

Network Forensic Analysis Report Done

By: Darrel Mills SOC

Darrel Mills, Security Engineers for X-Corp, supports the SOC team to analyze some discrepancies with alerting in the Kibana system and the manager has asked us to investigate. Yesterday our team confirmed that all the new alerts are working fine. Today we are going to monitor live traffic on the wire to detect any abnormalities that aren't reflected in the alerting system and report back to the SOC manager and the Engineer Manager with all our findings.

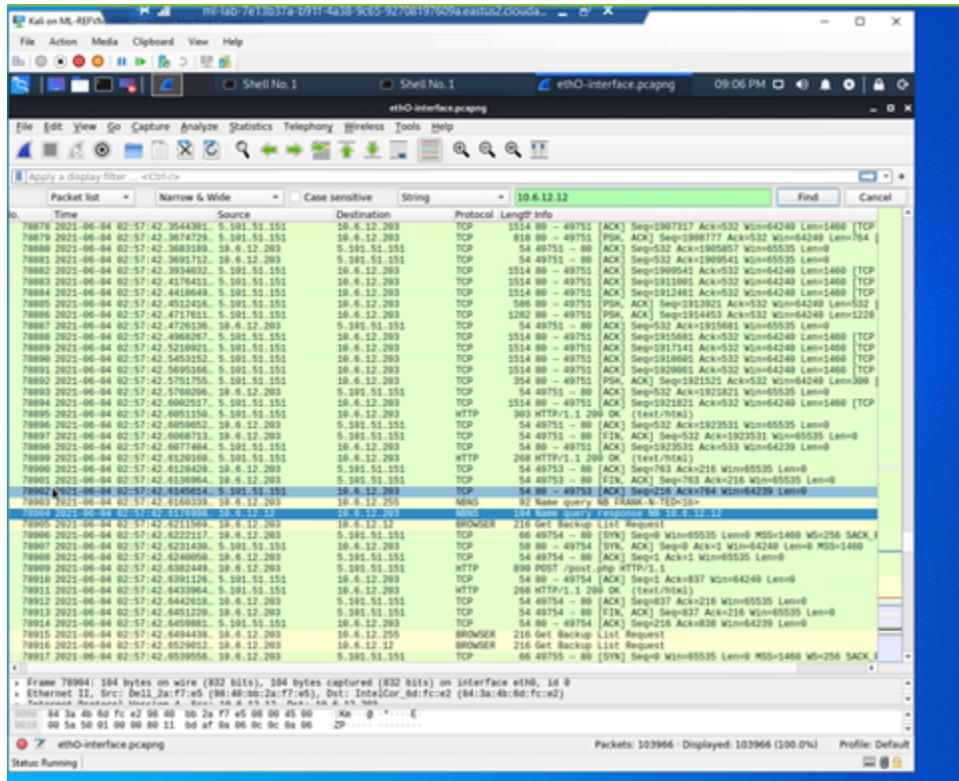
Time Thieves

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

Report was done by: Darrel Mills Cybersecurity Specialist

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

Answer: **Frank-n-ted.com IP 10.6.12.12 destination.**



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

Answer: **10.6.12.157**

3. What is the name of the malware downloaded to the 10.6.12.203 machine?

Answer: june11.dll HTTP/1.1

- Once you have found the file, export it to your Kali machine's desktop.

4. Upload the file to VirusTotal.com (<https://www.virustotal.com/gui/>).

5. What kind of malware is this classified as?

Answer: Malware was a Trojan

The screenshot shows the VirusTotal analysis interface. At the top, there's a navigation bar with a padlock icon, the URL <https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec>, and various icons for sharing and signing in. Below the bar, a large circular progress indicator shows 55 engines have detected the file out of 70. The main content area displays the file's SHA-256 hash, its size (549.84 KB), and the date it was uploaded (2020-10-25 22:21:52 UTC, 1 month ago). A 'Community Score' button is also present. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The DETECTION tab is selected, showing a list of engines and their findings:

Engine	Result	Reporter	Details
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@au!7OQgi	Bkav	W32.AIDetectVM.malware2
Cylance	Unsafe	Cynet	Malicious (score: 100)

Vulnerable Windows Machine

- Network range **172.16.4.0/24**
- IP **10.6.12.12** Frank-n-Ted-DC
- Domain **mind-hammer.net** is part of the infected computer
- DC Network lives at **172.16.4.4** and is named **Mind-Hammer-DC**.

- Network standard Gateway and Broadcast addresses.

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**

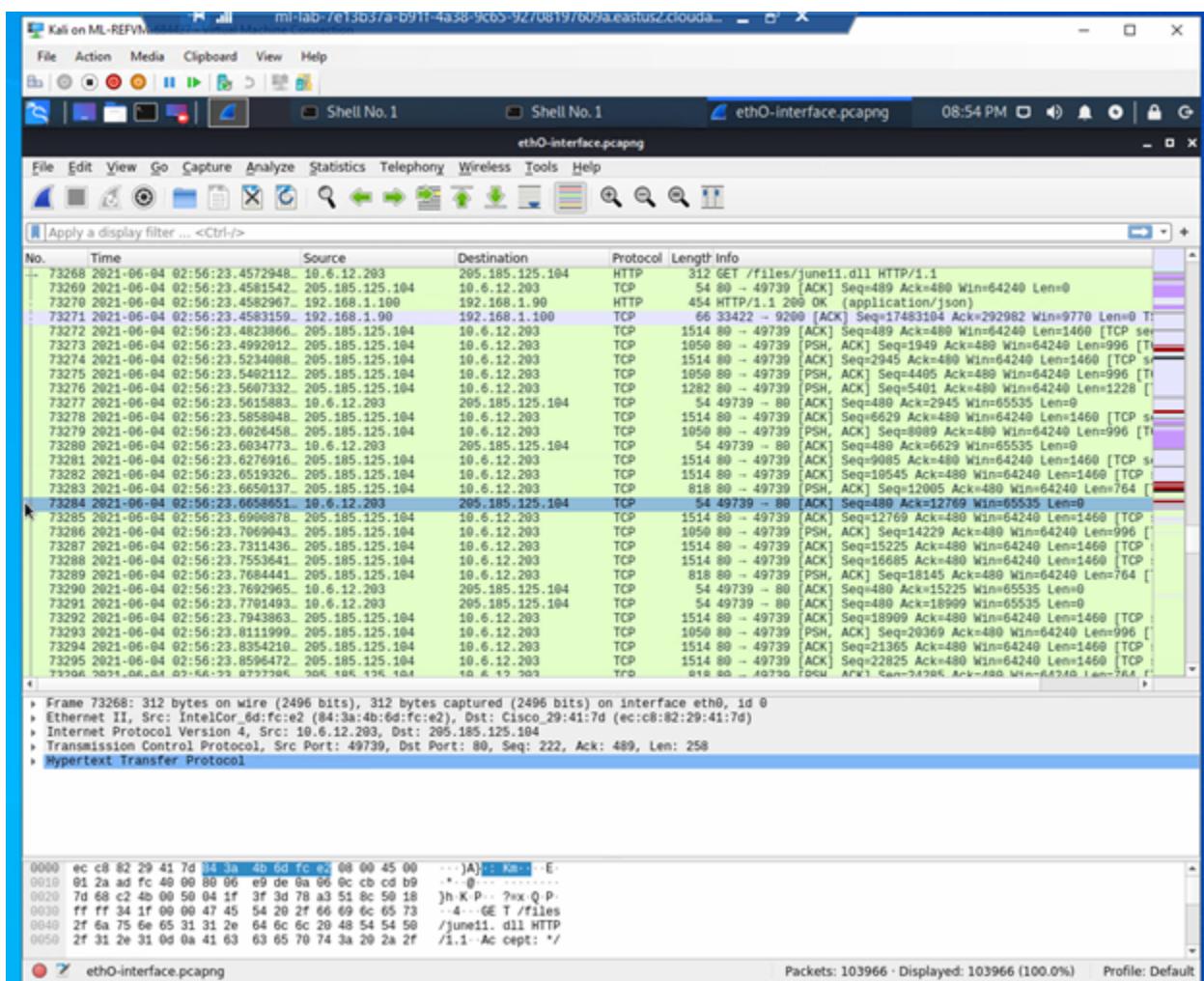
Report was done by: Darrel Mills Cybersecurity Specialist

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

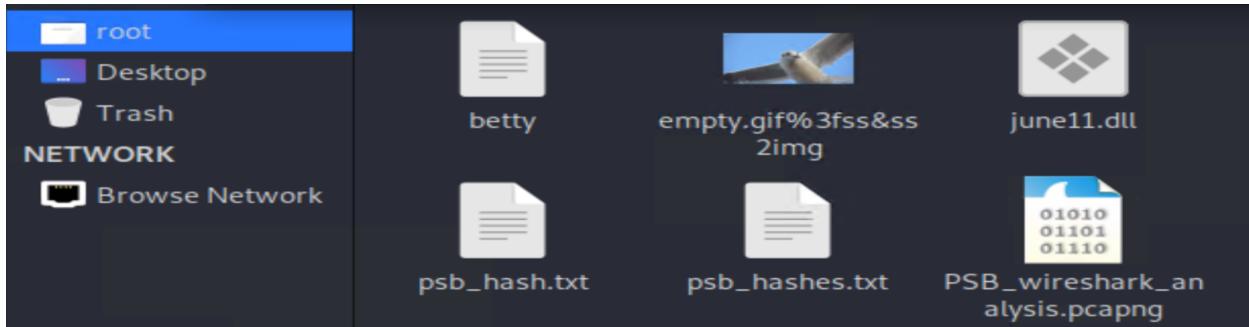
Answer: Mind-Hammer-DC

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

Answer: 205.185.125.104



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



Report was done by: Darrel Mills Cybersecurity Specialist

Illegal Downloads: IT found users torrenting on the network.
Darrel was instructed that 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 infringements.

