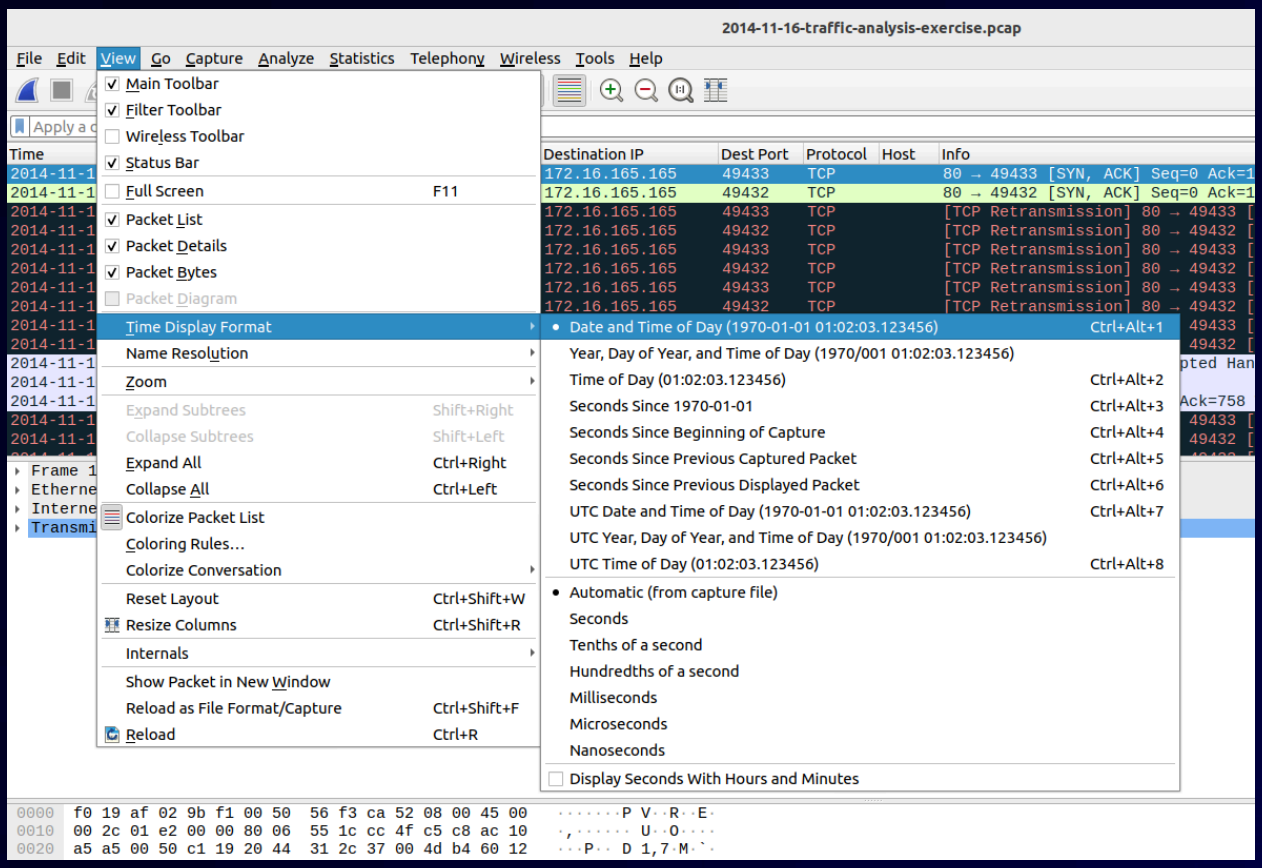
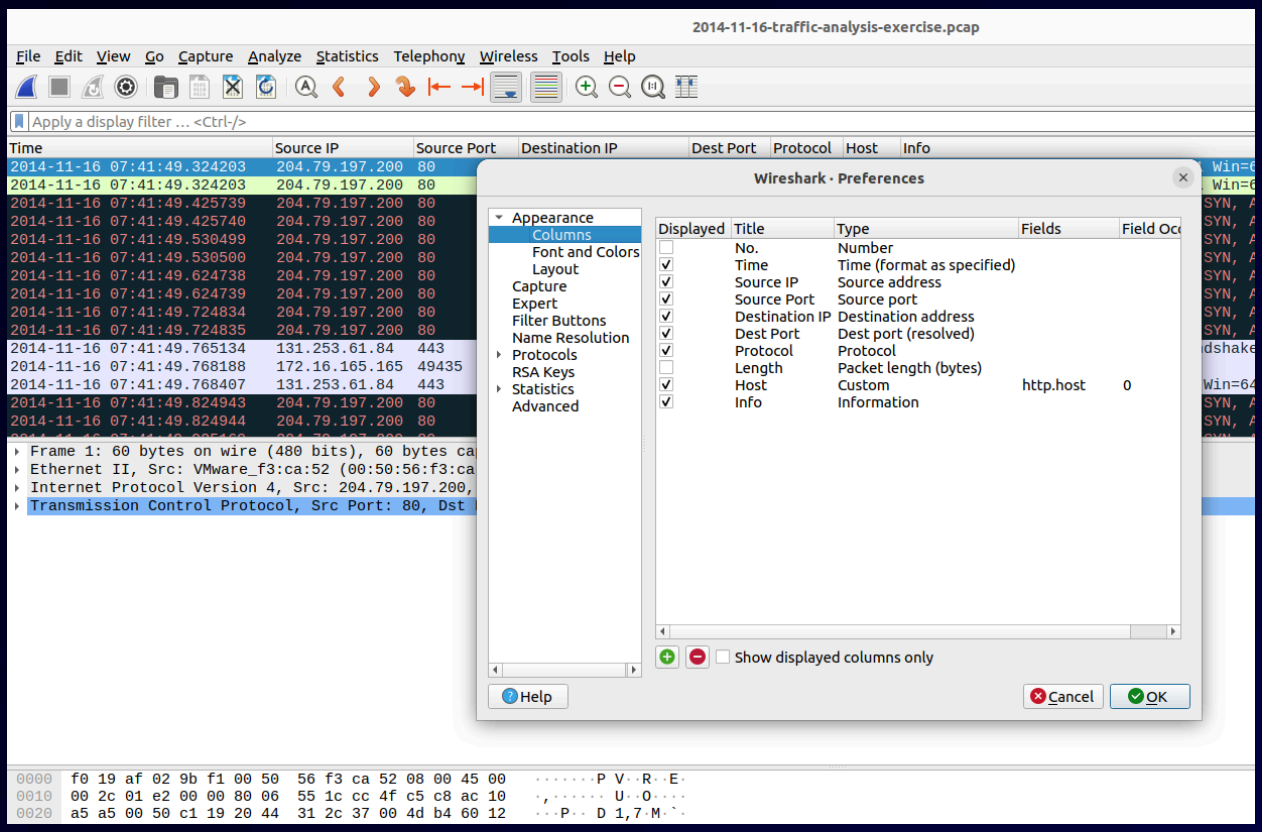
Wireshark Setup :

