**Ciberseguridad en SCI - Demos**

**5.- Comunicaciones no seguras**

INDICE

**5.- Comunicaciones no seguras.**

***Demo 10 - Comunicaciones no seguras* . Omron**

***Demo 11 - Comunicaciones no seguras* . Siemens**

**Demo 10 -Comunicaciones no seguras **

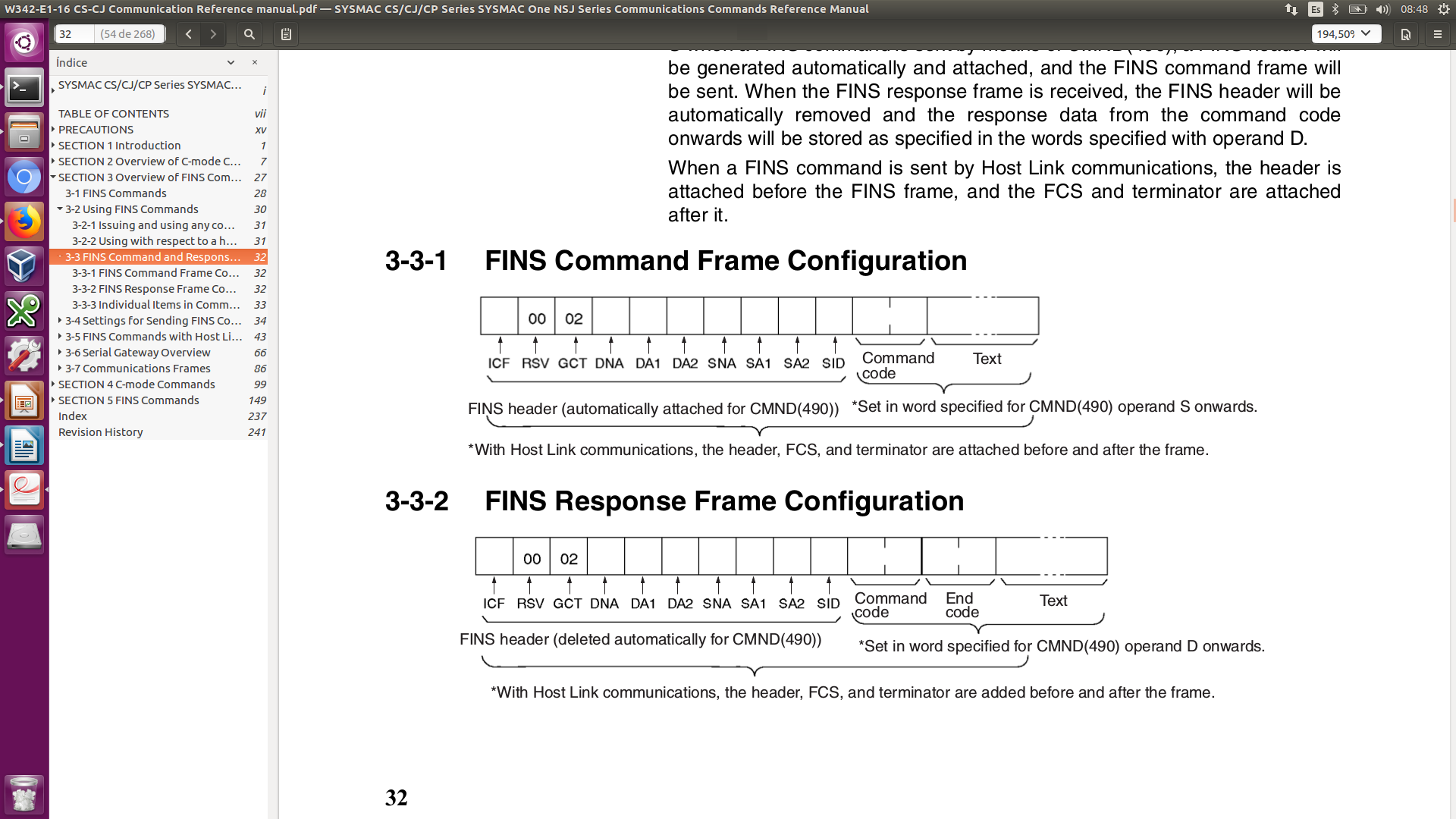
**En este apartado se va a trabajar con los paquetes de tráfico generados por Omron y Siemens en sus comunicaciones. La conclusión general es que el tráfico de información que se genera es visible y por lo tanto modificable con el riesgo que esto supone.**

**OMRON**

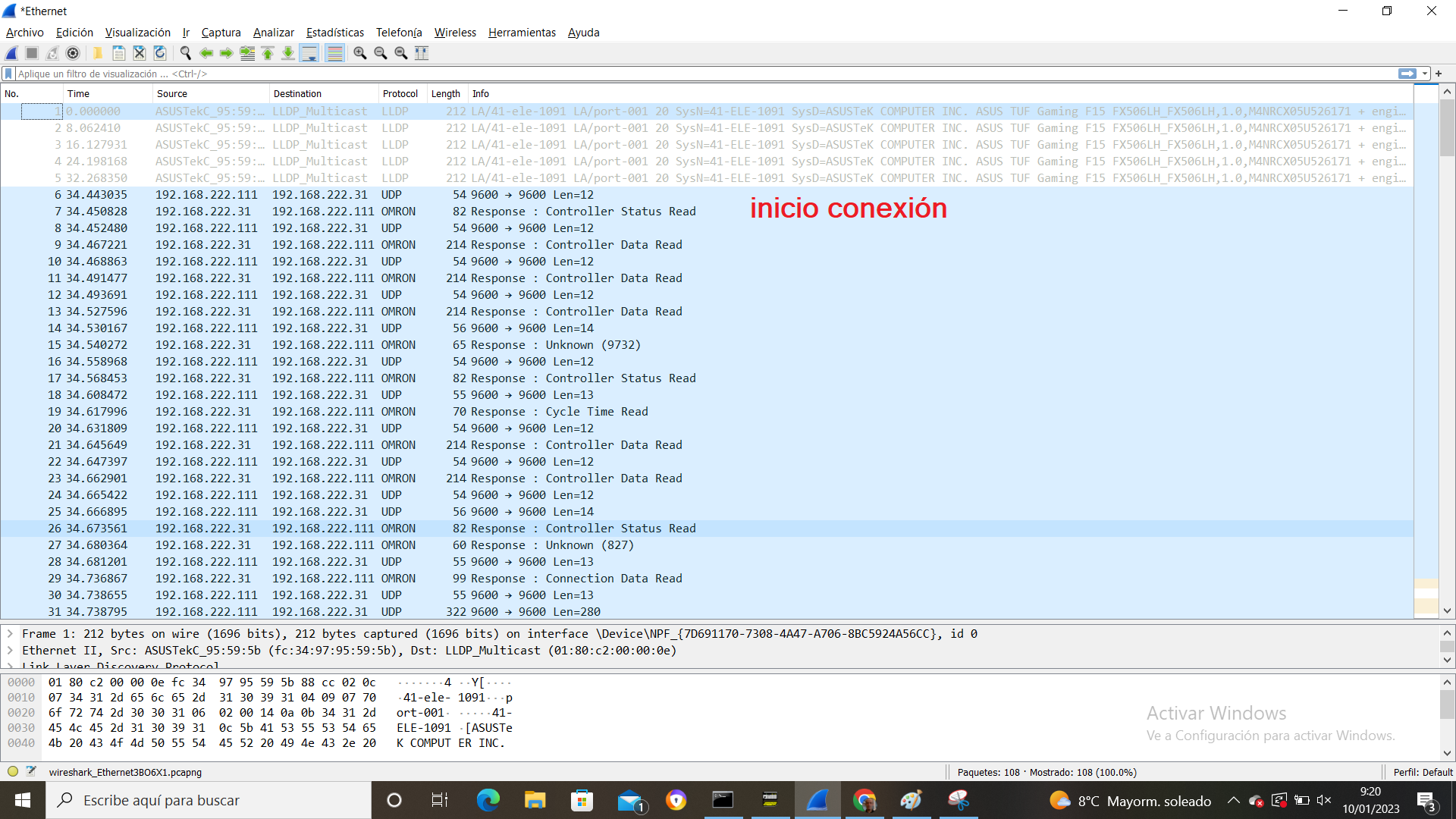
**FINS** (Factory Interface Network Service) es un protocolo propietario de Omron usado para comunicar sus PLC.

