2019 年 3 月 13 日

株式会社日新システムズ サポートセンター

SISCO 社公開

Wire Shark Based Network Analyzer について

SISCO 社が KNOWLEDGE CENTER(https://www.sisconet.com/knowledge-center/)にて公開している Wireshark をベースにした「Wire Shark Based Network Analyzer」について本書で説明します。

本ツールは、Wireshark をベースに作成されているため、通常の Wireshark と同様の方法で使用することで、IEC61850 のパケットを解析することが可能になります。

本ツールは 32bit 版の Wireshark を基に作成されたものになります。そのため、既にご使用のパソコンに 32bit 版の Wireshark がインストールされている場合は、アンインストールを実施の上、本ツールをインストールしてください。

尚、64bit 版の Wireshark がインストールされている場合は問題なく、そのままインストールすることが可能です。

■ インストール手順

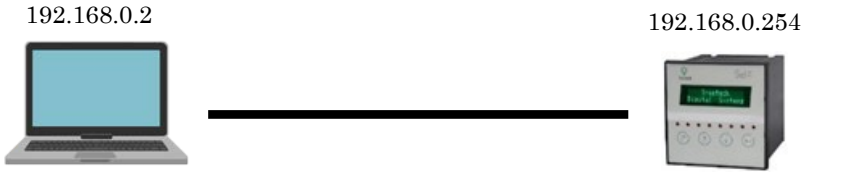
インストール手順は以下になります。

1. ダウンロードした Wireshark-win32-1.99.0-SkunkWorksIEC61850_02222017.exe を実行
2. Setup Wizard が起動するため、「Next」を選択
3. License Agreement が表示されるため、確認後「I Agree」を選択
4. Choose Components では「Next」を選択（デフォルトで問題ありません）
5. Choose Install Location にて、インストール先を選択し、「Next」を選択
6. Install WinPcap にて、「Install」を選択し、インストールを開始
   (途中、WinPcap の Setup Wizard が起動しますがデフォルトのまま実行してください)
7. Install Complete が表示されるので、「Next」を選択し、最後に「Finish」で終了

以上がインストール手順になります。基本的には一般的な Wireshark のインストール方法と同じです。

■ ツールの使用結果の比較

IEC61850 AX-SC4 のサーバとクライアントを用いて通信パケット情報を通常の Wireshark と本ツールでの解析結果の比較を記載します。



・AX-S4 61850 Explorer

・Wireshark Version 2.6.7

Or

Wire Shark Based Network Analyzer

AX-S4 61850 Server

本書で比較したパケットデータは上記の環境下において、クライアントからサーバに対する READ 要求時のパケットデータを各ツールでキャプチャした際の表示の違いを記載します。

パケット一覧部(Packet List)

Wireshark Version 2.6.7

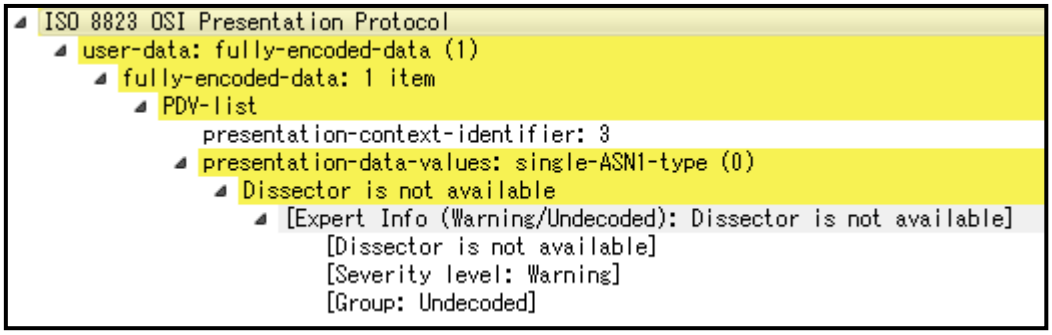
Source	Destination	Protocol	Length	Info
192.168.0.2	192.168.0.254	PRES	151	DATA TRANSFER (DT) SPDU

Wire Shark Based Network Analyzer

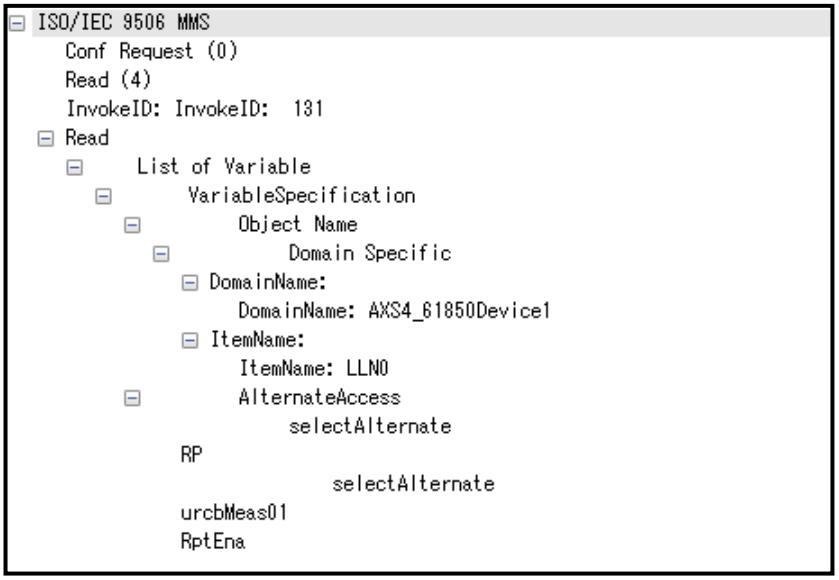
Source	Destination	Protocol	Length	Info
192.168.0.2	192.168.0.254	MMS	151	Conf Request: Read (InvokeID: 131)

MMS プロトコル部のパケット詳細部(Packet Details)

Wireshark Version 2.6.7



Wire Shark Based Network Analyzer



以上