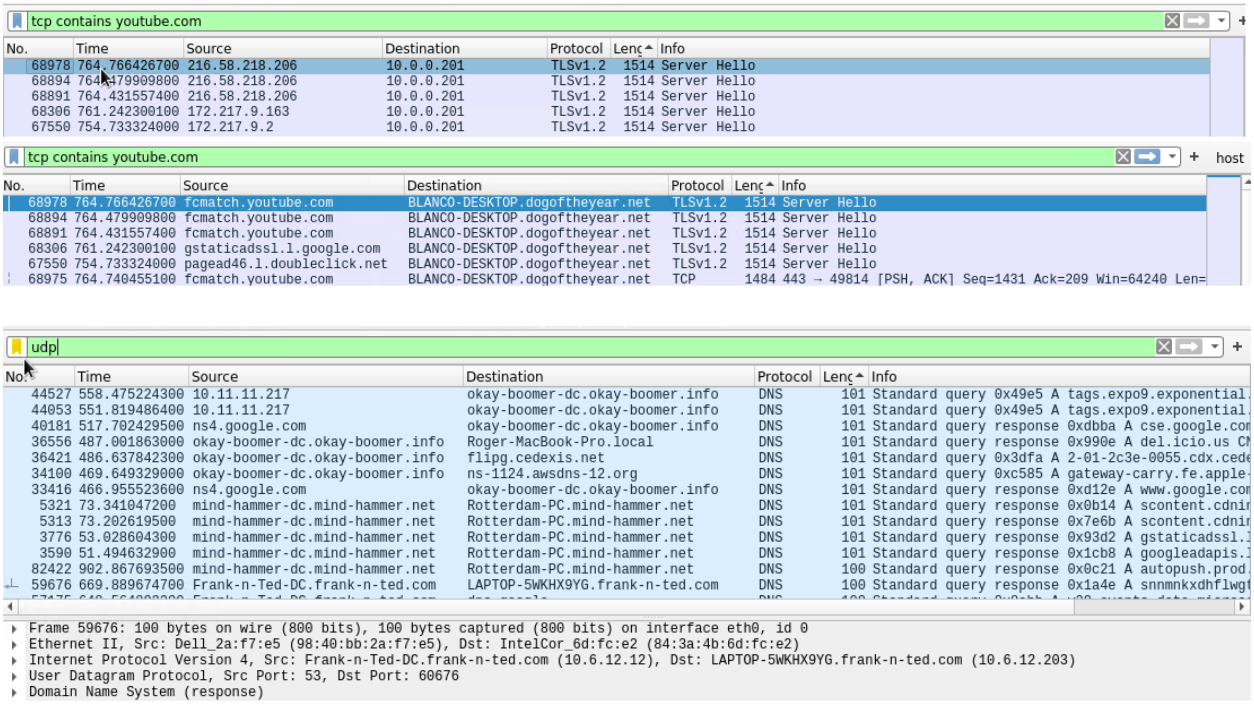
Network Analysis

Time Thieves

At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range10.6.12.0/24 .



You must inspect your traffic capture to answer the following questions:

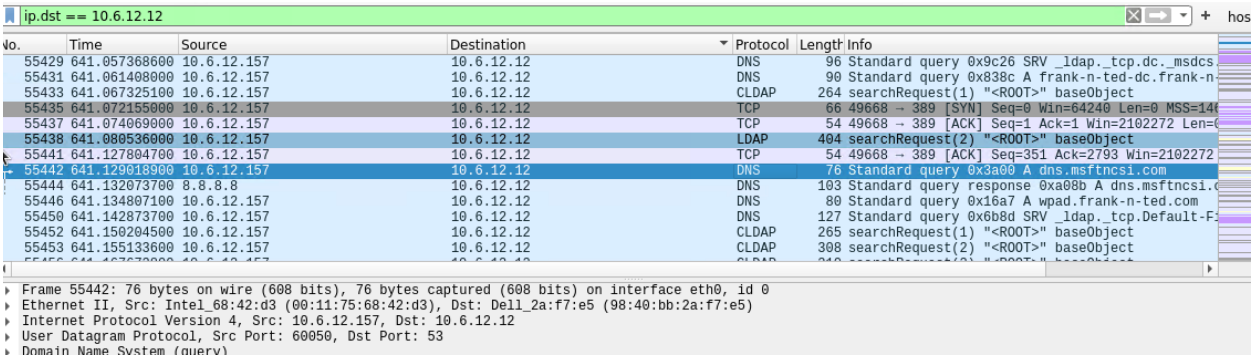
1. What is the domain name of the users' custom site?

   Frank-n-ted.com

2. What is the IP address of the Domain Controller (DC) of the AD network?

When I was exploring DNS protocol and destination IP addresses, I found the DC to be

10.6.12.157

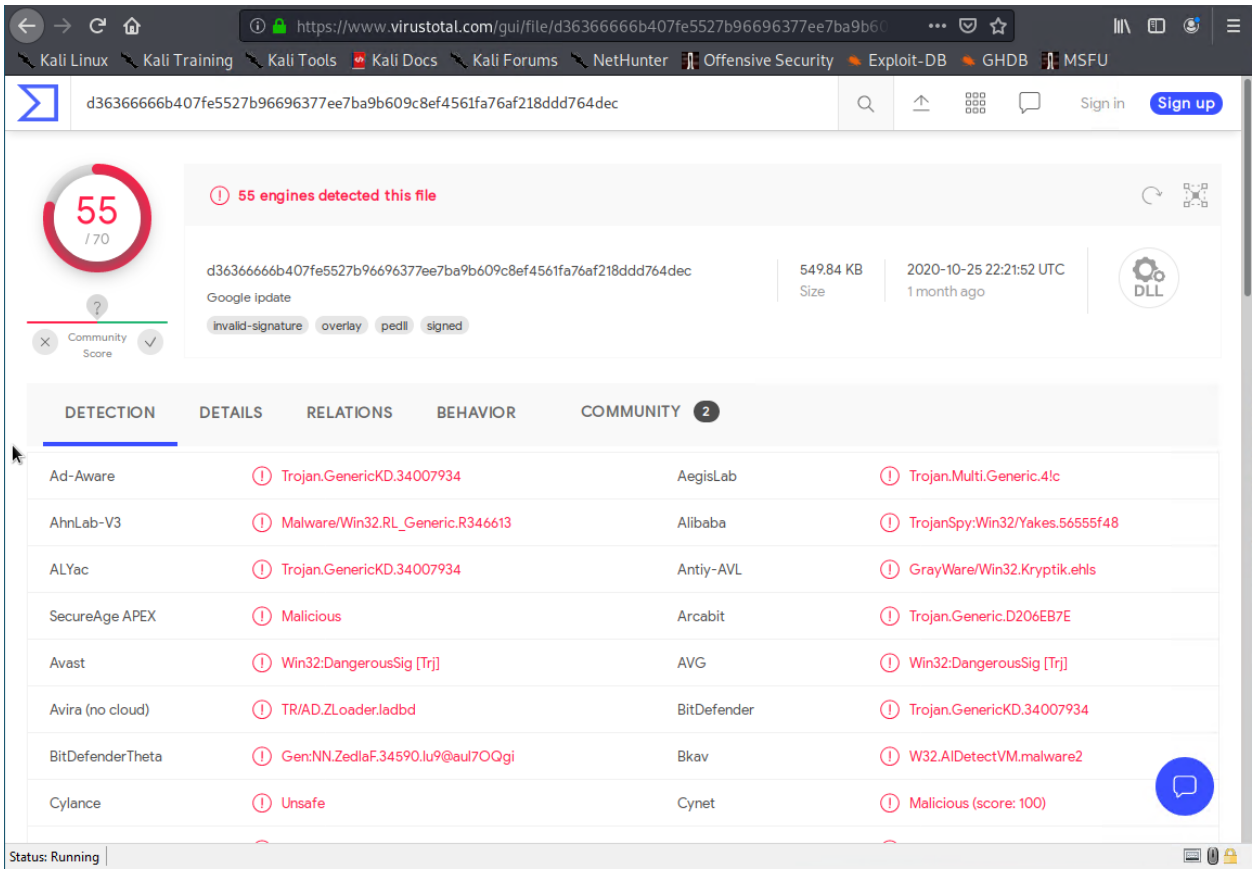


3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.

The file name is June11.dll

4. Upload the file to VirusTotal.com. What kind of malware is this classified as?

The malware is identified by most engines as being a Trojan.


https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b6
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Sign in
Sign up
55
/ 70
55 engines detected this file
d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Google ipdate
invalid-signature
overlay
pedll
signed
549.84 KB
Size
2020-10-25 22:21:52 UTC
1 month ago
DLL
Community Score
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 2
Ad-Aware
Trojan.GenericKD.34007934
AegisLab
Trojan.Multi.Generic.4!c
AhnLab-V3
Malware/Win32.RL_Generic.R346613
Alibaba
TrojanSpy:Win32/Yakes.56555f48
ALYac
Trojan.GenericKD.34007934
Antiy-AVL
GrayWare/Win32.Kryptik.ehls
SecureAge APEX
Malicious
Arcabit
Trojan.Generic.D206EB7E
Avast
Win32:DangerousSig [Trj]
AVG
Win32:DangerousSig [Trj]
Avira (no cloud)
TR/AD.ZLoader.ladbd
BitDefender
Trojan.GenericKD.34007934
BitDefenderTheta
Gen:NN.ZedlaF.34590.lu9@aul7OQgi
Bkav
W32.AIDetectVM.malware2
Cylance
Unsafe
Cynet
Malicious (score: 100)
Status: Running

Vulnerable Windows Machines

The Security team received reports of an infected Windows host on the network. They know the following:

- Machines in the network live in the range 172.16.4.0/24 .
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at 172.16.4.4 and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

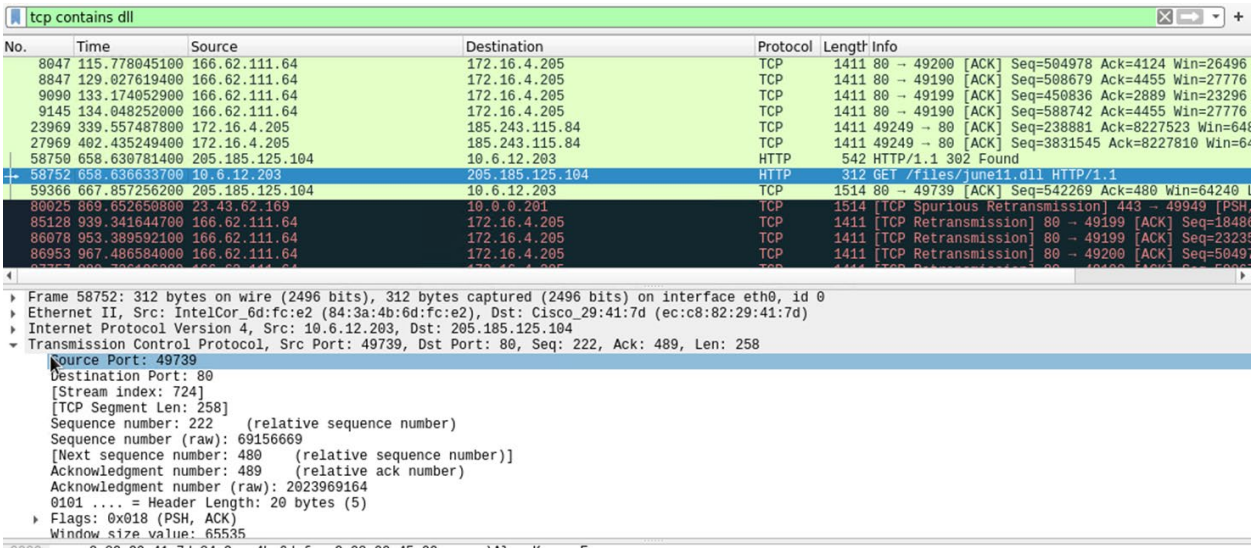
Inspect your traffic to answer the following questions:

1. Find the following information about the infected Windows machine:
    - Host name: ROTTERDAM-PC
    - IP address: 172.16.4.205
    - MAC address: 00:59:07:b0:63:a4

2. What is the username of the Windows user whose computer is infected?

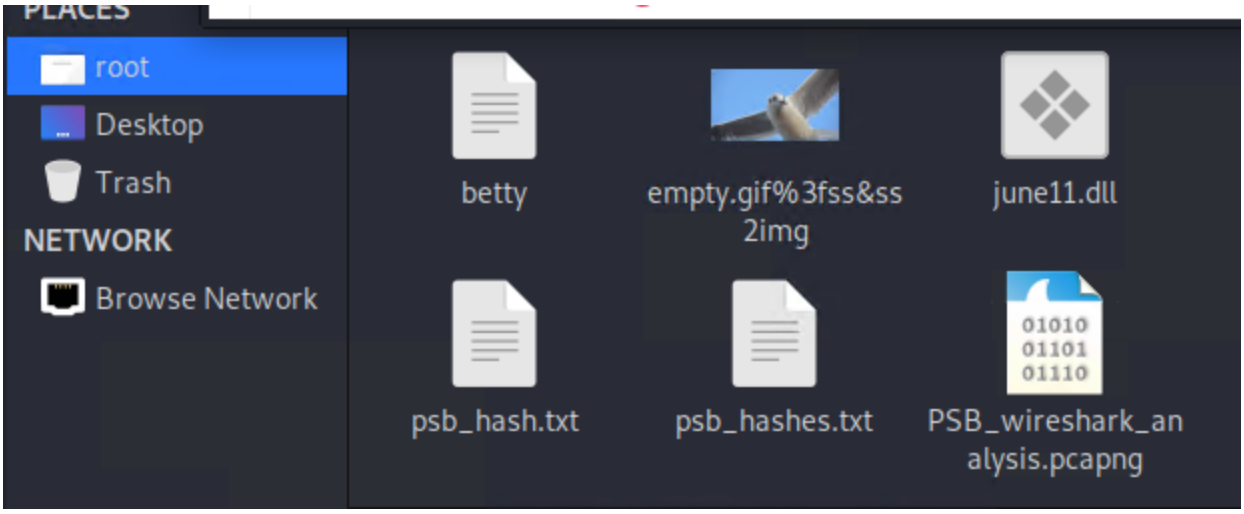
3. What are the IP addresses used in the actual infection traffic?

205.185.125.104



4. As a bonus, retrieve the desktop background of the Windows host.

With time constraints, I was not able to run commands to find specifics about a desktop background, however I did download all packets that had attachments for examination. All graphics would not suit a background other than an empty.gif file that containe d what looked like a seagull; perhaps this was used as a desktop graphic.



Illegal Downloads

IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloadin g operating systems. However, they have a strict policy against copyright infringement.

IT shared the following about the torrent activity:

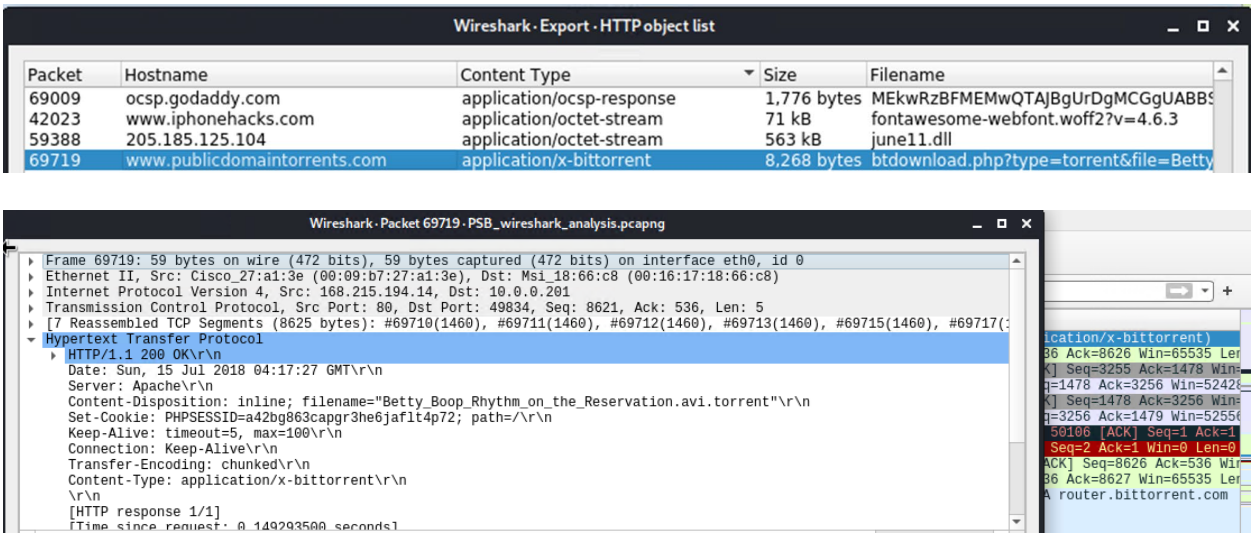
- The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
- The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

Your task is to isolate torrent traffic and answer the following questions:

1. Find the following information about the machine with I P address 10.0.0.201 :
    - MAC address 00:16:17:18:66:c8
    - Windows username PC BLANCO-DESKTOP
    - OS version

2. Which torrent file did the user download?

Betty_Boop_Rhythm_on_the_Reservation.avi



SCREENSHOTS USED AS EVIDENCE

Wireshark · Endpoints · PSB_wireshark_analysis.pcapng

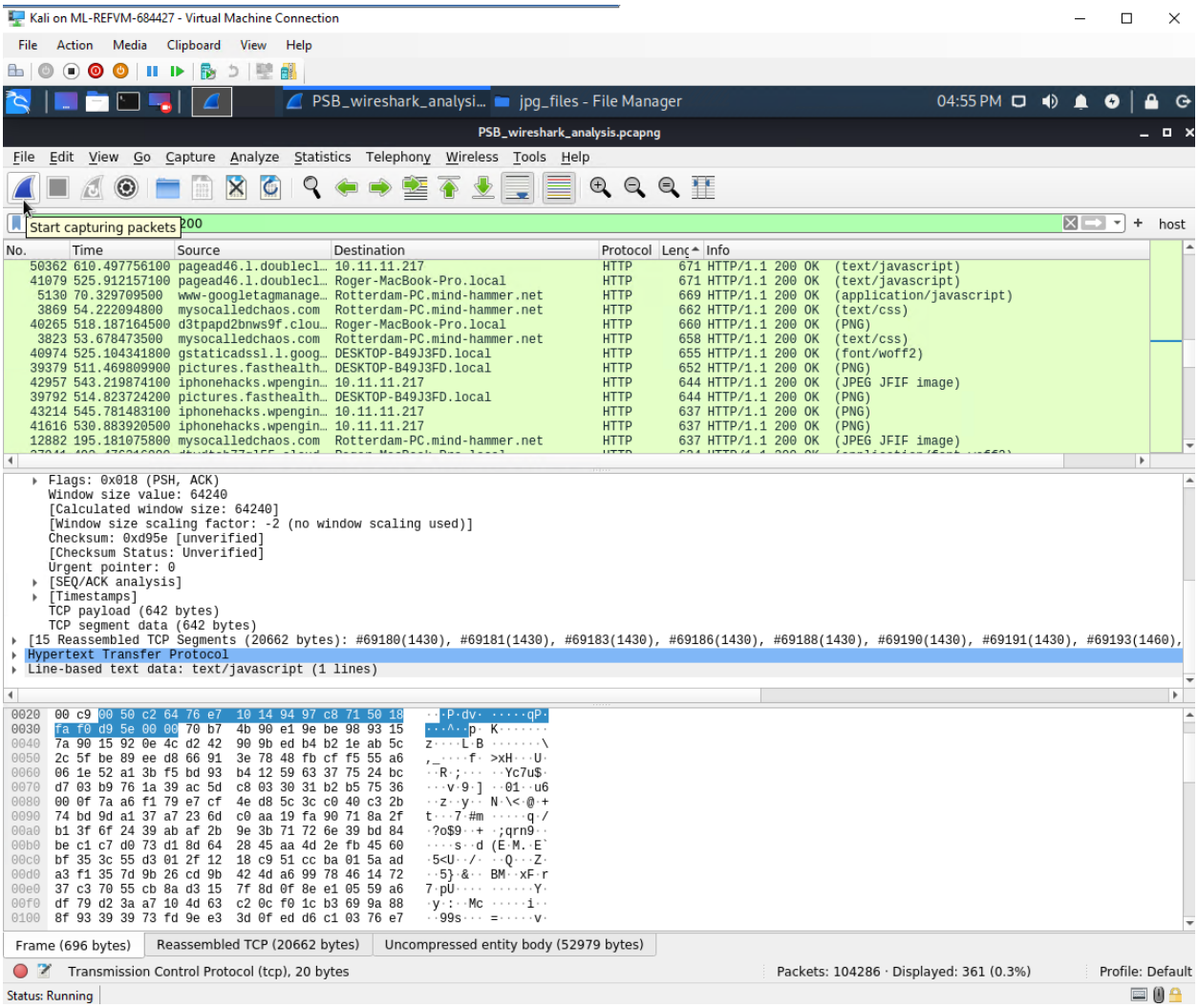
Ethernet · 30 | IPv4 · 808 | IPv6 · 2 | TCP · 1372 | UDP · 1977

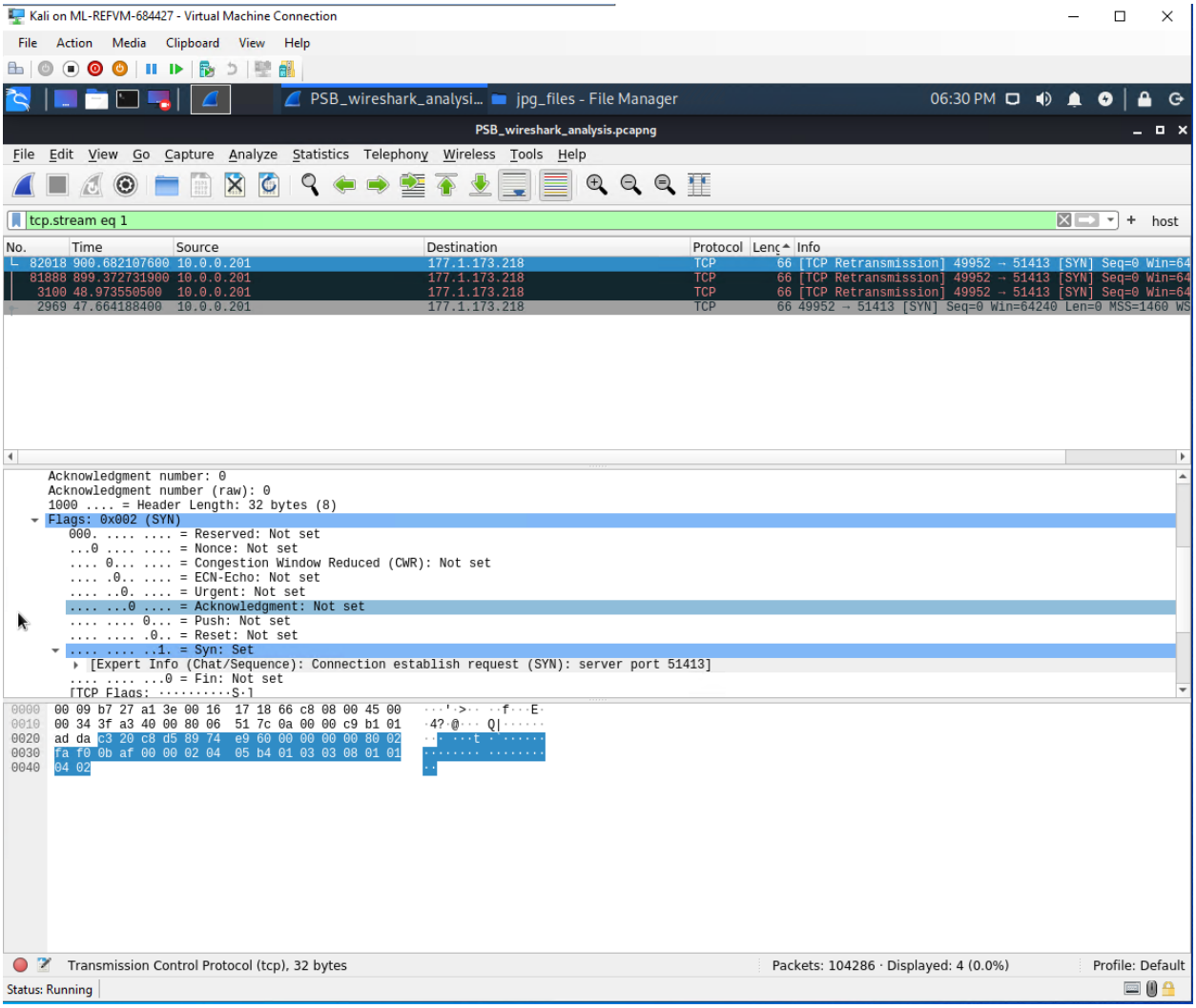
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number
172.16.4.205	51,364	45 M	21,973	10 M	29,391	34 M	—	—	—
185.243.115.84	30,344	26 M	15,195	16 M	15,149	9,831 k	—	—	—
10.0.0.201	19,503	12 M	8,355	841 k	11,148	12 M	—	—	—
166.62.111.64	15,728	16 M	11,354	15 M	4,374	321 k	—	—	—
10.11.11.200	7,536	3,911 k	3,912	399 k	3,624	3,511 k	—	—	—
10.6.12.203	7,410	5,574 k	2,567	399 k	4,843	5,175 k	—	—	—
23.43.62.169	6,934	7,045 k	4,652	6,920 k	2,282	124 k	—	—	—
10.11.11.179	5,806	3,215 k	2,942	320 k	2,864	2,894 k	—	—	—
64.187.66.143	4,883	3,637 k	2,648	3,492 k	2,235	144 k	—	—	—
5.101.51.151	4,326	4,246 k	3,262	4,177 k	1,064	68 k	—	—	—
10.11.11.11	4,139	700 k	1,712	274 k	2,427	426 k	—	—	—
10.11.11.217	4,037	1,954 k	2,094	238 k	1,943	1,715 k	—	—	—
151.101.50.208	3,270	2,220 k	1,657	2,108 k	1,613	112 k	—	—	—
10.6.12.12	2,852	700 k	1,332	329 k	1,520	371 k	—	—	—
10.6.12.157	2,408	809 k	1,231	285 k	1,177	524 k	—	—	—

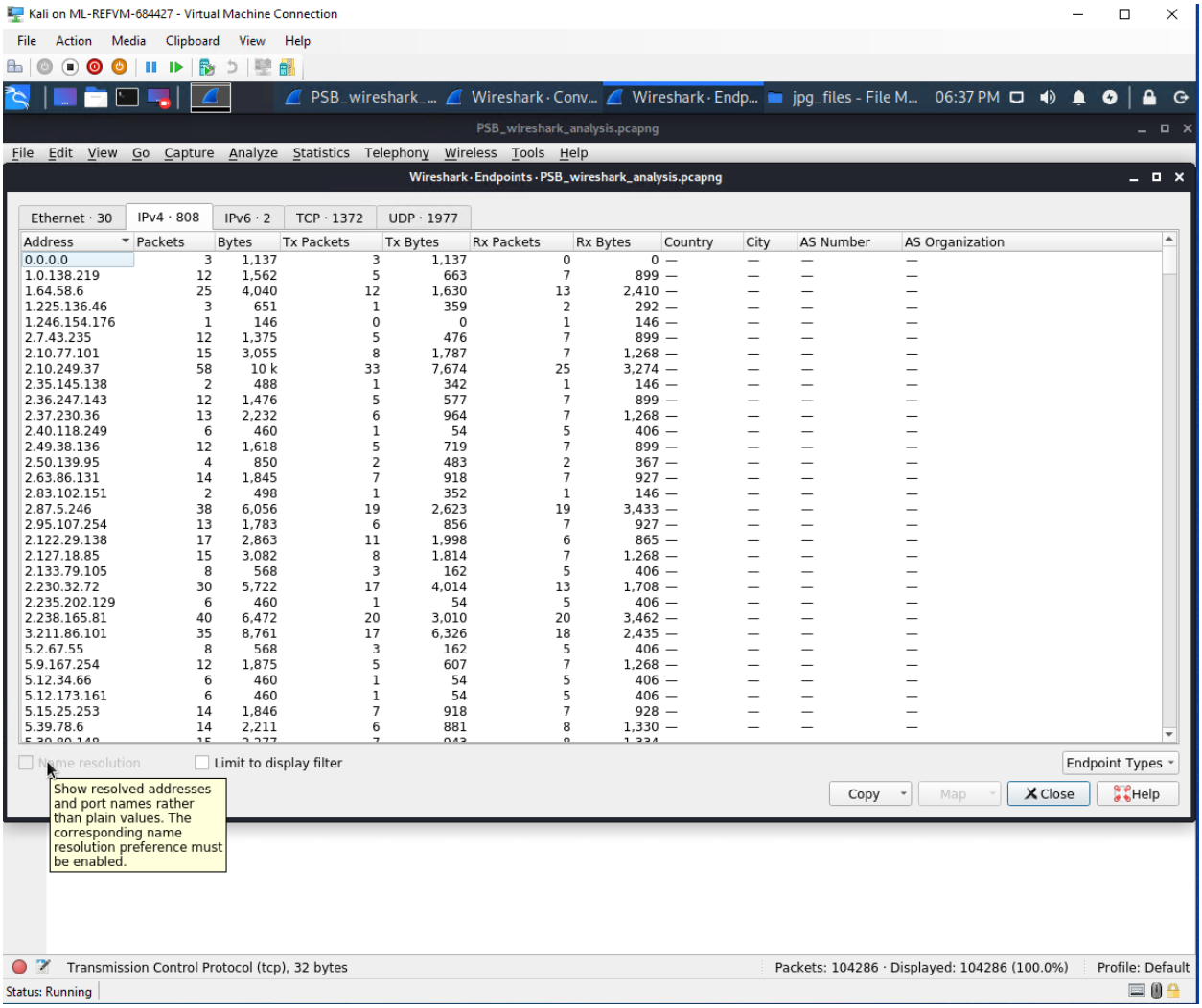
Wireshark · Endpoints · PSB_wireshark_analysis.pcapng

