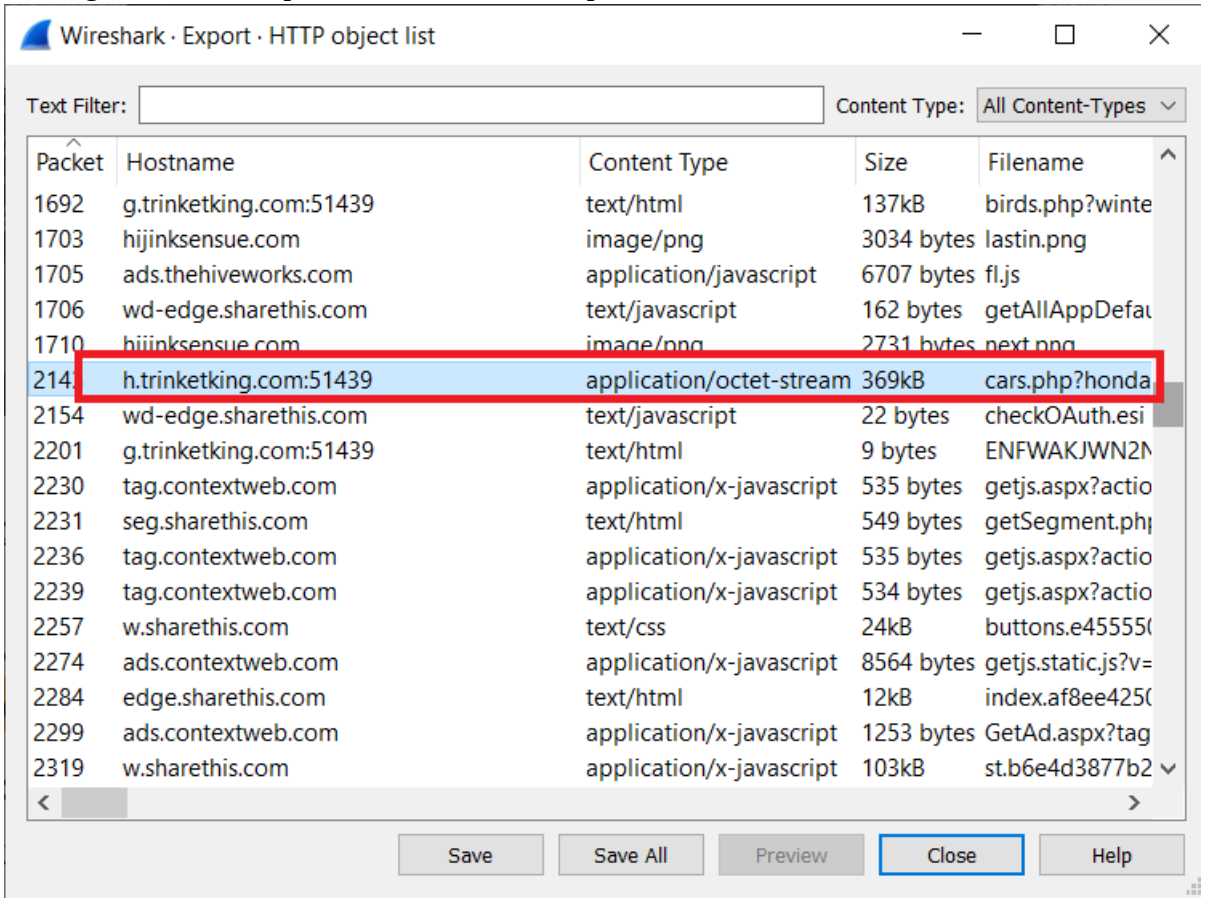
We know the name of the website from previous question, we can just look at the frame and get the IP address.Answer



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.

