
# Network Protection for Energy Control Systems

# CSP004_C_E

PRESENTATION BY:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
**AIT AUSTRIAN INSTITUTE OF TECHNOLOGY**

# Network Protection for Energy Control Systems

**These slides outline the essential offensive tools that will be used in this course.**

These tools are intended for use within this course to demonstrate how different tools can be employed for various cyberattack activities and address existing security weaknesses to avoid or mitigate related cyber risks. Therefore, all these practical activities are solely intended for educational purposes ONLY and not for any other malicious or unauthorized activities.

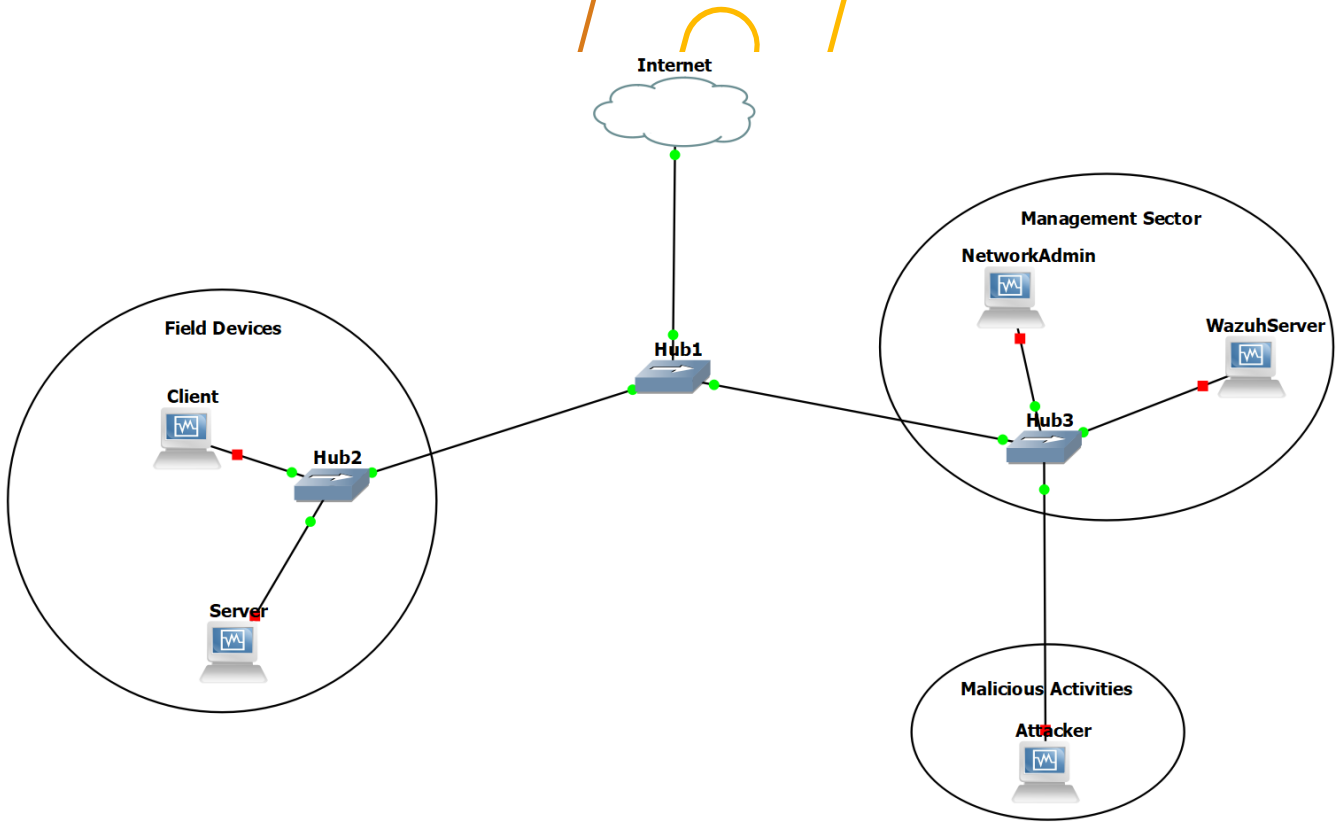
# GNS3 Simulator

# GNS3 Simulator

- **Field Devices**
  - Raspberry Pi running lightweight Linux version (Client and Server) for transmitting data over ModBus communication protocols using the pyModbusTCP.

- **Management Sector**
  - Network administration device for monitoring network traffic using Kali Linux.
  - Wazuh Server: Details to be addressed later.

- **Malicious Activities**
  - Kali Linux will be used to simulate various malicious activities targeting devices within this closed network.