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 BLANCODESKTOP**
- OS version: **Windows. NT 10.0; Win64; x 64**
- _ Host: **Publicdomaintorrents.info/r/n**

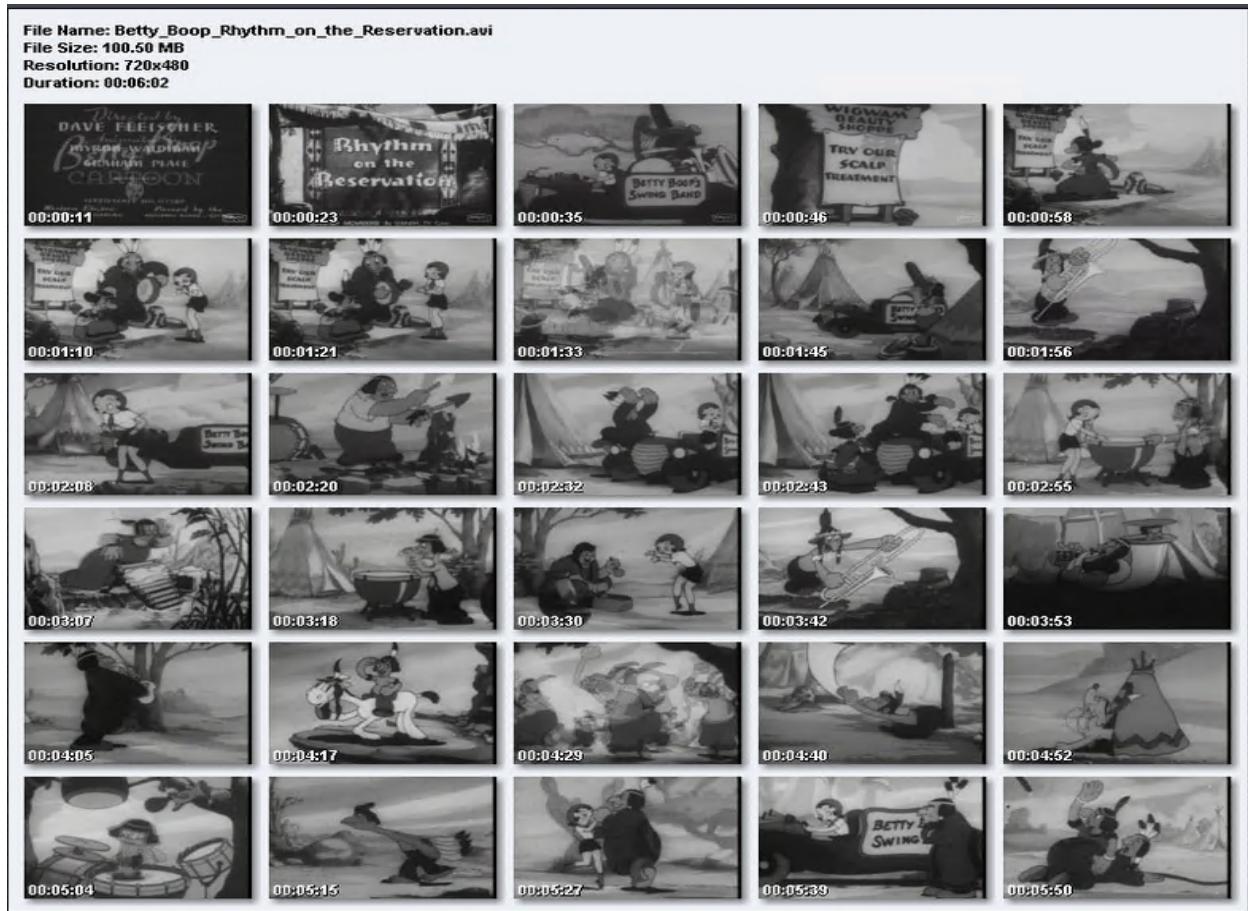
The screenshot shows a Wireshark session titled 'eth0capture.pcapng' with 112851 total packets and 7281 displayed. The packet list pane shows many DNS queries from the source IP 10.0.0.201. The details pane shows a selected DNS query for 'BLANCO-DESKTOP.dogoftheyear.net'. The bytes pane shows the raw hex and ASCII data of the selected packet. The status bar at the bottom indicates the session is 'Running'.

2. Which torrent file did the user download?

Answer: [Betty_Boop_Rhythm_on_the_Reservation.avi](#)

Trojan Malware

And carries the malicious package.



VirusTotal - Mozilla Firefox

virusTotal +

→ C 🌐 https://www.virustotal.com/gui/file/e3b0c44298fc1c149afbf4c8996f... ⚙️ 📮 ⚡

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB Sign

e3b0c44298fc1c149afbf4c8996fb92427ee41e4549b934ca49599fb7852b855

Looks like the community reputation score is being manipulated by the threat actor. Reported this to VT.

 sadew01 9 days ago

Delivered as a phishing email. Hyperlink(<https://547616.selcdn.ru/sog/iso4g.html>) goes to a Russian hosted TLD. Uses the email it sent to as a verification URL (which I have redacted). Pulls php files from a compromised server at <https://lyonsdavidson-lp.co.uk/include/>. This appears to have been compromised 24th per the file DTG on the web server. There are a large number of variants of PHP files that appear to be target specific.

 danross 10 days ago

Most definitely malware. It's using - WindowsUpdate.com - to pull in malicious files that are masked as Windows Updates. I've spent 2+ months dealing with a number of related malware.

That goes back to the recent Kaspersky article and what's been named - Moriya/TunnelSnake.

This being a related file.

 lemmeln84 14 days ago

outstanding one other version...

Report was done by: Darrel Mills Cybersecurity Specialist

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 - Packet 69719 - PSB_wireshark_analysis.pcapng

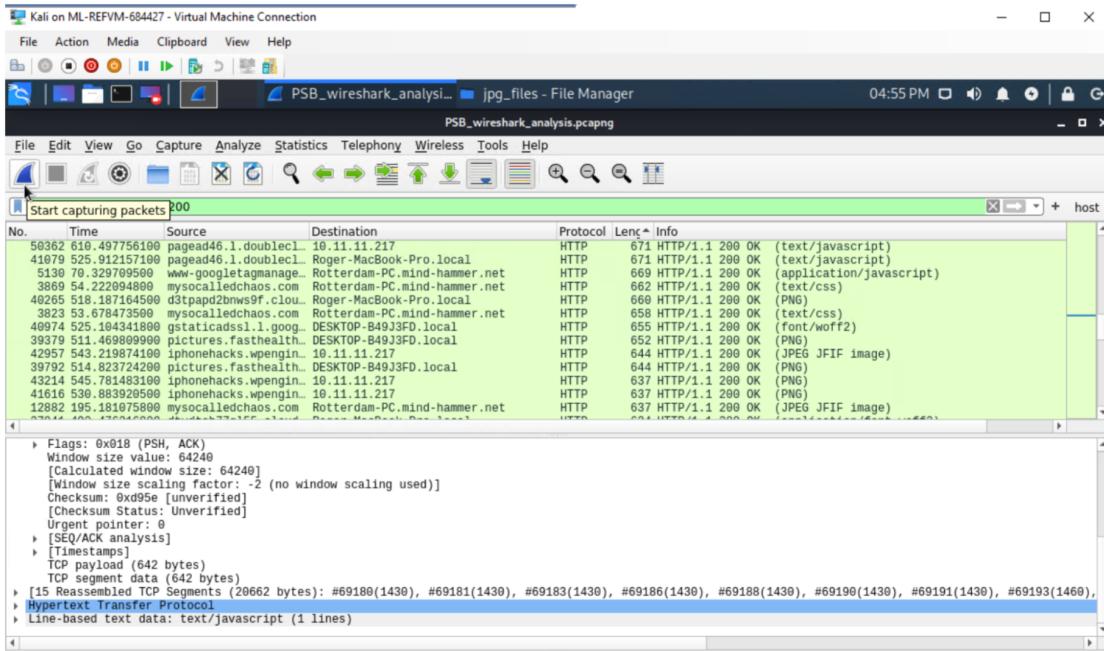
```

Frame 69719: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface eth0, id 0
  Ethernet II, Src: Cisco_27:a1:3e (00:09:b7:27:a1:3e), Dst: Ms1_18:66:c8 (00:16:17:18:66:c8)
  Internet Protocol Version 4, Src: 188.215.194.14, Dst: 10.0.0.1
  Transmission Control Protocol Src Port: 80, Dst Port: 49834
    Seq: 8621, Ack: 536, Len: 5
  [7] Reassembled TCP Segments (8625 bytes): #69719(1460), #69711(1460), #69712(1460), #69713(1460), #69715(1460), #69717(1460)
  Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
    Date: Sun, 15 Jul 2018 04:17:27 GMT\r\n
    Server: Apache/2.4.29 (Ubuntu)\r\n
    Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent"\r\n
    Set-Cookie: PHPSESSID=a42bb063capgr3he6jaflt4pt2; path=/\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Transfer-Encoding: chunked\r\n
    Content-Type: application/x-bittorrent\r\n
    \r\n
    [HTTP response 1/1]
    Time since request: 0.149293500 seconds
  
