

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 range 10.6.12.0/24 .

The figure consists of three vertically stacked NetworkMiner tool windows.
 1. The top window shows a list of TCP connections containing the domain 'youtube.com'. It lists several entries, each with columns for No., Time, Source, Destination, Protocol, Length, and Info. Most entries show TLSv1.2 connections to various IP addresses and ports, all labeled 'Server Hello'.
 2. The middle window shows a list of UDP traffic. It lists several entries, each with columns for No., Time, Source, Destination, Protocol, Length, and Info. Most entries show DNS queries to various domains like 'okay-boomer-dc.okay-boomer.info' and 'mind-hammer-dc.mind-hammer.net'.
 3. The bottom window shows a list of DNS traffic. It lists several entries, each with columns for No., Time, Source, Destination, Protocol, Length, and Info. It shows standard DNS queries and responses for various websites like 'www.google.com' and 'googleapis.com'.

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

Network Analysis Report by Paul Barrett

10.6.12.157

No.	Time	Source	Destination	Protocol	Length	Info
55429	641.057368600	10.6.12.157	10.6.12.12	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs
55431	641.061408000	10.6.12.157	10.6.12.12	DNS	99	Standard query 0x838 A frank-n-ted-dc.frank-n-ted.com
55433	641.067325100	10.6.12.157	10.6.12.12	LDAP	264	searchRequest(1) "<ROOT>" baseObject
55435	641.072155000	10.6.12.157	10.6.12.12	TCP	66	49668 - 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1440
55437	641.074069000	10.6.12.157	10.6.12.12	TCP	54	49668 - 389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
55438	641.080536000	10.6.12.157	10.6.12.12	LDAP	404	searchRequest(2) "<ROOT>" baseObject
55441	641.127804700	10.6.12.157	10.6.12.12	TCP	54	49668 - 389 [ACK] Seq=351 Ack=2793 Win=2102272
55442	641.129018900	10.6.12.157	10.6.12.12	DNS	76	Standard query 0x3a0 A dns.msftncsi.com
55444	641.132073700	8.8.8.8	10.6.12.12	DNS	103	Standard query response 0xa0bb A dns.msftncsi.com
55446	641.134807100	10.6.12.157	10.6.12.12	DNS	80	Standard query 0x16a7 A wpad.frank-n-ted.com
55450	641.142873700	10.6.12.157	10.6.12.12	DNS	127	Standard query 0x68d SRV _ldap._tcp.Default-P
55452	641.150204500	10.6.12.157	10.6.12.12	LDAP	265	searchRequest(1) "<ROOT>" baseObject
55453	641.155133600	10.6.12.157	10.6.12.12	LDAP	308	searchRequest(2) "<ROOT>" baseObject
55456	641.162673000	10.6.12.157	10.6.12.12	LDAP	260	searchRequest(3) "<ROOT>" baseObject

- 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

- Upload the file to [VirusTotal.com](https://www.virustotal.com). What kind of malware is this classified as?

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

Network Analysis Report by Paul Barrett

55 engines detected this file

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Google update

549.84 KB
Size

2020-10-25 22:21:52 UTC
1 month ago

DLL

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	① Trojan.GenericKD.34007934		AegisLab	① Trojan.Multi.Generic.4!c
AhnLab-V3	① Malware/Win32.RL_Generic.R346613		Alibaba	① TrojanSpy:Win32/Yakes.56555f48
ALYac	① Trojan.GenericKD.34007934		Antiy-AVL	① GrayWare/Win32.Kryptik.ehls
SecureAge APEX	① Malicious		Arcabit	① Trojan.Generic.D206EB7E
Avast	① Win32:DangerousSig [Trj]		AVG	① Win32:DangerousSig [Trj]
Avira (no cloud)	① TR/AD.ZLoader.ladbd		BitDefender	① Trojan.GenericKD.34007934
BitDefenderTheta	① Gen:NN.ZedlaF.34590.lu9@au17OQgi		Bkav	① W32.AIDetectVM.malware2
Cylance	① Unsafe		Cynet	① 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: ROTTERDAMPC
- 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

No.	Time	Source	Destination	Protocol	Length	Info
8047	115.778045100	166.62.111.64	172.16.4.205	TCP	1411	80 → 49200 [ACK] Seq=504978 Ack=4124 Win=26496
8847	129.027619400	166.62.111.64	172.16.4.205	TCP	1411	80 → 49190 [ACK] Seq=508679 Ack=4455 Win=27776
9096	133.174052900	166.62.111.64	172.16.4.205	TCP	1411	80 → 49199 [ACK] Seq=450836 Ack=2889 Win=23296
9145	134.048252000	166.62.111.64	172.16.4.205	TCP	1411	80 → 49190 [ACK] Seq=588742 Ack=4455 Win=27776
23969	339.557487800	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK] Seq=238881 Ack=8227523 Win=648
27969	402.435249400	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK] Seq=3831545 Ack=8227810 Win=648
58750	658.630781400	205.185.125.104	10.6.12.203	HTTP	542	HTTP/1.1 302 Found
58752	658.636633700	10.6.12.203	205.185.125.104	HTTP	312	GET /files/junel1.dll HTTP/1.1
59366	667.857256200	205.185.125.104	10.6.12.203	TCP	1514	80 → 49739 [ACK] Seq=542269 Ack=480 Win=64240
80025	869.652650800	23.43.62.169	10.6.0.201	TCP	1514	[TCP Spurious Retransmission] 443 → 49949 [PSH]
85128	939.341644700	166.62.111.64	172.16.4.205	TCP	1411	[TCP Retransmission] 80 → 49199 [ACK] Seq=18480
86078	953.389592100	166.62.111.64	172.16.4.205	TCP	1411	[TCP Retransmission] 80 → 49199 [ACK] Seq=23235
86953	967.486584900	166.62.111.64	172.16.4.205	TCP	1411	[TCP Retransmission] 80 → 49200 [ACK] Seq=504978
87755	980.700162000	166.62.111.64	172.16.4.205	TCP	1414	[TCP Retransmission] 80 → 49199 [ACK] Seq=504978

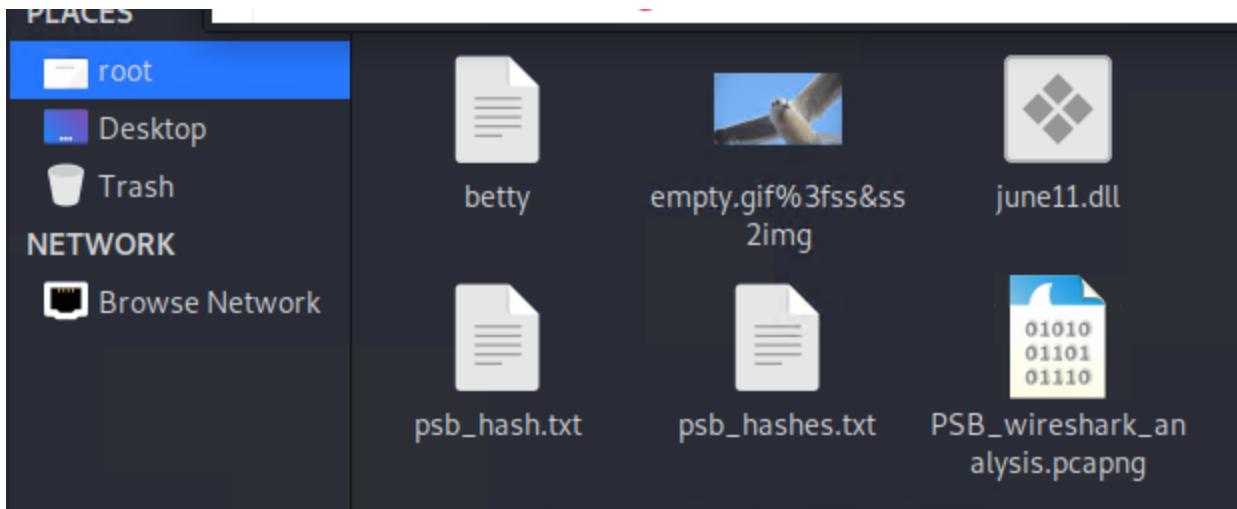
Frame 58752: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0
 ▶ Ethernet II, Src: IntelCor_6d:fce2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
 ▶ Internet Protocol Version 4, Src: 10.6.12.203, Dst: 205.185.125.104
 ▶ Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258

Source Port: 49739
 Destination Port: 80
 [Stream index: 724]
 [TCP Segment Len: 258]
 Sequence number: 222 (relative sequence number)
 Sequence number (raw): 69156669
 [Next sequence number: 480 (relative sequence number)]
 Acknowledgment number: 489 (relative ack number)
 Acknowledgment number (raw): 2023969164
 0101 = Header Length: 20 bytes (5)
 Flags: 0x018 (PSH, ACK)
 Window size value: 65535

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

[Network Analysis Report by Paul Barrett](#)

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 contained 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 downloading 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 DogOfTheYearDC.
- 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 IP address 10.0.0.201 :
 - MAC address 00:16:17:18:66:c8
 - Windows username PC BLANCQDESKTOP
 - OS version
2. Which torrent file did the user download?

Betty_Boop_Rhythm_on_the_Reservation.avi

The Wireshark interface displays two windows. The top window, titled "Wireshark - Export · HTTP object list", shows a table of network traffic. The bottom window, titled "Wireshark - Packet 69719 · PSB_wireshark_analysis.pcapng", shows a detailed view of a selected packet (Frame 69719). The selected packet is an HTTP response (HTTP/1.1 200 OK) from www.publicdomaintorrents.com to the user. The response body contains the content of the torrent file "Betty_Boop_Rhythm_on_the_Reservation.avi".

SCREENSHOTS USED AS EVIDENCE

Network Analysis Report by Paul Barrett

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	—	—	—
---	---	---	---	---	---	---	---	---	---

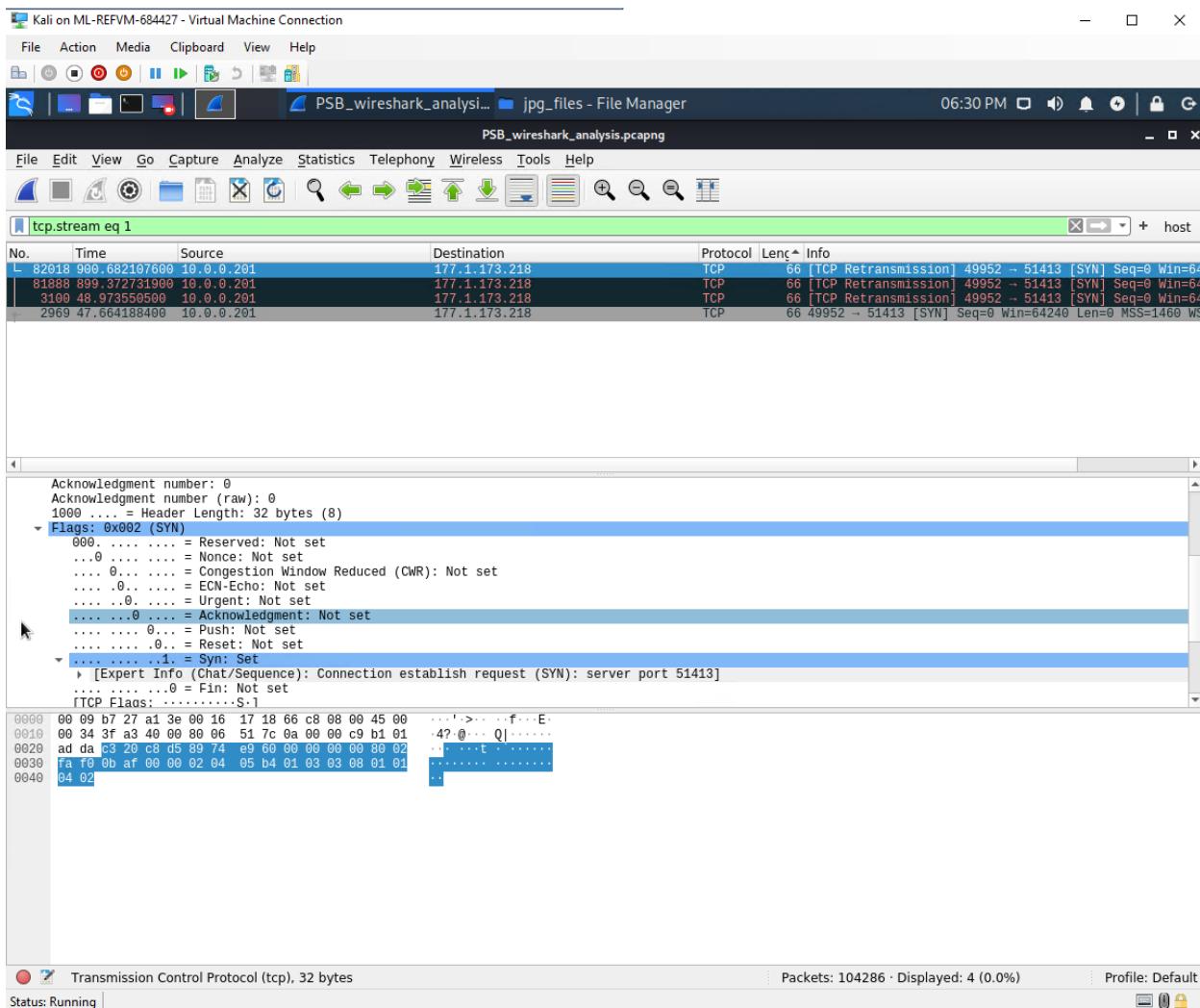
Wireshark - Endpoints · PSB_wireshark_analysis.pcapng									
Ethernet · 30	IPv4 · 808	IPv6 · 2	TCP · 1372	UDP · 1977					
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number
Rotterdam-PC.mind-hammer.net	51,364	45 M	21,973	10 M	29,391	34 M	—	—	—
b5689023.green.mattingsolutions.co	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	—	—	—
snnmnkxdhfliwgthqismb.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	—	—	—
---	---	---	---	---	---	---	---	---	---

Network Analysis Report by Paul Barrett

The screenshot shows a Wireshark interface with the following details:

- File Menu:** File, Action, Media, Clipboard, View, Help.
- Toolbar:** Includes icons for file operations like Open, Save, Print, and a search icon.
- Title Bar:** PSB_wireshark_analysis.pcapng - jpg_files - File Manager
- Time:** 04:55 PM
- Protocol:** PSB_wiresk_analysis.pcapng
- Packet List:** Shows 200 captured packets. The first few entries are:
 - No. 50362 Time 610.497756100 Source pagead46.1.doubleclick Destination 10.11.11.217 Protocol HTTP Lenc 671 Info (text/javascript)
 - No. 41079 Time 525.912157100 Source pagead46.1.doubleclick Destination Roger-MacBook-Pro.local Protocol HTTP Lenc 671 Info (text/javascript)
 - No. 5130 Time 70.327095000 Source www-googletagmanager-com Destination Rotterdam-PC.mind-hammer.net Protocol HTTP Lenc 669 Info (application/javascript)
 - No. 3869 Time 54.222094800 Source myoscalchedchaos.com Destination Rotterdam-PC.mind-hammer.net Protocol HTTP Lenc 662 Info (text/css)
 - No. 40265 Time 53.187164500 Source d3tpad2bnws9f.clou Destination Roger-MacBook-Pro.local Protocol HTTP Lenc 660 Info (text/css)
 - No. 3823 Time 53.678473500 Source myoscalchedchaos.com Destination Rotterdam-PC.mind-hammer.net Protocol HTTP Lenc 658 Info (text/css)
 - No. 40974 Time 54.329148000 Source statictdss1.l.google.com Destination DESKTOP-B49J3FD.local Protocol HTTP Lenc 655 Info (font/woff2)
 - No. 39379 Time 51.469809900 Source pictures.fasthealth.com Destination DESKTOP-B49J3FD.local Protocol HTTP Lenc 652 Info (font/woff2)
 - No. 42957 Time 53.219874100 Source iphonehacks.wpengine.net Destination 10.11.11.217 Protocol HTTP Lenc 644 Info (JPEG JFIF image)
 - No. 39792 Time 51.823724200 Source pictures.fasthealth.com Destination DESKTOP-B49J3FD.local Protocol HTTP Lenc 644 Info (JPEG JFIF image)
 - No. 43214 Time 54.5.781483100 Source iphonehacks.wpengine.net Destination 10.11.11.217 Protocol HTTP Lenc 637 Info (PNG)
 - No. 41616 Time 53.0.883920500 Source iphonehacks.wpengine.net Destination 10.11.11.217 Protocol HTTP Lenc 637 Info (PNG)
 - No. 12882 Time 195.181075800 Source myoscalchedchaos.com Destination Rotterdam-PC.mind-hammer.net Protocol HTTP Lenc 637 Info (JPEG JFIF image)
- Details View:** Shows flags (e.g., PSH, ACK), window size, checksum, and timestamp analysis.
- Hex View:** Displays the raw binary data for selected packets.
- Text View:** Shows line-based text data for selected packets.
- Status Bar:** Frame (696 bytes) Reassembled TCP (20662 bytes) Uncompressed entity body (52979 bytes) Packets: 104286 - Displayed: 361 (0.3%) Profile: Default Status: Running

Network Analysis Report by Paul Barrett



Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

PSB_wireshark_... Wireshark · Conv... Wireshark · Endp... jpg_files - File M... 06:37 PM

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	AS Organization
0.0.0.0	3	1,137	3	1,137	0	0	—	—	—	—
1.0.138.219	12	1,562	5	663	7	899	—	—	—	—
1.64.58.6	25	4,040	12	1,630	13	2,410	—	—	—	—
1.225.136.46	3	651	1	359	2	292	—	—	—	—
1.246.154.176	1	146	0	0	1	146	—	—	—	—
2.7.43.235	12	1,375	5	476	7	899	—	—	—	—
2.10.77.101	15	3,055	8	1,787	7	1,268	—	—	—	—
2.10.249.37	58	10 k	33	7,674	25	3,274	—	—	—	—
2.35.145.138	2	488	1	342	1	146	—	—	—	—
2.36.247.143	12	1,476	5	577	7	899	—	—	—	—
2.37.230.36	13	2,232	6	964	7	1,268	—	—	—	—
2.40.118.249	6	460	1	54	5	406	—	—	—	—
2.49.38.136	12	1,618	5	719	7	899	—	—	—	—
2.50.139.95	4	850	2	483	2	367	—	—	—	—
2.63.86.131	14	1,845	7	918	7	927	—	—	—	—
2.83.102.151	2	498	1	352	1	146	—	—	—	—
2.87.5.246	38	6,056	19	2,623	19	3,433	—	—	—	—
2.95.107.254	13	1,783	6	856	7	927	—	—	—	—
2.122.29.138	17	2,863	11	1,998	6	865	—	—	—	—
2.127.18.85	15	3,082	8	1,814	7	1,268	—	—	—	—
2.133.79.105	8	568	3	162	5	406	—	—	—	—
2.230.32.72	30	5,722	17	4,014	13	1,708	—	—	—	—
2.235.202.129	6	460	1	54	5	406	—	—	—	—
2.238.165.81	40	6,472	20	3,010	20	3,462	—	—	—	—
3.211.86.101	35	8,761	17	6,326	18	2,435	—	—	—	—
5.2.67.55	8	568	3	162	5	406	—	—	—	—
5.9.167.254	12	1,875	5	607	7	1,268	—	—	—	—
5.12.34.66	6	460	1	54	5	406	—	—	—	—
5.12.173.161	6	460	1	54	5	406	—	—	—	—
5.15.25.253	14	1,846	7	918	7	928	—	—	—	—
5.39.78.6	14	2,211	6	881	8	1,330	—	—	—	—
5.39.80.149	14	2,277	7	843	9	1,334	—	—	—	—

Name resolution Limit to display filter

Show resolved addresses and port names rather than plain values. The corresponding name resolution preference must be enabled.

Endpoint Types

Copy Map Close Help

Transmission Control Protocol (tcp), 32 bytes

Packets: 104286 · Displayed: 104286 (100.0%) · Profile: Default

Status: Running

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
69009	ocsp.godaddy.com	application/ocsp-response	1,776 bytes	MEkwRzBFMEMwQTAjBgUrDgMCGgUABBS
42023	www.iphonehacks.com	application/octet-stream	71 kB	fontawesome-webfont.woff2?v=4.6.3
59388	205.185.125.104	application/octet-stream	563 kB	june11.dll
69719	www.publicdomaintorrents.com	application/x-bittorrent	8,268 bytes	btdownload.php?type=torrent&file=Betty

Wireshark_bittorrent.png

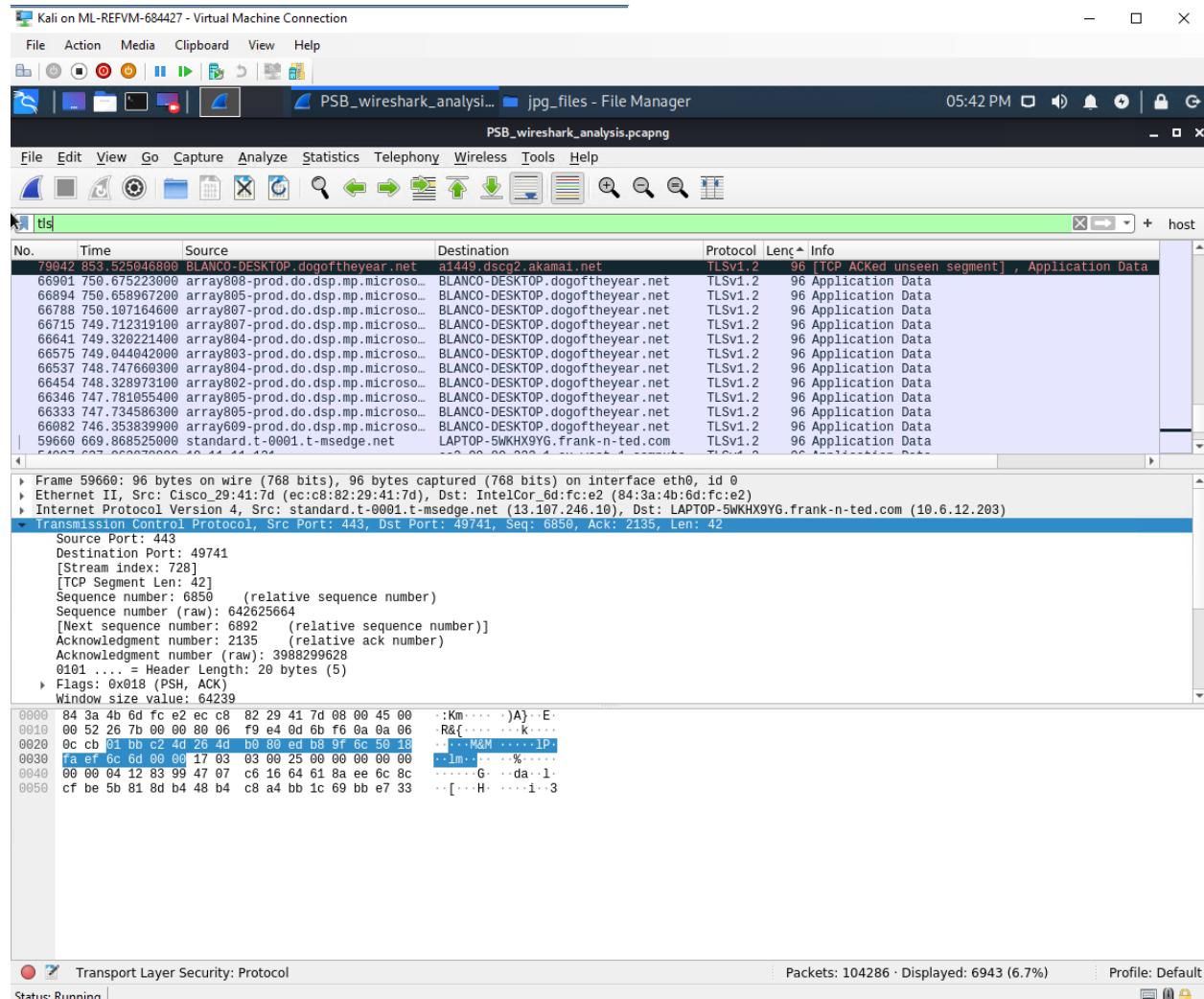
Network Analysis Report by Paul Barrett

The screenshot shows the Wireshark interface with the following details:

- File Menu:** File, Action, Media, Clipboard, View, Help.
- Toolbar:** Standard file operations like Open, Save, Print, Copy, Paste, etc.
- Network List:** PSB_wireshark_..., Wireshark · Conv..., Wireshark · Export..., jpg_files - File M...
- Time:** 06:58 PM
- Packet List:** Shows a list of 1366 captured packets, with the 69719th packet selected.
- Selected Packet Details:**
 - No.:** 69719
 - Time:** 10:34, 8752508...
 - Source:** 192.168.1.1
 - Destination:** 239.255.255.250
 - Protocol:** SSDP
 - Length:** 179
 - Info:** M-SEARCH * HTTP/1.1
- HTTP Object List:** A modal window titled "Wireshark · Export - HTTP object list" lists various resources from the selected packet, such as application/x-javascript files for digg.com and www.sabethahospital.com.
- Text Filter:** A field at the bottom left for filtering text.
- Frame Details:** Frame (1366 bytes) Reassembled TCP (3592678 bytes).
- Status Bar:** Status: Running | Packets: 104286 · Displayed: 614 (0.6%) | Profile: Default