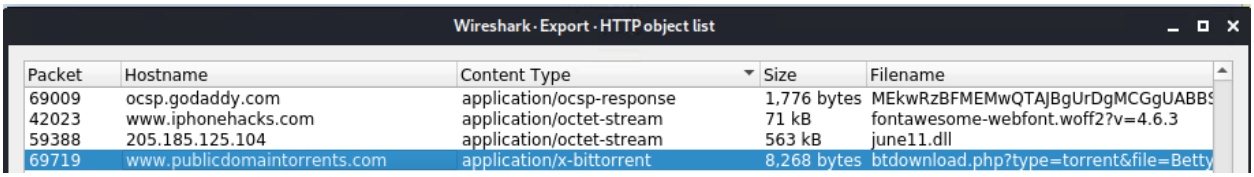
Ethernet · 30 | IPv4 · 808 | IPv6 · 2 | TCP · 1372 | UDP · 1977

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country
Rotterdam-PC.mind-hammer.net	51,364	45 M	21,973	10 M	29,391	34 M	—
b5689023.green.mattingsolutions.co	30,344	26 M	15,195	16 M	15,149	9,831 k	—
BLANCO-DESKTOP.dogoftheyear.net	19,503	12 M	8,355	841 k	11,148	12 M	—
mysocalledchaos.com	15,728	16 M	11,354	15 M	4,374	321 k	—
Gilbert-Win7-PC.okay-boomer.info	7,536	3,911 k	3,912	399 k	3,624	3,511 k	—
LAPTOP-5WKHX9YG.frank-n-ted.com	7,410	5,574 k	2,567	399 k	4,843	5,175 k	—
a1449.dscg2.akamai.net	6,934	7,045 k	4,652	6,920 k	2,282	124 k	—
Roger-MacBook-Pro.local	5,806	3,215 k	2,942	320 k	2,864	2,894 k	—
64-187-66-143.iprev.kci.net	4,883	3,637 k	2,648	3,492 k	2,235	144 k	—
snnmnkxdhflwgthqismb.com	4,326	4,246 k	3,262	4,177 k	1,064	68 k	—
okay-boomer-dc.okay-boomer.info	4,139	700 k	1,712	274 k	2,427	426 k	—
10.11.11.217	4,037	1,954 k	2,094	238 k	1,943	1,715 k	—
dualstack.com.imgix.map.fastly.net	3,270	2,220 k	1,657	2,108 k	1,613	112 k	—
Frank-n-Ted-DC.frank-n-ted.com	2,852	700 k	1,332	329 k	1,520	371 k	—
DESKTOP-86J4BX.frank-n-ted.com	2,408	809 k	1,231	285 k	1,177	524 k	—

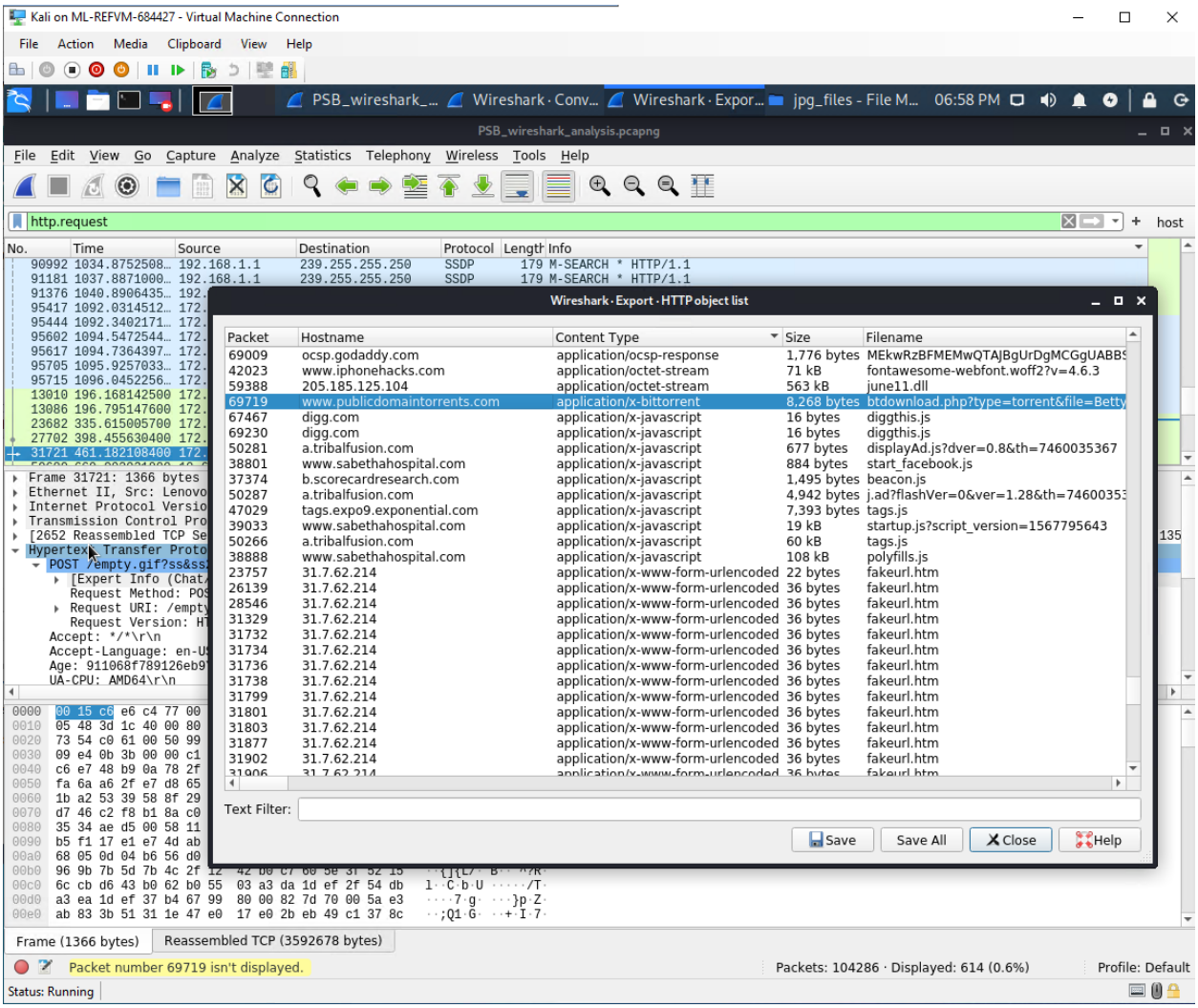

Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
PSB_wireshark_analysi... jpg_files - File Manager 04:55 PM
PSB_wireshark_analysis.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Start capturing packets
host
No. Time Source Destination Protocol Leng Info
50362 610.497756100 pagead46.l.doublecl… 10.11.11.217 HTTP 671 HTTP/1.1 200 OK (text/javascript)
41079 525.912157100 pagead46.l.doublecl… Roger-MacBook-Pro.local HTTP 671 HTTP/1.1 200 OK (text/javascript)
5130 70.329709500 www-googletagmanage… Rotterdam-PC.mind-hammer.net HTTP 669 HTTP/1.1 200 OK (application/javascript)
3869 54.222094800 mysocalledchaos.com Rotterdam-PC.mind-hammer.net HTTP 662 HTTP/1.1 200 OK (text/css)
40265 518.187164500 d3tpapd2bnws9f.clou… Roger-MacBook-Pro.local HTTP 660 HTTP/1.1 200 OK (PNG)
3823 53.678473500 mysocalledchaos.com Rotterdam-PC.mind-hammer.net HTTP 658 HTTP/1.1 200 OK (text/css)
40974 525.104341800 gstaticadssl.l.goog… DESKTOP-B49J3FD.local HTTP 655 HTTP/1.1 200 OK (font/woff2)
39379 511.469809900 pictures.fasthealth… DESKTOP-B49J3FD.local HTTP 652 HTTP/1.1 200 OK (PNG)
42957 543.219874100 iphonehacks.wpengin… 10.11.11.217 HTTP 644 HTTP/1.1 200 OK (JPEG JFIF image)
39792 514.823724200 pictures.fasthealth… DESKTOP-B49J3FD.local HTTP 644 HTTP/1.1 200 OK (PNG)
43214 545.781483100 iphonehacks.wpengin… 10.11.11.217 HTTP 637 HTTP/1.1 200 OK (PNG)
41616 530.883920500 iphonehacks.wpengin… 10.11.11.217 HTTP 637 HTTP/1.1 200 OK (PNG)
12882 195.181075800 mysocalledchaos.com Rotterdam-PC.mind-hammer.net HTTP 637 HTTP/1.1 200 OK (JPEG JFIF image)
Flags: 0x018 (PSH, ACK)
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0xd95e [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (642 bytes)
TCP segment data (642 bytes)
[15 Reassembled TCP Segments (20662 bytes): #69180(1430), #69181(1430), #69183(1430), #69186(1430), #69188(1430), #69190(1430), #69191(1430), #69193(1460),
Hypertext Transfer Protocol
Line-based text data: text/javascript (1 lines)
0020 00 c9 00 50 c2 64 76 e7 10 14 94 97 c8 71 50 18
0030 fa f0 d9 5e 00 00 70 b7 4b 90 e1 9e be 98 93 15
0040 7a 90 15 92 0e 4c d2 42 90 9b ed b4 b2 1e ab 5c
0050 2c 5f be 89 ee d8 66 91 3e 78 48 fb cf f5 55 a6
0060 06 1e 52 a1 3b f5 bd 93 b4 12 59 63 37 75 24 bc
0070 d7 03 b9 76 1a 39 ac 5d c8 03 30 31 b2 b5 75 36
0080 00 0f 7a a6 f1 79 e7 cf 4e d8 5c 3c c0 40 c3 2b
0090 74 bd 9d a1 37 a7 23 6d c0 aa 19 fa 90 71 8a 2f
00a0 b1 3f 6f 24 39 ab af 2b 9e 3b 71 72 6e 39 bd 84
00b0 be c1 c7 d0 73 d1 8d 64 28 45 aa 4d 2e fb 45 60
00c0 bf 35 3c 55 d3 01 2f 12 18 c9 51 cc ba 01 5a ad
00d0 a3 f1 35 7d 9b 26 cd 9b 42 4d a6 99 78 46 14 72
00e0 37 c3 70 55 cb 8a d3 15 7f 8d 0f 8e e1 05 59 a6
00f0 df 79 d2 3a a7 10 4d 63 c2 0c f0 1c b3 69 9a 88
0100 8f 93 39 39 73 fd 9e e3 3d 0f ed d6 c1 03 76 e7
Frame (696 bytes)
Reassembled TCP (20662 bytes)
Uncompressed entity body (52979 bytes)
Transmission Control Protocol (tcp), 20 bytes
Packets: 104286 · Displayed: 361 (0.3%)
Profile: Default
Status: Running


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
PSB_wireshark_analysi... jpg_files - File Manager 06:30 PM
PSB_wireshark_analysis.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 1
host
No. Time Source Destination Protocol Leng Info
82018 900.682107600 10.0.0.201 177.1.173.218 TCP 66 [TCP Retransmission] 49952 → 51413 [SYN] Seq=0 Win=64
81888 899.372731900 10.0.0.201 177.1.173.218 TCP 66 [TCP Retransmission] 49952 → 51413 [SYN] Seq=0 Win=64
3100 48.973550500 10.0.0.201 177.1.173.218 TCP 66 [TCP Retransmission] 49952 → 51413 [SYN] Seq=0 Win=64
2969 47.664188400 10.0.0.201 177.1.173.218 TCP 66 49952 → 51413 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS
Acknowledgment number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....1. = Syn: Set
[Expert Info (Chat/Sequence): Connection establish request (SYN): server port 51413]
....0 = Fin: Not set
[TCP Flags: ·····S·]
0000 00 09 b7 27 a1 3e 00 16 17 18 66 c8 08 00 45 00
0010 00 34 3f a3 40 00 80 06 51 7c 0a 00 00 c9 b1 01
0020 ad da c3 20 c8 d5 89 74 e9 60 00 00 00 00 80 02
0030 fa f0 0b af 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
Transmission Control Protocol (tcp), 32 bytes
Packets: 104286 · Displayed: 4 (0.0%)
Profile: Default
Status: Running

