upna

Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

# Sistema online de disección de protocolos en trazas de paquetes

# Indice

- Introducción
- Prototipo
  - Python
  - MySQL
  - Grafana
- Tiempos de ejecución
  - Tiempos de procesado
  - Tiempos de visualización
- Conclusiones y mejoras

# Introducción

- El aumento del número de dispositivos con acceso a Internet y sus reducidos costes, el incremento del ancho de banda de las redes y la gran cantidad de contenido disponible ha provocado que el volumen de información transmitida sea mayor.
- El análisis de las capturas de tráfico se complica.
- Se ha elaborado un complemento a una herramienta previa [1] para obtener información global de la captura.

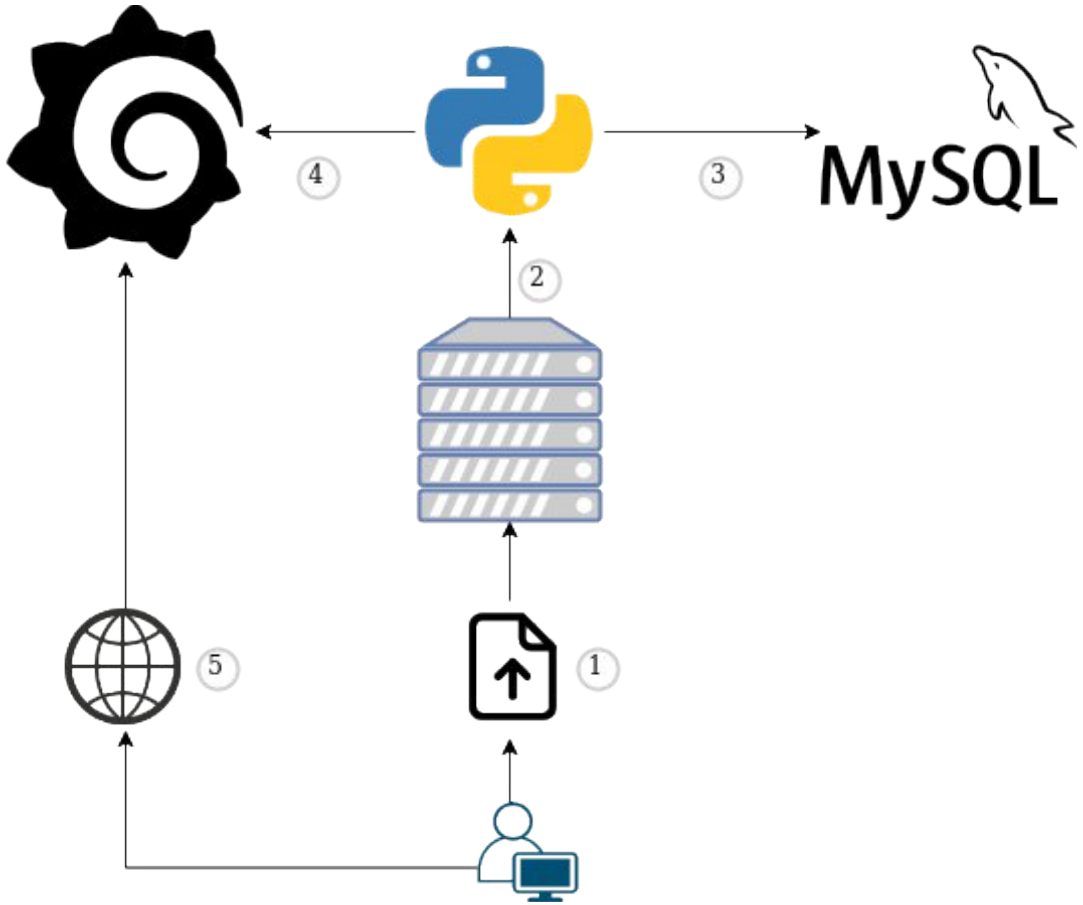
[1]: Arellano Lahuerta, L. (2017). Prototipo analizador de tramas online. Trabajo Fin de Grado. Pamplona: Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación.

