KEAMANAN JARINGAN

Data Mining KNIME

OLEH :

Mochammad Jauhar Ulul Albab
(3122640044)

PROGRAM STUDI TEKNIK INFORMATIKA

DEPARTEMEN TEKNIK INFORMATIKA DAN

KOMPUTER POLITEKNIK ELEKTRONIKA

NEGERI SURABAYA

2022/2023

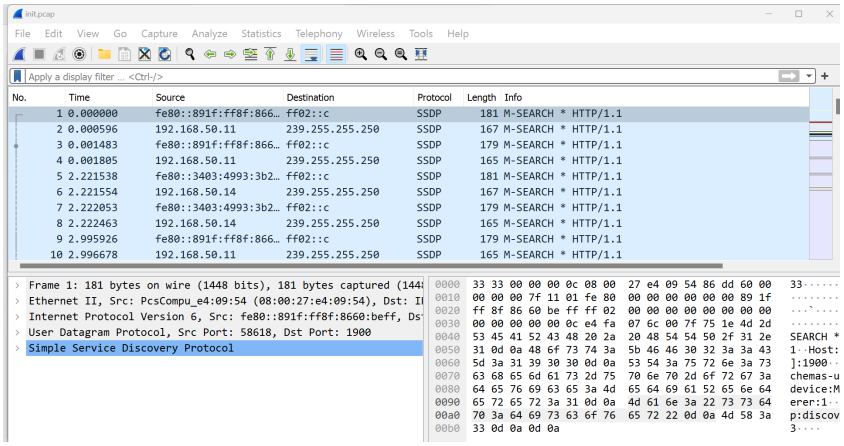
Laporan Praktikum

1. Terdapat 5 file hasil download yaitu, init.pcap, init2.pcap, init3.pcap, init4.pcap, init5.pcap

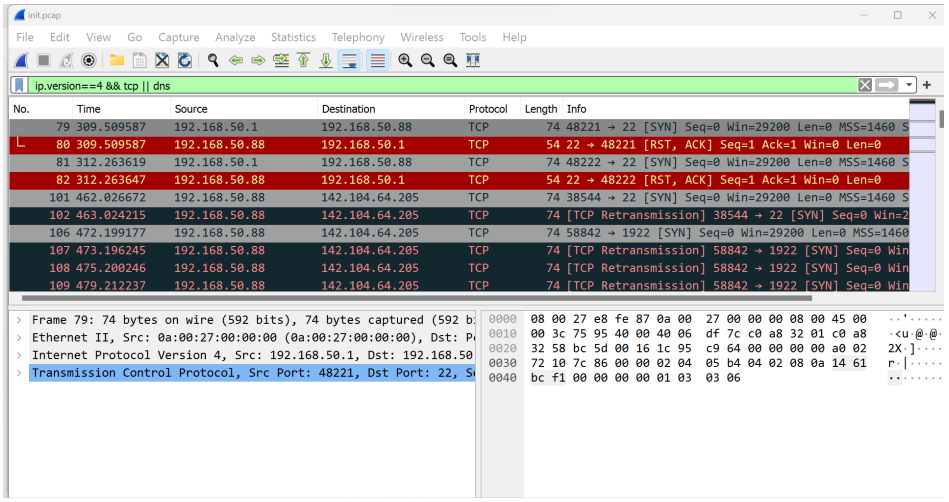
Name	Date modified	Type	Size
init	28/11/2017 16:52	Wireshark capture file	163.160 KB
init2	28/11/2017 16:51	Wireshark capture file	576.966 KB
init3	28/11/2017 16:51	Wireshark capture file	159.862 KB
init4	28/11/2017 16:52	Wireshark capture file	656.556 KB
init5	28/11/2017 16:52	Wireshark capture file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