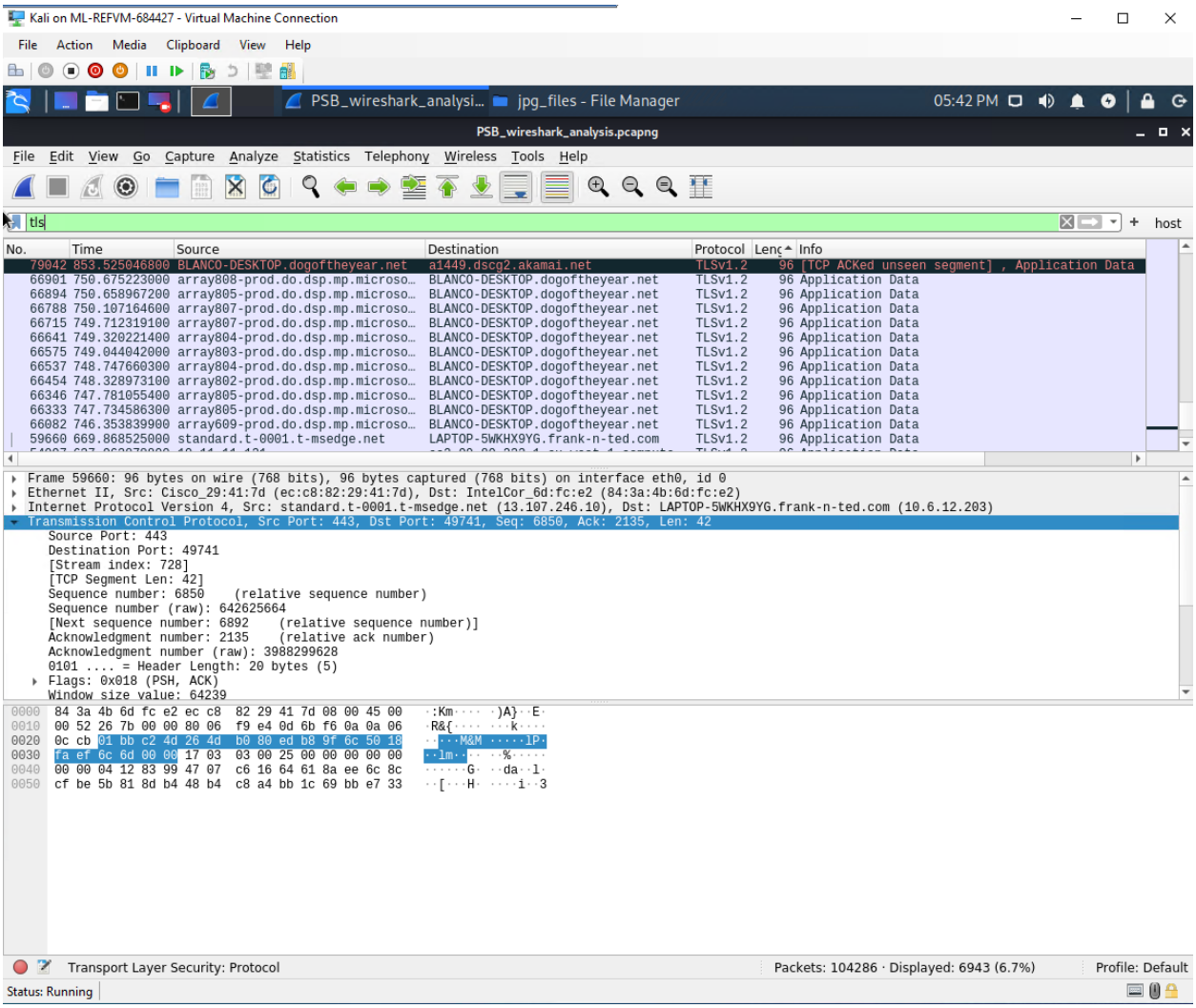




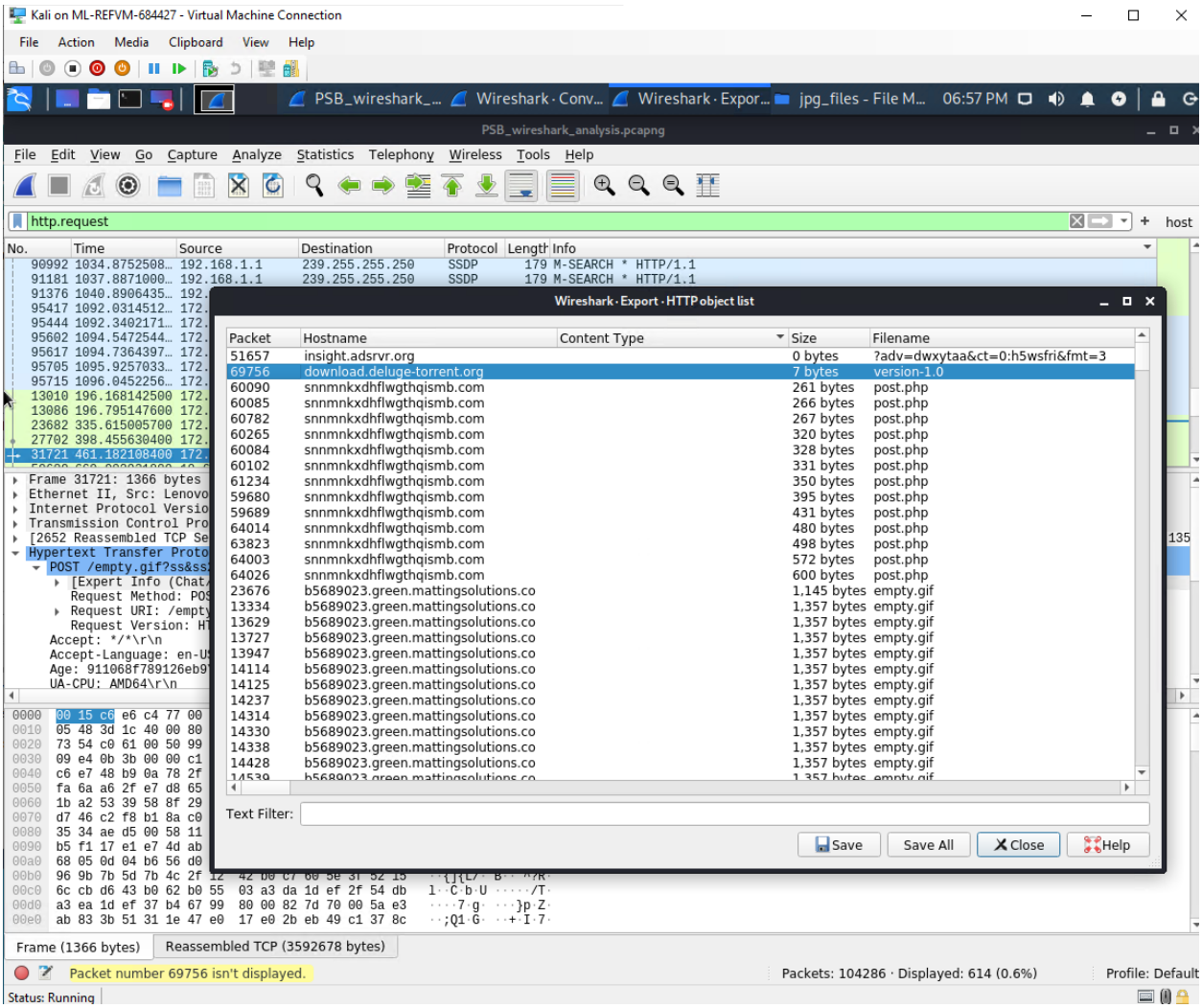
Wireshark_bittorrent.png



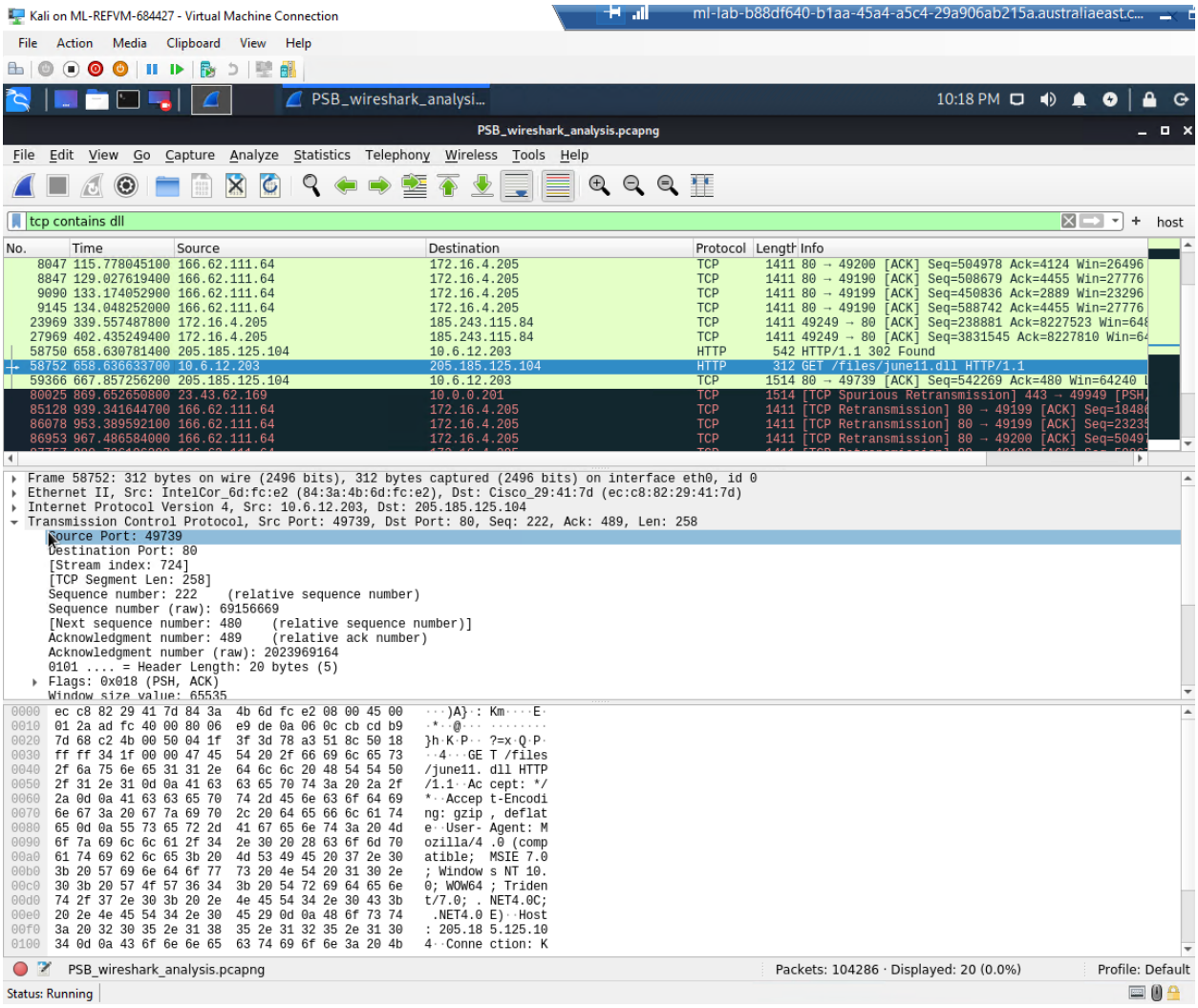
Wireshark_bittorrent1.png



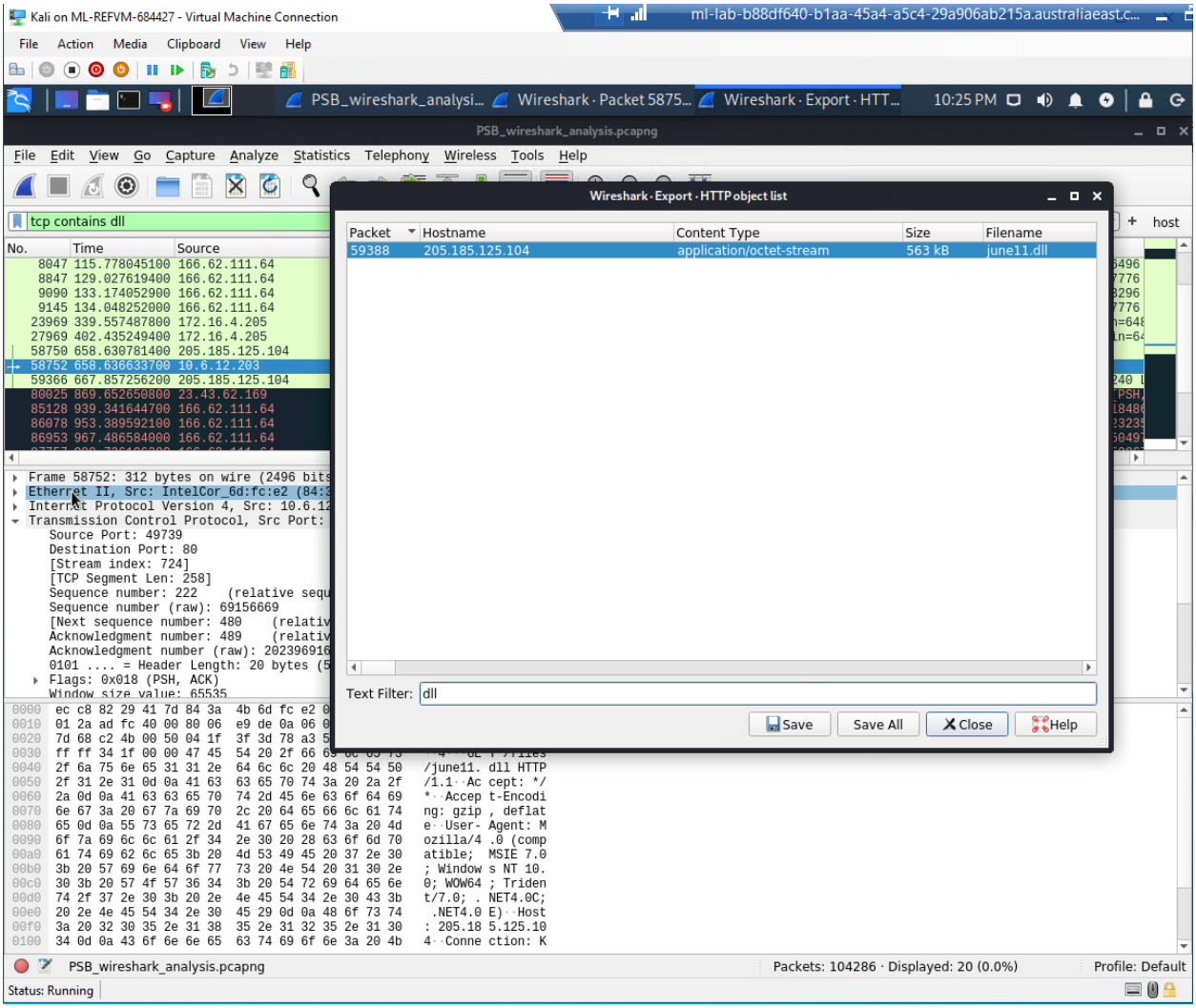
Wireshark_BLANCODESKTOP.png



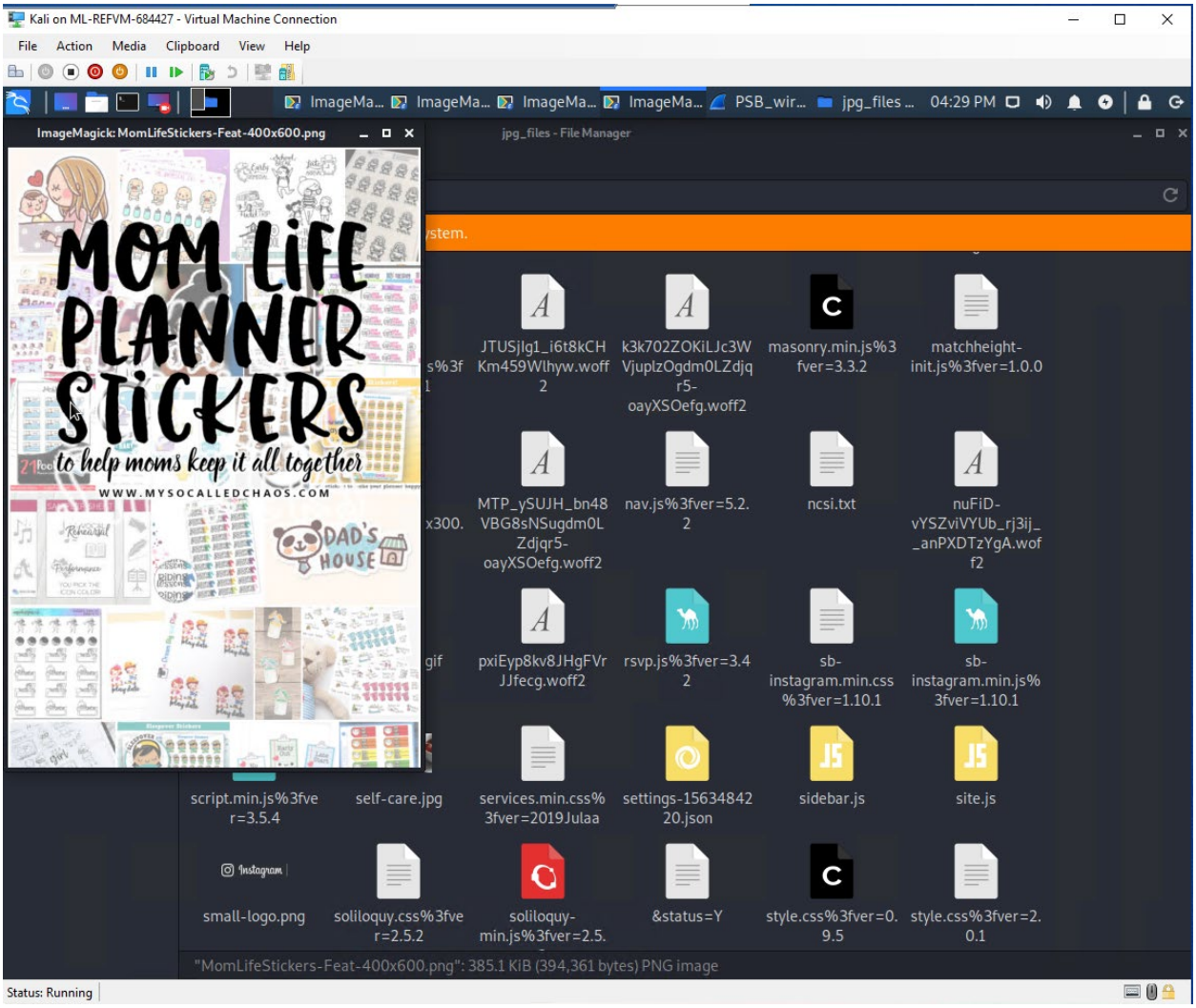
Wireshark_deluge_torrent.org.png



Wireshark_dll_file_to_test1

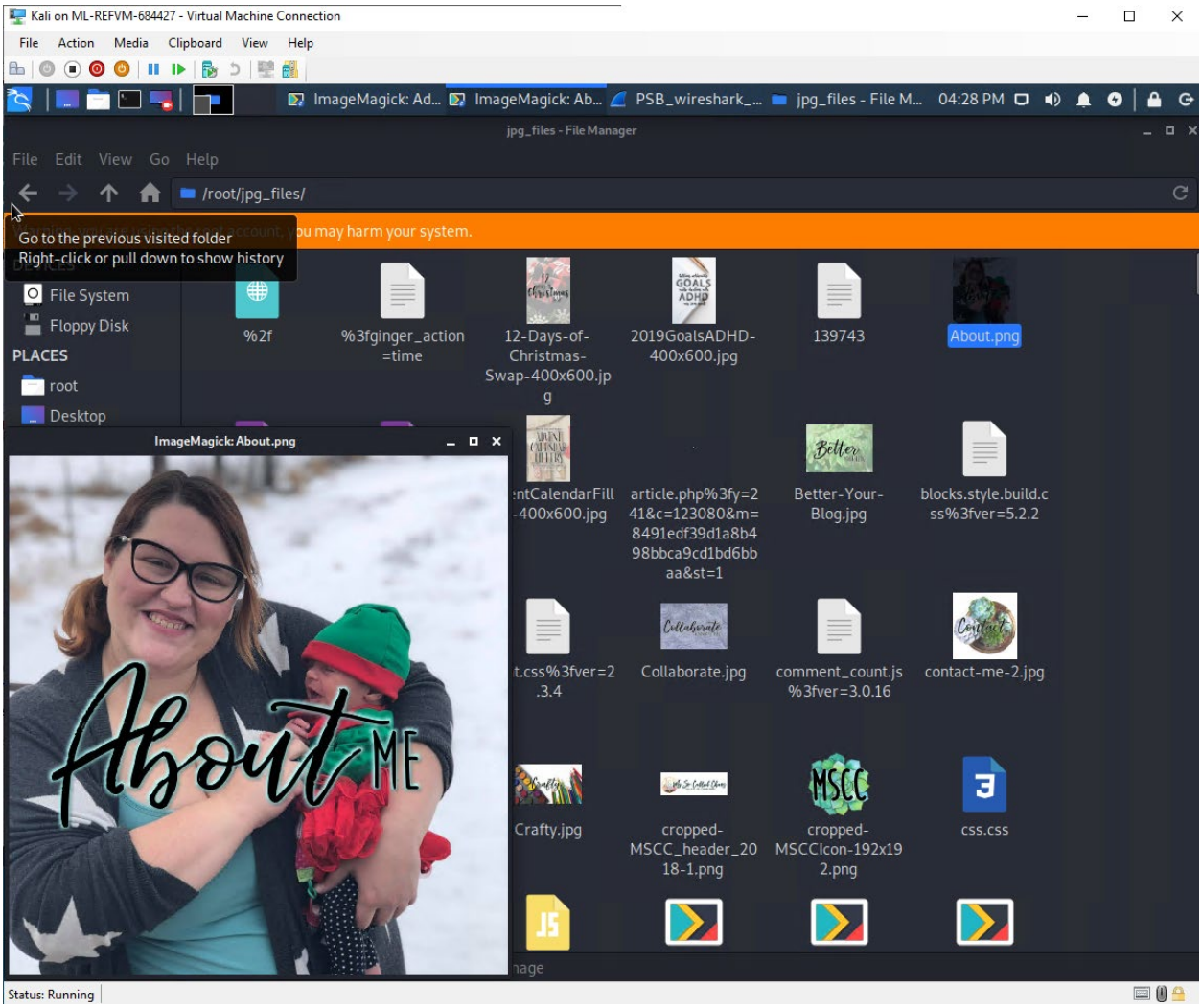


Wireshark_dll_file_to_test2

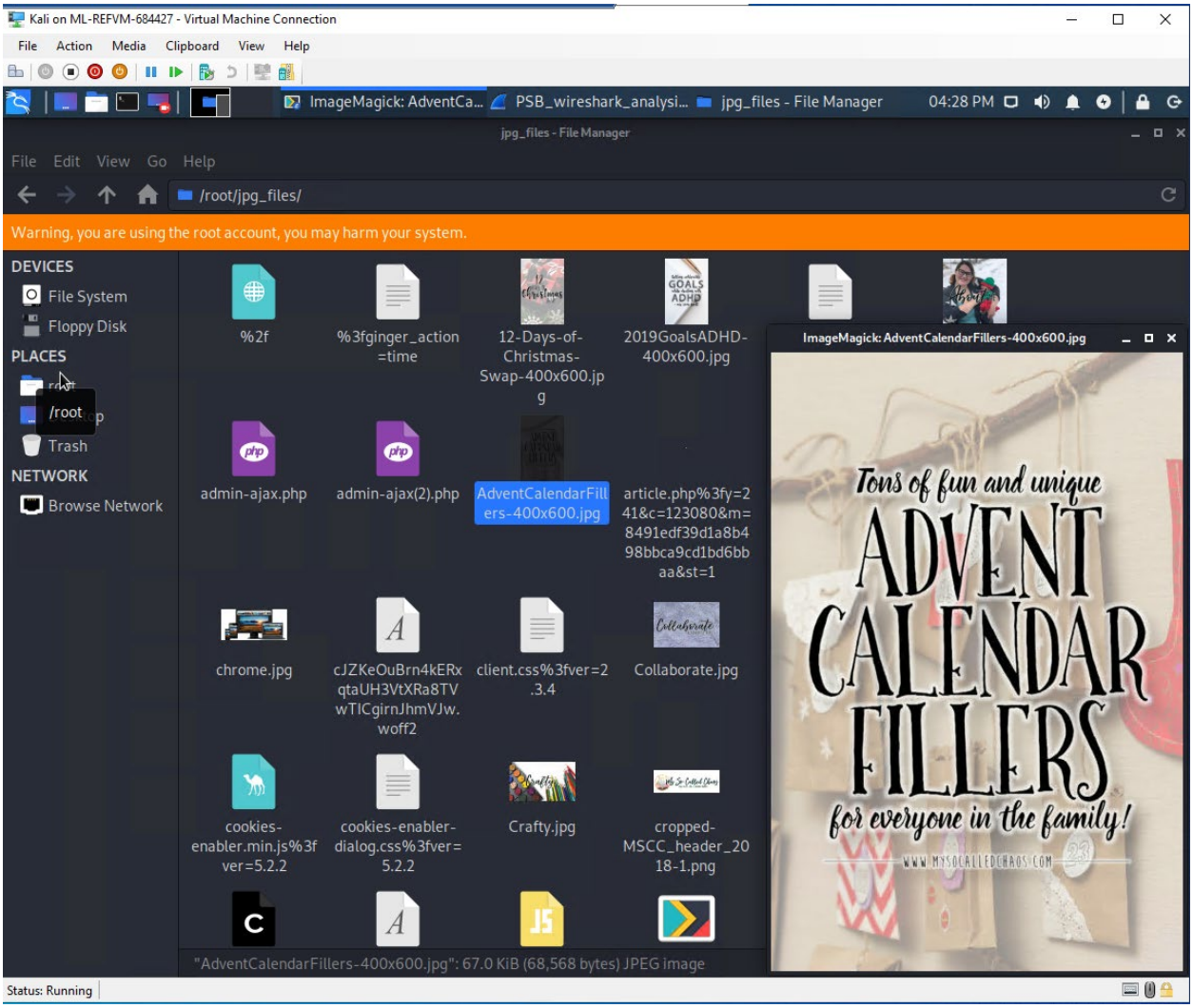


Wireshark_html_evidence1

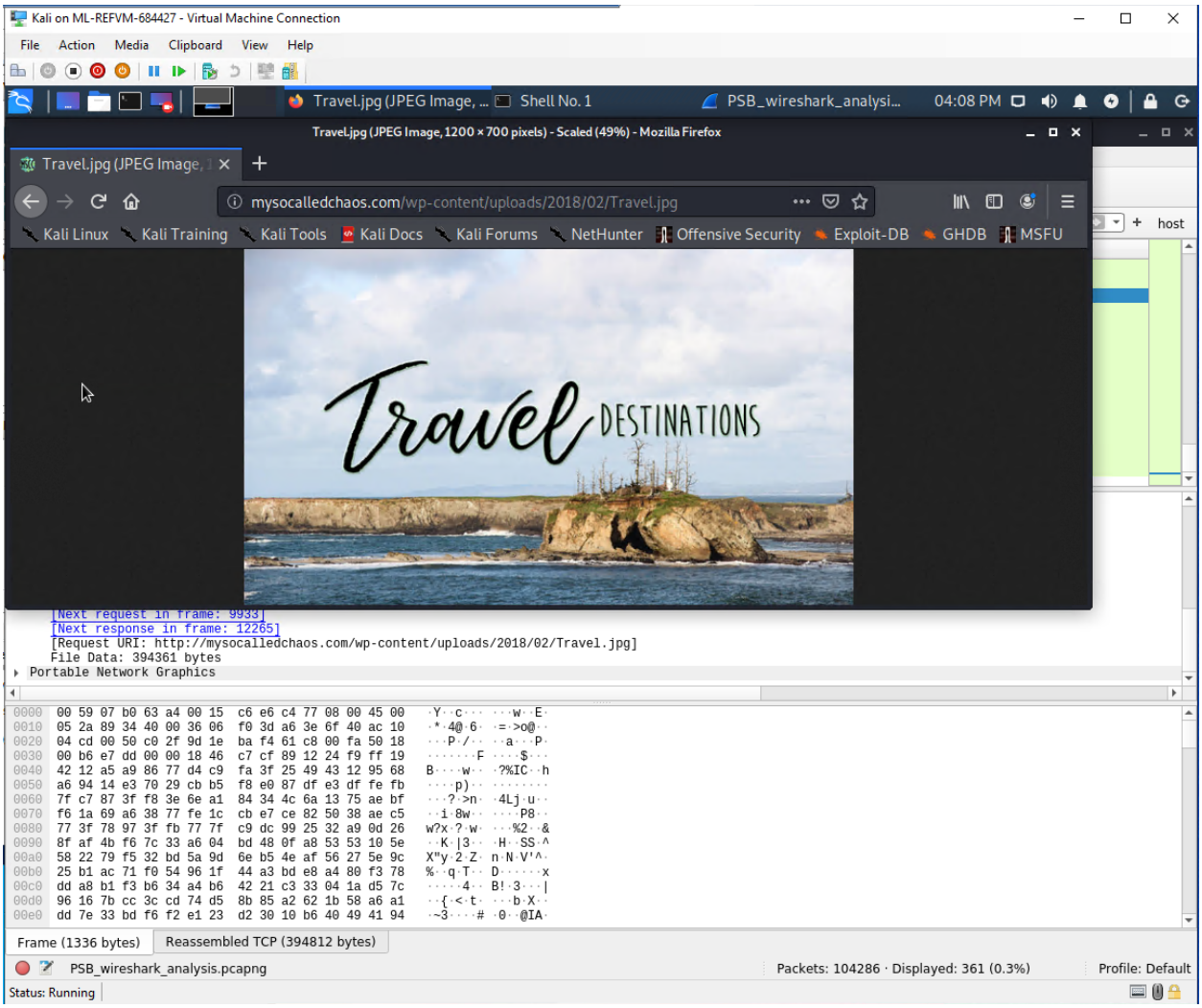
Wireshark_html_evidence2



