

Wireshark Setup :

1. Change Time display setting

- View — Time Display Format — Date and Time of Day

The screenshot shows the Wireshark interface with the 'View' menu open. The 'Time Display Format' option is selected, which has opened a submenu. In this submenu, the 'Date and Time of Day (1970-01-01 01:02:03.123456)' option is highlighted, which has a keyboard shortcut of 'Ctrl+Alt+1'. Other options in the submenu include 'Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)', 'Time of Day (01:02:03.123456)', 'Seconds Since 1970-01-01', 'Seconds Since Beginning of Capture', 'Seconds Since Previous Captured Packet', 'Seconds Since Previous Displayed Packet', 'UTC Date and Time of Day (1970-01-01 01:02:03.123456)', 'UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)', and 'UTC Time of Day (01:02:03.123456)'. There is also an 'Automatic (from capture file)' section with options for 'Seconds', 'Tenths of a second', 'Hundredths of a second', 'Milliseconds', 'Microseconds', and 'Nanoseconds'. At the bottom of the submenu, there is a checkbox for 'Display Seconds With Hours and Minutes'.

Destination IP	Dest Port	Protocol	Host	Info
172.16.165.165	49433	TCP	80 → 49433	[SYN, ACK] Seq=0 Ack=1
172.16.165.165	49432	TCP	80 → 49432	[SYN, ACK] Seq=0 Ack=1
172.16.165.165	49433	TCP		[TCP Retransmission] 80 → 49433
172.16.165.165	49432	TCP		[TCP Retransmission] 80 → 49432
172.16.165.165	49433	TCP		[TCP Retransmission] 80 → 49433
172.16.165.165	49432	TCP		[TCP Retransmission] 80 → 49432
172.16.165.165	49433	TCP		[TCP Retransmission] 80 → 49433
172.16.165.165	49432	TCP		[TCP Retransmission] 80 → 49432

0000 f0 19 af 02 9b f1 00 50 56 f3 ca 52 08 00 45 00 P V . R . E .
 0010 00 2c 01 e2 00 00 80 06 55 1c cc 4f c5 c8 ac 10 ., U . . 0
 0020 a5 a5 00 50 c1 19 20 44 31 2c 37 00 4d b4 60 12 . . P . . D 1, 7 . M . . .

2. Add Source and Destination Port

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

2014-11-16-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Time	Source IP	Source Port	Destination IP	Dest Port	Protocol	Host	Info
2014-11-16 07:41:49.324203	204.79.197.200	80					
2014-11-16 07:41:49.324203	204.79.197.200	80					
2014-11-16 07:41:49.425739	204.79.197.200	80					
2014-11-16 07:41:49.425740	204.79.197.200	80					
2014-11-16 07:41:49.530499	204.79.197.200	80					
2014-11-16 07:41:49.530500	204.79.197.200	80					
2014-11-16 07:41:49.624738	204.79.197.200	80					
2014-11-16 07:41:49.624739	204.79.197.200	80					
2014-11-16 07:41:49.724834	204.79.197.200	80					
2014-11-16 07:41:49.724835	204.79.197.200	80					
2014-11-16 07:41:49.765134	131.253.61.84	443					
2014-11-16 07:41:49.768188	172.16.165.165	49435					
2014-11-16 07:41:49.768407	131.253.61.84	443					
2014-11-16 07:41:49.824943	204.79.197.200	80					
2014-11-16 07:41:49.824944	204.79.197.200	80					
2014-11-16 07:41:49.824945	204.79.197.200	80					

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: VMware_f3:ca:52 (00:50:56:f3:ca:52), Dst: 08:00:2b:00:00:00

Internet Protocol Version 4, Src: 204.79.197.200, Dst: 131.253.61.84

Transmission Control Protocol, Src Port: 80, Dst Port: 443

0000 f0 19 af 02 0b f1 00 50 56 f3 ca 52 08 00 45 00P V..R..E..

0010 00 2c 01 e2 00 00 80 06 55 1c cc 4f c5 c8 ac 10 ..,.....U..0....

0020 a5 a5 00 50 c1 19 20 44 31 2c 37 00 4d b4 60 12 ...P...D 1,7..M..

3. For long filters we can create buttons.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request or tls.handshake.type eq 1 or (tcp.flags.syn eq 1 and tcp.flags.ack eq 0) b1

Filter Buttons Preferences... Label: b1 Filter: http.request or tls.handshake.type eq 1 or (tcp.flags.syn eq 1 and tcp.flags.ack eq 0)

Comment: Enter a comment for the filter button

Time	Source IP	Source Port	Destination IP	Dest Port	Protocol	Host	Info
2024-08-04 23:02:31.431684	172.17.0.99	49765	172.17.0.17	389	TCP	49765 -> 389 [SYN] Seq=8 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1	

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

2014-11-16-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

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.trustandprobarealty.com
2014-11-16 07:42:12.988847	172.16.165.165	49452	37.200.69.143	80	HTTP	stand.trustandprobarealty.com
2014-11-16 07:42:19.780018	172.16.165.165	49452	37.200.69.143	80	HTTP	stand.trustandprobarealty.com
2014-11-16 07:42:30.072404	172.16.165.165	49451	37.200.69.143	80	HTTP	stand.trustandprobarealty.com
2014-11-16 07:42:41.007904	172.16.165.165	49452	37.200.69.143	80	HTTP	stand.trustandprobarealty.com