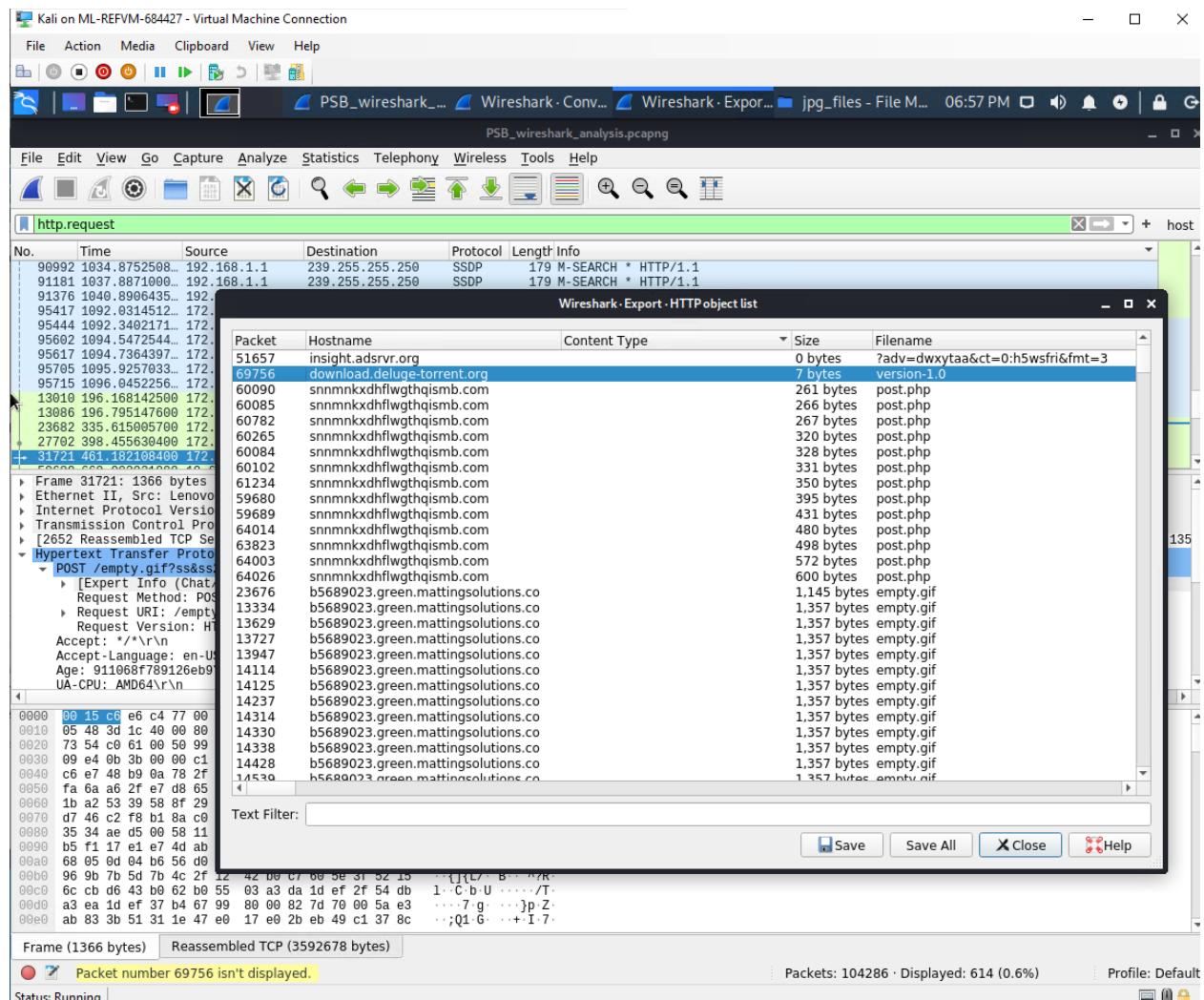
Wireshark bittorrent1.png

Network Analysis Report by Paul Barrett



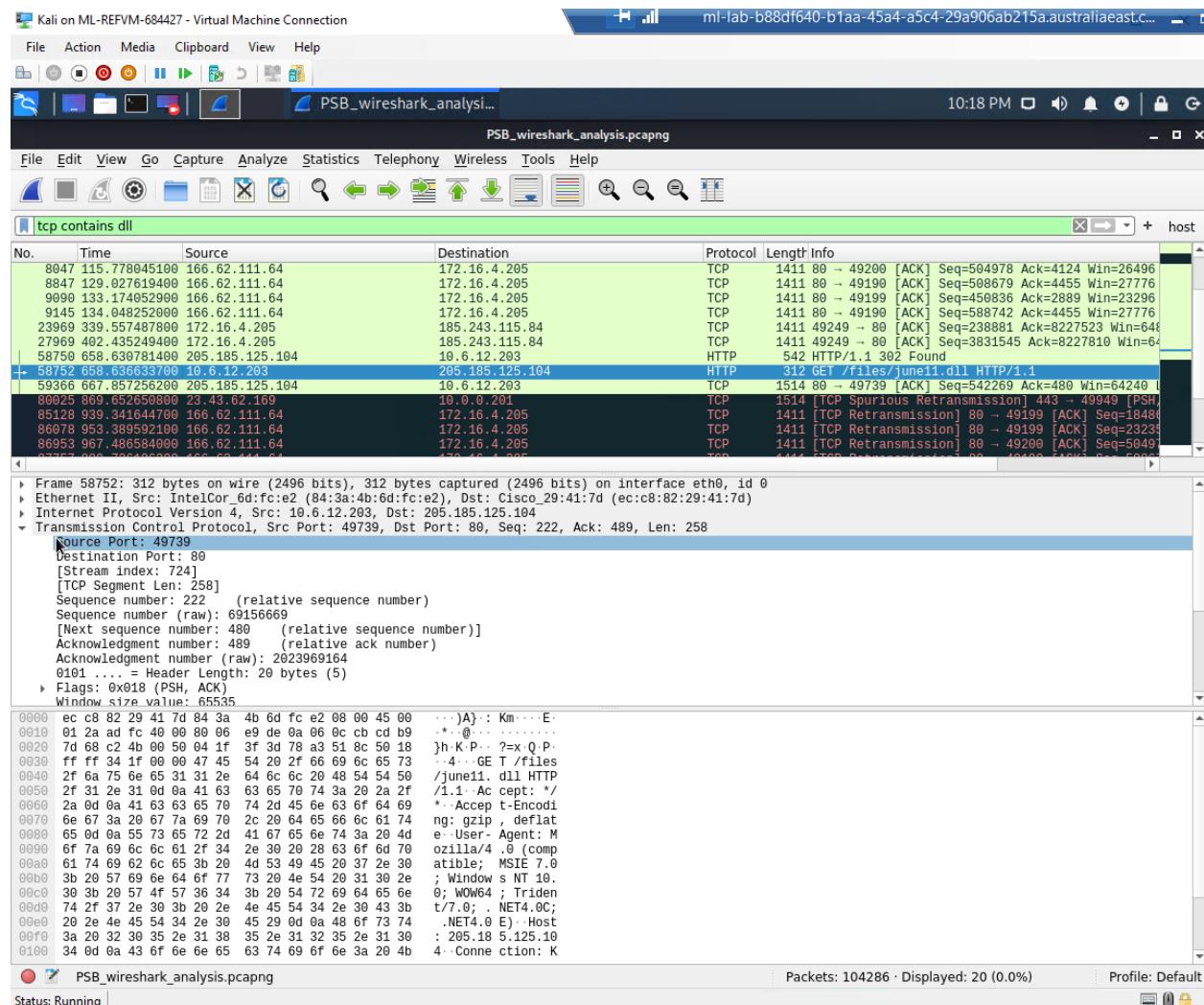
Wireshark_BLANCQDESKTOP.png

Network Analysis Report by Paul Barrett



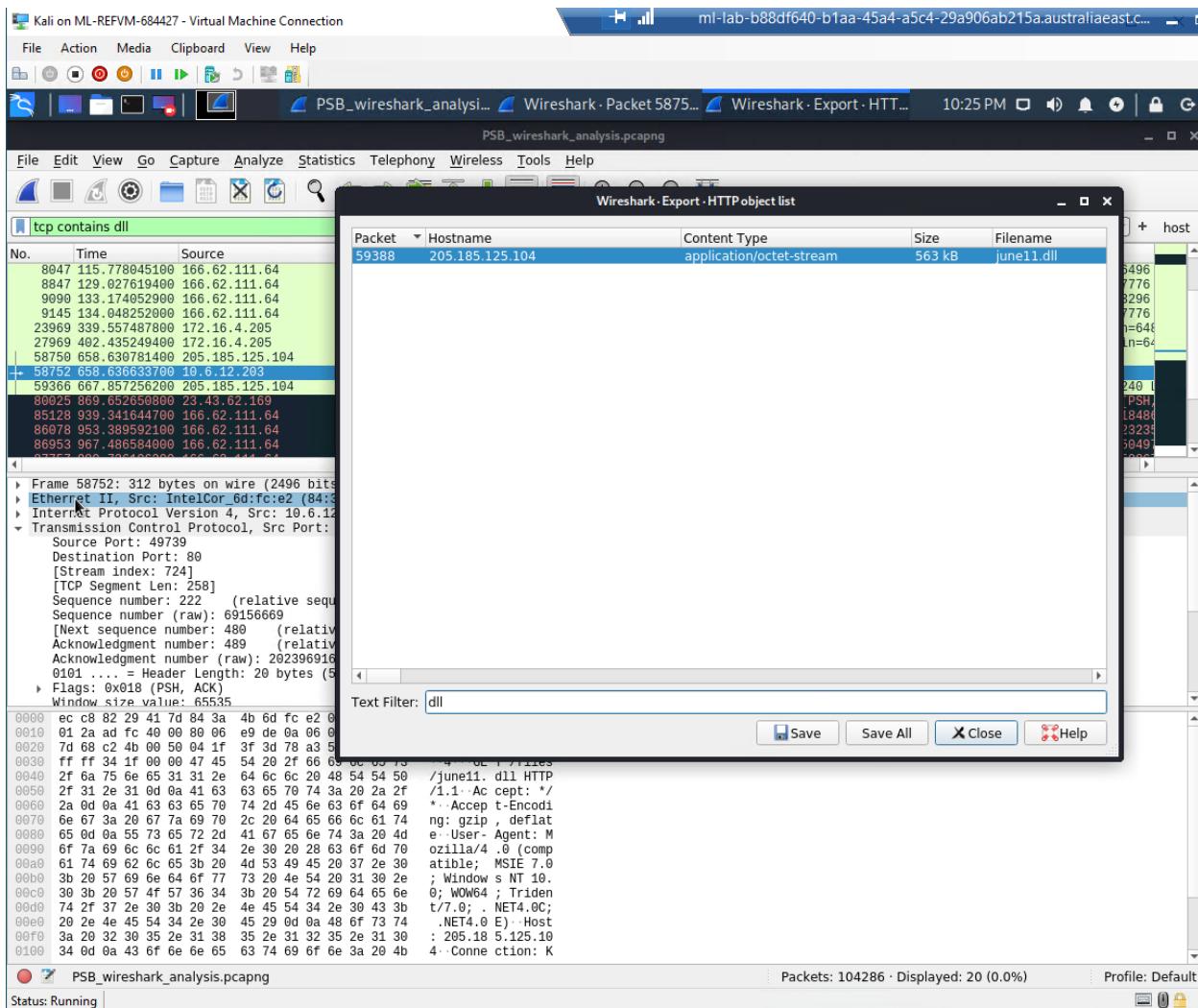
Wireshark_deluge_torrent.org.png

Network Analysis Report by Paul Barrett



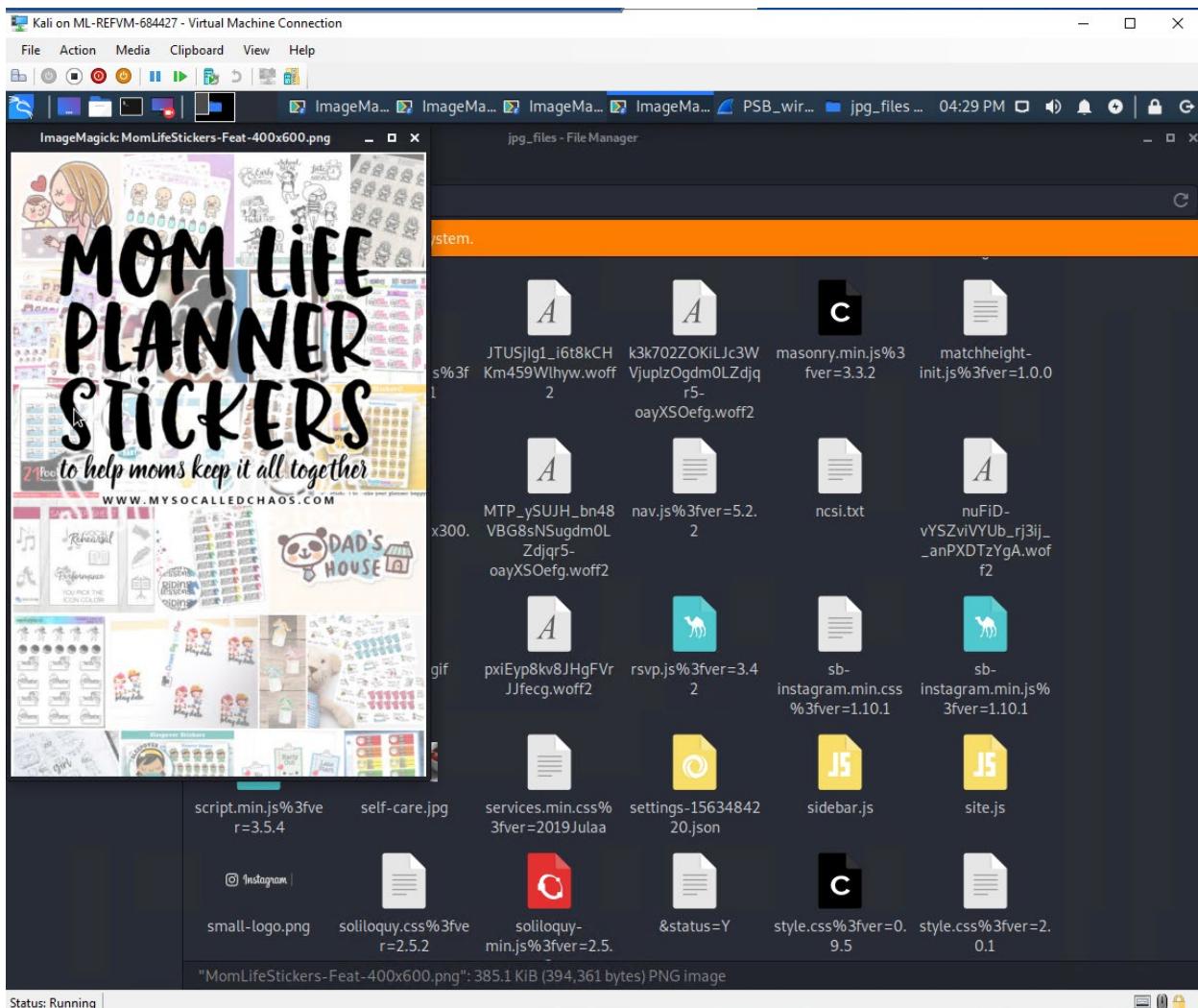
Wireshark_dll_file_to_test1

Network Analysis Report by Paul Barrett



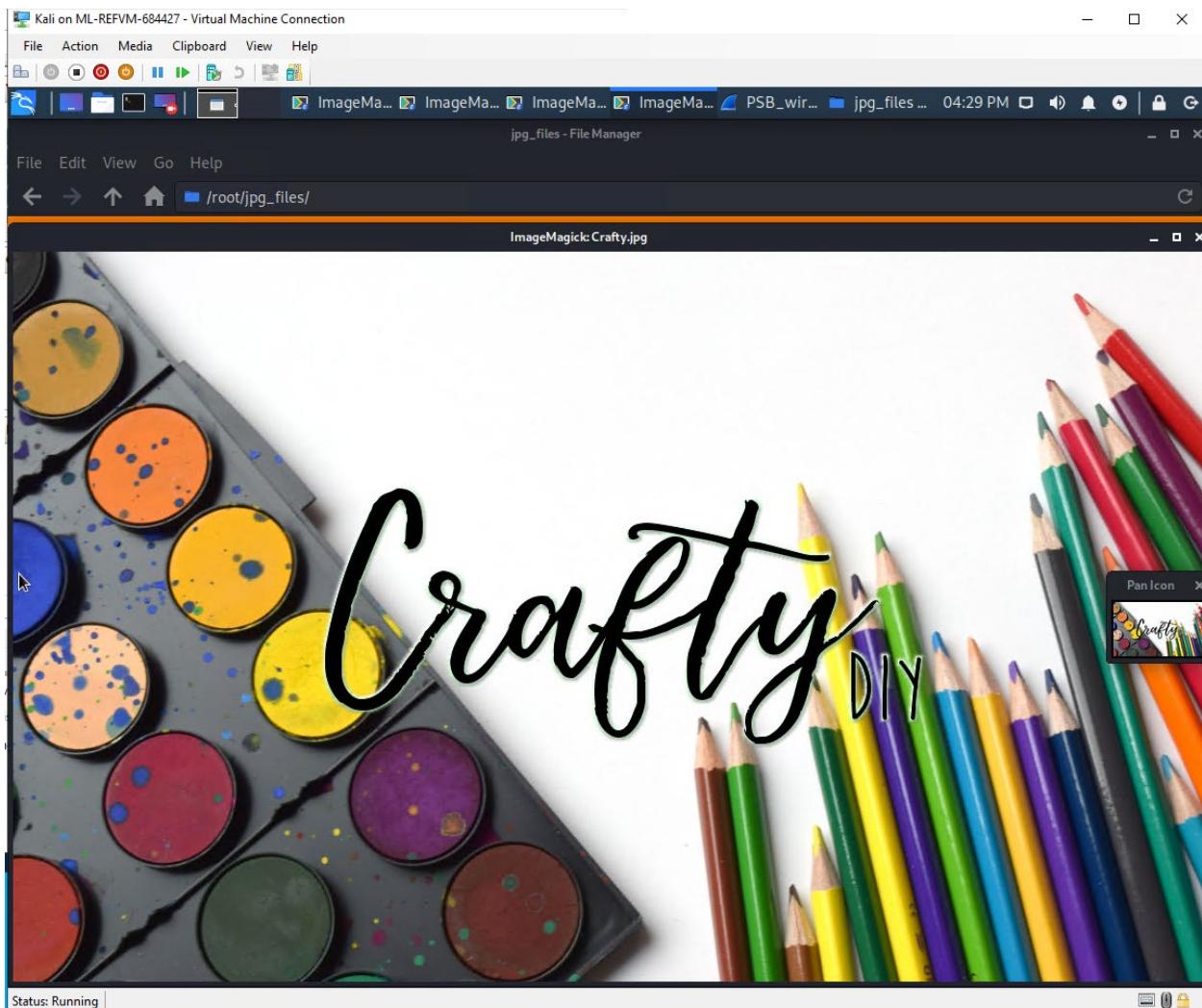
Wireshark_dll_file_to_test2

Network Analysis Report by Paul Barrett



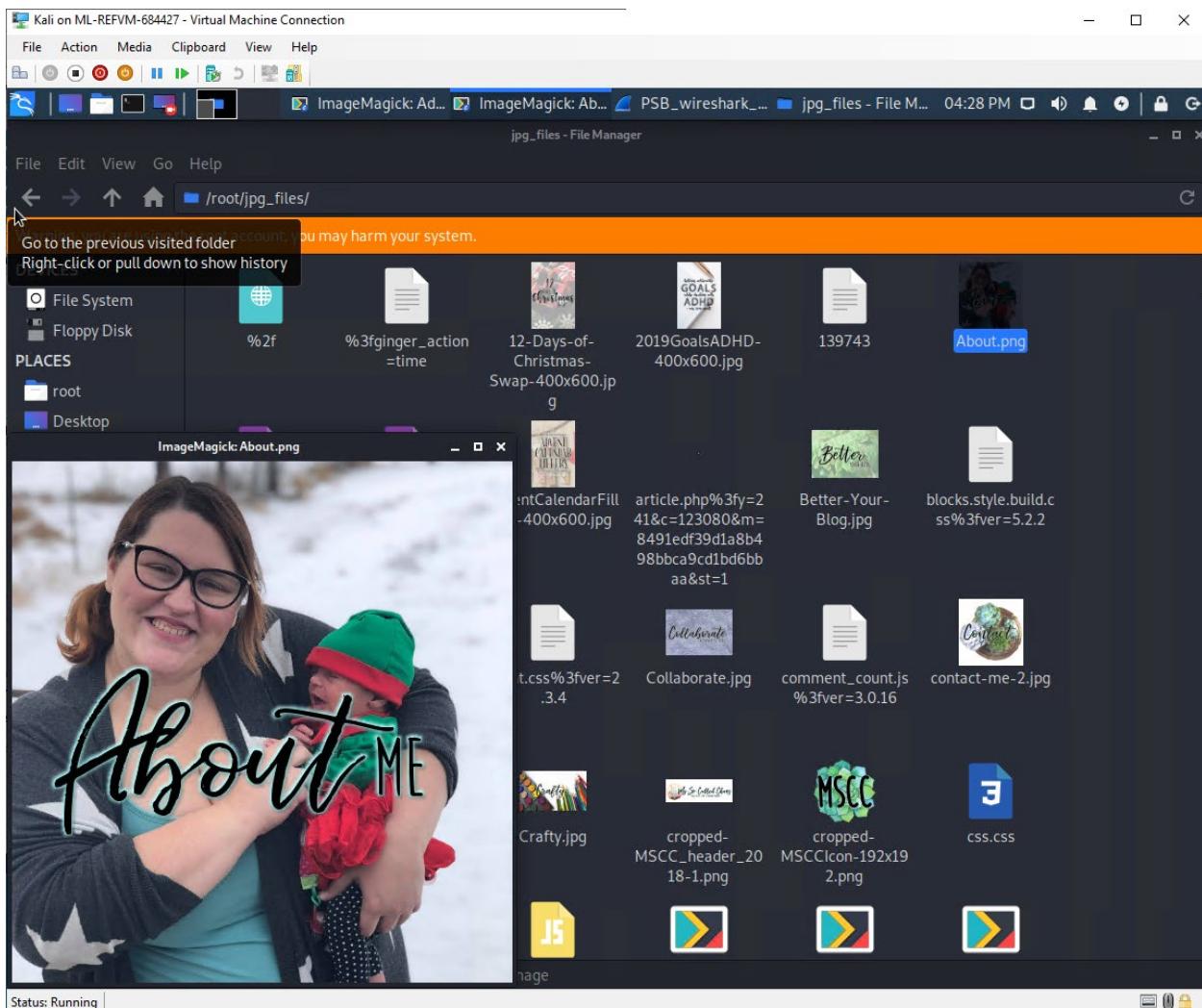
Wireshark_html_evidence1

Network Analysis Report by Paul Barrett



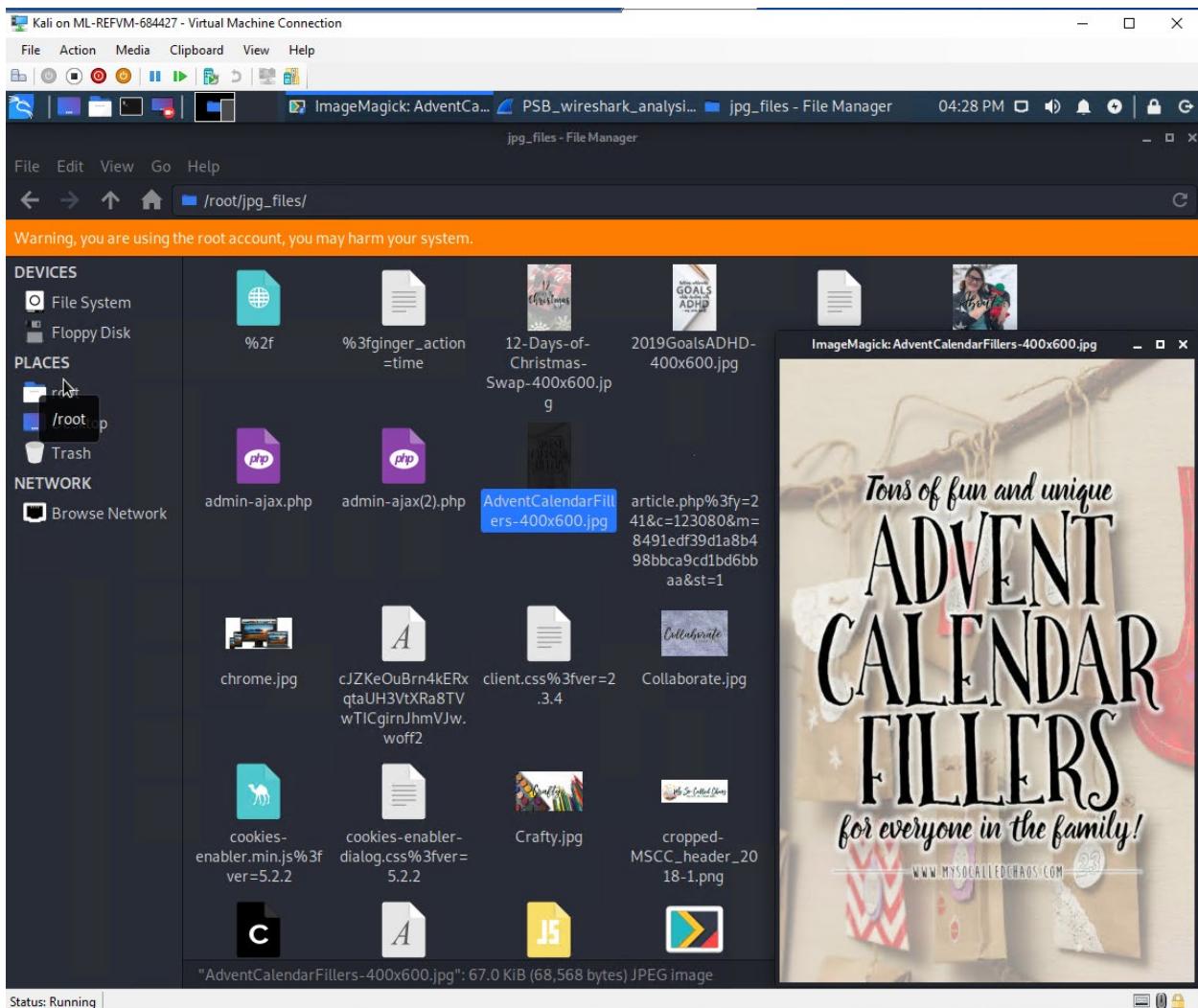
Wireshark_html_evidence2

Network Analysis Report by Paul Barrett



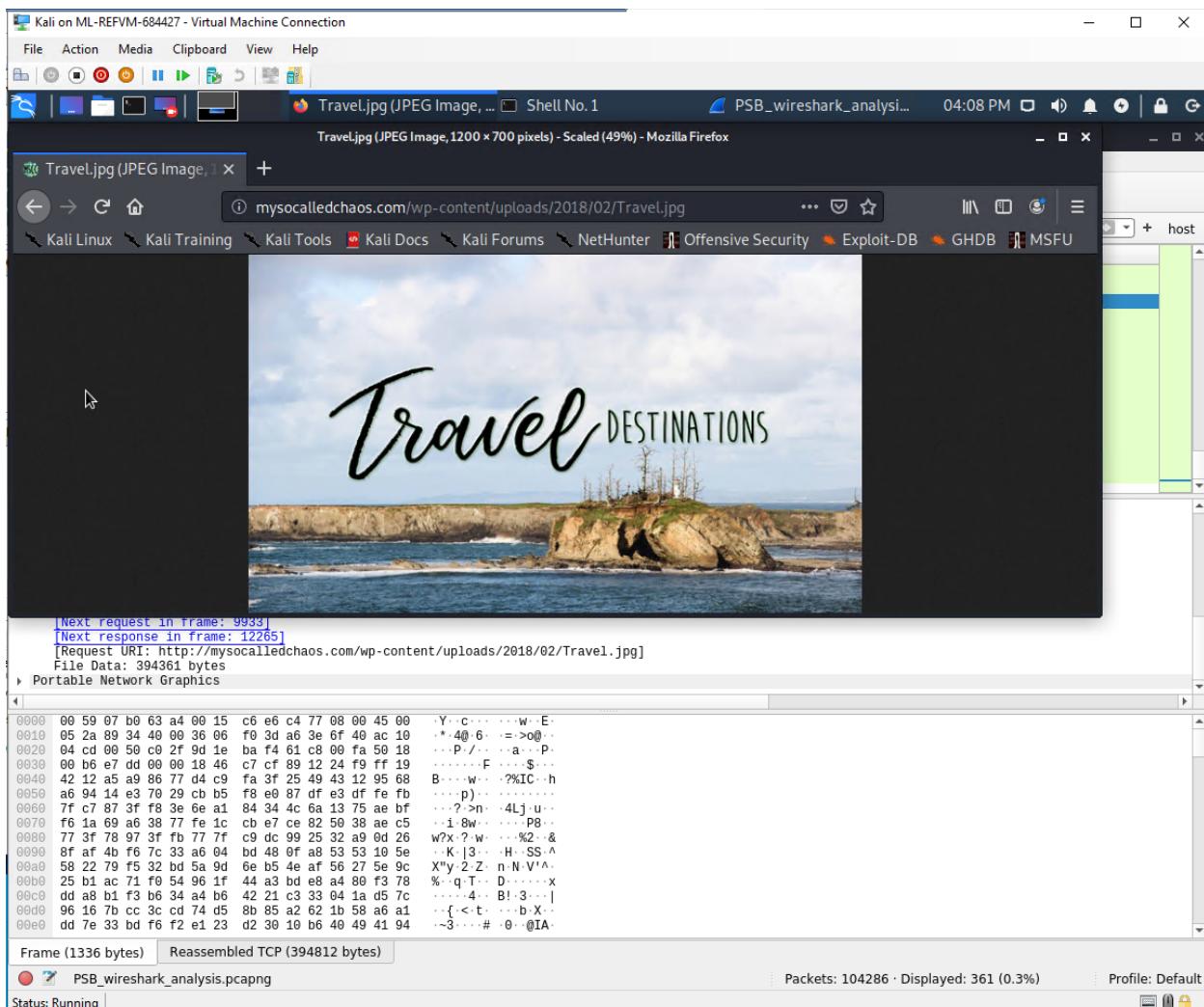
Wireshark_html_evidence3

Network Analysis Report by Paul Barrett



Wireshark_html_evidence4

Network Analysis Report by Paul Barrett



Wireshark_html_evidence5

Network Analysis Report by Paul Barrett

The screenshot shows a Wireshark interface running on a Kali Linux VM. The main pane displays a list of network packets, primarily HTTP requests from various sources to a destination IP of 192.168.1.147. The packet details and bytes panes provide detailed information about one specific packet, which appears to be a POST request for a login or payment page. The packet details pane shows fields like 'Flags: 0x018 (PSH, ACK)', 'Window size value: 64240', and 'TCP payload (1435 bytes)'. The bytes pane shows the raw hex and ASCII data of the TCP payload, which includes form fields such as 'cmd', 'art', 'name', 'item_name', and 'item_n'. The status bar at the bottom indicates 'Status: Running'.