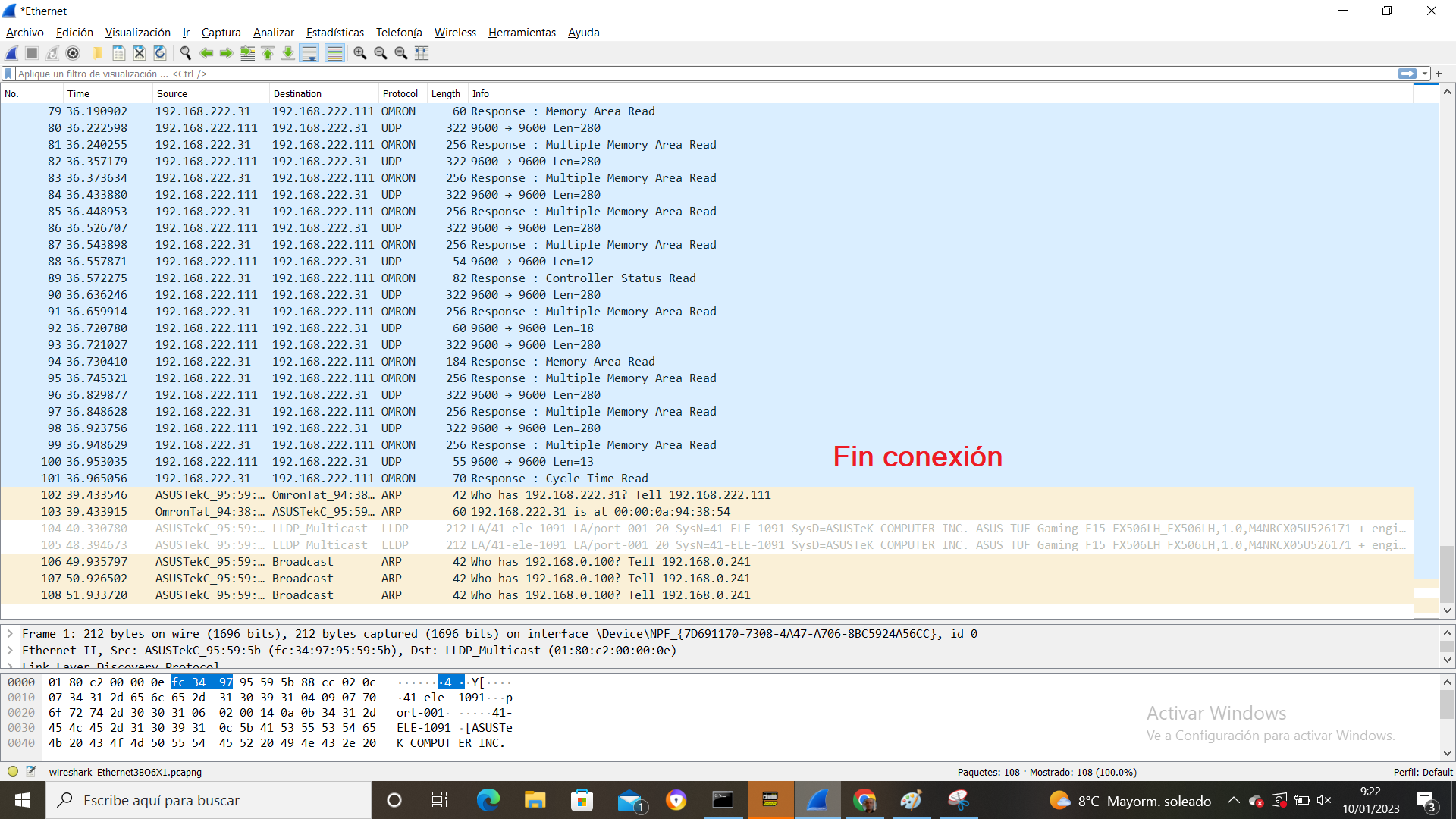
Existen dos métodos que se pueden utilizar en la capa de transporte, uno orientado a la velocidad en la transmisión (**UDP**) y el otro orientado a la fiabilidad de la conexión (**TCP**).Los datos que se envían y reciben sobre la red Ethernet utilizan el puerto 9600 para la comunicación .

La trama FINS consta de una cabecera y del comando FINS y no implementa medidas de seguridad nativas en su capa de aplicación

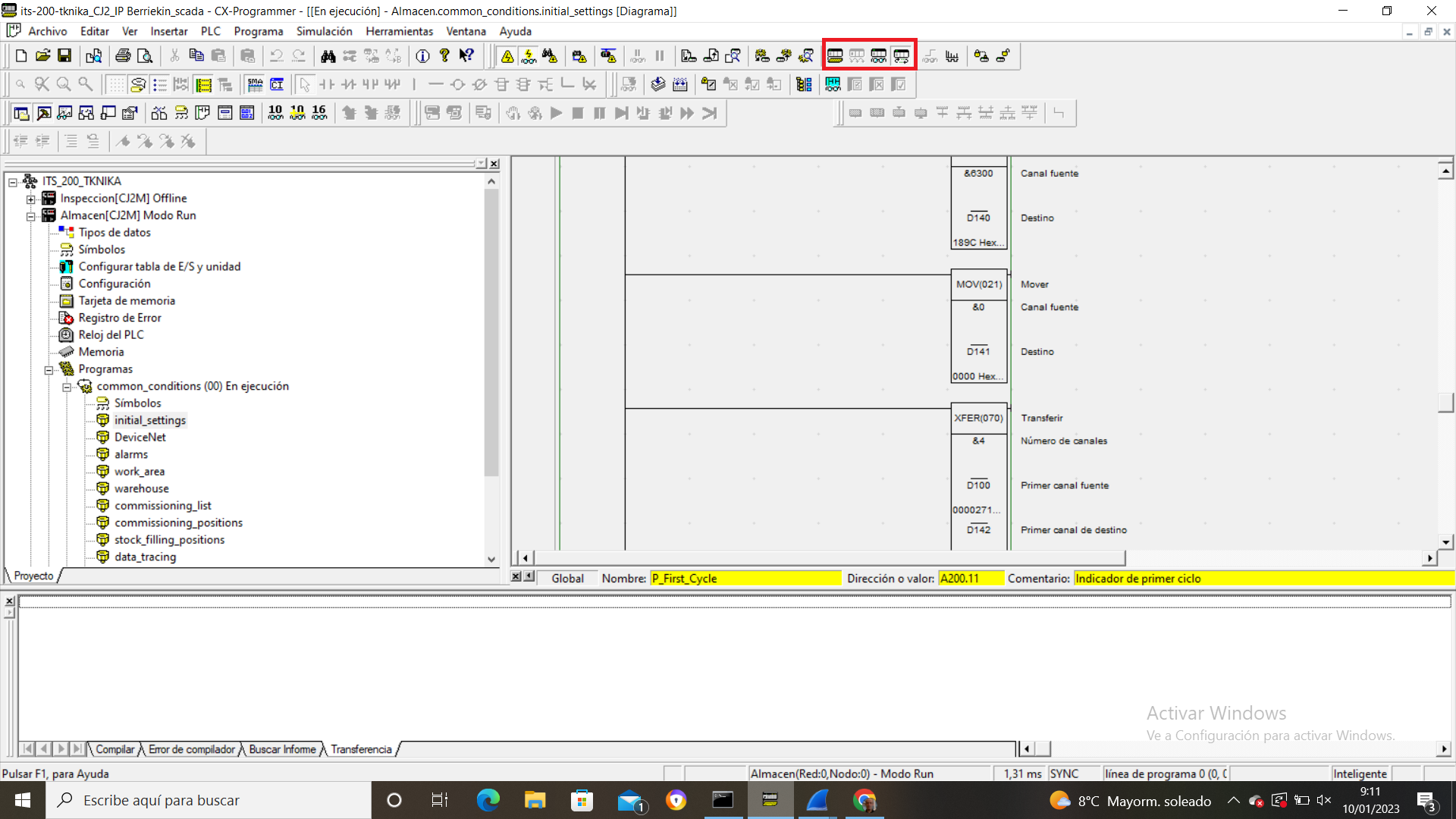


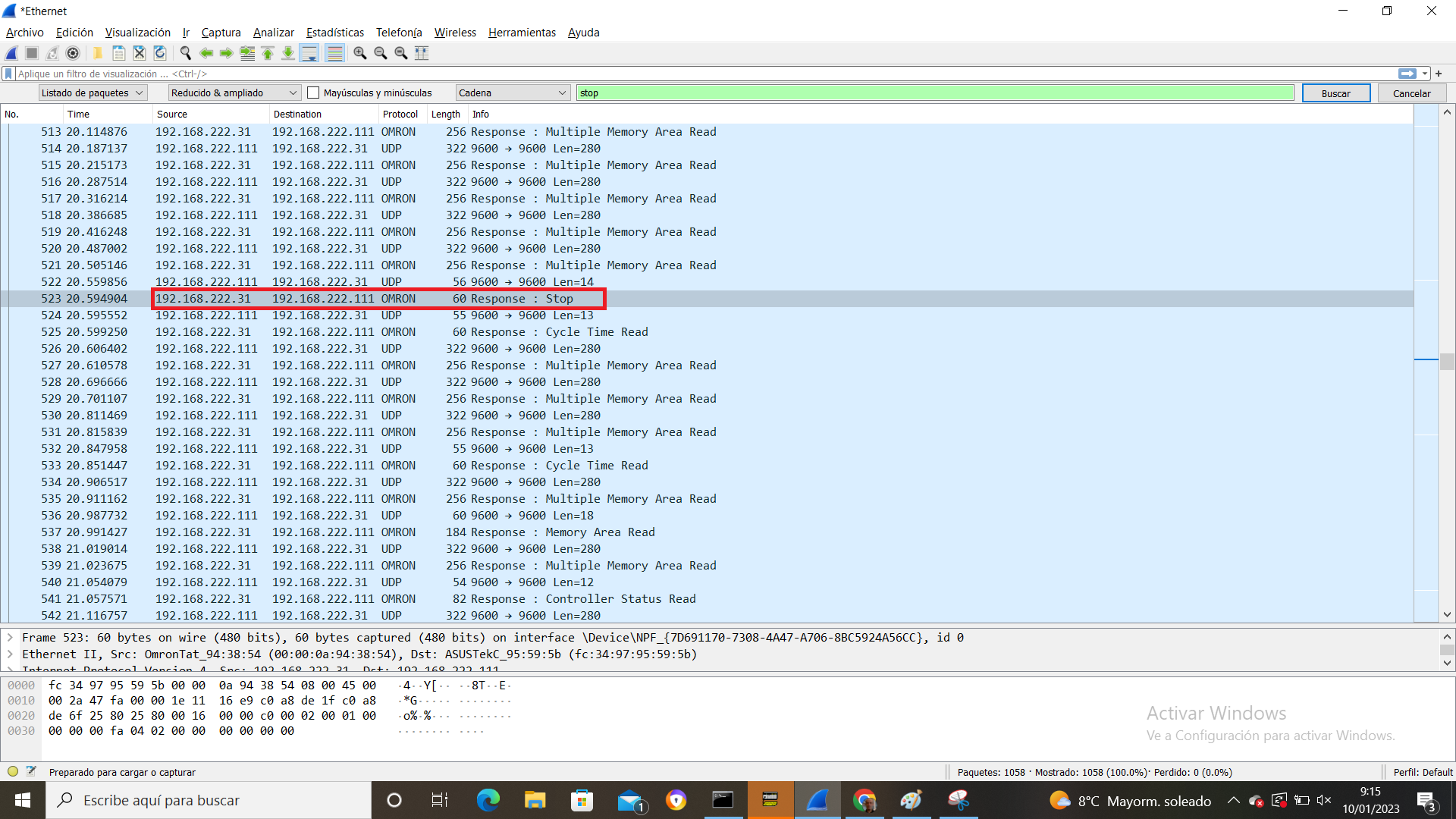
Si ponemos wireshark en captura y nos conectamos al PLC Omron veremos cómo se inicia y finaliza la comunicación.

