Today Exercise for Mr Hanis Class was Network Forensics.



Hint: it is from skr ctf(so sad, I spend so much time)

Shark Of Wire 2  
 20   
I lose my network data again... Luckily I always got a backup pcap file! Please help me find my "flag" its important!  
Flag format: SKR{flag}  
  
 Note: There were some stego and crypto elements  
 Difficulty: Medium   
Hint 1:Notice there were some image files?   
Hint 2: I got login in a website, using godam as username. But sorry I forgot the password... It also used for a zip file that I kept it somewhere...

Prerequisite : Download pcap file provided by Mr Hanis

|  |
| --- |
|  |

To make the following session interesting, Mr Hanis will Role Play as  
 Doc Hudson(chief crew)   


My Friend will roleplay as The King(former champion racer)

  
and I will roleplay as Mcqueen(champion racer) 

First, Open kali linux, launch wireshark and drag the pcap file to wireshark

A screenshot of a computer

Description automatically generated

Damn, so many messy characters!





Ok, Doc I will do it



|  |
| --- |
| Mcqueen:  Hey Doc, what can I do? Like turning left to go right? |



|  |
| --- |
| Doc Hudson:  Hey Kid, remember in network forensics proctocol is the number one rule (ICMP,TCP/IP, HTTP,HTTPS). Here is some strategy for you. |
| 1)analyze,follow, tcp or anything stream |
| 2)statistics, proctocol hierachy |
| 3) go to filter area, search ftp or http, if it is green, it is available |
| 4) If it is images/data how you extract?  ans:Go to file, export object,http,save all |



|  |
| --- |
| Mcqueen:  Kachow, time to prove I am speed. |
| Mcqueen:  Hey, doc how simple is this flag. |



|  |
| --- |
| Doc:  Hahaha kid, you are still too naïve.    First, go to exports objects -> http -> save all |



|  |
| --- |
| Mcqueen:  Then what? Which file I should start with? |



|  |
| --- |
| The King(Strip Weathers):  Yo Kid, How about start with that Malaysia Flag jpg file? And try to binwalk it |



|  |
| --- |
| Mcqueen:    Ok, I saw a hidden zip file. How to extract it? After some reading from stack over flow.  I got this!    Then, I unzip it |



|  |
| --- |
| Mcqueen:  Hey King, what is the password. |



|  |
| --- |
| The King(Strip Weathers):  Yo Kid, Look closely at the hint 2.  A screenshot of a computer  Description automatically generated |



|  |
| --- |
| Mcqueen:    Ok, I just got a mystery\_letter.jpg now what? |



|  |
| --- |
| Hey Son, have you ever tried the almighty all knowing 345 cubic inch V8 engine(Chatgpt)?  Try to ask. |



|  |
| --- |
| Mcqueen:    Shark Of Wire 2  20  I lose my network data again... Luckily I always got a backup pcap file! Please help me find my "flag" its important!  Flag format: SKR{flag}  Note: There were some stego and crypto elements  Difficulty: Medium  Hint 1:Notice there were some image files?  Hint 2: I got login in a website, using godam as username. But sorry I forgot the password... It also used for a zip file that I kept it somewhere...  Steps I gone through:  1) Downloaded network\_data.pcap file  2) Open and anlyze with wireshark  3) Extracted objects from wireshark.  4) found some files which include flag.html, s3cr3t\_fl4g.jpg  5) use binwalk s3cr3t\_fl4g.jpg, found hidden zip file.  6) extract the hidden zip file with binwalk -e s3cr3t\_fl4g.jpg ,then unzip the zip file with password found in flag.html which is password123  7) Saw a image which is mystery\_lettery.jpg, someone tell me it is about steganography  8) Got stucked,and ask chatgpt |



|  |
| --- |
| **Use Steghide**: You can try using steghide to extract hidden data from mystery\_letter.jpg. Since you mentioned the passphrase was an issue earlier, here’s how you can proceed:  bash  Copy code  steghide extract -sf mystery\_letter.jpg -p password123 |



|  |
| --- |
| Mcqueen:  You liars, this does not work at all. |



|  |
| --- |
| The King:  Open Your eyes and try to read from the mystery\_letter, You will feel the power of rotary engine. |



|  |
| --- |
| Mcqueen: The above message is about “steghide is a steganography program that is able to data in various kinds of”  Vroom, can’t read the others!!!!!  As I remember I won piston cup(first blood) and received the forbidden fuel    Hmm, It is time to use the forbidden fuel(OSINT) for extra power!  I am SPEED!!! |



|  |
| --- |
| Mcqueen:  The words in the mystery\_letter is actually from <https://library.mosse-institute.com/articles/2022/07/steghide-hiding-data-in-plain-sight/steghide-hiding-data-in-plain-sight.html>  Now I provide the full paragraph to 345 cubic inch hemi engine(chatgpt), “Steghide is a steganography program that is able to hide data in various kinds of image and audio files. The color respectively sample-frequencies are not changed thus making the embedding resistant against first-order statistical tests. “  And ask the almightly engine to identify the below text and I get “Cuffjbeq vf U4px3e5g3t”  Which is “Phssword is H4ck3r5t3g” |