1. Change Time display setting
    - View — Time Display Format — Date and Time of Day

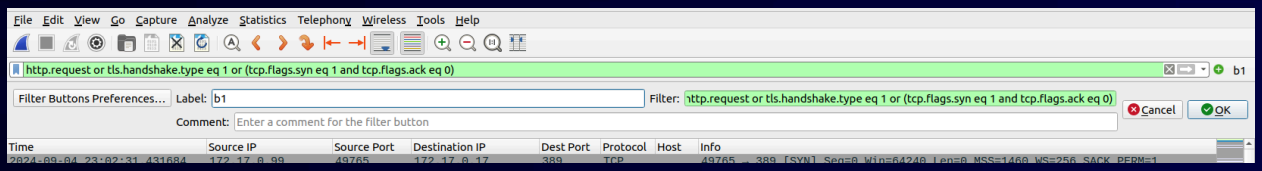


2. Add Source and Destination Port

- Right-Click — Column Preferences — [+] icon — add the required fields
- Select required fields



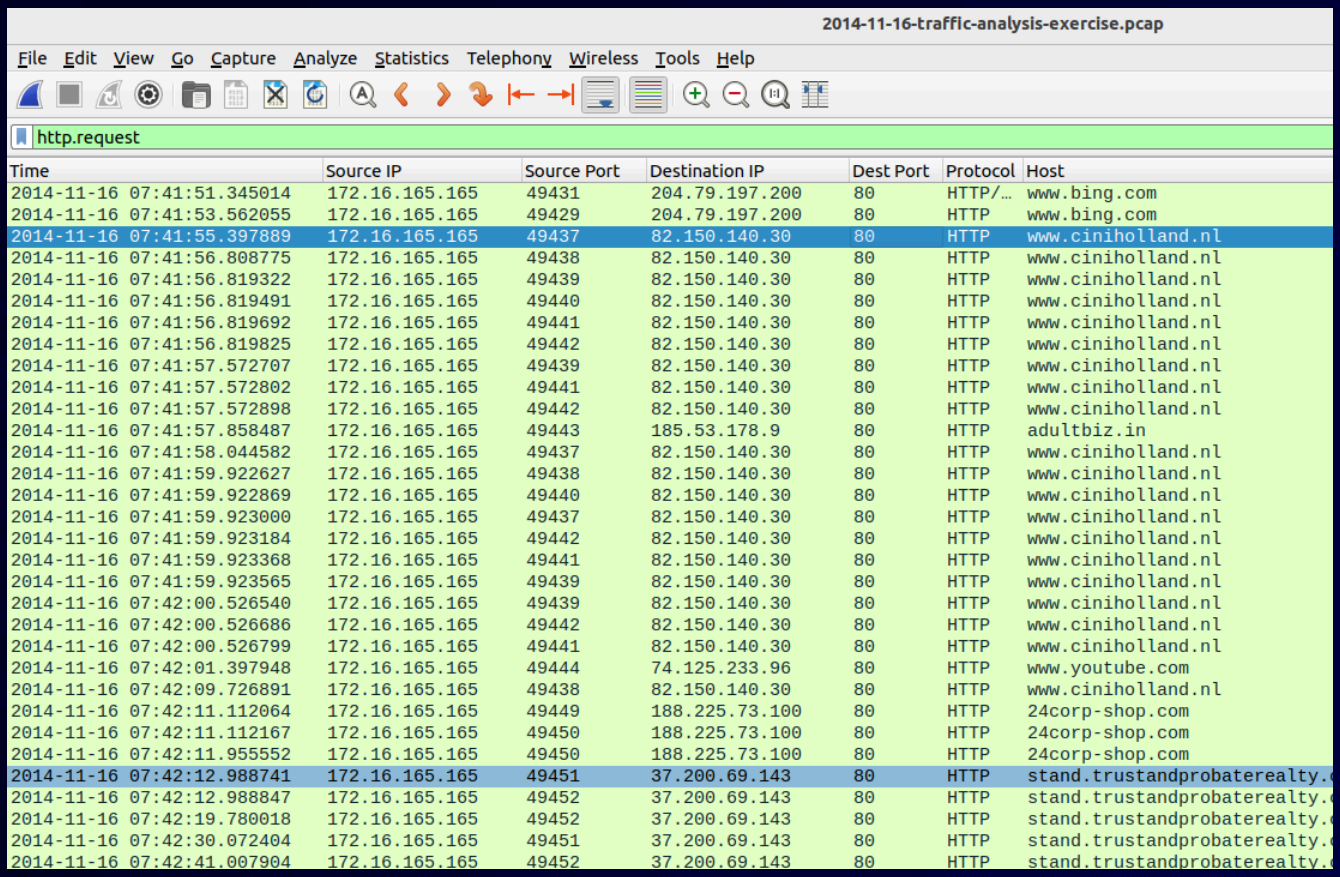
3. For long filters we can create buttons.



Answer these Questions :

