

LAPORAN RESMI
PRAKTIKUM KEAMANAN JARINGAN
DATA MINING



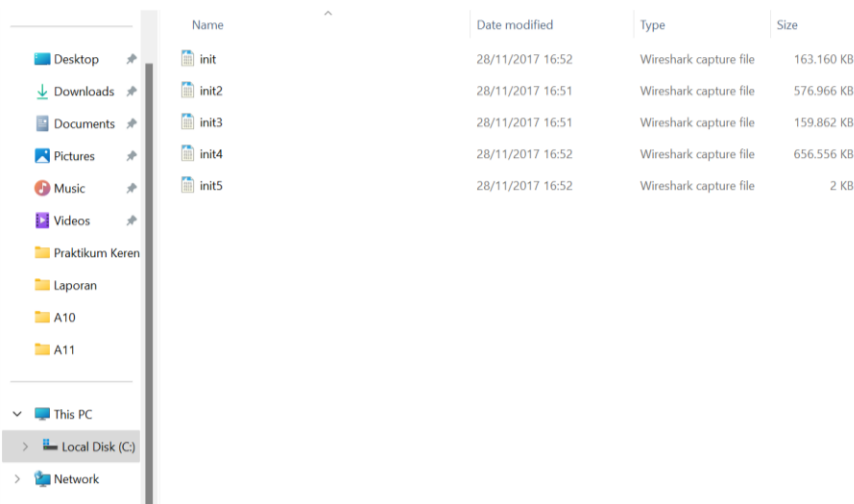
Oleh :

Tarisa Dinda Deliyanti 3122640037

D4 LJ Teknik Informatika B

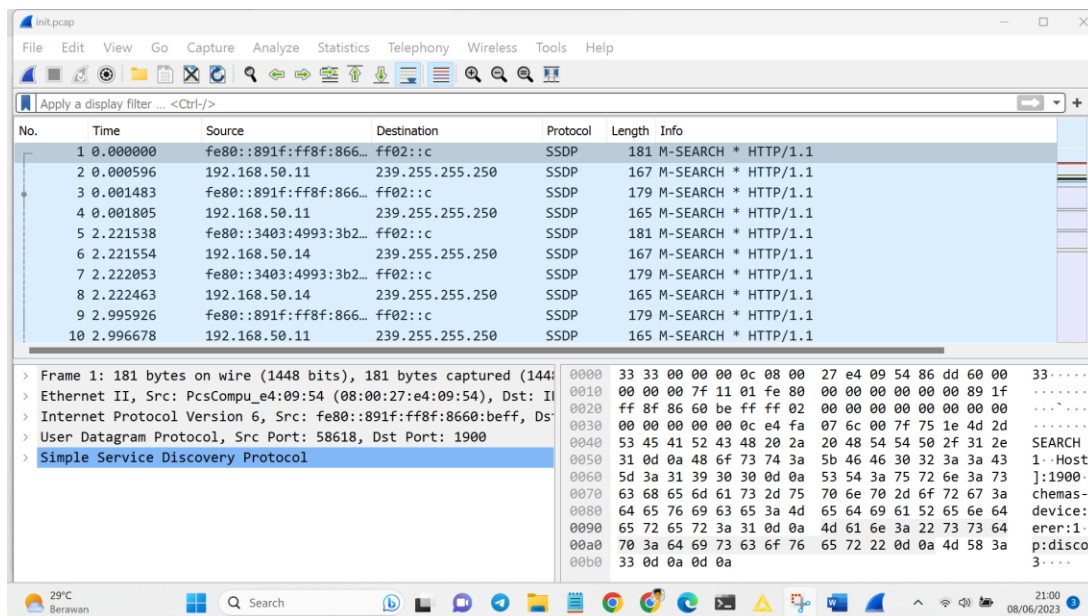
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
TAHUN AJARAN 2022/2023

1. Bagi file menjadi lima bagian : init.pcap, init2.pcap, init3.pcap, init4.pcap, init5.pcap



Name	Date modified	Type	Size
init	28/11/2017 16:52	Wireshark capture file	163.160 KB
init2	28/11/2017 16:51	Wireshark capture file	576.966 KB
init3	28/11/2017 16:51	Wireshark capture file	159.862 KB
init4	28/11/2017 16:52	Wireshark capture file	656.556 KB
init5	28/11/2017 16:52	Wireshark capture file	2 KB

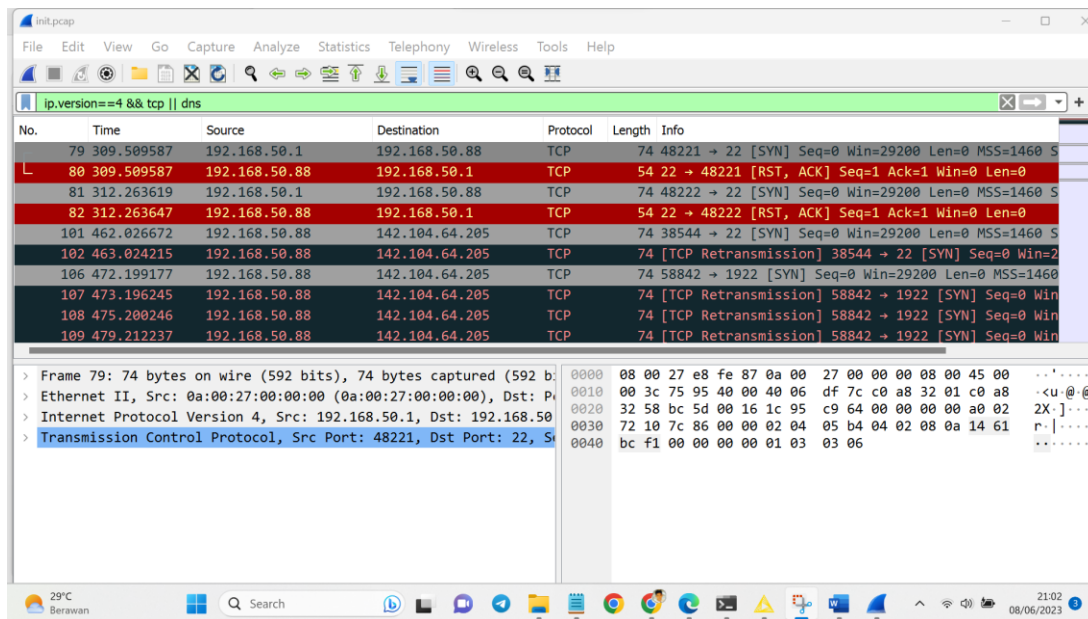
2. Kemudian buka file tersebut secara bergantian menggunakan Wireshark. Pada langkah ini kita gunakan file init.pcap