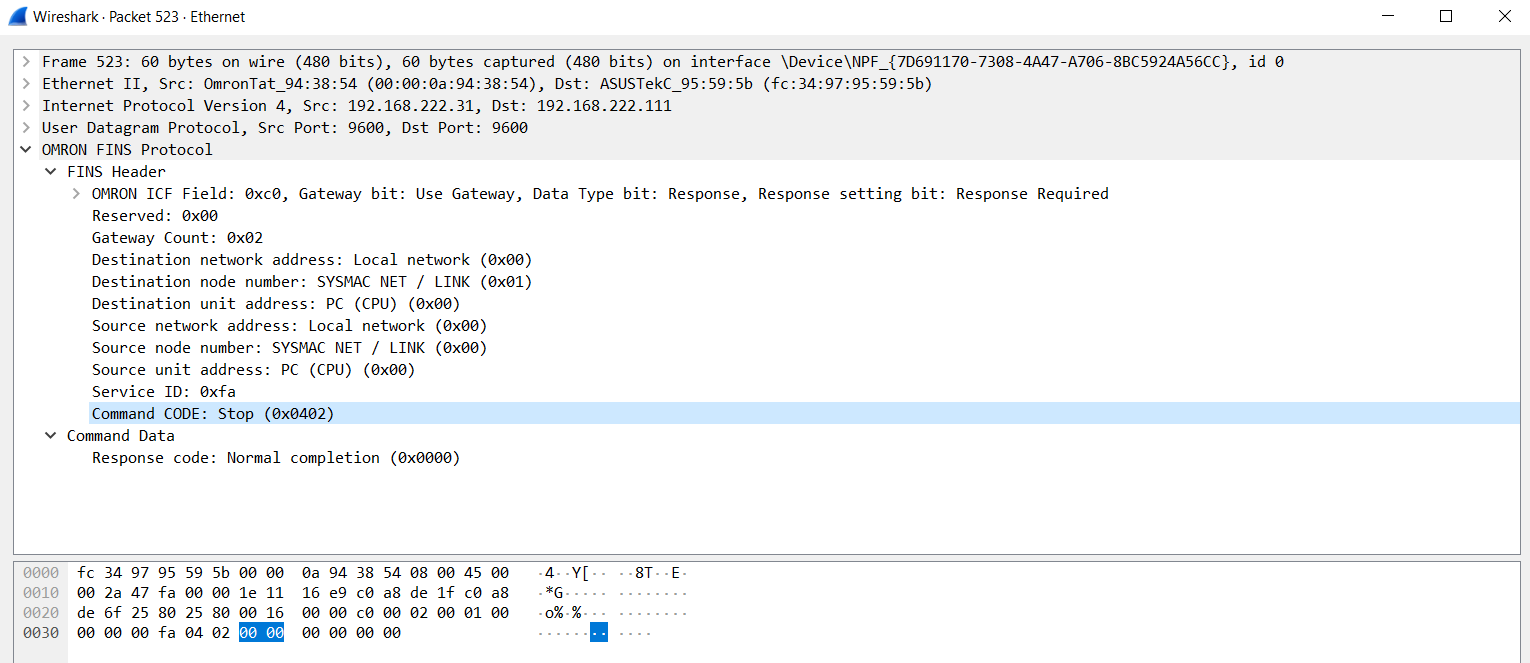




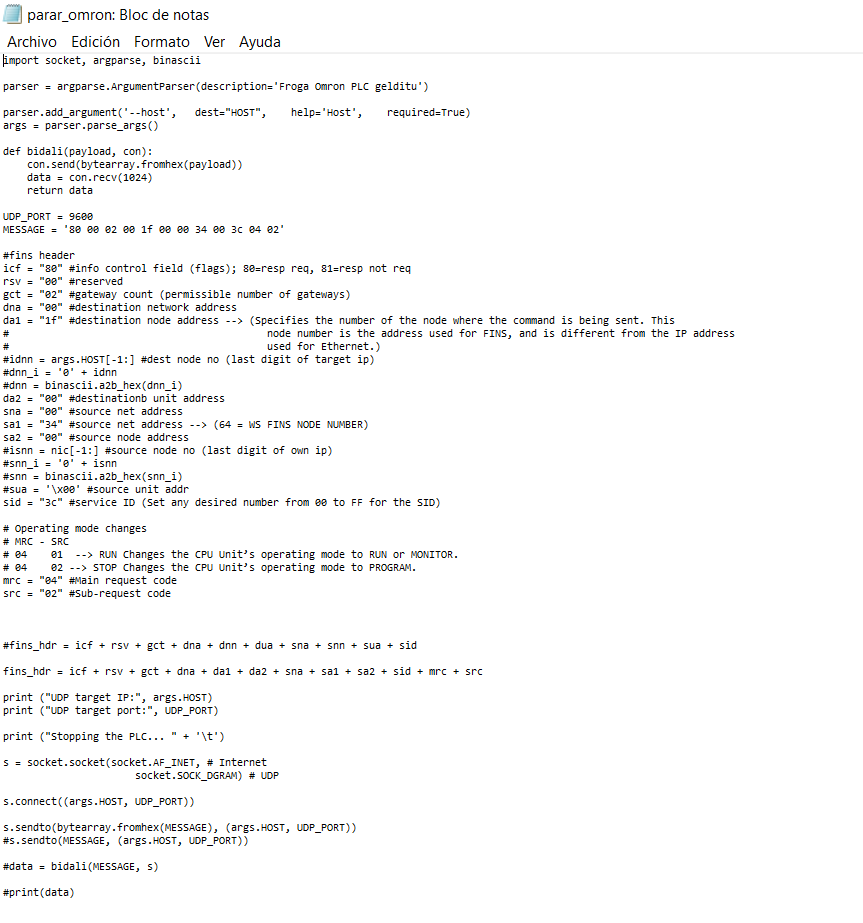
Otro evento detectable es la parada de la CPU. Al pasar al modo monitor podemos ver la orden de parada en wireshark.





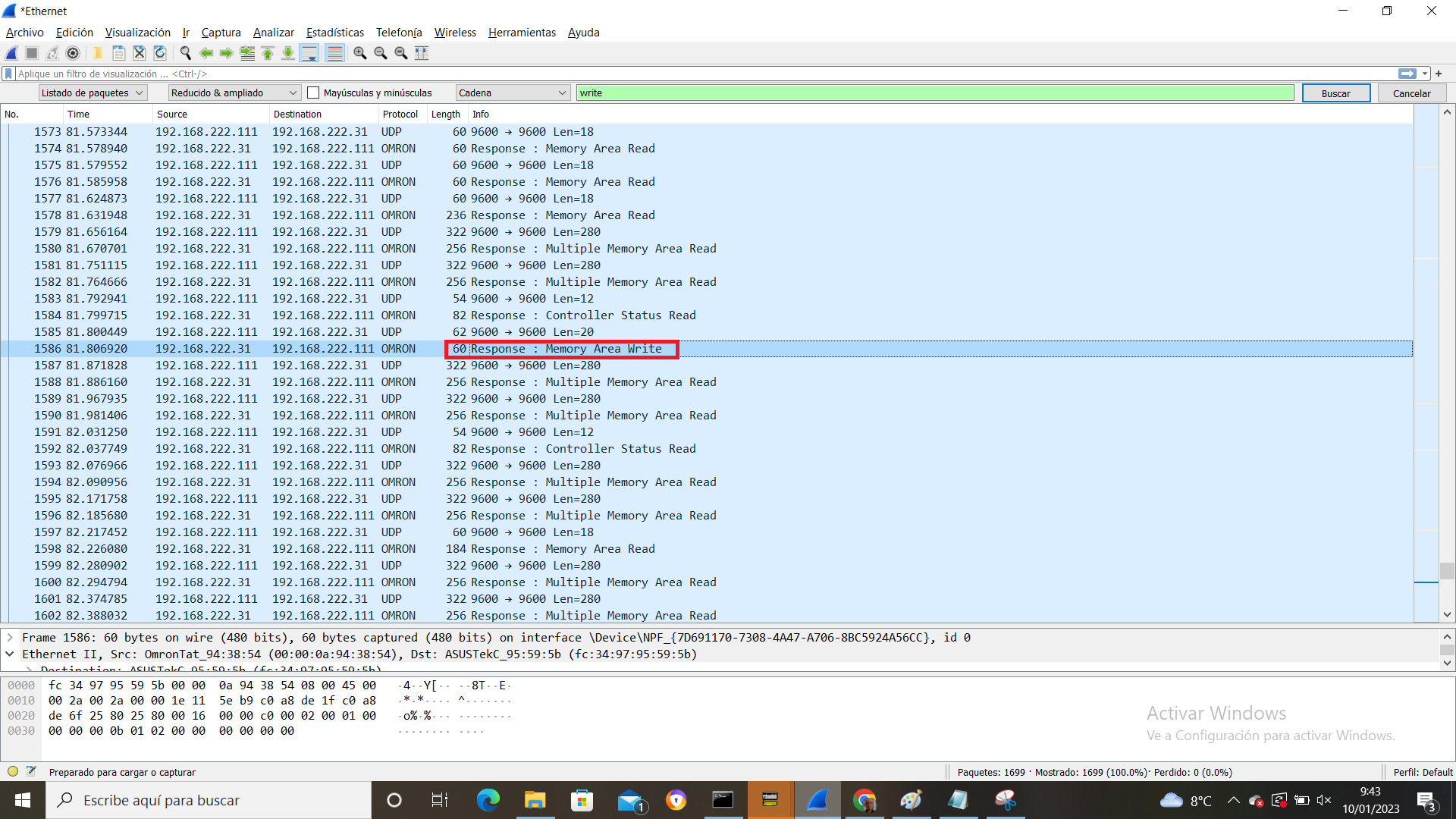


Sabiendo interpretar la orden de parada y teniendo el conocimiento adecuado se puede crear un script con el código de manera que este script fuerza la parada de la CPU.



