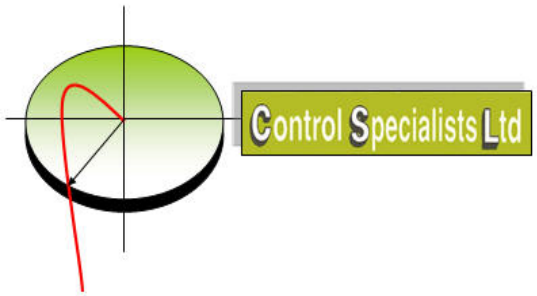
An Introduction to PROFINET Frame Analysis using

Peter Thomas
Control Specialists Ltd

www.controlspecialists.co.uk



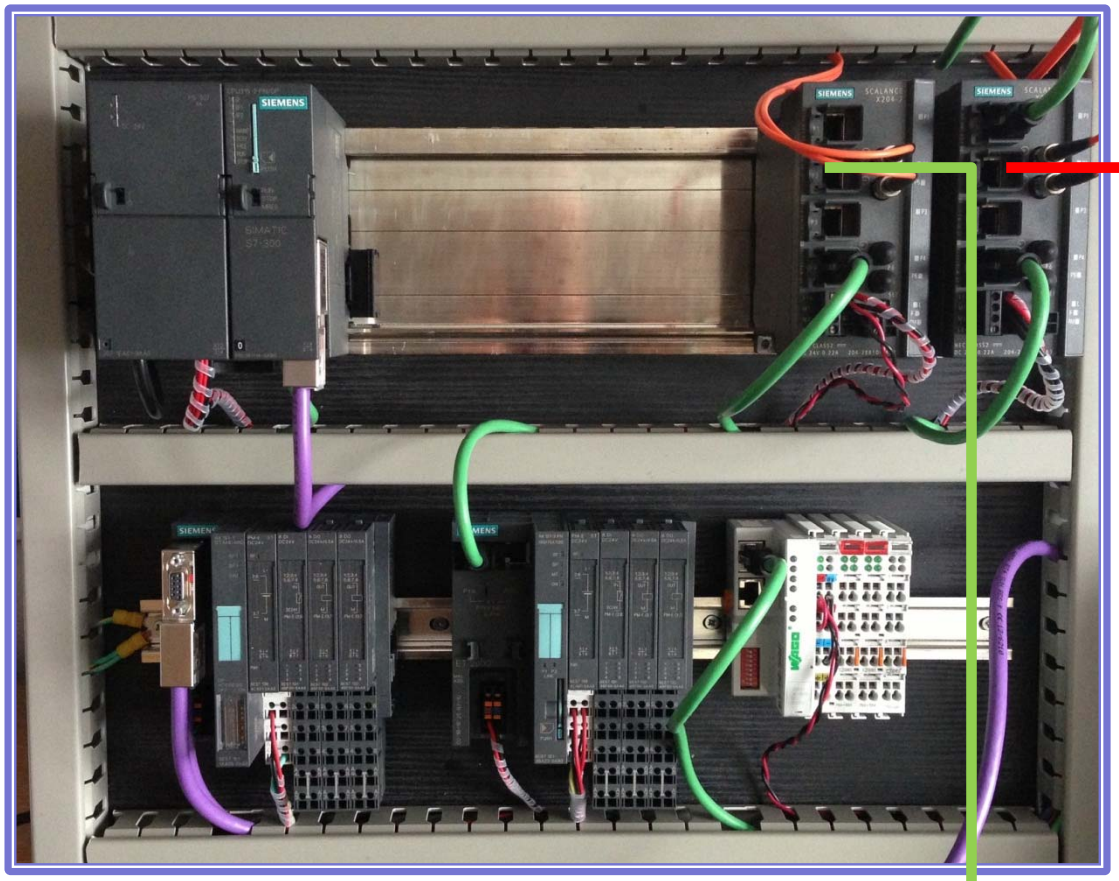
Objectives

- To gain an understanding of the way in which PROFINET devices communicate with one another over Ethernet.
- To learn how to capture the PROFINET Frames using Wireshark®.
- To analyse the captured frames to gain an understanding and purpose of the various protocols.
- This is a topic covered in more detail in the Certified Profinet Engineers Course

What is Wireshark?

