Kerjakan secara seksama dan detail

Lihatlah pada folder “bahan” dan lakukan file carving pada file-file tersebut, alat-alat yang digunakan bebas, eksplore secara mandiri

Jawaban harus berupa screenshoot pembuktian dan penjelasannya

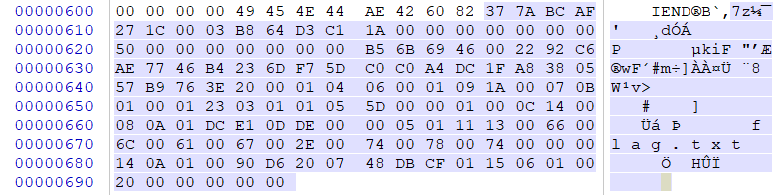
Kumpulkan sebelum jam 17:00 WIB ke email [**wahyuadi@ittelkom-pwt.ac.id**](mailto:wahyuadi@ittelkom-pwt.ac.id)

**Dengan subject UTS\_DigitalForensik\_Kelas(tuliskan kelas anda)**

Jawablah soal berikut

1. Di dalam file barcode.png terdapat file lain, temukan file tersebut dan apa isi file tersebut?

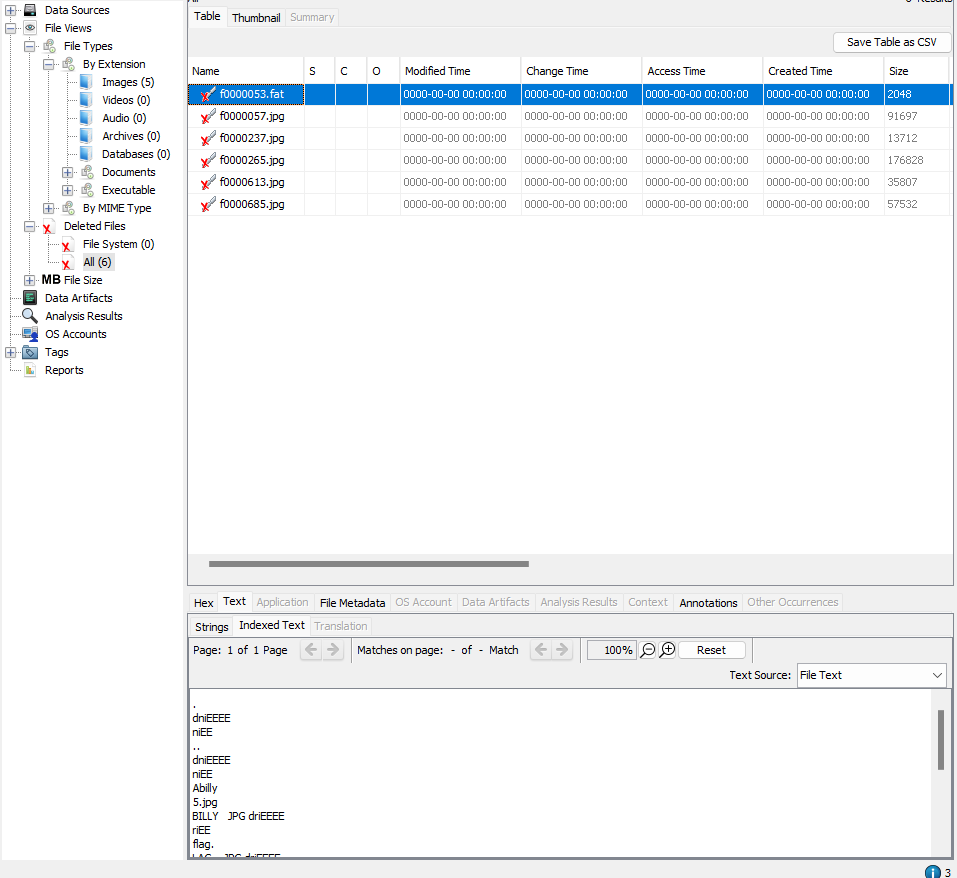
Jawab :



File tersebut merupakan file berformat Zip, yang didalamnya terdapat file lagi berformat TXT. Didalam file TXT tersebut berisi sebuah string yaitu **EKSi7MktjOpvwesurw0v**