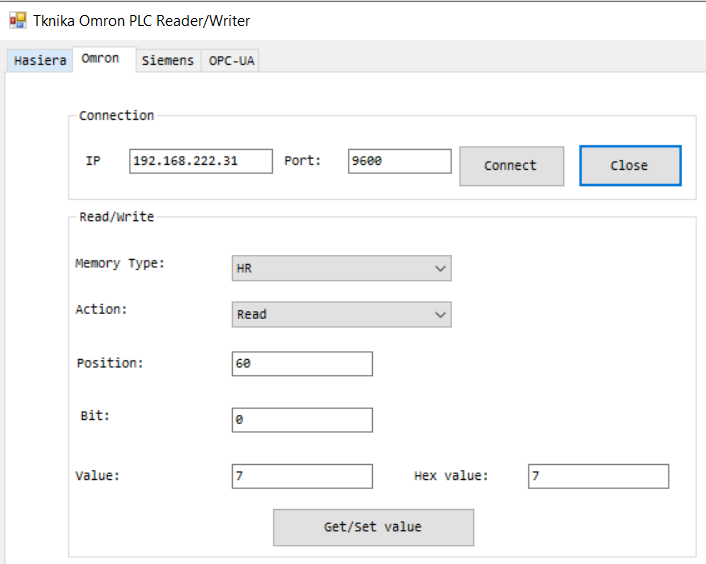
Cada vez que se escribe en la memoria del PLC se genera tráfico de escritura (Memory Area Write)

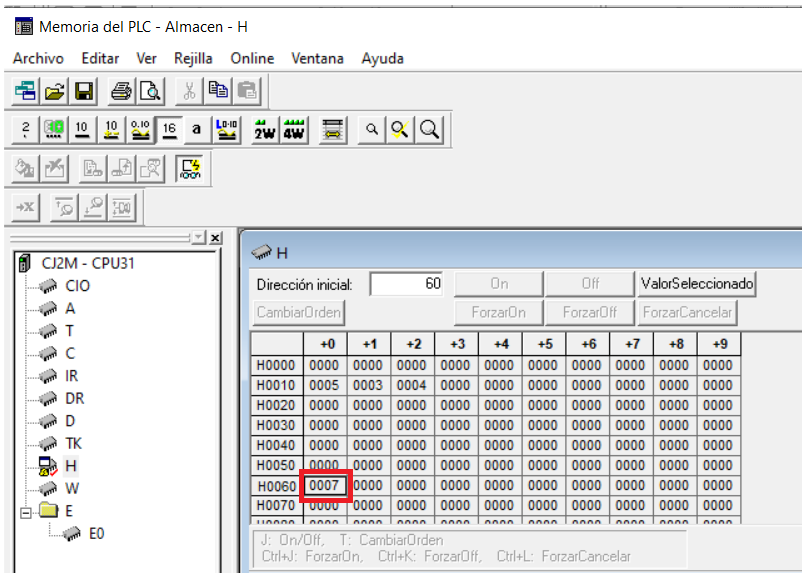




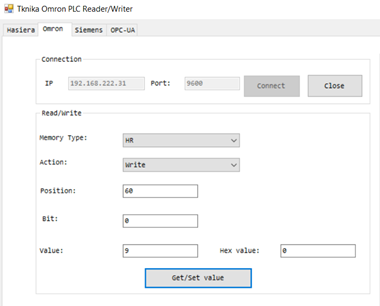
**La conclusión inicial era que el tráfico generado es visible mediante Wireshark. Teniendo el conocimiento adecuado de programación, o buscado en internet :-) , se puede crear un programa que mande las órdenes directamente al PLC.**

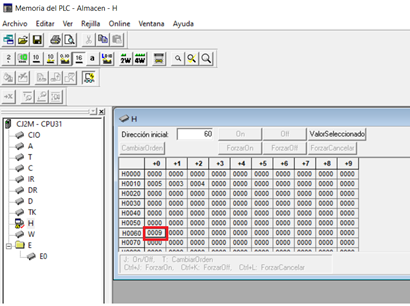
Desde el panel ejecutable Tknika se lanza el panel que puede conectar con el PLC y mandarle órdenes directamente.En el ejemplo se lee un dato de la memoria del PLC H0060 = 0007

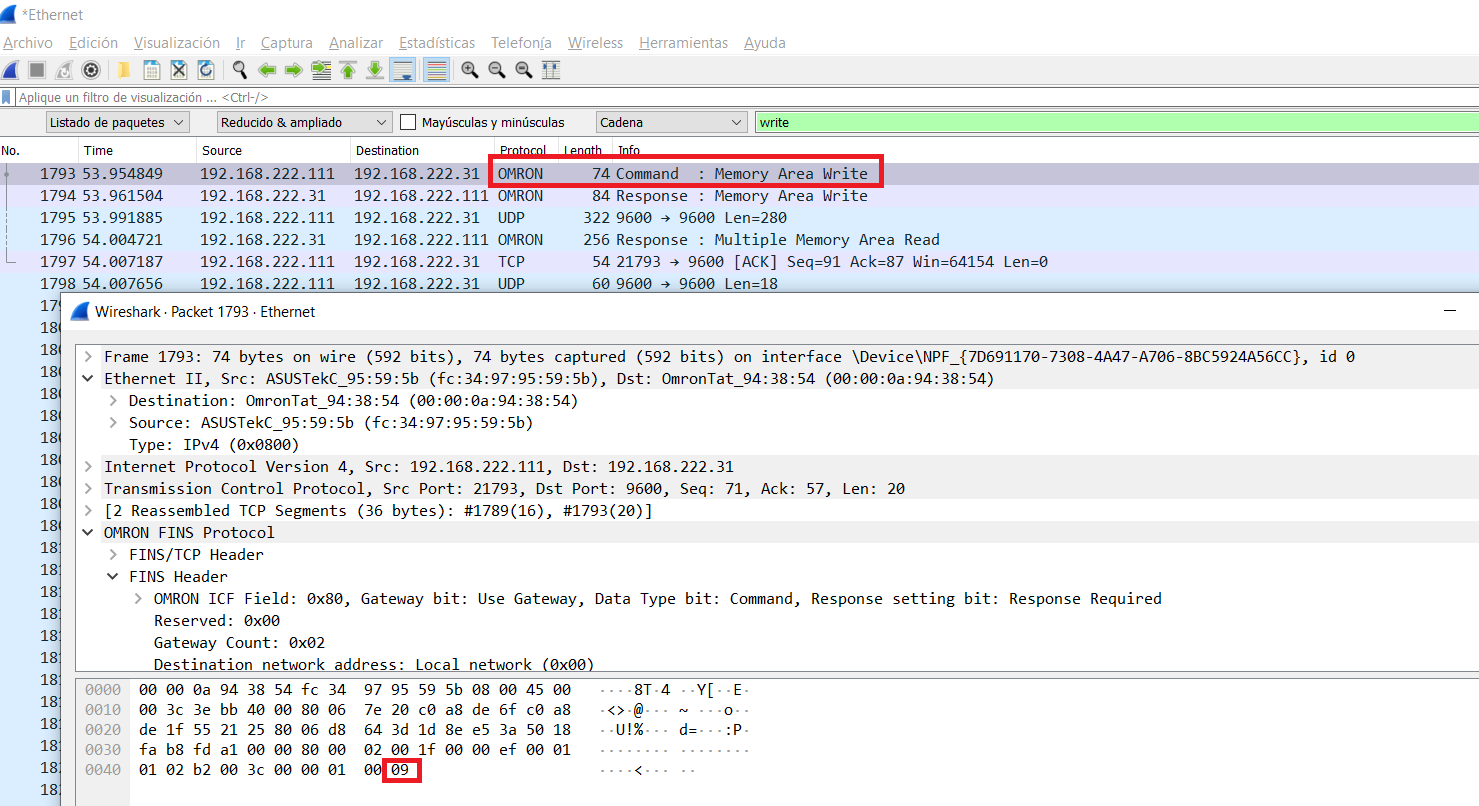




De manera parecida se puede escribir sobre las posiciones de memoria y mediante Wireshark visualizamos los datos de escritura.







**Demo 11 -Comunicaciones no seguras **

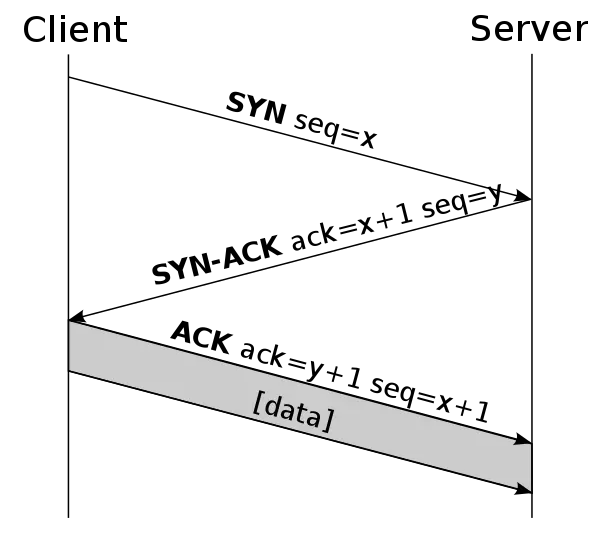
**SIEMENS**

La arquitectura de los sistemas de control industrial de Siemens consta de PLC Simatic S7 que se comunican con una estación de ingeniería TIA y SCADA HMI por un lado, y controlan los sistemas industriales por el otro lado. Se afirma que las versiones más nuevas de la arquitectura son seguras contra atacantes sofisticados, ya que utilizan protocolos y primitivos criptográficos avanzados.

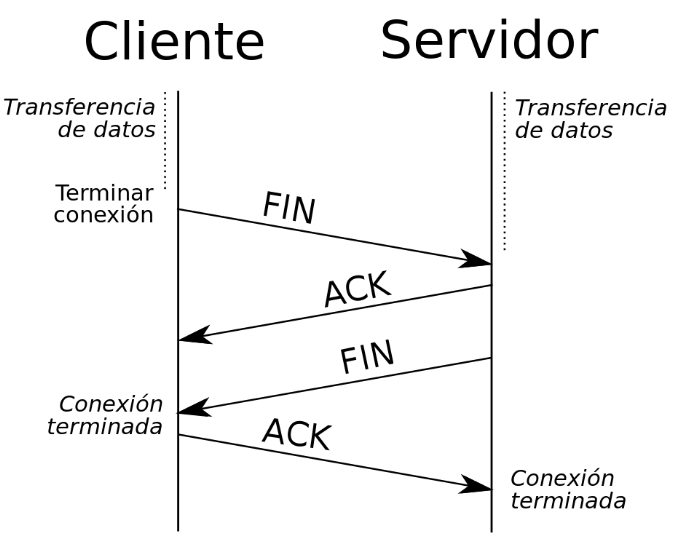
### Establecimiento de la conexión entre cliente y servidor, y desconexión en TCP

La principal característica del protocolo TCP es que es un **protocolo orientado a conexión**, para poder establecer una conexión entre cliente y servidor, es totalmente necesario establecer una conexión previa con dicho servidor.