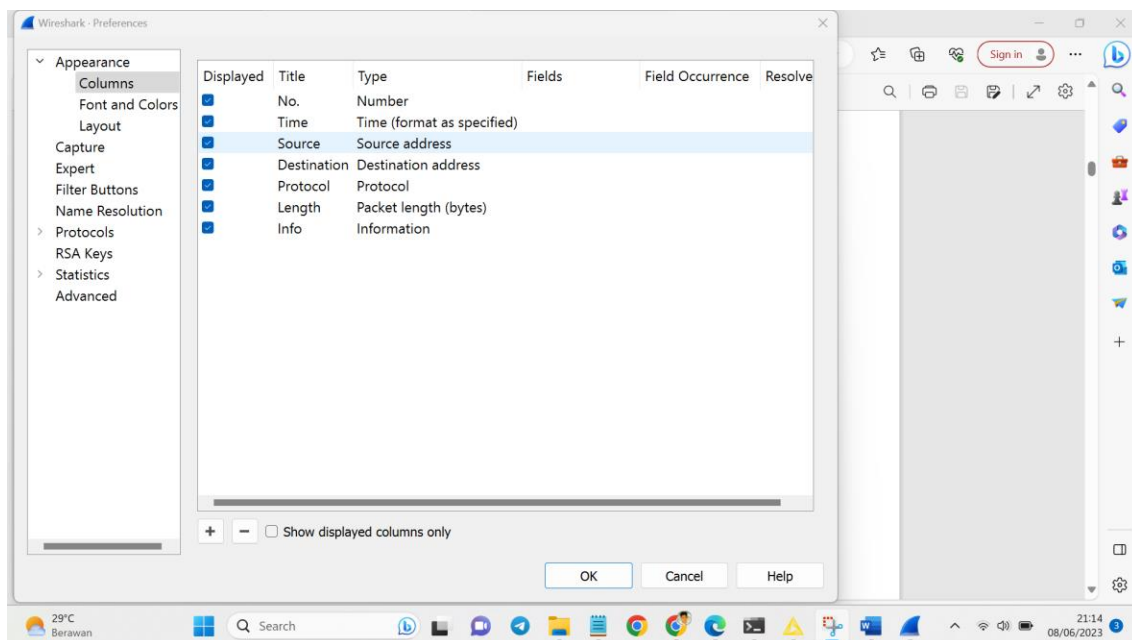
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::891f:ff8f:866...	ff02::c	SSDP	181	M-SEARCH * HTTP/1.1
2	0.000596	192.168.50.11	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
3	0.001483	fe80::891f:ff8f:866...	ff02::c	SSDP	179	M-SEARCH * HTTP/1.1
4	0.001805	192.168.50.11	239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1
5	2.221538	fe80::3403:4993:3b2...	ff02::c	SSDP	181	M-SEARCH * HTTP/1.1
6	2.221554	192.168.50.14	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
7	2.222053	fe80::3403:4993:3b2...	ff02::c	SSDP	179	M-SEARCH * HTTP/1.1
8	2.222463	192.168.50.14	239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1
9	2.995926	fe80::891f:ff8f:866...	ff02::c	SSDP	179	M-SEARCH * HTTP/1.1
10	2.996678	192.168.50.11	239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1

Frame 1: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface 0
Ethernet II, Src: PcsCompu_e4:09:54 (08:00:27:e4:09:54), Dst: ff02::c
Internet Protocol Version 6, Src: fe80::891f:ff8f:8660:beff, Dst: ff02::c
User Datagram Protocol, Src Port: 58618, Dst Port: 1900
Simple Service Discovery Protocol