# Prototipo

- Consiste en un lector de capturas de tráfico de red.
- Procesa y almacena los paquetes.
- Permite visualizar la traza.

| Capa 2 | | | Capa 3 | | Capa 4 | | Otro |
|---|---|---|---|---|---|---|---|
| MAC origen | MAC destino | Ethertype | IP origen | IP destino | Puerto origen | Puerto destino | Timestamp |

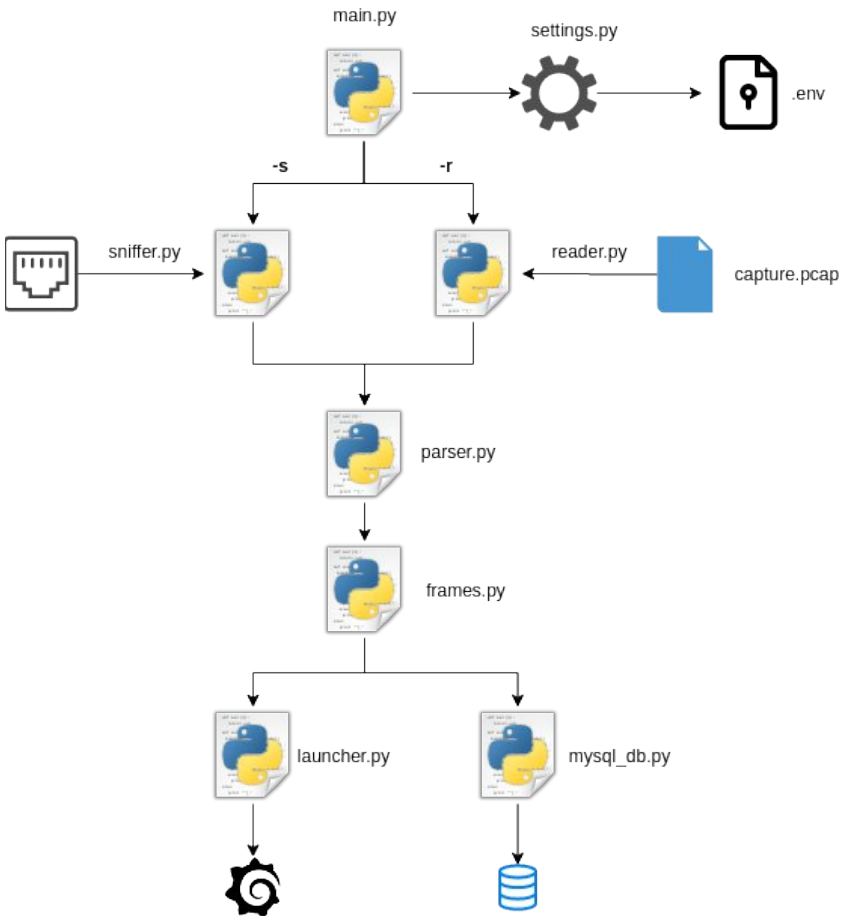
# Prototipo



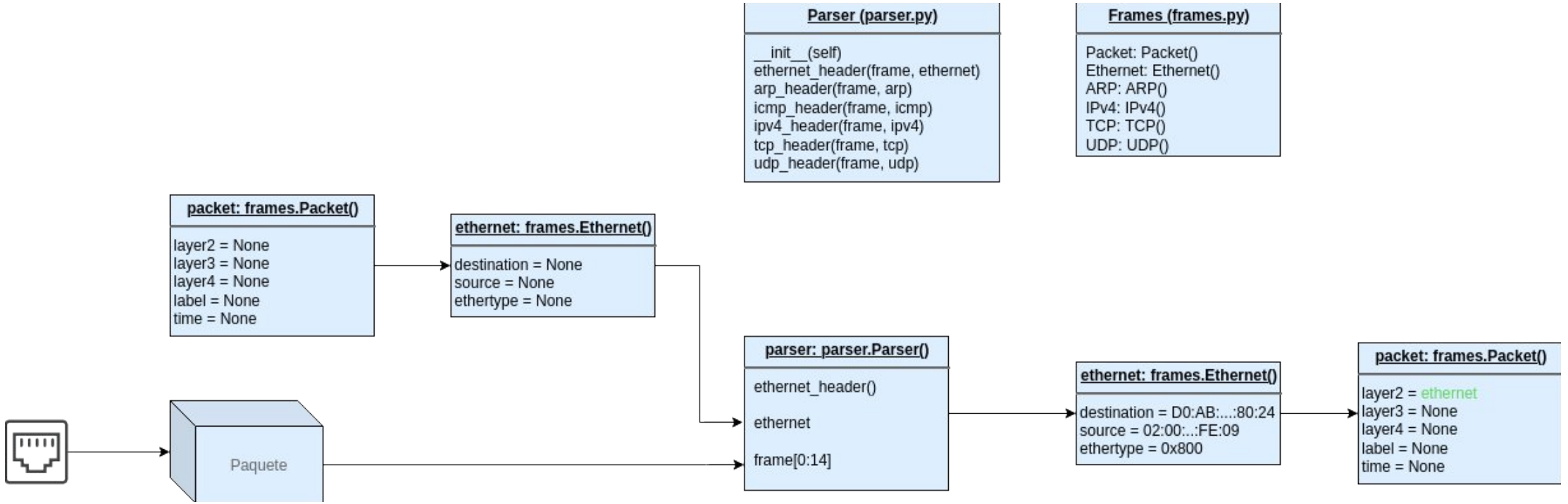
# Prototipo

- Python: Lenguaje de programación de alto nivel. Permite realizar prototipos y pruebas de concepto debido a su sencillez y la gran cantidad de librerías existentes.
- MySQL: Gestor de bases de datos relacionales de gran popularidad. Permite crear distintas bases de datos, tablas y usuarios.
- Grafana: Aplicación web de código abierto que permite visualizar de manera interactiva métricas almacenadas en distintas fuentes de datos. Permite monitorizar sistemas en tiempo real.