Wireshark_http200a

Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

PSB_wireshark_analysis.pcapng jpg_files - File Manager

05:08 PM

PSB_wireshark_analysis.pcapng

/root

File Edit view Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code == 200

No.	Time	Source	Destination	Protocol	Len	Info
69165	765.407581000	files.publicdomaintorrents.com	BLANCO-DESKTOP.dogoftheyear.net	HTTP	1489	HTTP/1.1 200 OK (text/html)
61780	792.388169200	snnmmnxkdhflwgthqismb.com	LAPTOP-5WKHX9Y9G.frank-n-ted.com	HTTP	1441	HTTP/1.1 200 OK (text/html)
4110	56.647694700	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	HTTP	1404	HTTP/1.1 200 OK (application/javascript)
4118	56.679262500	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	HTTP	1402	HTTP/1.1 200 OK (application/javascript)
39462	512.450948600	pictures.fasthealth.com	DESKTOP-B493FD.local	HTTP	1389	HTTP/1.1 200 OK (PNG)
60071	676.208169900	snnmmnxkdhflwgthqismb.com	LAPTOP-5WKHX9Y9G.frank-n-ted.com	HTTP	1371	HTTP/1.1 200 OK (text/html)
36701	488.525096100	d2vh5eny7syxed.cloudflare.net	Roger-MacBook-Pro.local	HTTP	1371	HTTP/1.1 200 OK (PNG)
+ 39935	516.171334300	www.sabethospital.com	DESKTOP-B493FD.local	HTTP	1363	HTTP/1.1 200 OK (JPEG/JFIF image)
4282	58.600426600	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	HTTP	1362	HTTP/1.1 200 OK (application/javascript)
40574	521.806837700	dtydtsb770155.cloudflare.net	Roger-MacBook-Pro.local	HTTP	1360	HTTP/1.1 200 OK (application/font-woff2)
35151	476.645083400	d2vh5eny7syxed.cloudflare.net	Roger-MacBook-Pro.local	HTTP	1343	HTTP/1.1 200 OK (application/javascript)
4518	61.925202500	gstaticadssl1.google.com	Rotterdam-PC.mind-hammer.net	HTTP	1343	HTTP/1.1 200 OK (font/woff2)
9927	147.2129860400	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	HTTP	1336	HTTP/1.1 200 OK (PNG)

Transmission Control Protocol, Src Port: 80, Dst Port: 50178, Seq: 268, Ack: 465, Len: 1309

Source Port: 80
Destination Port: 50178
[Stream index: 340]
[TCP Segment Len: 1309]
Sequence number: 268 (relative sequence number)
Sequence number (raw): 3394105059
[Next sequence number: 1578 (relative sequence number)]
Acknowledgment number: 465 (relative ack number)
Acknowledgment number (raw): 3053729208
0101 ... = Header Length: 20 bytes (5)
Flags: 0x019 (FIN, PSH, ACK)
Window size value: 237
[Calculated window size: 30336]
[Window size scaling factor: 128]
Checksum: 0x08e5 [unverified]

Frame (1363 bytes) Reassembled TCP (1576 bytes)

Transmission Control Protocol (tcp), 20 bytes

Packets: 104286 · Displayed: 361 (0.3%) · Profile: Default

Status: Running

Wireshark_http200b

Network Analysis Report by Paul Barrett

The screenshot shows a Wireshark interface with the following details:

- File Bar:** Kali on ML-REFVM-684427 - Virtual Machine Connection, File, Action, Media, Clipboard, View, Help.
- Toolbar:** Standard file operations like Open, Save, Print, and a search icon.
- Address Bar:** Server Not Found - Mozi... Shell No.1, PSB_wireshark_analysis.pcapng, 04:07 PM.
- Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Packet List:** A table showing packet details. The selected packet (4282) is highlighted in blue. The table includes columns: No., Time, Source, Destination, Protocol, Len, Info.
- Selected Packet Details:**
 - Time: 492.1769445000
 - Source: 13.33.255.25
 - Destination: 10.11.11.179
 - Protocol: HTTP
 - Len: 1335
 - Info: HTTP/1.1 200 OK (application/font-woff2)
- Selected Packet Bytes:** Shows the raw byte sequence of the selected packet.
- Selected Packet Hex:** Shows the hex representation of the selected packet.
- Status Bar:** Packets: 104286 · Displayed: 361 (0.3%) · Profile: Default · Status: Running.

Wireshark_http200c

Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Server Not Found - Mozi... [Shell No. 1] PSB_wireshark_analysis.pcapng 04:06 PM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code == 200

No.	Time	Source	Destination	Protocol	Len	Info
37022	492.1769445000	13.33.255.25	19.11.11.179	HTTP	1335	HTTP/1.1 200 OK (application/font-woff2)
40393	519.7979972000	13.33.255.25	10.11.11.179	HTTP	1335	HTTP/1.1 200 OK (application/font-woff2)
9927	147.2129604000	166.62.111.64	172.16.4.205	HTTP	1336	HTTP/1.1 200 OK (PNG)
4518	61.9252025000	172.174.4.163	172.16.4.205	HTTP	1343	HTTP/1.1 200 OK (font/woff2)
35151	476.6450834000	143.204.29.89	10.11.11.179	HTTP	1343	HTTP/1.1 200 OK (application/javascript)
40574	521.8068377000	13.33.255.25	10.11.11.179	HTTP	1360	HTTP/1.1 200 OK (application/font-woff2)
4282	58.6004260000	166.62.111.64	172.16.4.205	HTTP	1362	HTTP/1.1 200 OK (application/javascript)
39933	516.1713340000	12.133.50.21	10.11.11.195	HTTP	1363	HTTP/1.1 200 OK (JPEG JFIF image)
36701	488.5250961000	143.204.29.89	10.11.11.179	HTTP	1371	HTTP/1.1 200 OK (PNG)
60071	776.2081699000	5.101.51.151	10.6.12.203	HTTP	1371	HTTP/1.1 200 OK (text/html)
+ 39462	512.4509486000	12.133.50.22	10.11.11.195	HTTP	1389	HTTP/1.1 200 OK (PNG)
4115	56.6792625000	166.62.111.64	172.16.4.205	HTTP	1402	HTTP/1.1 200 OK (application/javascript)
4110	56.6476947000	166.62.111.64	172.16.4.205	HTTP	1404	HTTP/1.1 200 OK (application/javascript)
61786	792.3881692000	5.101.51.151	10.6.12.203	HTTP	1441	HTTP/1.1 200 OK (text/html)
69165	765.4975810000	168.215.194.14	10.0.0.201	HTTP	1489	HTTP/1.1 200 OK (text/html)

Last-Modified: Fri, 23 Aug 2019 15:18:14 GMT\r\n
Etag: "95049f-99a3-590ca509fd980"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 39331\r\n
Connection: close\r\n
Content-Type: image/png\r\n
Content-Language: UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 2.472800100 seconds]
[Request in frame: 39299]
[Request URI: http://pictures.fasthealth.com/pictures/283173.png?last_modified=1566573494]
File Data: 39331 bytes

Frame (1389 bytes) Reassembled TCP (39598 bytes)

PSB_wireshark_analysis.pcapng Packets: 104286 · Displayed: 361 (0.3%) Profile: Default

Status: Running

Wireshark_http200d

Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Server Not Found - Mozi... [Shell No. 1] PSB_wireshark_analysis.pcapng 04:06 PM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code == 200

No.	Time	Source	Destination	Protocol	Length	Info
37022	492.1769445000	13.33.255.25	10.11.11.179	HTTP	1335	HTTP/1.1 200 OK (application/font-woff2)
40393	519.7979972000	13.33.255.25	10.11.11.179	HTTP	1335	HTTP/1.1 200 OK (application/font-woff2)
9927	147.2129604000	166.62.111.64	172.16.4.205	HTTP	1336	HTTP/1.1 200 OK (PNG)
4518	61.9252025000	172.16.4.163	172.16.4.205	HTTP	1343	HTTP/1.1 200 OK (font/woff2)
35151	476.6450834000	143.204.29.89	10.11.11.179	HTTP	1343	HTTP/1.1 200 OK (application/javascript)
40574	521.8068377000	13.33.255.25	10.11.11.179	HTTP	1360	HTTP/1.1 200 OK (application/font-woff2)
4282	58.6004266000	166.62.111.64	172.16.4.205	HTTP	1362	HTTP/1.1 200 OK (application/javascript)
39933	516.1713343000	12.133.50.21	10.11.11.195	HTTP	1363	HTTP/1.1 200 OK (JPEG JFIF image)
36701	488.5250961000	143.204.29.89	10.11.11.179	HTTP	1371	HTTP/1.1 200 OK (PNG)
60071	676.2081699000	5.101.51.151	10.6.12.203	HTTP	1371	HTTP/1.1 200 OK (text/html)
39462	512.4599486000	12.133.50.22	10.11.11.195	HTTP	1389	HTTP/1.1 200 OK (PNG)
+ 4115	56.6792625000	166.62.111.64	172.16.4.205	HTTP	1402	HTTP/1.1 200 OK (application/javascript)
+ 4110	56.6476947000	166.62.111.64	172.16.4.205	HTTP	1404	HTTP/1.1 200 OK (application/javascript)
+ 61786	702.5881692000	5.101.51.151	10.6.12.203	HTTP	1441	HTTP/1.1 200 OK (text/html)
+ 69165	765.4675810000	168.215.194.14	10.0.0.201	HTTP	1489	HTTP/1.1 200 OK (text/html)

```
X-Backend: all_requests\r\n
Accept-Ranges: bytes\r\n
\r\n
[HTTP response 7/14]
[Time since request: 0.202552300 seconds]
[Prev request in frame: 3983]
[Prev response in frame: 4086]
[Request in frame: 4087]
[Next request in frame: 4116]
[Next response in frame: 4215]
[Request URI: http://mysocalledchaos.com/wp-content/uploads/2018/02/Beauty.jpg]
Content-encoded entity body (gzip): 861 bytes -> 1852 bytes
File Data: 1852 bytes
▶ Media Type
```

```
0000 00 59 07 b0 63 a4 00 15 c6 e6 c4 77 08 00 45 00 Y·c... ·w·E·
0010 05 6c 5b 1a 40 00 36 06 1e 16 a6 3e 6f 40 ac 10 1[ @ 6... >0...
0020 04 cd 00 50 c8 26 2b cf 41 77 7e 25 bd df 50 18 ..P-& Aw-%·P·
0030 00 ad d6 70 00 08 48 54 54 50 2f 31 2e 33 20 32 ..p·HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 4c 61 73 74 2d 4d 6f 64 69 00 OK ·L ast-Modi
0050 66 69 65 64 3a 20 46 72 69 2c 20 31 39 29 4a 61 fied: Fr i, 19 Ja
0060 6e 20 32 30 31 38 20 30 32 3a 32 39 3a 35 33 29 n 2018 0 2:29:53
0070 47 4d 54 0d 0a 45 54 61 67 3a 20 22 37 33 63 2d GMT- ETa g: "73c-
0080 35 36 33 31 37 64 61 66 64 38 61 34 30 26 67 7a 56317daf d8a40-qz
0090 69 70 22 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 ip"- Cac he-Contr
00a0 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 36 38 34 38 ol: max- age=6048
00b0 30 30 0d 0a 45 78 70 69 72 65 73 3a 20 54 75 65 00 Expi res: Tue
00c0 2c 20 32 33 26 4a 75 6c 28 32 30 31 39 28 31 31 , 23 Jul 2019 11
00d0 3a 30 38 34 30 36 20 47 4d 54 0d 0a 43 6f 6e 74 :08:06 G MI·Cont
00e0 65 6e 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a ent-Encod ing: gz
```

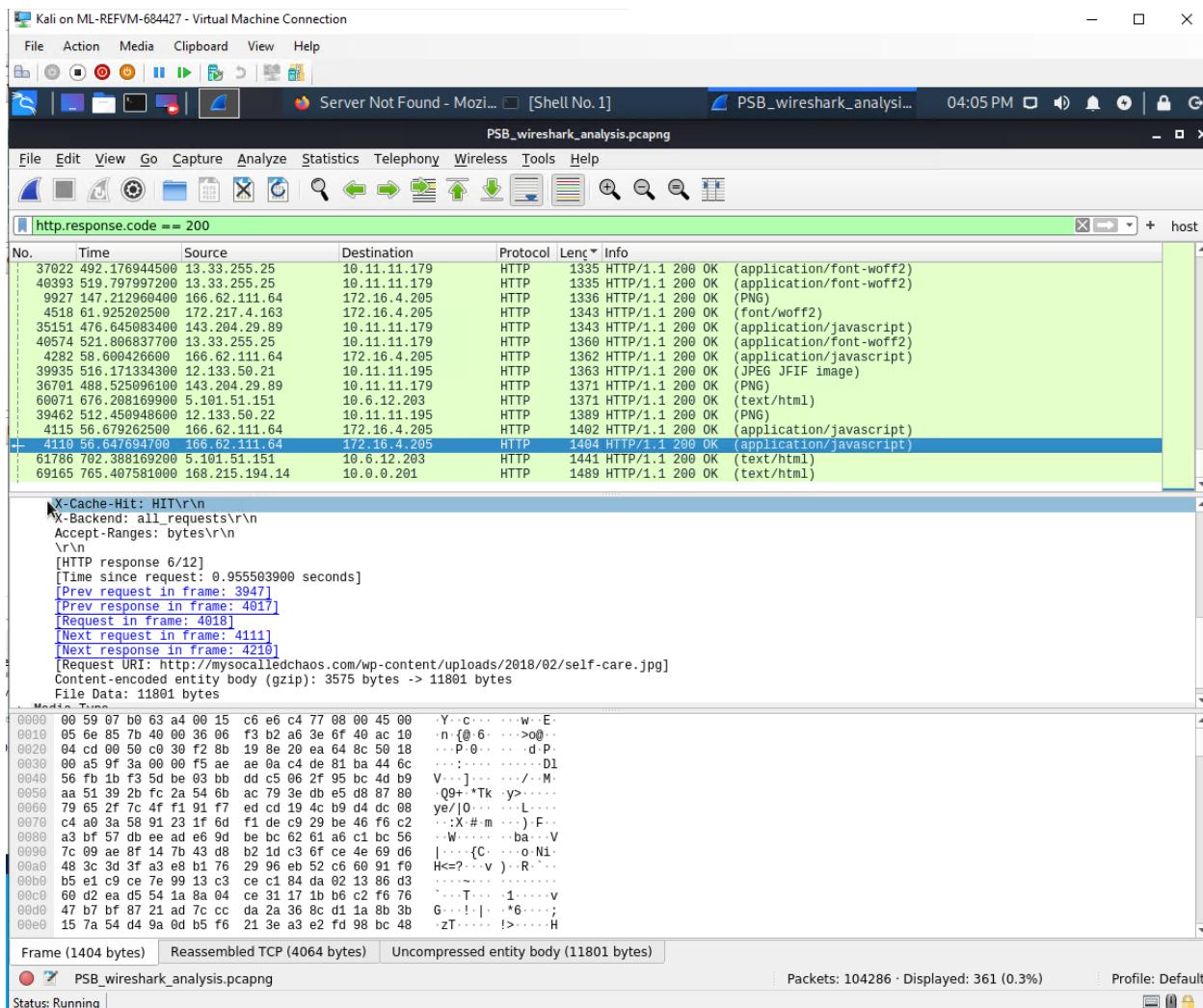
Frame (1402 bytes) Uncompressed entity body (1852 bytes)

PSB_wireshark_analysis.pcapng Packets: 104286 · Displayed: 361 (0.3%) Profile: Default

Status: Running

Wireshark_http200e

Network Analysis Report by Paul Barrett



Wireshark_http200f

Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Server Not Found - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.113 Safari/537.36 [Shell No. 1] PSB_wireshark_analysis.pcapng 04:04 PM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code == 200

No.	Time	Source	Destination	Protocol	Length	Info
37922	492.176944500	13.33.255.25	10.11.11.179	HTTP	1335	HTTP/1.1 200 OK (application/font-woff2)
40393	519.797997200	13.33.255.25	10.11.11.179	HTTP	1335	HTTP/1.1 200 OK (application/font-woff2)
9927	147.2129660400	166.62.111.64	172.16.4.205	HTTP	1336	HTTP/1.1 200 OK (PNG)
4518	61.925202500	172.217.4.163	172.16.4.205	HTTP	1343	HTTP/1.1 200 OK (font/woff2)
35151	476.645683400	143.204.29.89	10.11.11.179	HTTP	1343	HTTP/1.1 200 OK (application/javascript)
40574	521.806837700	13.33.255.25	10.11.11.179	HTTP	1360	HTTP/1.1 200 OK (application/font-woff2)
4282	58.600426600	166.62.111.64	172.16.4.205	HTTP	1362	HTTP/1.1 200 OK (application/javascript)
39935	516.171334300	12.133.50.21	10.11.11.195	HTTP	1363	HTTP/1.1 200 OK (JPEG JFIF image)
36701	488.525096100	143.204.29.89	10.11.11.179	HTTP	1371	HTTP/1.1 200 OK (PNG)
60073	676.208169900	5.101.51.151	10.6.12.203	HTTP	1371	HTTP/1.1 200 OK (text/html)
39462	512.450948600	12.133.50.22	10.11.11.195	HTTP	1389	HTTP/1.1 200 OK (PNG)
4115	56.679262500	166.62.111.64	172.16.4.205	HTTP	1402	HTTP/1.1 200 OK (application/javascript)
4119	56.647694700	166.62.111.64	172.16.4.205	HTTP	1404	HTTP/1.1 200 OK (application/javascript)
+ 61786	782.388169200	5.191.51.151	10.6.12.293	HTTP	1441	HTTP/1.1 200 OK (text/html)
+ 69165	765.407581000	168.215.184.14	10.0.0.201	HTTP	1489	HTTP/1.1 200 OK (text/html)

```

Content-Type: text/html; charset=UTF-8\r\n
Transfer-Encoding: chunked\r\n
Connection: close\r\n
Vary: Accept-Encoding\r\n
Vary: Accept-Encoding\r\n
\r\n
[HTTP response 1/1]
[Time since request: 26.078086400 seconds]
[Request in frame: 60102]
[Request URI: http://smnmmnkxdhflwgthqismb.com/post.php]
  HTTP chunked response
  File Data: 926352 bytes
> Line-based text data: text/html (7379 lines)

```

```

00000000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK.
00000010 0a 53 65 72 76 65 72 3a 20 6e 67 69 6e 78 0d 0a .Server: nginx.
00000020 44 61 74 65 3a 20 46 72 69 2c 20 31 32 20 4a 75 Date: Fr 1, 12 Ju
00000030 6e 20 32 30 32 30 20 31 37 3a 31 37 3a 31 32 20 n 2020 1 7:17:12
00000040 47 4d 54 0d 0a 43 6f 6e 74 65 66 74 2d 54 79 70 GMT-Content-Type
00000050 65 3a 20 74 65 78 74 2f 68 74 6e 6c 3b 20 63 68 e: text/html; ch
00000060 61 72 73 65 74 3d 55 54 46 2d 38 0d 0a 54 72 61 arset:UTF-8-Tra
00000070 66 73 66 65 72 4d 6e 63 6f 64 69 6e 67 3a 20 nsfer-En coding:
00000080 63 68 75 66 6b 65 64 0d 0a 43 6f 6e 6e 65 63 74 chunked-Connect
00000090 69 67 6e 3a 20 63 6c 6f 73 65 0d 0a 56 61 72 79 ion: cl se-Vary
000000a0 3a 20 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e : Accept -Encoding
000000b0 67 0d 0a 56 61 72 79 3a 20 41 63 63 65 70 74 2d g-Vary: Accept-
000000c0 45 6e 63 6f 64 69 6e 67 0d 0a 0d 0a 31 66 33 38 Encoding ...if38
000000d0 0d 0a 02 4c 2b 10 64 70 92 1a c8 53 9e 2d 27 67 ..L+dp...S-'g
000000e0 4a 6b 12 79 83 e7 2b 03 4a 08 ae 43 4d 46 6e ec Jk...+J-CMFN
```

Frame (1441 bytes) Reassembled TCP (927299 bytes) De-chunked entity body (926352 bytes)

HTTP Response For-URI (http.response_for.uri) Packets: 104286 · Displayed: 361 (0.3%) Profile: Default

Status: Running

Wireshark_http200g

Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Server Not Found - Mozi... [Shell No. 1] PSB_wireshark_analysis.pcapng 04:04 PM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code == 200

No.	Time	Source	Destination	Protocol	Len	Info
37022	492.1769445000	13.33.255.25	10.11.11.179	HTTP	1335	HTTP/1.1 200 OK (application/font-woff2)
40393	519.7979972000	13.33.255.25	10.11.11.179	HTTP	1335	HTTP/1.1 200 OK (application/font-woff2)
9927	147.2129604000	166.62.111.64	172.16.4.205	HTTP	1336	HTTP/1.1 200 OK (PNG)
4518	61.9252025000	12.133.255.25	172.16.4.205	HTTP	1343	HTTP/1.1 200 OK (font/woff2)
35151	476.6450834000	143.204.29.89	10.11.11.179	HTTP	1343	HTTP/1.1 200 OK (application/javascript)
40574	521.8068377000	13.33.255.25	10.11.11.179	HTTP	1360	HTTP/1.1 200 OK (application/font-woff2)
4282	58.6004266000	166.62.111.64	172.16.4.205	HTTP	1362	HTTP/1.1 200 OK (application/javascript)
39933	516.1713343000	12.133.50.21	10.11.11.195	HTTP	1363	HTTP/1.1 200 OK (JPEG JFIF image)
36701	488.5250961000	143.204.29.89	10.11.11.179	HTTP	1371	HTTP/1.1 200 OK (PNG)
60671	676.2081699000	5.101.51.151	10.6.12.203	HTTP	1371	HTTP/1.1 200 OK (text/html)
39462	512.4509486000	12.133.50.22	10.11.11.195	HTTP	1389	HTTP/1.1 200 OK (PNG)
4115	56.6792625000	166.62.111.64	172.16.4.205	HTTP	1402	HTTP/1.1 200 OK (application/javascript)
4110	56.6476947000	166.62.111.64	172.16.4.205	HTTP	1404	HTTP/1.1 200 OK (application/javascript)
61786	702.3881692000	5.101.51.151	10.6.12.203	HTTP	1441	HTTP/1.1 200 OK (text/html)
+ 69165	765.4075810000	168.215.194.14	10.0.0.201	HTTP	1489	HTTP/1.1 200 OK (text/html)

```

Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Transfer-Encoding: chunked\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.272021400 seconds]
[Request in frame: 69126]
[Next request in frame: 69167]
[Next response in frame: 69417]
[Request URI: http://publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrab.jpg]
HTTP chunked response
File Data: 10724 bytes
Time based font data font.html (771 bytes)