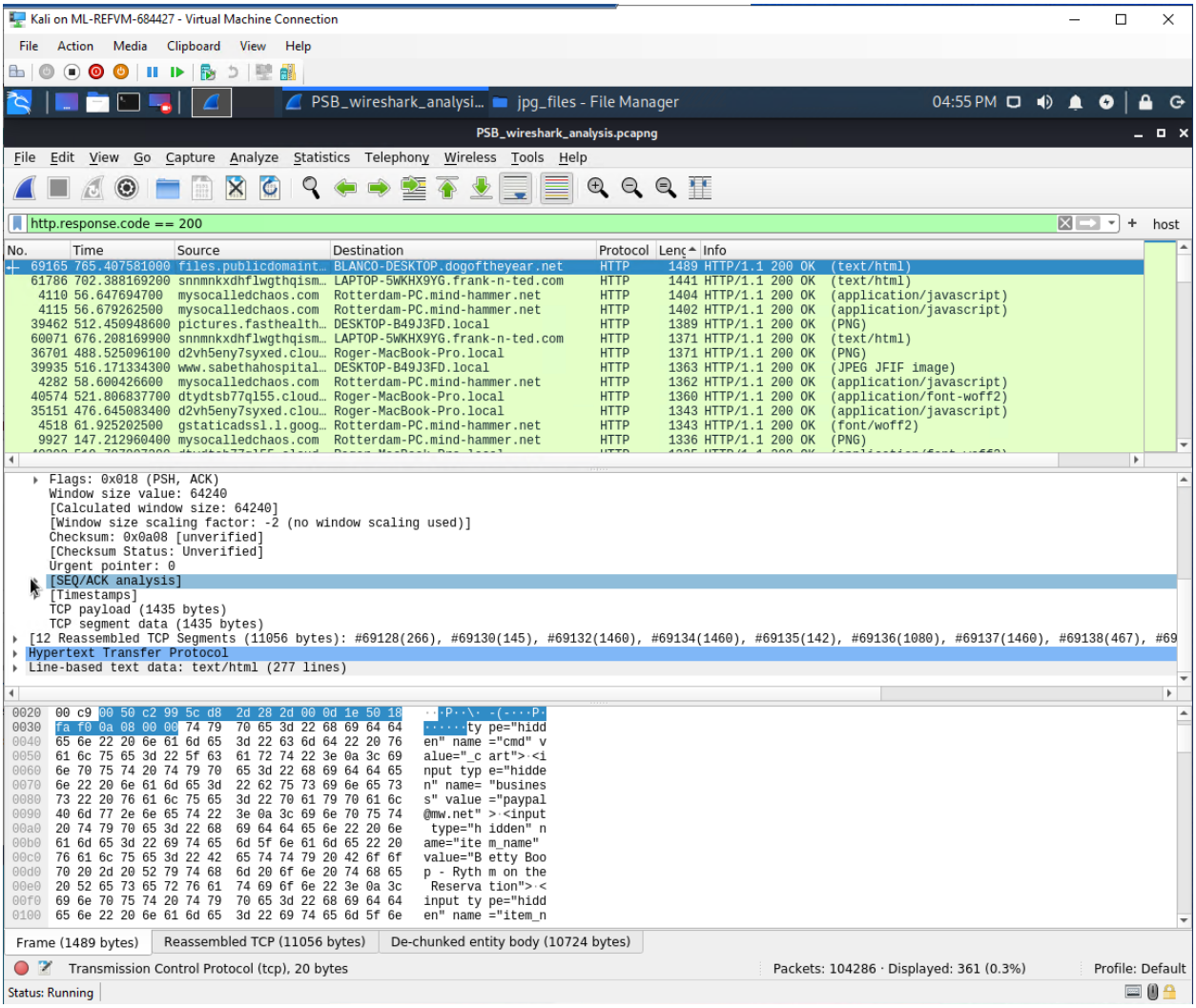
Wireshark_html_evidence3



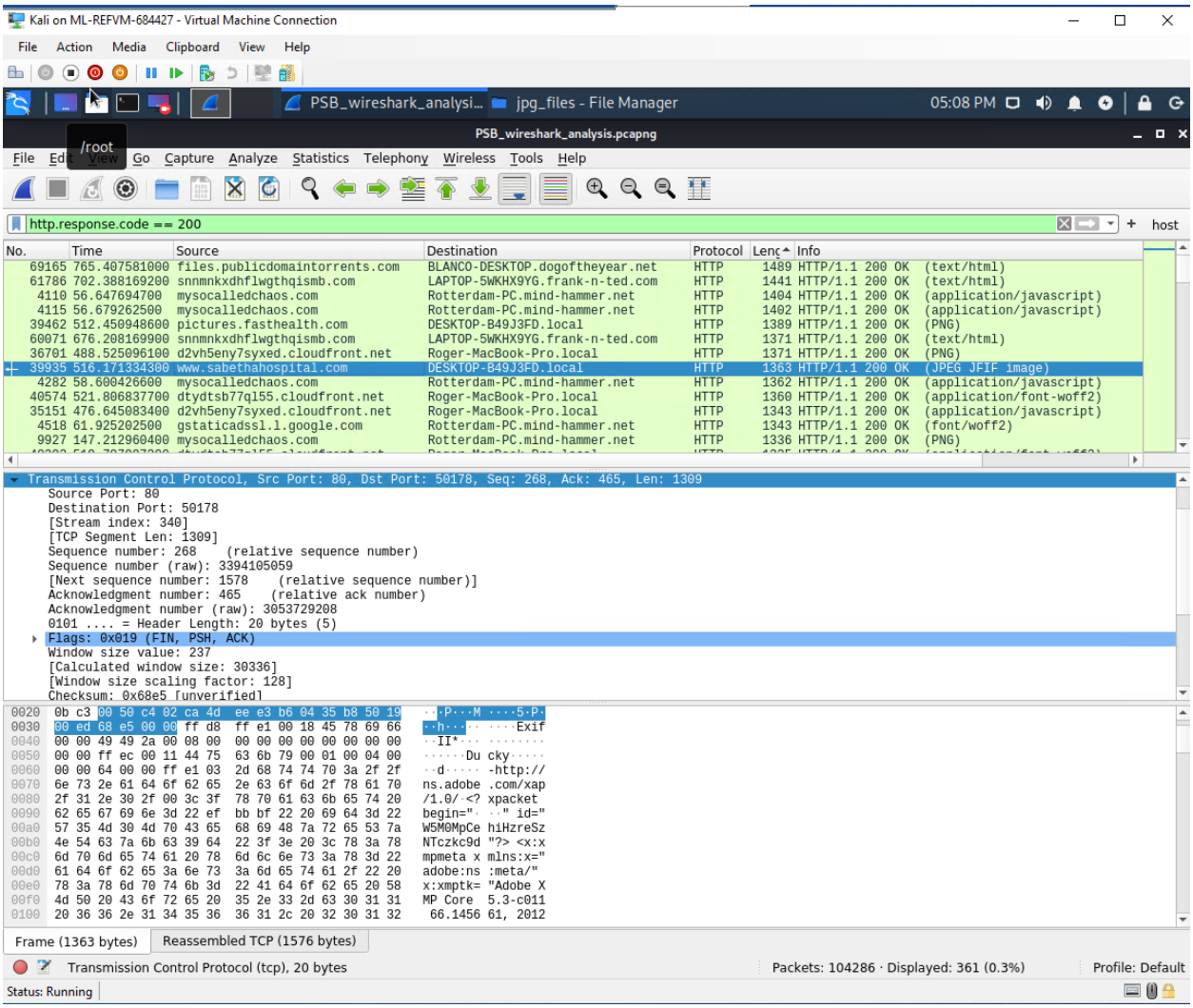
Wireshark_html_evidence4



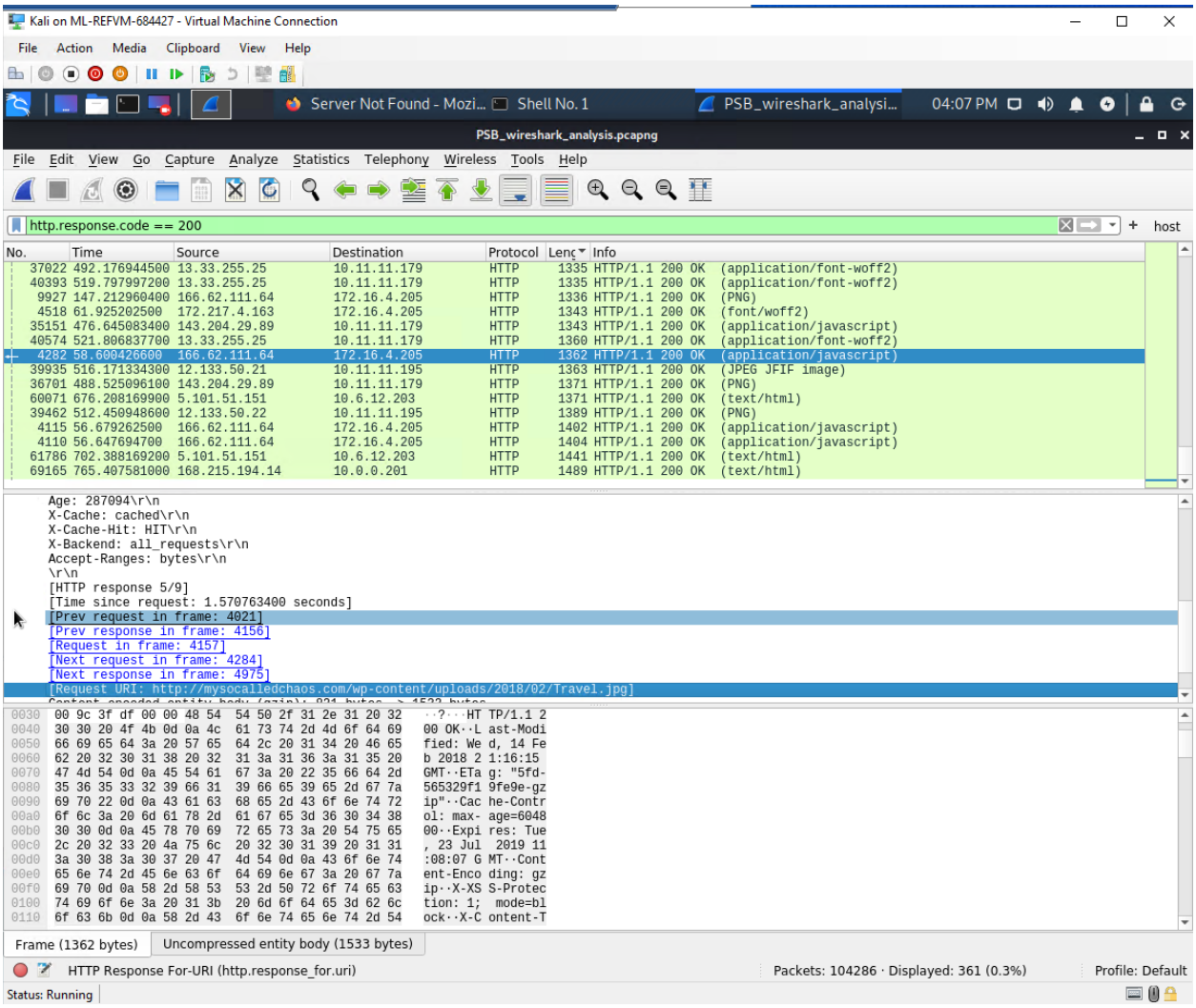
Wireshark_html_evidence5



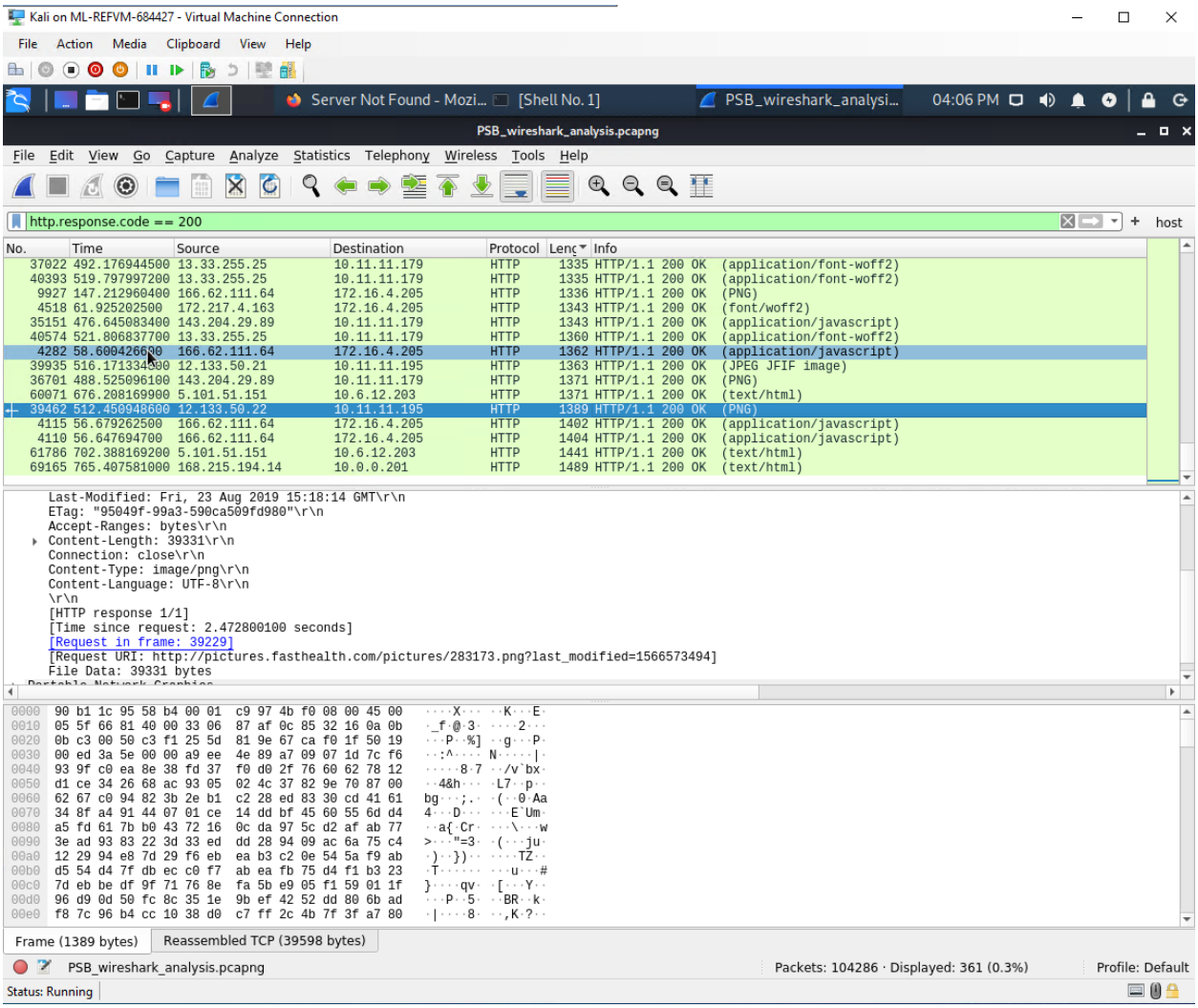
Wireshark_http200a



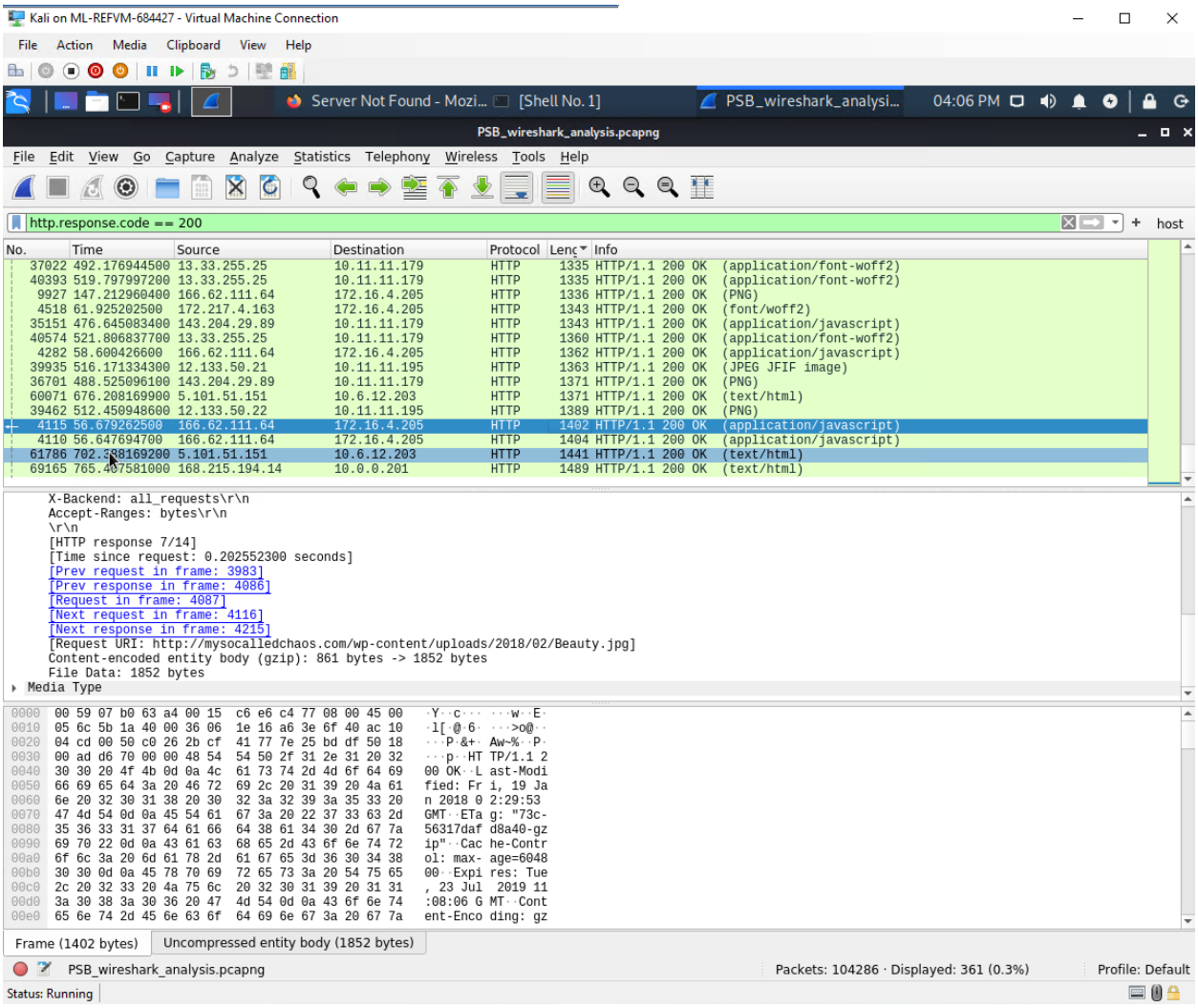
Wireshark_http200b



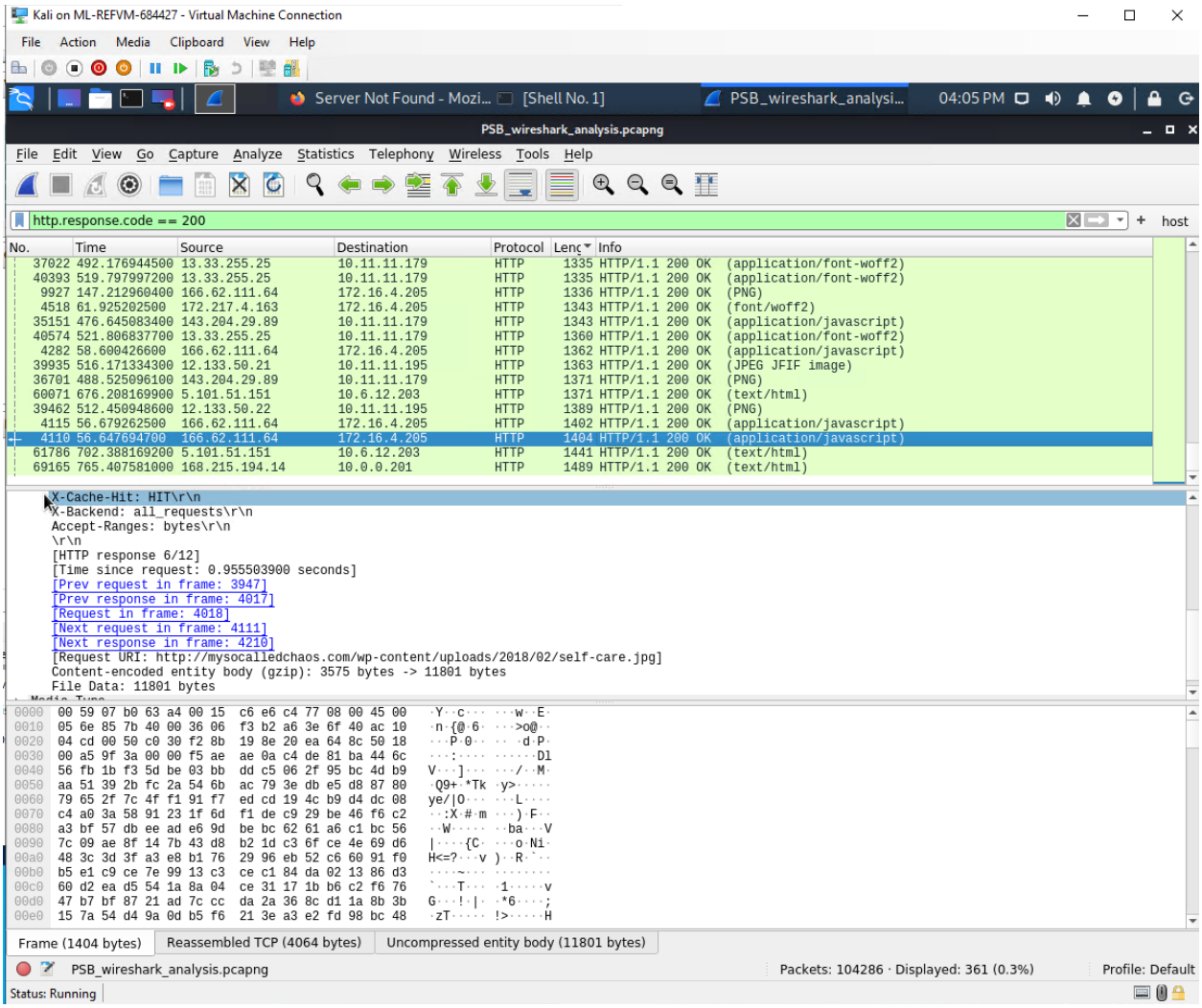
Wireshark_http200c



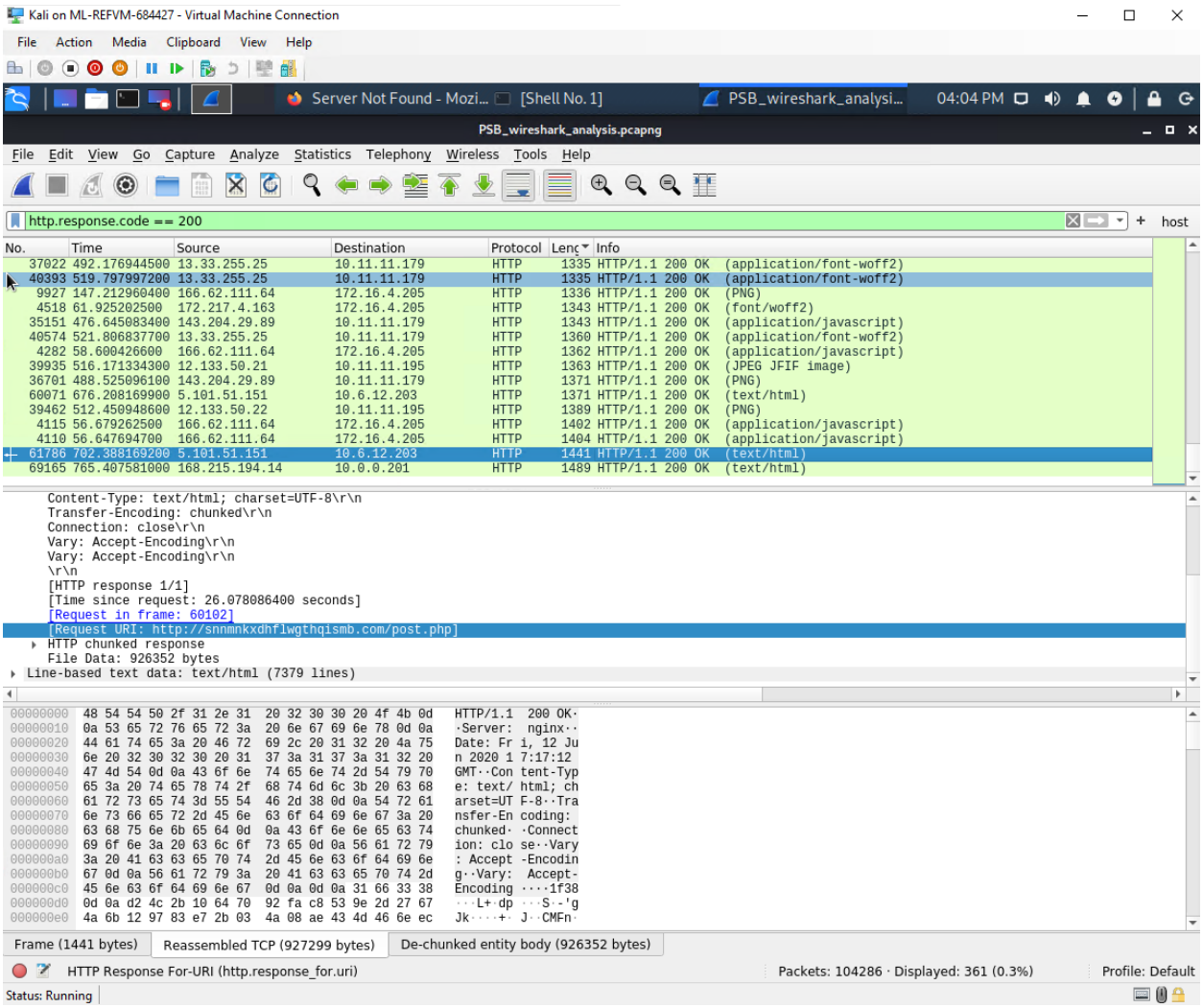
Wireshark_http200d



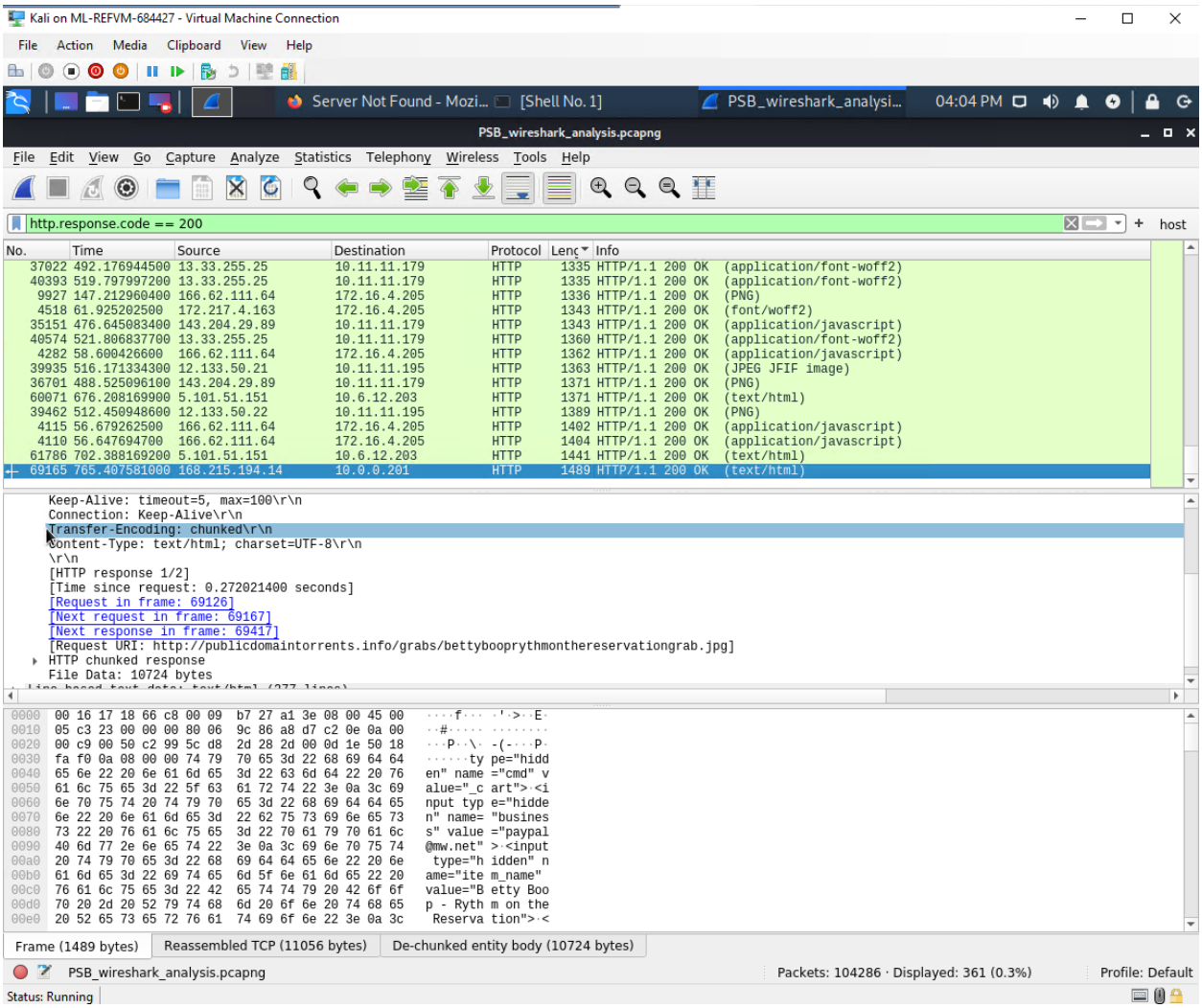
Wireshark_http200e



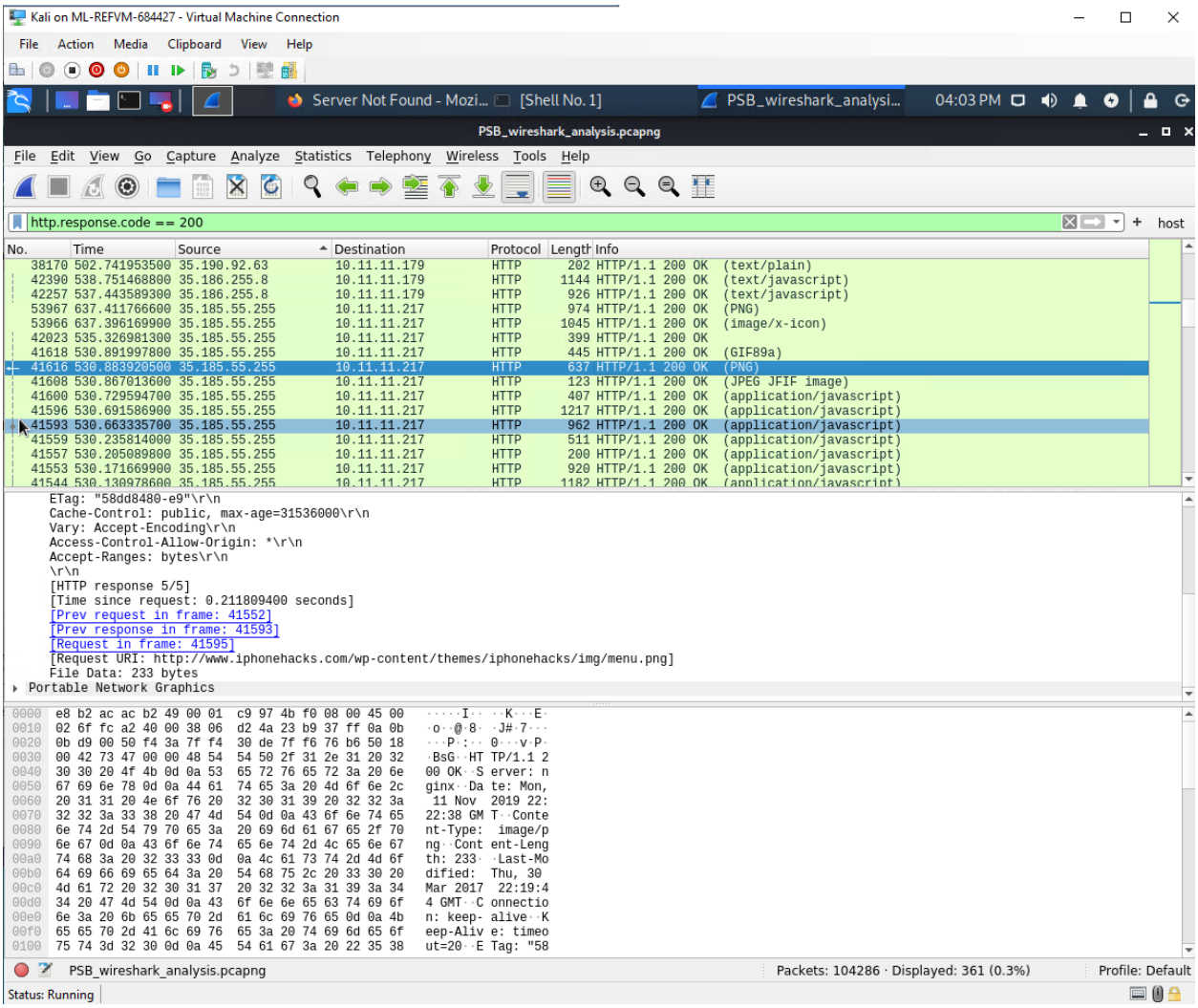
Wireshark_http200f