2. Kemudian buka file tersebutsecara bergantian menggunakan Wireshark.

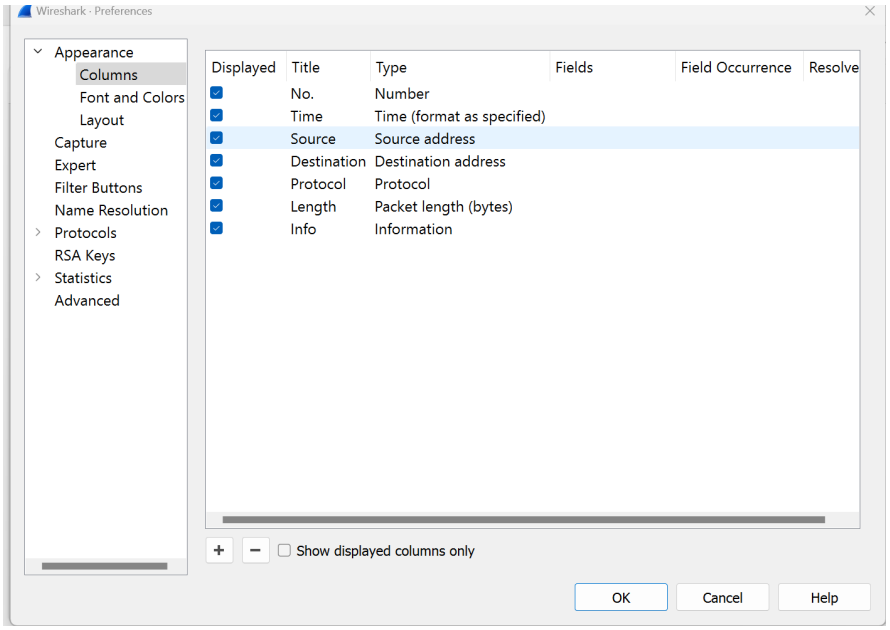
file init.pcap

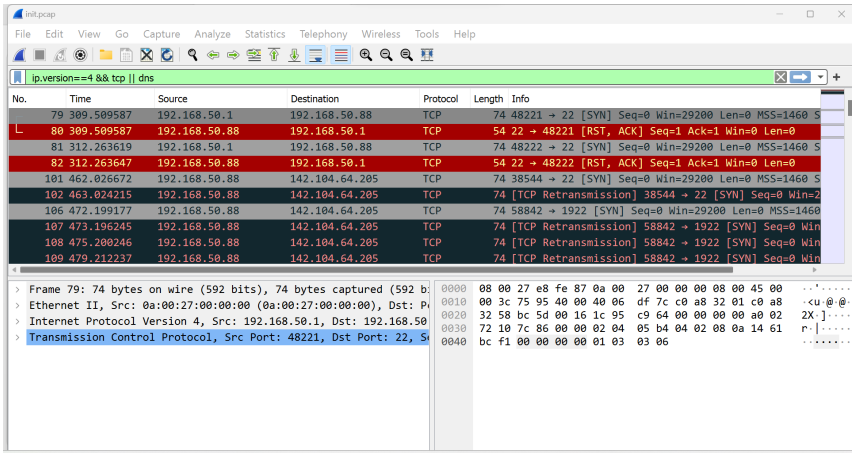


3. Untuk proses analisa yang akan dilakukan nantinya, kita mengambil data dengan ip versi 4 dan protocol TCP, DNS saja.

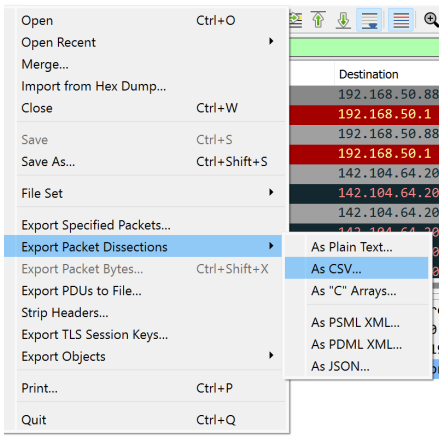


4. Untuk mendapatkan delta time display, klik Edit – Preferences – Column



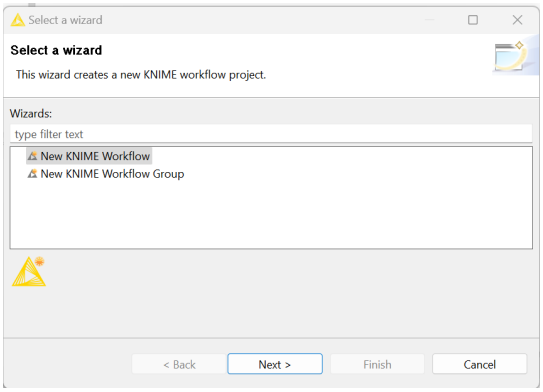


5. Export file pcap ke format csv.