Getting Started with GNS3 | GNS3 Documentation

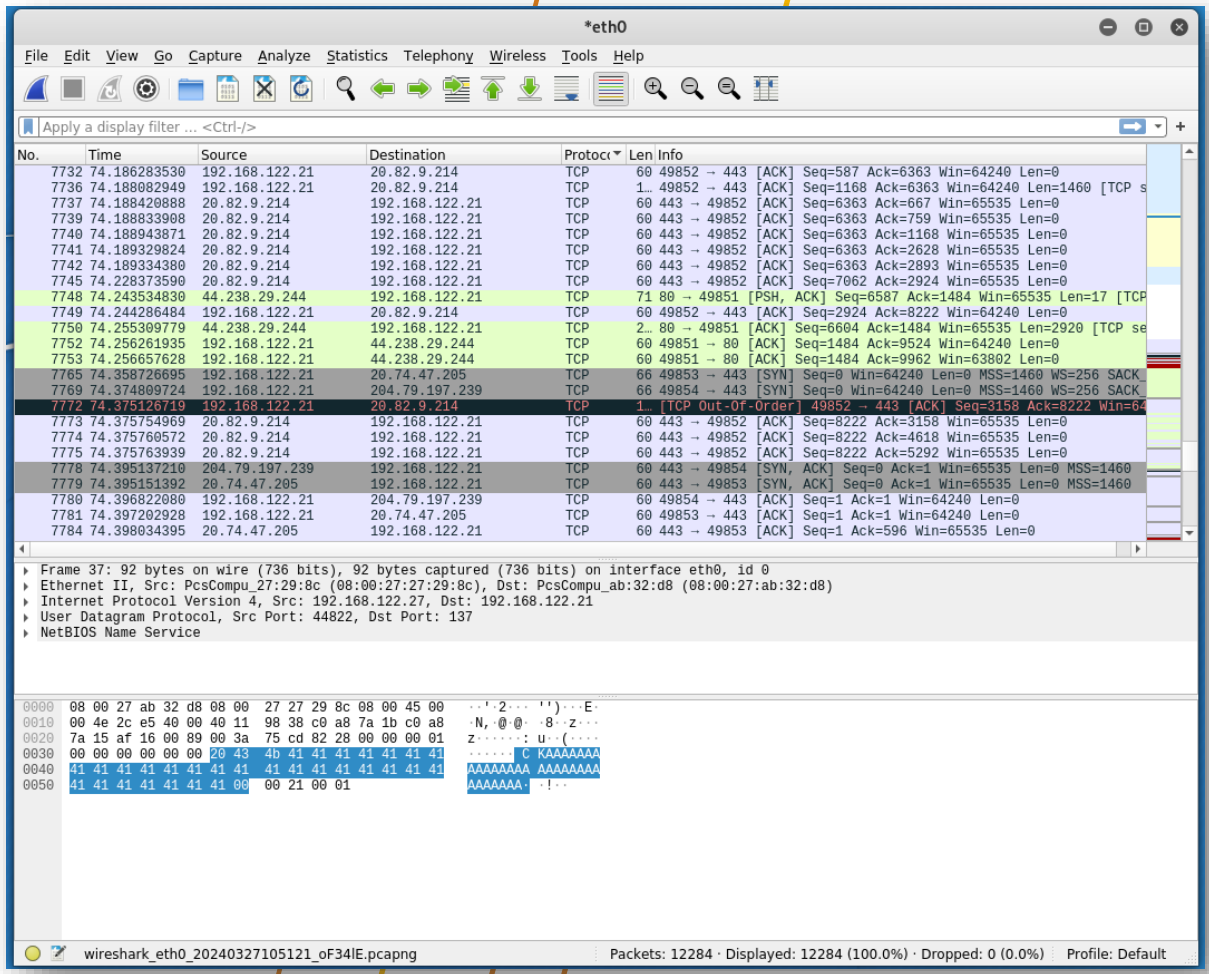
# Offensive Tools

## Wireshark

# Wireshark Sniffing & Packets Analysis

- **Wireshark** is a network protocol **analyzer** designed to help network **administrators** keep track of what is **happening** in their network.
- When you **become** an **MITM**, the **Wireshark tool** can be used to **sniff** and **analyze** traffic **sent** and **received** by the targets.