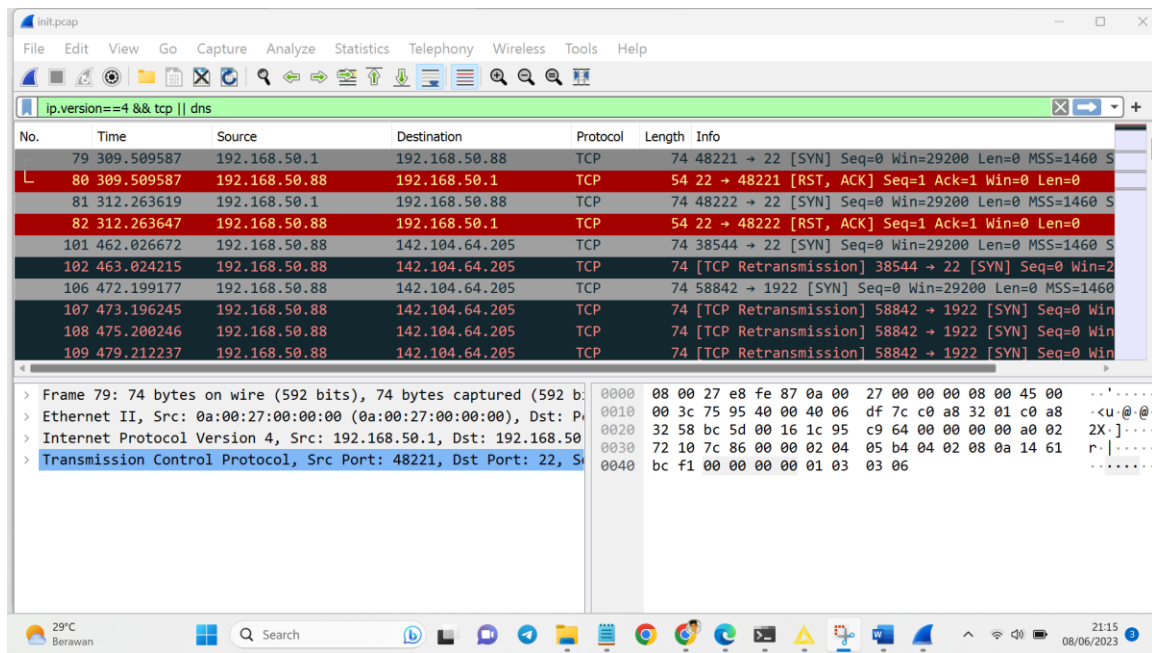
3. Untuk proses analisa yang akan dilakukan nantinya, kita akan mengambil data dengan ip versi 4 (ipv4) dan protocol TCP, DNS saja. Untuk proses tersebut dapat dilakukan pada wireshark menggunakan perintah `ip.version == 4 && tcp || dns` pada kolom display filter tepat dibawah toolbar.



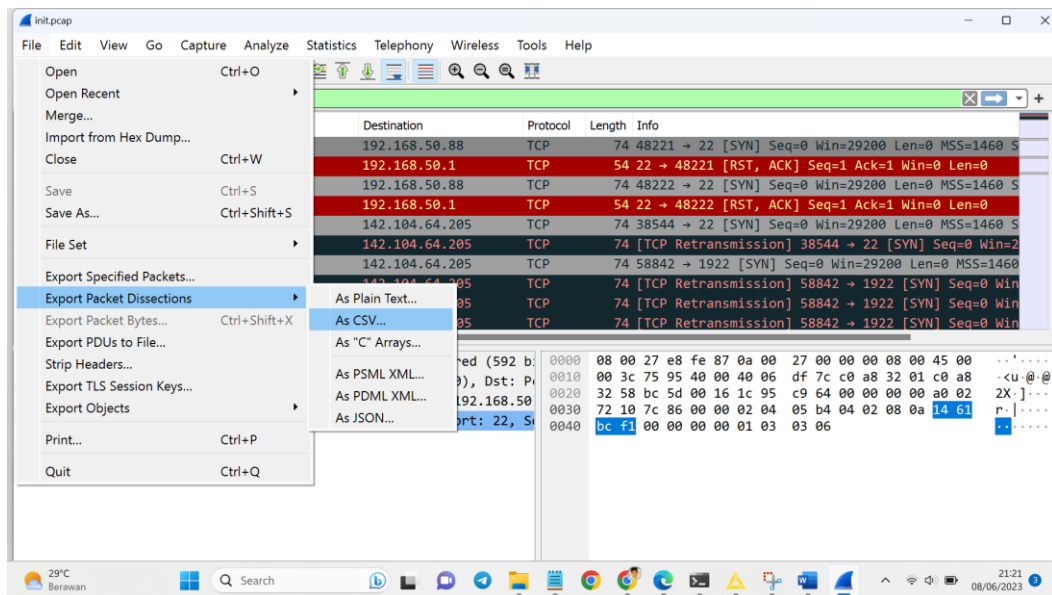
4. Untuk mendapatkan delta time dan delta time dan delta time display, klik Edit – Preferences – Column



Hasilnya

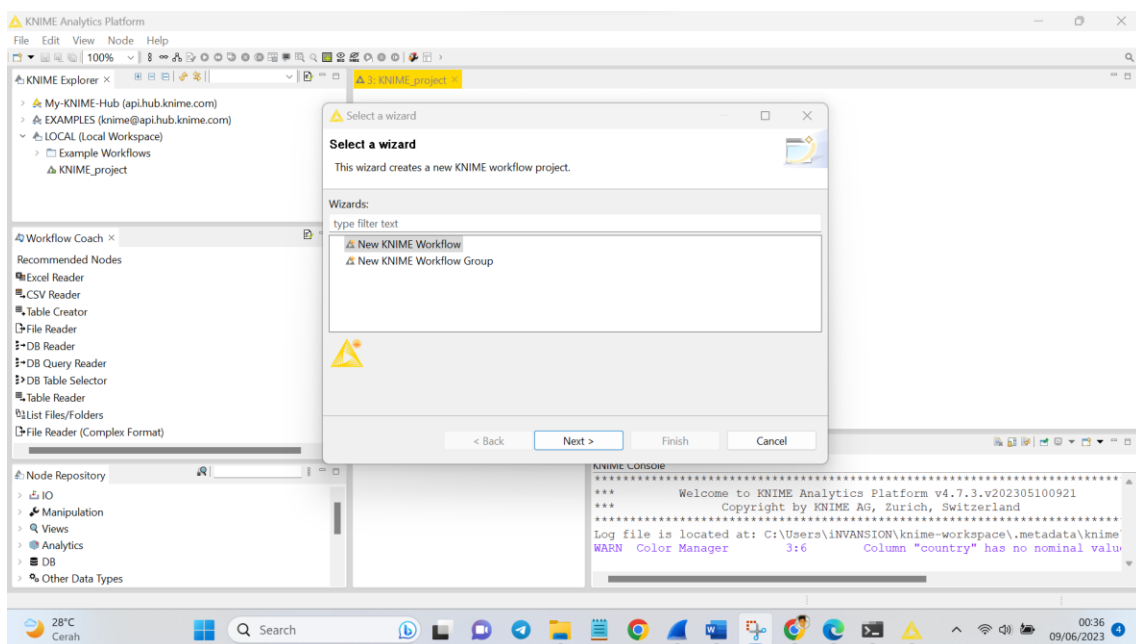


5. Export file pcap tersebut terformat Comma-separated Value (.csv) dengan cara klik File – Export Packet Dissections – As CSV. Yang perlu diperhatikan yaitu pada Pacet Range, pastikan yang terpilih yaitu Displayed, karena data pada Displayed ini sudah terfilter dengan ip version 4.