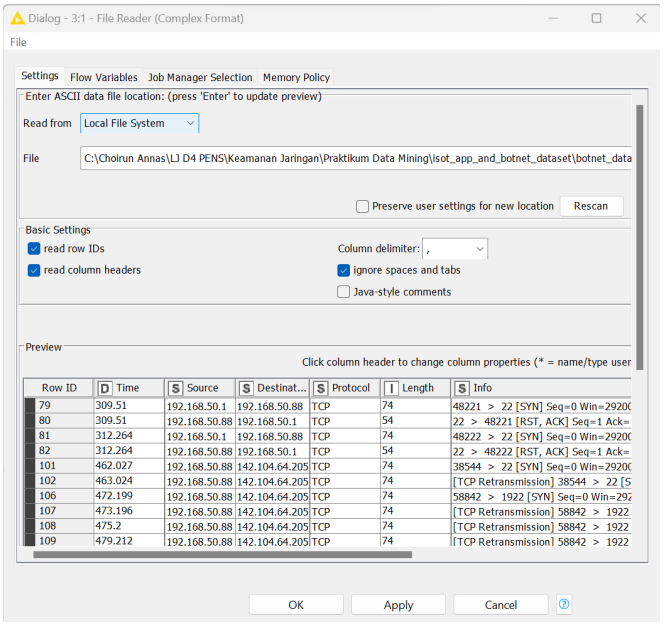


Name	Date modified	Type	Size
init	08/06/2023 23:42	Microsoft Excel Com...	43.481 KB
init	28/11/2017 16:52	Wireshark capture file	163.160 KB
init2	08/06/2023 23:48	Microsoft Excel Com...	43.481 KB
init2	28/11/2017 16:51	Wireshark capture file	576.966 KB
init3	08/06/2023 23:51	Microsoft Excel Com...	149.525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

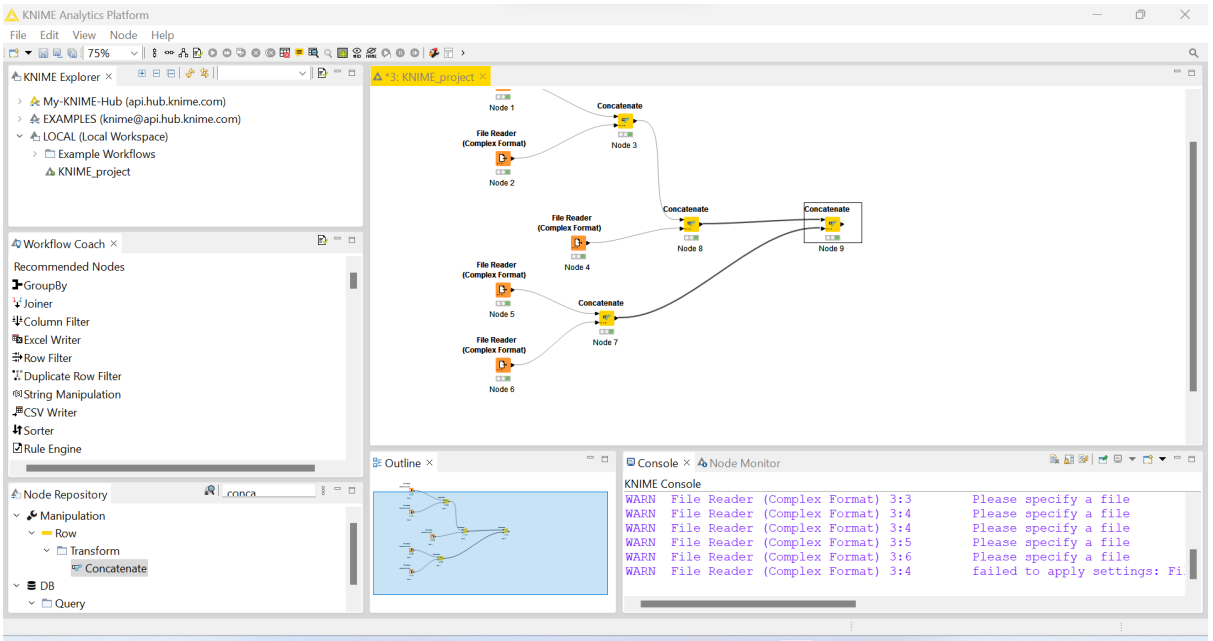
5. membuat workflow/project baru.