```

```

0000 00 16 17 18 66 c8 00 09 b7 27 a1 3e 08 00 45 00 ...f... '...>..E
0010 05 c3 23 00 00 00 80 06 9c 86 a8 d7 c2 0e 0a 00 ...#.....
0020 00 c9 00 5c 02 99 5c d8 2d 28 2d 00 00 1e 50 18 ...P \` -(-.-P
0030 fa f0 0a 00 00 00 74 79 78 65 3d 22 63 6d 64 22 20 76 .....ty pe="hidd
0040 65 6e 22 20 6e 61 6d 65 3d 22 63 6d 64 22 20 76 en" name ="cmd" v
0050 61 6c 75 65 3d 22 5f 63 61 72 74 22 3e 0a 3c 69 alue="c art"><1
0060 66 70 75 74 20 74 79 79 65 3d 22 68 69 64 64 65 input typ e="hidde
0070 62 22 20 6e 61 6d 65 3d 22 62 75 73 69 6e 65 73 n" name ="busines
0080 73 22 20 76 61 6c 75 65 3d 22 70 61 79 78 61 6c s" value ="paypal
0090 40 6d 77 2e 6e 65 74 22 3e 0a 3c 69 6e 70 75 74 @mw.net" ><input
00a0 20 74 79 70 65 3d 22 68 69 64 64 65 6e 22 20 6e type="h idden" n
00b0 61 6d 65 3d 22 69 74 65 6d 5f 6e 61 6d 65 22 20 ame="ite _name"
00c0 76 61 6c 75 65 3d 22 42 65 74 74 79 20 42 6f 6f value="B etty Boo
00d0 70 20 2d 20 52 79 74 68 6d 20 6f 6e 20 74 68 65 p - Ryth m on the
00e0 20 52 65 73 65 72 76 61 74 69 6f 6e 22 3e 0a 3c Reserva tion"><

```

Frame (1489 bytes) Reassembled TCP (11056 bytes) De-chunked entity body (10724 bytes)

PSB_wireshark_analysis.pcapng Packets: 104286 · Displayed: 361 (0.3%) Profile: Default

Status: Running

Wireshark_http200h

Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Server Not Found - Mozi... [Shell No. 1] PSB_wireshark_analysis.pcapng 04:03 PM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code == 200

No.	Time	Source	Destination	Protocol	Length	Info
38170	502.7419535000	35.199.92.63	10.11.11.179	HTTP	202	HTTP/1.1 200 OK (text/plain)
42390	538.7514688000	35.186.255.8	10.11.11.179	HTTP	1144	HTTP/1.1 200 OK (text/javascript)
42257	537.4435893000	35.186.255.8	10.11.11.179	HTTP	926	HTTP/1.1 200 OK (text/javascript)
53967	637.4117660000	35.185.55.255	10.11.11.217	HTTP	974	HTTP/1.1 200 OK (PNG)
53966	637.3961699000	35.185.55.255	10.11.11.217	HTTP	1045	HTTP/1.1 200 OK (image/x-icon)
42023	535.3269813000	35.185.55.255	10.11.11.217	HTTP	399	HTTP/1.1 200 OK
41618	530.8919978000	35.185.55.255	10.11.11.217	HTTP	445	HTTP/1.1 200 OK (GIF89a)
+ 41618	530.8839205000	35.185.55.255	10.11.11.217	HTTP	637	HTTP/1.1 200 OK (PNG)
41608	530.8676136000	35.185.55.255	10.11.11.217	HTTP	123	HTTP/1.1 200 OK (JPEG JFIF image)
41608	530.7295947000	35.185.55.255	10.11.11.217	HTTP	407	HTTP/1.1 200 OK (application/javascript)
41594	530.6915869000	35.185.55.255	10.11.11.217	HTTP	1217	HTTP/1.1 200 OK (application/javascript)
+ 41593	530.6633357000	35.185.55.255	10.11.11.217	HTTP	962	HTTP/1.1 200 OK (application/javascript)
41559	530.2358140000	35.185.55.255	10.11.11.217	HTTP	511	HTTP/1.1 200 OK (application/javascript)
41557	530.2050808000	35.185.55.255	10.11.11.217	HTTP	200	HTTP/1.1 200 OK (application/javascript)
41553	530.1716699000	35.185.55.255	10.11.11.217	HTTP	920	HTTP/1.1 200 OK (application/javascript)
41544	530.1309786000	35.185.55.255	10.11.11.217	HTTP	1182	HTTP/1.1 200 OK (application/javascript)

```

ETag: "58dd08480-e9"\r\n
Cache-Control: public, max-age=31536000\r\n
Vary: Accept-Encoding\r\n
Access-Control-Allow-Origin: *\r\n
Accept-Ranges: bytes\r\n
\r\n
[HTTP response 5/5]
[Time since request: 0.211809400 seconds]
[Prev request in frame: 41552]
[Prev response in frame: 41593]
[Request in frame: 41593]
[Request URI: http://www.iphonehacks.com/wp-content/themes/iphonehacks/img/menu.png]
[File Data: 233 bytes]
Portable Network Graphics
0000 e8 b2 ac ac b2 49 00 01 c9 97 4b f0 08 00 45 00 .....I...K..E.
0010 02 6f fc a2 48 00 38 06 d2 4a 23 b9 37 ff 0a 0b o @ 8...J# 7...
0020 0b dd 00 50 f4 3a 7f 4f 36 de 7f f6 76 b6 50 18 ...P;... 0..v.P.
0030 00 42 73 47 00 00 48 54 54 50 2f 31 2e 31 20 32 BsG .HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 53 65 72 76 65 72 3a 20 6e 00 OK .S erver: n
0050 67 69 6e 78 0d 0a 44 61 74 65 3a 20 4d 6f 6e 2c ginx .Da te: Mon,
0060 20 31 31 20 4e 6f 76 29 32 30 31 39 20 32 32 3a 11 Nov 2019 22:
0070 32 32 3a 33 38 20 47 4d 54 0d 0a 43 6f 6e 74 65 22:38 Gh T. Conte
0080 6e 74 2d 54 79 70 65 3a 20 69 6d 61 67 65 2f 70 nt-Type: image/p
0090 6e 67 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 ng. Cont ent-Leng
00a0 74 68 3a 20 32 33 0d 0a 4c 61 73 74 2d 4d 6f th: 233 .Last-Mo
00b0 64 69 66 69 65 64 3a 29 54 68 75 2c 20 33 39 20 dified: Thu, 30
00c0 4d 61 72 20 32 30 31 37 26 32 32 3a 31 39 3a 34 Mar 2017 22:19:4
00d0 34 20 47 4d 54 0d 0a 43 6f 6e 66 65 63 74 69 6f 4 GMT .C onnectio
00e0 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 4b n: keep- alive .K
00f0 65 65 70 2d 41 6c 69 76 65 3a 20 74 69 6d 65 6f eep-Aliv e: timo
0100 ut=20 .E Tag: "58

```

PSB_wireshark_analysis.pcapng Packets: 104286 Displayed: 361 (0.3%) Profile: Default

Status: Running

Wireshark_http200i

Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Server Not Found - Mozilla [Shell No. 1] PSB_wireshark_analysis.pcapng 04:01 PM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code == 200

No.	Time	Source	Destination	Protocol	Length	Info
68803	764.156489400	72.21.91.29	10.0.0.201	OCSP	842	Response
68767	764.030626300	72.21.91.29	10.0.0.201	OCSP	842	Response
68766	764.017151100	72.21.91.29	10.0.0.201	OCSP	842	Response
68736	763.895055100	72.21.91.29	10.0.0.201	OCSP	842	Response
68734	763.881596400	72.21.91.29	10.0.0.201	OCSP	842	Response
68733	763.868118800	72.21.91.29	10.0.0.201	OCSP	842	Response
31796	461.454898700	72.21.91.29	172.16.4.205	OCSP	842	Response
31794	461.436762200	72.21.91.29	172.16.4.205	OCSP	842	Response
31752	61.266233200	72.21.91.29	172.16.4.205	OCSP	842	Response
31749	461.247138900	72.21.91.29	172.16.4.205	OCSP	842	Response
+ 69479	769.964256500	72.21.202.62	10.0.0.201	HTTP	1310	HTTP/1.1 200 OK (text/html)
35733	483.117443100	67.199.248.26	10.11.11.179	HTTP	538	HTTP/1.1 200 OK (application/javascript)
40184	517.732618400	66.171.225.80	10.11.11.179	OCSP	979	Response
38894	506.098543900	66.171.225.80	10.11.11.179	OCSP	979	Response
40190	517.795058600	66.171.225.75	10.11.11.179	OCSP	518	Response
69949	99.454591000	54.230.89.184	172.16.4.205	HTTP	432	HTTP/1.1 200 OK (text/html)
Server: Server\r\np3p: policyref="http://rcm.amazon.com/w3c/p3p-us.xml",CP="CAO DSP LAW CUR ADM IVAo IVDo CONo OTPo OUR DELi PUBl OTRi BUS PHY ONL UNI PUR FIN COM NAV INT Cache-control: no-store\r\nContent-Length: 8205\r\nConnection: close\r\nContent-Type: text/html\r\n\r\n[HTTP response 1/1]\r\n[Time since request: 0.144745400 seconds]\r\n[Request in frame: 69479]						
[Request URI [truncated]: http://rcm-na.amazon-adsystem.com/e/cm?t=publicdomainf-20&o=1&p=4&l=o&vpid=40C236A13FDD0B68&ref-url=http%3A//publicdomainfo]						
File Data: 8285 bytes						
Line-based text data: text/html (1 lines)						
Frame (1310 bytes) Reassembled TCP (8556 bytes)						
HTTP Response For-URI (http.response_for.uri) Packets: 104286 · Displayed: 361 (0.3%) Profile: Default						
Status: Running						

Wireshark_http200j

Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

[Shell No. 1] PSB_wireshark_analysis.pcapng 03:56 PM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code == 200

No.	Time	Source	Destination	Protocol	Length	Info
43214	545.781483100	94.31.29.96	10.11.11.217	HTTP	637	HTTP/1.1 200 OK (PNG)
43167	545.279139100	94.31.29.96	10.11.11.217	HTTP	936	HTTP/1.1 200 OK (JPEG JFIF image)
43131	544.792663100	94.31.29.96	10.11.11.217	HTTP	469	HTTP/1.1 200 OK (JPEG JFIF image)
43105	544.425734900	94.31.29.96	10.11.11.217	HTTP	549	HTTP/1.1 200 OK (JPEG JFIF image)
43094	544.361281100	94.31.29.96	10.11.11.217	HTTP	563	HTTP/1.1 200 OK (JPEG JFIF image)
43092	544.330712500	94.31.29.96	10.11.11.217	HTTP	292	HTTP/1.1 200 OK (JPEG JFIF image)
43078	544.224233100	94.31.29.96	10.11.11.217	HTTP	450	HTTP/1.1 200 OK (JPEG JFIF image)
43075	544.187858000	94.31.29.96	10.11.11.217	HTTP	272	HTTP/1.1 200 OK (JPEG JFIF image)
43061	544.112372700	94.31.29.96	10.11.11.217	HTTP	367	HTTP/1.1 200 OK (JPEG JFIF image)
43061	544.069269700	94.31.29.96	10.11.11.217	HTTP	619	HTTP/1.1 200 OK (JPEG JFIF image)
43053	544.026431700	94.31.29.96	10.11.11.217	HTTP	237	HTTP/1.1 200 OK (JPEG JFIF image)
43050	543.993551500	94.31.29.96	10.11.11.217	HTTP	832	HTTP/1.1 200 OK (PNG)
43038	543.921152100	94.31.29.96	10.11.11.217	HTTP	278	HTTP/1.1 200 OK (JPEG JFIF image)
43033	543.863990100	94.31.29.96	10.11.11.217	HTTP	342	HTTP/1.1 200 OK (JPEG JFIF image)
43017	543.797891500	94.31.29.96	10.11.11.217	HTTP	436	HTTP/1.1 200 OK (JPEG JFIF image)
43010	543.661498600	94.31.29.96	10.11.11.217	HTTP	614	HTTP/1.1 200 OK (PNG)

```

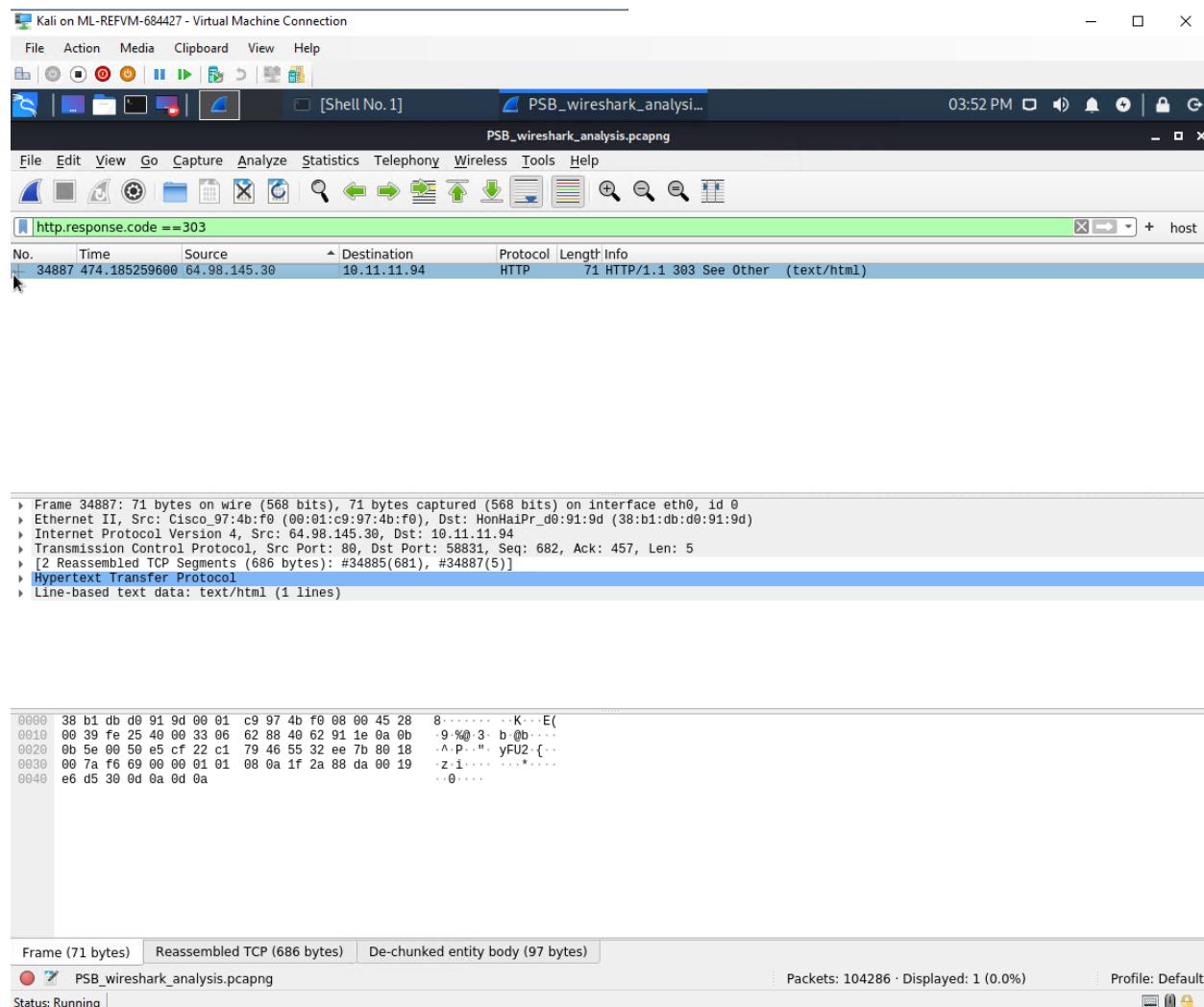
Etag: "5d91f8c7-6ec"\r\n
Cache-Control: public, max-age=31536000\r\n
Vary: Accept-Encoding\r\n
Access-Control-Allow-Origin: *\r\n
Server: NetDNA-cache/2.2\r\n
X-Cache: HIT\r\n
Accept-Ranges: bytes\r\n
\r\n
[HTTP response 5/5]
[Time since request: 0.417405600 seconds]
[Prev request in frame: 43071]
[Prev response in frame: 43092]
[Request in frame: 43101]
[Request URI: http://cdn.iphonehacks.com/wp-content/uploads/2019/09/11pro-grass-rear-iphonehacks-67x67.jpg]

```

Frame (469 bytes) Reassembled TCP (2126 bytes)	Packets: 104286 · Displayed: 361 (0.3%)	Profile: Default
HTTP Response For-URI (http.response_for.uri)	Status: Running	

Wireshark_http200k

Network Analysis Report by Paul Barrett



Wireshark_http303a

Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

PSB_wireshark_analysis.pcapng jpg_files - File Manager

04:47 PM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp contains jpg

No.	Time	Source	Destination	Protocol	Length	Info
41579	530.5705964000	10.11.11.217	35.185.55.255	HTTP	499	GET /wp-content/themes/iphonenhacks/img/logo.jpg HTTP/1.1
12277	186.1965206000	172.16.4.295	93.95.100.178	HTTP	375	GET /browserfiles/img/chrome.jpg HTTP/1.1
91184	1037.9050597	172.16.4.295	93.95.100.178	TCP	375 [TCP Retransmission]	49239 - 80 [PSH, ACK] Seq=1 Ack=1 Win=66304 Len=321
42937	543.0556758000	10.11.11.217	94.31.29.96	HTTP	508	GET /wp-content/uploads/2017/11/iPhone-X-Home-screen-194x129.jpg HTTP/1...
42942	543.0824202000	10.11.11.217	94.31.29.96	HTTP	503	GET /wp-content/uploads/2019/10/checkrain-teaser-194x129.jpg HTTP/1...
43002	543.5926935000	10.11.11.217	94.31.29.96	HTTP	508	GET /wp-content/uploads/2017/11/iPhone-X-Body-Shots-1-194x129.jpg HTTP/1...
43003	543.6011937000	10.11.11.217	94.31.29.96	HTTP	531	GET /wp-content/uploads/2017/11/iPhone-X-Lock-screen-No-Notifications-Lo...
43033	543.9292344000	10.11.11.217	94.31.29.96	HTTP	505	GET /wp-content/uploads/2019/09/iphone-11-pro-camera-67x67.jpg HTTP/1.1
43045	543.9431135000	10.11.11.217	94.31.29.96	HTTP	508	GET /wp-content/uploads/2019/10/airpods-pro-tips-tricks-67x67.jpg HTTP/1...
43047	543.9511203000	10.11.11.217	94.31.29.96	HTTP	500	GET /wp-content/uploads/2019/10/inprogress-iph-67x67.jpg HTTP/1.1
43063	544.1064997000	10.11.11.217	94.31.29.96	HTTP	507	GET /wp-content/uploads/2019/10/note10plus-iphone11pro-67x67.jpg HTTP/1...
43065	544.1204194000	10.11.11.217	94.31.29.96	HTTP	501	GET /wp-content/uploads/2019/07/macbook-pro-2019-67x67.jpg HTTP/1.1
43070	544.1322925000	10.11.11.217	94.31.29.96	HTTP	495	GET /wp-content/uploads/2019/11/BentoStack-67x67.jpg HTTP/1.1
43071	544.1416182000	10.11.11.217	94.31.29.96	HTTP	593	GET /wp-content/uploads/2019/09/Apple_watch_series_5-gold-aluminum-case-...
43095	544.9275400000	10.11.11.217	94.31.29.96	HTTP	500	GET /wp-content/uploads/2019/09/iphonexr-67x67.jpg HTTP/1.1

Transmission Control Protocol, Src Port: 80, Dst Port: 49757, Seq: 11559, Ack: 410, Len: 1460

Source Port: 80
 Destination Port: 49757
 [Stream index: 865]
 [TCP Segment Len: 1460]
 Sequence number: 11559 (relative sequence number)
 Sequence number (raw): 48465047
 [Next sequence number: 13019 (relative sequence number)]
 Acknowledgment number: 410 (relative ack number)
 Acknowledgment number (raw): 2013719029
 0101 . . . = Header Length: 20 bytes (5)
 Flags: 0x018 (PSH, ACK)
 Window size value: 64240
 [Calculated window size: 64240]
 [Window size scaling factor: -2 (no window scaling used)]
 Checksum: 0xd94 [unverified]

```
0020 00 c9 00 50 c2 5d 02 e3 84 97 78 06 e9 f5 50 18 ..P]..x...P
0030 fa f8 2d 94 00 00 00 32 63 0d 0a 3c 74 72 3e 3c .....2 c.<tr>
0040 74 64 3e 3a 61 20 68 72 65 66 3d 6e 73 68 6f 77 td>a hr ef=nshow
0050 6d 6f 76 69 65 2e 68 74 6d 6c 3f 6d 6f 76 69 65 movie.htm?movie
0060 69 64 3d 34 37 38 3e 0d 0a 31 34 0d 0a 58 6f 70 id=478> 14-Pop
0070 65 79 65 20 66 6f 72 20 58 72 65 73 69 64 65 6e eye for Presiden
0080 74 0d 0a 34 0d 0a 3c 2f 61 3e 0d 0a 31 38 0d 0a t: 4 .</a>..18..
0090 20 3c 69 6d 67 20 73 72 63 3d 70 64 61 2e 6a 70 <img sr=c:pda.jpg
00a0 67 3e 3c 2f 69 6d 67 3e 0d 0a 32 32 0d 0a 20 3c g=</img>..22..<
00b0 69 6d 67 20 73 72 63 3d 70 73 70 2e 67 69 66 3e img src= psp.gif>
00c0 3c 2f 69 6d 67 3e 3c 2f 74 64 3e 3c 2f 74 72 3e /><img> td></tr>
00d0 0d 0a 32 63 0d 0a 3c 74 72 3e 3c 74 64 3e 3c 61 .2c .<t r><d><a
00e0 20 68 72 65 66 3d 6e 73 68 6f 77 6d 6f 76 69 65 href=s:Immovie
00f0 2e 68 74 6d 6c 3f 6d 6f 76 69 66 69 64 3d 34 37 .html?mo vield=47
0100 39 3e 0d 0a 31 64 60 0a 58 6f 70 65 79 65 20 2d 9>.id. Popeye -
0110 20 46 72 69 67 68 74 20 74 6f 20 74 68 65 20 46 Fright to the F
0120 69 6e 69 73 68 0d 0a 34 0d 0a 3c 2f 61 3e 0d 0a inish.4 .</a>..
```

Transmission Control Protocol (tcp), 20 bytes

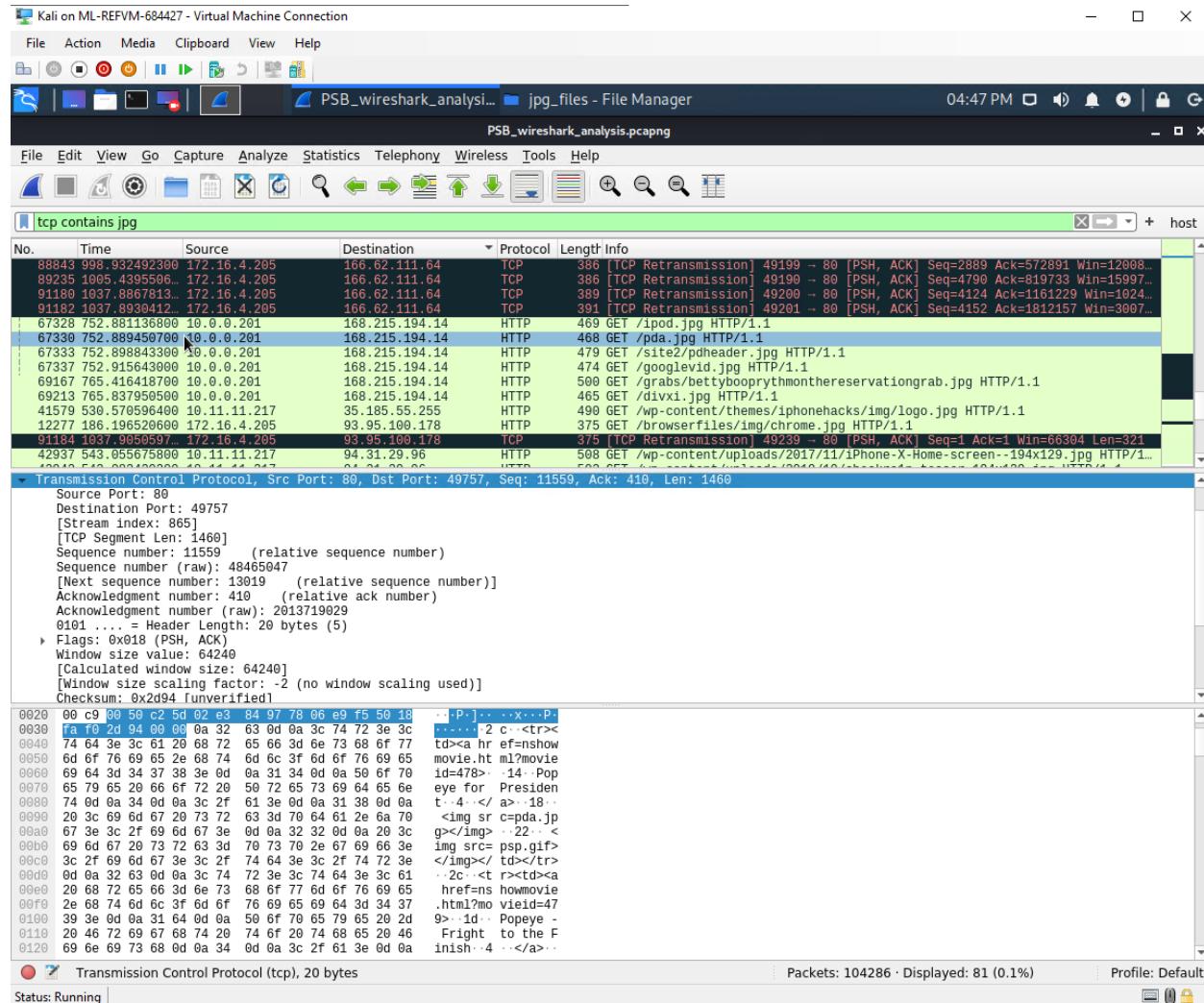
Packets: 104286 · Displayed: 81 (0.1%)