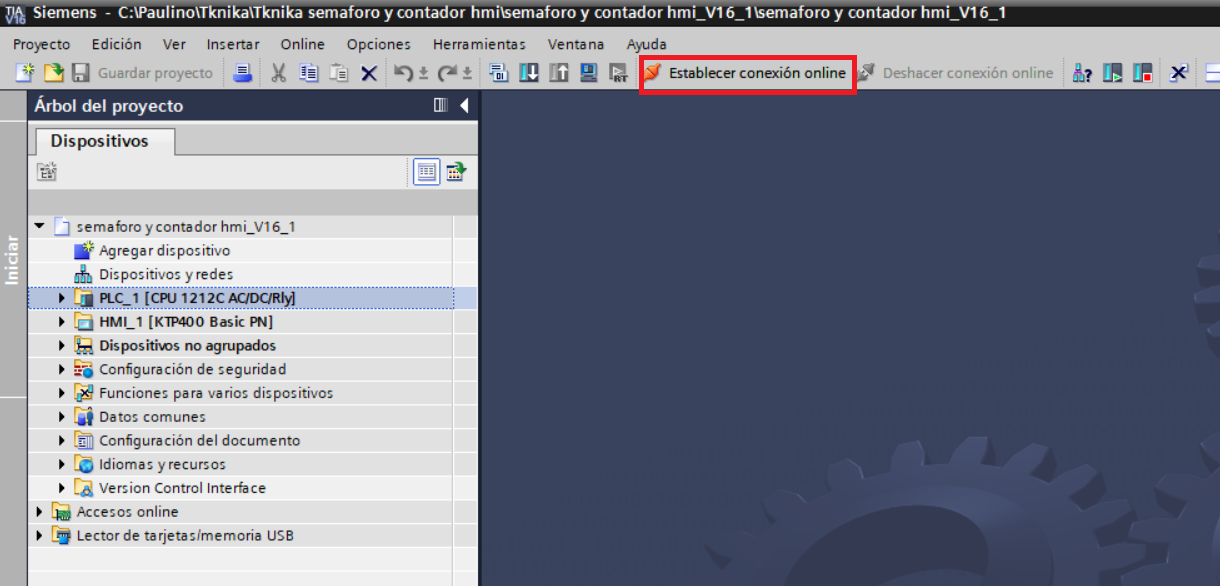
Esta conexión previa se denomina **3-way handshake**, y consiste básicamente en que el cliente (el que inicia la conexión) envía un mensaje SYN al servidor (el que recibe la conexión). Posteriormente, el servidor le enviará un mensaje de tipo SYN-ACK, indicando que puede empezar a enviar información, finalmente, el cliente envía un ACK indicando que lo ha recibido correctamente, y ya se empieza a enviar toda la información entre cliente y servidor de manera bidireccional.

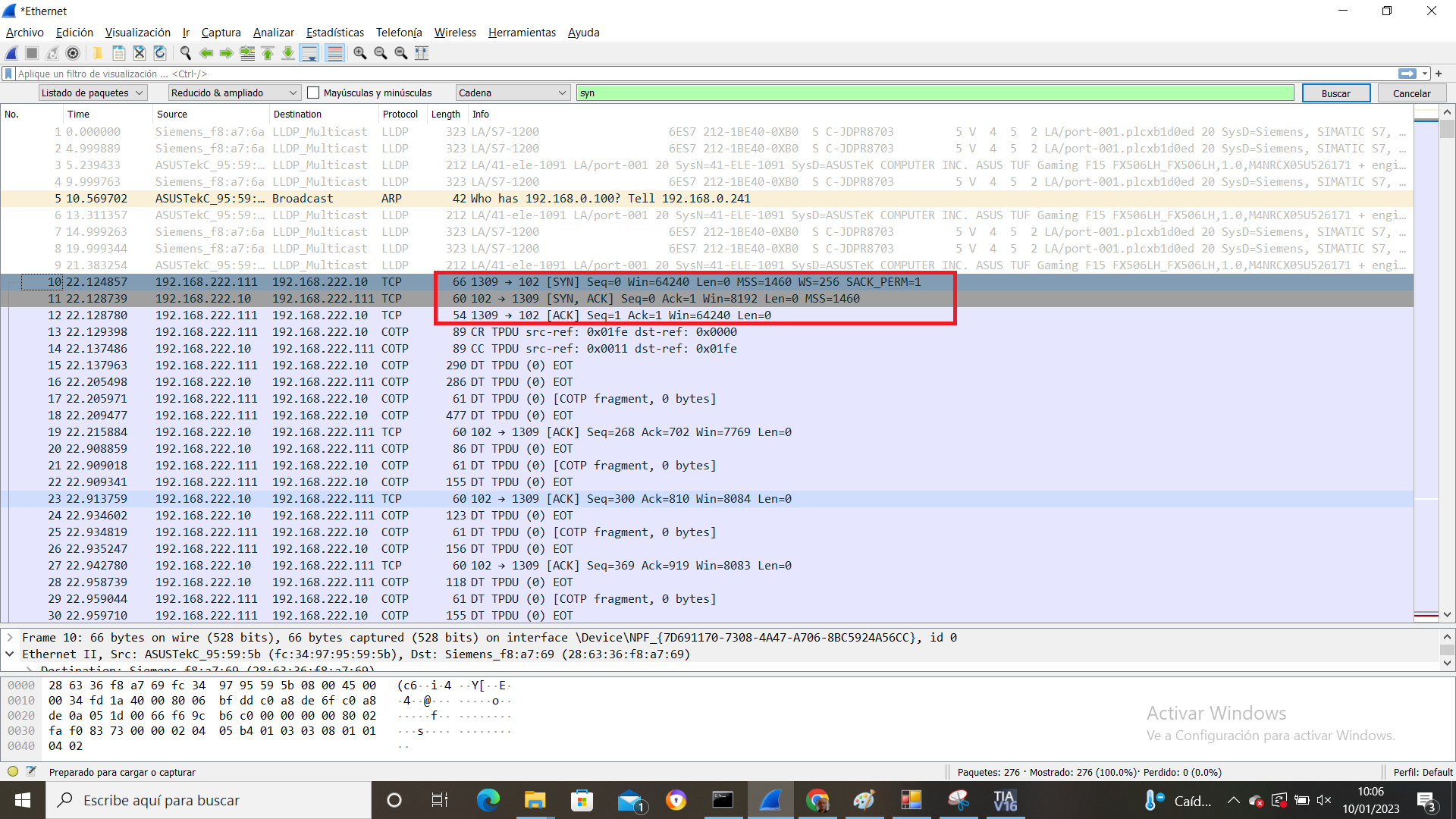


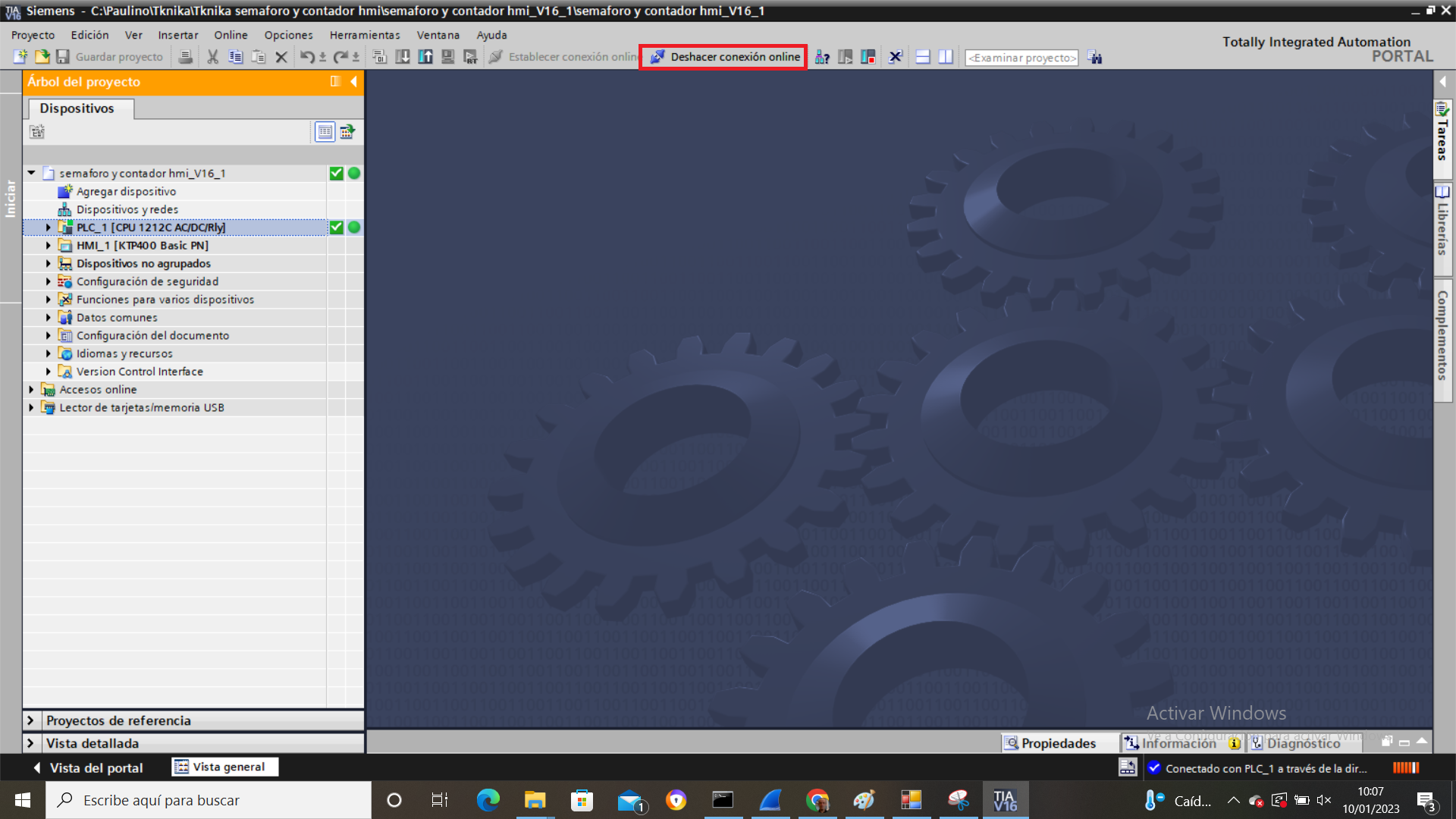
Para **finalizar la conexión**, el que quiere finalizar la conexión envía un mensaje FIN, y el host que lo recibe enviará un mensaje ACK junto con otro mensaje FIN, de tal forma que, el equipo que ha iniciado la finalización de la conexión, le envíe un último ACK y se cerrará el socket abierto.