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

2014-11-16-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcpc

Time	Source IP	Source Port	Destination IP	Dest Port	Protocol	Host	Info
2014-11-16 07:42:51.526441	172.16.165.165	68	255.255.255.255	67	DHCP		DHCP Inform - Transaction ID 0x92e7cbf7
2014-11-16 07:42:51.526819	172.16.165.254	67	172.16.165.165	68	DHCP		DHCP ACK - Transaction ID 0x92e7cbf7
2014-11-16 07:49:38.484531	172.16.165.165	68	172.16.165.254	67	DHCP		DHCP Request - Transaction ID 0xd71286ce
2014-11-16 07:49:38.485550	172.16.165.254	67	172.16.165.165	68	DHCP		DHCP ACK - Transaction ID 0xd71286ce

Frame 3020: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits)

Ethernet II, Src: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: VMware_e9:71:c8 (00:50:56:e9:71:c8)

Internet Protocol Version 4, Src: 172.16.165.165, Dst: 172.16.165.254

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Request)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xd71286ce

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 172.16.165.165

Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

Option: (53) DHCP Message Type (Request)

Option: (61) Client identifier

Option: (12) Host Name

Length: 12

Host Name: K34EN6W3N-PC

Option: (81) Client Fully Qualified Domain Name

Option: (60) Vendor class identifier

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

2014-11-16-traffic-analysis-exercise.pcap

Telephony Wireless Tools Help

Wireshark · Export · HTTP object list

Text Filter:

Content Type:

Packet	Hostname	Content Type	Size
52	www.bing.com	text/xml	948 bytes
130	www.bing.com	image/gif	42 bytes
311	www.ciniholland.nl	text/css	927 bytes
313	www.ciniholland.nl	text/javascript	237 bytes
314	www.ciniholland.nl	text/css	702 bytes
318	www.ciniholland.nl	text/html	61 kB
340	www.ciniholland.nl	text/css	4,807 bytes
341	www.ciniholland.nl	text/javascript	7,200 bytes
401	www.ciniholland.nl	text/css	1,092 bytes
432	www.ciniholland.nl	text/javascript	8,913 bytes
445	www.ciniholland.nl	text/javascript	16 kB
495	adultbiz.in	text/html	8,638 bytes
533	www.ciniholland.nl	text/javascript	93 kB
569	www.ciniholland.nl	image/gif	1,270 bytes
572	www.ciniholland.nl	image/gif	577 bytes
573	www.ciniholland.nl	image/gif	536 bytes
595	www.ciniholland.nl	image/gif	4,660 bytes
596	www.ciniholland.nl	image/gif	2,476 bytes
597	www.ciniholland.nl	image/gif	2,316 bytes
598	www.ciniholland.nl	image/gif	65 bytes
654	www.ciniholland.nl	image/jpeg	19 kB
661	www.ciniholland.nl	image/jpeg	10 kB
976	www.ciniholland.nl	image/vnd.microsoft.icon	17 kB
1074	3dscg.chase.com	text/html	888 bytes

351 bytes captured (2808 bits)

Wireshark · Export · HTTP object list				
Text Filter:		Content Type: application/java-ai		
Packet	Hostname	Content Type	Size	Filename
2489	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=3703&PHPSESSID=njr
2502	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=9229&PHPSESSID=njr

Wireshark · Export · HTTP object list				
Text Filter:		Content Type: application/x-msd		
Packet	Hostname	Content Type	Size	Filename
1991	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=16&PHPSESSID=njr
2379	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=95&PHPSESSID=njr
2977	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=803295&PHPSESSID

Wireshark · Export · HTTP object list				
Text Filter:		Content Type: application/x-shoc		
Packet	Hostname	Content Type	Size	Filename
2394	stand.trustandprobaterealty.com	application/x-shockwave-flash	8,227 bytes	index.php?req=swf&num=809&PHPSESSID=njr
2415	stand.trustandprobaterealty.com	application/x-shockwave-flash	8,227 bytes	index.php?req=swf&num=7533&PHPSESSID=nj

Checking if these hashes are malicious in VirusTotal :

```
jagz24@jagz24:~/Desktop$ ls
a.out      'index.php%3freq=jar&num=3703&PHPSESSID=njrMnruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZD3lZjZlZjI5Yzc50Tg3MzE1MzJkMmEXN2M4NmJlOTM.jar'
Facading  lpc.pcapng
jagz24@jagz24:~/Desktop$ openssl dgst -md5 'index.php%3freq=jar&num=3703&PHPSESSID=njrMnruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZD3lZjZlZjI5Yzc50Tg3MzE1MzJkMmEXN2M4NmJlOTM.jar'
MD5(index.php%3freq=jar&num=3703&PHPSESSID=njrMnruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZD3lZjZlZjI5Yzc50Tg3MzE1MzJkMmEXN2M4NmJlOTM.jar)= 1e34fdebbf655cebea78b45e43520dd1
jagz24@jagz24:~/Desktop$
```


NOTE :

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