```

Location/x-bittorrent
 86 Ack=8626 Win=65535 Len=0
 Seq=3255 Ack=1478 Win=65535
 > ACK Seq=3256 Ack=1479 Win=65535
 > Seq=3257 Ack=1479 Win=65535
 > Seq=3258 Ack=1479 Win=65535
 > Seq=3259 Ack=1479 Win=65535
 > Seq=3260 Ack=1479 Win=65535
 > Seq=3261 Ack=1479 Win=65535
 > Seq=3262 Ack=1479 Win=65535
 > Seq=3263 Ack=1479 Win=65535
 > Seq=3264 Ack=1479 Win=65535
 > Seq=3265 Ack=1479 Win=65535
 > Seq=3266 Ack=1479 Win=65535
 > Seq=3267 Ack=1479 Win=65535
 > Seq=3268 Ack=1479 Win=65535
 > Seq=3269 Ack=1479 Win=65535
 > Seq=3270 Ack=1479 Win=65535
 > Seq=3271 Ack=1479 Win=65535
 > Seq=3272 Ack=1479 Win=65535
 > Seq=3273 Ack=1479 Win=65535
 > Seq=3274 Ack=1479 Win=65535
 > Seq=3275 Ack=1479 Win=65535
 > Seq=3276 Ack=1479 Win=65535
 > Seq=3277 Ack=1479 Win=65535
 > Seq=3278 Ack=1479 Win=65535
 > Seq=3279 Ack=1479 Win=65535
 > Seq=3280 Ack=1479 Win=65535
 > Seq=3281 Ack=1479 Win=65535
 > Seq=3282 Ack=1479 Win=65535
 > Seq=3283 Ack=1479 Win=65535
 > Seq=3284 Ack=1479 Win=65535
 > Seq=3285 Ack=1479 Win=65535
 > Seq=3286 Ack=1479 Win=65535
 > Seq=3287 Ack=1479 Win=65535
 > Seq=3288 Ack=1479 Win=65535
 > Seq=3289 Ack=1479 Win=65535
 > Seq=3290 Ack=1479 Win=65535
 > Seq=3291 Ack=1479 Win=65535
 > Seq=3292 Ack=1479 Win=65535
 > Seq=3293 Ack=1479 Win=65535
 > Seq=3294 Ack=1479 Win=65535
 > Seq=3295 Ack=1479 Win=65535
 > Seq=3296 Ack=1479 Win=65535
 > Seq=3297 Ack=1479 Win=65535
 > Seq=3298 Ack=1479 Win=65535
 > Seq=3299 Ack=1479 Win=65535
 > Seq=3300 Ack=1479 Win=65535
 > Seq=3301 Ack=1479 Win=65535
 > Seq=3302 Ack=1479 Win=65535
 > Seq=3303 Ack=1479 Win=65535
 > Seq=3304 Ack=1479 Win=65535
 > Seq=3305 Ack=1479 Win=65535
 > Seq=3306 Ack=1479 Win=65535
 > Seq=3307 Ack=1479 Win=65535
 > Seq=3308 Ack=1479 Win=65535
 > Seq=3309 Ack=1479 Win=65535
 > Seq=3310 Ack=1479 Win=65535
 > Seq=3311 Ack=1479 Win=65535
 > Seq=3312 Ack=1479 Win=65535
 > Seq=3313 Ack=1479 Win=65535
 > Seq=3314 Ack=1479 Win=65535
 > Seq=3315 Ack=1479 Win=65535
 > Seq=3316 Ack=1479 Win=65535
 > Seq=3317 Ack=1479 Win=65535
 > Seq=3318 Ack=1479 Win=65535
 > Seq=3319 Ack=1479 Win=65535
 > Seq=3320 Ack=1479 Win=65535
 > Seq=3321 Ack=1479 Win=65535
 > Seq=3322 Ack=1479 Win=65535
 > Seq=3323 Ack=1479 Win=65535
 > Seq=3324 Ack=1479 Win=65535
 > Seq=3325 Ack=1479 Win=65535
 > Seq=3326 Ack=1479 Win=65535
 > Seq=3327 Ack=1479 Win=65535
 > Seq=3328 Ack=1479 Win=65535
 > Seq=3329 Ack=1479 Win=65535
 > Seq=3330 Ack=1479 Win=65535
 > Seq=3331 Ack=1479 Win=65535
 > Seq=3332 Ack=1479 Win=65535
 > Seq=3333 Ack=1479 Win=65535
 > Seq=3334 Ack=1479 Win=65535
 > Seq=3335 Ack=1479 Win=65535
 > Seq=3336 Ack=1479 Win=65535
 > Seq=3337 Ack=1479 Win=65535
 > Seq=3338 Ack=1479 Win=65535
 > Seq=3339 Ack=1479 Win=65535
 > Seq=3340 Ack=1479 Win=65535
 > Seq=3341 Ack=1479 Win=65535
 > Seq=3342 Ack=1479 Win=65535
 > Seq=3343 Ack=1479 Win=65535
 > Seq=3344 Ack=1479 Win=65535
 > Seq=3345 Ack=1479 Win=65535
 > Seq=3346 Ack=1479 Win=65535
 > Seq=3347 Ack=1479 Win=65535
 > Seq=3348 Ack=1479 Win=65535
 > Seq=3349 Ack=1479 Win=65535
 > Seq=3350 Ack=1479 Win=65535
 > Seq=3351 Ack=1479 Win=65535
 > Seq=3352 Ack=1479 Win=65535
 > Seq=3353 Ack=1479 Win=65535
 > Seq=3354 Ack=1479 Win=65535
 > Seq=3355 Ack=1479 Win=65535
 > Seq=3356 Ack=1479 Win=65535
 > Seq=3357 Ack=1479 Win=65535
 > Seq=3358 Ack=1479 Win=65535
 > Seq=3359 Ack=1479 Win=65535
 > Seq=3360 Ack=1479 Win=65535
 > Seq=3361 Ack=1479 Win=65535
 > Seq=3362 Ack=1479 Win=65535
 > Seq=3363 Ack=1479 Win=65535
 > Seq=3364 Ack=1479 Win=65535
 > Seq=3365 Ack=1479 Win=65535
 > Seq=3366 Ack=1479 Win=65535
 > Seq=3367 Ack=1479 Win=65535
 > Seq=3368 Ack=1479 Win=65535
 > Seq=3369 Ack=1479 Win=65535
 > Seq=3370 Ack=1479 Win=65535
 > Seq=3371 Ack=1479 Win=65535
 > Seq=3372 Ack=1479 Win=65535
 > Seq=3373 Ack=1479 Win=65535
 > Seq=3374 Ack=1479 Win=65535
 > Seq=3375 Ack=1479 Win=65535
 > Seq=3376 Ack=1479 Win=65535
 > Seq=3377 Ack=1479 Win=65535
 > Seq=3378 Ack=1479 Win=65535
 > Seq=3379 Ack=1479 Win=65535
 > Seq=3380 Ack=1479 Win=65535
 > Seq=3381 Ack=1479 Win=65535
 > Seq=3382 Ack=1479 Win=65535
 > Seq=3383 Ack=1479 Win=65535
 > Seq=3384 Ack=1479 Win=65535
 > Seq=3385 Ack=1479 Win=65535
 > Seq=3386 Ack=1479 Win=65535
 > Seq=3387 Ack=1479 Win=65535
 > Seq=3388 Ack=1479 Win=65535
 > Seq=3389 Ack=1479 Win=65535
 > Seq=3390 Ack=1479 Win=65535
 > Seq=3391 Ack=1479 Win=65535
 > Seq=3392 Ack=1479 Win=65535
 > Seq=3393 Ack=1479 Win=65535
 > Seq=3394 Ack=1479 Win=65535
 > Seq=3395 Ack=1479 Win=65535
 > Seq=3396 Ack=1479 Win=65535
 > Seq=3397 Ack=1479 Win=65535
 > Seq=3398 Ack=1479 Win=65535
 > Seq=3399 Ack=1479 Win=65535
 > Seq=3400 Ack=1479 Win=65535
 > Seq=3401 Ack=1479 Win=65535
 > Seq=3402 Ack=1479 Win=65535
 > Seq=3403 Ack=1479 Win=65535
 > Seq=3404 Ack=1479 Win=65535
 > Seq=3405 Ack=1479 Win=65535
 > Seq=3406 Ack=1479 Win=65535
 > Seq=3407 Ack=1479 Win=65535
 > Seq=3408 Ack=1479 Win=65535
 > Seq=3409 Ack=1479 Win=65535
 > Seq=3410 Ack=1479 Win=65535
 > Seq=3411 Ack=1479 Win=65535
 > Seq=3412 Ack=1479 Win=65535
 > Seq=3413 Ack=1479 Win=65535
 > Seq=3414 Ack=1479 Win=65535
 > Seq=3415 Ack=1479 Win=65535
 > Seq=3416 Ack=1479 Win=65535
 > Seq=3417 Ack=1479 Win=65535
 > Seq=3418 Ack=1479 Win=65535
 > Seq=3419 Ack=1479 Win=65535
 > Seq=3420 Ack=1479 Win=65535
 > Seq=3421 Ack=1479 Win=65535
 > Seq=3422 Ack=1479 Win=65535
 > Seq=3423 Ack=1479 Win=65535
 > Seq=3424 Ack=1479 Win=65535
 > Seq=3425 Ack=1479 Win=65535
 > Seq=3426 Ack=1479 Win=65535
 > Seq=3427 Ack=1479 Win=65535
 > Seq=3428 Ack=1479 Win=65535
 > Seq=3429 Ack=1479 Win=65535
 > Seq=3430 Ack=1479 Win=65535
 > Seq=3431 Ack=1479 Win=65535
 > Seq=3432 Ack=1479 Win=65535
 > Seq=3433 Ack=1479 Win=65535
 > Seq=3434 Ack=1479 Win=65535
 > Seq=3435 Ack=1479 Win=65535
 > Seq=3436 Ack=1479 Win=65535
 > Seq=3437 Ack=1479 Win=65535
 > Seq=3438 Ack=1479 Win=65535
 > Seq=3439 Ack=1479 Win=65535
 > Seq=3440 Ack=1479 Win=65535
 > Seq=3441 Ack=1479 Win=65535
 > Seq=3442 Ack=1479 Win=65535
 > Seq=3443 Ack=1479 Win=65535
 > Seq=3444 Ack=1479 Win=65535
 > Seq=3445 Ack=1479 Win=65535
 > Seq=3446 Ack=1479 Win=65535
 > Seq=3447 Ack=1479 Win=65535
 > Seq=3448 Ack=1479 Win=65535
 > Seq=3449 Ack=1479 Win=65535
 > Seq=3450 Ack=1479 Win=65535
 > Seq=3451 Ack=1479 Win=65535
 > Seq=3452 Ack=1479 Win=65535
 > Seq=3453 Ack=1479 Win=65535
 > Seq=3454 Ack=1479 Win=65535
 > Seq=3455 Ack=1479 Win=65535
 > Seq=3456 Ack=1479 Win=65535
 > Seq=3457 Ack=1479 Win=65535
 > Seq=3458 Ack=1479 Win=65535
 > Seq=3459 Ack=1479 Win=65535
