Documentación del Proyecto: Analizador de Paquetes PCAP

1. Descripción

Este proyecto es una herramienta interactiva en Python para analizar archivos de captura de paquetes de red (PCAP) utilizando la biblioteca **PyShark**. Permite inspeccionar paquetes, filtrar por protocolo o rango de tiempo, visualizar payloads, encabezados, IPs de origen y destino, así como exportar la información a archivos de texto.

El proyecto incluye interfaz de línea de comandos con colores mediante **Colorama** para facilitar la lectura de resultados.

2. Requisitos

Python 3.8 o superior

Librerías de Python:

`pyshark`

`colorama`

Instalación de librerías:

```
pip install pyshark colorama
```

Nota: PyShark requiere **Wireshark** o **TShark** instalado y configurado en el PATH del sistema.

3. Estructura del Proyecto

```
proyecto_pcap/
│
├─ main.py                  # Script principal del analizador
├─ export/                  # Carpeta donde se guardan las exportaciones
└─ README.md                # Documentación del proyecto
```

`main.py` contiene toda la lógica del programa.

`export/` se crea automáticamente para guardar archivos exportados.

`README.md` proporciona la documentación y guía de uso.

4. Funcionamiento General

1. El usuario ingresa la ruta de un archivo `.pcap`.
2. Se carga la captura completa para permitir acceso aleatorio a los paquetes.
3. Se muestra un resumen de todos los paquetes:
    - Número
    - Hora
    - Protocolo principal
    - IP de origen y destino
    - Indicación de payload (sí/no)
4. El usuario puede ingresar comandos para analizar paquetes individuales o filtrar la captura.
5. Los resultados pueden exportarse a archivos de texto dentro de la carpeta `export`.

5. Comandos Disponibles

Comando	Descripción
`exit`	Termina el programa.
`-h`	Muestra la ayuda con todos los comandos disponibles.
`-pl [num]`	Mostrar payload del paquete `[num]`.
`-hex [num]`	Mostrar payload en hexadecimal del paquete `[num]`.
`-hdr [num]`	Mostrar encabezados completos del paquete `[num]`.
`-src [num]`	Mostrar IP de origen del paquete `[num]`.
`-dst [num]`	Mostrar la IP de destino del paquete `[num]`.
`-proto [num]`	Mostrar protocolo principal del paquete `[num]`.
`-all [num]`	Mostrar resumen completo del paquete `[num]`.
`-filter=[PROTOCOLO]`	Mostrar sólo paquetes que contengan ese protocolo. Ej: `-filter=TCP`.
`-time=[HH:MM:SS]-[HH:MM:SS]`	Filtrar paquetes por rango de hora.

`-count`	Mostrar total de paquetes cargados y cantidad con/sin payload.
`-export [archivo]`	Exportar la información de paquetes a un archivo de texto.
`-clear`	Limpiar la pantalla de la terminal.

6. Ejemplos de Uso

Mostrar payload del paquete 10:

```
-pl 10
```

Filtrar paquetes TCP entre 10:00:00 y 11:00:00:

```
-filter=TCP -time=10:00:00-11:00:00
```

Exportar la información del paquete 5 a un archivo:

```
-all 5 -export paquete5
```

7. Notas Adicionales

- Los paquetes que no tengan capa IP muestran `N/A` en origen/destino.
- El payload se muestra en verde si existe y en rojo si no.
- La exportación agrega automáticamente la extensión `.txt` si no se proporciona.
- Se recomienda usar archivos PCAP relativamente pequeños para evitar alto consumo de memoria, ya que la carga completa de la captura se realiza en memoria.