Status: Running

Profile: Default

Wireshark_jpg1

Network Analysis Report by Paul Barrett



Wireshark_jpg2

Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

PSB_wireshark_analysis.pcapng jpg_files - File Manager

04:46 PM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp contains jpg

No.	Time	Source	Destination	Protocol	Length	Info
39910	515.9981394000	10.11.11.195	12.133.50.21	HTTP	520	GET /docs/health-bk.jpg HTTP/1.1
35191	476.9582129000	10.11.11.179	143.204.29.89	HTTP	519	GET /time/photoessays/2011/Libya_ruins/libya_ruins_01.jpg HTTP/1.1
4327	59.1797790400	172.16.4.295	166.62.111.64	HTTP	402	GET /wp-content/uploads/2018/02/fleshy-in-this-2571786.jpg HTTP/1.1
4980	68.0639468000	172.16.4.295	166.62.111.64	HTTP	392	GET /wp-content/uploads/2018/02/contact-me-2.jpg HTTP/1.1
5193	69.7566176000	172.16.4.295	166.62.111.64	HTTP	391	GET /wp-content/uploads/2018/02/Collaborate.jpg HTTP/1.1
5450	75.3986691000	172.16.4.295	166.62.111.64	HTTP	396	GET /wp-content/uploads/2018/02/Better-Your-Blog.jpg HTTP/1.1
6030	84.6985360000	172.16.4.295	166.62.111.64	HTTP	419	GET /wp-content/uploads/2019/03/Financial-Planner-stickers-feat-400x600.jpg HTTP/1.1
6478	91.9111530000	172.16.4.295	166.62.111.64	HTTP	401	GET /wp-content/uploads/2019/01/2019GoalsADHD-400x600.jpg HTTP/1.1
6707	95.1452932000	172.16.4.295	166.62.111.64	HTTP	409	GET /wp-content/uploads/2018/11/AdventCalendarFillers-400x600.jpg HTTP/1.1
6824	97.0166316000	172.16.4.295	166.62.111.64	HTTP	413	GET /wp-content/uploads/2018/11/12-Days-of-Christmas-Swap-400x600.jpg HTTP/1.1
7632	108.9986082000	172.16.4.295	166.62.111.64	HTTP	391	GET /wp-content/uploads/2018/02/Good-Eats-1.jpg HTTP/1.1
7686	109.7449368000	172.16.4.295	166.62.111.64	HTTP	386	GET /wp-content/uploads/2018/02/Crafty.jpg HTTP/1.1
9154	134.1177847000	172.16.4.295	166.62.111.64	HTTP	389	GET /wp-content/uploads/2018/02/HomeDecor.jpg HTTP/1.1
9385	137.8348030000	172.16.4.295	166.62.111.64	HTTP	386	GET /wp-content/uploads/2018/02/Family.jpg HTTP/1.1
00000-147-0000000000	172.16.4.295	166.62.111.64	HTTP	202	GET /wp-content/uploads/2018/02/Travel-1.jpg HTTP/1.1	

Transmission Control Protocol, Src Port: 80, Dst Port: 49757, Seq: 11559, Ack: 410, Len: 1460

Source Port: 80
Destination Port: 49757
[Stream index: 865]
[TCP Segment Len: 1460]
Sequence number: 11559 (relative sequence number)
Sequence number (raw): 48465047
[Next sequence number: 13019 (relative sequence number)]
Acknowledgment number: 410 (relative ack number)
Acknowledgment number (raw): 2013719029
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x2d94 [unverified]

```
0020 00 c9 90 50 c2 5d 02 e3 84 97 78 06 e9 f5 50 18 ...-P...-x-x-P:  

0030 fa f0 2d 94 00 00 00 32 63 0d 0a 3c 74 72 3e 3c .....-2 c-<tr><  

0040 74 64 3e 3c 61 20 68 72 65 66 3d 6e 73 68 6f 77 td>a hr ef=nshow  

0050 6d 6f 76 66 65 2e 68 74 6d 6c 3f 6d 6f 76 69 65 movie.htm?movie  

0060 69 64 3d 34 37 38 3e 0d 0a 31 34 0d 0a 50 6f 70 id=478> 14·Pop  

0070 65 79 65 20 66 6f 72 29 58 72 65 73 69 64 65 6e eye for Presiden  

0080 74 0d 0a 34 0d 0a 3c 2f 61 3e 0d 0a 31 38 0d 0a t·4·</a>·18·  

0090 20 3c 69 6d 67 20 73 72 63 3d 70 64 61 2e 6a 70 <img sr=c:pda.jp  

00a0 67 3e 3c 2f 69 6d 67 3e 0d 0a 32 32 0d 0a 20 3c g></img> ·22··<  

00b0 69 6d 67 20 73 72 63 3d 70 73 70 2e 67 69 66 3e img src= psp.gif>  

00c0 3c 2f 69 6d 67 3e 3c 2f 74 64 3e 3c 2f 74 72 3e </img></td></tr>  

00d0 0d 0a 32 63 0d 0a 3c 74 72 3e 3c 74 64 3e 3c 61 ..2c-<t><d><a  

00e0 20 68 72 65 66 3d 6e 73 68 6f 77 6d 6f 76 69 65 href=n howmovie  

00f0 2e 68 74 6d 6c 3f 6d 6f 76 69 65 69 64 3d 34 37 .html?mo vield=47  

0100 39 3e 0d 0a 31 64 0d 0a 50 6f 70 65 79 65 20 2d 9>·1d· Popeye -  

0110 20 46 72 69 68 74 20 74 6f 20 74 68 65 20 46 Fright to the F  

0120 69 6e 69 73 68 0d 0a 34 0d 0a 3c 2f 61 3e 0d 0a inish·4 ·<a>..
```

Transmission Control Protocol (tcp), 20 bytes

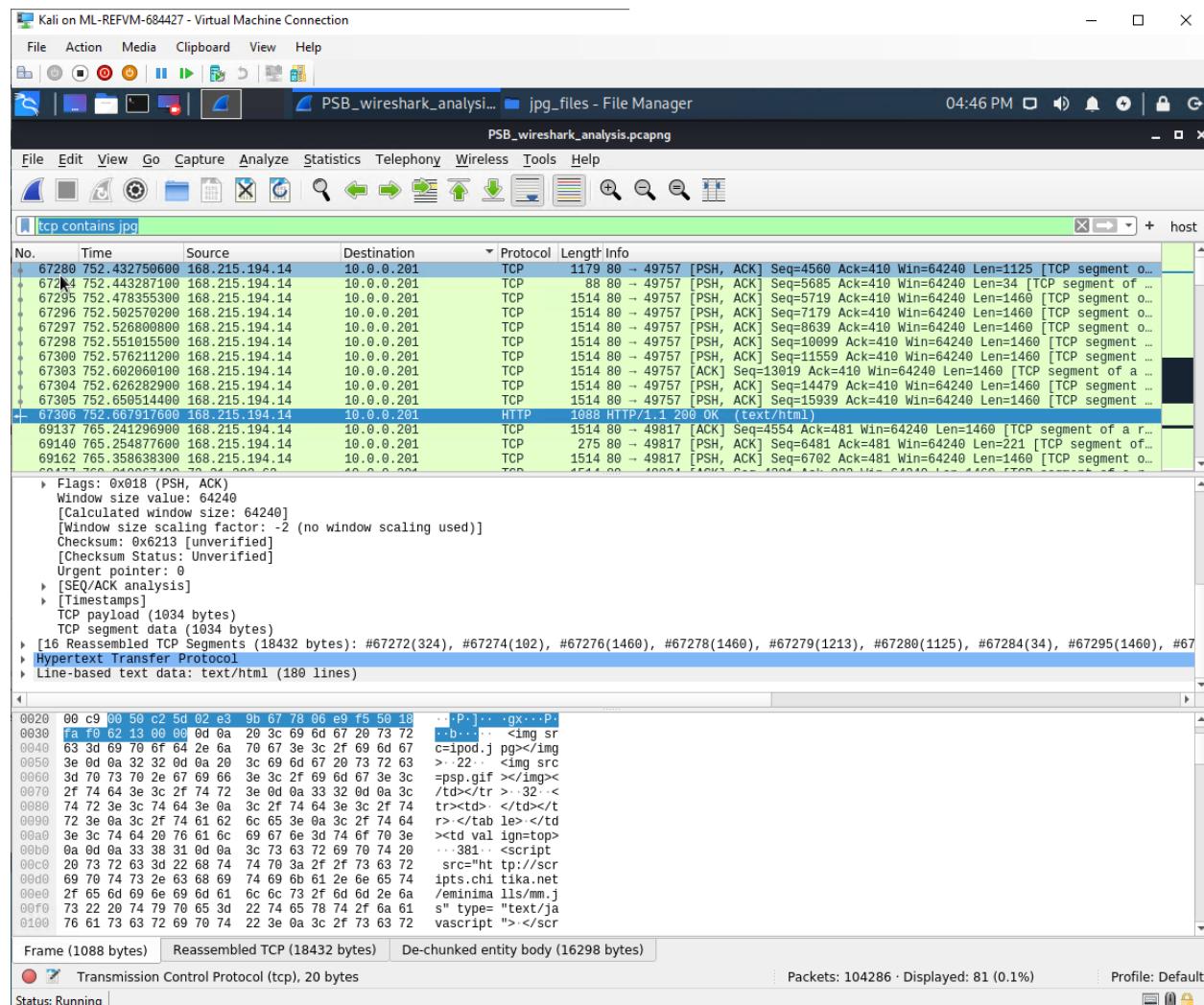
Packets: 104286 · Displayed: 81 (0.1%)

Status: Running

Profile: Default

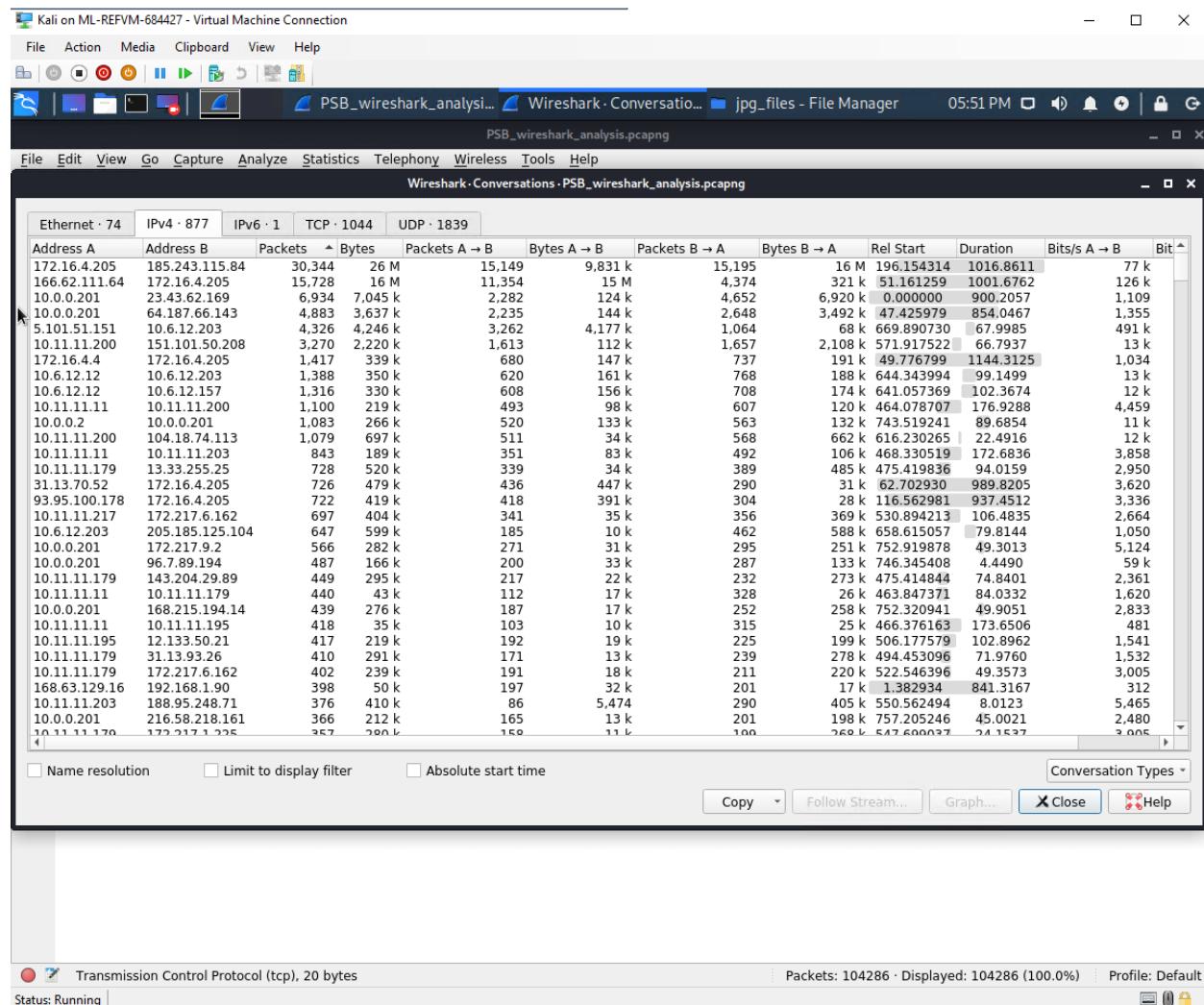
Wireshark_jpg3

Network Analysis Report by Paul Barrett



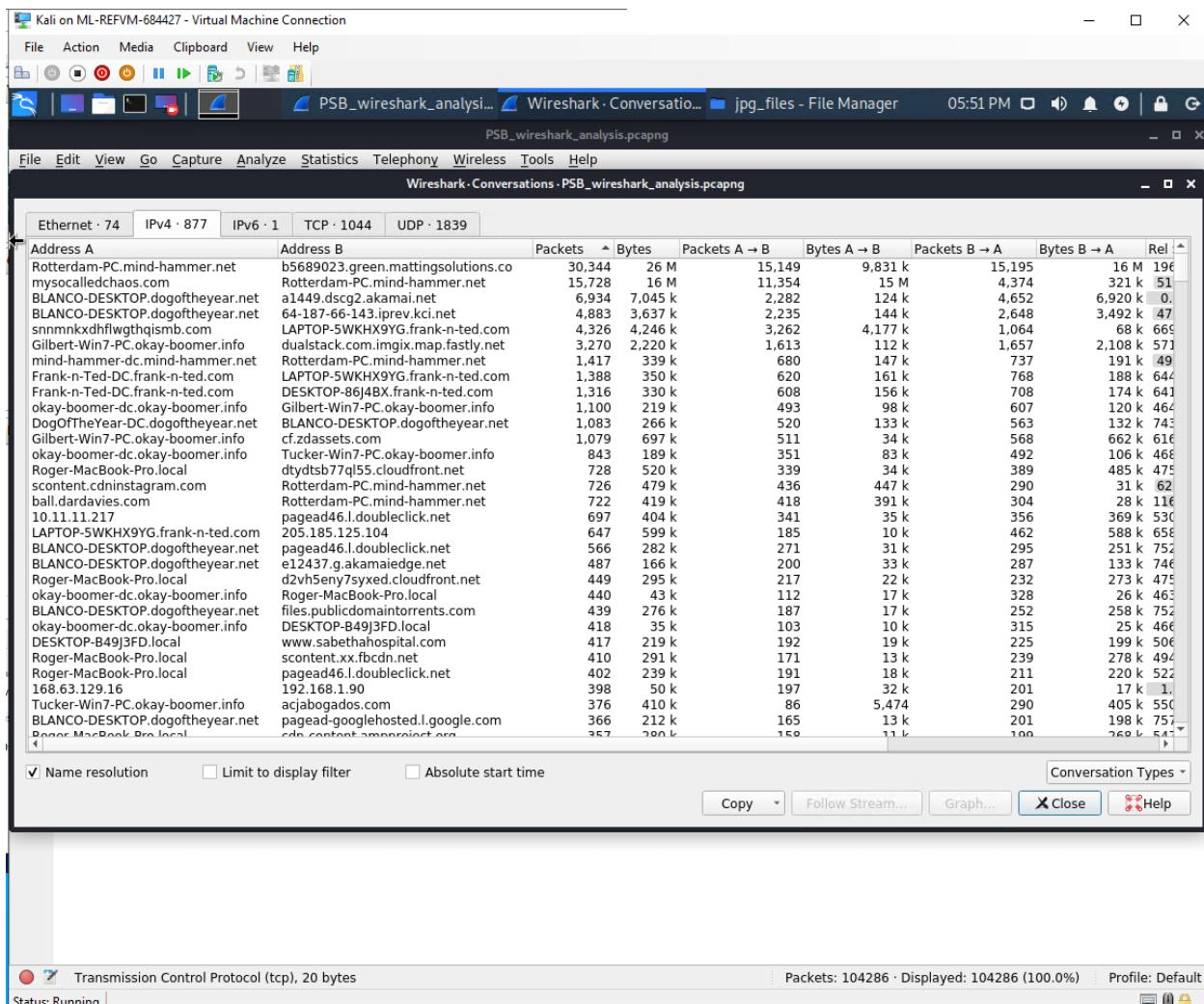
Wireshark_jpg4

Network Analysis Report by Paul Barrett



Wireshark_most_active_IP1

Network Analysis Report by Paul Barrett



Wireshark_most_active_IP2

Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

PSB_wireshark_analysis.pcapng jpg_files - File Manager

05:25 PM

PSB_wireshark_analysis.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp Stop capturing packets

No.	Time	Source	Destination	Protocol	Len	Info
34217	476.020609000	gsp64-ssl.ls-apple.com.akadns.n...	10.11.11.217	TCP	1384	443 - 62518 [PSH, ACK] Seq=1 Ack=518 Win=41932
33598	467.751003300	gsp85-ssl.ls2.apple.com.akadns...	10.11.11.217	TCP	1384	443 - 62516 [PSH, ACK] Seq=1331 Ack=518 Win=41932
33597	467.728848200	gsp85-ssl.ls2.apple.com.akadns...	10.11.11.217	TCP	1384	443 - 62516 [PSH, ACK] Seq=1 Ack=518 Win=41932
77578	831.503988900	arc.msn.com.nsatic.net	BLANCO-DESKTOP.dogoftheyear.net	TLSv1.2	1379 Server Hello, Certificate, Certificate Status,	
77569	831.406659700	arc.msn.com.nsatic.net	BLANCO-DESKTOP.dogoftheyear.net	TLSv1.2	1379 Server Hello, Certificate, Certificate Status,	
77562	831.309327000	arc.msn.com.nsatic.net	BLANCO-DESKTOP.dogoftheyear.net	TLSv1.2	1379 Server Hello, Certificate, Certificate Status,	
51711	620.612141800	pagead.l.doubleclick.net	Gilbert-Win7-PC.okay-boomer.info	TLSv1.2	1379 Application Data	
51316	618.468716000	www-google-analytics.l.google.c...	Gilbert-Win7-PC.okay-boomer.info	TLSv1.2	1379 Application Data	
51014	615.669739400	www-googletagmanager.l.google.c...	Gilbert-Win7-PC.okay-boomer.info	TLSv1.2	1379 Application Data	
54545	639.043677900	10.11.11.121	cloud-p2m2-ext.elb.samsungcloud...	TLSv1.2	1376 Application Data, Application Data	
69717	770.514487600	files.publicdomaintorrents.com	BLANCO-DESKTOP.dogoftheyear.net	TCP	1374 80 - 49834 [PSH, ACK] Seq=7301 Ack=536 Win=642	
85858	950.516949300	scontent.cdninstagram.com	Rotterdam-PC.mind-hammer.net	TCP	1371 [TCP Retransmission] 443 - 49223 [PSH, ACK] Seq=7301 Ack=536 Win=642	
60671	676.288169900	snmmnxkdhflwgthqismb.com	LAPTOP-SWKH9Y6.frank-n-ted.com	HTTP	1371 HTTP/1.1 200 OK (text/html)	

Frame 60971: 1371 bytes on wire (10968 bits), 1371 bytes captured (10968 bits) on interface eth0, id 0

Ethernet II, Src: Cisco_29:41:7d (ec:c8:82:29:41:7d), Dst: IntelCor_6d:fcc:e2 (84:3a:4b:6d:fcc:e2)

Internet Protocol Version 4, Src: snmmnxkdhflwgthqismb.com (5.101.51.151), Dst: LAPTOP-SWKH9Y6.frank-n-ted.com (10.6.12.203)

- Transmission Control Protocol, Src Port: 80, Dst Port: 49744, Seq: 370489, Ack: 696, Len: 1317

Source Port: 80
 Destination Port: 49744
 [Stream index: 732]
 [TCP Segment Len: 1317]
 Sequence number: 370489 (relative sequence number)
 Sequence number (raw): 1077633906
 [Next sequence number: 371807 (relative sequence number)]
 Acknowledgment number: 696 (relative ack number)
 Acknowledgment number (raw): 1364565903
 0101.... = Header Length: 20 bytes (5)
 Flags: 0x010 (FIN, PSH, ACK)

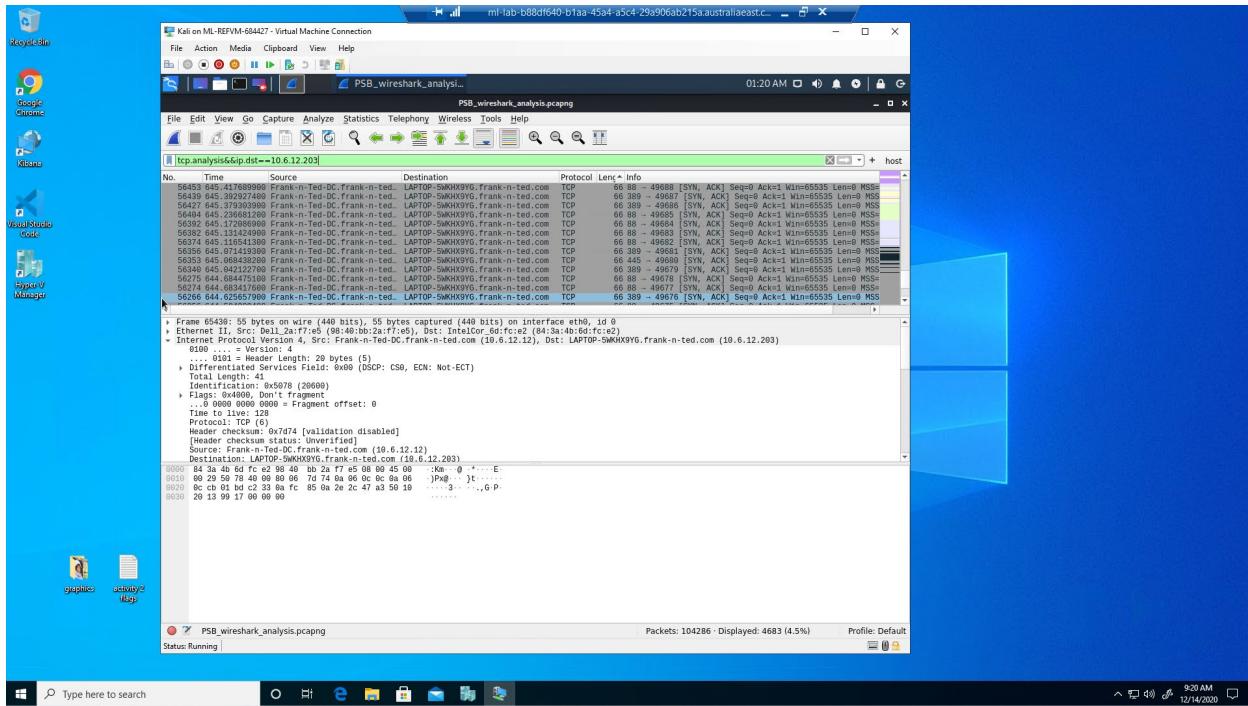
Frame (1371 bytes) Reassembled TCP (371805 bytes) De-chunked entity body (371221 bytes)

Transmission Control Protocol: Protocol Packets: 104286 · Displayed: 92280 (88.5%) Profile: Default