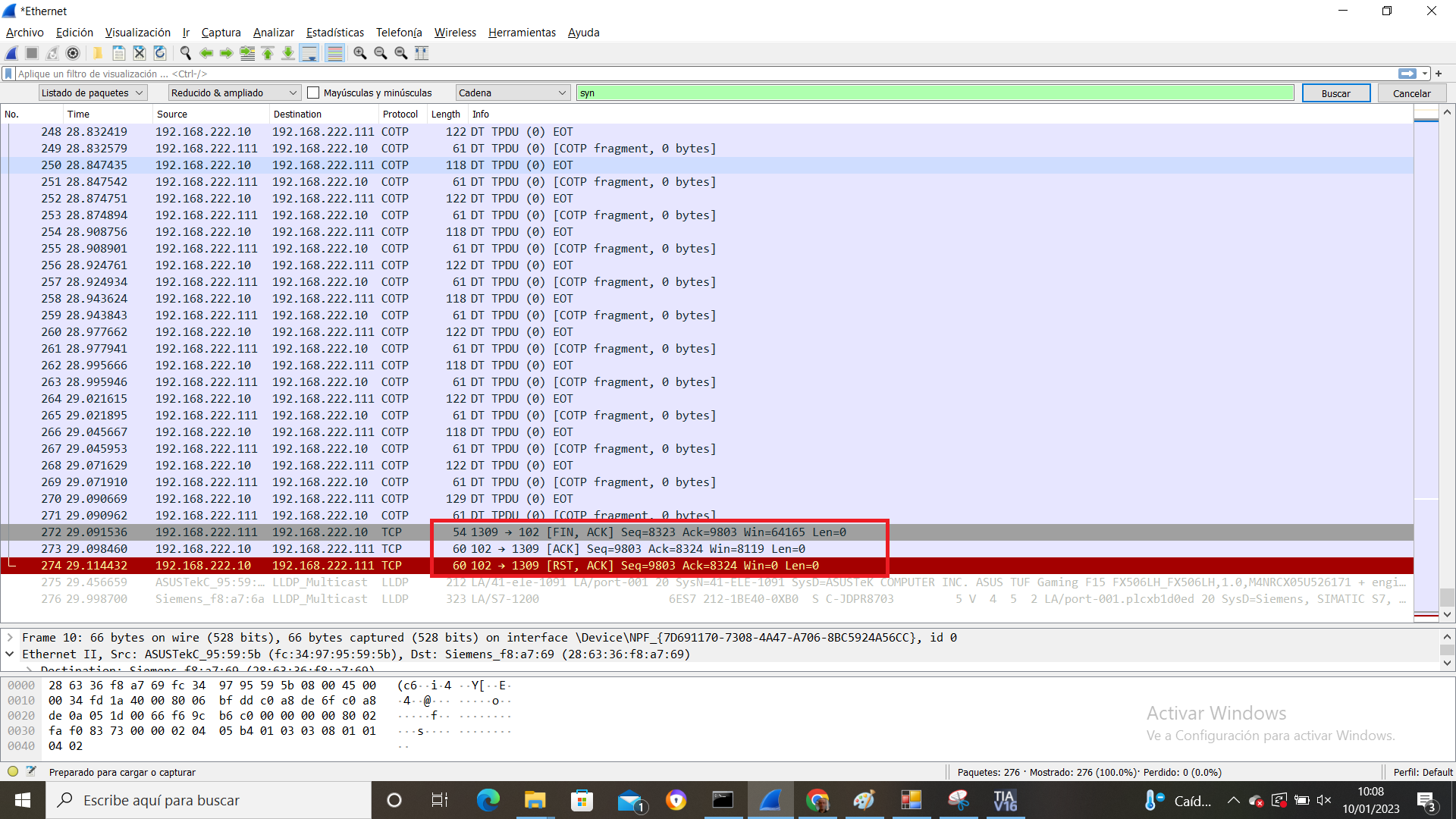


Este proceso se puede visualizar si ponemos Wireshark en captura durante la conexión y desconexión de Tia Portal y el PLC.









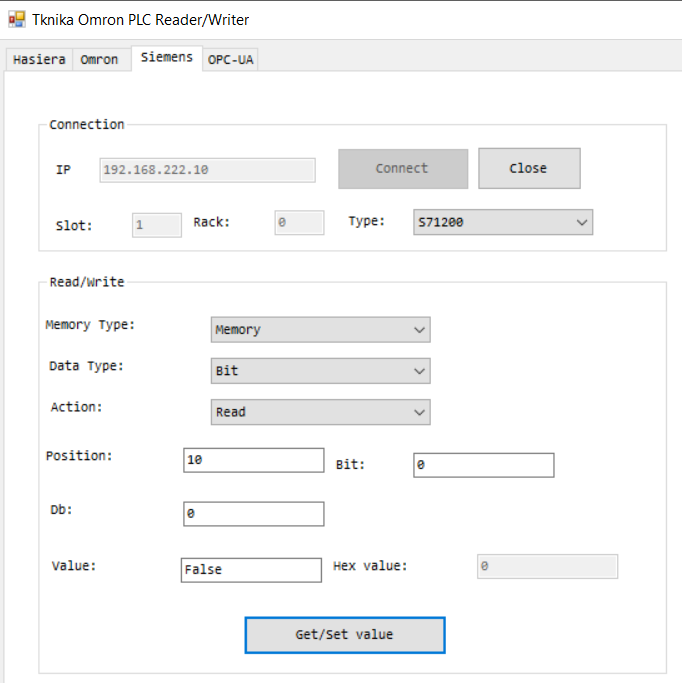
La integridad de los mensajes que intercambian los PLC TIA y S7-1500 está protegida por un código de autenticación de mensajes.Si realizamos acciones de parada o escritura sobre el PLC no visualizamos dichos eventos como ocurría con la comunicación Omron.

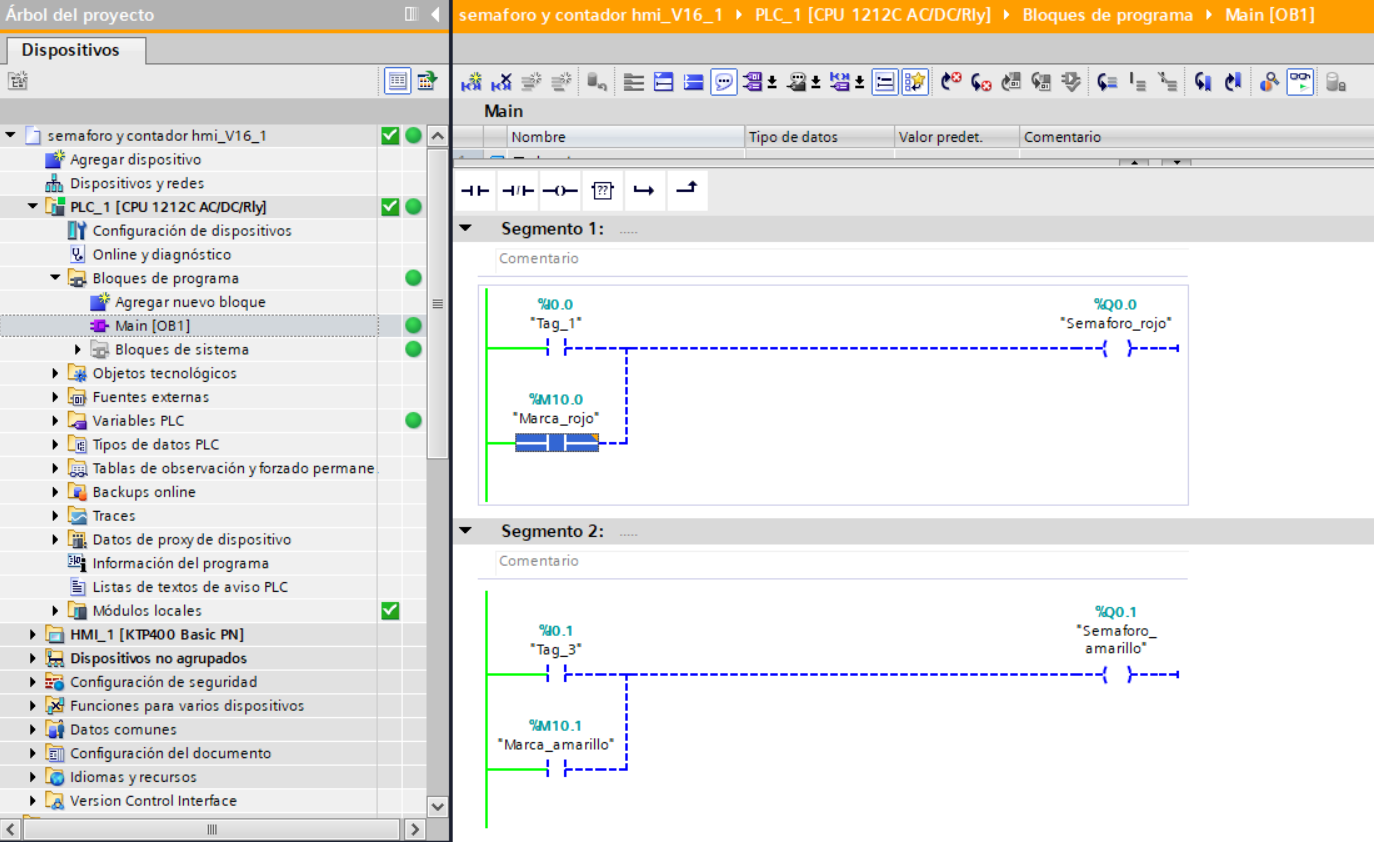


En este caso se utiliza el panel ejecutable para conectarse al PLC y realizar operaciones de escritura y lectura en la memoria y bases de datos DB.