1. Didalam file disk.img terdapat file yang rusak. Anda harus menemukan file tersebut

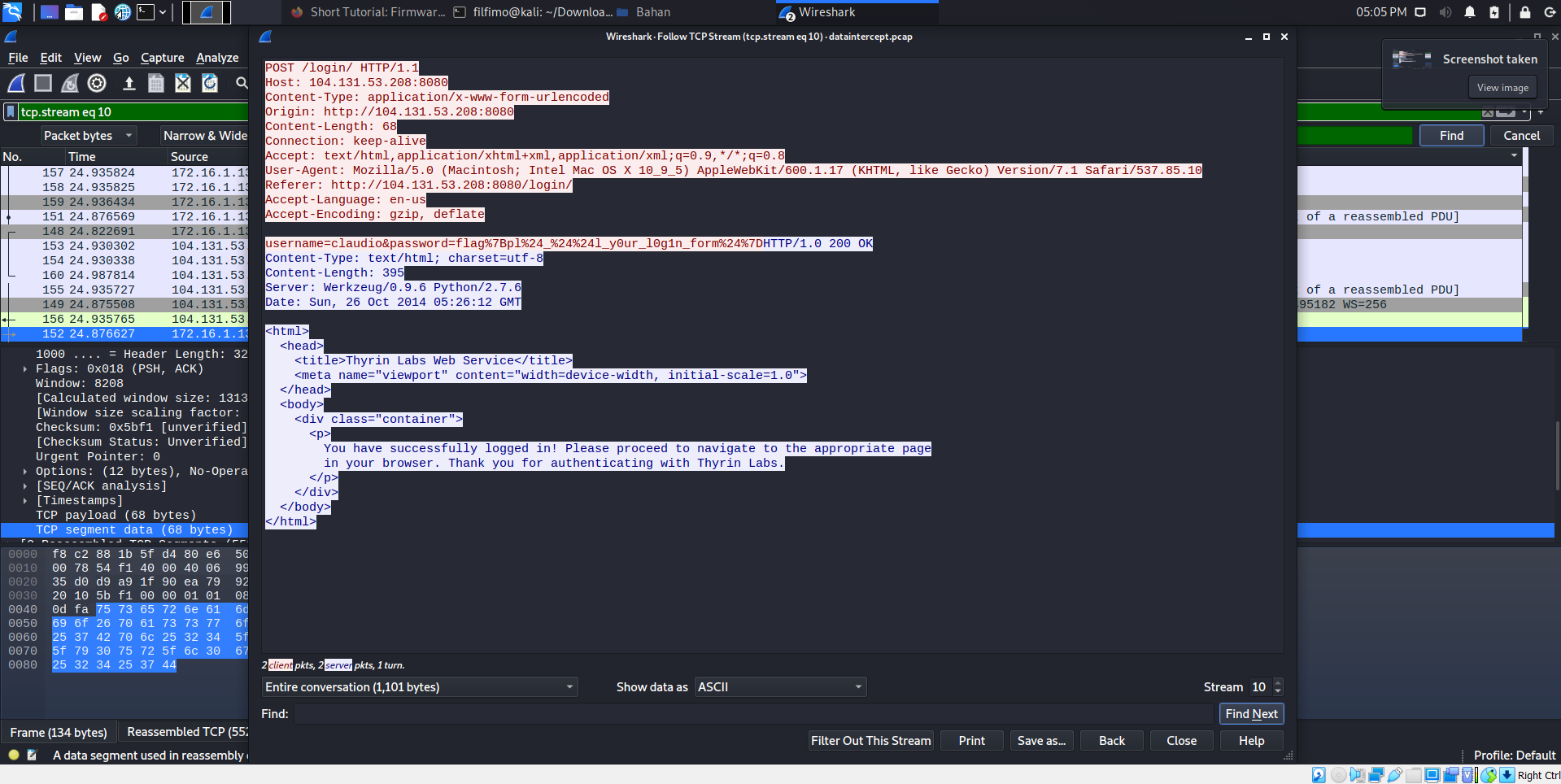
Jawab :



Di dalam file disk.img terdapat 6 file yang terbaca pada Autopsy

1. *f*0000053.fat, file inilah yang tidak dapat dibuka oleh Autopsy.
2. *f*0000057.jpg, file ini dapat dibuka oleh Autopsy dan berupa gambar dua ekor kucing.
3. *f*0000237.jpg, file ini dapat dibuka oleh Autopsy dan berupa gambar bertuliskan *flag: i\_can\_has\_cheezburger*.
4. *f*0000265.jpg, file ini dapat dibuka oleh Autopsy dan berupa gambar seekor anak kucing abu-abu.
5. *f*0000613.jpg, file ini dapat dibuka oleh Autopsy dan berupa gambar seekor kucing dengan kalimat “pew pew pew”.
6. *f*0000685.jpg, file ini dapat dibuka oleh Autopsy dan berupa gambar seekor kucing sedang memiringkan kepalanya.
7. Didalam file dataintercept.pcap terdapat password, temukan password tersebut (jangan terjebak dengan apa yang kalian lihat, temukan passwordnya dan gunakan <https://r12a.github.io/app-conversion/> sebagai unicodenya

Jawab :



**username=claudio&password=flag%7Bpl%24\_%24%24l\_y0ur\_l0g1n\_form%24%7D**

Dari line diatas diketahui bahwa **claudio** merupakan*username*. Kemudian untuk *password* dikarenakan membuka *POST Request* dengan mengikuti *TCP Stream* maka *password* dapat dilihat seperti diatas. **flag%7Bpl%24\_%24%24l\_y0ur\_l0g1n\_form%24%7D** merupakan *password* yang telah diisi, dikarenakan ini didalam *web traffic*, *password* di *encoded* menggunakan UTF-8, kemudia dilakukanlah konversi, sehingga diperoleh **pl$\_$$l\_y0ur\_l0g1n\_form$**.

1. File Kucing .jpg merupakan file termodifikasi temukan informasi yang ada didalamnya gunakan <https://www.base64decode.org> untuk mengesktrak datanya.

Jawab :



Ditemukan sebuah *resource* didalam file Kucing .jpg, yaitu **cGljb0NURnt0aGVfbTN0YWRhdGFfMXNfbW9kaWZpZWR9**, dan jika di konversi akan didapatkan hasil, seperti gambar di bawah ini :