- Wireshark® is a network protocol analyser. It lets you capture and interactively browse the traffic running on a computer network.
- It is not dedicated to Proifinet and as such cannot be compared to ProfiTrace.
- It is free to download and available from www.wireshark.org

Frame Capturing – Mirrored Ports



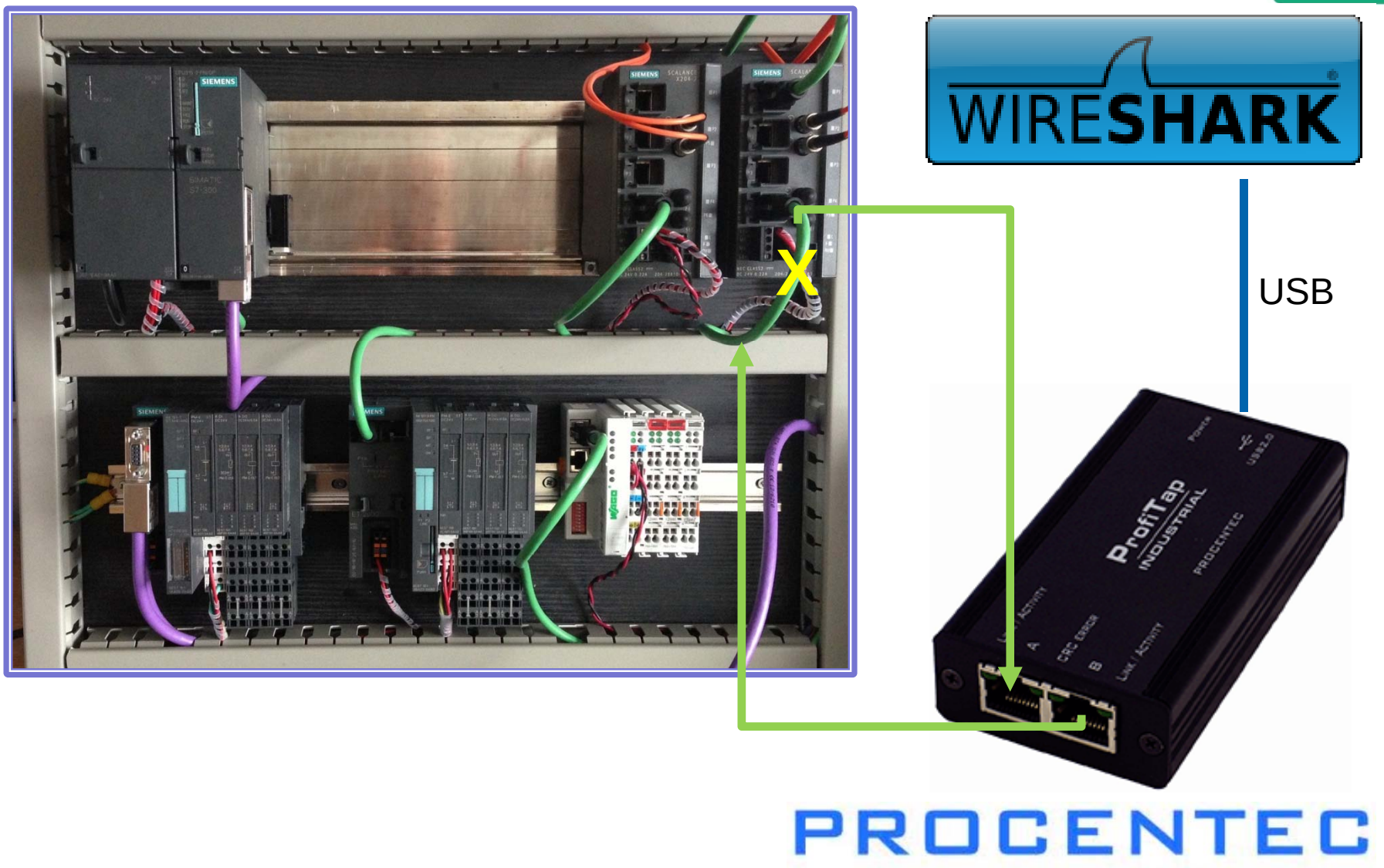
WIRESHARK

LAN LAN

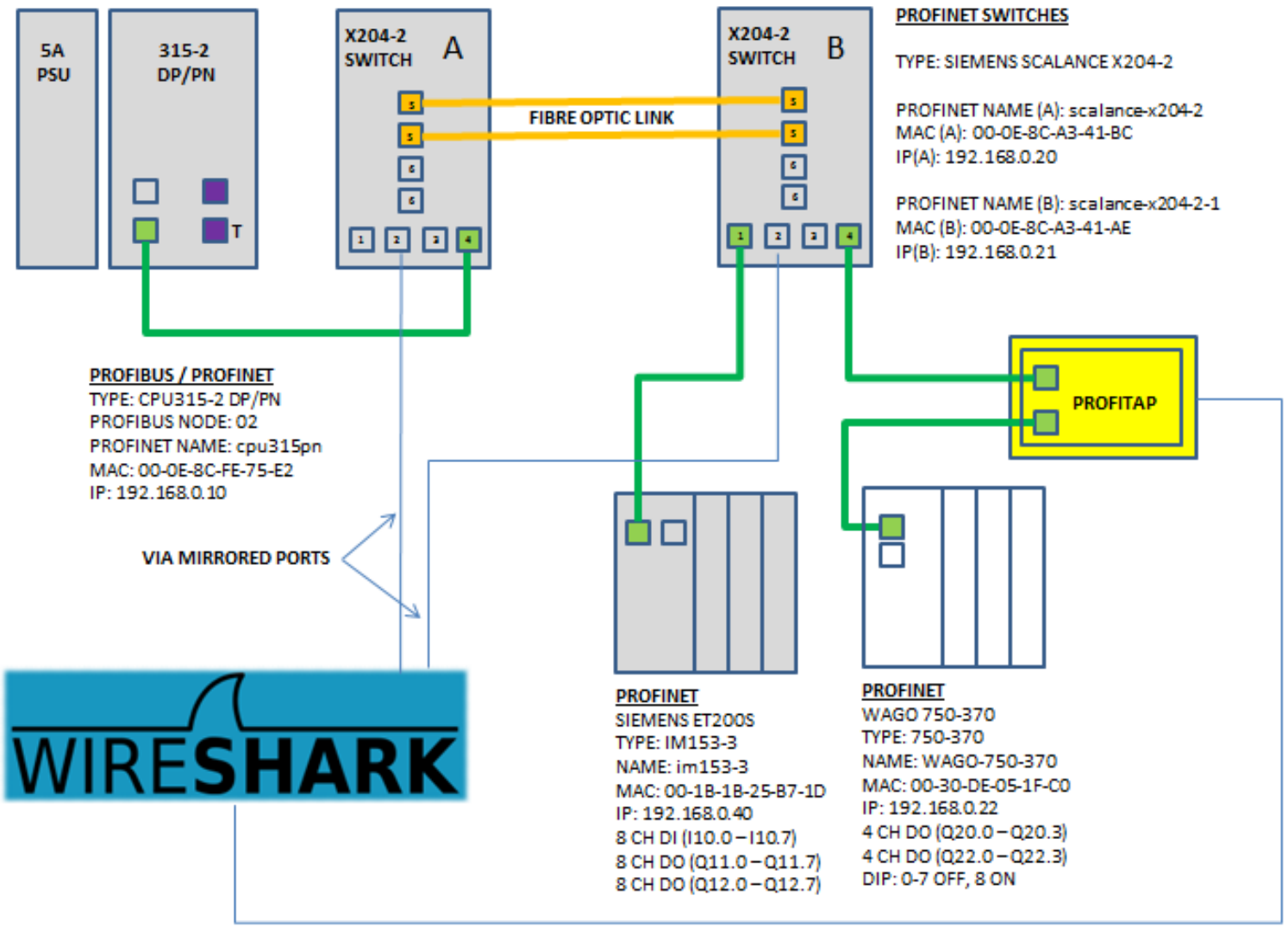
Switch B – Port 2
(IM153-3 ONLY)

Switch A – Port 2
(IM153-3 & WAGO)