Status: Running

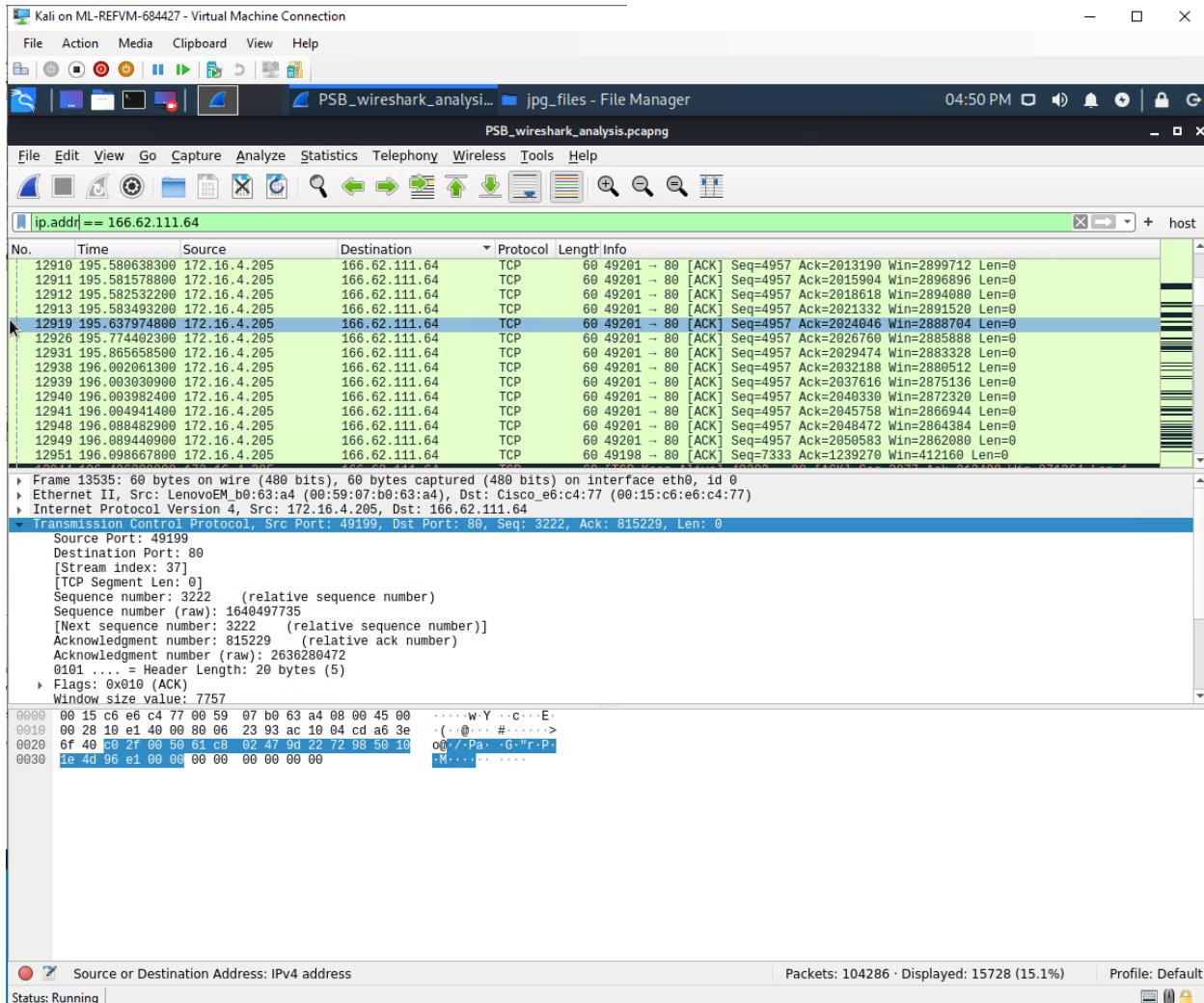
Wireshark_tcp

Network Analysis Report by Paul Barrett



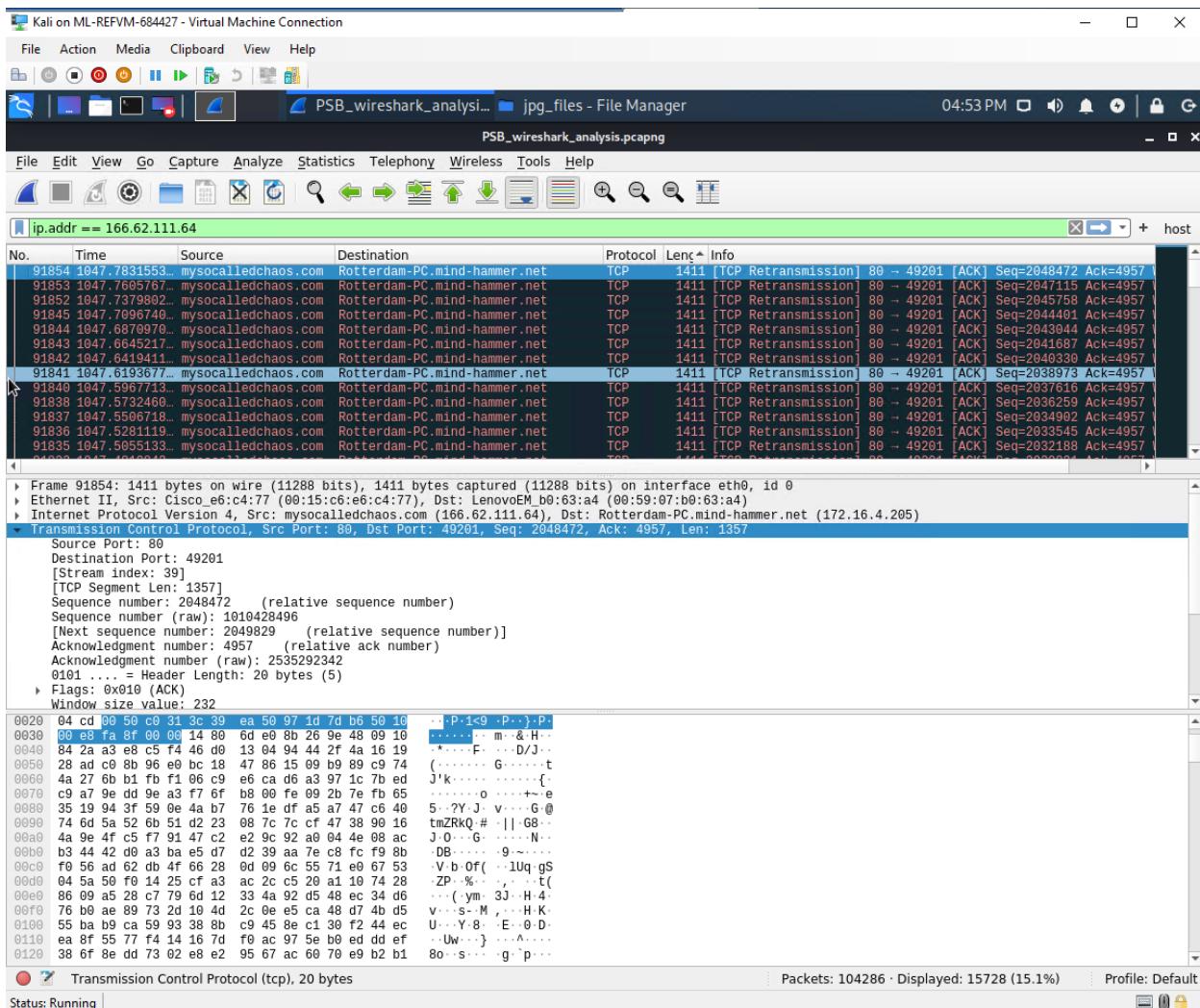
Wireshark_tcp_10.6.12.203

Network Analysis Report by Paul Barrett



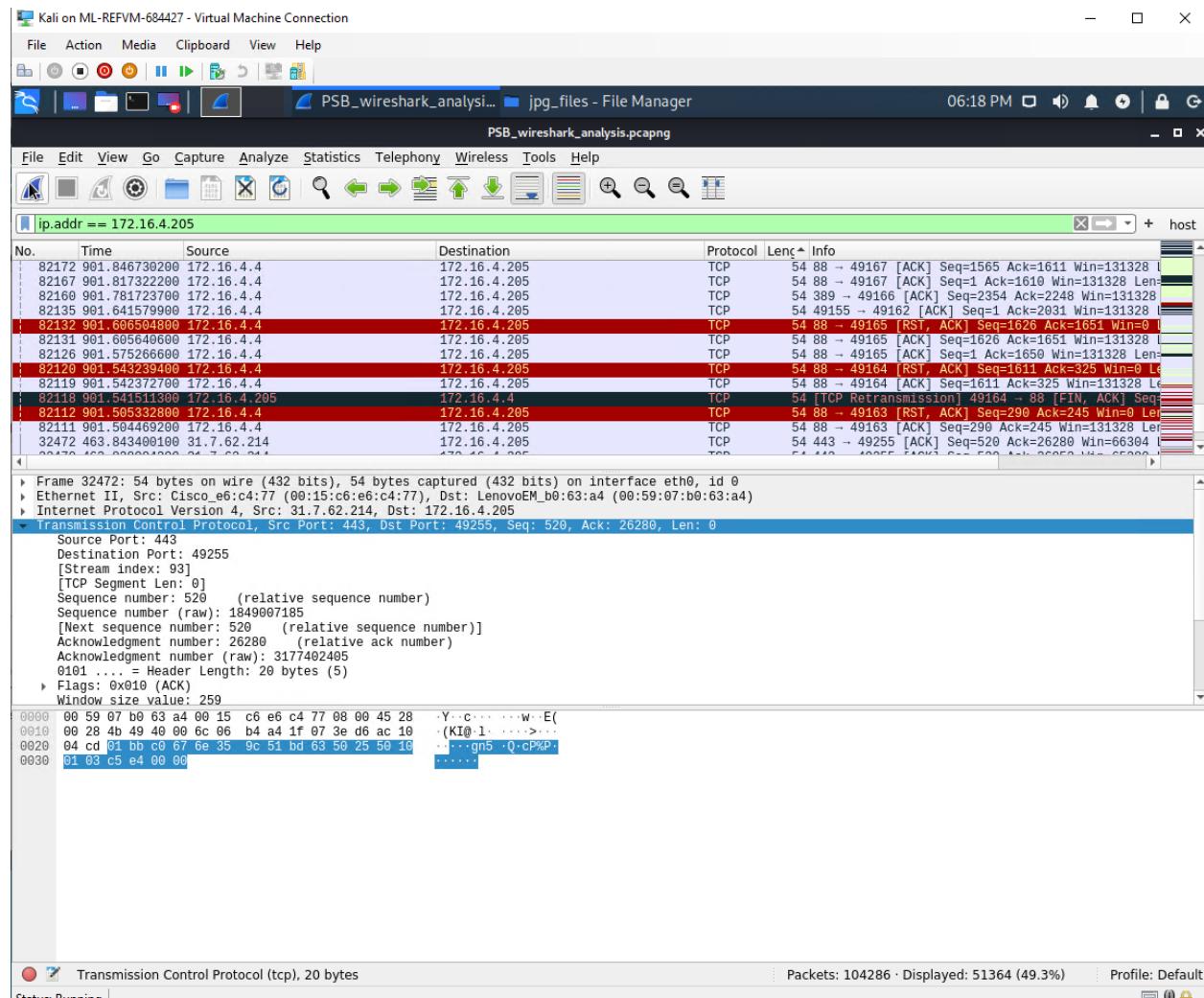
Wireshark_tcp_166.62.111.64a

Network Analysis Report by Paul Barrett



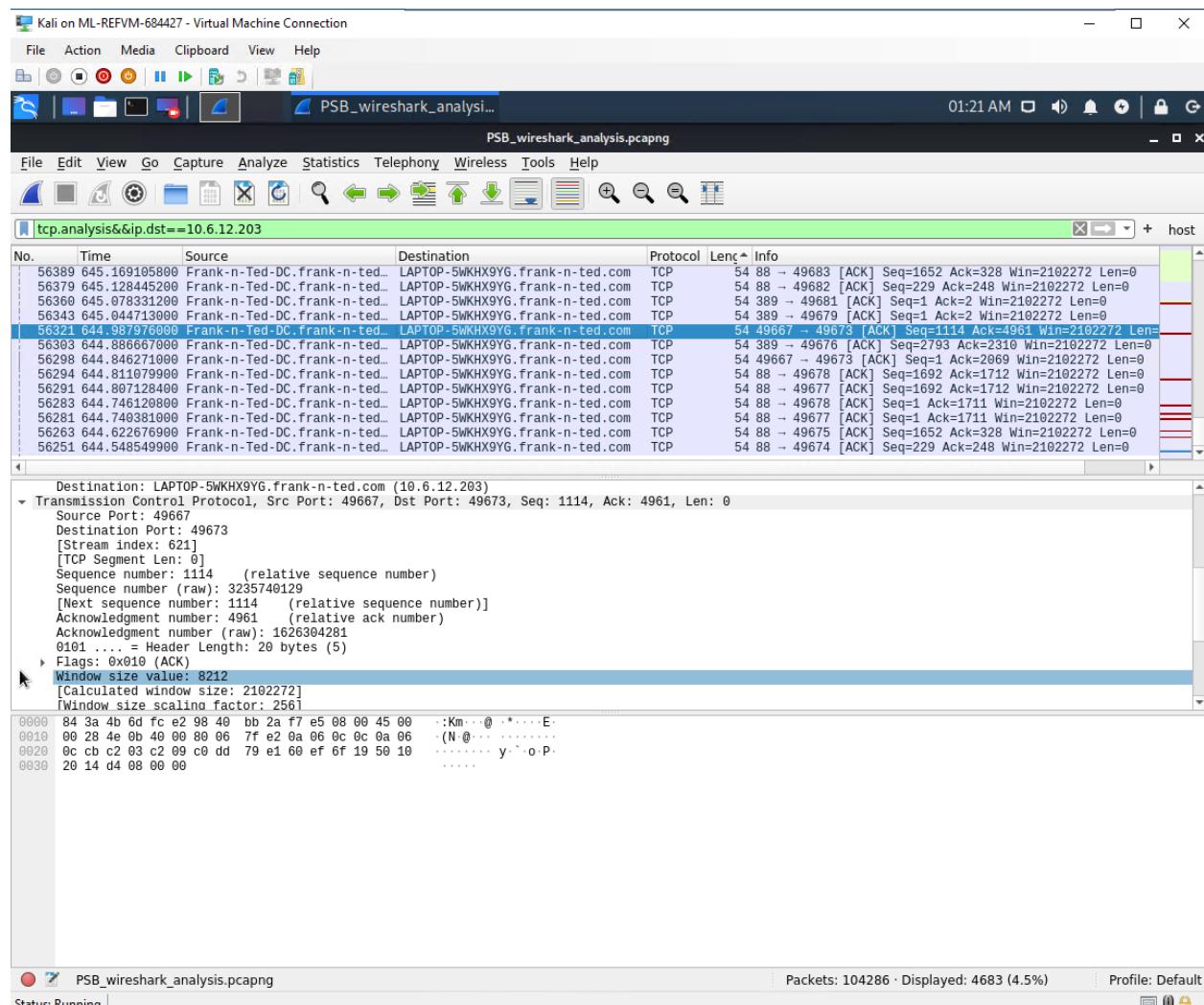
Wireshark_tcp_166.62.111.64b

Network Analysis Report by Paul Barrett



Wireshark_tcp_172.16.4.205

Network Analysis Report by Paul Barrett



Wireshark_tcp_analysis

Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

[Shell No. 1] PSB_wireshark_analysis.pcapng 03:46 PM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp contains facebook

No.	Time	Source	Destination	Protocol	Length	Info
1	45710 566.644182900	31.13.93.26	10.11.11.195	TLSv1.2	1411	Server Hello
2	39864 515.515630500	31.13.93.26	10.11.11.195	TLSv1.2	1411	Server Hello
3	39860 515.462959000	31.13.93.26	10.11.11.195	TLSv1.2	1411	Server Hello
4	83326 912.100228900	166.62.111.64	172.16.4.205	TCP	1411	[TCP Retransmission] 80 ~ 49190 [ACK] Seq=87182 Ack=3492 Win=25344 Len=1357
5	4416 60 391684900	166.62.111.64	172.16.4.205	TCP	1411	80 ~ 49190 [ACK] Seq=87182 Ack=3492 Win=25344 Len=1357 [TCP segment of a reasse...
6	34519 471.227959000	143.204.29.34	10.11.11.179	TCP	1411	80 ~ 50221 [ACK] Seq=15971 Ack=400 Win=30208 Len=1345 TSval=3244903534 TSecr=95...
7	34507 471.043146100	143.204.29.34	10.11.11.179	TCP	1411	80 ~ 50221 [ACK] Seq=5211 Ack=400 Win=30208 Len=1345 TSval=3244903534 TSecr=95...
8	34486 470.929442400	143.204.29.34	10.11.11.179	TCP	1300	80 ~ 50221 [PSH, ACK] Seq=592 Ack=400 Win=30208 Len=1234 TSval=3244903526 TSecr=...
9	41628 530.916999700	10.11.11.217	31.13.93.26	TLSv1.3	583	Client Hello
10	45708 566.620735600	10.11.11.195	31.13.93.26	TLSv1.2	263	Client Hello
11	39820 515.115137300	10.11.11.195	31.13.93.26	TLSv1.2	263	Client Hello
12	39818 515.088352400	10.11.11.195	31.13.93.26	TLSv1.2	263	Client Hello
13	38777 506.417949700	10.11.11.195	12.133.50.21	HTTP	439	GET /common.js/start_facebook.js HTTP/1.1
14	37615 497.445421200	10.11.11.179	31.13.93.26	TLSv1.3	583	Client Hello
15	37314 494.496035300	10.11.11.179	31.13.93.26	TLSv1.3	583	Client Hello

Frame 83326: 1411 bytes on wire (11288 bits), 1411 bytes captured (11288 bits) on interface eth0, id 0

Ethernet II, Src: Cisco_e6:c4:77 (00:15:6:e:c4:77), Dst: LenovoEM_b6:63:a4 (00:59:07:b0:63:a4)

Internet Protocol Version 4, Src: 166.62.111.64, Dst: 172.16.4.205

Transmission Control Protocol, Src Port: 80, Dst Port: 49190, Seq: 87182, Ack: 3492, Len: 1357

```

0000  00 59 07 b0 63 a4 00 15 c6 e6 c4 77 08 00 45 00  Y..c...w-E.
0010  05 75 5b 21 40 00 36 06 1e 06 a6 3e 6f 48 ac 10  u[!@ 6...>o@..
0020  04 cd 00 50 c0 26 2b cf 62 47 7e 25 c1 e1 50 10  ..P+& bG-%..P
0030  00 c6 e2 a3 00 00 38 20 30 2d 31 2e 32 37 35 2d  ....8 0-1.275-
0040  20 32 34 35 2d 31 2e 37 36 34 2d 2e 37 33 34 73  .245-1.7 64-.7345
0050  2d 2e 37 33 34 2d 31 2e 38 37 37 2d 2e 37 33 34  -.734-1. 077-.
0060  2d 31 2e 37 36 34 56 37 2e 34 37 63 36 2d 2e 36  -.1.764V7 .47c0-.6
0070  38 38 2e 32 34 35 2d 31 2e 32 37 35 2d 37 33 34  88.245-1 .275.734
0080  2d 31 2e 37 36 34 73 31 2e 30 37 37 2d 2e 37 33  -.1.764s1 .077-.73
0090  34 20 31 2e 37 33 34 2d 2e 37 33 34 68 32 32 2e  4 1.764- .734h22.
00a0  39 38 34 63 2e 38 38 29 39 31 28 32 32 37 35  984c.688 0 1.275
00b0  2d 32 34 35 20 31 2e 37 36 34 2e 37 33 34 53 33  .245 1.7 64.734S3
00c0  30 20 36 2e 37 38 33 29 33 39 20 37 2e 34 37 7a  0 6.783 38 7.47z
00d0  22 3e 3c 2f 76 61 74 68 3e 0a 3c 2f 73 79 6d 62  "></path ></symbol"
00e0  6f 6c 3e 0a 3c 73 79 6d 62 6f 6c 20 69 64 3d 22  o1><symbol id="social-facebook" viewBox="0 0 32 32"/>
00f0  73 6f 63 69 61 6c 2d 66 61 63 65 62 6f 6f 6b 22
0100  20 76 69 65 77 42 6f 78 3d 22 30 20 30 28 33 32

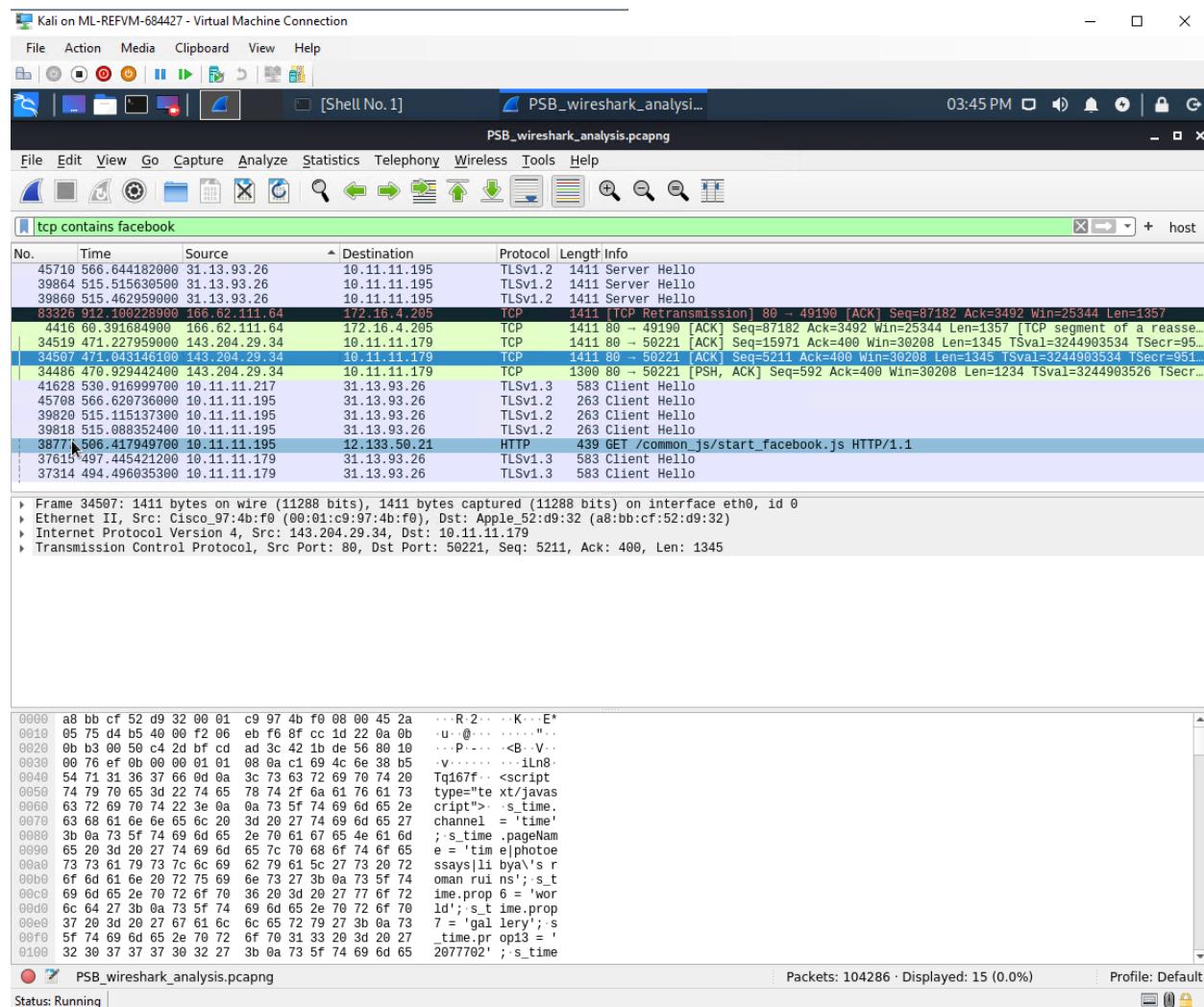
```