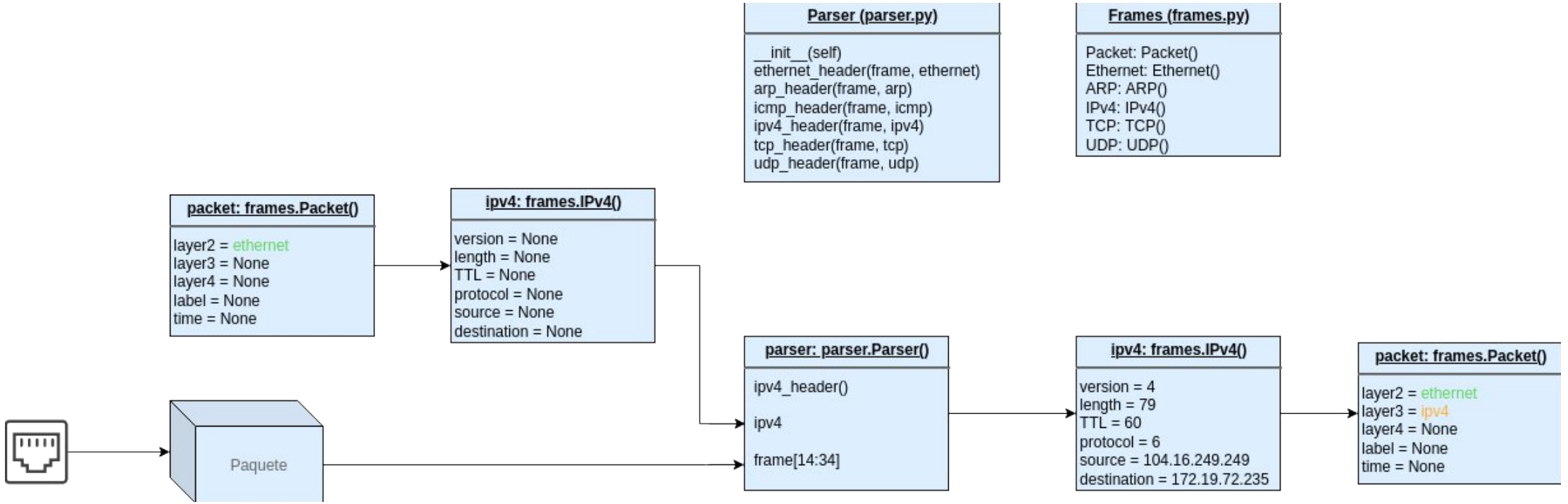
# Prototipo: Python



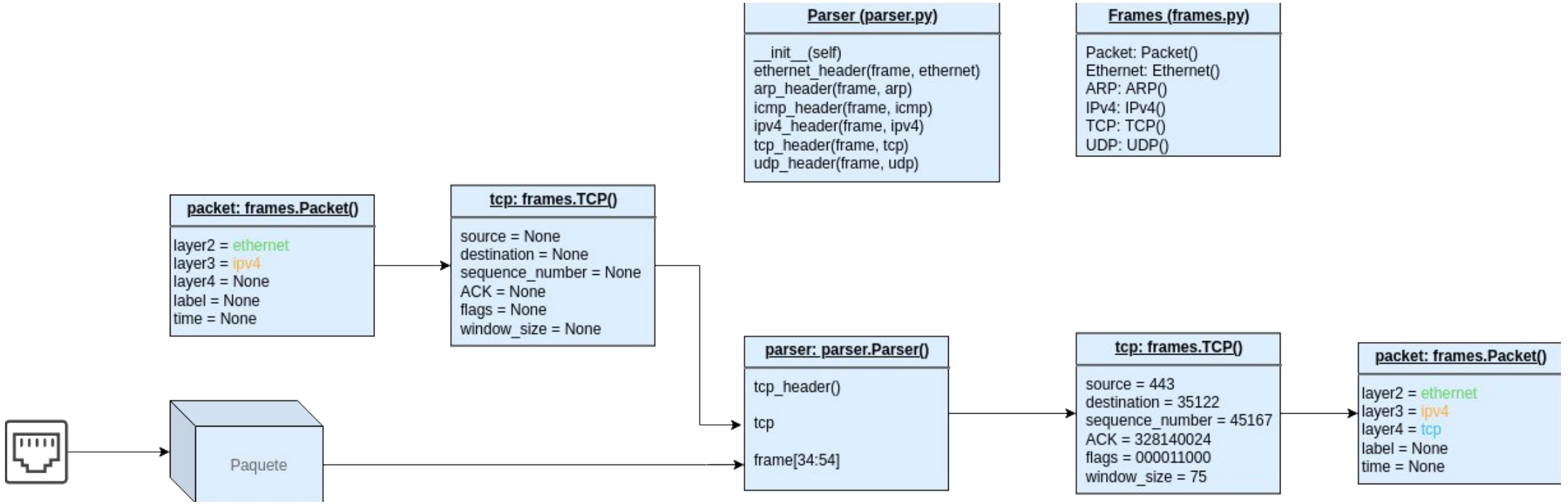
# Python: Paso 1



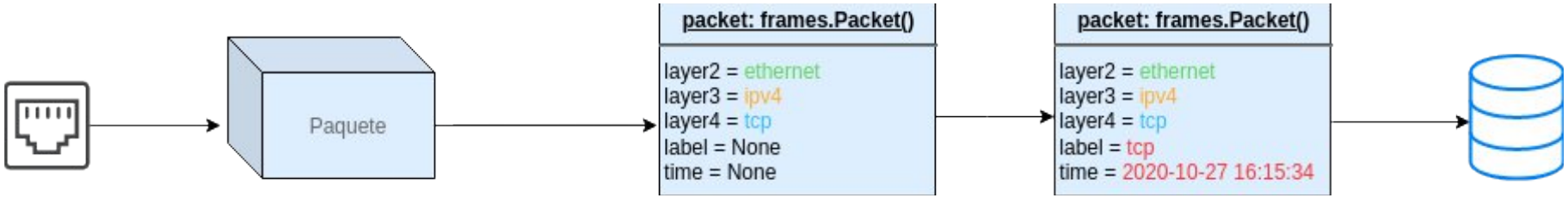
# Python: Paso 2



# Python: Paso 3



# Python: Paso 4



# Prototipo: MySQL

| Field | Type | Null | Key | Default | Extra |
|---|---|---|---|---|---|
| packetID | int(11) | NO | PRI | NULL | auto_increment |
| srcMAC | varchar(17) | NO | | NULL | |
| dstMAC | varchar(17) | NO | | NULL | |
| etherType | varchar(6) | NO | | NULL | |
| srcIP | varchar(15) | NO | | NULL | |
| dstIP | varchar(15) | NO | | NULL | |
| protocol | tinyint(1) unsigned | YES | | NULL | |
| srcPort | smallint(2) unsigned | YES | | NULL | |
| dstPort | smaillint(2) unsigned | YES | | NULL | |
| timestamp | timestamp | NO | | CURRENT_TIMESTAMP | |