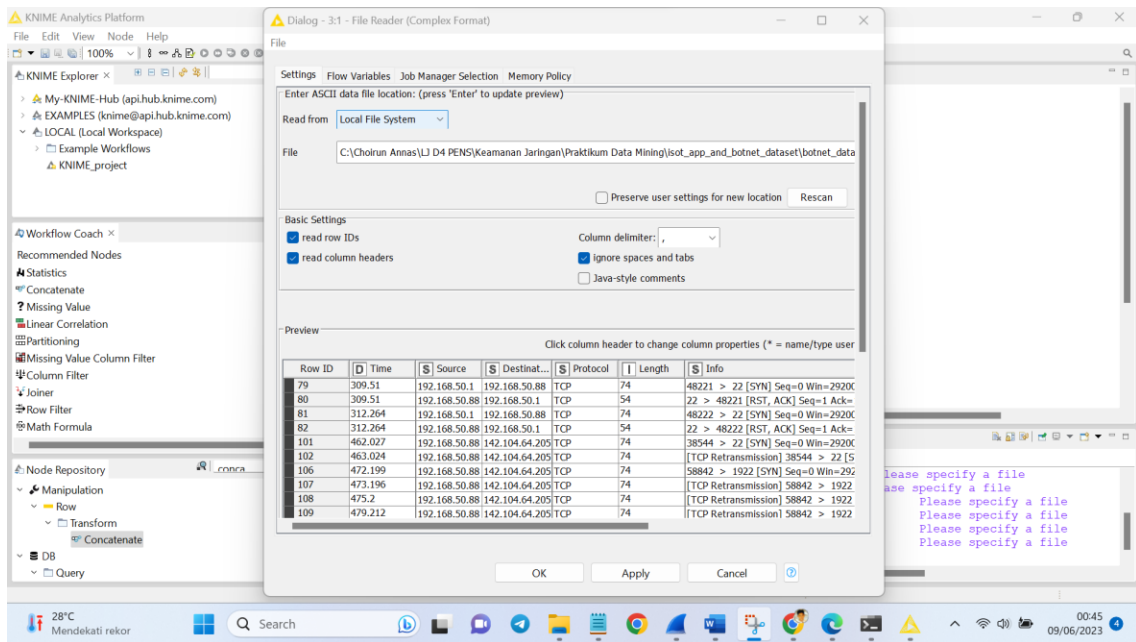


	Name	Date modified	Type	Size
Desktop	init	08/06/2023 23:42	Microsoft Excel Com...	43.481 KB
Downloads	init	28/11/2017 16:52	Wireshark capture file	163.160 KB
Documents	init2	08/06/2023 23:48	Microsoft Excel Com...	43.481 KB
Pictures	init2	28/11/2017 16:51	Wireshark capture file	576.966 KB
Music	init3	08/06/2023 23:51	Microsoft Excel Com...	149.525 KB
Videos	init3	28/11/2017 16:51	Wireshark capture file	159.862 KB
Praktikum Ke	init4	09/06/2023 00:02	Microsoft Excel Com...	354.000 KB
Laporan	init4	28/11/2017 16:52	Wireshark capture file	656.556 KB
Praktikum Da	init5	09/06/2023 00:25	Microsoft Excel Com...	1 KB
botnet_data	init5	28/11/2017 16:52	Wireshark capture file	2 KB

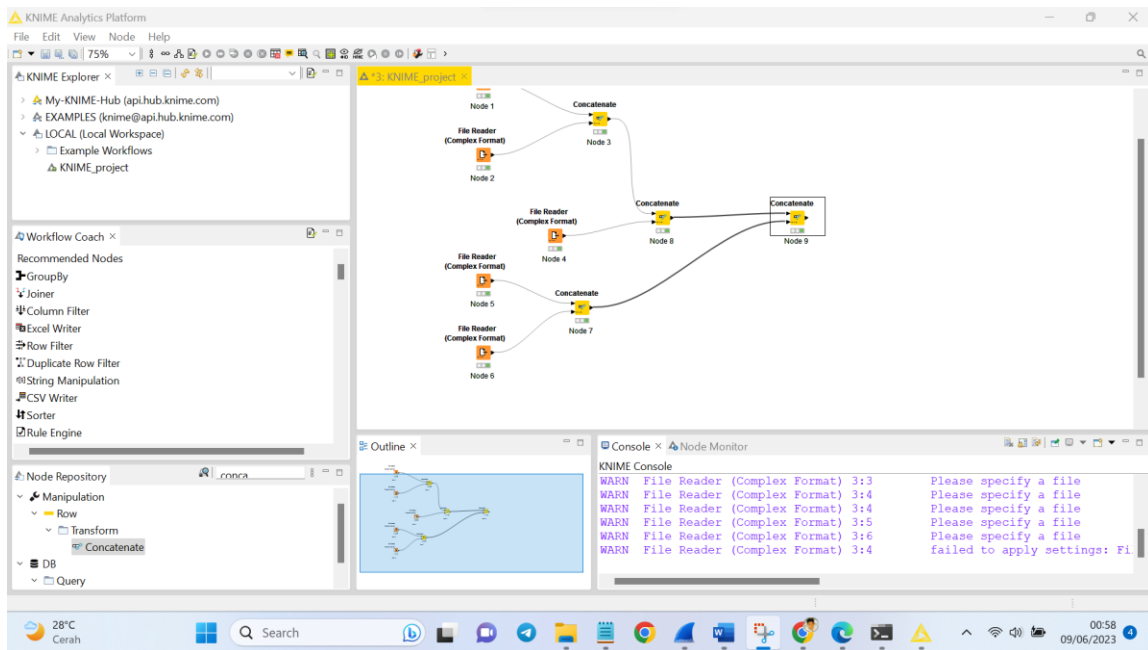
6. Membuat workflow/project baru. Dengan cara klik File – New – New Knime Workflow – Tulis Nama workflow dan Lokasi workflow tersebut – Klik Finish