Packets: 104286 · Displayed: 15 (0.0%) · Profile: Default

Status: Running

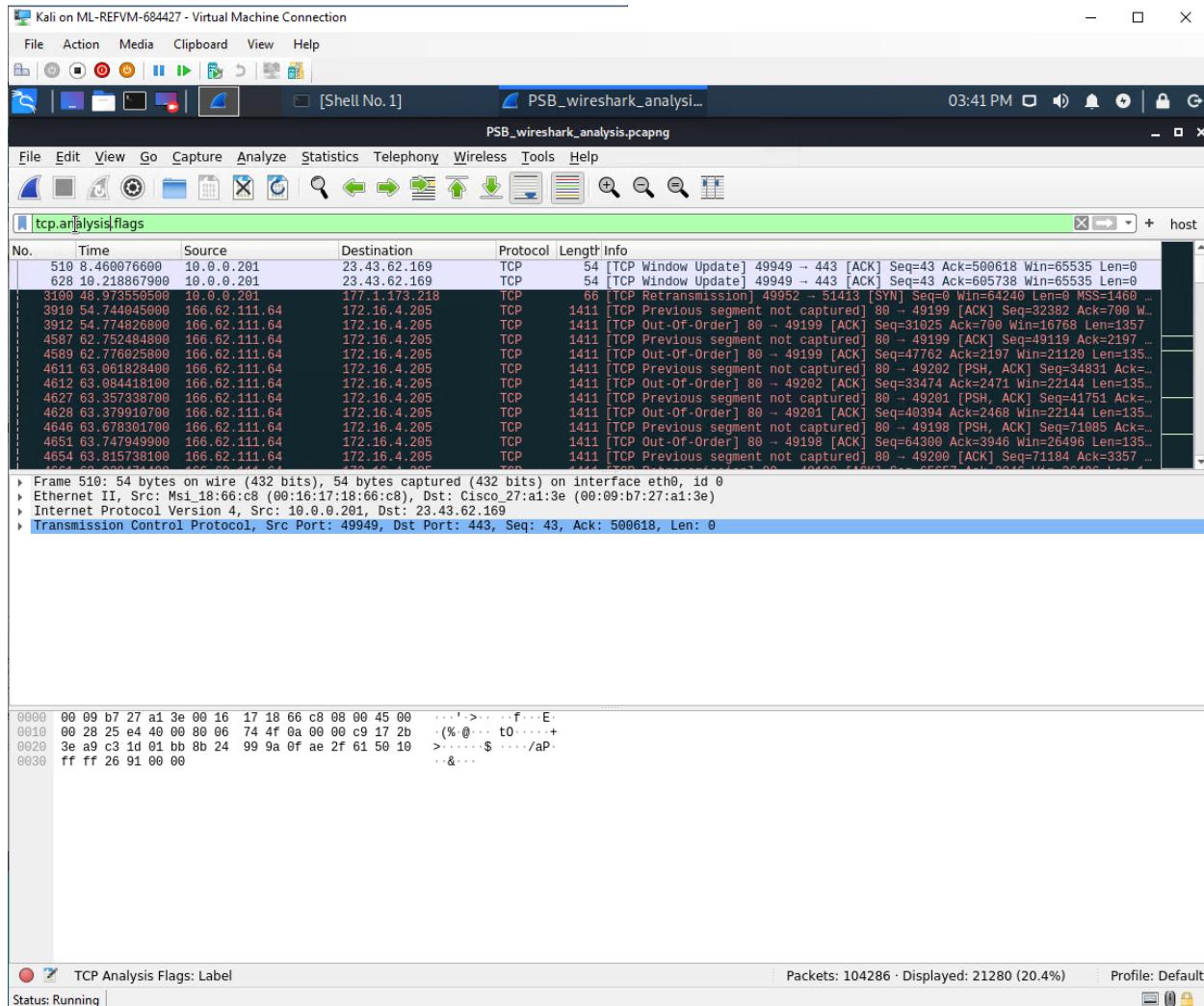
Wireshark_tcp_facebook1

Network Analysis Report by Paul Barrett



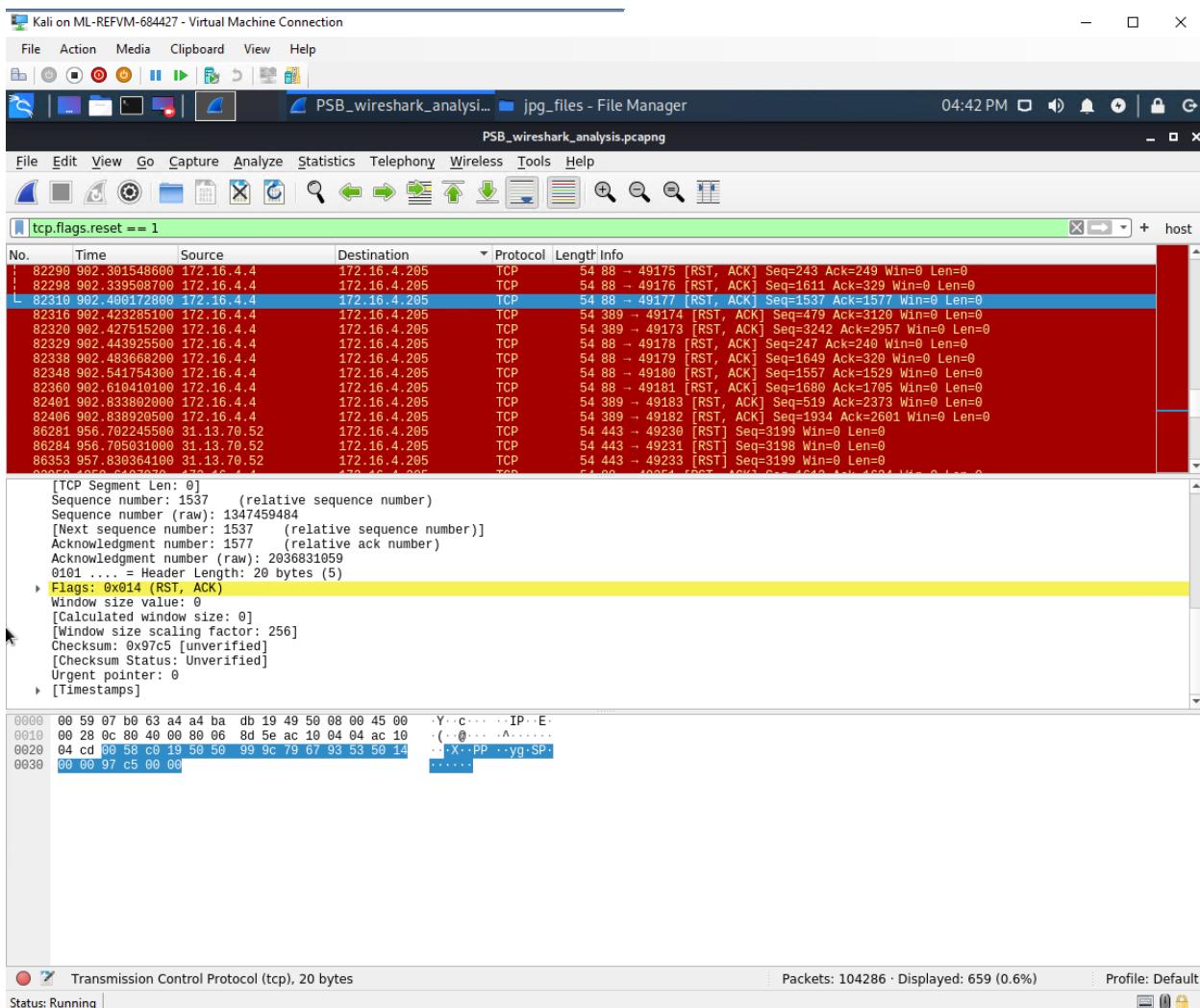
Wireshark_tcp_facebook2

Network Analysis Report by Paul Barrett



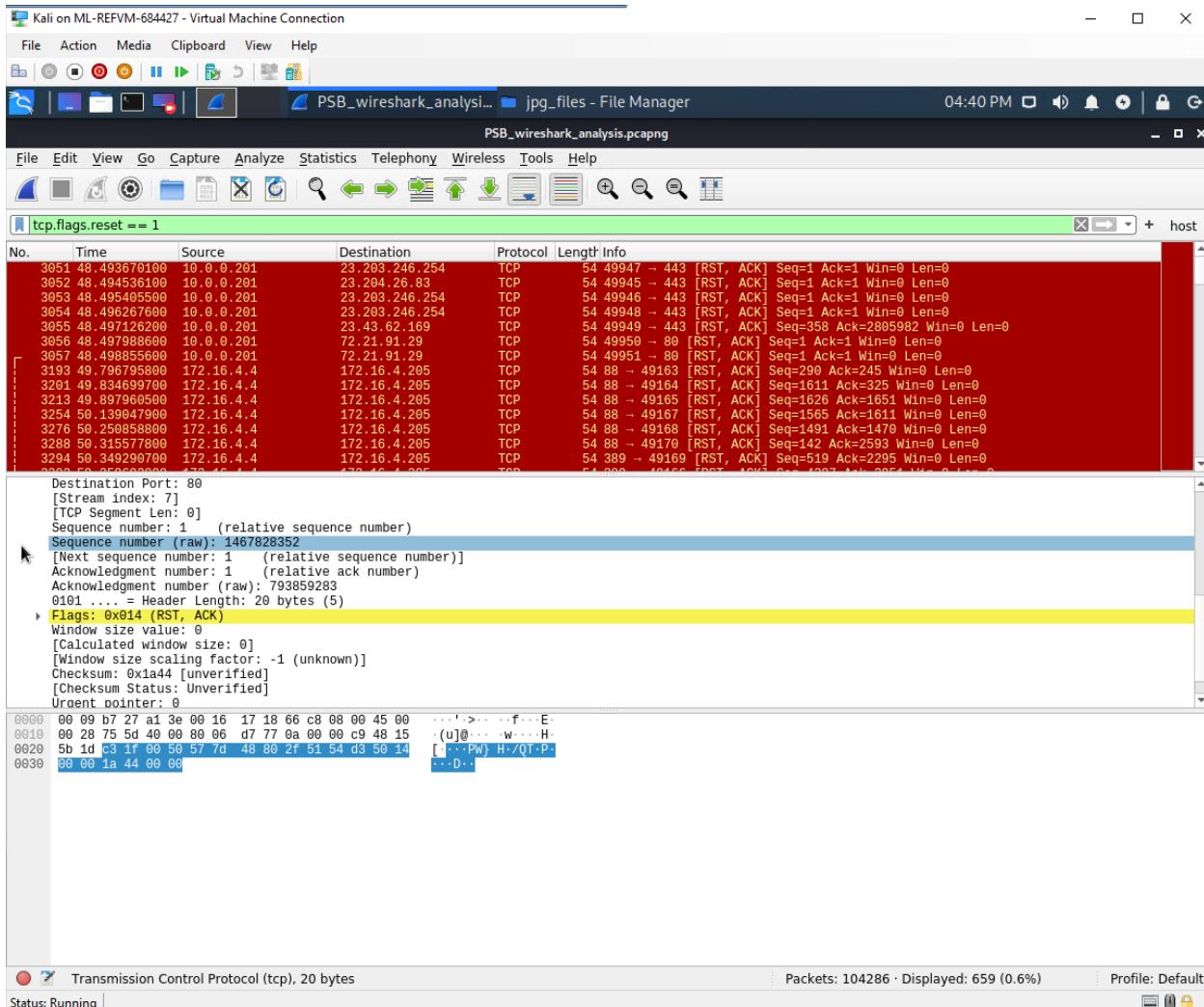
Wireshark_tcp_flags

Network Analysis Report by Paul Barrett



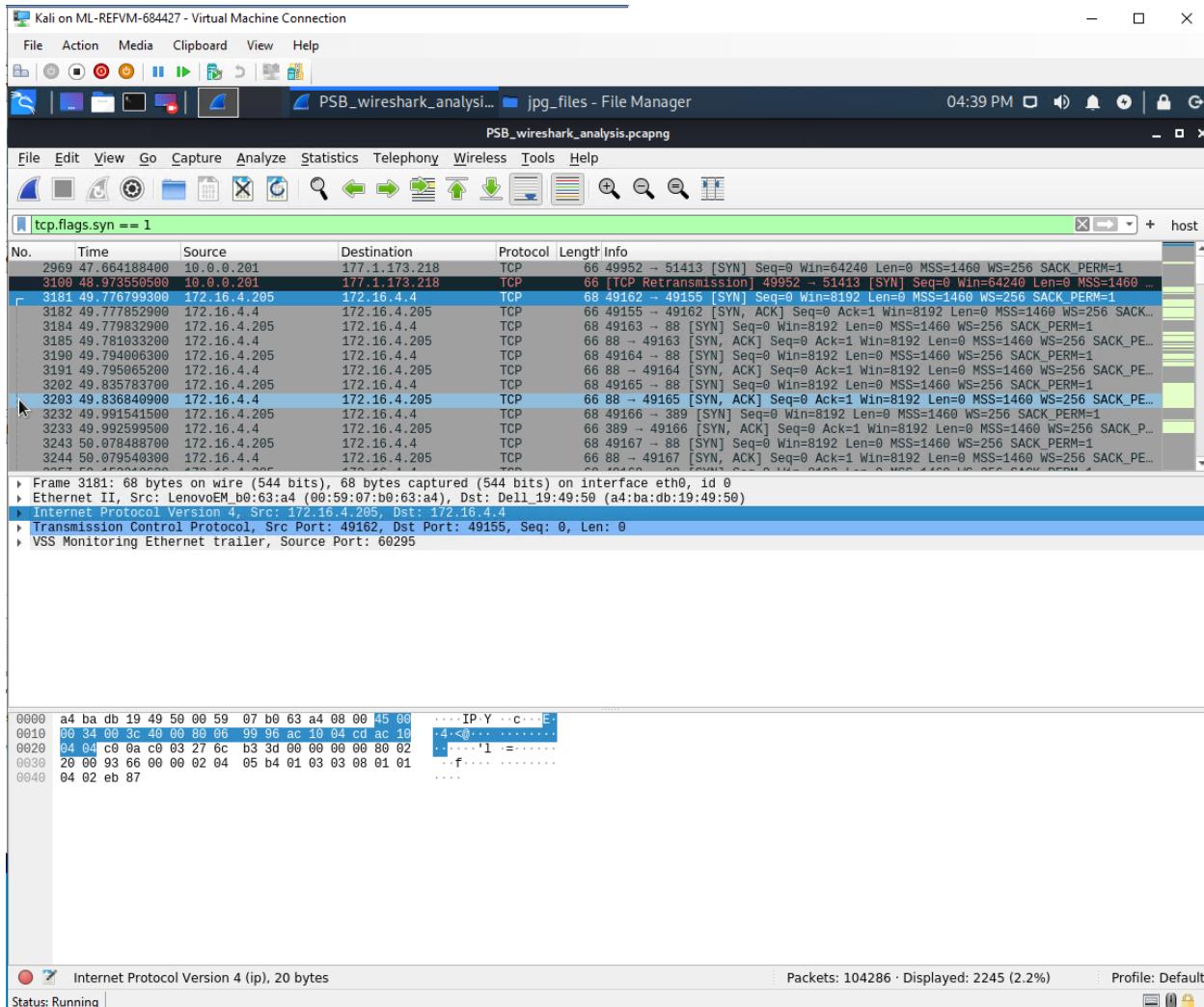
Wireshark_tcp_flags_reset1

Network Analysis Report by Paul Barrett



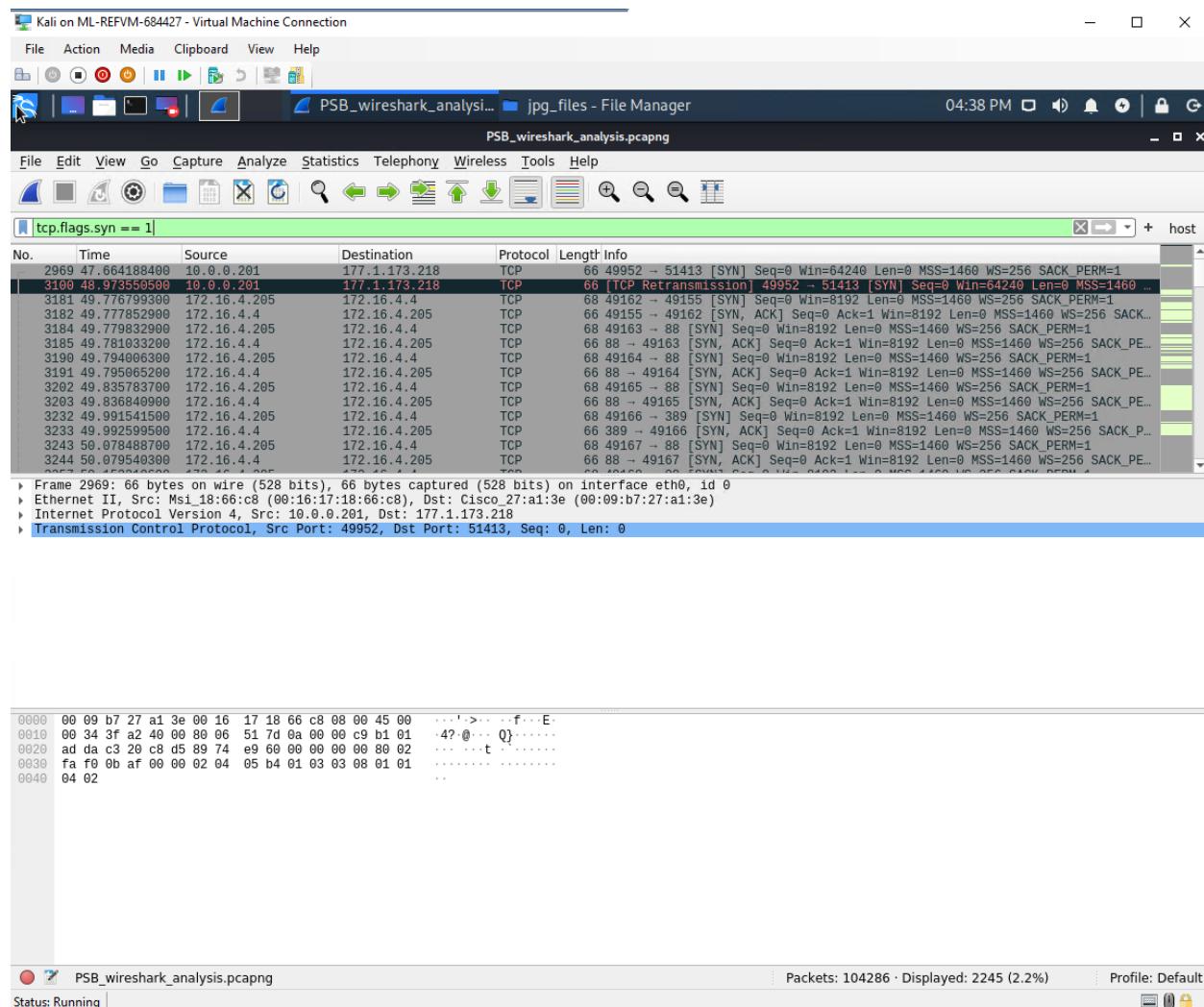
Wireshark_tcp_flags_reset2

Network Analysis Report by Paul Barrett



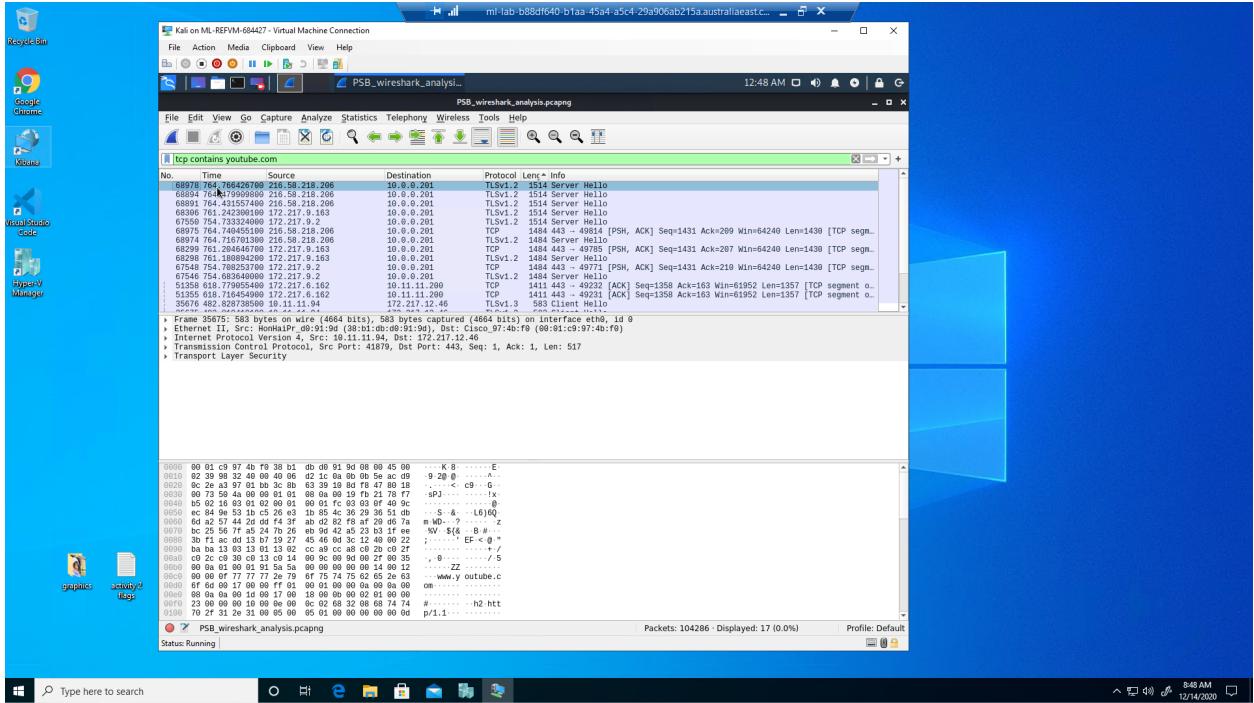
Wireshark_tcp_flags_syn1

Network Analysis Report by Paul Barrett

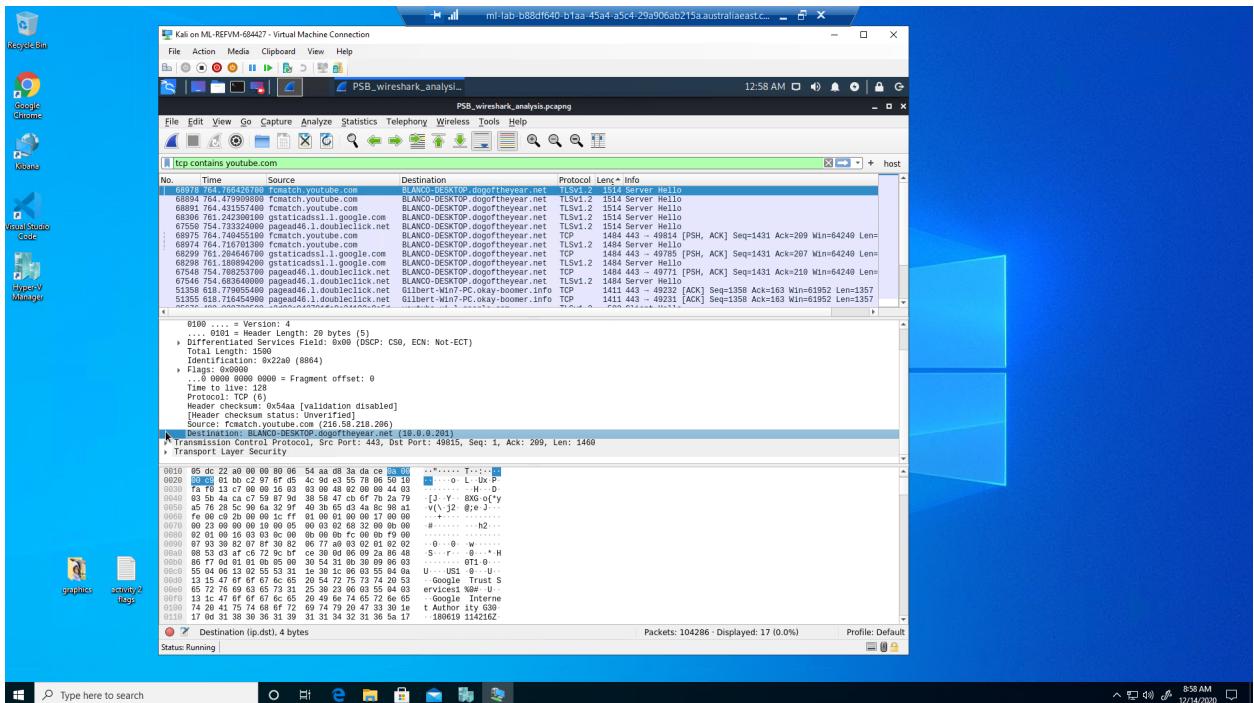


Wireshark_tcp_flags_syn2

Network Analysis Report by Paul Barrett

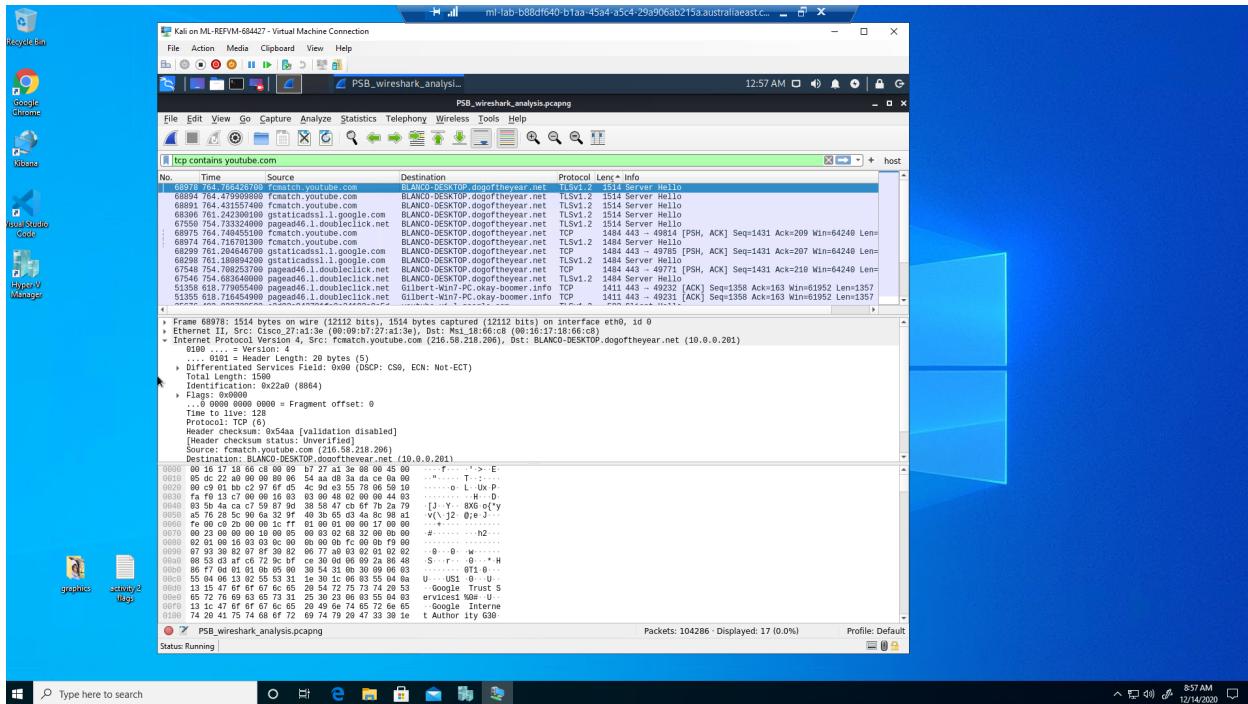


Wireshark_tcp_youtube1



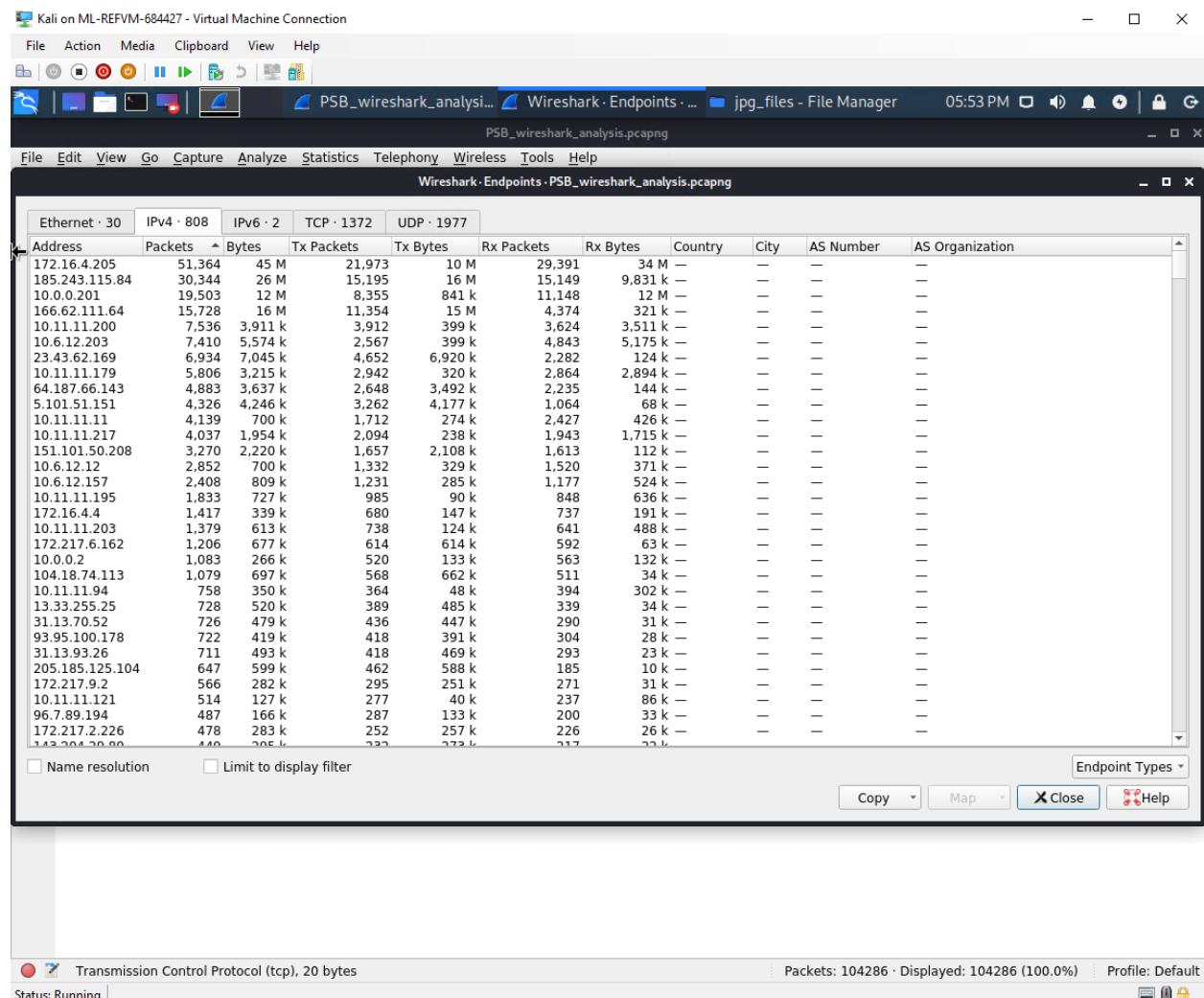
Wireshark tcp youtube2

Network Analysis Report by Paul Barrett



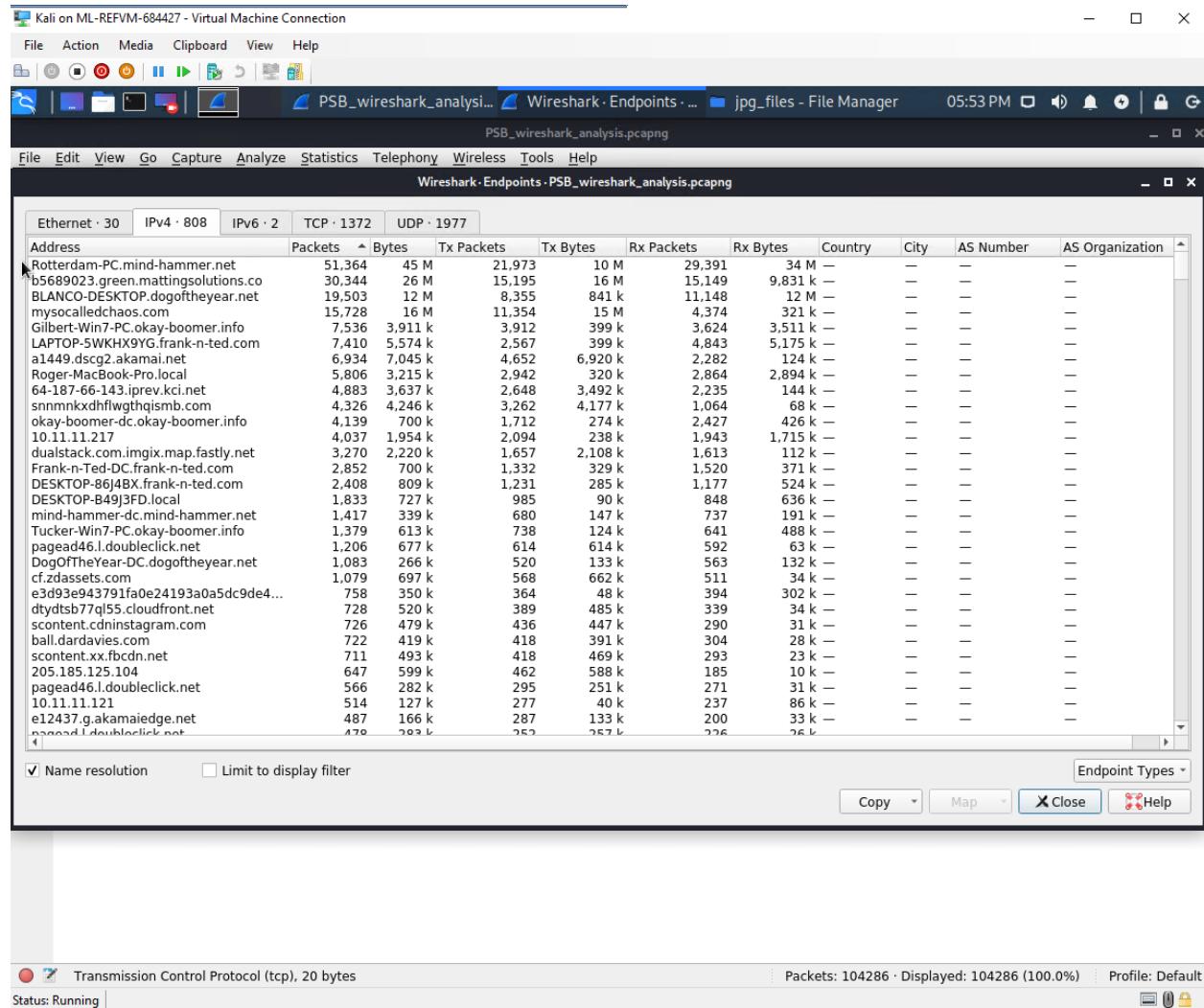
Wireshark_tcp_youtube2a

Network Analysis Report by Paul Barrett



Wireshark_top_talkers1

Network Analysis Report by Paul Barrett



Wireshark_top_talkers2

Network Analysis Report by Paul Barrett

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

PSB_wireshark_analysis.pcapng Wireshark · Conversatio... jpg_files - File Manager 06:45 PM host