Frame Capturing – ProfiTap



Frame Capturing Ports



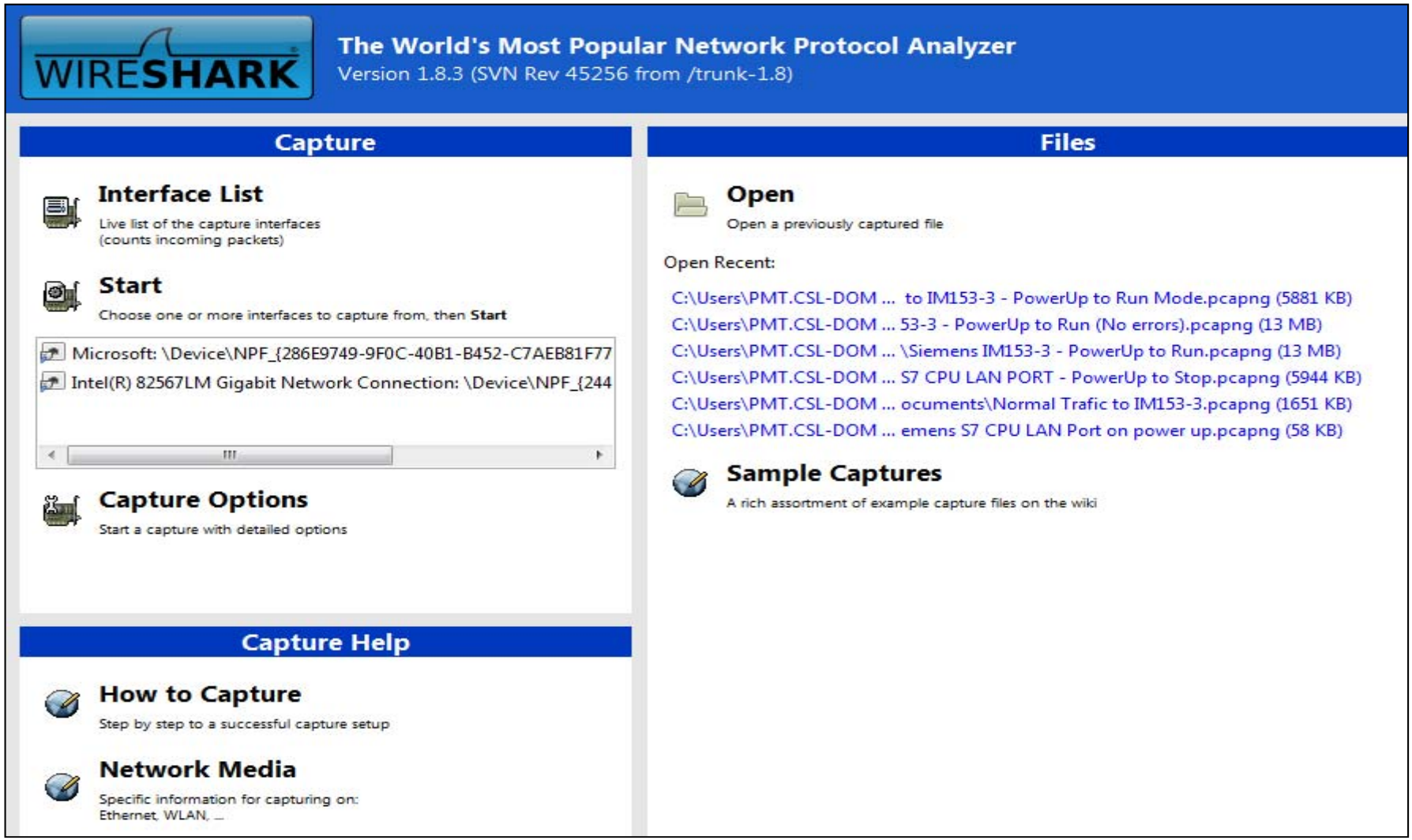
Scope of this workshop

- Wireshark® will be used to capture and analyse Profinet traffic during the following events:-
  - Start-Up
  - Data Exchange
  - Loss of Module
  - Loss of Communications
  - Duplicate Device Name