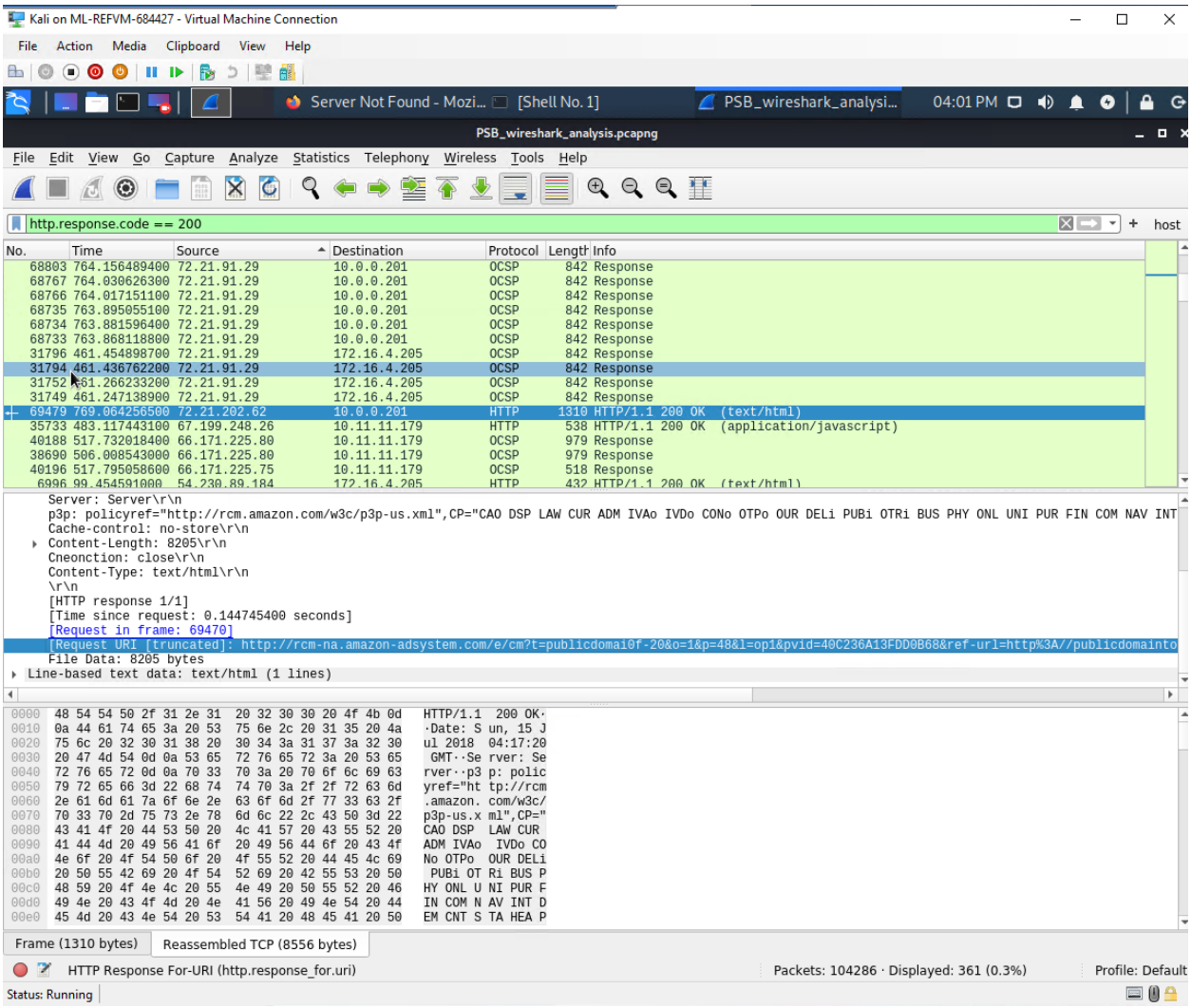
Wireshark_http200g



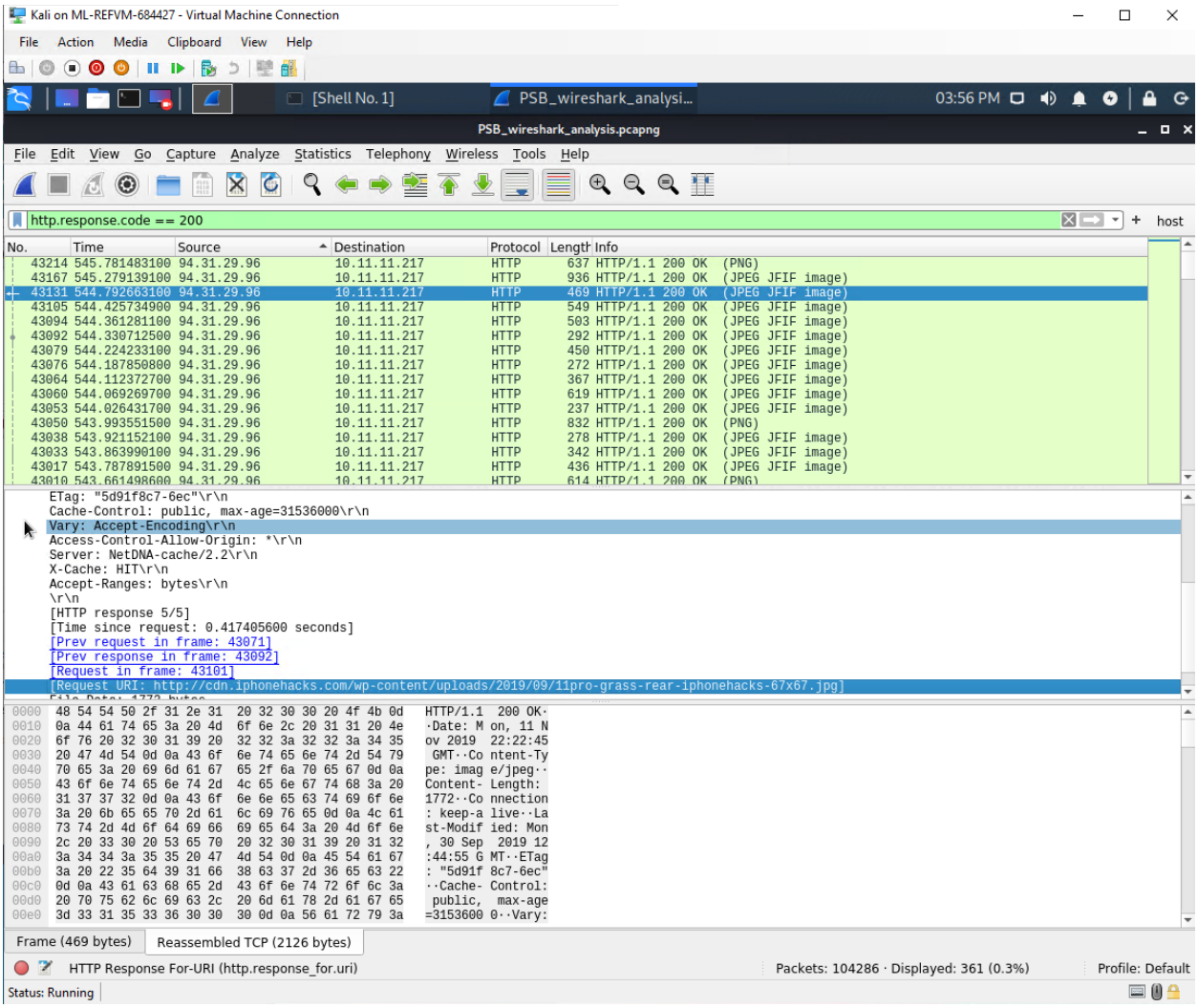
Wireshark_http200h



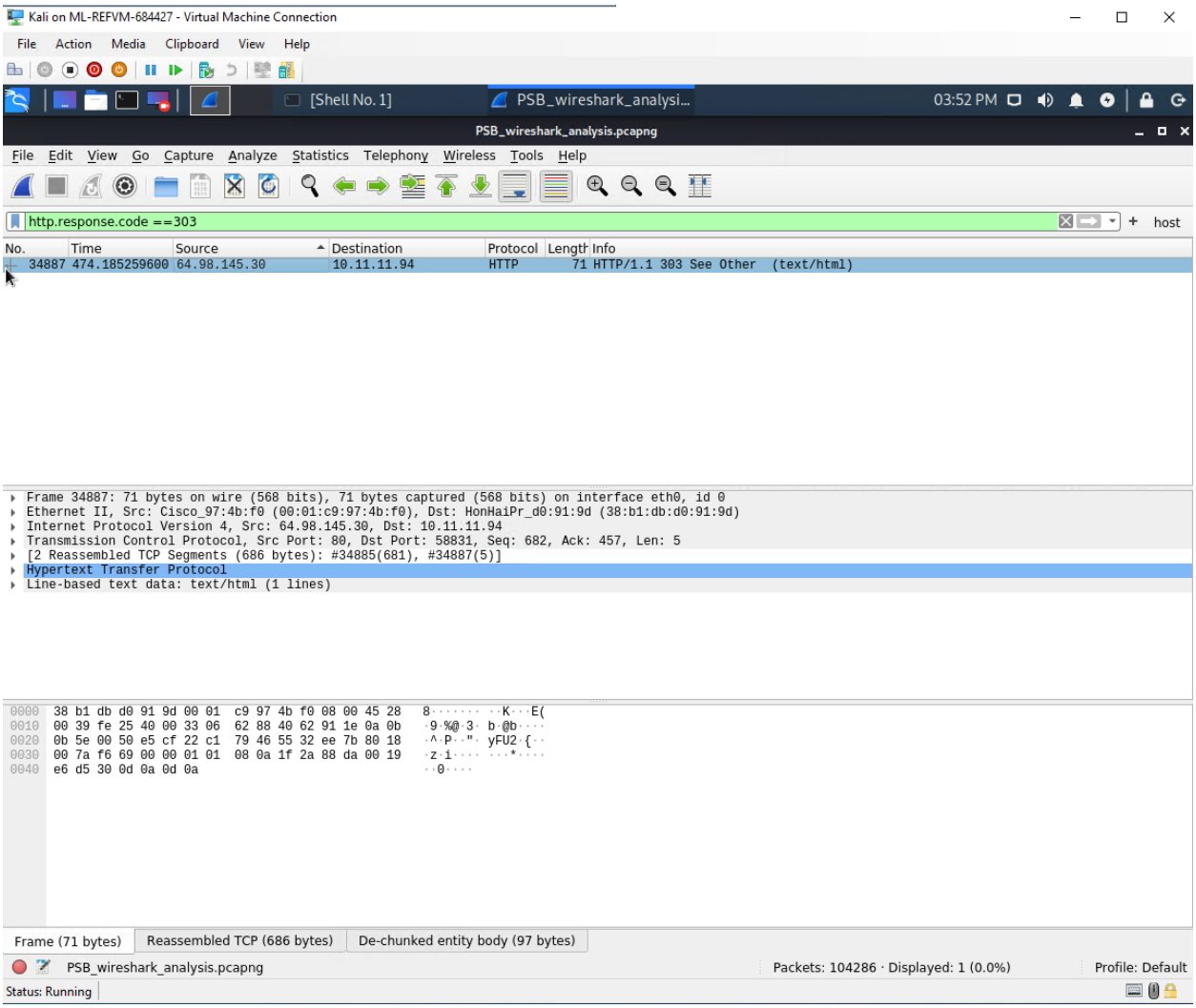
Wireshark_http200i



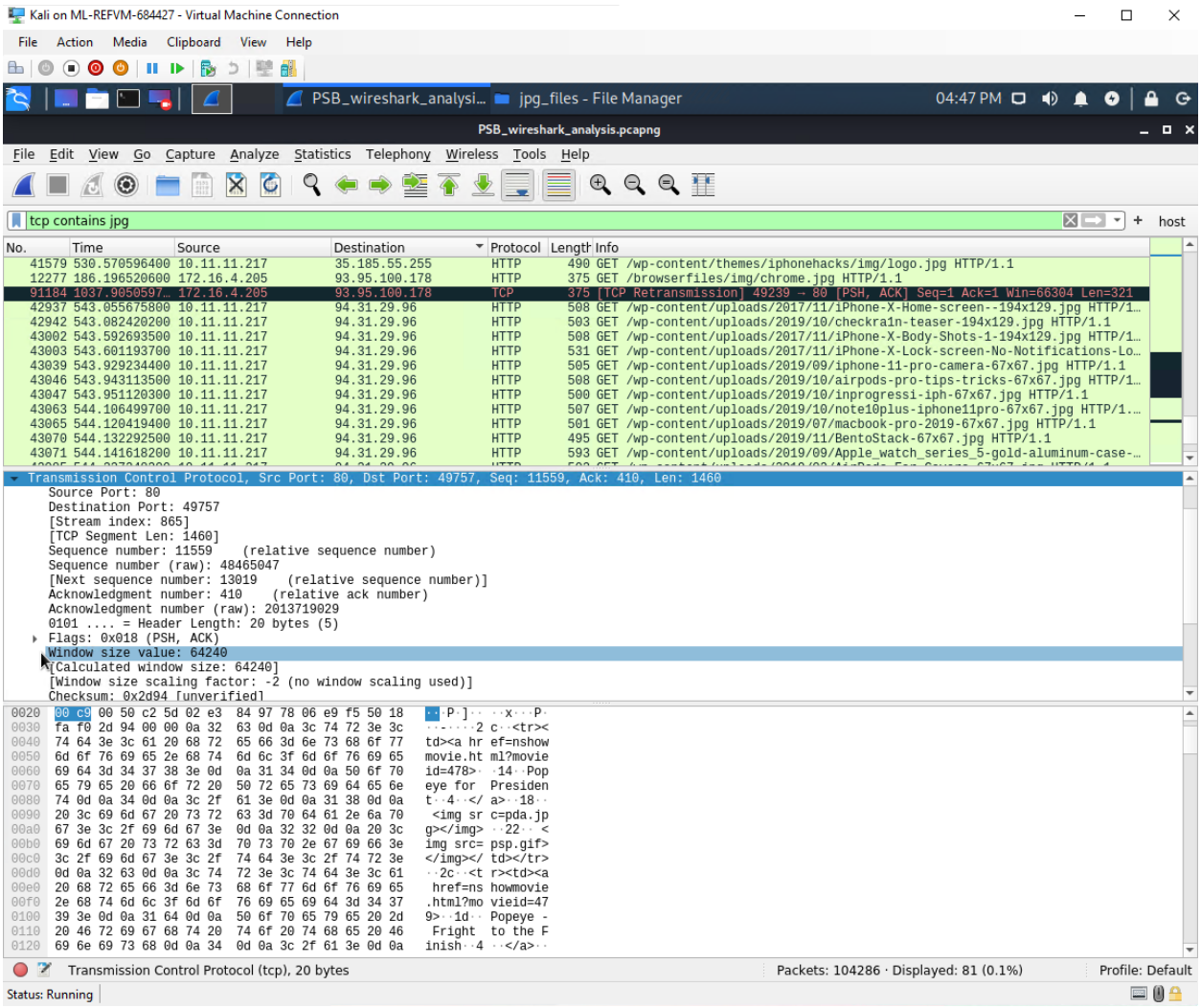
Wireshark_http200j



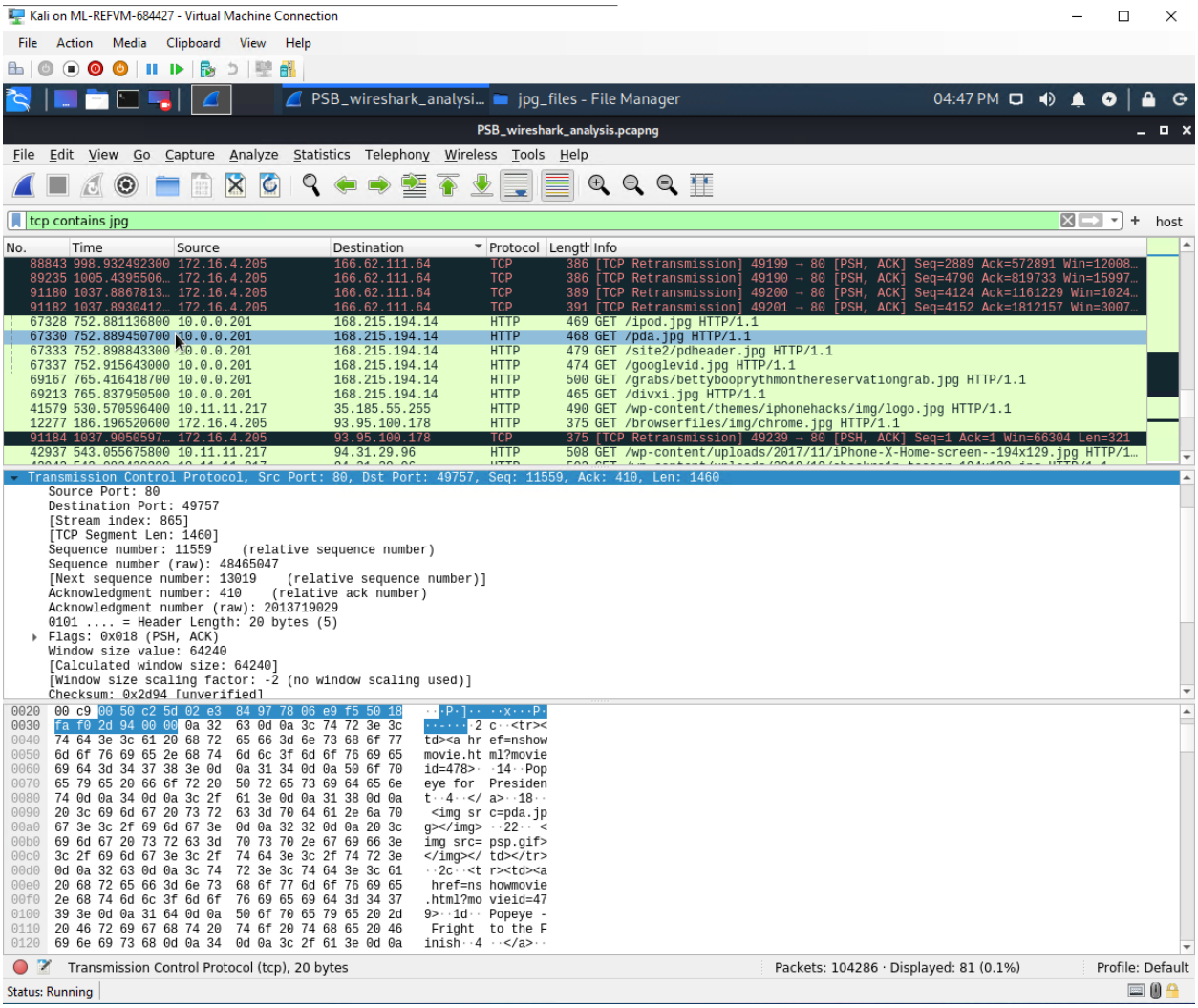
Wireshark_http200k



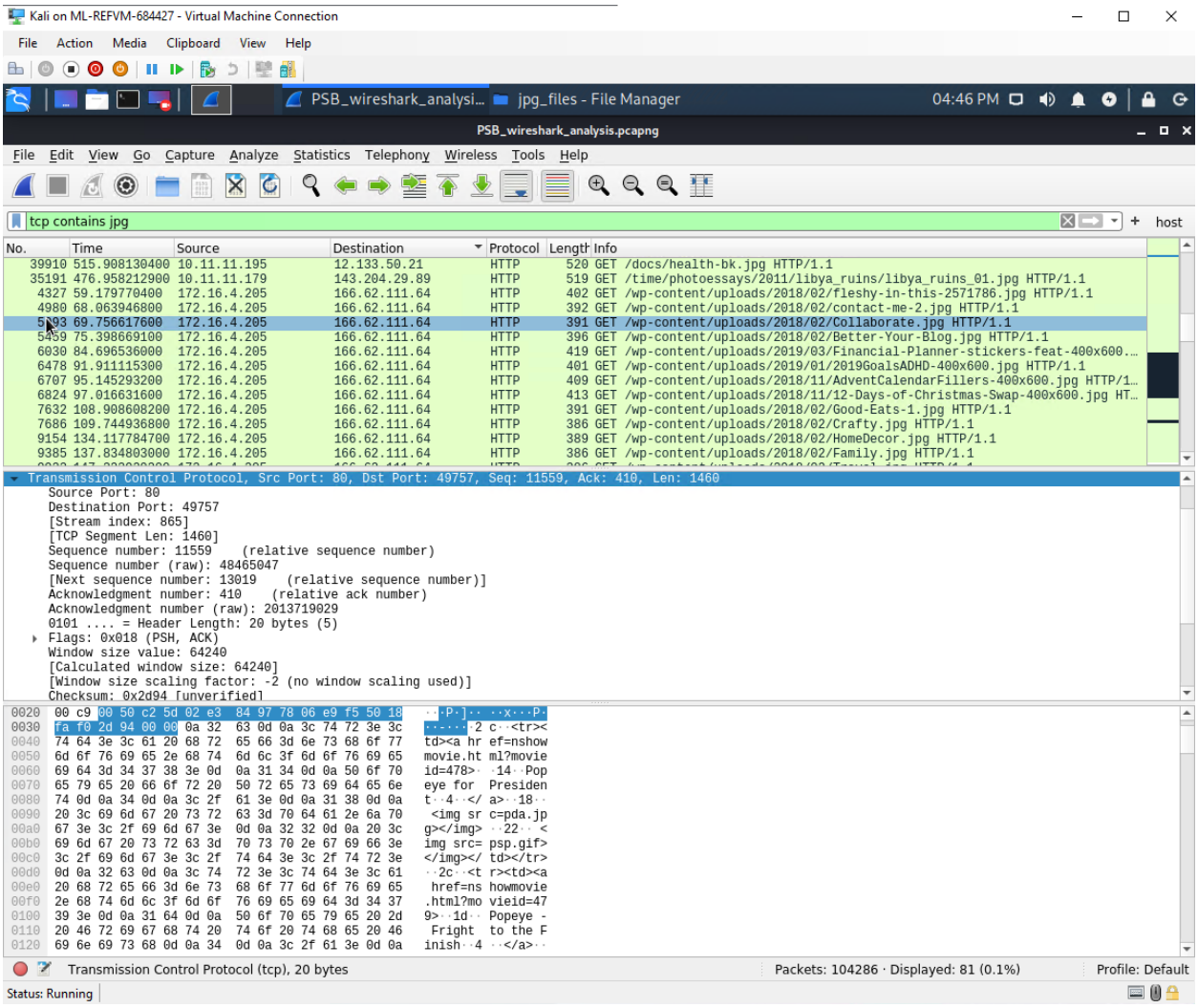
Wireshark_http303a



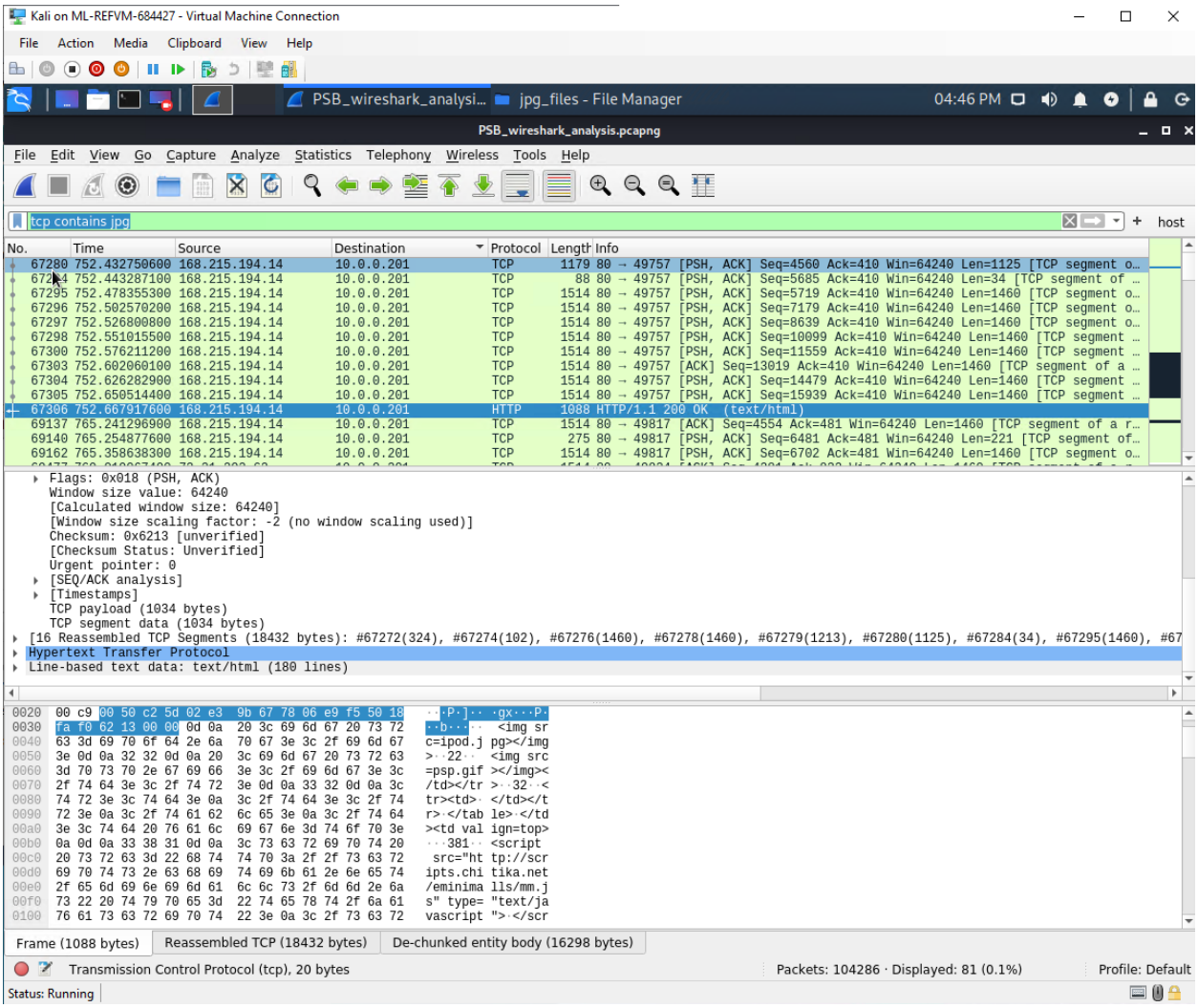
Wireshark_jpg1



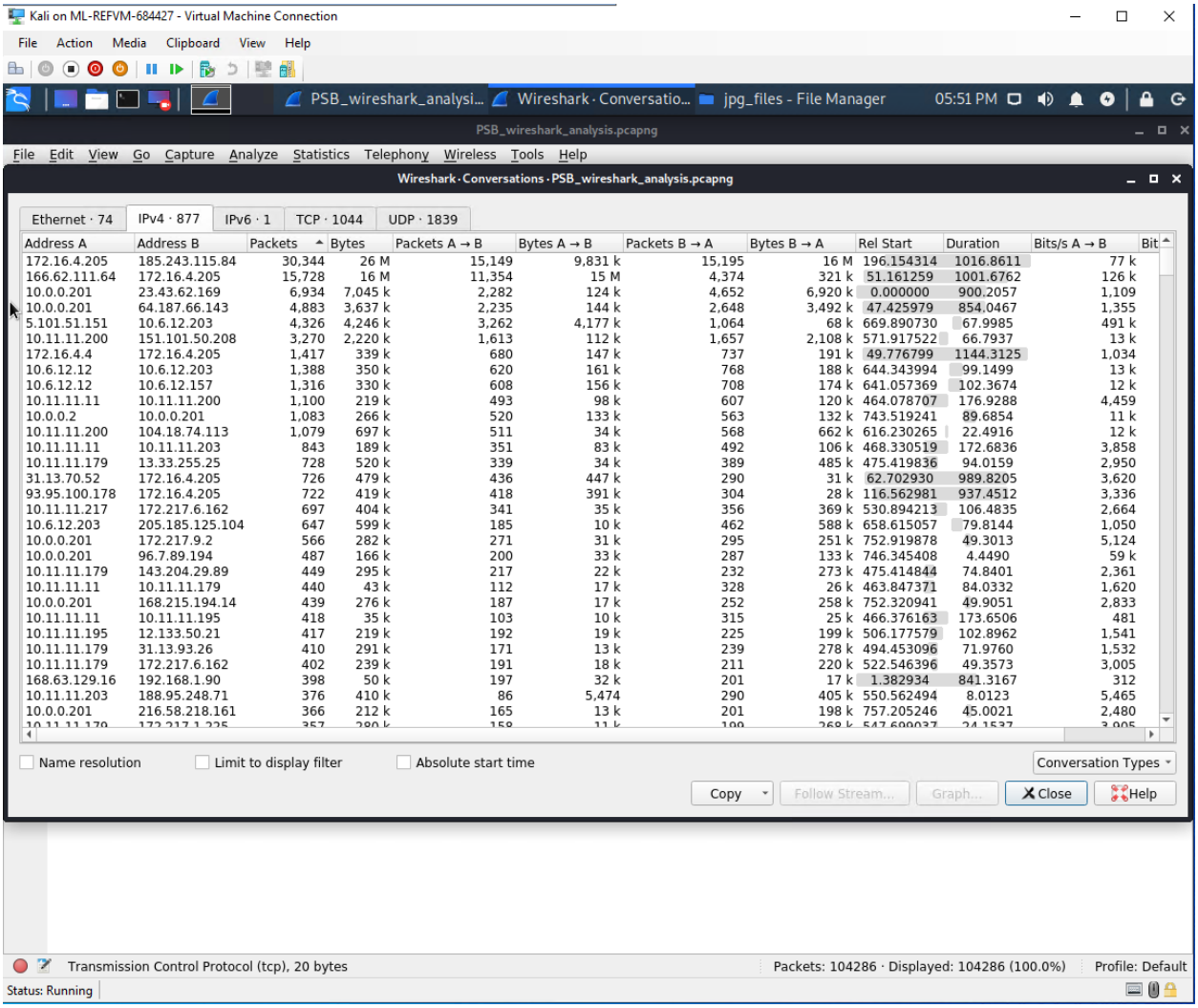
Wireshark_jpg2



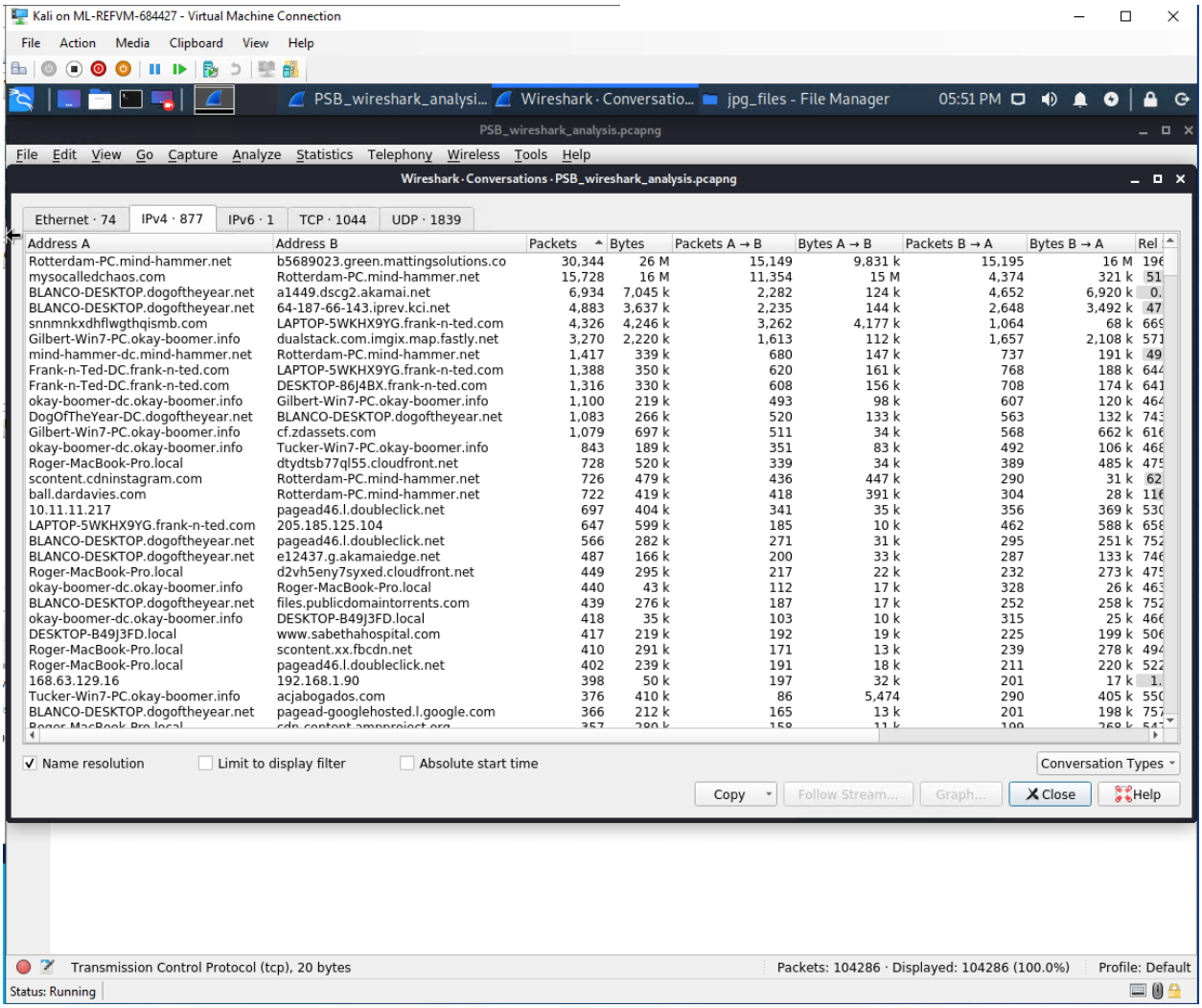
Wireshark_jpg3



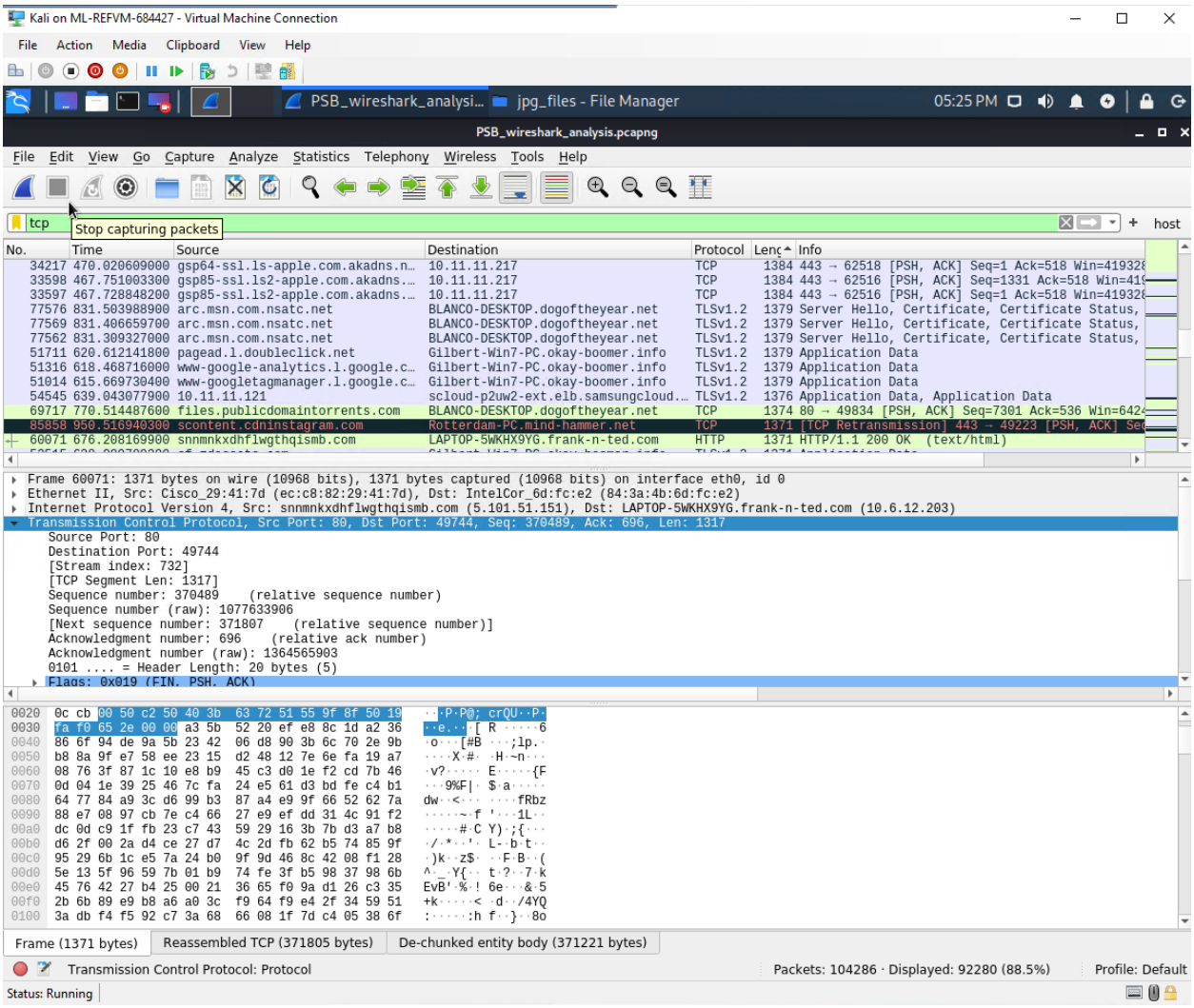