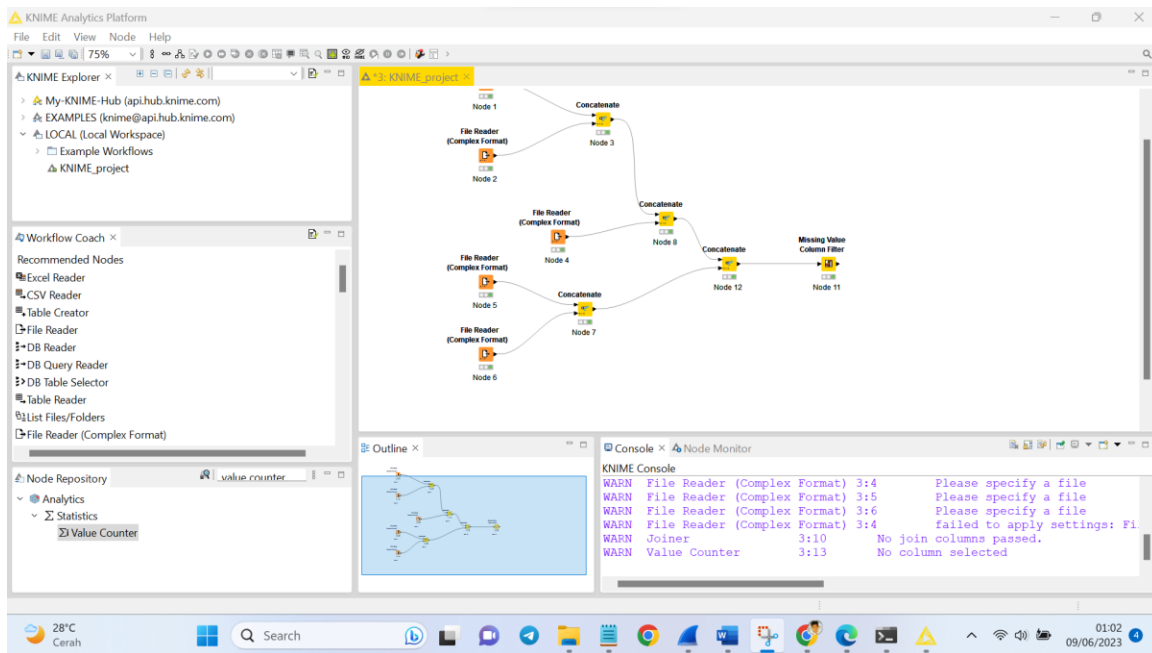
7. Tambahkan data ke dalam file reader



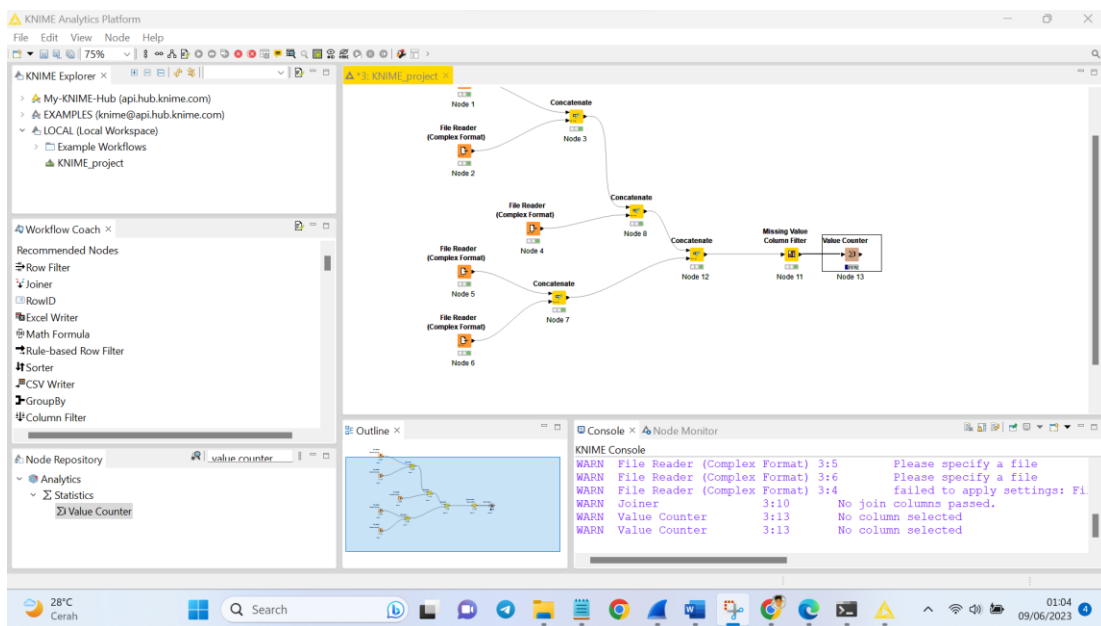
8. Gabungkan kelima data dengan menggunakan concatenate dan data reader seperti gambar di bawah