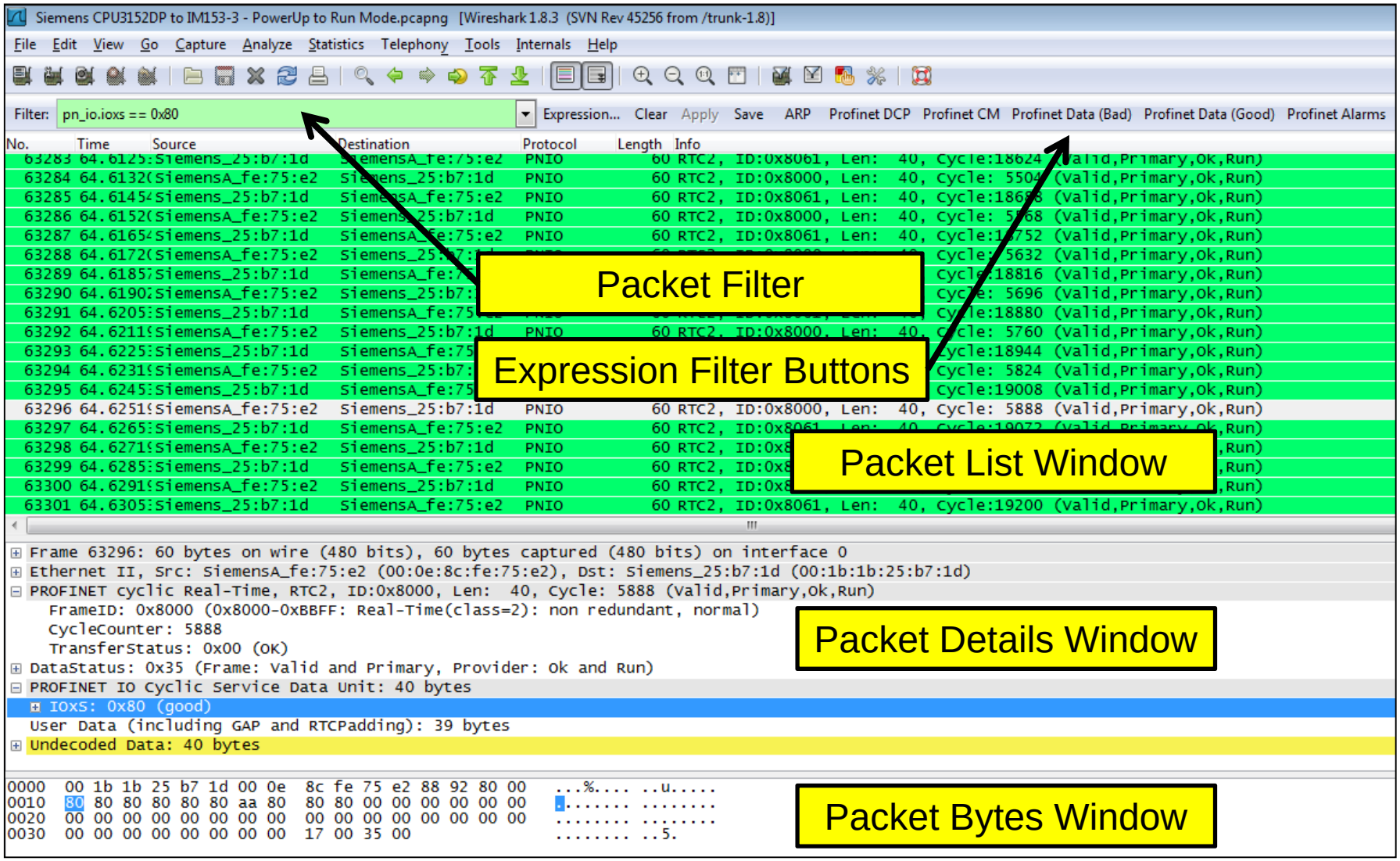
Equipment used in this workshop

- Siemens S7 PLC Hardware & Switches.
- Wago IO
- ProfiTap & Netilities from Procentec
- Wireshark® Network Protocol Analyser.