**Green** – TCP packets
**Dark blue** - is DNS packet
**Black** – TCP packets that have an issue

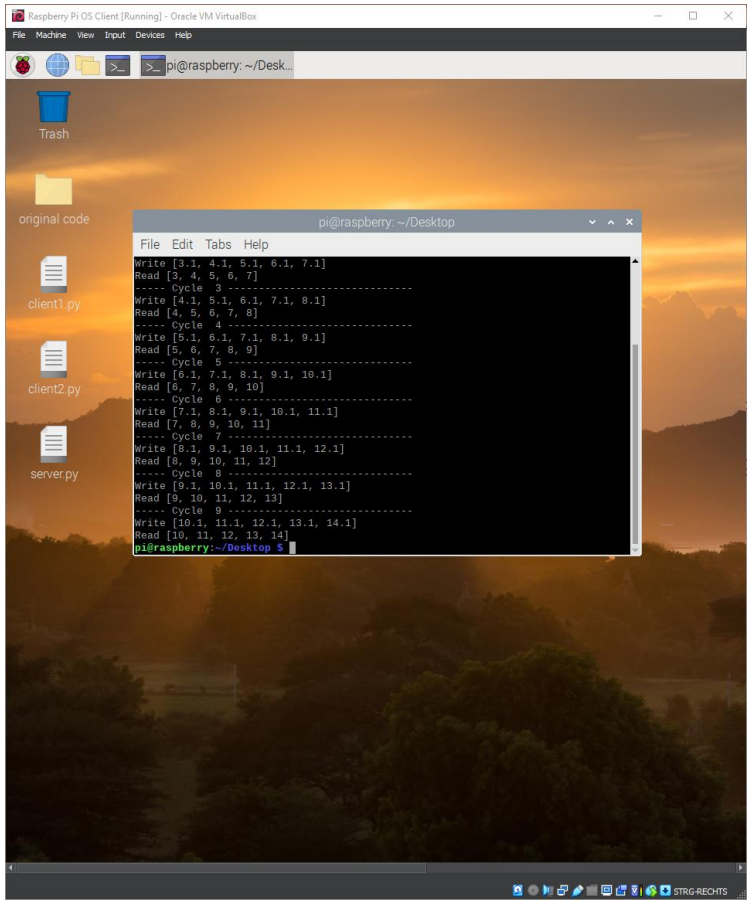


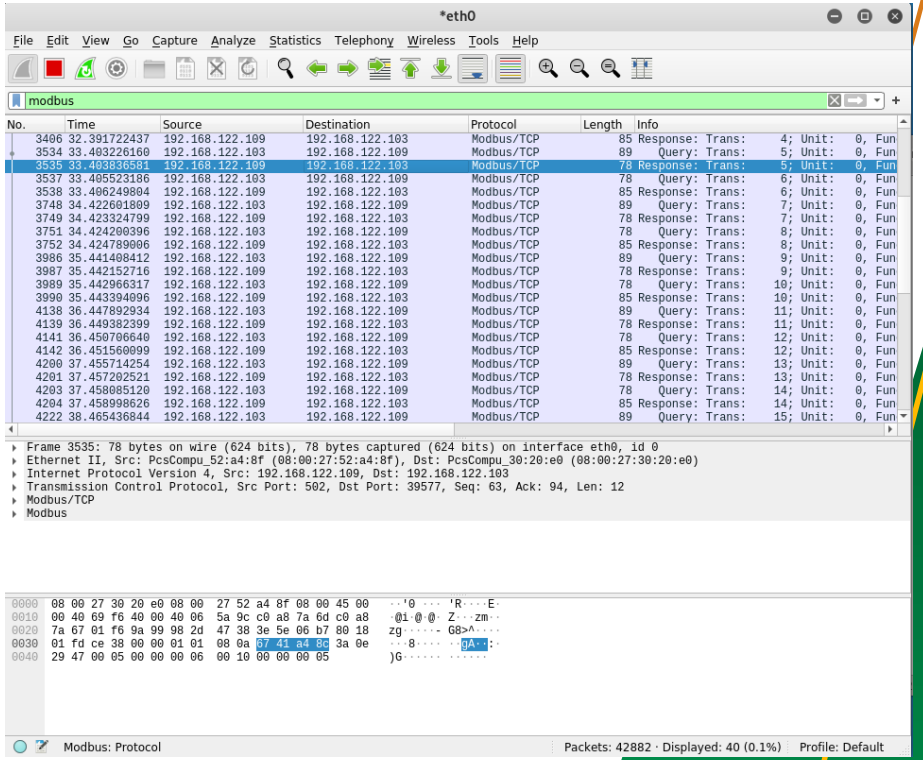
# Wireshark – Client/Server Example

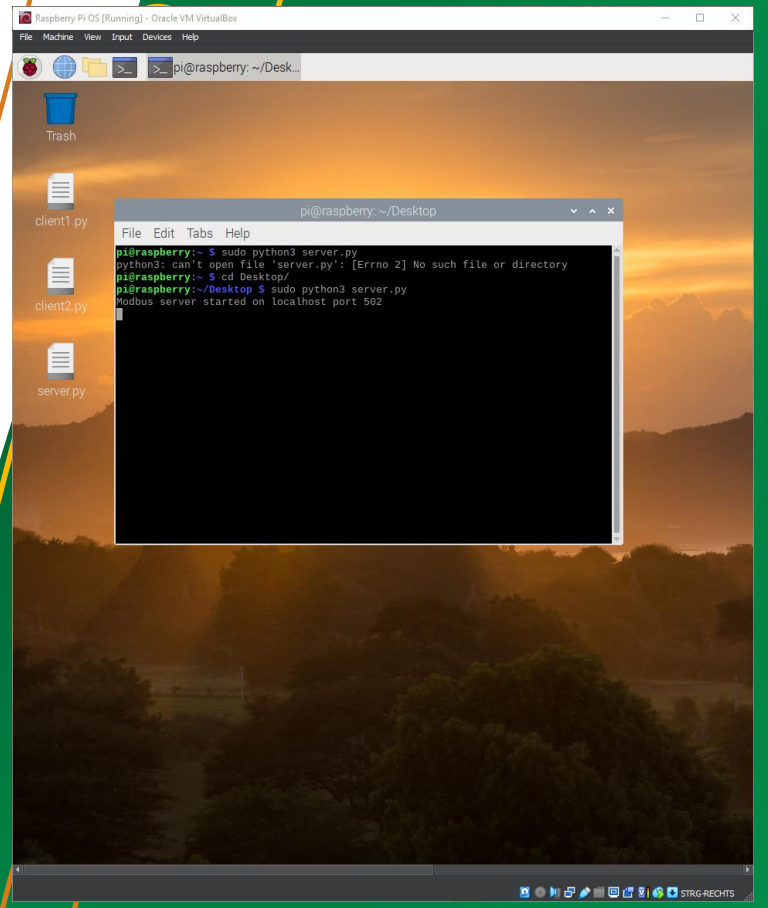
- In the Server/Client example, we have two Linux machines: the client sending data to the server through the **ModbusTCP** protocol.

- When the attacker is a **Man-in-the-Middle**, Wireshark tool can be used for capturing all data transmitting, and other actions could be applied, such as:
  - Filtering collected data (**Modbus**)
  - Analysis traffic