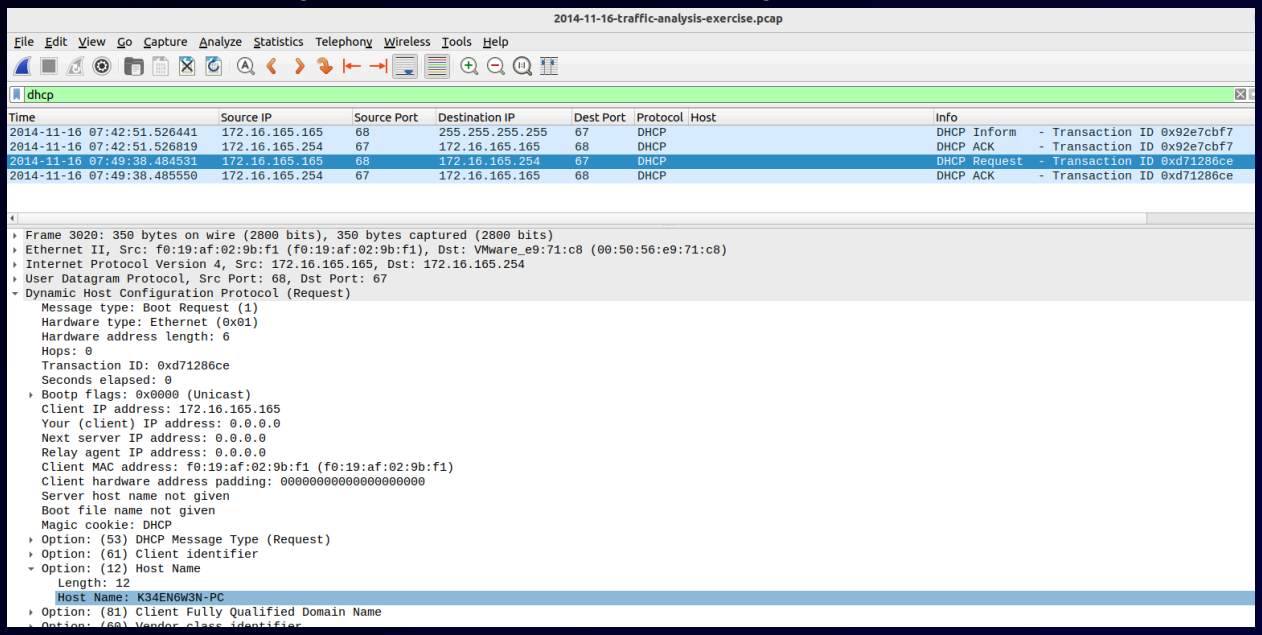
1. What is the IP address of the Windows VM that gets infected?
2. What is the host name of the Windows VM that gets infected?
3. What is the MAC address of the infected VM?
4. What is the IP address of the compromised web site?
5. What is the domain name of the compromised web site?
6. What is the IP address and domain name that delivered the exploit kit and malware?
7. What is the domain name that delivered the exploit kit and malware?
8. Extract the exploit file(s). What is(are) the md5 file hash(es)?