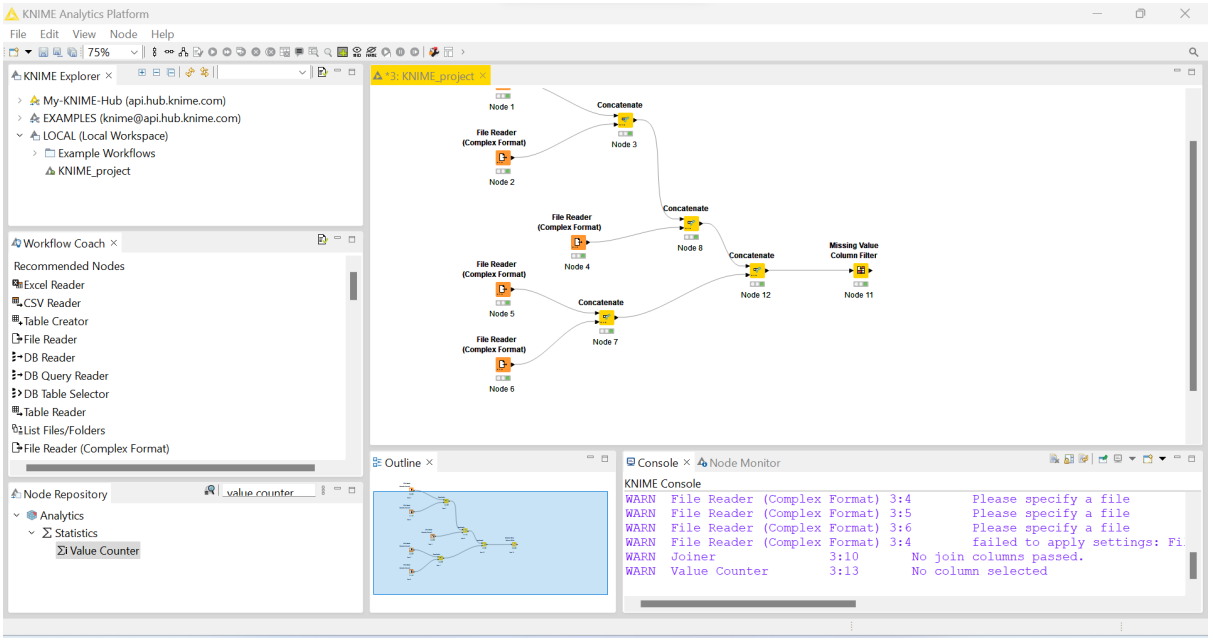
6. Tambahkan data kedalam file reader



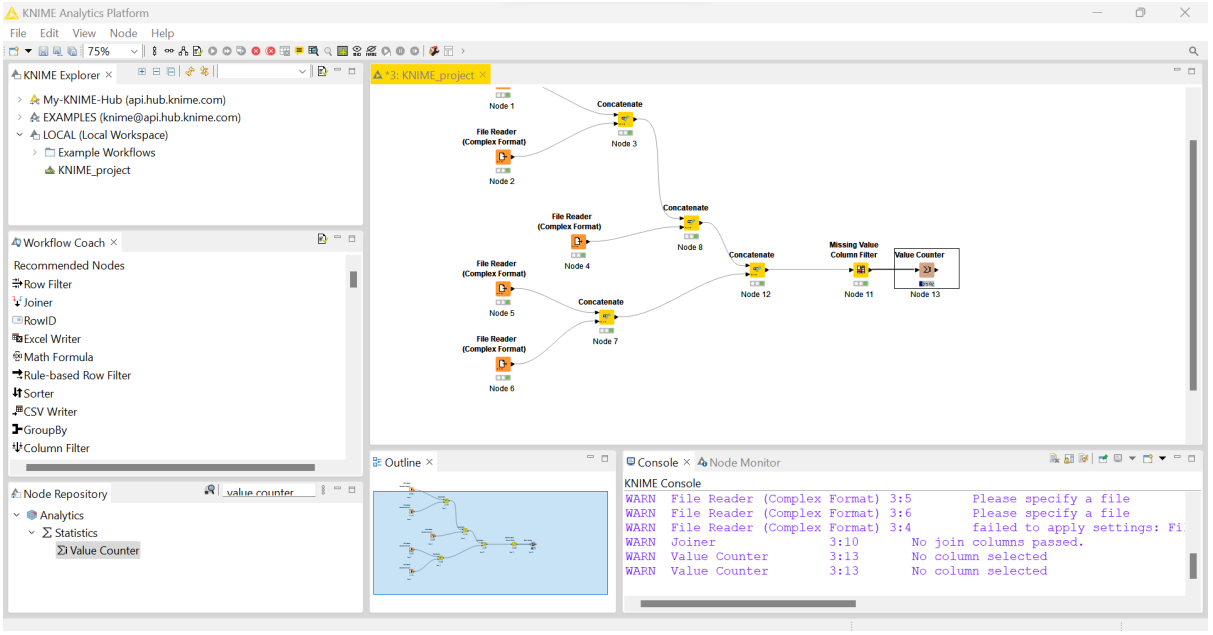
7. Gabungkan kelima data dengan menggunakan concatenate dan data reader