 > Seq=3460 Ack=1479 Win=65535
 > Seq=3461 Ack=1479 Win=65535
 > Seq=3462 Ack=1479 Win=65535
 > Seq=3463 Ack=1479 Win=65535
 > Seq=3464 Ack=1479 Win=65535
 > Seq=3465 Ack=1479 Win=65535
 > Seq=3466 Ack=1479 Win=65535
 > Seq=3467 Ack=1479 Win=65535
 > Seq=3468 Ack=1479 Win=65535
 > Seq=3469 Ack=1479 Win=65535
 > Seq=3470 Ack=1479 Win=65535
 > Seq=3471 Ack=1479 Win=65535
 > Seq=3472 Ack=1479 Win=65535
 > Seq=3473 Ack=1479 Win=65535
 > Seq=3474 Ack=1479 Win=65535
 > Seq=3475 Ack=1479 Win=65535
 > Seq=3476 Ack=1479 Win=65535
 > Seq=3477 Ack=1479 Win=65535
 > Seq=3478 Ack=1479 Win=65535
 > Seq=3479 Ack=1479 Win=65535
 > Seq=3480 Ack=1479 Win=65535
 > Seq=3481 Ack=1479 Win=65535
 > Seq=3482 Ack=1479 Win=65535
 > Seq=3483 Ack=1479 Win=65535
 > Seq=3484 Ack=1479 Win=65535
 > Seq=3485 Ack=1479 Win=65535
 > Seq=3486 Ack=1479 Win=65535
 > Seq=3487 Ack=1479 Win=65535
 > Seq=3488 Ack=1479 Win=65535
 > Seq=3489 Ack=1479 Win=65535
 > Seq=3490 Ack=1479 Win=65535
 > Seq=3491 Ack=1479 Win=65535
 > Seq=3492 Ack=1479 Win=65535
 > Seq=3493 Ack=1479 Win=65535
 > Seq=3494 Ack=1479 Win=65535
 > Seq=3495 Ack=1479 Win=65535
 > Seq=3496 Ack=1479 Win=65535
 > Seq=3497 Ack=1479 Win=65535
 > Seq=3498 Ack=1479 Win=65535
 > Seq=3499 Ack=1479 Win=65535
 > Seq=3500 Ack=1479 Win=65535
 > Seq=3501 Ack=1479 Win=65535
 > Seq=3502 Ack=1479 Win=65535
 > Seq=3503 Ack=1479 Win=65535
 > Seq=3504 Ack=1479 Win=65535
 > Seq=3505 Ack=1479 Win=65535
 > Seq=3506 Ack=1479 Win=65535
 > Seq=3507 Ack=1479 Win=65535
 > Seq=3508 Ack=1479 Win=65535
 > Seq=3509 Ack=1479 Win=65535
 > Seq=3510 Ack=1479 Win=65535
 > Seq=3511 Ack=1479 Win=65535
 > Seq=3512 Ack=1479 Win=65535
 > Seq=3513 Ack=1479 Win=65535
 > Seq=3514 Ack=1479 Win=65535
 > Seq=3515 Ack=1479 Win=65535
 > Seq=3516 Ack=1479 Win=65535
 > Seq=3517 Ack=1479 Win=65535
 > Seq=3518 Ack=1479 Win=65535
 > Seq=3519 Ack=1479 Win=65535
 > Seq=3520 Ack=1479 Win=65535
 > Seq=3521 Ack=1479 Win=65535
 > Seq=3522 Ack=1479 Win=65535
 > Seq=3523 Ack=1479 Win=65535
 > Seq=3524 Ack=1479 Win=65535
 > Seq=3525 Ack=1479 Win=65535
 > Seq=3526 Ack=1479 Win=65535
 > Seq=3527 Ack=1479 Win=65535
 > Seq=3528 Ack=1479 Win=65535
 > Seq=3529 Ack=1479 Win=65535
 > Seq=3530 Ack=1479 Win=65535
 > Seq=3531 Ack=1479 Win=65535
 > Seq=3532 Ack=1479 Win=65535
 > Seq=3533 Ack=1479 Win=65535
 > Seq=3534 Ack=1479 Win=65535
 > Seq=3535 Ack=1479 Win=65535
 > Seq=3536 Ack=1479 Win=65535
 > Seq=3537 Ack=1479 Win=65535
 > Seq=3538 Ack=1479 Win=65535
 > Seq=3539 Ack=1479 Win=65535
 > Seq=3540 Ack=1479 Win=65535
 > Seq=3541 Ack=1479 Win=65535
 > Seq=3542 Ack=1479 Win=65535
 > Seq=3543 Ack=1479 Win=65535
 > Seq=3544 Ack=1479 Win=65535
 > Seq=3545 Ack=1479 Win=65535
 > Seq=3546 Ack=1479 Win=65535
 > Seq=3547 Ack=1479 Win=65535
 > Seq=3548 Ack=1479 Win=65535
 > Seq=3549 Ack=1479 Win=65535
 > Seq=3550 Ack=1479 Win=65535
 > Seq=3551 Ack=1479 Win=65535
 > Seq=3552 Ack=1479 Win=65535
 > Seq=3553 Ack=1479 Win=65535
 > Seq=3554 Ack=1479 Win=65535
 > Seq=3555 Ack=1479 Win=65535
 > Seq=3556 Ack=1479 Win=65535
 > Seq=3557 Ack=1479 Win=65535
 > Seq=3558 Ack=1479 Win=65535
 > Seq=3559 Ack=1479 Win=65535
 > Seq=3560 Ack=1479 Win=65535
 > Seq=3561 Ack=1479 Win=65535
 > Seq=3562 Ack=1479 Win=65535
 > Seq=3563 Ack=1479 Win=65535
 > Seq=3564 Ack=1479 Win=65535
 > Seq=3565 Ack=1479 Win=65535
 > Seq=3566 Ack=1479 Win=65535
 > Seq=3567 Ack=1479 Win=65535
 > Seq=3568 Ack=1479 Win=65535
 > Seq=3569 Ack=1479 Win=65535
 > Seq=3570 Ack=1479 Win=65535
 > Seq=3571 Ack=1479 Win=65535
 > Seq=3572 Ack=1479 Win=65535
 > Seq=3573 Ack=1479 Win=65535
 > Seq=3574 Ack=1479 Win=65535
 > Seq=3575 Ack=1479 Win=65535
 > Seq=3576 Ack=1479 Win=65535
 > Seq=3577 Ack=1479 Win=65535
 > Seq=3578 Ack=1479 Win=65535
 > Seq=3579 Ack=1479 Win=65535
 > Seq=3580 Ack=1479 Win=65535
 > Seq=3581 Ack=1479 Win=65535
 > Seq=3582 Ack=1479 Win=65535
 > Seq=3583 Ack=1479 Win=65535
 > Seq=3584 Ack=1479 Win=65535
 > Seq=3585 Ack=1479 Win=65535
 > Seq=3586 Ack=1479 Win=65535
 > Seq=3587 Ack=1479 Win=65535
 > Seq=3588 Ack=1479 Win=65535
 > Seq=3589 Ack=1479 Win=65535
 > Seq=3590 Ack=1479 Win=65535
 > Seq=3591 Ack=1479 Win=65535
 > Seq=3592 Ack=1479 Win=65535
 > Seq=3593 Ack=1479 Win=65535
 > Seq=3594 Ack=1479 Win=65535
 > Seq=3595 Ack=1479 Win=65535
 > Seq=3596 Ack=1479 Win=65535
 > Seq=3597 Ack=1479 Win=65535
 > Seq=3598 Ack=1479 Win=65535
 > Seq=3599 Ack=1479 Win=65535
 > Seq=3600 Ack=1479 Win=65535
 > Seq=3601 Ack=1479 Win=65535
 > Seq=3602 Ack=1479 Win=65535
 > Seq=3603 Ack=1479 Win=65535
 > Seq=3604 Ack=1479 Win=65535
 > Seq=3605 Ack=1479 Win=65535
 > Seq=3606 Ack=1479 Win=65535
 > Seq=3607 Ack=1479 Win=65535
 > Seq=3608 Ack=1479 Win=65535
 > Seq=3609 Ack=1479 Win=65535
 > Seq=3610 Ack=1479 Win=65535
 > Seq=3611 Ack=1479 Win=65535
 > Seq=3612 Ack=1479 Win=65535
 > Seq=3613 Ack=1479 Win=65535
 > Seq=3614 Ack=1479 Win=65535
 > Seq=3615 Ack=1479 Win=65535
 > Seq=3616 Ack=1479 Win=65535
 > Seq=3617 Ack=1479 Win=65535
 > Seq=3618 Ack=1479 Win=65535
 > Seq=3619 Ack=1479 Win=65535
 > Seq=3620 Ack=1479 Win=65535
 > Seq=3621 Ack=1479 Win=65535
 > Seq=3622 Ack=1479 Win=65535
 > Seq=3623 Ack=1479 Win=65535
 > Seq=3624 Ack=1479 Win=65535
 > Seq=3625 Ack=1479 Win=65535
 > Seq=3626 Ack=1479 Win=65535
 > Seq=3627 Ack=1479 Win=65535
 > Seq=3628 Ack=1479 Win=65535
 > Seq=3629 Ack=1479 Win=65535
 > Seq=3630 Ack=1479 Win=65535
 > Seq=3631 Ack=1479 Win=65535
 > Seq=3632 Ack=1479 Win=65535
 > Seq=3633 Ack=1479 Win=65535
 > Seq=3634 Ack=1479 Win=65535
 > Seq=3635 Ack=1479 Win=65535
 > Seq=3636 Ack=1479 Win=65535
 > Seq=3637 Ack=1479 Win=65535
 > Seq=3638 Ack=1479 Win=65535
 > Seq=3639 Ack=1479 Win=65535
 > Seq=3640 Ack=1479 Win=65535
 > Seq=3641 Ack=1479 Win=65535
 > Seq=3642 Ack=1479 Win=65535
 > Seq=3643 Ack=1479 Win=65535
 > Seq=3644 Ack=1479 Win=65535
 > Seq=3645 Ack=1479 Win=65535
 > Seq=3646 Ack=1479 Win=65535
 > Seq=3647 Ack=1479 Win=65535
 > Seq=3648 Ack=1479 Win=65535
 > Seq=3649 Ack=1479 Win=65535
 > Seq=3650 Ack=1479 Win=65535
 > Seq=3651 Ack=1479 Win=65535
 > Seq=3652 Ack=1479 Win=65535
 > Seq=3653 Ack=1479 Win=65535
 > Seq=3654 Ack=1479 Win=65535
 > Seq=3655 Ack=1479 Win=65535
 > Seq=3656 Ack=1479 Win=65535
 > Seq=3657 Ack=1479 Win=65535
 > Seq=3658 Ack=1479 Win=65535
 > Seq=3659 Ack=1479 Win=65535
 > Seq=3660 Ack=1479 Win=65535
 > Seq=3661 Ack=1479 Win=65535
 > Seq=3662 Ack=1479 Win=65535
 > Seq=3663 Ack=1479 Win=65535
 > Seq=3664 Ack=1479 Win=65535
 > Seq=3665 Ack=1479 Win=65