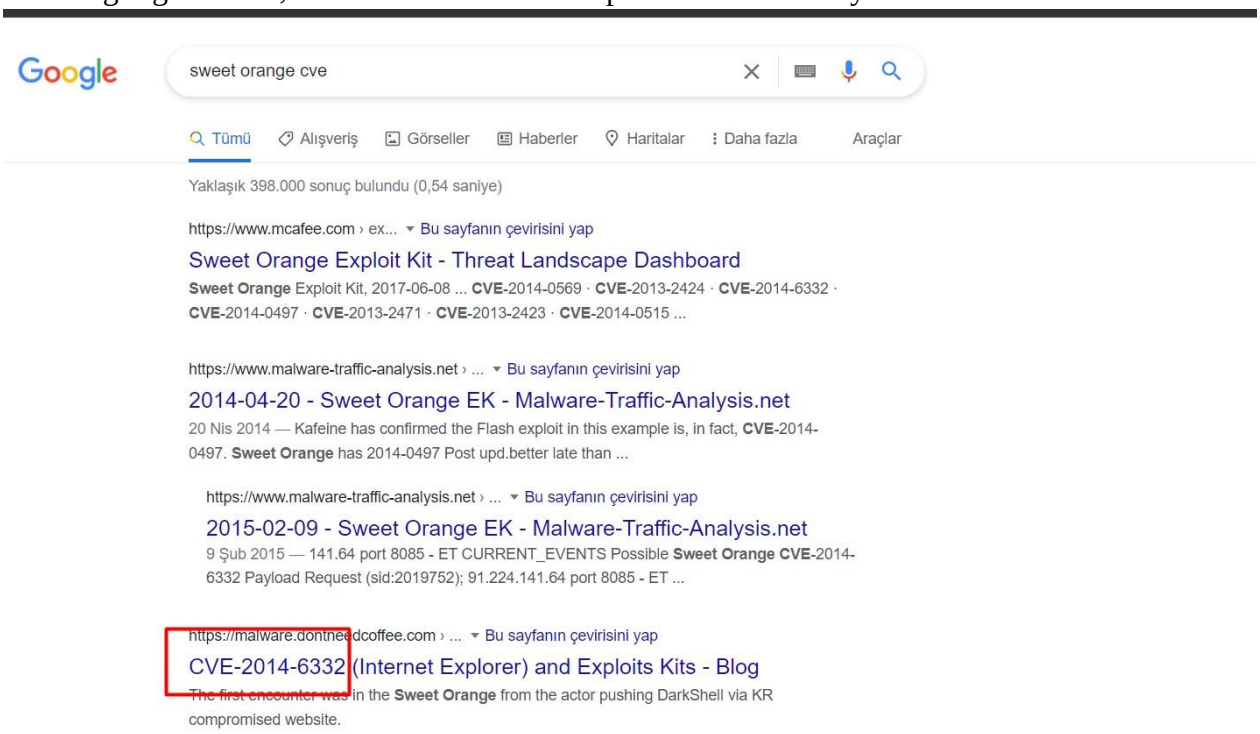


Packet	Hostname	Content Type	Size	Filename
1692	g.trinketking.com:51439	text/html	137kB	birds.php?winte
1703	hijinksensue.com	image/png	3034 bytes	lastin.png
1705	ads.thehiveworks.com	application/javascript	6707 bytes	fl.js
1706	wd-edge.sharethis.com	text/javascript	162 bytes	getAllAppDefau
1710	hijinksensue.com	image/png	2731 bytes	next.png
214	h.trinketking.com:51439	application/octet-stream	369kB	cars.php?honda
2154	wd-edge.sharethis.com	text/javascript	22 bytes	checkOAuth.esi
2201	g.trinketking.com:51439	text/html	9 bytes	ENFWAKJWN2N
2230	tag.contextweb.com	application/x-javascript	535 bytes	getjs.aspx?actio
2231	seg.sharethis.com	text/html	549 bytes	getSegment.ph
2236	tag.contextweb.com	application/x-javascript	535 bytes	getjs.aspx?actio
2239	tag.contextweb.com	application/x-javascript	534 bytes	getjs.aspx?actio
2257	w.sharethis.com	text/css	24kB	buttons.e45555
2274	ads.contextweb.com	application/x-javascript	8564 bytes	getjs.static.js?v=
2284	edge.sharethis.com	text/html	12kB	index.af8ee425
2299	ads.contextweb.com	application/x-javascript	1253 bytes	GetAd.aspx?tag
2319	w.sharethis.com	application/x-javascript	103kB	st.b6e4d3877b2

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

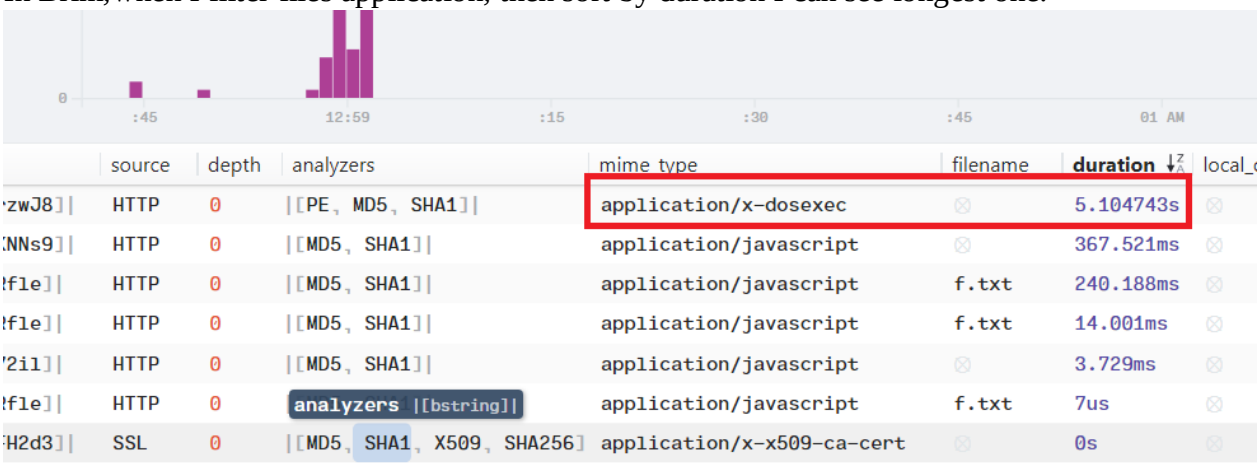
Q.11) What is the CVE of the exploited vulnerability?