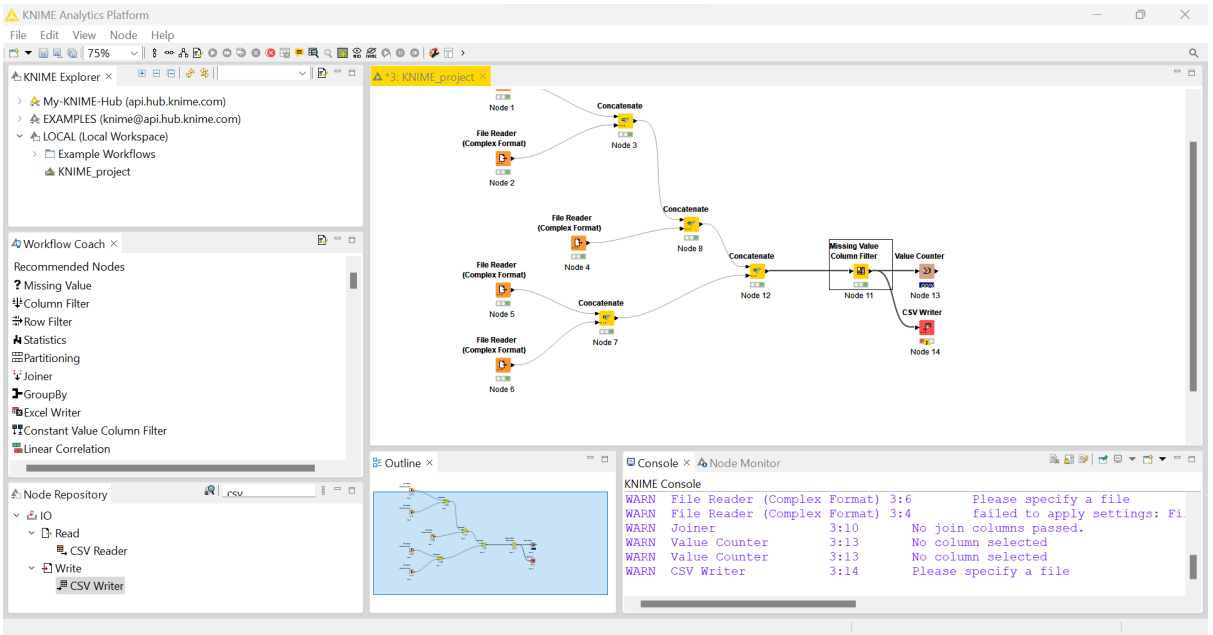
8. Untuk melakukan labeling data normal kita akan menggunakan Node Missing Value. Node ini digunakan untuk mengisi data kosong.