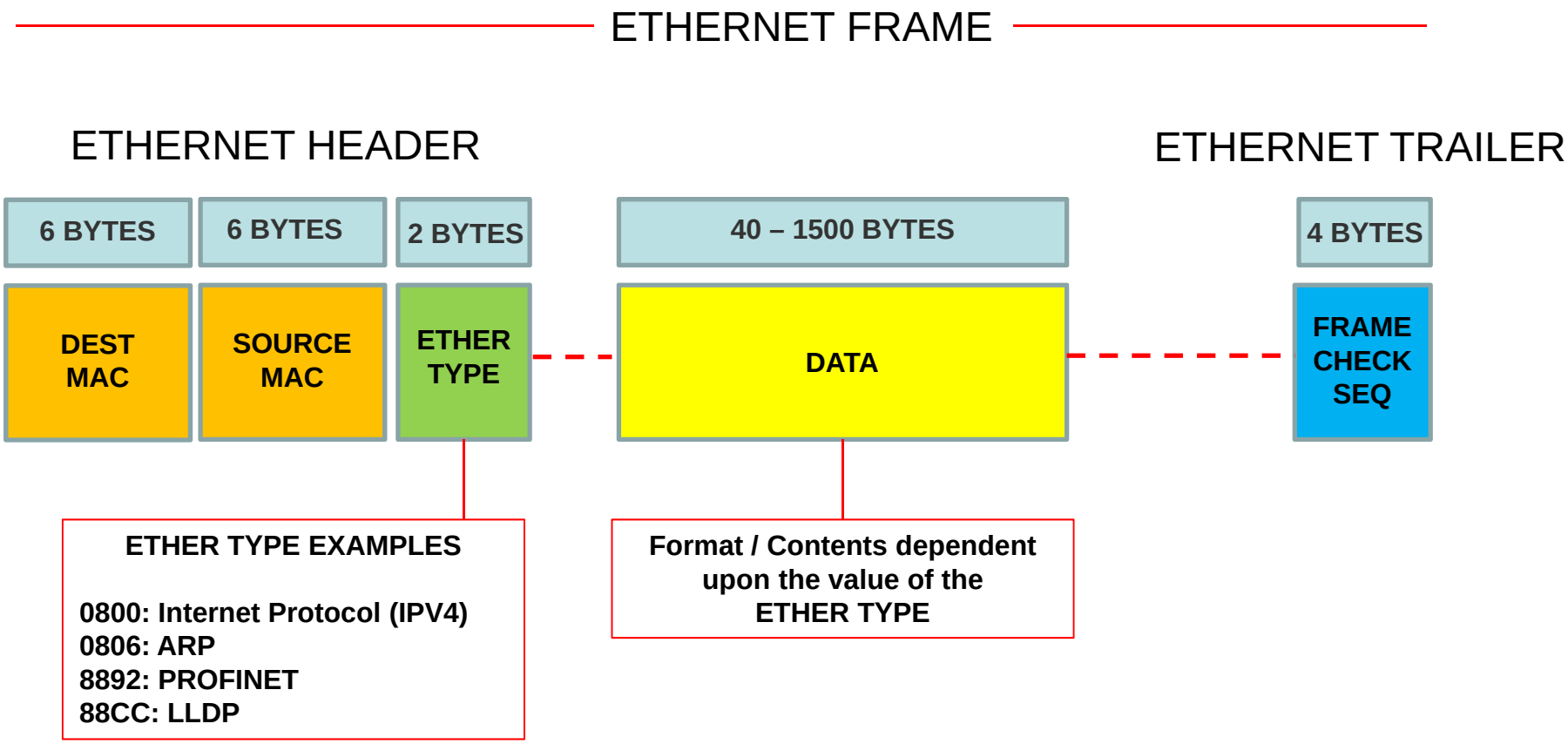
WIRESHARK - HomePage



WIRESHARK – Frame Analysis



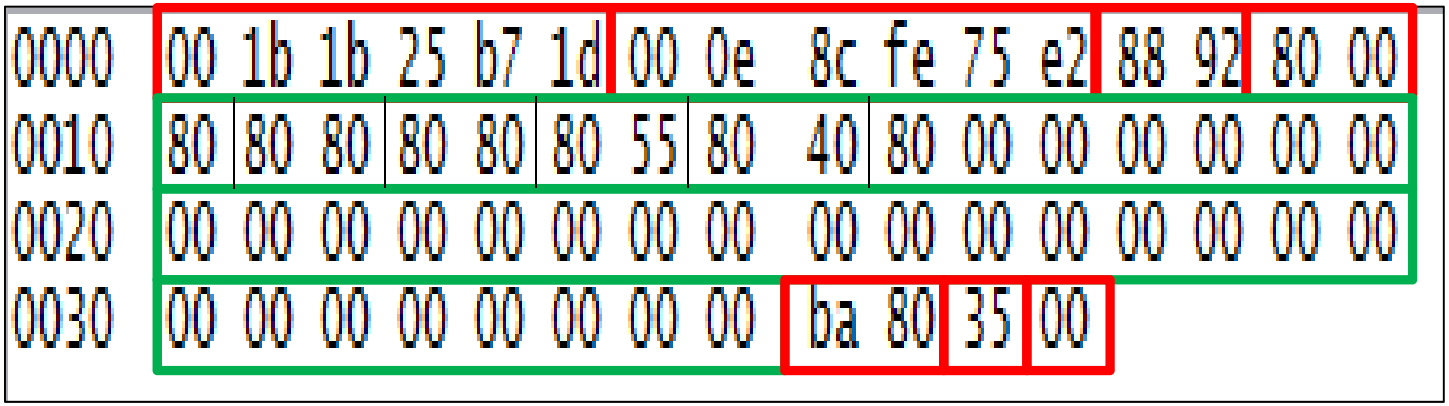
IEEE 802.3 EtherNet Frame



Note – VLAN Tags, IFG, Preamble and SFD bytes not shown.