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



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.

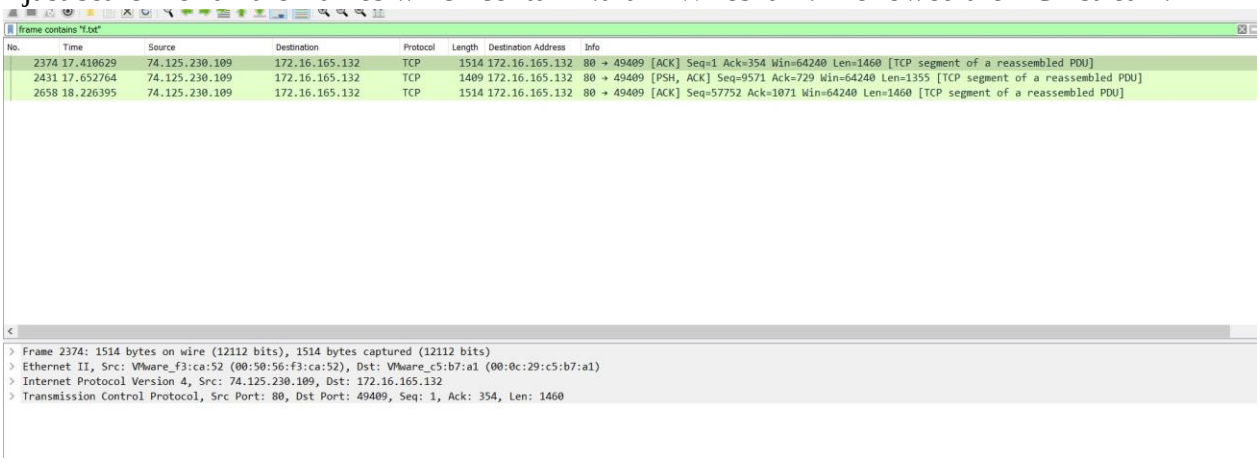


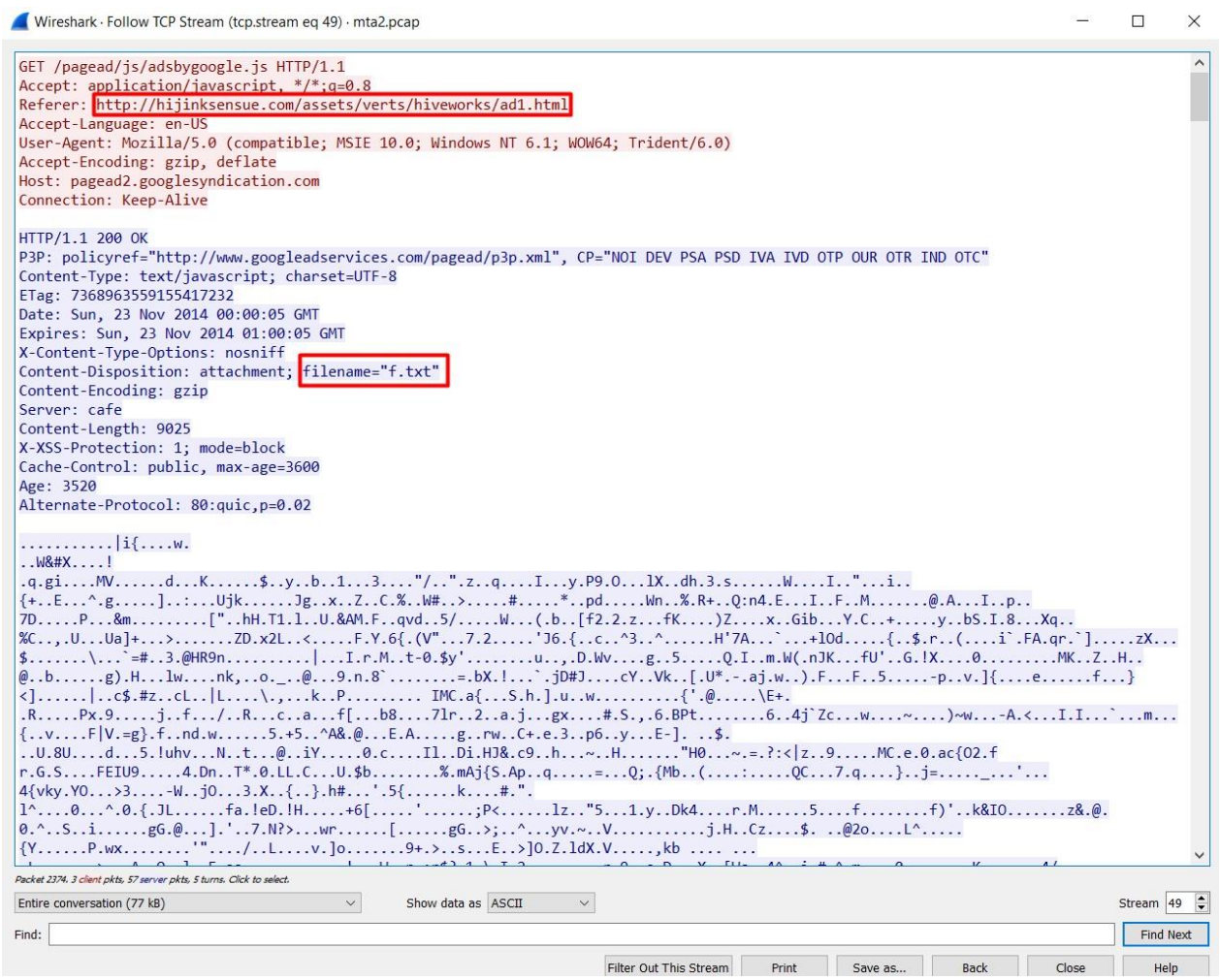
	source	depth	analyzers	mime_type	filename	duration	local_
zwJ8]]	HTTP	0	[[PE, MD5, SHA1]]	application/x-dosexec		5.104743s	
NNs9]]	HTTP	0	[[MD5, SHA1]]	application/javascript		367.521ms	
fle]]	HTTP	0	[[MD5, SHA1]]	application/javascript	f.txt	240.188ms	