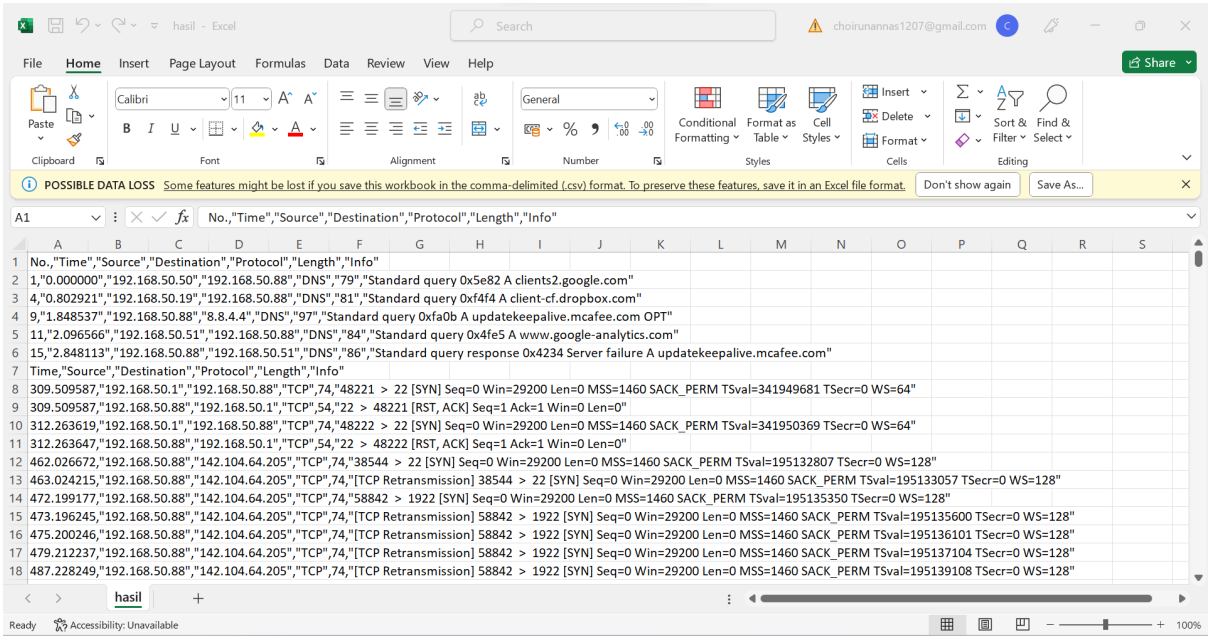


9. Untuk memastikan bahwa kolom label sudah terisi dengan value Malicious atau Normal, dapat menggunakan node Value Counter. Node ini berfungsi untuk menghitung jumlah seluruh value pada kolom terpilih.



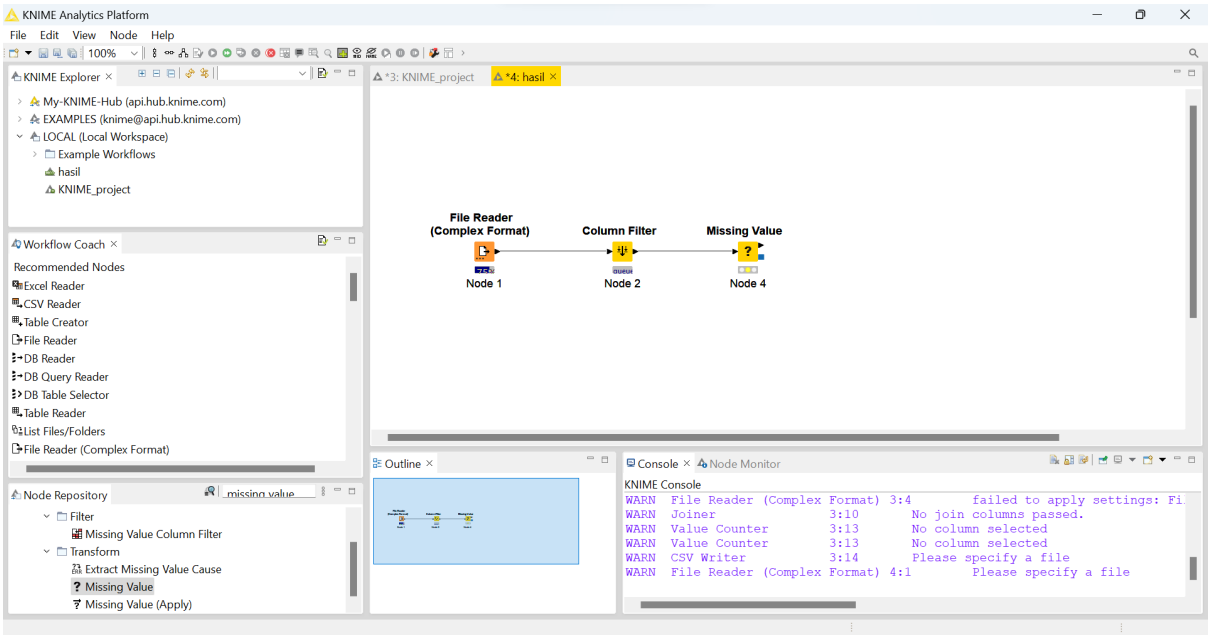
10. Export file ke dalam format .csv dengan menggunakan node CSV Writer