Wireshark - Endpoints - PSB_wireshark_analysis.pcapng													
Ethernet · 30	IPv4 · 808	IPv6 · 2	TCP · 1372	UDP · 1977	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	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.mattingolutions.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-5WKH9YGY.frank-n-ted.com	7,410	5,574 k	2,567	399 k	4,843	5,175 k	—	—	—	—	—
a1449.dsccg2.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.kcl.net	4,883	3,637 k	2,648	3,492 k	2,235	144 k	—	—	—	—	—
snnmnkxdhfwlwthqismb.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.imgur.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	—	—	—	—	—



Report was done by: Darrel Mills Cybersecurity Specialist

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

PSB_wireshark_analysis.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

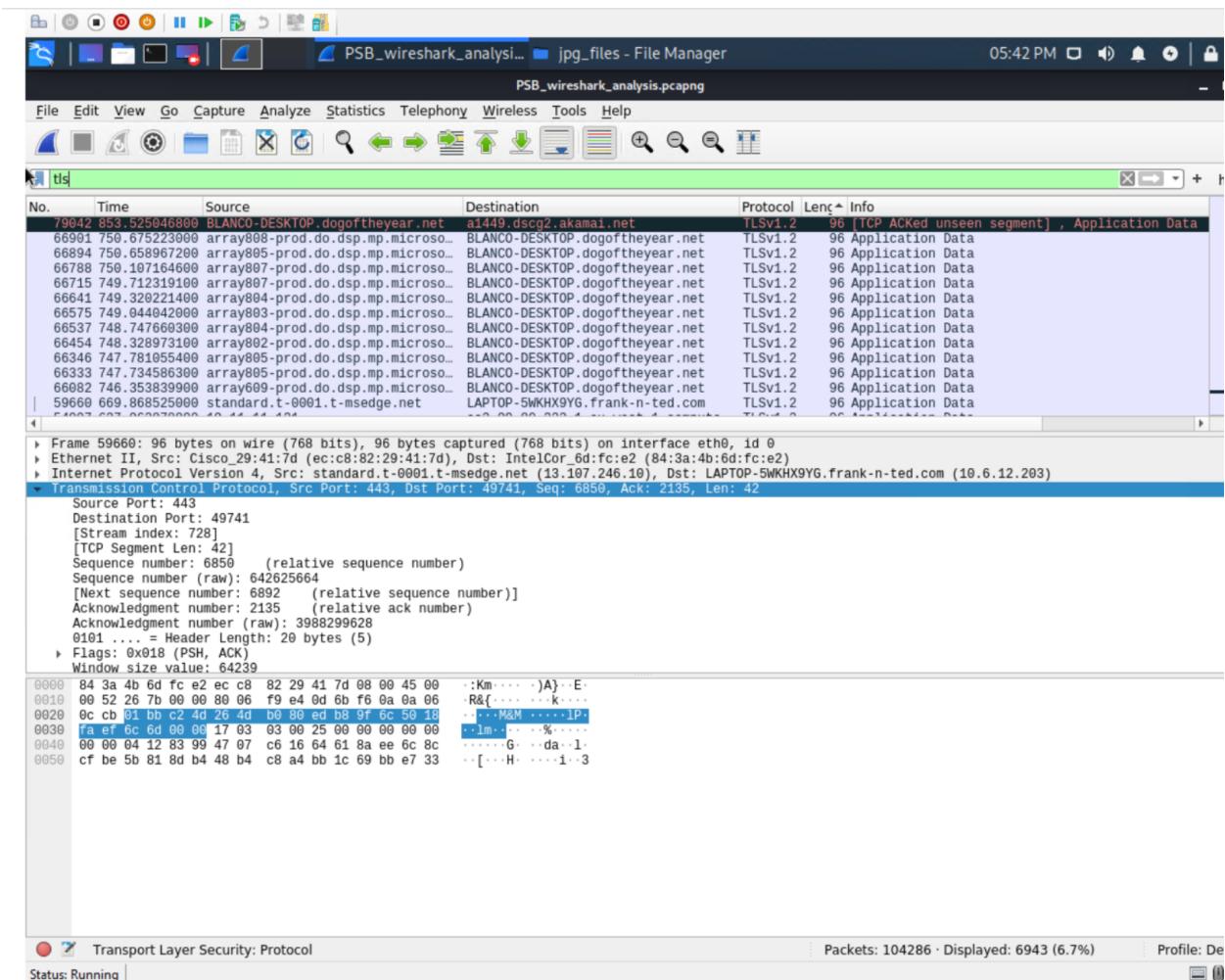
Wireshark - Endpoints - PSB_wireshark_analysis.pcapng

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	—	—	—	—
5.39.80.140	15	3,277	7	843	0	1,334	—	—	—	—