Wireshark_jpg4



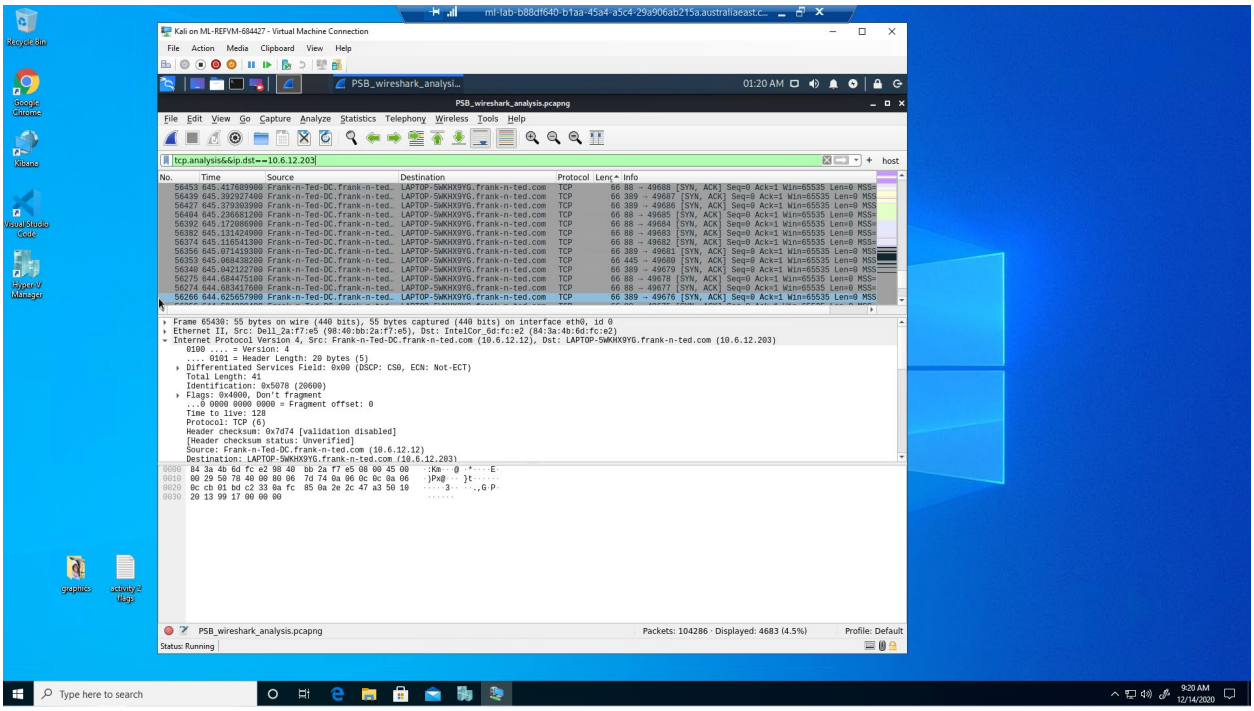
Wireshark_most_active_IP1



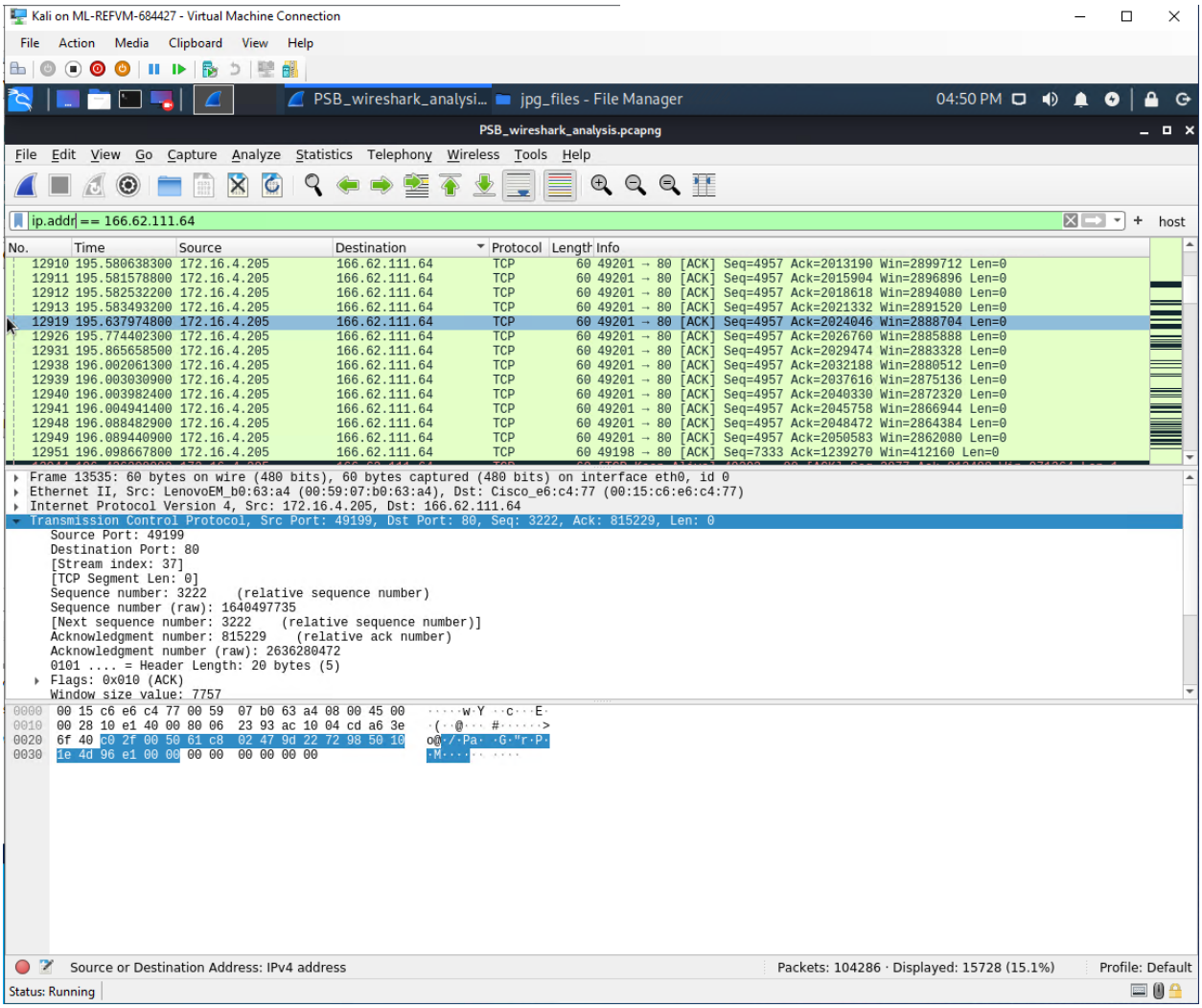
Wireshark_most_active_IP2



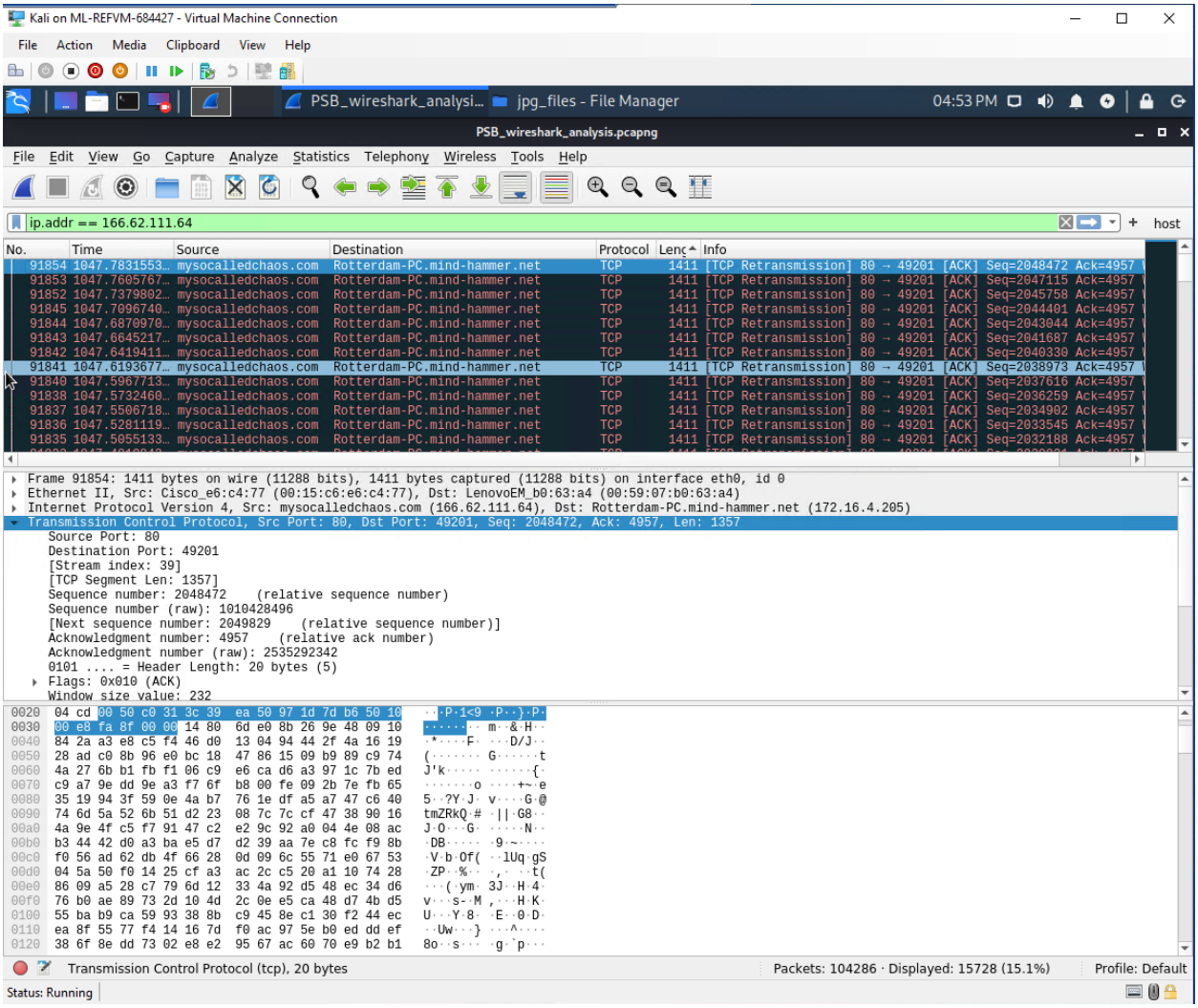
Wireshark_tcp



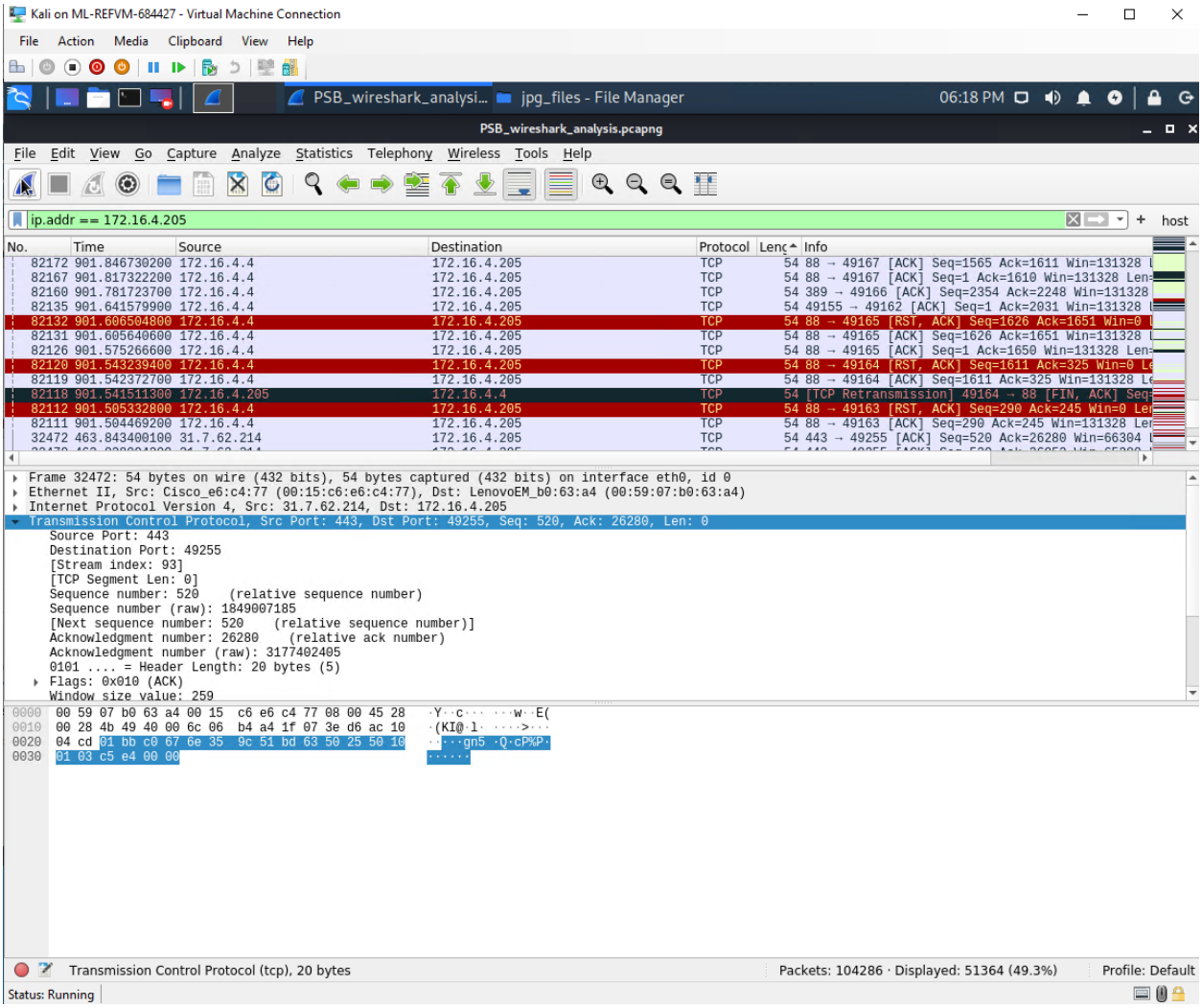
Wireshark_tcp_10.6.12.203



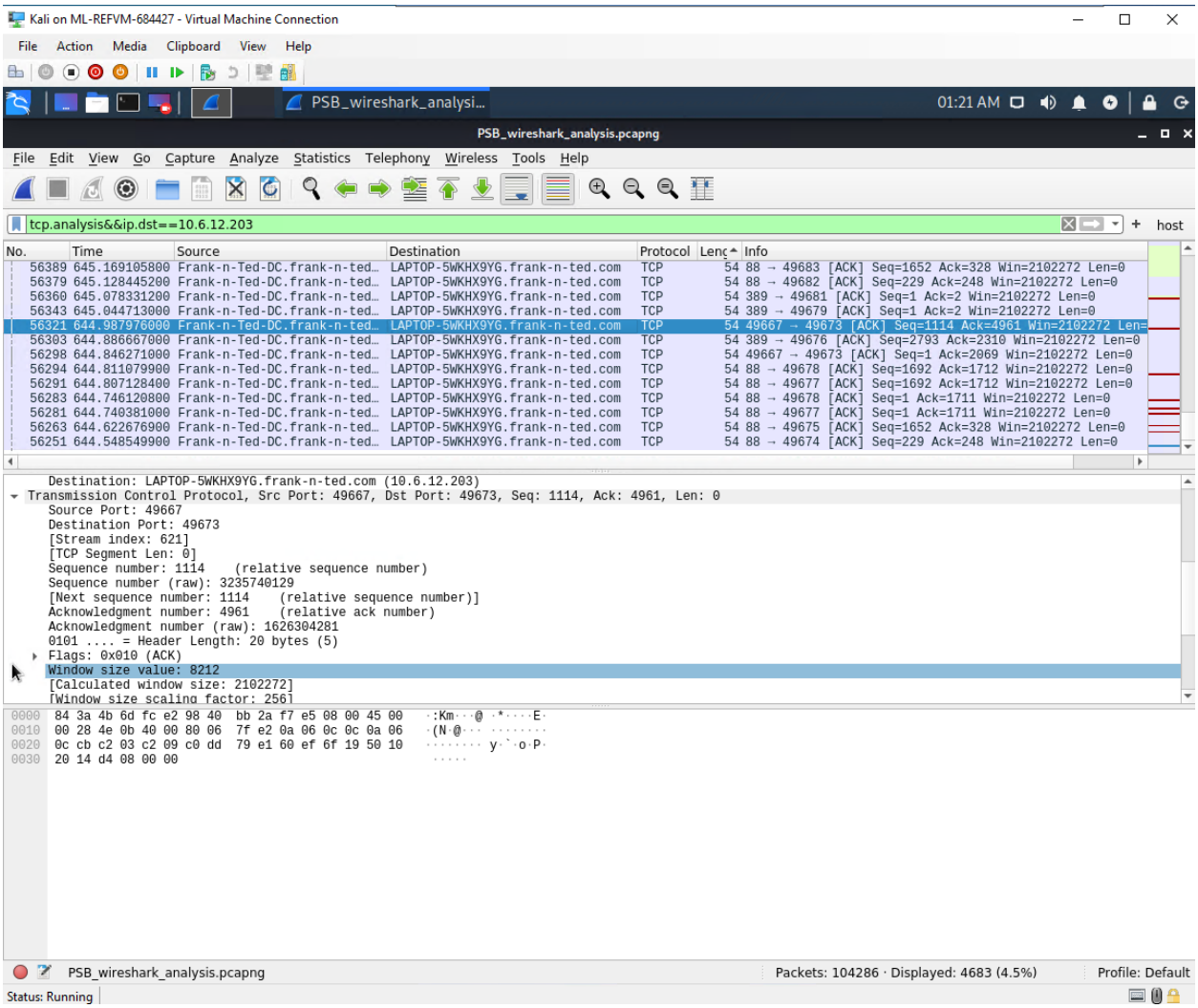
Wireshark_tcp_166.62.111.64a



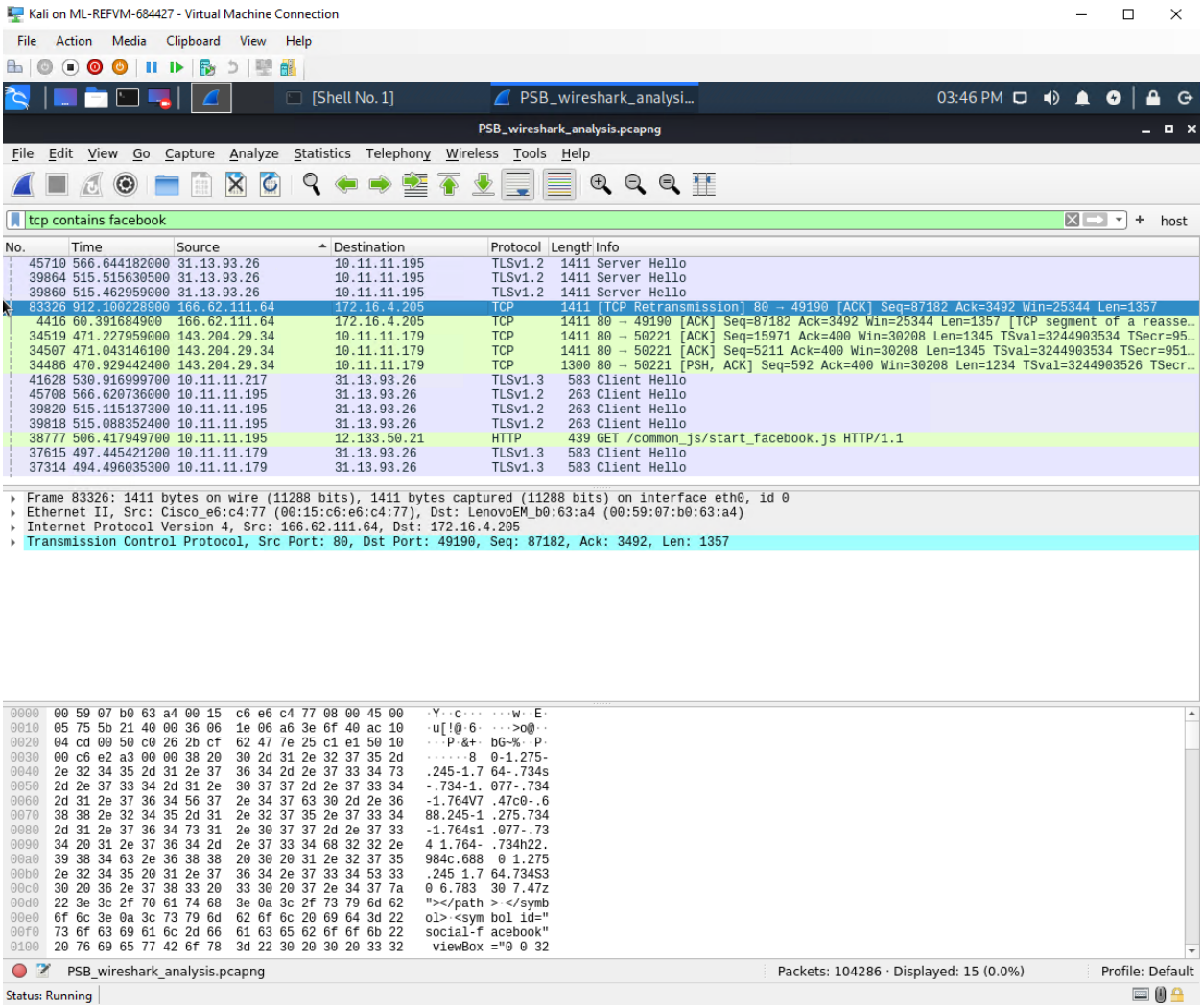
Wireshark_tcp_166.62.111.64b



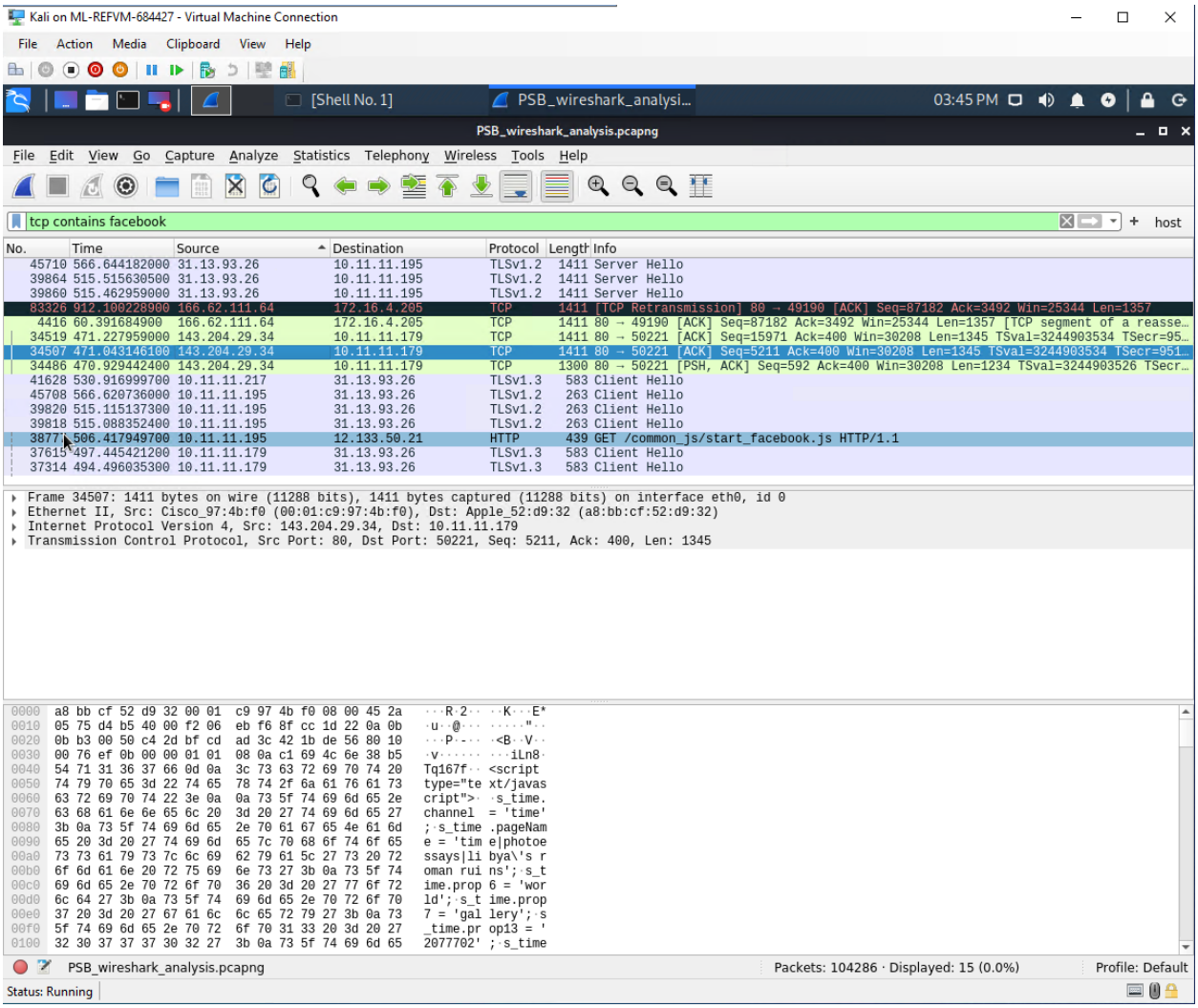
Wireshark_tcp_172.16.4.205



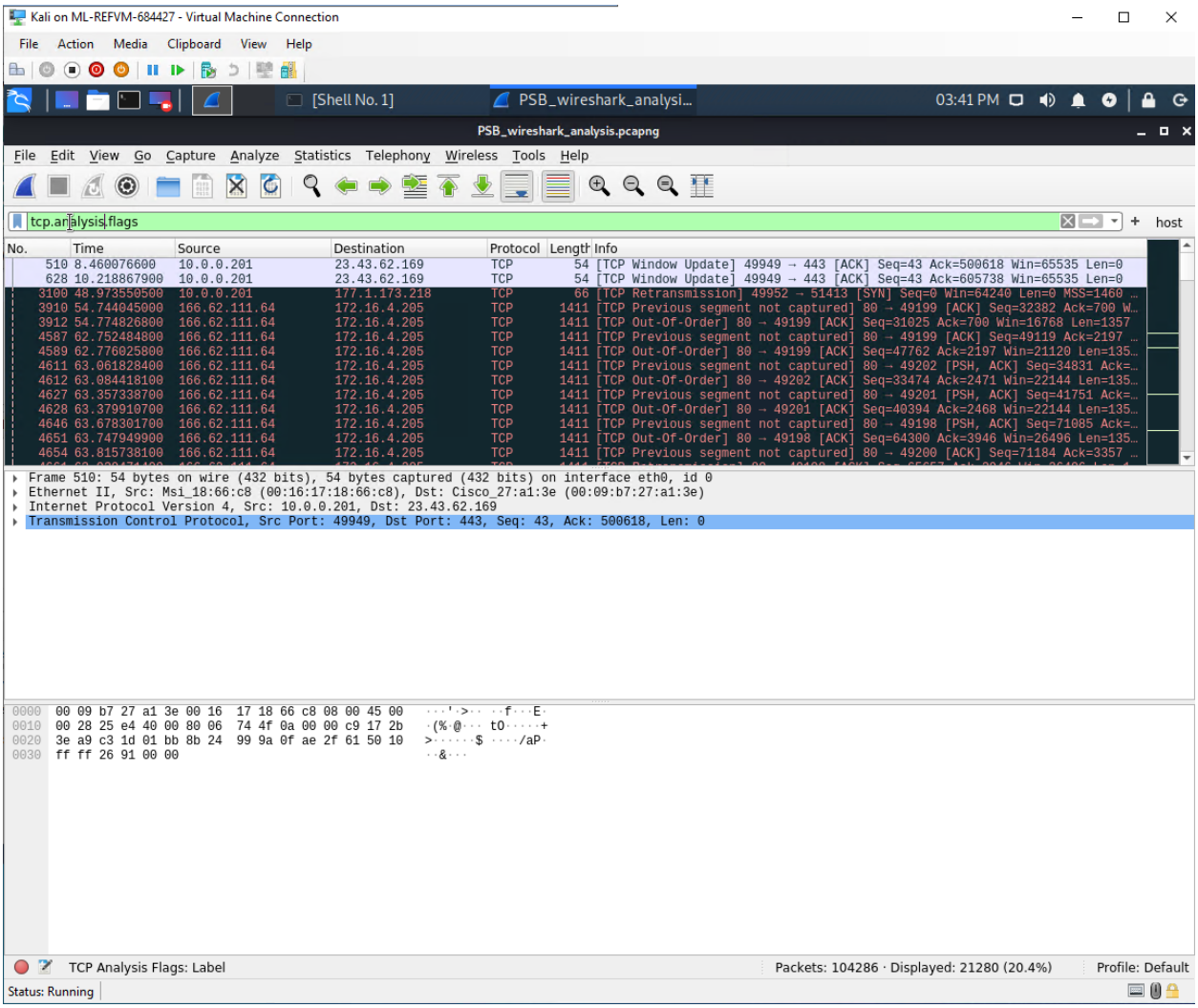
Wireshark_tcp_analysis



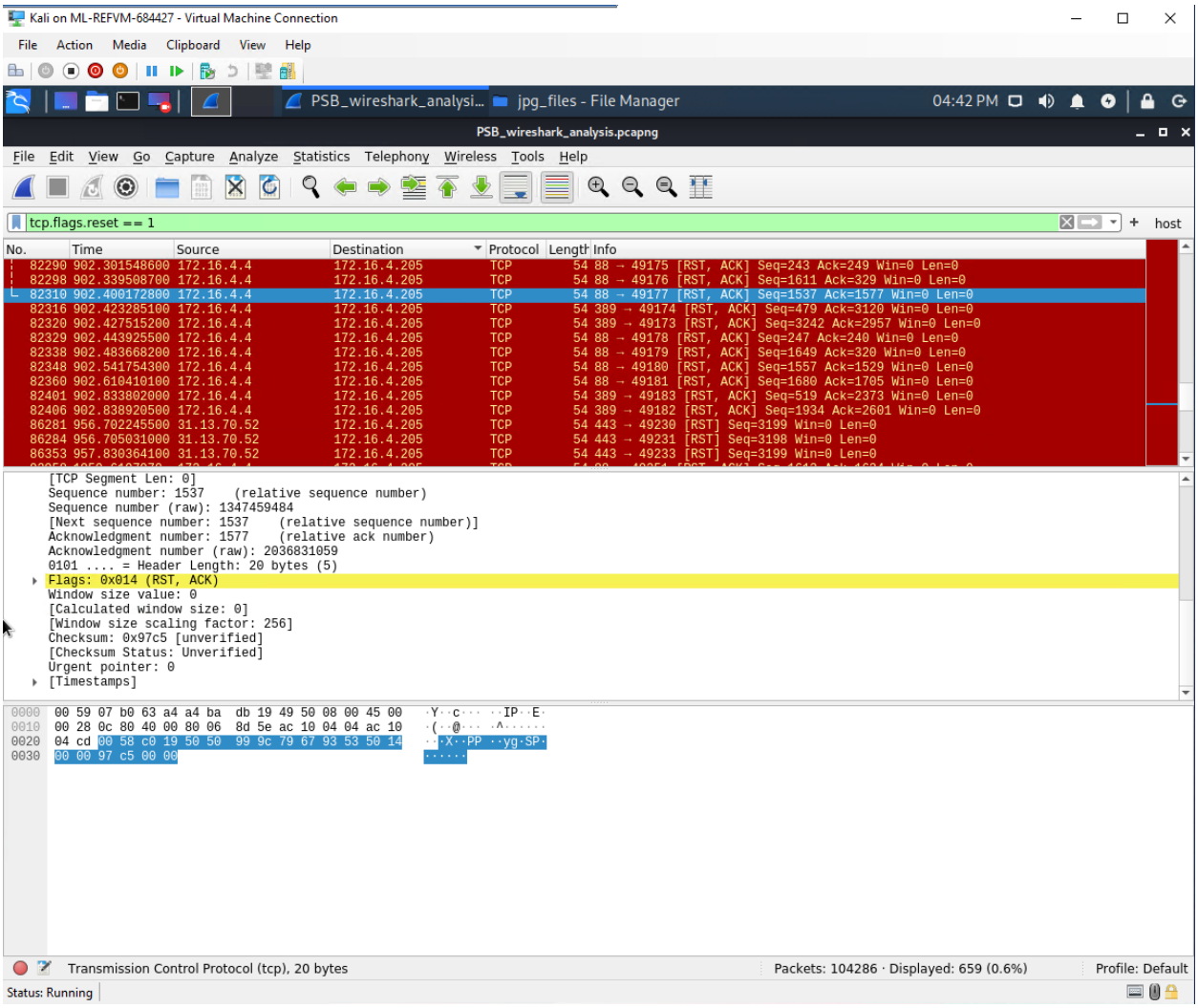