# Wireshark – Client/Server Example



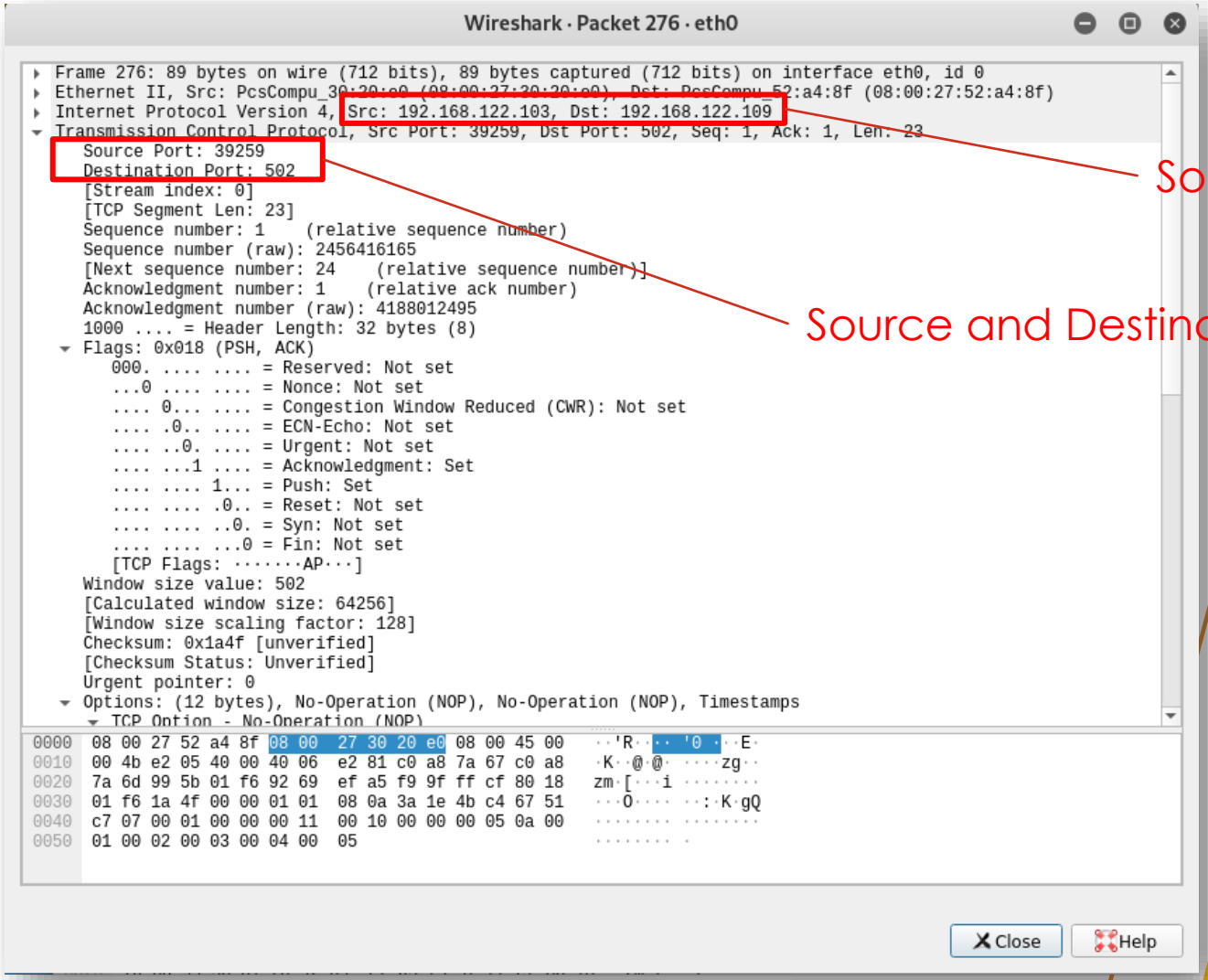




Client

Kali

Server

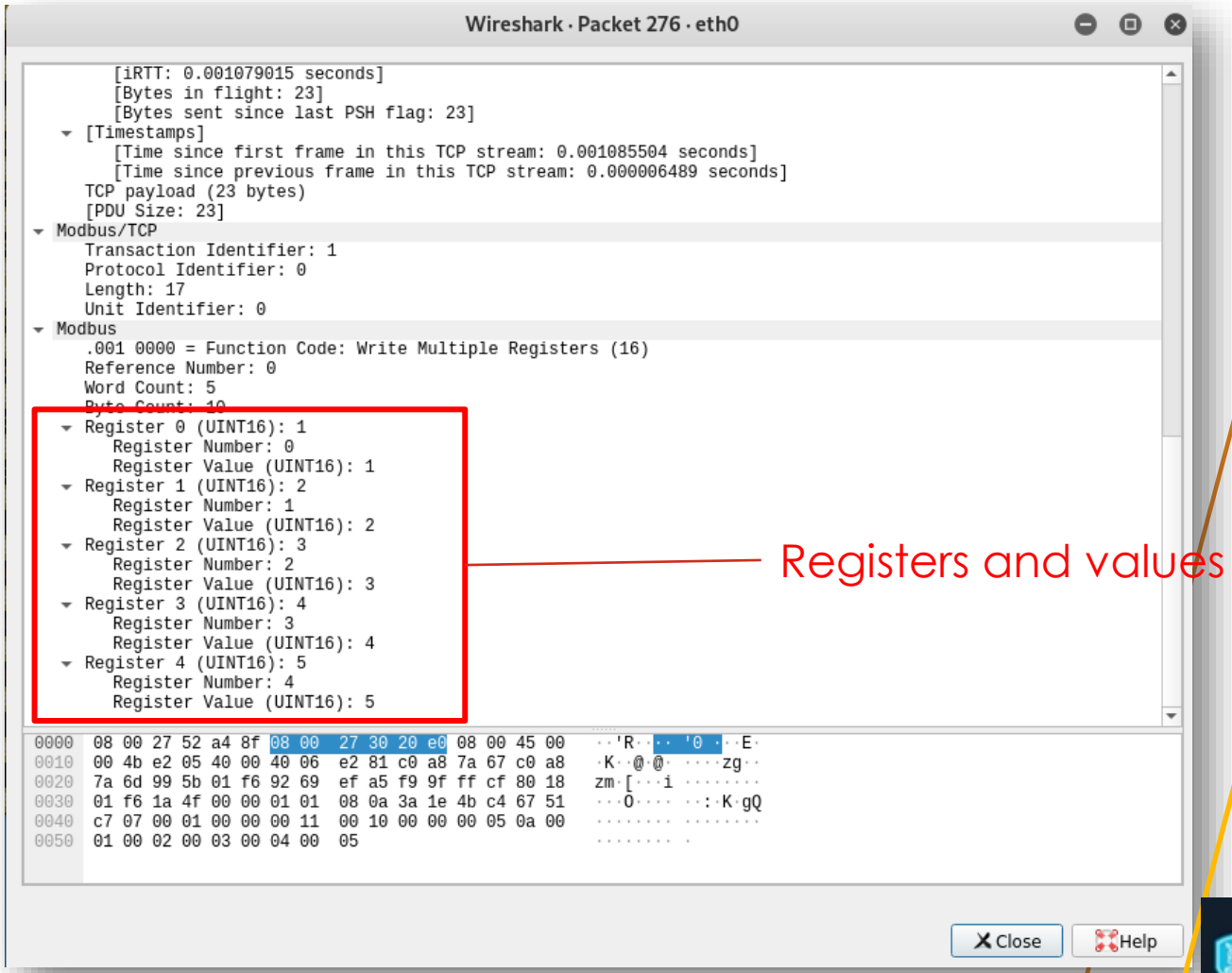
# Wireshark – Client/Server Example




Source and Destination IP

Source and Destination Ports

# Wireshark – Client/Server Example




Registers and values

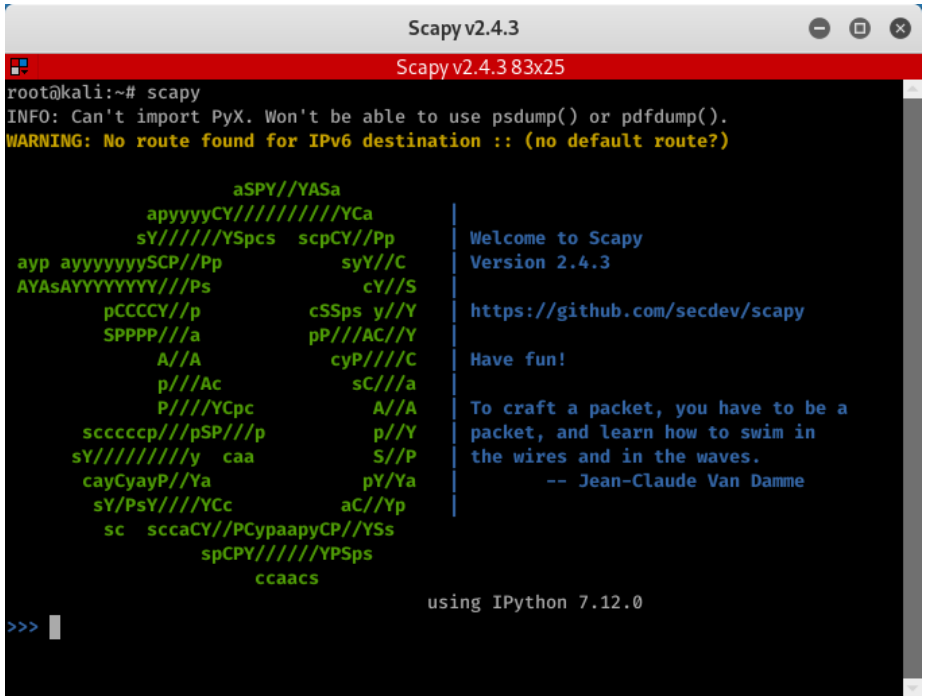