# Prototipo: MySQL

```
+-----------------------------------------------------------------+
| Grants for OSniffy@localhost                                    |
+-----------------------------------------------------------------+
| GRANT USAGE ON *.* TO 'OSniffy'@'localhost'                     |
| GRANT ALL PRIVILEGES ON `OSniffy`.* TO 'OSniffy'@'localhost'    |
+-----------------------------------------------------------------+
+-----------------------------------------------------------------+
| Grants for OSniffy_Grafana@localhost                            |
+-----------------------------------------------------------------+
| GRANT USAGE ON *.* TO 'OSniffy_Grafana'@'localhost'             |
| GRANT SELECT ON `OSniffy`.* TO 'OSniffy_Grafana'@'localhost'    |
+-----------------------------------------------------------------+
```

# Prototipo: Grafana

# Prototipo: Grafana

# Tiempos de ejecución

- Se quiere analizar la capacidad de procesado y el tiempo necesario para visualizar las trazas.
- Se ha utilizado tres trazas para simular los comportamientos más habituales [2].
  - Navegación web (39Mb): 59.635 paquetes
  - Vídeo a 1080p (120Mb): 136.797 paquetes
  - Descarga de ficheros (1Gb): 1.061.088 paquetes

[2]: Labayen, Víctor & Magaña, Eduardo & Morató, Daniel & Izal, Mikel. (2020). Online classification of user activities using machine learning on network traffic.
Computer Networks. 181. 107557.10.1016/j.comnet.2020.107557.

# Tiempos de procesado

- Procesar bloques de paquetes antes de almacenarlos.

| | 1 paquete | 10 paquetes | 100 paquetes | 1.000 paquetes | 10.000 paquetes | 20.000 paquetes | 50.000 paquetes | 100.000 paquetes |
|---|---|---|---|---|---|---|---|---|
| **39Mb** | 150.07s | 27.68s | 11.08s | 8.35s | 7.40s | 9.02s | 7.63s | 6.78s |
| **120Mb** | 443.89s | 114.98s | 39.17s | 19.52s | 19.21s | 20.00s | 19.20s | 18.05s |
| **1Gb** | 3599.27s | 865.21s | 323.95s | 165.18s | 137.14s | 140.2s | 124.38s | 118.88s |

- Bloques de 100.000 paquetes para lectura de capturas.
- Bloques de 10.000 paquetes para captura en tiempo real.

# Tiempos de visualización

| | Paquetes por protocolo | Nº de IPs y MACs | Últimos 50 paquetes | Paquetes por segundo |
|---|---|---|---|---|
| **Peticiones** (39Mb) | 186ms | 394ms | 300ms | 298ms |
| **Procesado** (39Mb) | 2ms | <1ms | 1ms | <1ms |
| **Peticiones** (120Mb) | 318ms | 493ms | 531ms | 468ms |
| **Procesado** (120Mb) | 3ms | <1ms | 1ms | <1ms |
| **Peticiones** (1Gb) | 1.02s | 2.44s | 2.43s | 2.46ms |
| **Procesado** (1Gb) | 2ms | <1ms | <1ms | <1ms |

| | Direcciones IP origen | Direcciones IP destino | Puertos origen | Puertos destino |
|---|---|---|---|---|
| **Peticiones** (39Mb) | 398ms | 327ms | 244ms | 297ms |
| **Procesado** (39Mb) | 1ms | <1ms | 1ms | <1ms |
| **Peticiones** (120Mb) | 646ms | 645ms | 420ms | 411ms |
| **Procesado** (120Mb) | <1ms | <1ms | <1ms | <1ms |
| **Peticiones** (1Gb) | 2.83s | 2.84s | 1.46s | 1.56s |
| **Procesado** (1Gb) | <1ms | <1ms | <1ms | <1ms |

# Conclusiones y mejoras

- Complemento sencillo pero potente y fácil de usar.
- Permite visualizar trazas en un tiempo aceptable.
- Traducir el código a C e integrar con la herramienta previa.
- Securizar y testear el código.
- Añadir nuevos protocolos y paneles a Grafana.
- Evaluar el uso de bases de datos no relacionales para optimizar los tiempos de visualización.