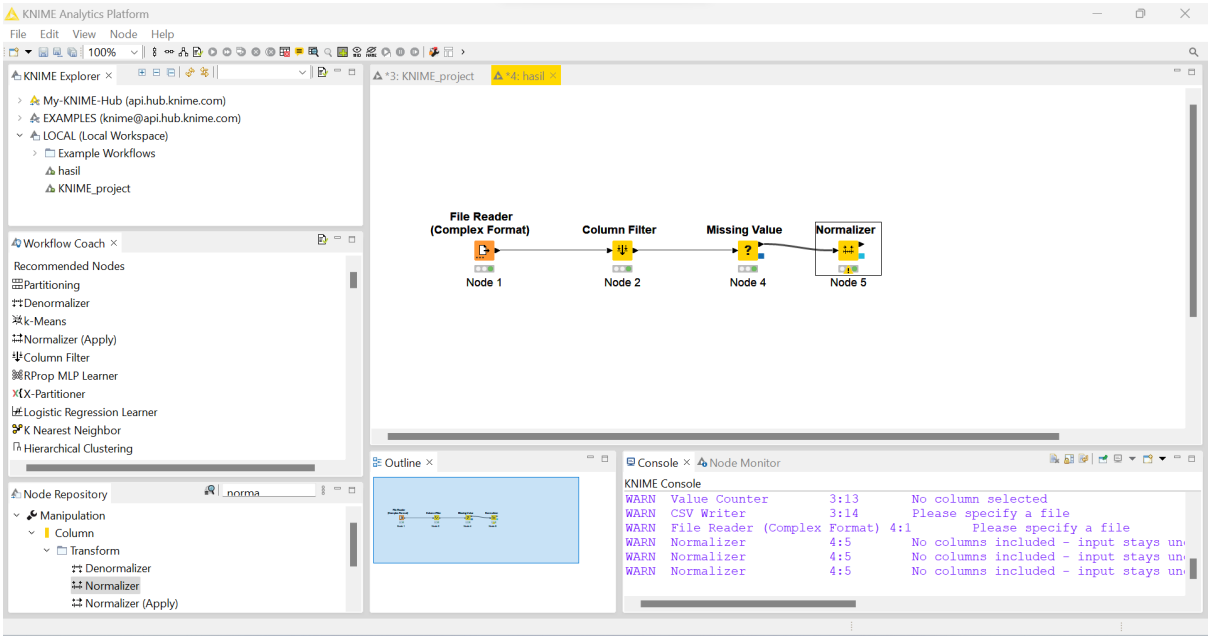


11. Data Pre Processing

Proses dimana 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.