# Offensive Tools

## Scapy

# SCAPY: Create/Send a Packet

## Create packets on Scapy

- Start Scapy, and a Python command line within Scapy will open




## Use Wireshark to catch the ICMP message

- Assign the packet to a variable, say P.
  - >> **P = IP()**
- Define the IP Source (make it a fake IP, for example, a gateway IP address):
  - >> **P.src = "192.168.122.1"**
- Define the IP Target (victim machine):
  - >> **P.dst = "192.168.122.103"**
- Send the packet
  - **send(P)**

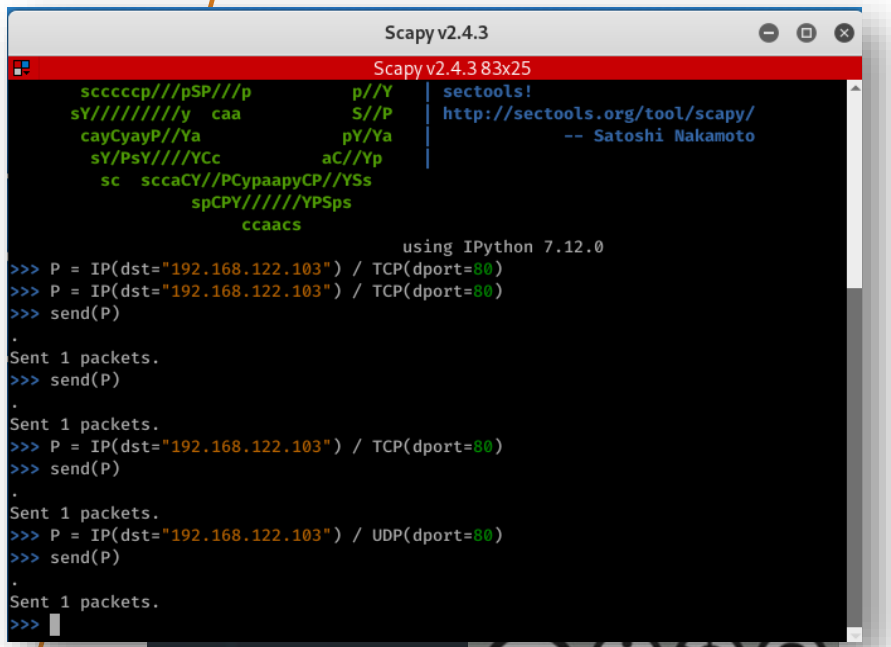
# SCAPY: Create/Send a Packet

## Multiple Packet Creation

- **Create multi-layer packets** (e.g., combining IP with TCP or UDP layers) to simulate different network protocols.