Wireshark_tcp_facebook1



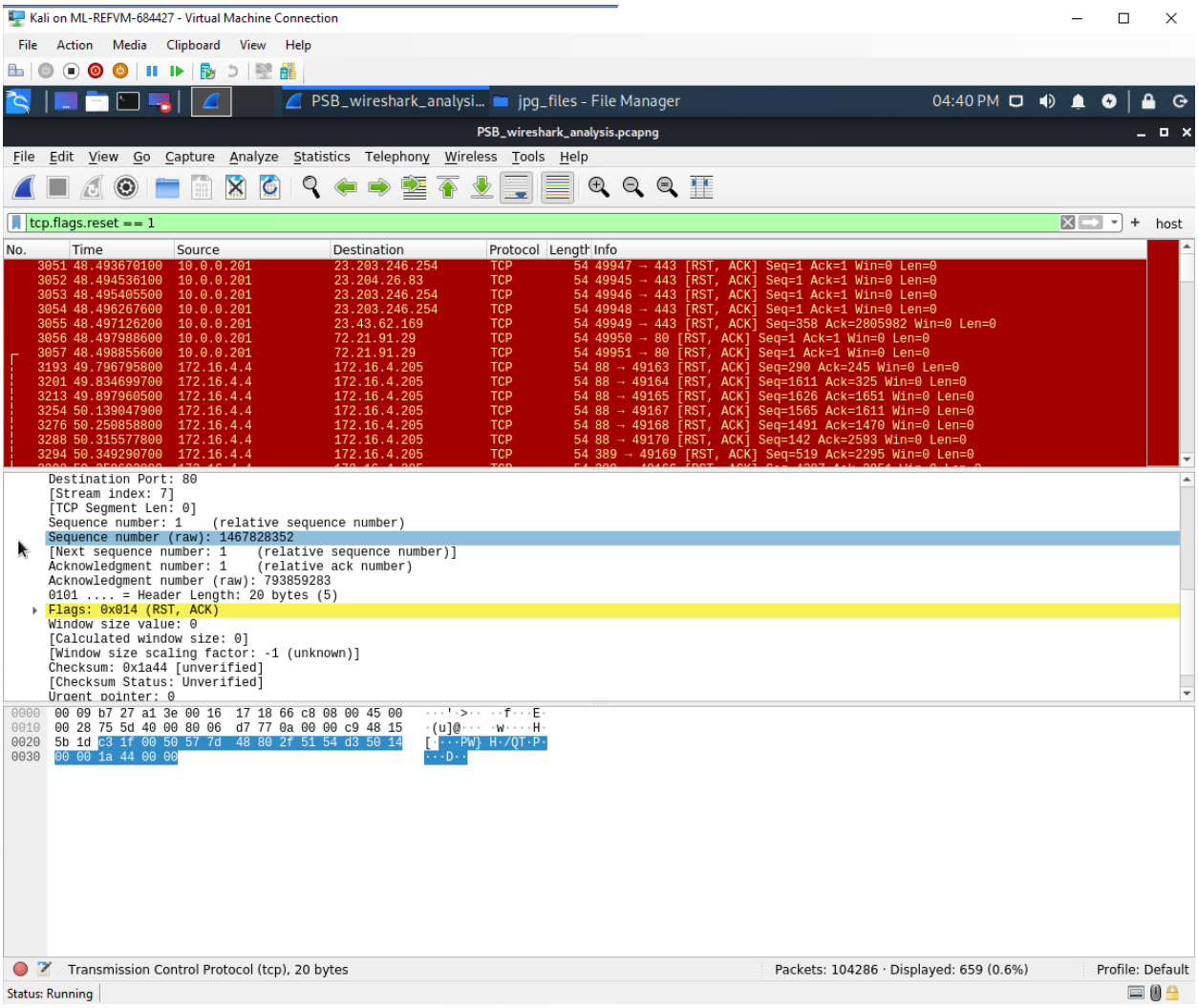
Wireshark_tcp_facebook2



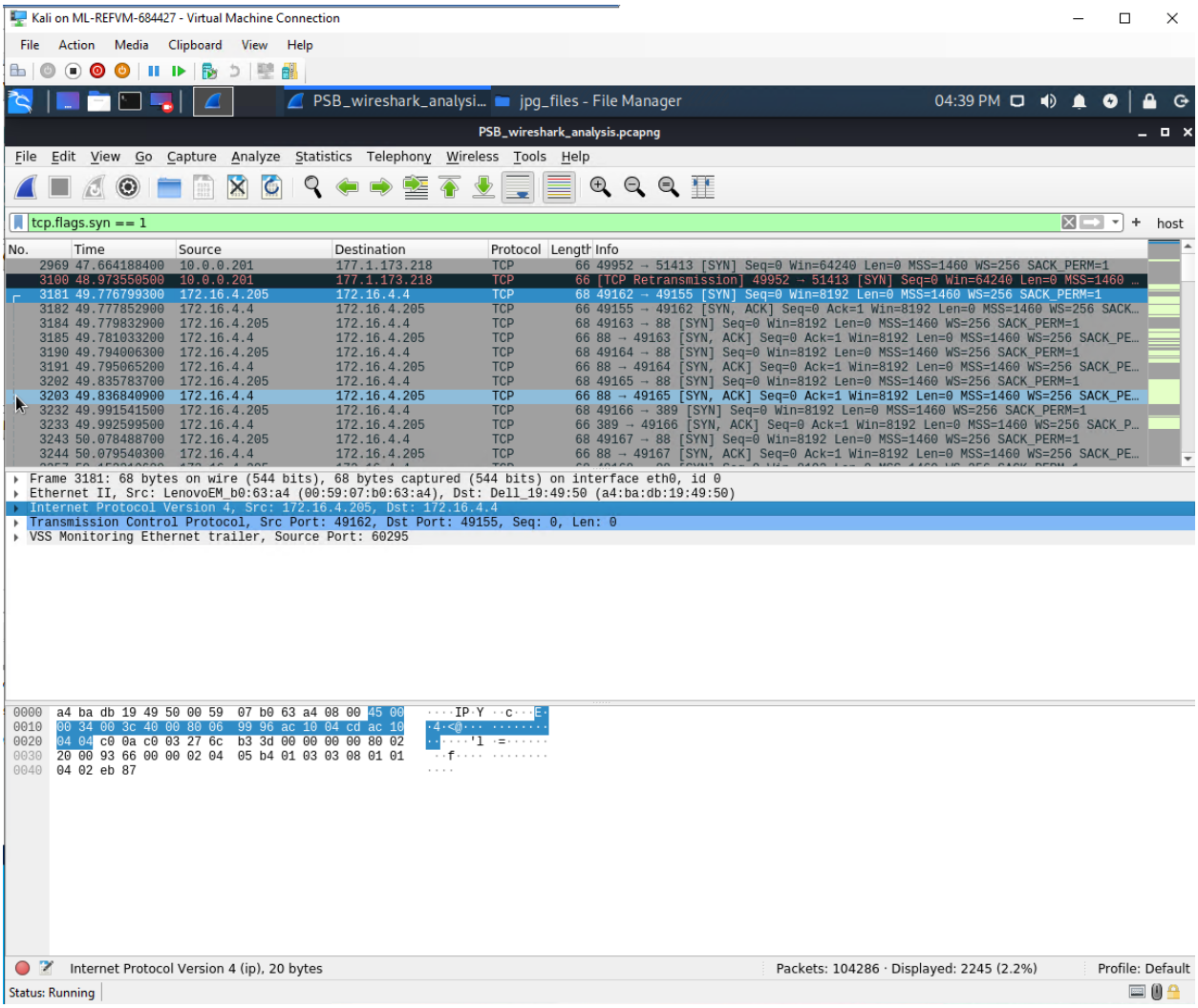
Wireshark_tcp_flags



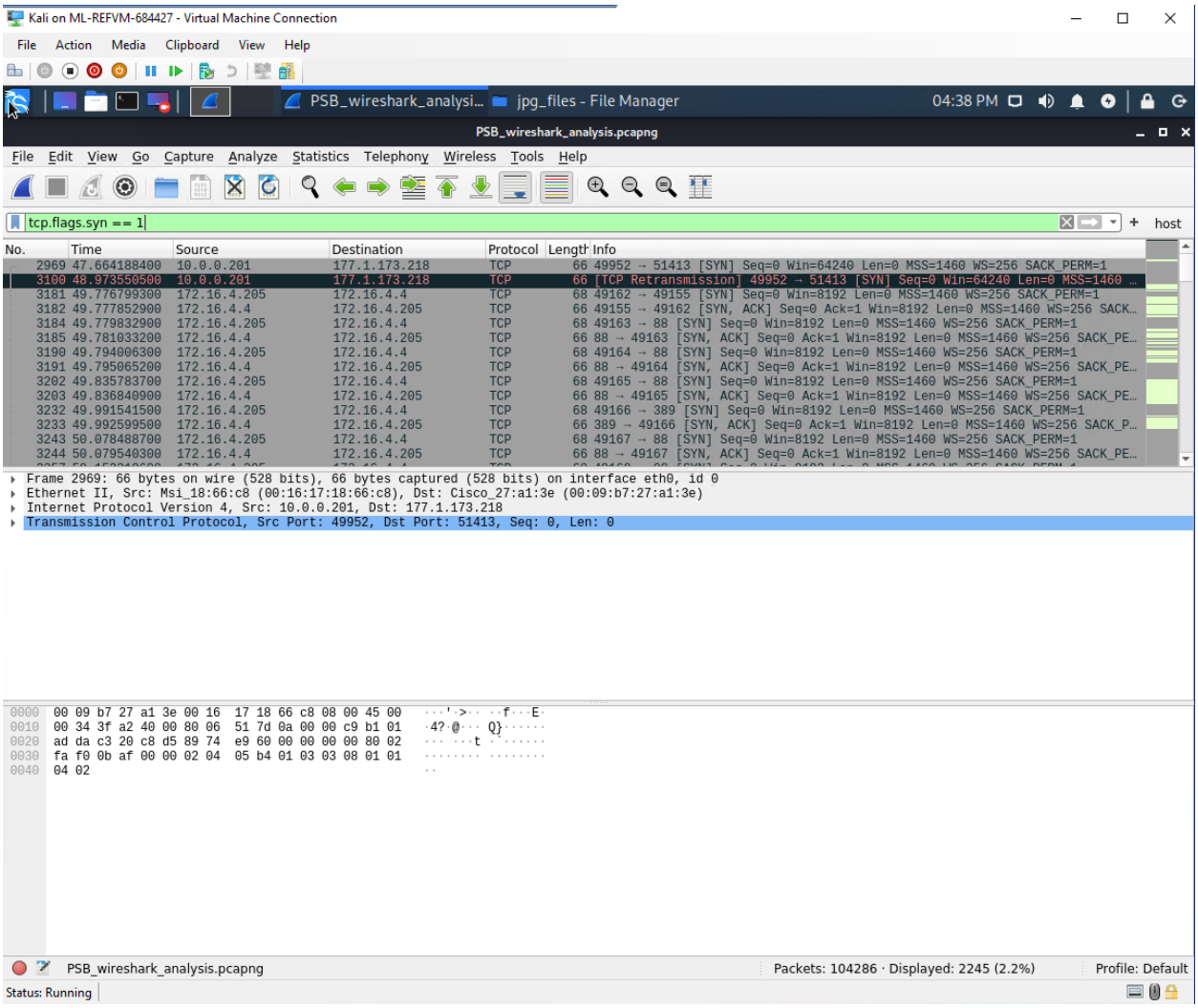
Wireshark_tcp_flags_reset1



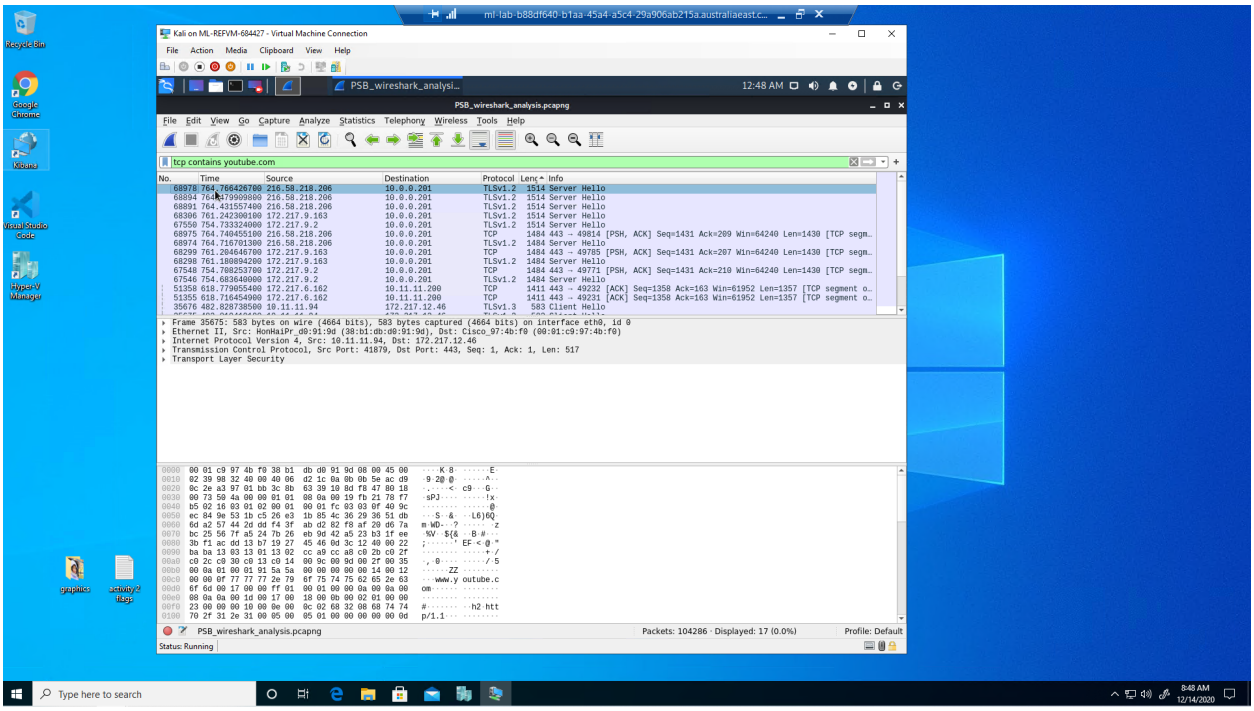
Wireshark_tcp_flags_reset2



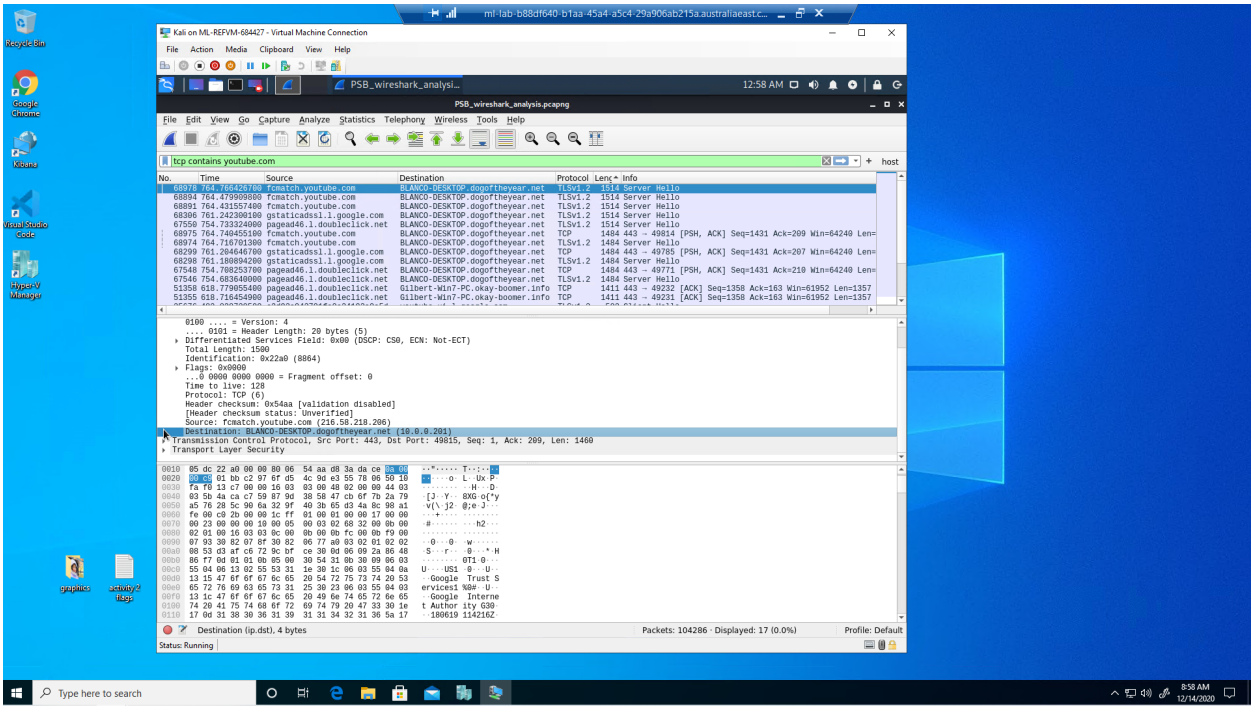
Wireshark_tcp_flags_syn1



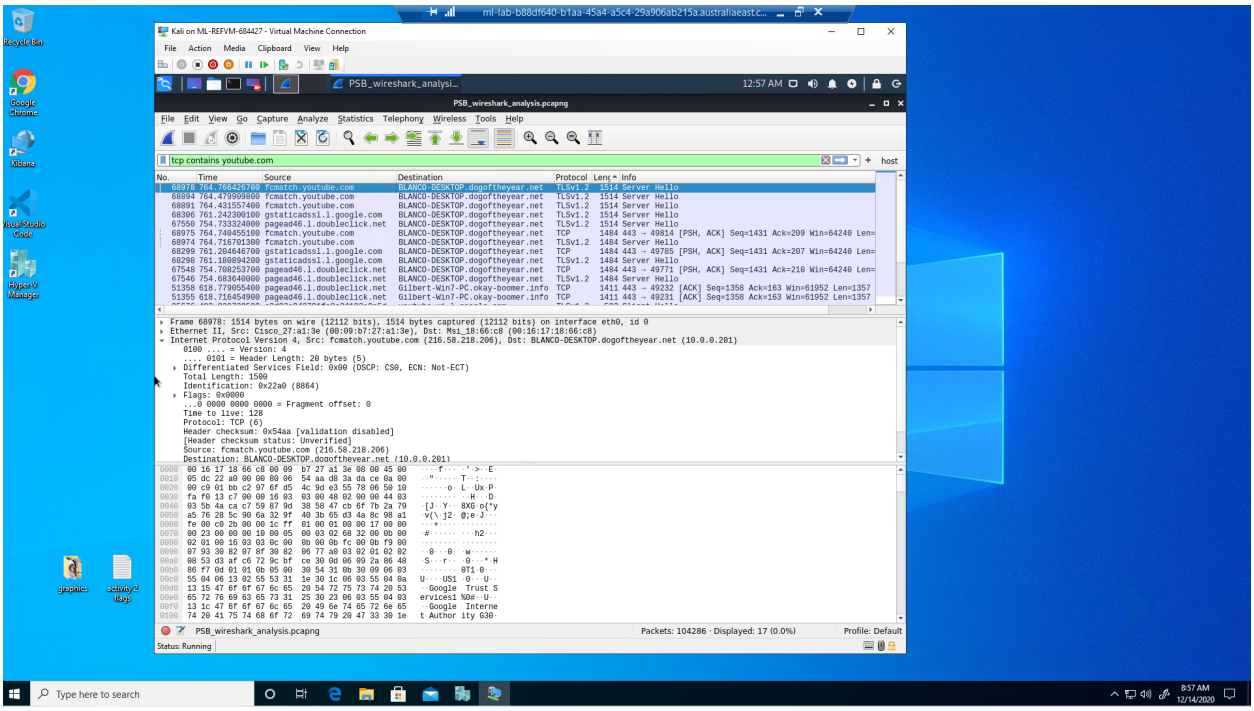
Wireshark_tcp_flags_syn2



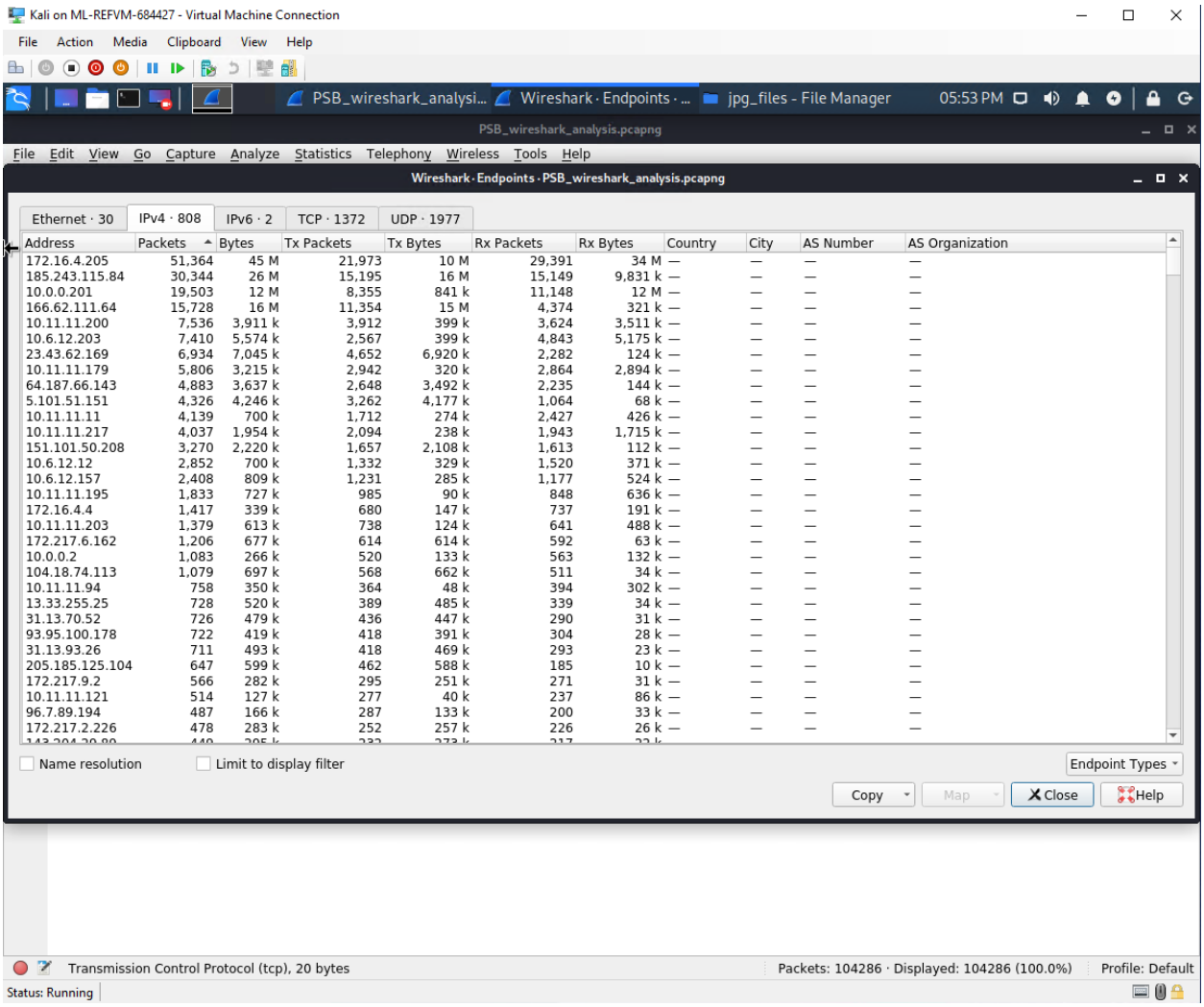
Wireshark_tcp_youtube1



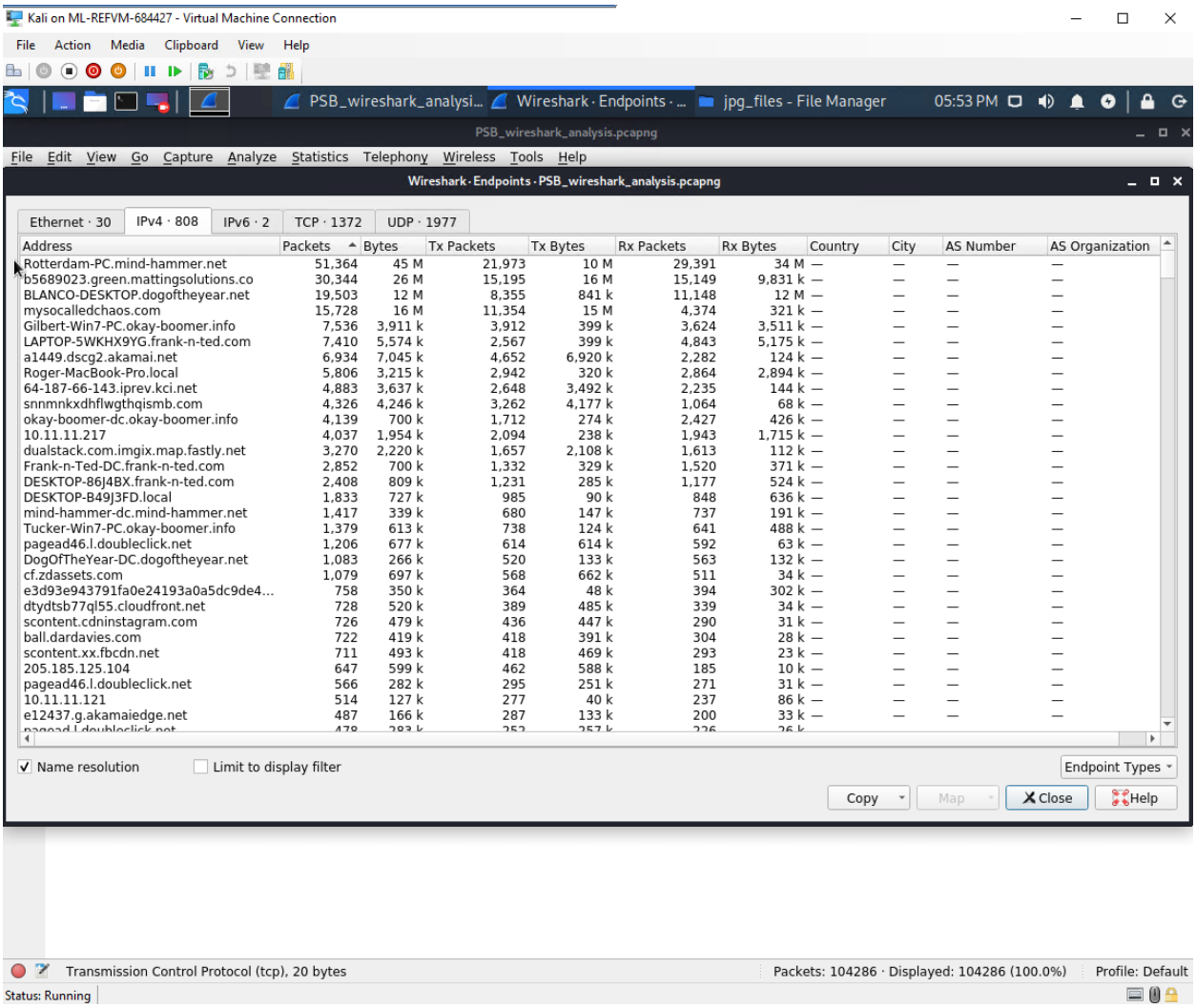
Wireshark_tcp_youtube2