Profinet Frame

SOURCE ADDRESS DESTINATION ADDRESS ETHERTYPE FRAME ID

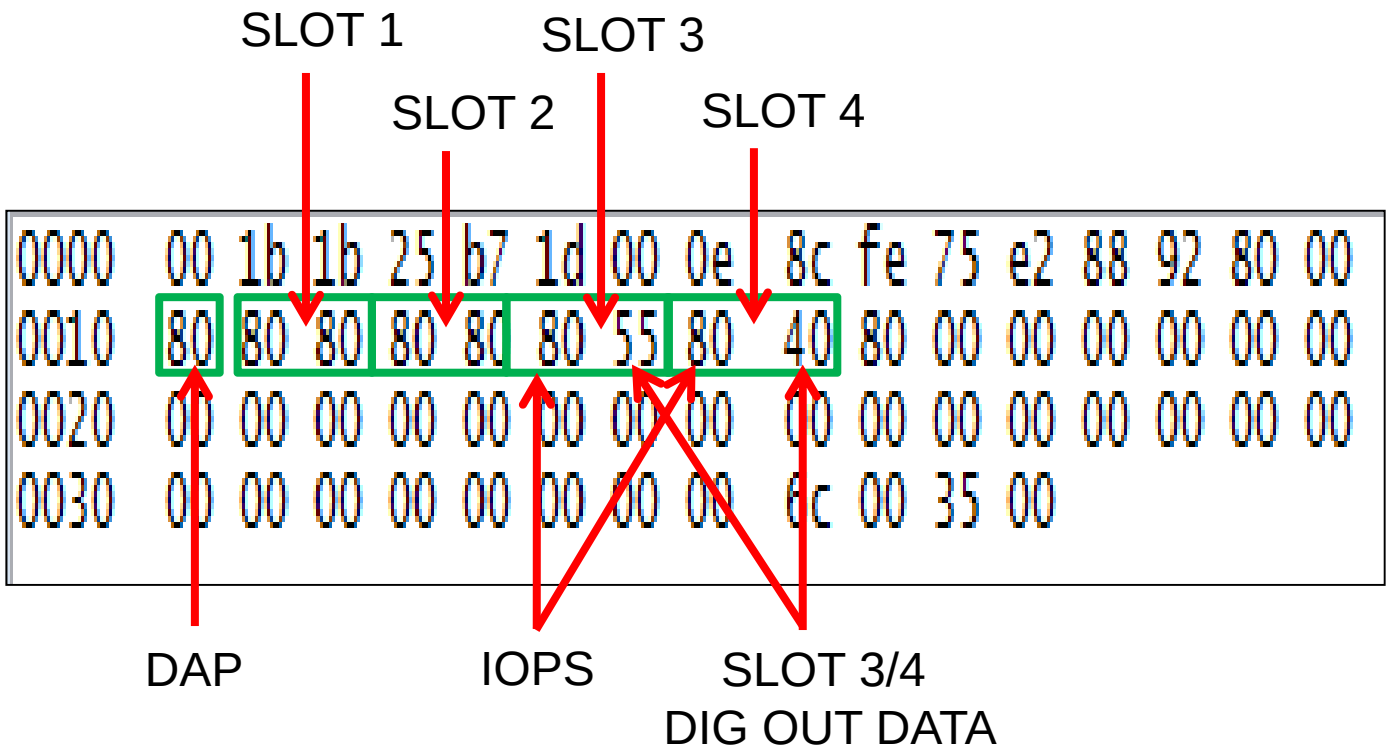


PROFINET IO DATA CYCLE COUNTER DATA STATUS TXFR STATUS

-- APPLICATION PROTOCOL DATA UNIT STATUS --

ETHERTYPE 8892 = PROFINET, FRAME ID 8000 = REAL TIME CLASS 2

Profinet Frame (CPU to OUTPUTS)



DAP = DEVICE ACCESS POINT (IO DEVICE STATUS) 00 = BAD, 80 = GOOD

IOPS = IO PROVIDER STATUS (DATA STATUS @ CPU) 00 = BAD, 80 = GOOD

Common Protocols

- PNIO-DCP – Name / IP Address Assignment
- PNIO-CM – Start-up Services.
- PNIO – Cyclic IO Data Exchange

- PN-PTCP – Time Syncronisation
- PNIO-AL – Acyclic Alarms / Events

- ARP – IP Address – MAC Address Lookup
- LLDP – Device Identity & Properties.

Protocol Usage: Start-up to Data Exchange

*** DEVICE NAME ASSIGNMENT**

Device Names can be set up Manually, prior to connecting to the network, or Automatically on power-up.

Manual name assignment uses PNIO-DCP and tools such as the Primary Set-Up Tool from Siemens or Netilities from Procentec.

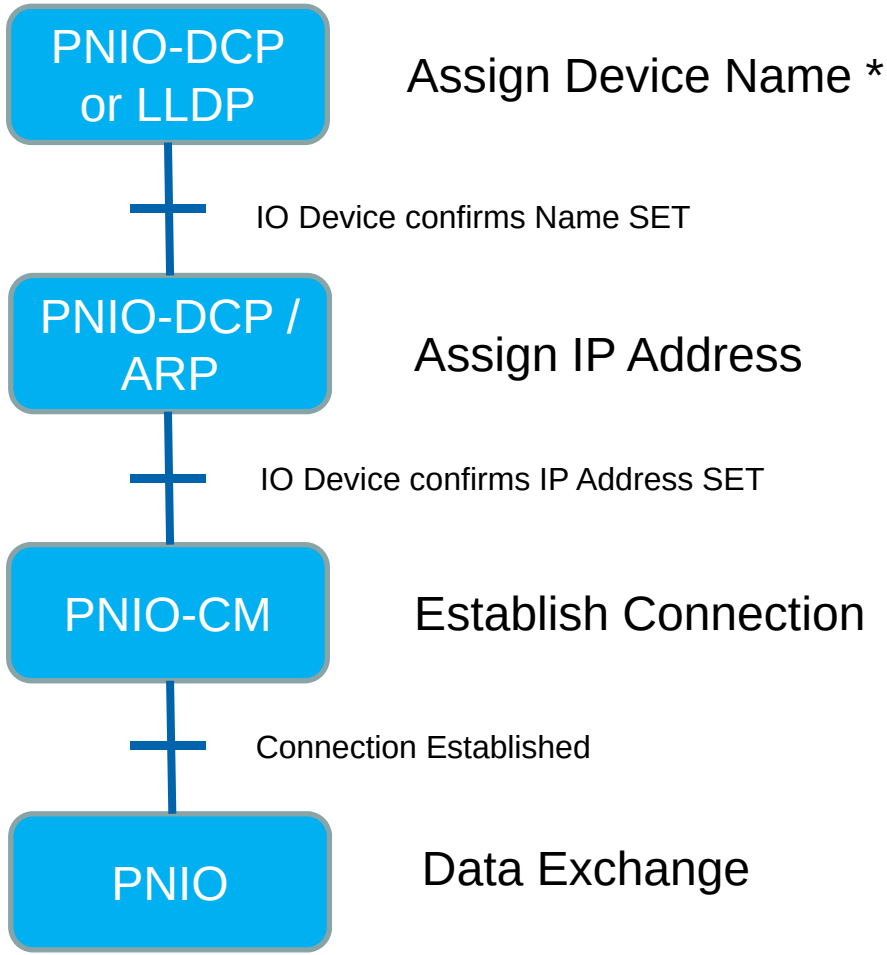
Automatic name assignment uses the LLDP protocol and requires the use of a Profinet Topology Configuration Tool.