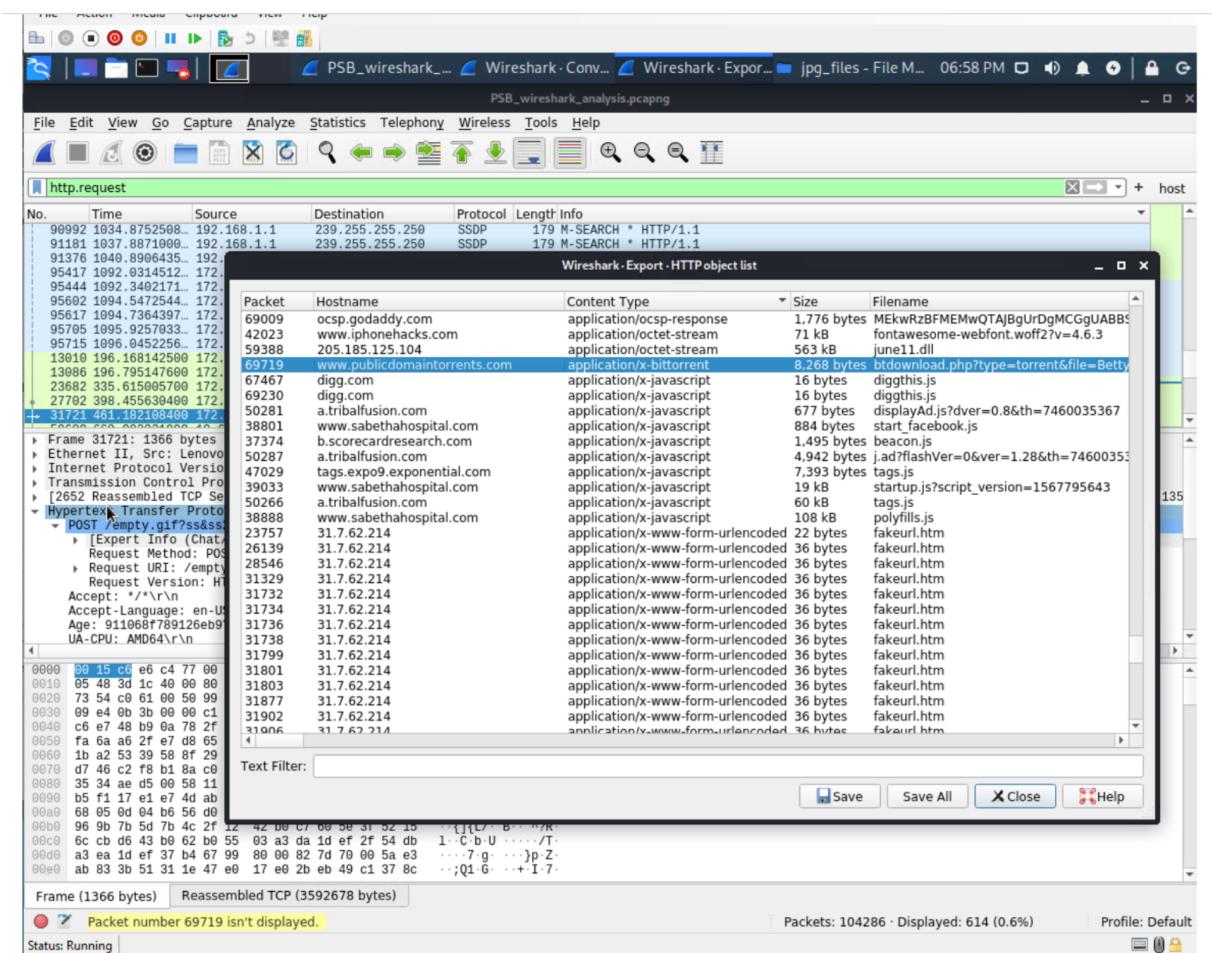
Wireshark - Export - HTTP object list

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

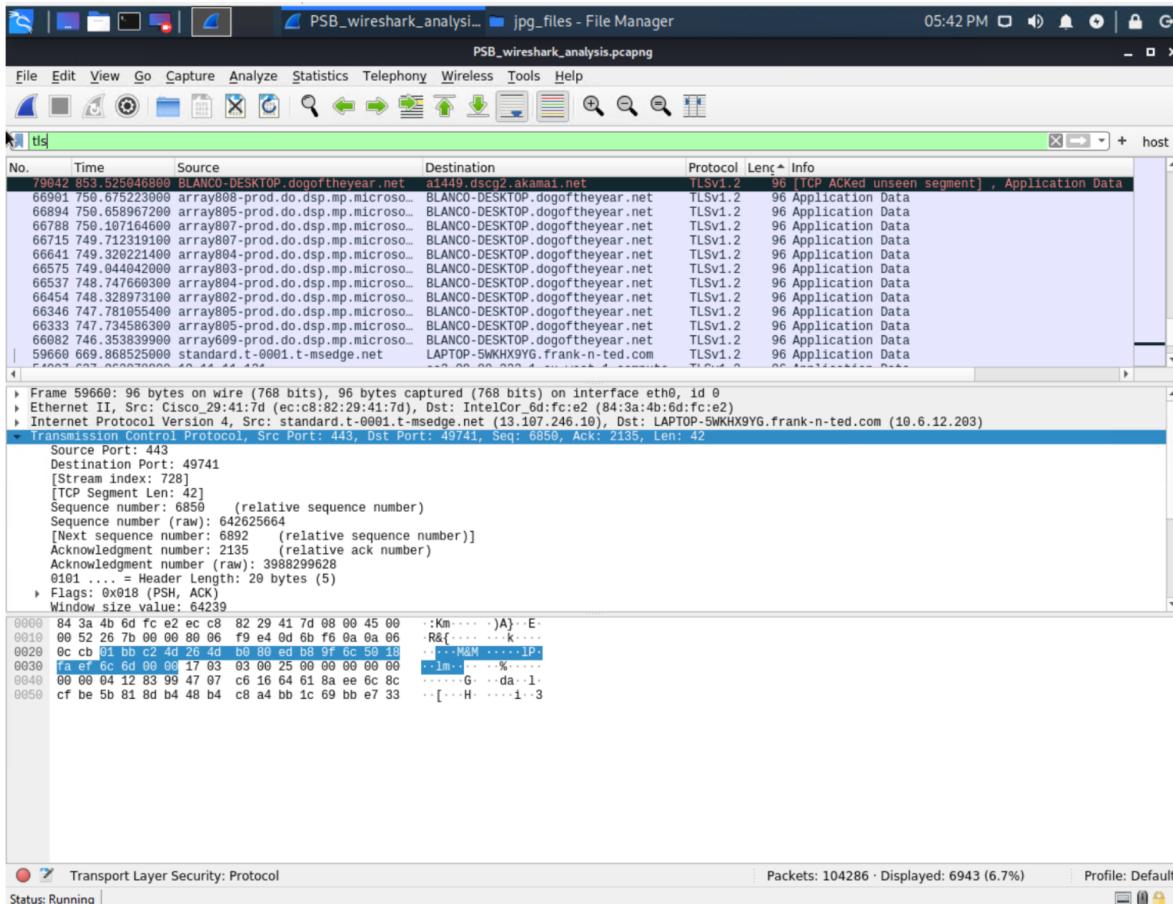
Wireshark_bittorrent.png



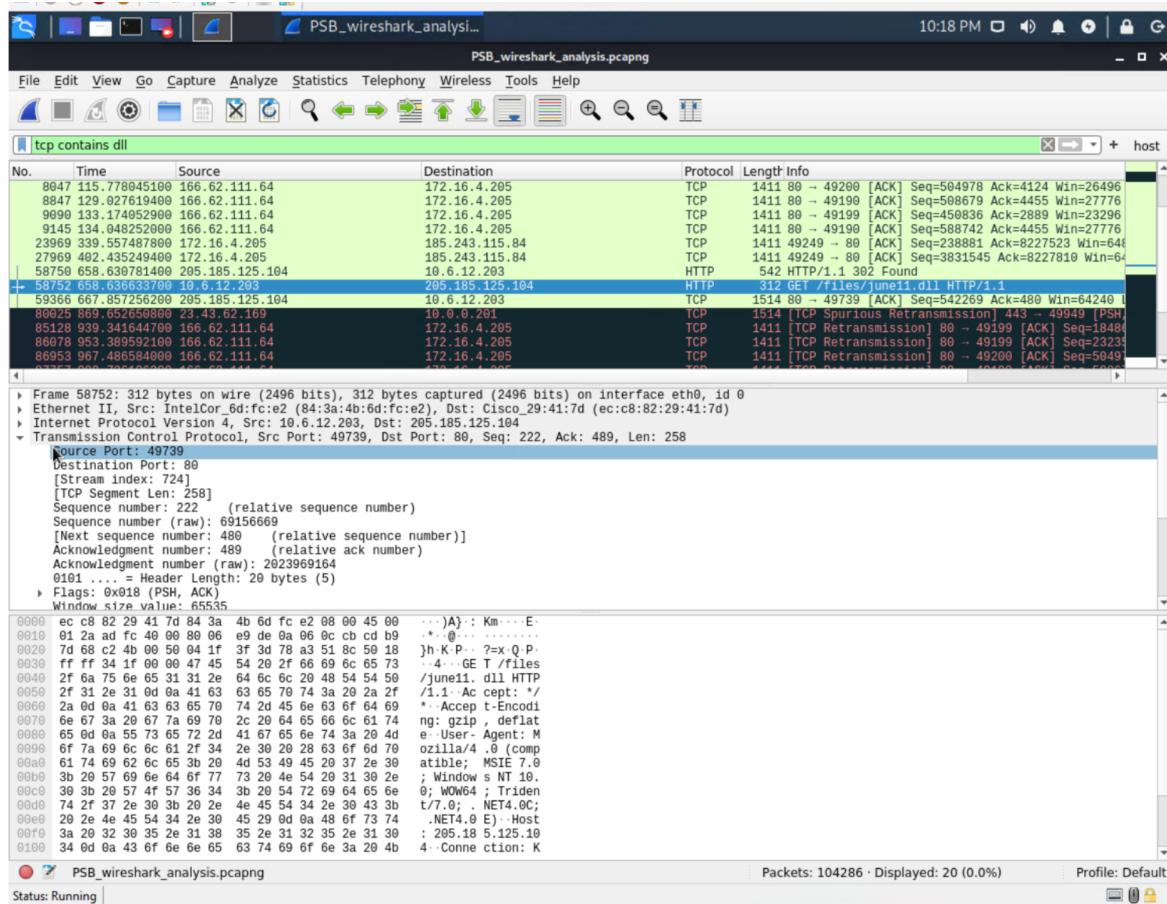
Wireshark BLANCQDESKTOP.png



