

PACKETS ANALYSIS

By Leonardo Cantarella

INTRODUCTION

This project aims to give more informations about network packets that pass through a device.

Thanks to the used technologies, packets can be processed in real-time and can be enriched with other details.

TSHARK (“THE SNIFFER”)

```
ib2R5J3MgZ29p4gR2V0IGluIHRoZS  
hZG93czogVGhhCdziHRoZSB0LnYu  
pbjogT2gsIGFsbCB      odCwgSSds  
keSB0byBTY3Vwc      4ldCBwbGVh  
kbyB5b3UgcmV      i8gQ29tZQpp  
0aGluZyBoZ      xRpbi4gQW5k  
0eSBpc2xh      3biBmb3IgaX  
0ZZIKYW5      IGJ1YWN0ZX  
gYSBjbG      IGhvcm16b2  
zb3J0I      Ugc2hhcG  
sZCBNYW46IE9oVnaG46IFdoeSBhcm  
KT2xkIE1hbjogkganVzdCBwdXQgc2  
hbmQgdWgsIEknJzb3JiIHNvbWUgb2
```

The terminal version of Wireshark.

This is the base of the “stack”.

Packets are our source to be analyzed, so Tshark “sniffs” them from a network interface, and writes them in a file using a JSON format.

This is the raw data tha will be taken by ...

LOGSTASH (“THE PIPE”)



Logstash can read from that file and can make usable that data by using some basic filtering and ensuring that JSON packets arrives to ...

KAFKA (“THE BROKER”)



Kafka stores our packets and make possible the streaming of them.
He is the intermediate from the source to the elaboration made by ...

SPARK (“THE CORE”)



Spark is the core of the elaboration of the raw packets that arrives from tshark.

Spark elaborates the packets by using web API and machine learnin model to enrich our data adding:

- Geolocation
- Application protocol detection (by port)
- Ip abuse
- Anomaly detection (using machine learning model)

ELASTICSEARCH (“THE INDEXER”)



Elasticsearch stores and indexes the enriched data processed by Spark. It allows for efficient querying and analysis of large datasets, supporting real-time search and analytics

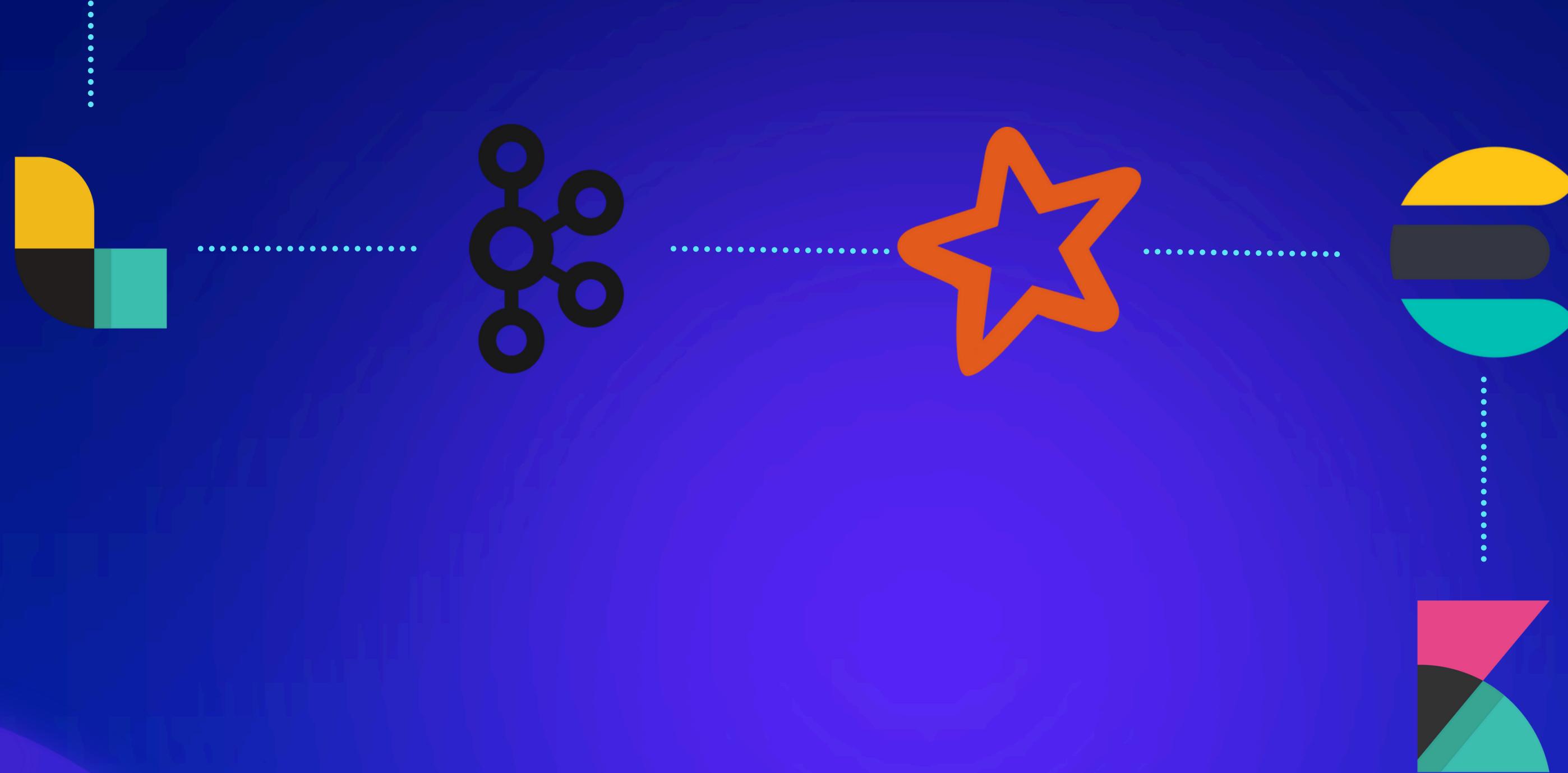
KIBANA (“THE VIEWER”)



Allows to make graphics views in simple way, using a user-friendly interface, interacting with real-time data and helping to understand complex data in a more easy and understandable representation

PACKETS FLOW

```
ib2R5J3Mg229p4gR2VOIGluIHRoZS  
hZG93czogVGhhhdCdzIHRoZSB0LnYu  
pbjogT2gsIGFsbCB odCwgSSds  
kesBObbyBTY3Vwc 4ldCBwbGVh  
kbyB5b3UgcwV i8gQ29tZQpp  
oAGluzyBoZ xRpbi4gQW5k  
0eSBpc2xh 3biBmb3IgaX  
0ZXIKYW5 IGJ1YWN0ZX  
gYSBjbG IGHvcm16b2  
zb3JOI Ugc2hhcG  
sZCBNYW46IE9oVnaG46IFdoeSBhcw  
KT2xkIE1hbjogkganVzdCBwdXQgc2  
hbmQgdWgsIEknJzb3JiIHNVbWUgb2
```



THANK YOU!