SIEMENS

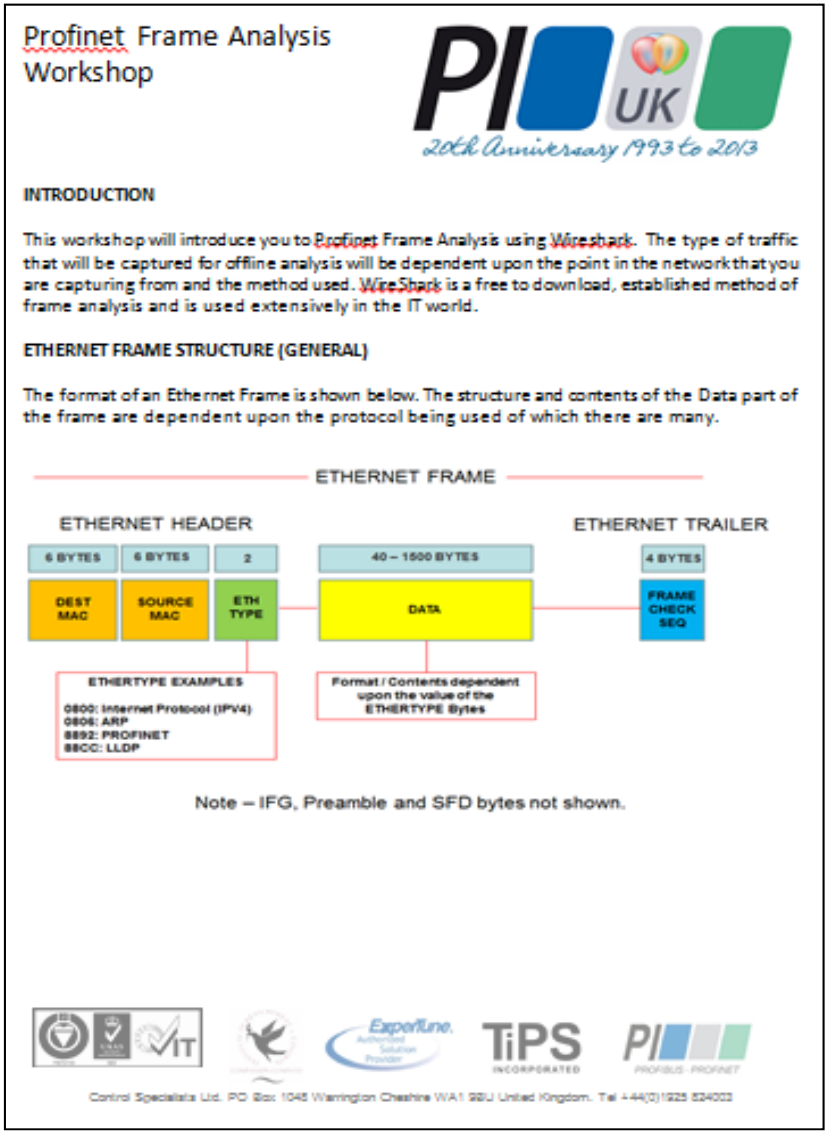
Primary Setup Tool

NET ILITIES

PROCENTEC



Practical Workshop



Profinet Frame Analysis Workshop

PI UK 20th Anniversary 1993 to 2013

INTRODUCTION

This workshop will introduce you to Profinet Frame Analysis using Wireshark. The type of traffic that will be captured for offline analysis will be dependent upon the point in the network that you are capturing from and the method used. WireShark is a free to download, established method of frame analysis and is used extensively in the IT world.

ETHERNET FRAME STRUCTURE (GENERAL)

The format of an Ethernet Frame is shown below. The structure and contents of the Data part of the frame are dependent upon the protocol being used of which there are many.

Note – IFG, Preamble and SFD bytes not shown.

Control Specialists Ltd. PO Box 1045 Warrington Cheshire WA1 9BU United Kingdom. Tel 44(0)1925 824003

- Step-by-Step Guide
- Overview