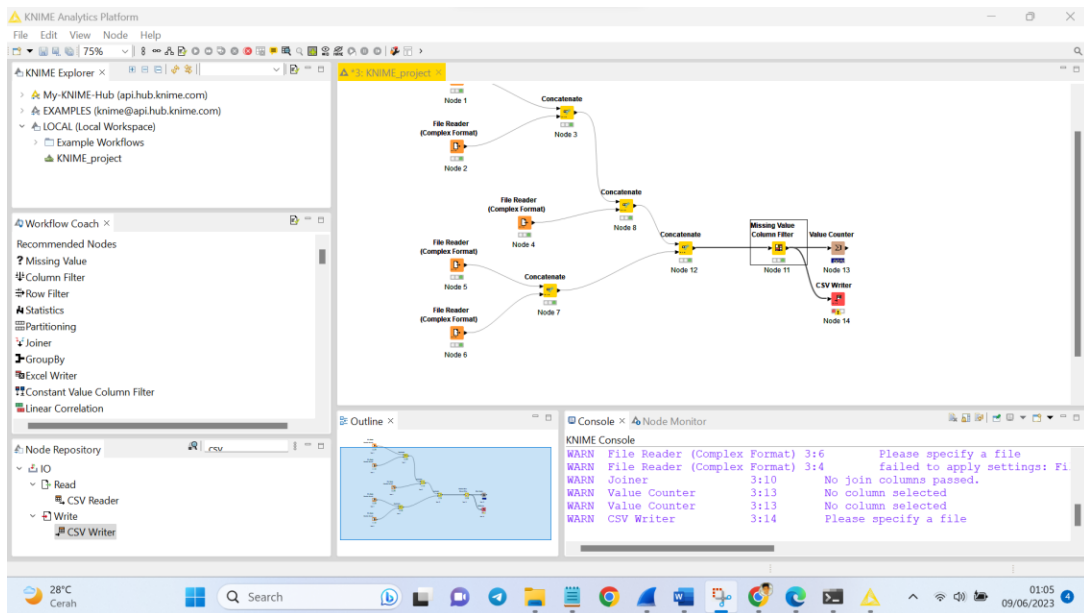
9. Untuk melakukan labeling data normal kita akan menggunakan Node Missing Value. Node ini digunakan untuk mengisi data kosong.



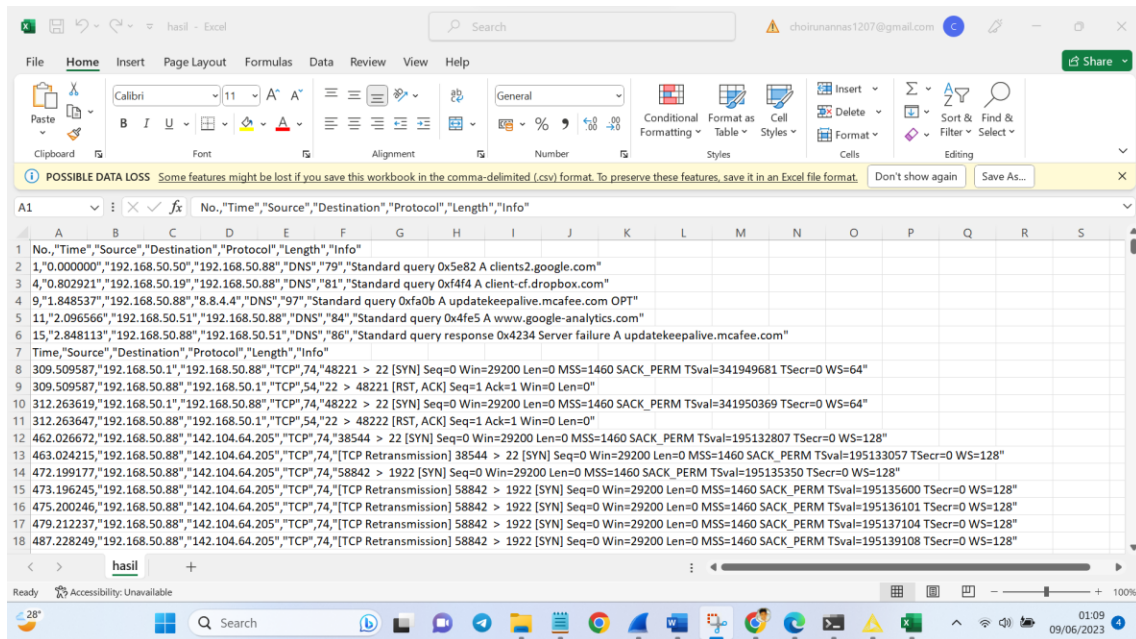
10. Untuk memastikan bahwa kolom label sudah terisi dengan value Malicious atau Normal, dapat menggunakan node Value Counter. Node ini berfungsi untuk menghitung jumlah seluruh value pada kolom terpilih.