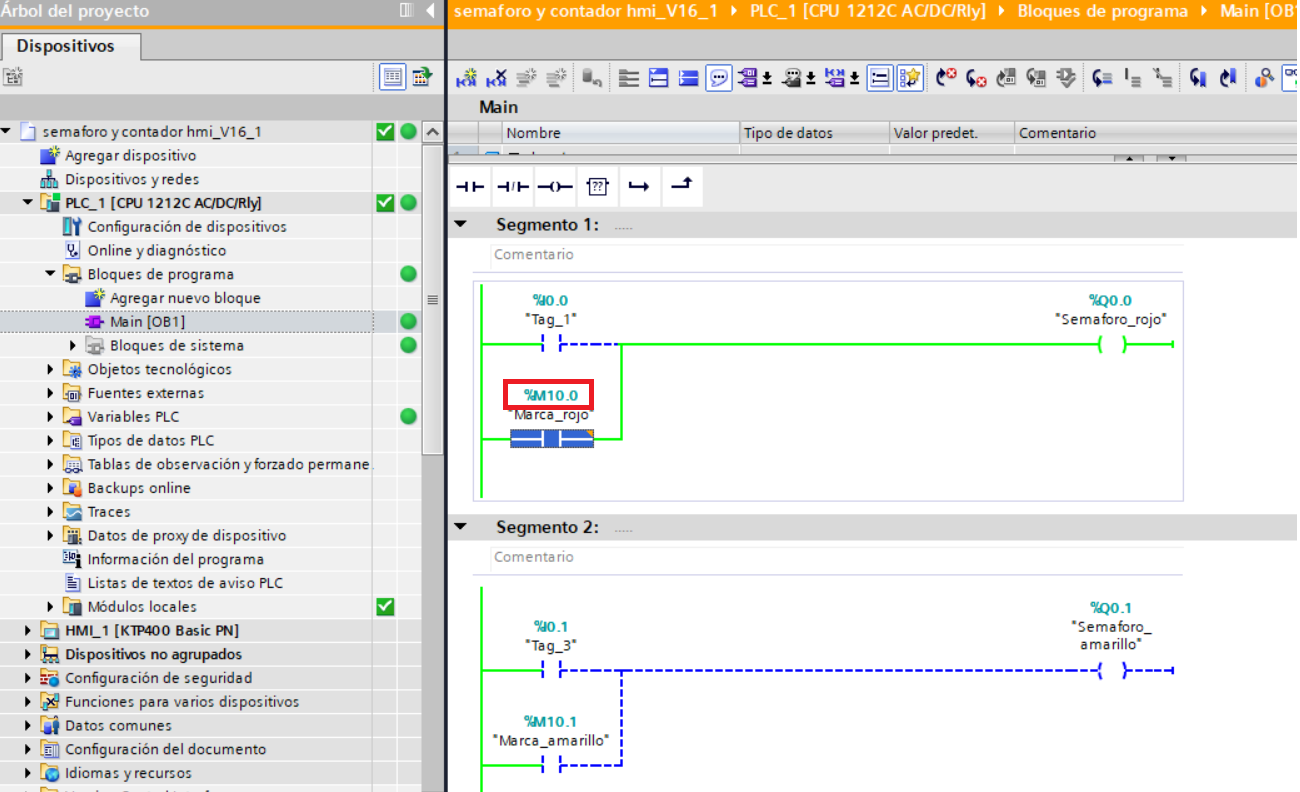
**PUT / GET tiene que estar habilitado en el PLC para permitir la conexión.**

Ejemplo de lectura/escritura sobre la marca M10.0 . La lectura inicial nos devuelve el valor “False”.

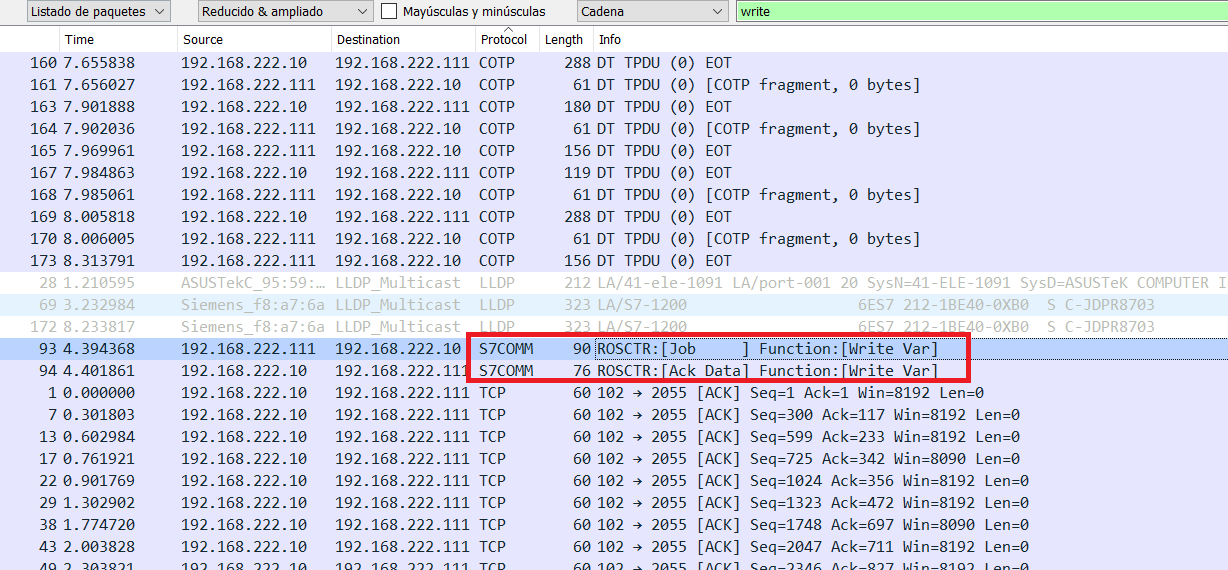


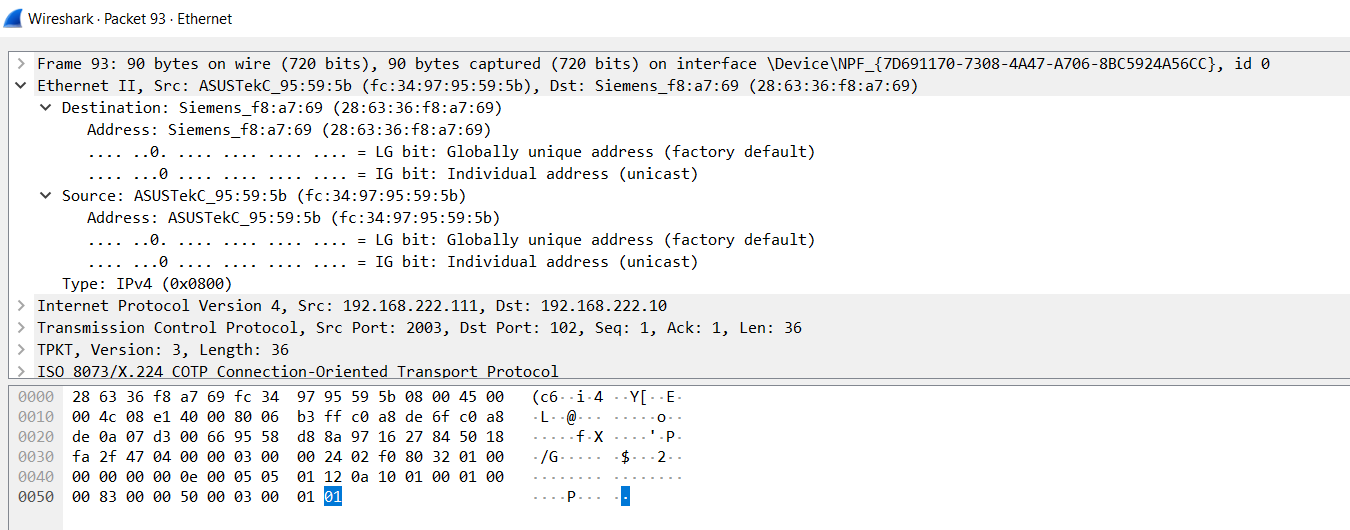


Podemos forzar el valor a “True” desde el panel poniéndolo en modo escritura “Write” activando la marca correspondiente.