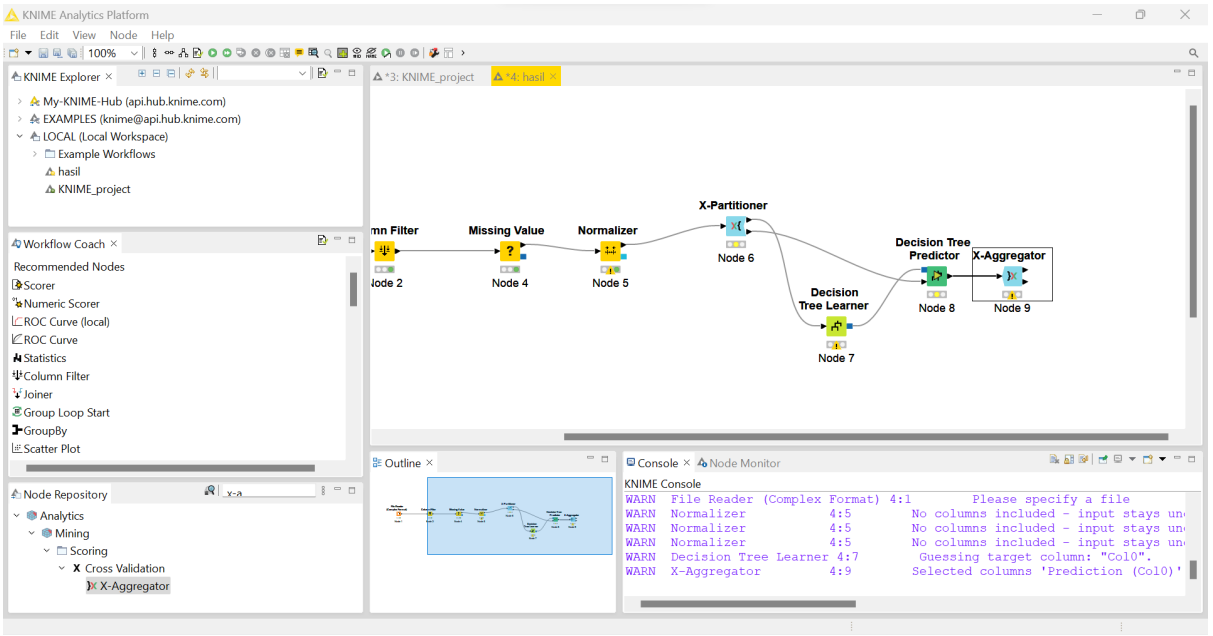


12. Proses data transformation, pada proses ini data akan diubah ke format yang sesuai untuk proses data mining. Node yang digunakan pada tahap ini yaitu Normalizer. Berikut konfigurasinya

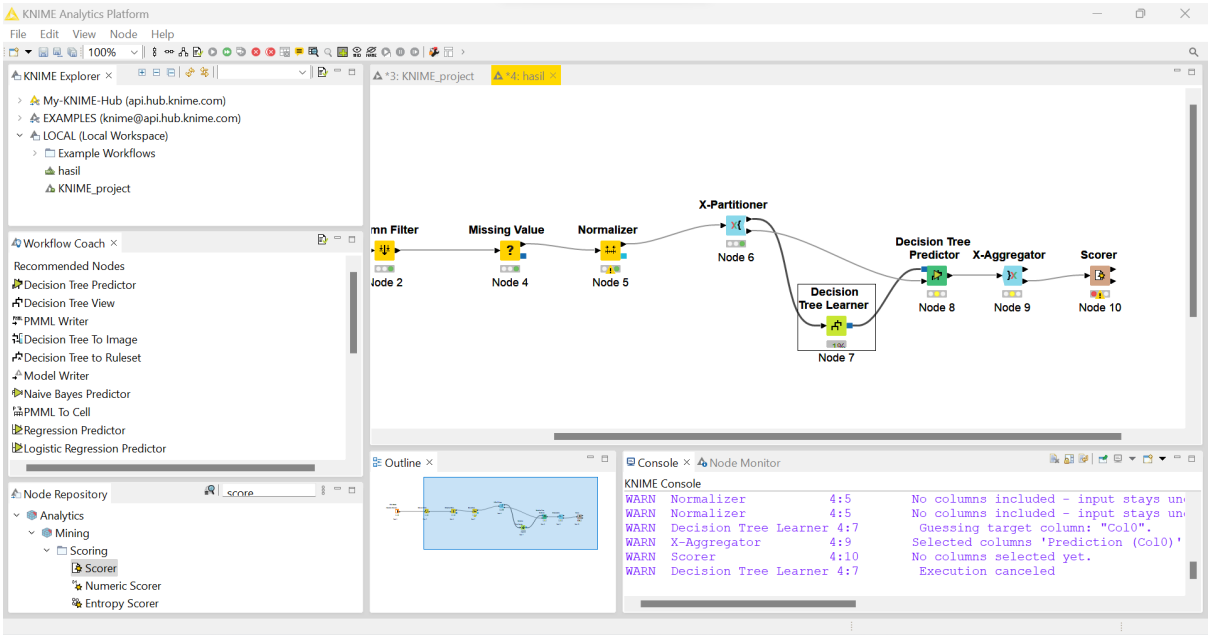


13. Data Mining

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



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



15. Hasil Prediksi