11. Export file ke dalam format .csv dengan menggunakan node CSV Writer

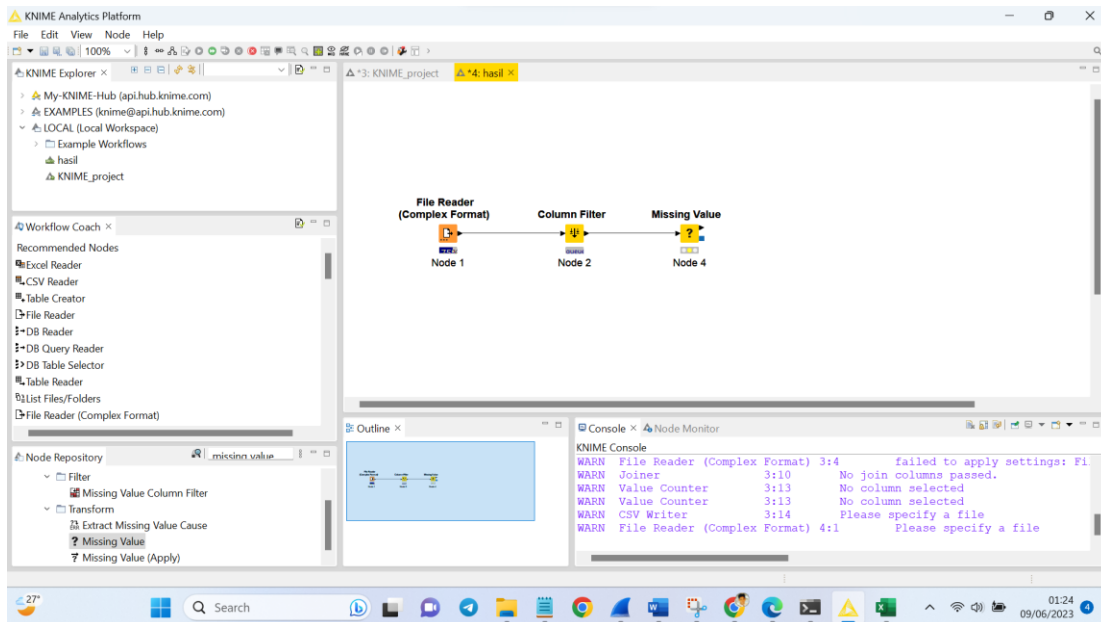


Saya menaruh data di dalam file hasil.csv

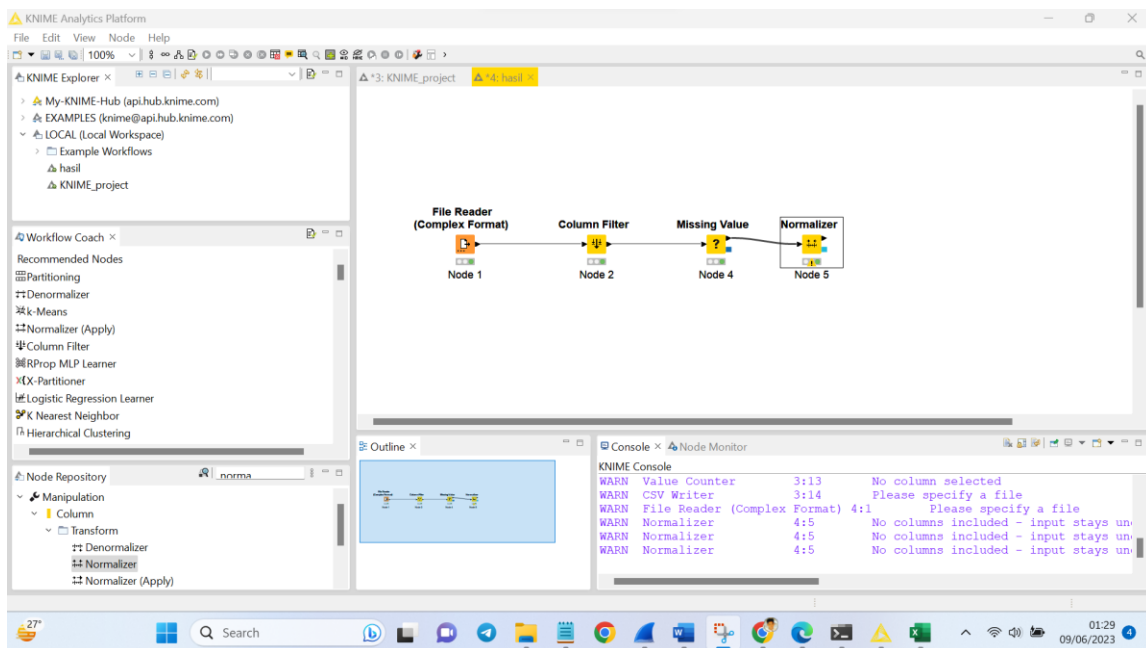


12. Data Pre Processing

Proses di mana data akan dibersihkan (cleaning) karena biasanya didalam suatu data terdapat nilai-nilai yang tidak sempurna atau bahkan terdapat nilai-nilai yang hilang atau kosong yang nantinya akan dapat mempengaruhi proses kedepannya. Pada proses ini kita membutuhkan Node-node berikut : File Reader, Column Filter, Missing Value.