- TCP Packet
  - >> **P = IP(dst="192.168.122.103") / TCP(dport=80)**
- Send the packet
  - **send(P)**

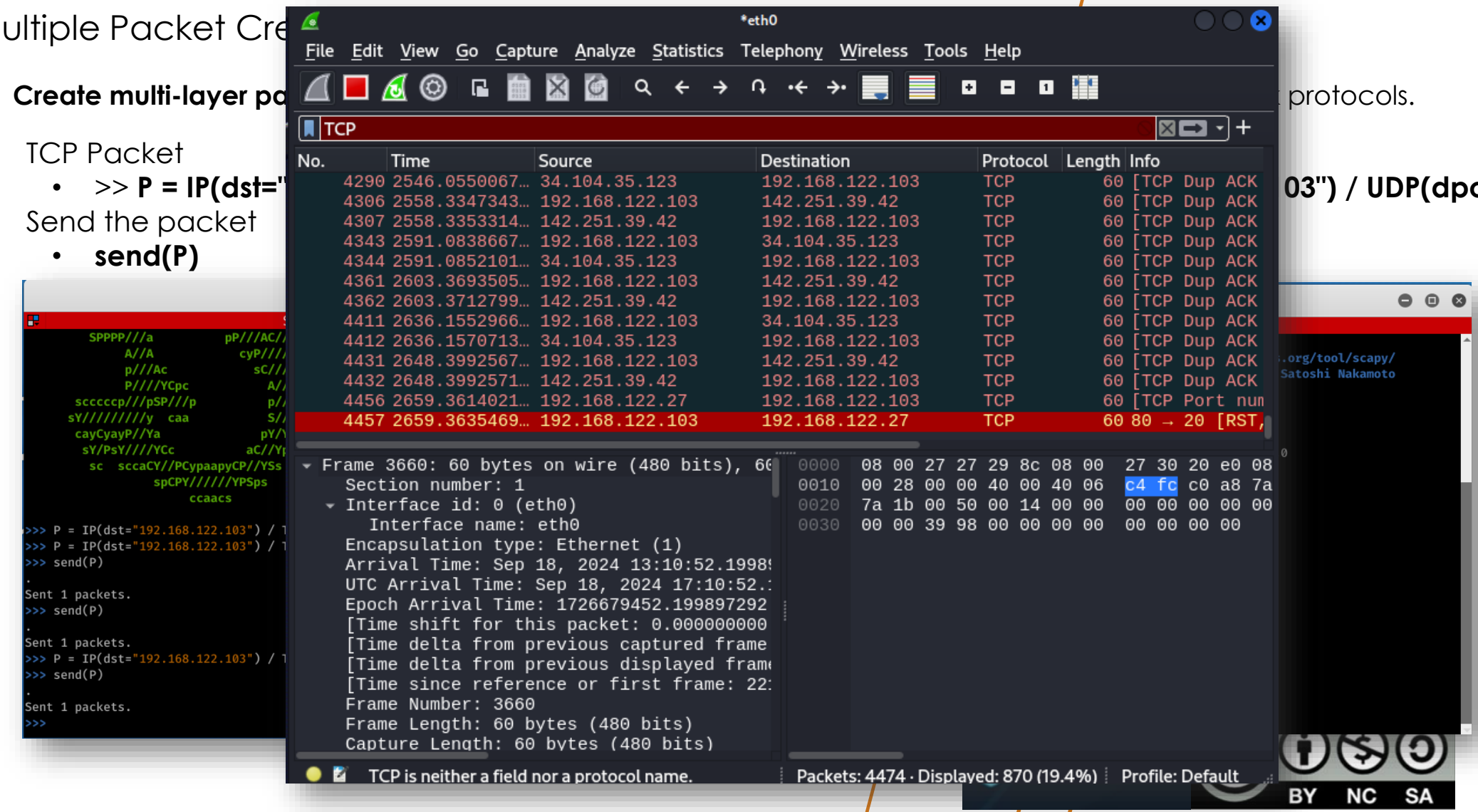

- UDP Packet
  - >> **P = IP(dst="192.168.122.103") / UDP(dport=80)**
- Send the packet
  - **send(P)**



# SCAPY: Create/Send a Packet

Multiple Packet Cre

- **Create multi-layer pa** protocols.
  - TCP Packet
    - >> **P = IP(dst="** **03") / UDP(dport=80)**
  - Send the packet
    - **send(P)**