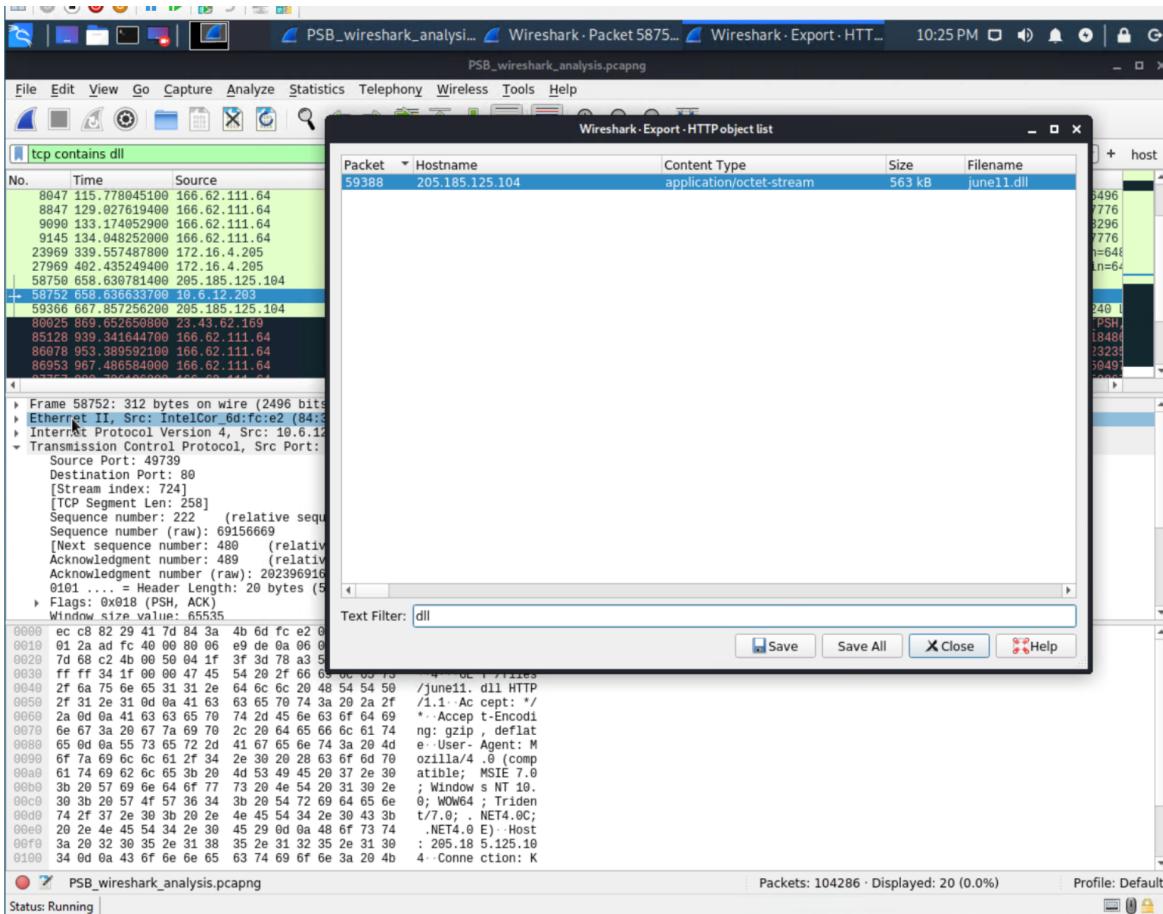
Wireshark_bittorrent1.png



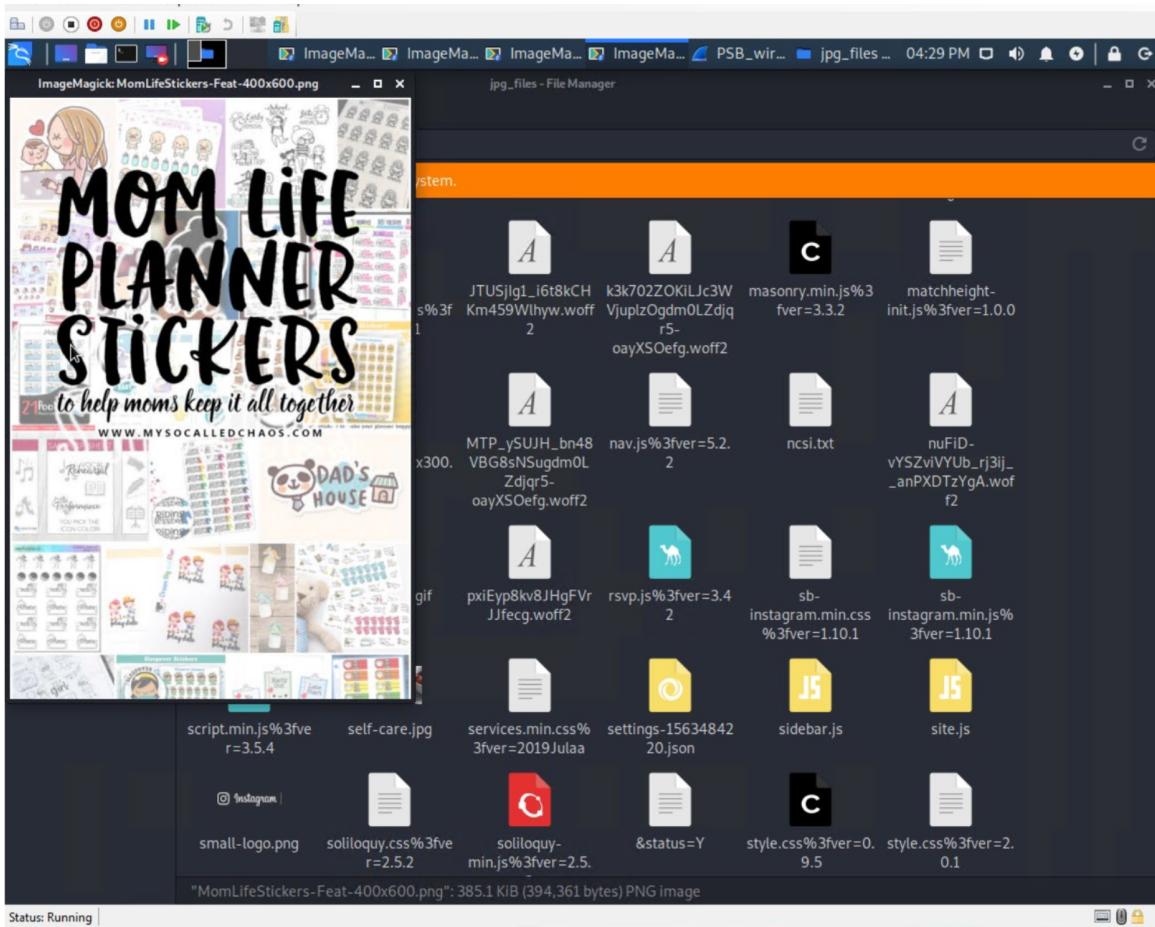
Wireshark_BLANCODESKTOP.png



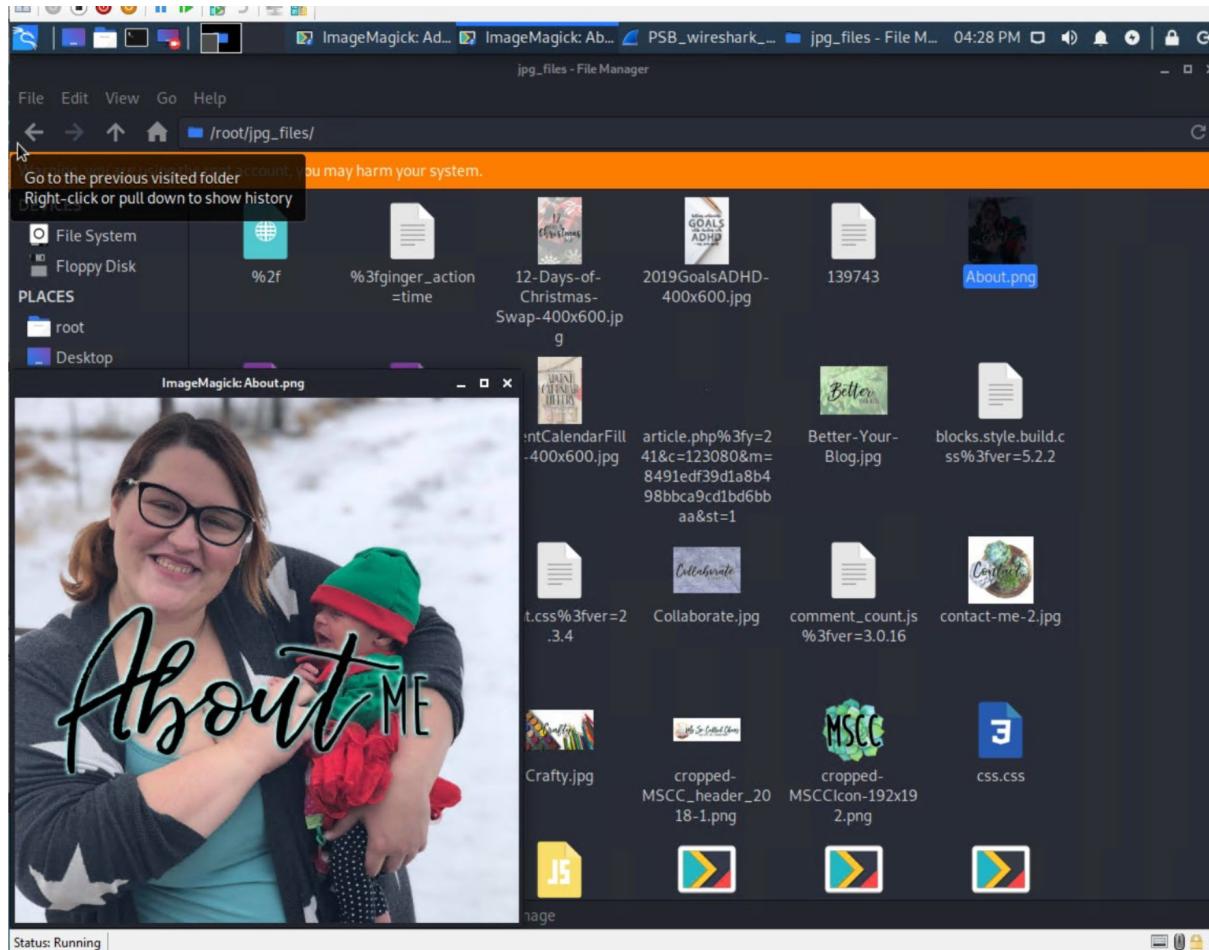
Wireshark_dll_file_to_test1



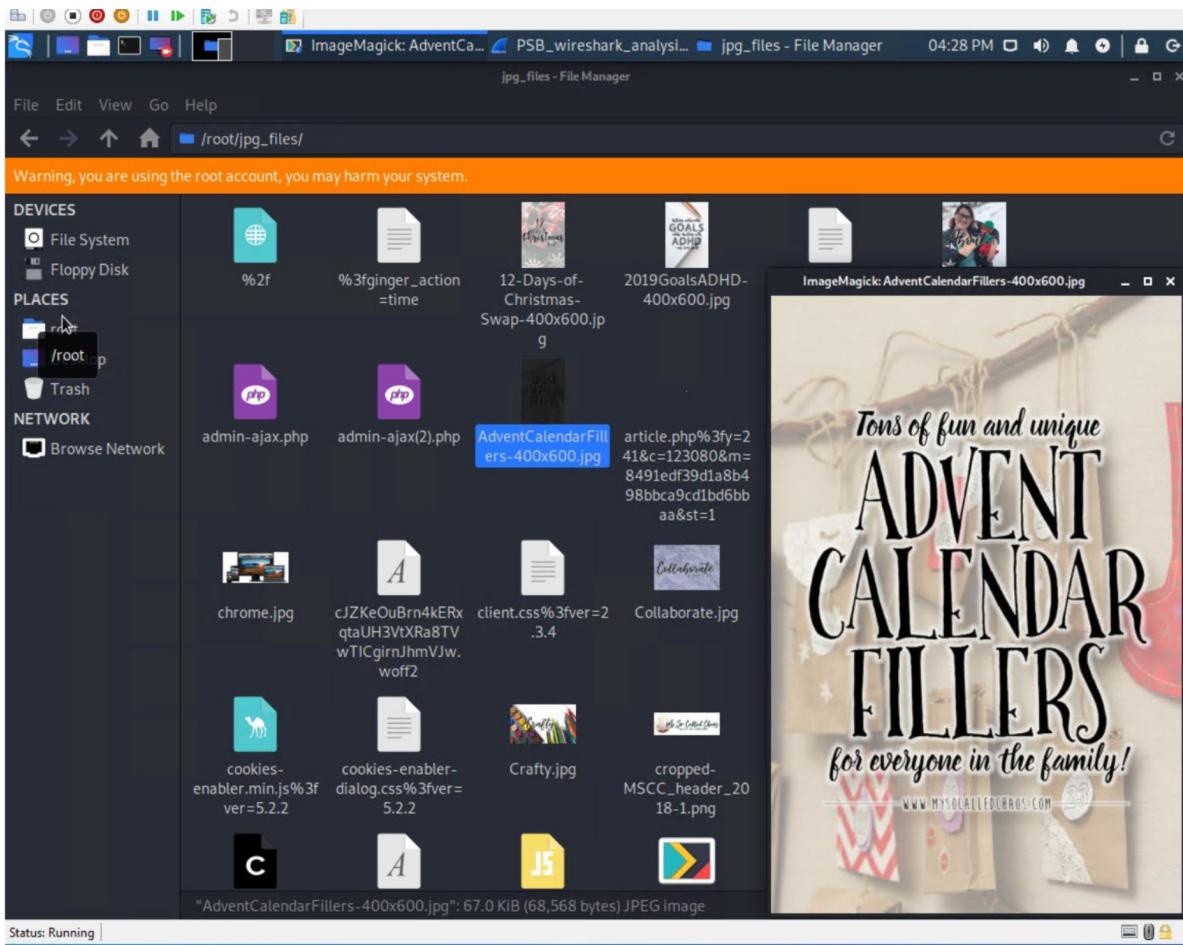
Wireshark_dll_file_to_test2