tcp contains jpg

No.	Time	Source	Destination	Protocol	Length	Info
43085	544.2372483000	19.11.11.217	94.31.29.96	HTTP	503	GET /wp-content/uploads/2019/02/AirPods-Ear-Cov...
42942	543.0824202000	19.11.11.217	94.31.29.96	HTTP	503	GET /wp-content/uploads/2019/10/checkrain-tease...
43065	544.1204194000	19.11.11.217	94.31.29.96	HTTP	501	GET /wp-content/uploads/2019/07/macbook-pro-20...
69167	765.4164187000	19.0.0.201	168.215.194.14	HTTP	500	GET /grabs/bettybooprythmonthereservationgrab.j...
43047	543.9511203000	19.11.11.217	94.31.29.96	HTTP	500	GET /wp-content/uploads/2019/10/inprogressi-ip...
43087	544.2517285000	19.11.11.217	94.31.29.96	HTTP	495	GET /wp-content/uploads/2018/02/appleglassdispl...
43070	544.1322925000	19.11.11.217	94.31.29.96	HTTP	495	GET /wp-content/uploads/2019/11/BentoStack-67x...
41570	530.5705964000	19.11.11.217	35.185.55.255	HTTP	495	GET /wp-content/themes/iphonehacks/img/logo.jp...
39017	508.5902912000	19.11.11.195	12.133.50.21	HTTP	483	GET /pictures/content/180215.jpg HTTP/1.1
67333	752.8988433000	19.0.0.201	168.215.194.14	HTTP	479	GET /site2/pdheader.jpg HTTP/1.1
38937	508.0443900000	19.11.11.195	12.133.50.21	HTTP	475	GET /splash/button-1.jpg HTTP/1.1
38775	506.4031725000	19.11.11.195	12.133.50.21	HTTP	475	GET /splash/button-2.jpg HTTP/1.1
+ 67337	752.9156430000	19.0.0.201	168.215.194.14	HTTP	474	GET /googlevid.jpg HTTP/1.1

Request Method: GET
 Request URI: /googlevid.jpg
 Request Version: HTTP/1.1
 Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation\r\n
 Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5\r\n
 Accept-Language: en-US\r\n
 Accept-Encoding: gzip, deflate\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
 Host: publicdomaintorrents.info\r\n
 Connection: Keep-Alive\r\n
 \r\n
 [Full request URI: http://publicdomaintorrents.info/googlevid.jpg]
 [HTTP request 2/2]
 [Prev request in frame: 67282]
 [Response in frame: 67384]

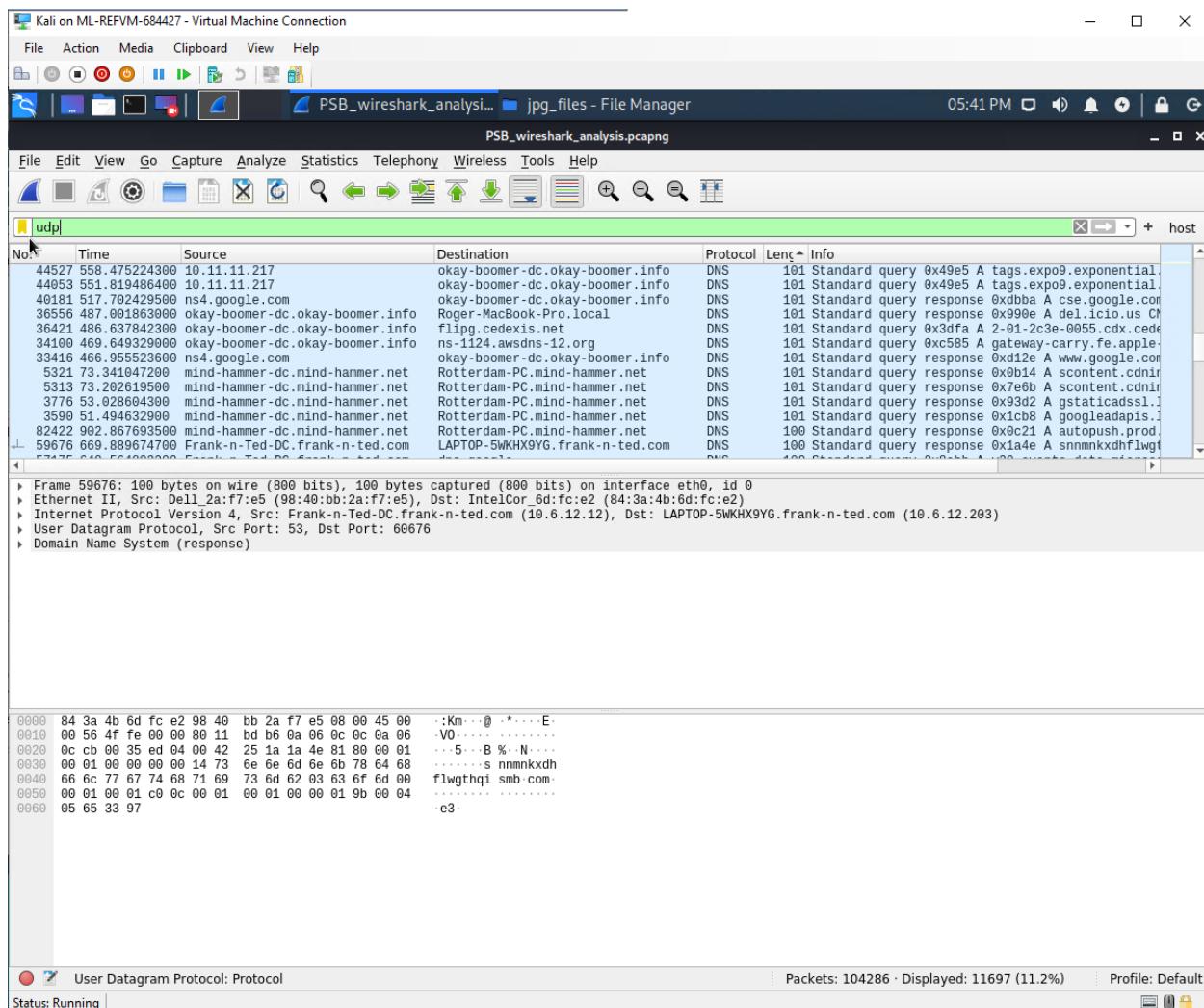
```
0020 c2 0e c2 5c 06 50 5e 11 22 d8 41 34 94 e5 50 18 ..\r\nff ff c0 35 06 00 47 45 54 29 2f 67 6f 6f 67 6c ..-GE T /googl\n0048 65 76 69 64 2e 6a 70 67 26 48 54 50 2f 31 2e evid.jpg HTTP/1.\n0050 31 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 1: Refer er: http\n0052 ://publi cdomaint\n0058 3a 2f 70 75 62 66 69 63 64 6f 6d 61 69 6e 74 orrents. info/nsh\n0070 6f 72 72 65 6e 74 73 2e 69 6e 66 6f 2f 6e 73 68 owcat.ht m1?categ\n0080 6f 77 63 61 74 2e 68 74 60 6c 3f 63 61 74 65 67 ory=anim ation: A\n0088 6f 72 79 3d 61 6e 69 6d 61 74 69 6f 6e 0d 0a 41 cept: i mage/png\n0090 63 63 65 70 74 3a 29 69 60 61 67 65 2f 70 6e 67 ,image/s vg+xml,i\n0098 2c 69 6d 61 67 65 2f 73 76 67 2b 78 6d 6c 2c 69 mage/*;q=0.8,*/\n00b0 6d 61 67 65 2f 2a 3b 71 3d 30 2e 38 2c 2a 2f 2a ;q=0.5 - Accept-L\n00d0 3b 71 3d 30 2e 35 0d 0a 41 63 65 70 74 2d 4c anguage: en-US-\n00e0 61 6e 67 75 61 67 65 3a 26 65 68 2d 55 53 6d 0c Accept-E ncoding:\n00f0 41 63 63 65 76 74 2d 45 6e 63 6f 64 69 66 67 3a gzip, d eflate..\n0100 20 67 7a 69 78 2c 20 64 65 66 6c 61 74 65 0d 0a User-Age nt: Mozi\n0110 55 73 65 72 2d 41 67 65 66 74 3a 20 4d 6f 7a 69 lla/5.0 (Windows\n0120 6c 6e 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73
```

Packets: 104286 · Displayed: 81 (0.1%) · Profile: Default

Status: Running

Wireshark_torrent

Network Analysis Report by Paul Barrett



Wireshark_udp

Network Analysis Report by Paul Barrett

The screenshot shows a Kali Linux desktop environment with several windows open:

- VirusTotal - Mozilla Firefox:** The main window displays the VirusTotal analysis for file d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec. It shows a community score of 55/70 and detections from Ad-Aware and AhnLab-V3. The results indicate the file is a Trojan.GenericKD.34007934 and Malware/Win32.RL_Generic.R346613.
- Wireshark - Packets:** A smaller window showing network traffic analysis.
- File Manager:** A file browser window showing files in the root directory, including betty, empty.gif%3fss&ss2img, june11.dll, psb_hash.txt, psb_hashes.txt, and PSB_wireshark_analysis.pcapng.
- Terminal:** A terminal window showing a command-line interface.

Wireshark_virustotal1

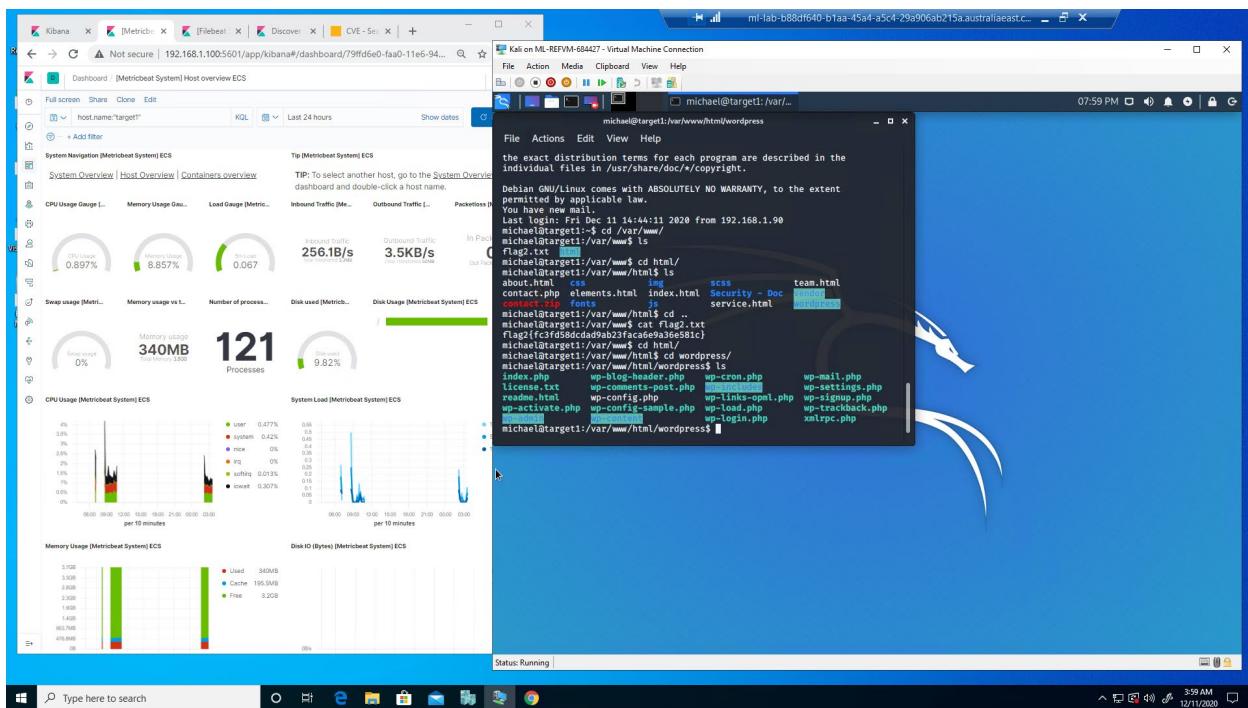
Network Analysis Report by Paul Barrett

The screenshot shows a Kali Linux desktop environment with several open windows. The main window is a Mozilla Firefox browser displaying the VirusTotal analysis page for the file hash d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec. The VirusTotal interface indicates that 55 engines have detected this file. The 'DETECTION' tab is selected, showing results from various antivirus engines:

Detection Engine	Result	Reporter	Description
Ad-Aware	① Trojan.GenericKD.34007934	AegisLab	① Trojan.Multi.Generic.4lc
AhnLab-V3	① Malware/Win32.RL_Generic.R346613	Alibaba	① TrojanSpy:Win32/Yakes.56555f48
ALYac	① Trojan.GenericKD.34007934	Antiy-AVL	① GrayWare/Win32.Kryptik.ehls
SecureAge APEX	① Malicious	Arcabit	① Trojan.Generic.D206EB7E
Avast	① Win32:DangerousSig [Trj]	AVG	① Win32:DangerousSig [Trj]
Avira (no cloud)	① TR/AD.ZLoader.ladbd	BitDefender	① Trojan.GenericKD.34007934
BitDefenderTheta	① Gen:NN.ZedlaF.34590.lu9@au7OQgi	Bkav	① W32.AIDetectVM.malware2
Cylance	① Unsafe	Cynet	① Malicious (score: 100)

Wireshark_virustotal2

Network Analysis Report by Paul Barrett



wordpress_directory1

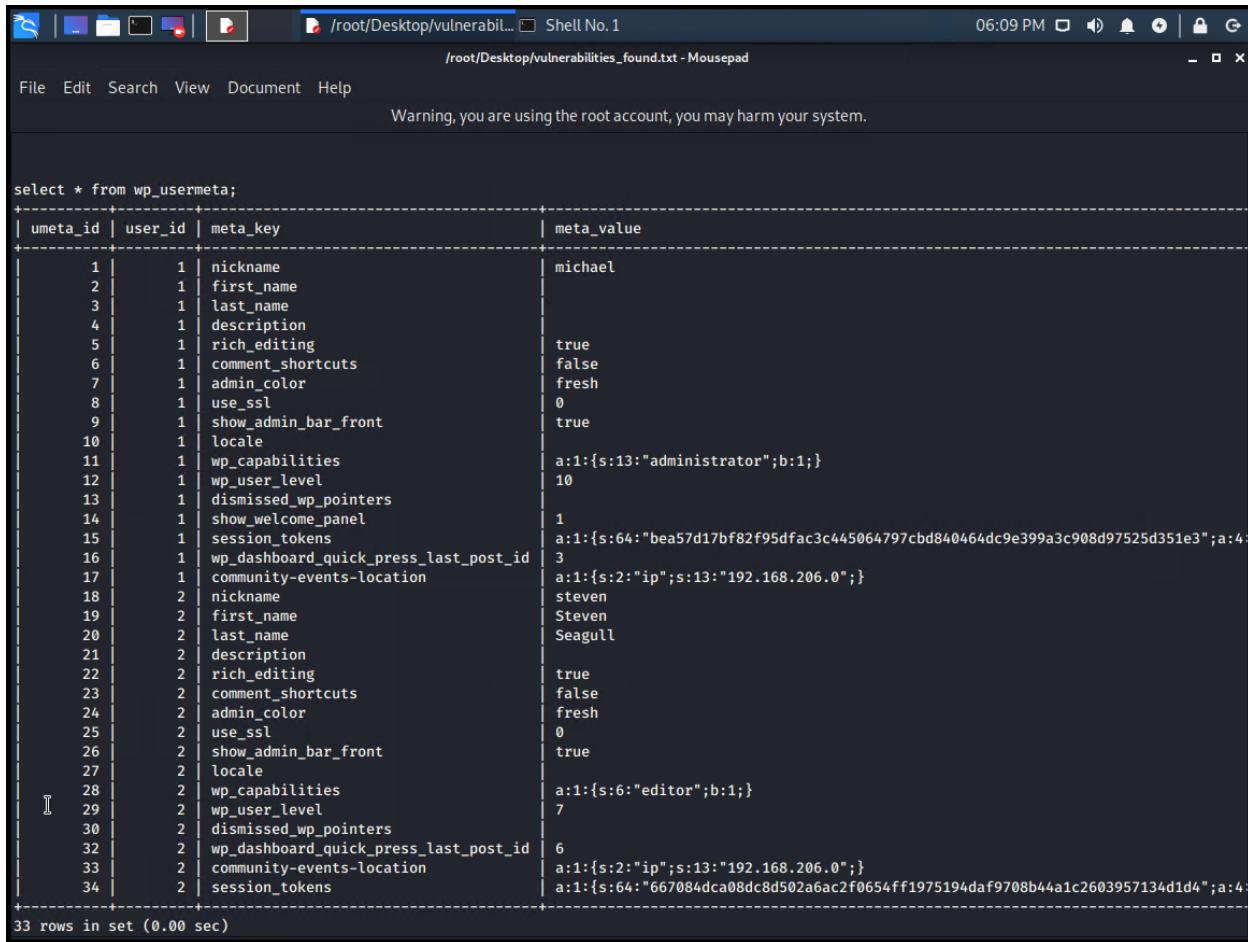
```
michael@target1:/var/www/html/wordpress$ cd wp-content/
michael@target1:/var/www/html/wordpress/wp-content$ ls
index.php languages plugins themes upgrade
michael@target1:/var/www/html/wordpress/wp-content$ cat index.php
<?php
// Silence is golden.
michael@target1:/var/www/html/wordpress/wp-content$ ssh steven@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.
ECDSA key fingerprint is 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hosts.
steven@192.168.1.110's password:
```

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Dec 15 21:25:35 2020 from 192.168.1.90
$ cd /var/www/html/wordpress/
$ ls
index.php wp-admin wp-content wp-config-sample.php wp-links-opml.php wp-settings.php
license.txt wp-blog-header.php wp-content TEXT wp-load.php wp-signup.php
readme.html wp-comments-post.php wp-cron.php wp-login.php wp-trackback.php
wp-activate.php wp-config.php wp-includes wp-mail.php xmlrpc.php
$ cat wp-config.php
```

Wordpress_directory2

Network Analysis Report by Paul Barrett



The screenshot shows a terminal window titled "Shell No. 1" with the command "/root/Desktop/vulnerabilities_found.txt - Mousepad". The window title bar also displays the path "/root/Desktop/vulnerabilities_found.txt". The status bar at the bottom right shows the time as 06:09 PM. A warning message "Warning, you are using the root account, you may harm your system." is visible.

The terminal content is a MySQL query result for the "wp_usermeta" table:

```
select * from wp_usermeta;
+-----+-----+-----+
| umeta_id | user_id | meta_key           | meta_value
+-----+-----+-----+
|       1   |     1   | nickname          | michael
|       2   |     1   | first_name        |
|       3   |     1   | last_name         |
|       4   |     1   | description       |
|       5   |     1   | rich_editing      | true
|       6   |     1   | comment_shortcuts | false
|       7   |     1   | admin_color       | fresh
|       8   |     1   | use_ssl            | 0
|       9   |     1   | show_admin_bar_front | true
|      10  |     1   | locale             |
|      11  |     1   | wp_capabilities    | a:1:{s:13:"administrator";b:1;}
|      12  |     1   | wp_user_level      | 10
|      13  |     1   | dismissed_wp_pointers | 1
|      14  |     1   | show_welcome_panel | a:1:{s:64:"bea57d17bf82f95dfac3c445064797cbd840464dc9e399a3c908d97525d351e3";a:4:
|      15  |     1   | session_tokens      | 3
|      16  |     1   | wp_dashboard_quick_press_last_post_id | a:1:{s:2:"ip";s:13:"192.168.206.0";}
|      17  |     1   | community-events-location | a:1:{s:2:"ip";s:13:"192.168.206.0";}
|      18  |     2   | nickname          | steven
|      19  |     2   | first_name         | Steven
|      20  |     2   | last_name          | Seagull
|      21  |     2   | description        |
|      22  |     2   | rich_editing       | true
|      23  |     2   | comment_shortcuts | false
|      24  |     2   | admin_color        | fresh
|      25  |     2   | use_ssl             | 0
|      26  |     2   | show_admin_bar_front | true
|      27  |     2   | locale              |
|      28  |     2   | wp_capabilities     | a:1:{s:6:"editor";b:1;}
|      29  |     2   | wp_user_level       | 7
|      30  |     2   | dismissed_wp_pointers | 6
|      31  |     2   | wp_dashboard_quick_press_last_post_id | a:1:{s:2:"ip";s:13:"192.168.206.0";}
|      32  |     2   | session_tokens      | a:1:{s:64:"667084dca08dc8d502a6ac2f0654ff1975194daf9708b44a1c2603957134d1d4";a:4:
|      33  |     2   | community-events-location | a:1:{s:2:"ip";s:13:"192.168.206.0";}
|      34  |     2   | session_tokens      |
+-----+-----+-----+
33 rows in set (0.00 sec)
```

Wordpress_usermeta

```
michael@target1:/var/www/html/wordpress/wp-content - □ ×
File Actions Edit View Help

 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define('AUTH_KEY',         '0&ItXmn^q2d[e*yB:9,L:rR<B`h+DG,zQ&SN{Or3zalh.JE+Q!Gi:L7U[(T:J5ay'];
define('SECURE_AUTH_KEY',  'y@^*[q{}NKZAKK{,AA4y-Ia*swA6/0@&r{+RS*N!p1&a$*ctt+ I/!/?A/Tip(BG');
define('LOGGED_IN_KEY',    '.D4}RE4rW2C@9^Bp%#U6i)?cs7,@e]YD:R~fp#hXOk$4o/yD08b7I&/F7SBSLPlj');
define('NONCE_KEY',        '4L{Cq,%ce2?RT7zue#R3DezpNq4sFvcCzF@zdmgL/fKpaGX:EpJt/]xZW1_H646');
define('AUTH_SALT',         '@@?u*YKtt:o/T&V;cbb'.GaJ0./S@dn$t2~n+lr3{PktK]2,*y/b%<BH-Bd#I{oE');
define('SECURE_AUTH_SALT', 'f0Dc#lKmEJi(:-3+x.V#]Wy@mCmp%njtmFb6`_80[8FK,ZQ=+HH/$& mn=]=/cvd');
define('LOGGED_IN_SALT',   '}STRHqy,4scy7v > .. Hc WD*h7rnYq]H`-glDfTVUaOwlh!-/?=3u;##:Rj1]7@');
define('NONCE_SALT',       'i(#~[sXA TbJJfdn&D;0bd`p$r,~.o/?%m<H+<>Vj+,nLvX!-jjjV-o6*HDh5Td{');

/**#@-*/
/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_';

/** Write Out Where Is Cut Text Justify Cut Pos
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG

```

Wp_content_salted