fle]]	HTTP	0	[[MD5, SHA1]]	application/javascript	f.txt	14.001ms	
2il]]	HTTP	0	[[MD5, SHA1]]	application/javascript		3.729ms	
fle]]	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.





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.

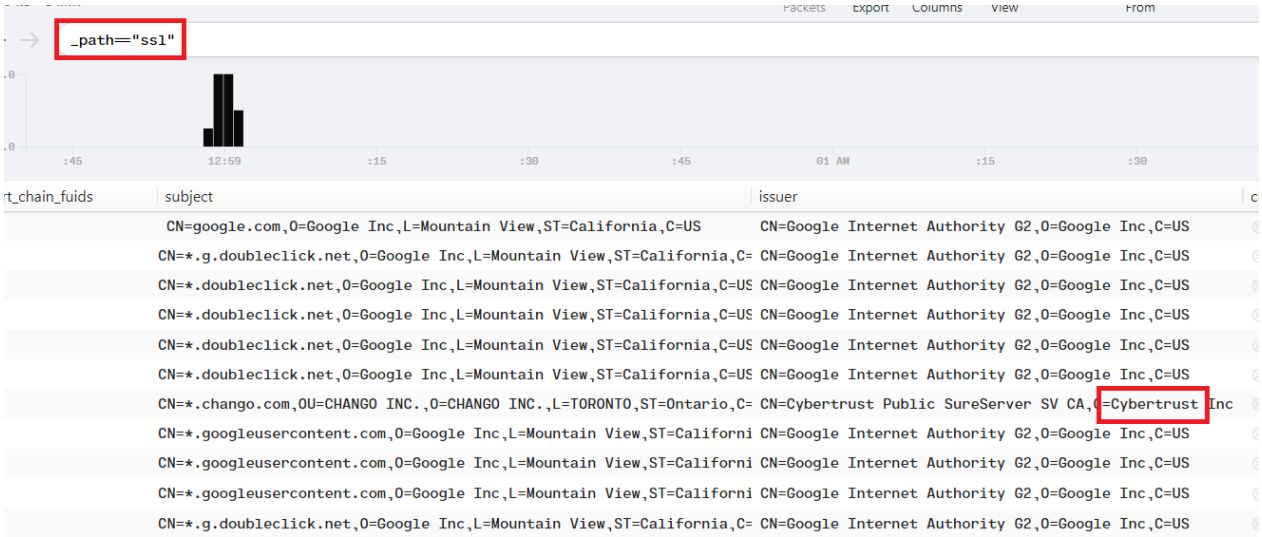
23/11/2014

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.



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