Answer for 1,4,5,6,7

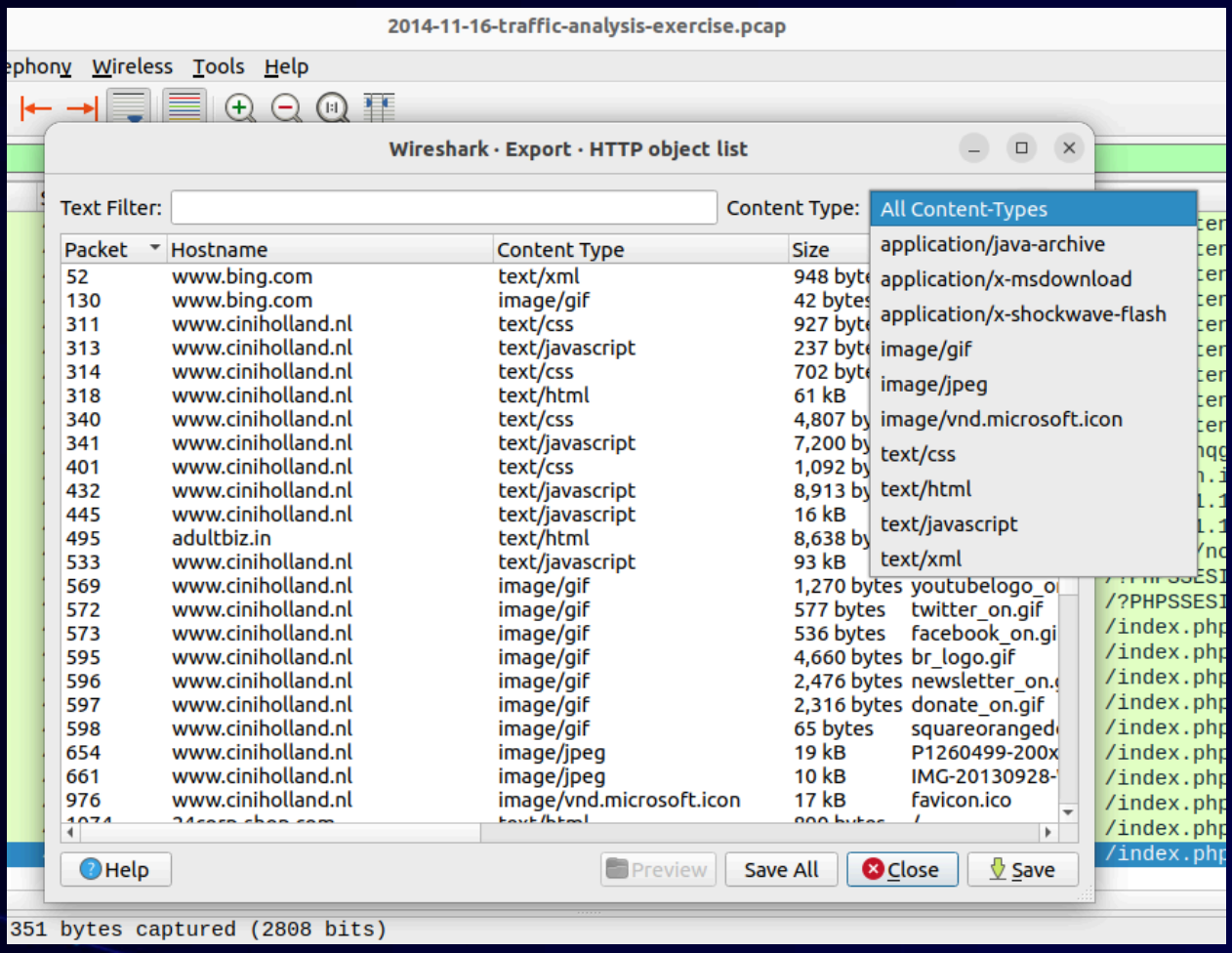


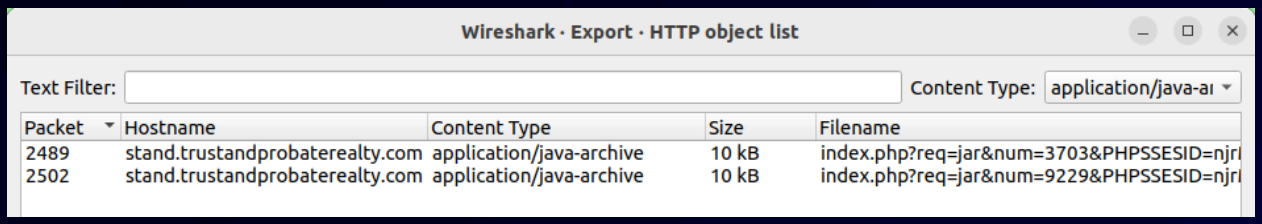
Time	Source IP	Source Port	Destination IP	Dest Port	Protocol	Host
2014-11-16 07:41:51.345014	172.16.165.165	49431	204.79.197.200	80	HTTP/…	www.bing.com
2014-11-16 07:41:53.562055	172.16.165.165	49429	204.79.197.200	80	HTTP	www.bing.com
2014-11-16 07:41:55.397889	172.16.165.165	49437	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:56.808775	172.16.165.165	49438	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:56.819322	172.16.165.165	49439	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:56.819491	172.16.165.165	49440	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:56.819692	172.16.165.165	49441	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:56.819825	172.16.165.165	49442	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:57.572707	172.16.165.165	49439	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:57.572802	172.16.165.165	49441	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:57.572898	172.16.165.165	49442	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:57.858487	172.16.165.165	49443	185.53.178.9	80	HTTP	adultbiz.in
2014-11-16 07:41:58.044582	172.16.165.165	49437	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:59.922627	172.16.165.165	49438	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:59.922869	172.16.165.165	49440	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:59.923000	172.16.165.165	49437	