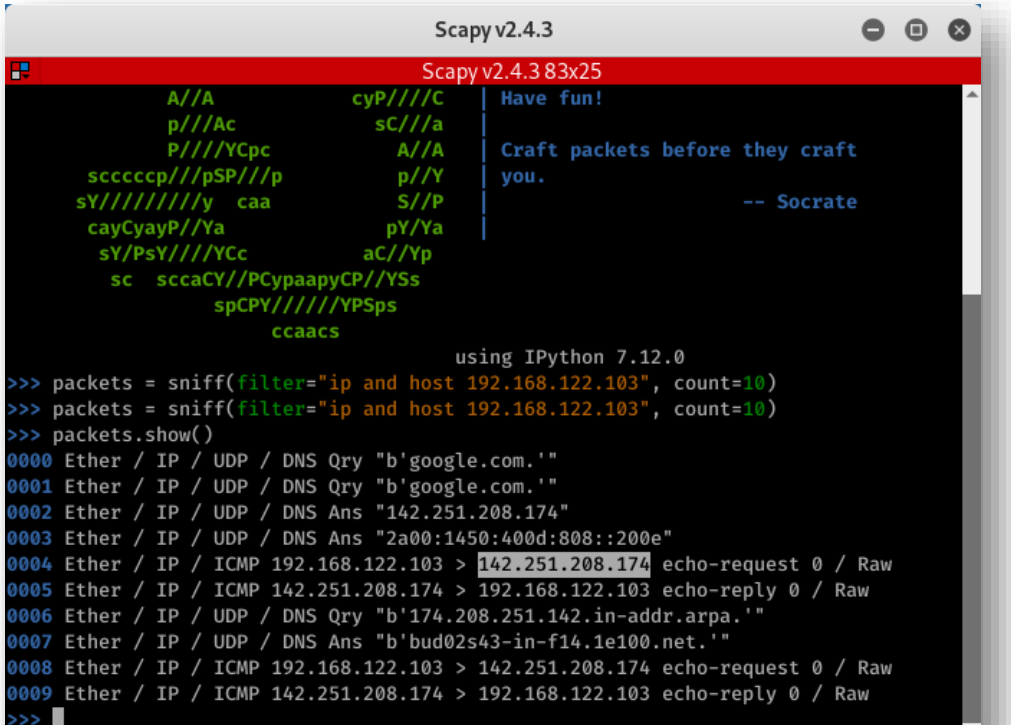


# SCAPY: Create/Send a Packet

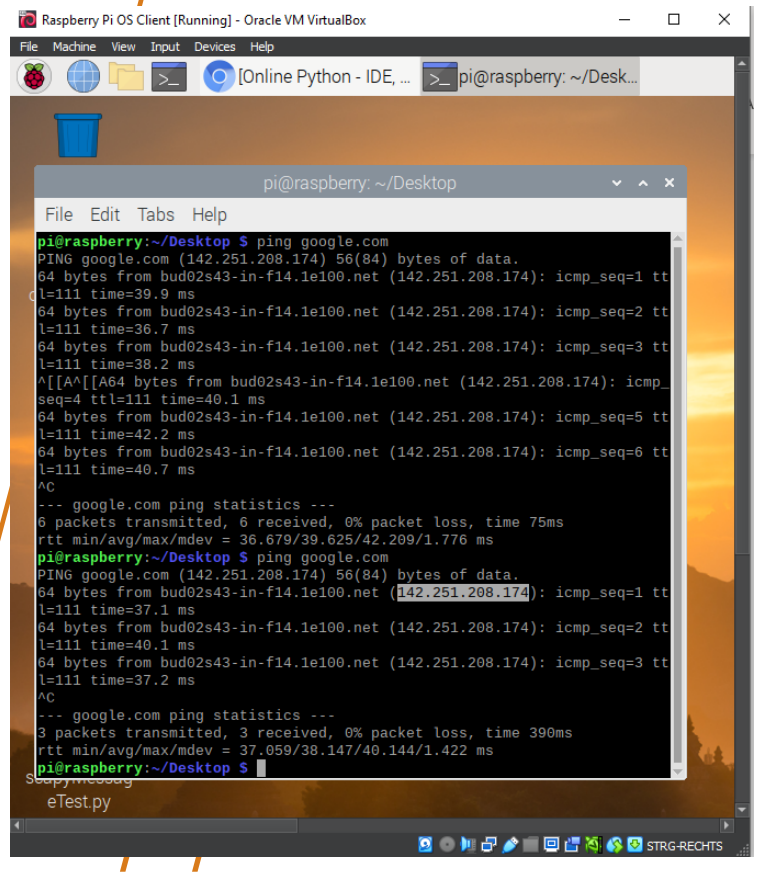
**Packet Sniffing**

Scapy can be used to perform sniffing capabilities and monitor network traffic.

- TCP Packet
  - **packets = sniff(filter="ip and host 192.168.122.103", count=10)**
- Show all collected packets
  - **packets.show()**




- **The victim machine doing anything; for example, ping to google**



# Thank you

Please send all questions to:
Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at
Stefan Schauer
Stefan.Schauer@ait.ac.at