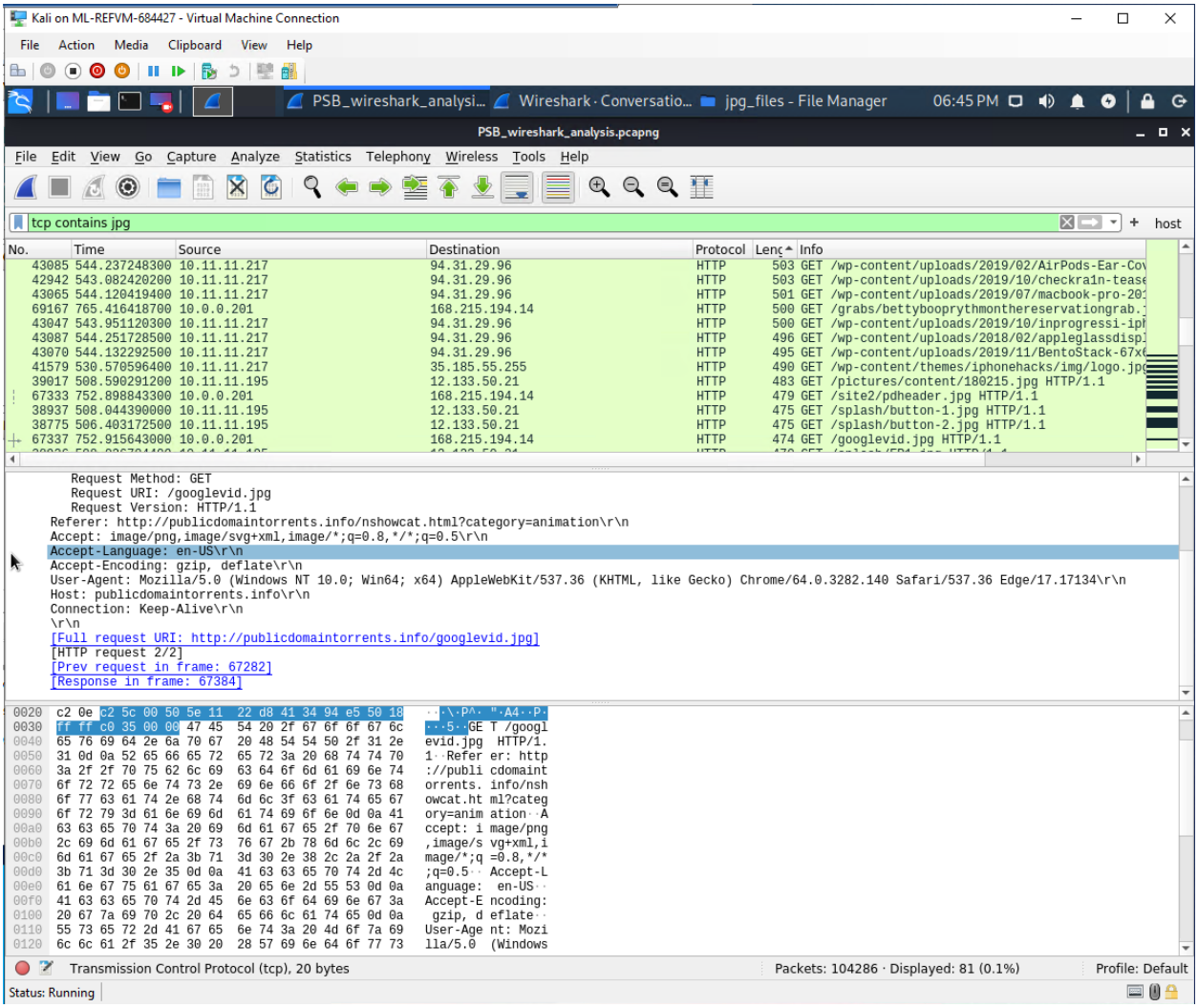
Wireshark_tcp_youtube2a



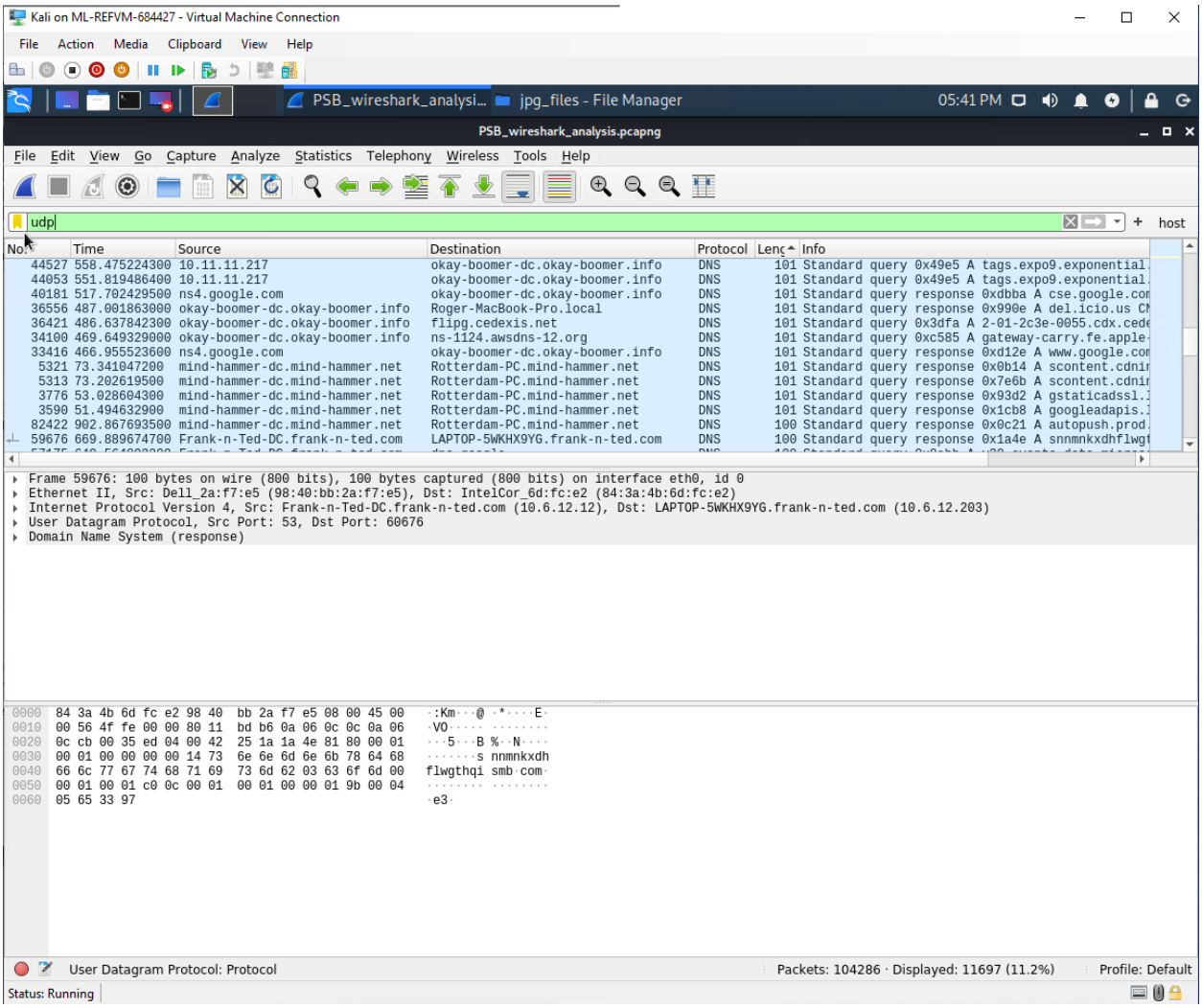
Wireshark_top_talkers1



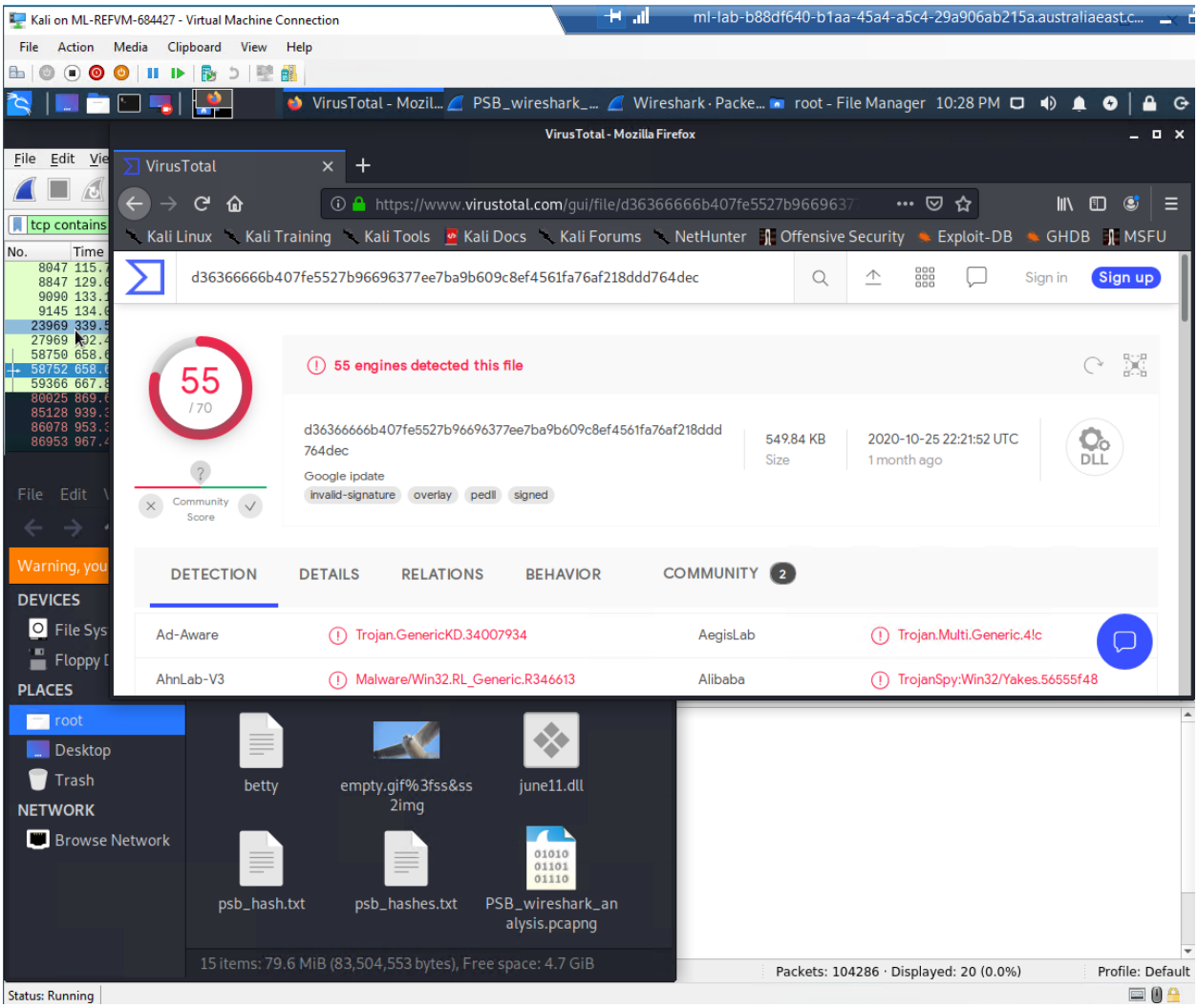
Wireshark_top_talkers2



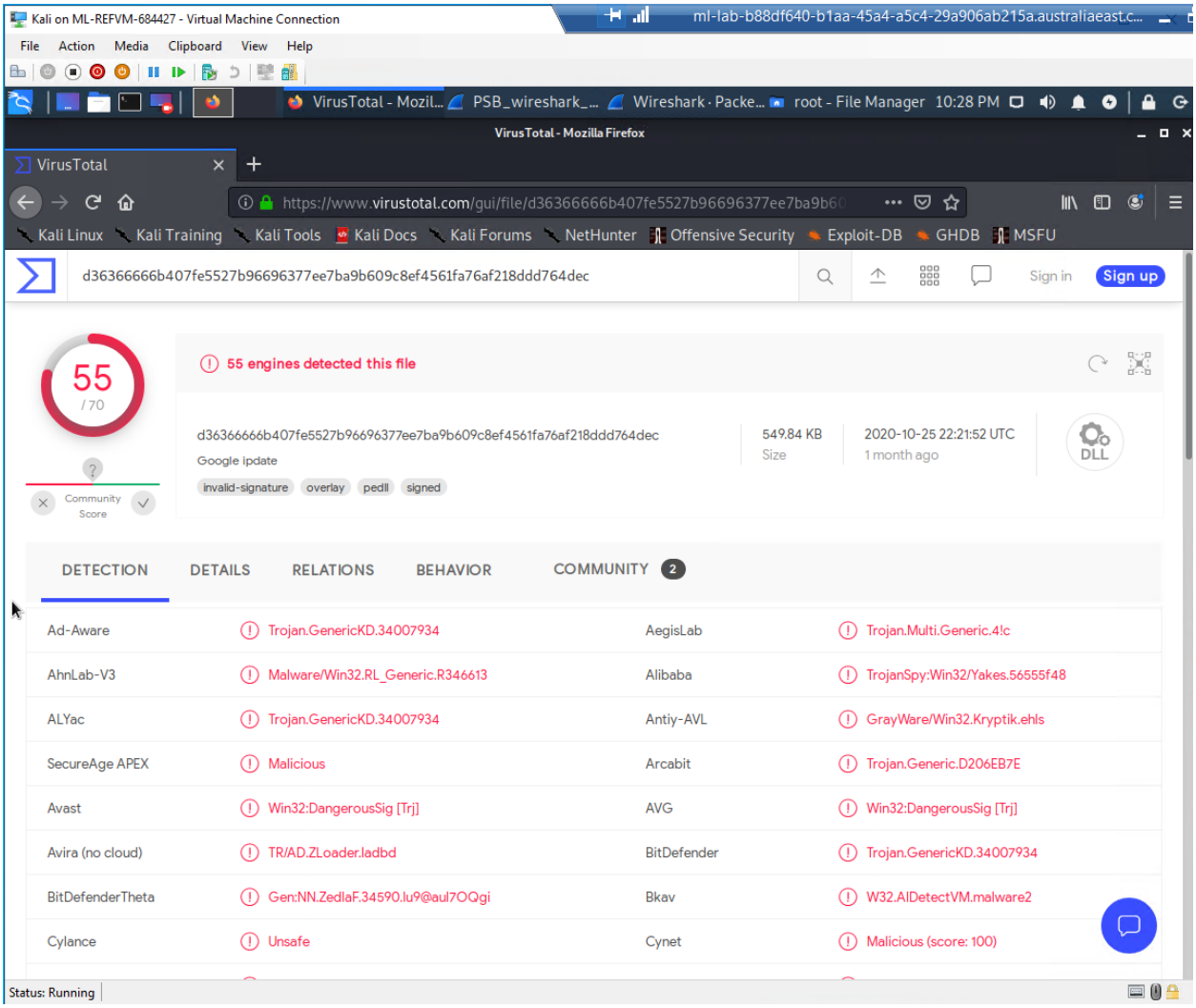
Wireshark_torrent



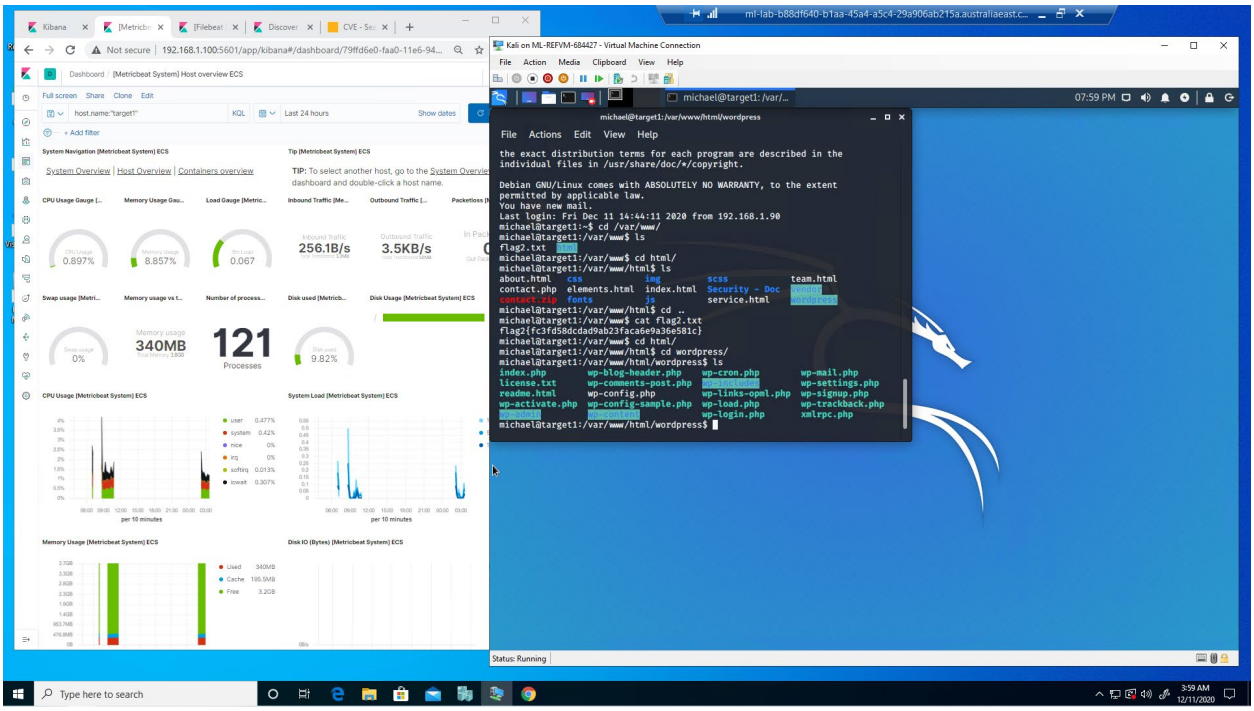
Wireshark_udp



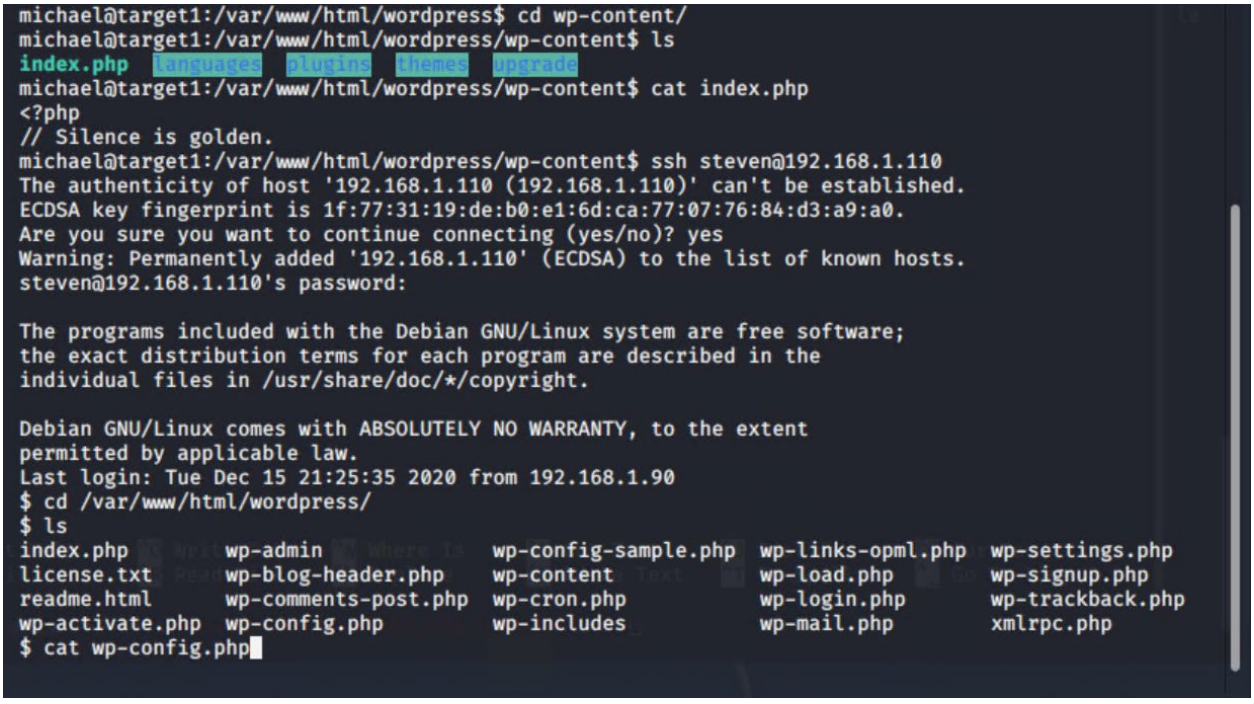
Wireshark_virustotal1



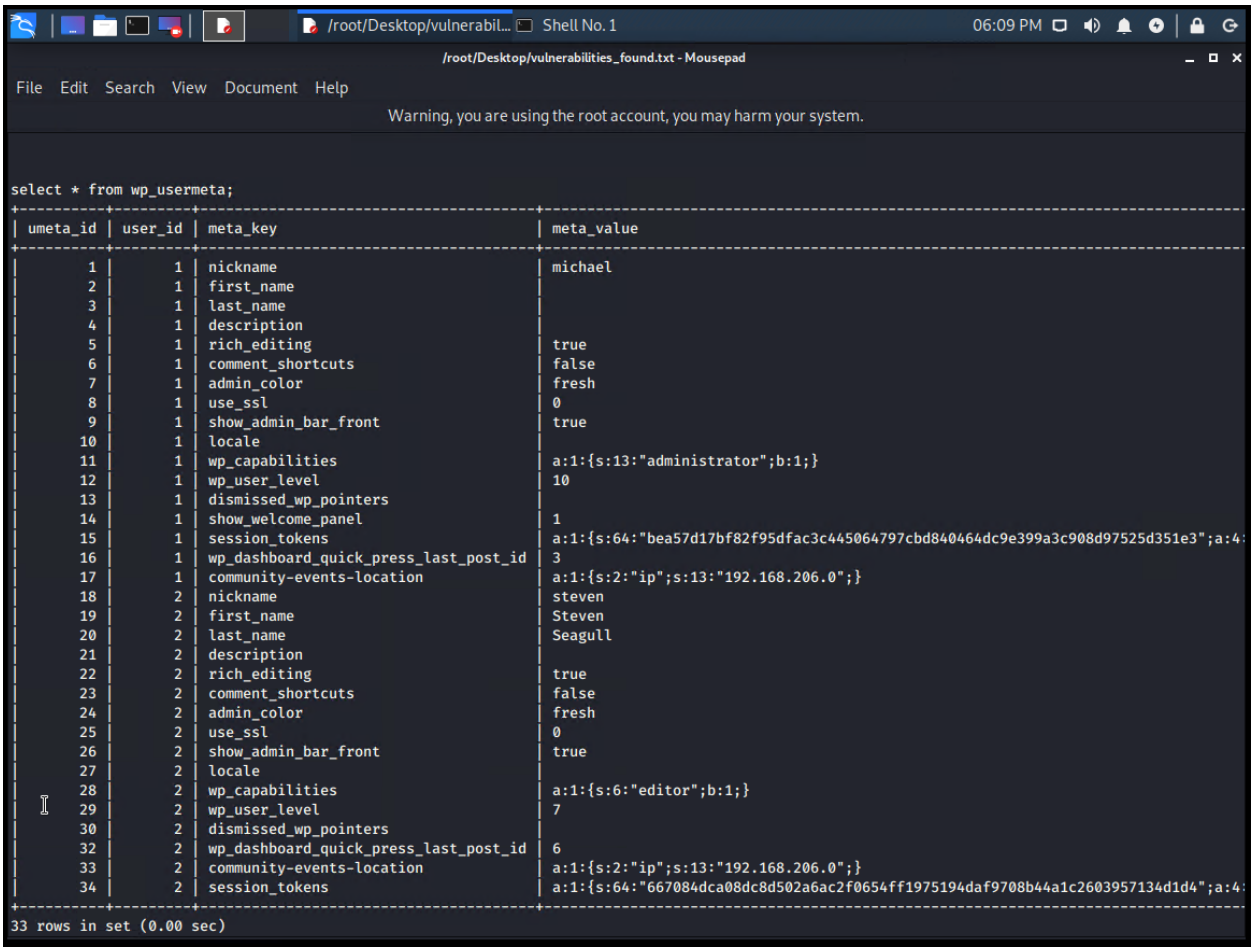
Wireshark_virustotal2



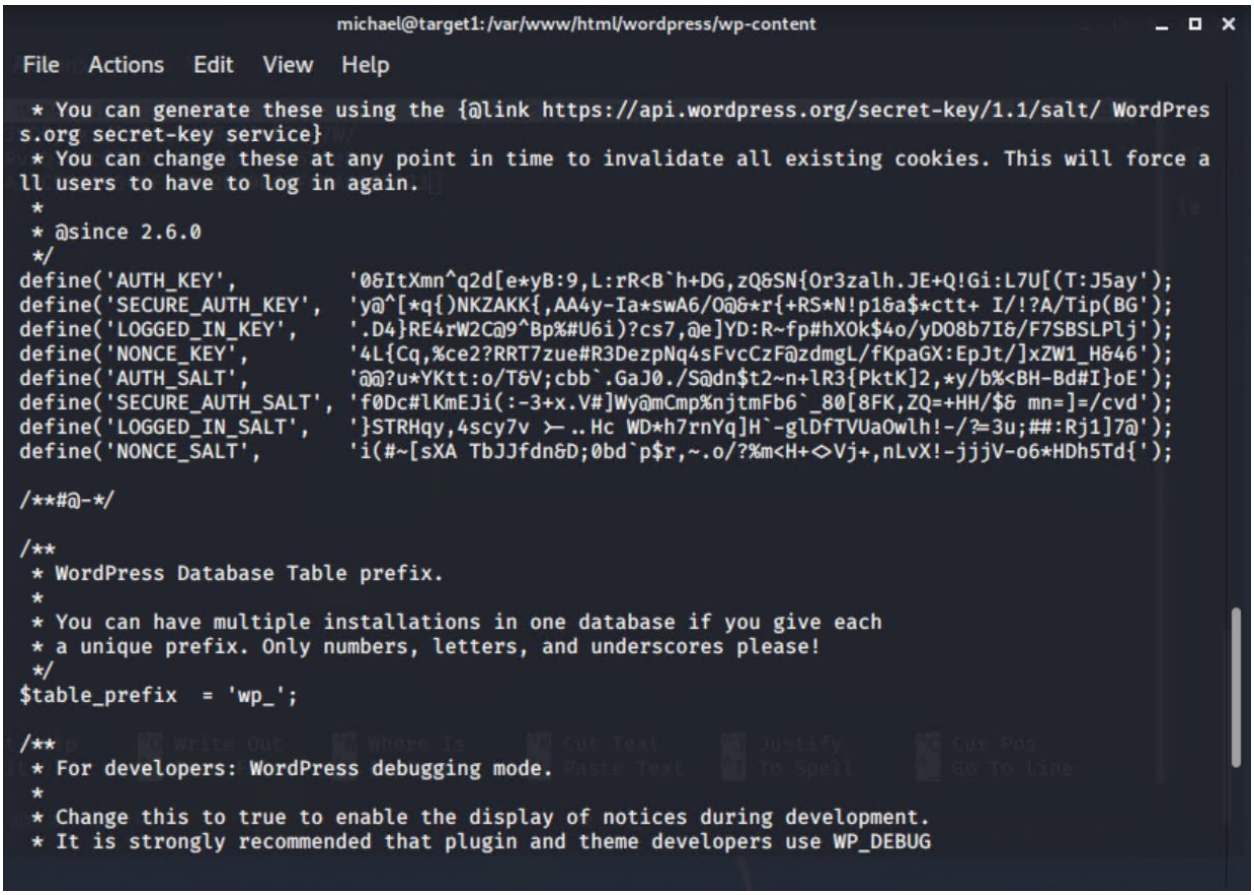
wordpress_directory1



Wordpress_directory2



Wordpress_usermeta



Wp_content_salted