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:59.923184	172.16.165.165	49442	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:59.923368	172.16.165.165	49441	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:41:59.923565	172.16.165.165	49439	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:42:00.526540	172.16.165.165	49439	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:42:00.526686	172.16.165.165	49442	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:42:00.526799	172.16.165.165	49441	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:42:01.397948	172.16.165.165	49444	74.125.233.96	80	HTTP	www.youtube.com
2014-11-16 07:42:09.726891	172.16.165.165	49438	82.150.140.30	80	HTTP	www.ciniholland.nl
2014-11-16 07:42:11.112064	172.16.165.165	49449	188.225.73.100	80	HTTP	24corp-shop.com
2014-11-16 07:42:11.112167	172.16.165.165	49450	188.225.73.100	80	HTTP	24corp-shop.com
2014-11-16 07:42:11.955552	172.16.165.165	49450	188.225.73.100	80	HTTP	24corp-shop.com
2014-11-16 07:42:12.988741	172.16.165.165	49451	37.200.69.143	80	HTTP	stand.trustandprobaterealty.c
2014-11-16 07:42:12.988847	172.16.165.165	49452	37.200.69.143	80	HTTP	stand.trustandprobaterealty.c
2014-11-16 07:42:19.780018	172.16.165.165	49452	37.200.69.143	80	HTTP	stand.trustandprobaterealty.c
2014-11-16 07:42:30.072404	172.16.165.165	49451	37.200.69.143	80	HTTP	stand.trustandprobaterealty.c
2014-11-16 07:42:41.007904	172.16.165.165	49452	37.200.69.143	80	HTTP	stand.trustandprobaterealty.c

