# Tugas Training CaKru Day 5

# Networking: OSI Layer 101 dan Wireshark

NAMA : Christian Valerioksana Laujerly Sebayang

NIM : 16523079

**Cara Menjawab:**

Pilih menu File > Make a copy, untuk dokumen ini. Isi pada kolom jawaban.

Deadline : **23 Maret 2024, pukul 23.59 WIB**

Pengumpulan: <https://forms.gle/ckqLXcd7k2p9KpCt7>

Anda diberikan sebuah captured traffic yang dapat diunduh pada link berikut:

[traffic.zip](https://drive.google.com/file/d/1xsRUL7E2vkCju_G5M1RwsDc2f56juEyP/view?usp=sharing)

Tugas anda adalah menganalisis traffic network tersebut. Sebagai problem setter yang baik, kami memberikan langkah-langkah untuk menyelesaikan tugas tersebut. Silakan menambahkan screenshot gambar untuk mendukung penjelasan.

## Tugas Day 5

### Network Protocol Filter

|  |
| --- |
| Deskripsi  File di atas berisi 2407 paket. Tidak mungkin Anda menganalisis satu per satu. Oleh karena itu, lakukanlah penyaringan protokol jaringan pada kolom yang di-highlight warna hijau. |
| Jawaban  Protokol: insert\_here  Alasan: insert\_here |

### Akun pengguna

|  |
| --- |
| Deskripsi  Tampaknya, pengguna melakukan beberapa percobaan login.  Dapatkah kamu menemukan kredensial asli pengguna? |
| Jawaban  Username: insert\_here  Password: insert\_here  Alasan: insert\_here |

### Redirect

|  |
| --- |
| Deskripsi  Apabila berhasil login, halaman/lokasi manakah yang akan dikunjungi pengguna? |
| Jawaban  Nama file atau full url: insert\_here  Alasan: insert\_here |

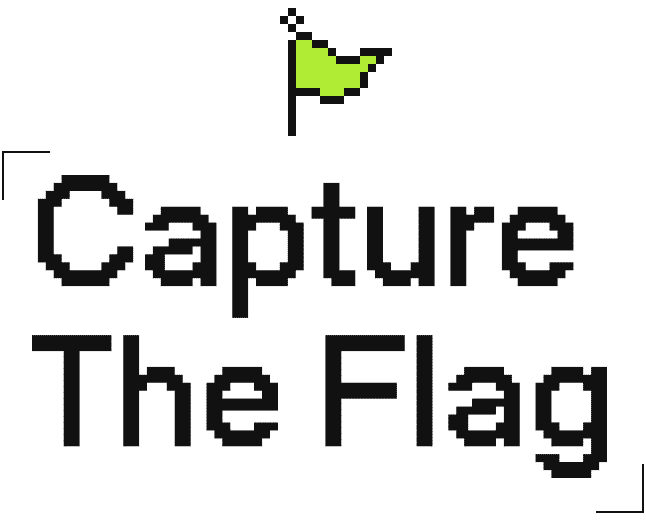
### Extract File

|  |
| --- |
| Deskripsi  Pada halaman/lokasi di jawaban pertanyaan 3, seharusnya pengguna diberikan 3 buah url. Pengguna mengklik salah satu link sehingga mengunduh suatu file. File apa yang pengguna unduh?  File yang benar adalah sebuah file yang dapat dijalankan dan memberikan suatu link. Link tersebut berisi sebuah **bendera** dengan format **FLAG{}** |
| Jawaban  Nama file: insert\_here  Flag: FLAG{insert\_here}  Alasan: insert\_here |

### Summary

|  |
| --- |
| Deskripsi  Jelaskan cara kerja web yang pengguna akses dan  pengetahuan apa yang Anda dapatkan setelah mengerjakan tugas menggunakan Wireshark? |
| Jawaban  Cara kerja web:  Web di atas sepertinya memiliki N buah halaman, yaitu.  Halaman utama adalah …  Mekanisme login adalah …  …  …  …  Wireshark:  Wireshark keren banget, Terima kasih Wireshark. |

## BONUS



Mungkin ada yang enjoy ngerjainnya. Jadi, kami menyiapkan soal BONUS, maksimal +15 poin.

Anda diberikan sebuah captured traffic yang dapat diunduh pada link berikut:

[bonus\_day5.zip](https://drive.google.com/file/d/12upVc5jn730CPkXYQ0C9IYeLP8ydn8t1/view?usp=sharing)

Tugas anda adalah mendapatkan **FLAG** pada paket dengan format . Sebagai problem setter yang baik, kami memberikan langkah-langkah untuk menyelesaikan tugas tersebut.

1. Identifikasi ekstensi file bendera dengan pencocokan hex signature.

Referensi: [List of file signatures - Wikipedia](https://en.wikipedia.org/wiki/List_of_file_signatures)

1. Lakukan filter dengan command berikut.

data.data contains "ext123"

1. Extract setiap paket yang mengandung bendera
2. Langkah-langkah yang Anda lakukan dapat dirangkum dalam kolom di bawah

### Story telling aja jawabnya dan kalo bisa tambahkan screenshot gambar yang mendukung.

Contoh writeup: [Writeup-Netcomp CTF UGM.pdf](https://drive.google.com/file/d/11WJGl7-rJahpwo38uMZ5FJL1CE8xV4ro/view?usp=sharing)

|  |
| --- |
| Jawaban |