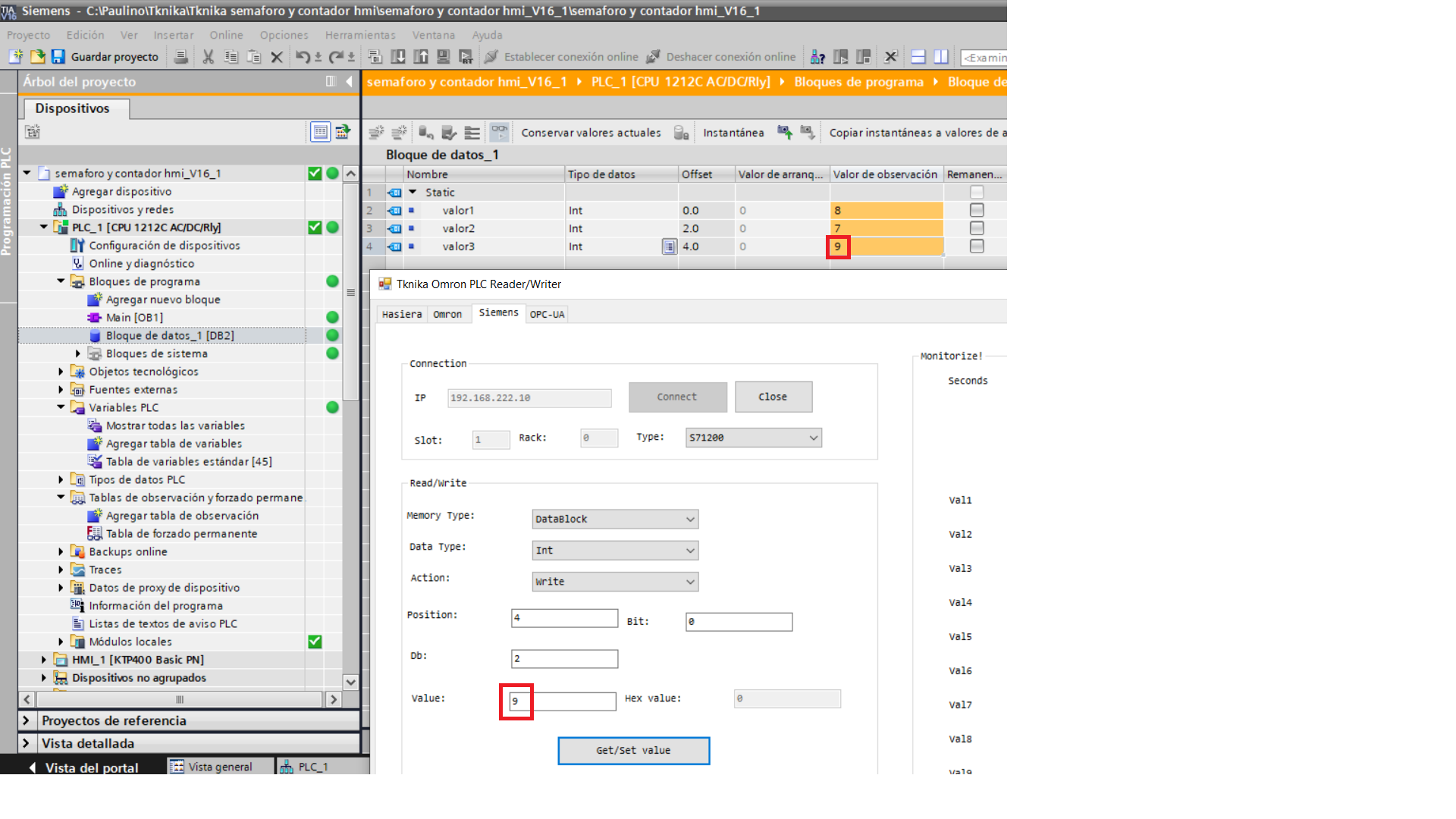


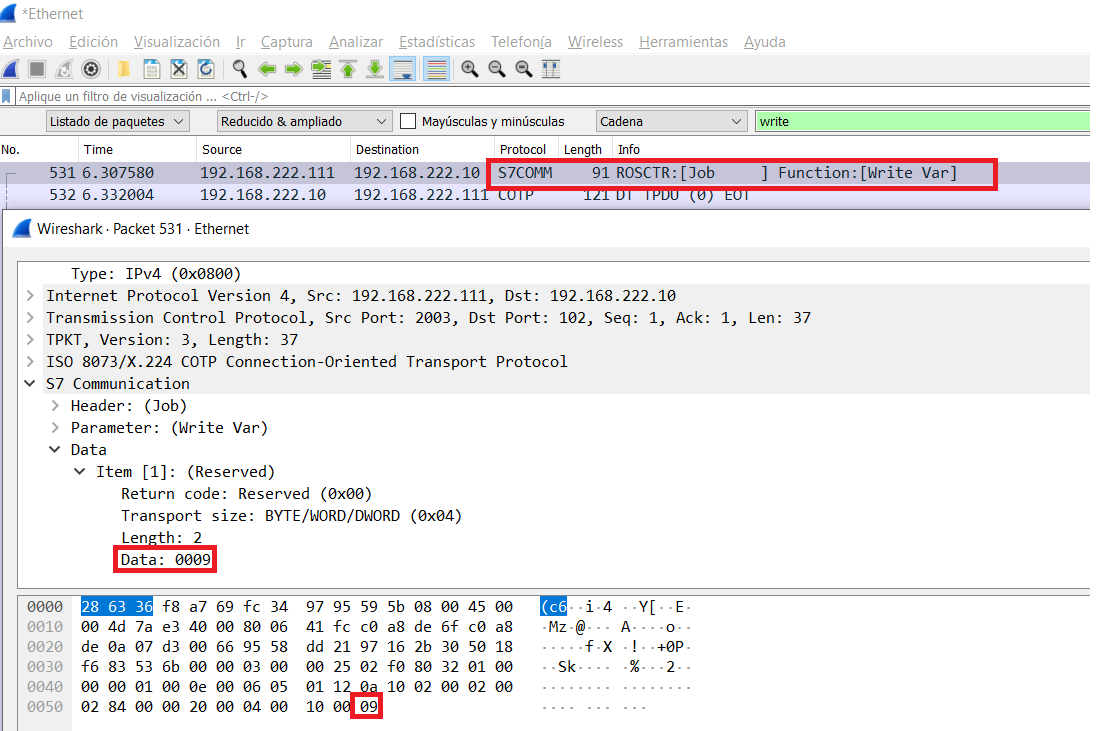
Este evento de escritura es visible poniendo Wireshark en captura de paquetes.



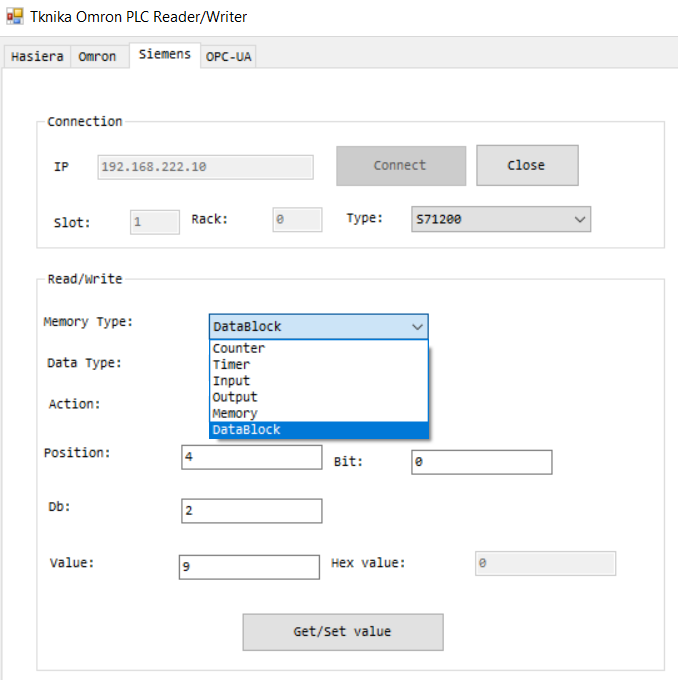


Podemos escribir sobre una DB ( En propiedades quitar acceso optimizado) . Por ejemplo: escribimos un 9 en DB2 para el valor2 (Posición 4.0) . La captura de Wireshark muestra el evento y el dato de escritura .



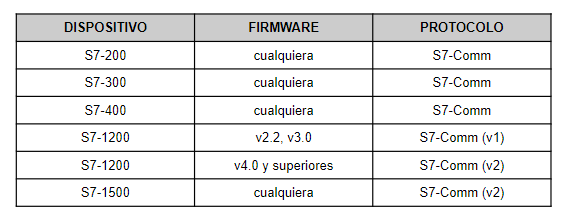


De manera similar podemos actuar sobre contadores,temporizadores…

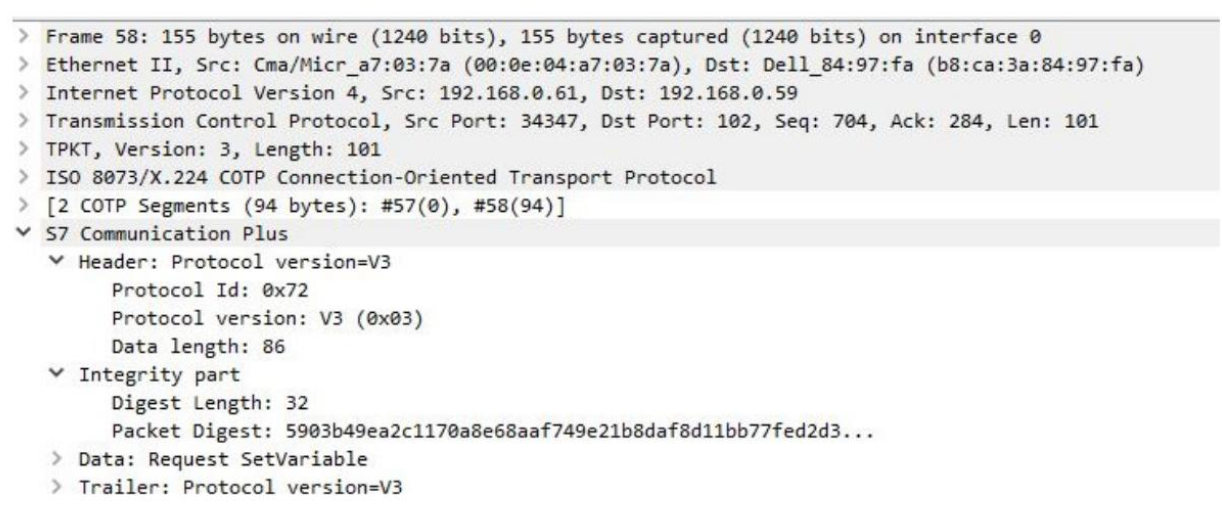


**Protocolo seguro?**

Dado que Siemens actualiza regularmente su software y firmware, es importante consultar las versiones de protocolo de las diversas versiones de firmware de TIA y PLC.De manera global se ha hecho la siguiente clasificación, según versiones de dispositivo, Firmware y protocolo:



La implementación TCP/IP del protocolo S7 se comunica a través del conocido puerto TCP 102. S7 funciona sobre el protocolo de transporte orientado a conexiones (COTP) y TPKT de ISO. Tanto TPKT como COTP agregan sus propios encabezados (dentro del segmento TCP). Así, el mensaje S7 se encapsula dentro del paquete COTP



Como se mencionó anteriormente, la integridad de los mensajes que intercambian los PLC TIA y S7-1500 está protegida por un código de autenticación de mensajes. Se calcula bajo una clave secreta (simétrica), que denominamos sessionKey, compartida entre el PLC y el TIA.

El protocolo de enlace se realiza en los primeros cuatro mensajes de una sesión, que realizan el establecimiento de la clave de sesión criptográfica. Todos los demás mensajes de la sesión (a partir del quinto mensaje) están entonces protegidos por integridad.

**Hay un estudio que muestra que incluso las últimas versiones de los dispositivos y protocolos siguen siendo vulnerables. Después de aplicar ingeniería inversa al protocolo criptográfico, se puede crear una estación de ingeniería no autorizada que puede hacerse pasar por TIA ante el PLC e inyectar cualquier mensaje favorable al atacante**.

**Rogue7: Rogue Engineering-Station ataque a S7 PLC Simatic**

<https://i.blackhat.com/USA-19/Thursday/us-19-Bitan-Rogue7-Rogue-Engineering-Station-Attacks-On-S7-Simatic-PLCs-wp.pdf>

<https://i.blackhat.com/USA-19/Thursday/us-19-Bitan-Rogue7-Rogue-Engineering-Station-Attacks-On-S7-Simatic-PLCs.pdf>