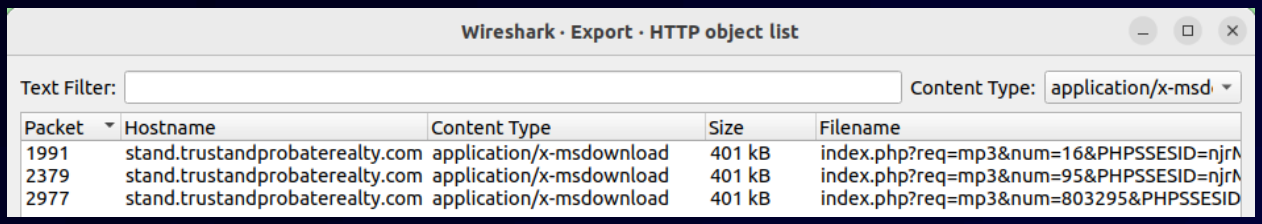
Answer for 2,3 : Finding Hostname and MAC address using dhcp

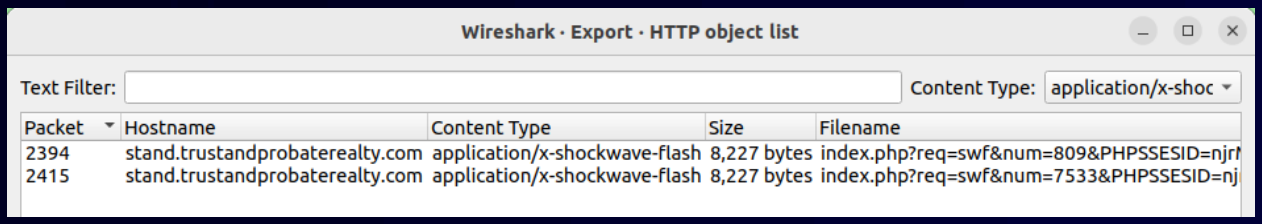


Answer for 8 : Extract the exploit file(s). What is(are) the md5 file hash(es)?

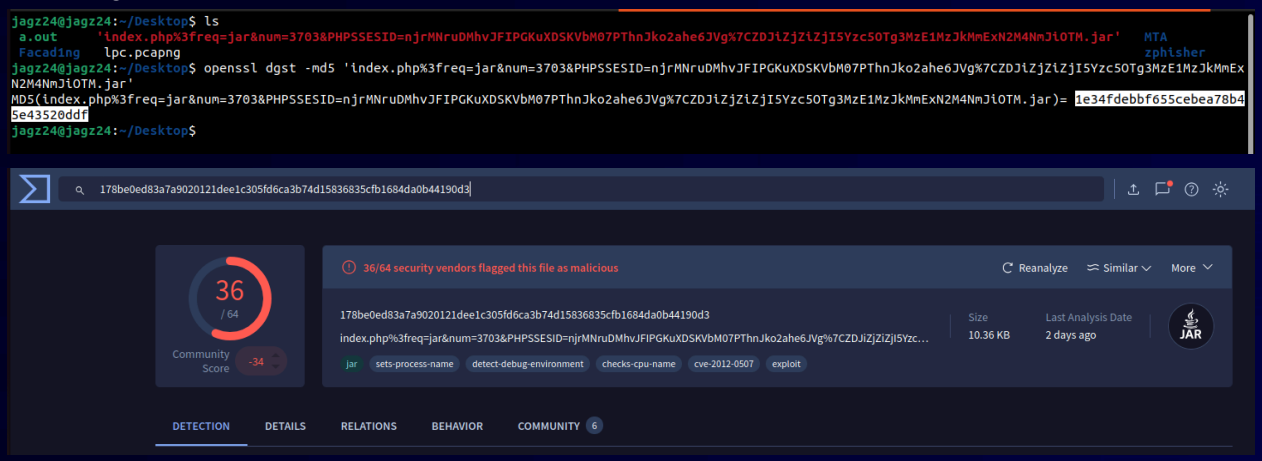








Checking if these hashes are malicious in VirusTotal :



NOTE :

- The Analysis differs from each pcap files.
- There are many levels for finding information. The above are only level 1.