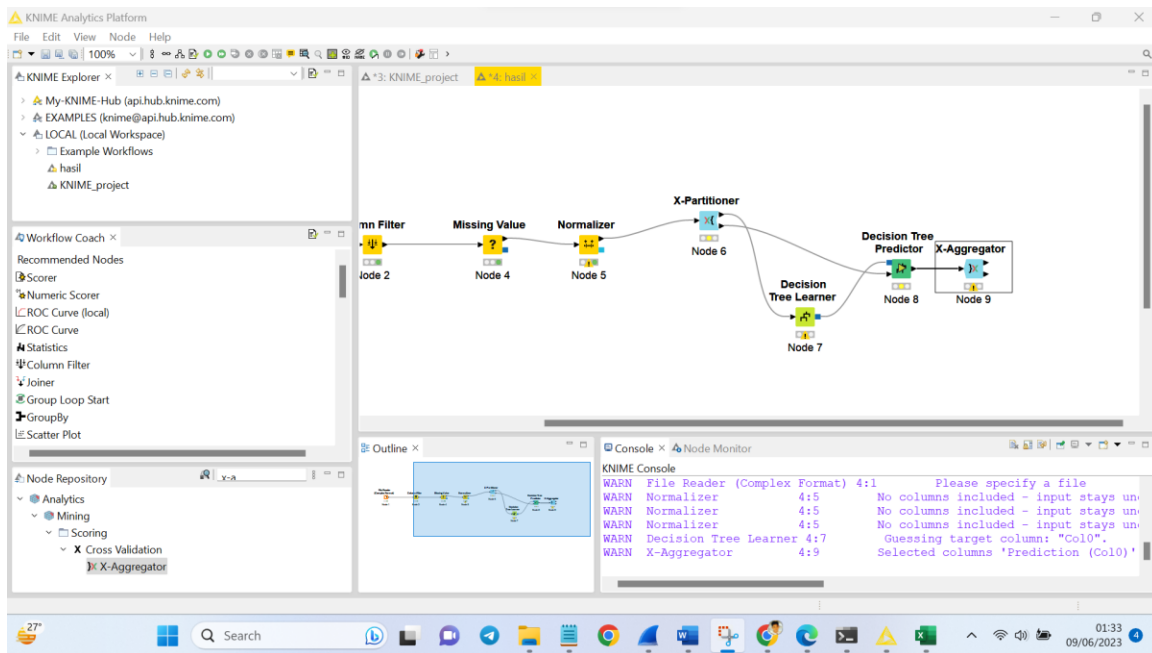


13. Proses data transformation, pada proses ini data akan diubah ke format yang sesuai untuk proses data mining. Node yang digunakan pada tahap ini yaitu Normalizer. Berikut konfigurasinya

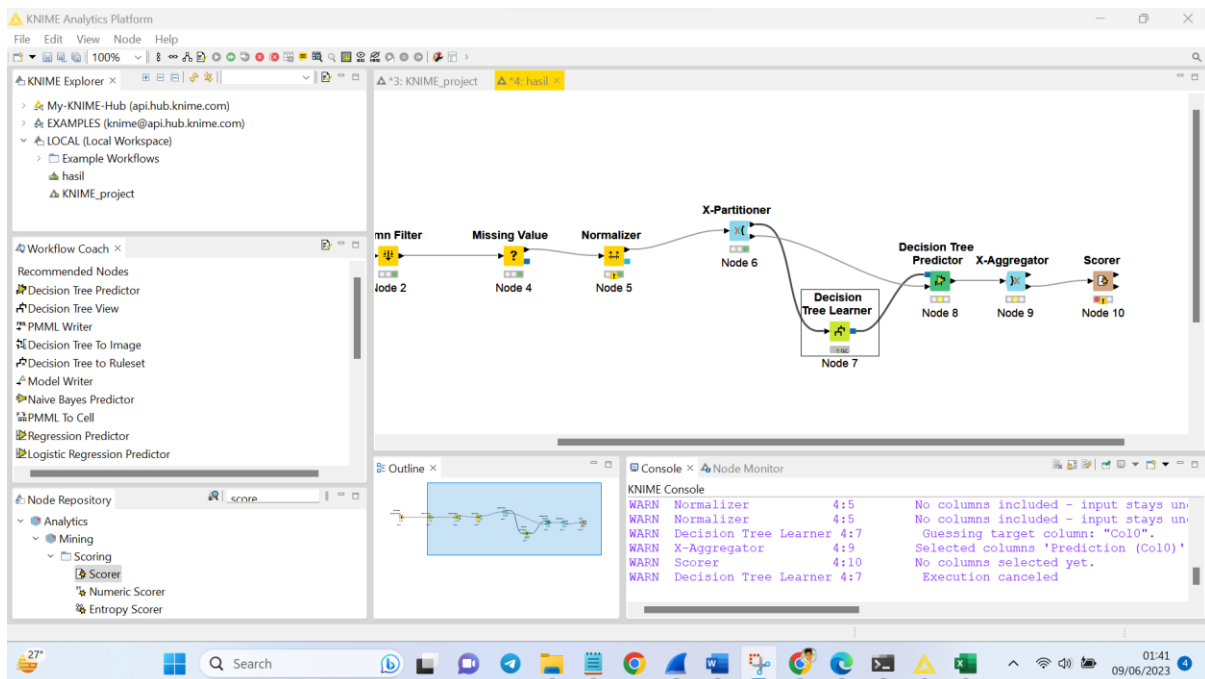


14. Data Mining

Setelah menyelesaikan tahap data transformation, kita akan menjalankan proses Data Mining, dalam proses ini kita akan menggunakan Metode Klasifikasi Decision Tree dengan teknik Cross Validation. Pada proses ini kita membutuhkan Node-node berikut : X-Partitioner, Decision Tree Learner, Decision Tree Predictor, X-Aggregator Sehingga akan membentuk flow seperti ini



15. Node Scorer yang didalamnya terdapat perhitungan untuk melihat seberapa baik model ini dengan menggunakan teknik confusion matrix. Berikut konfigurasi.



16. Hasil Prediksi

KNIME Analytics Platform

File Edit View Node Help

100%

KNIME Explorer

- My-KNIME-Hub (api.hub.knime.com)
- EXAMPLES (knime@api.hub.knime.com)
- LOCAL (Local Workspace)
 - Example Workflows
 - hasil
 - KNIME Project

Workflow Coach

Recommended Nodes

- ROC Curve
- Feature Selection Loop End
- ROC Curve (local)
- Column Filter
- Row Filter
- Excel Writer
- CSV Writer
- Numeric Scorer
- Table Row to Variable

Node Repository

- IO
- Manipulation
- Views
- Analytics
- DB
- Other Data Types

Confusion Matrix - 3:10 - Scorer

File Hilite

Size of Tes...	0	1	2
0	6	0	0
1	3	0	0
2	1	0	0

Correct classified: 6
Accuracy: 60%
Cohen's kappa (κ): 0%

Wrong classified: 4
Error: 40%

Decision Tree Predictor

X-Aggregator

Scorer

Node 8

Node 9

Node 10

Scorer 3:8 Node created an empty data table

Scorer 3:8 Node created an empty data table

Scorer 3:8 Node created an empty data table

3:10 Errors overwriting node settings wi

28°C
Cerah

Search

09:24
09/06/2023