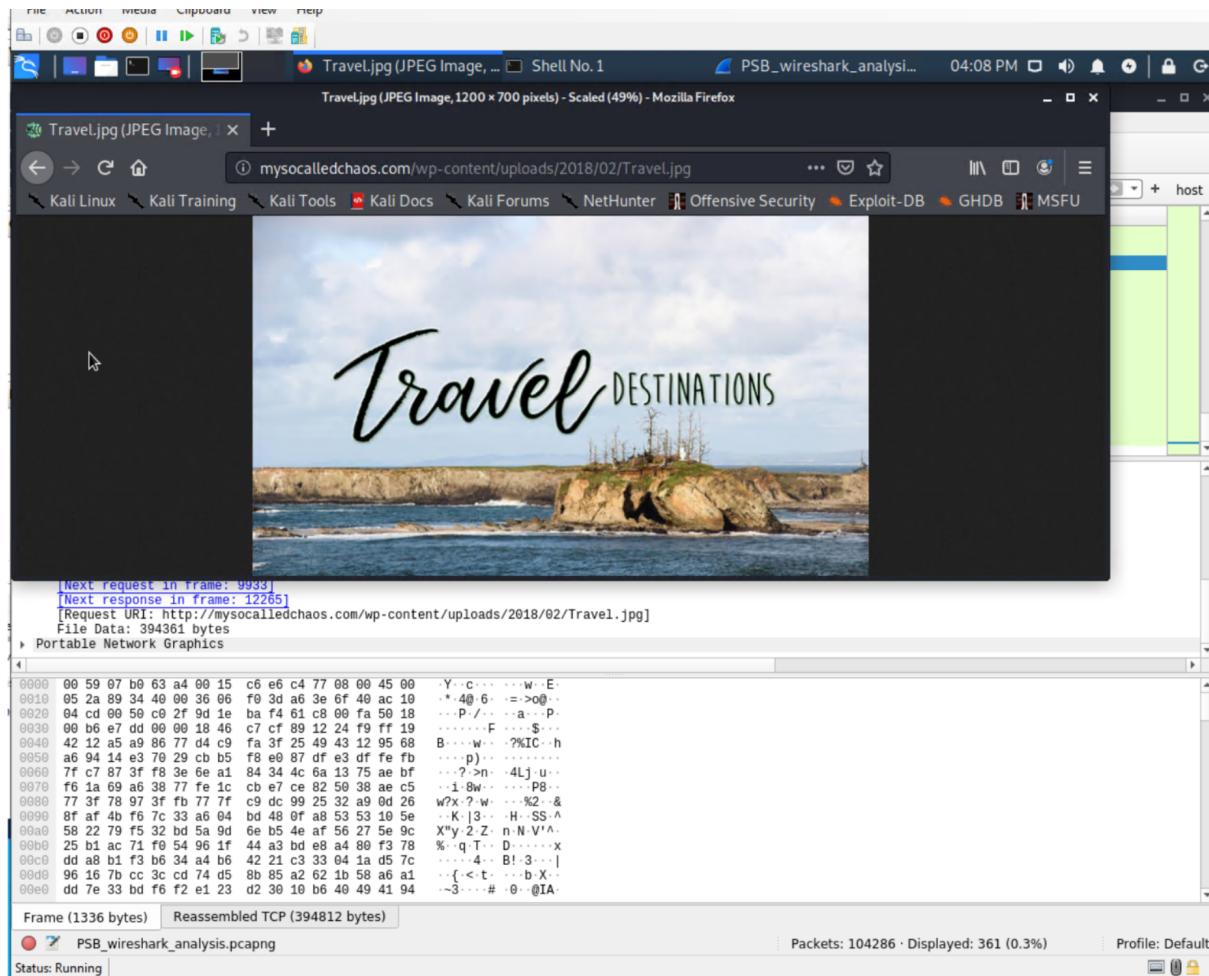
Wireshark html evidence1



Wireshark_html_evidence3



Wireshark_html_evidence4



Wireshark html evidence5



The End

Report was done by: Darrel Mills Cybersecurity Specialist

This Concludes my Report

By

Darrel Mills Cybersecurity Specialist