# **TShark Challenge I: Teamwork**

**Task 1 – Introduction**

* **TShark** = Wireshark’s command-line version.
* Useful for **automated analysis**, scripting, and working on servers without GUI.
* Supports filters, statistics, extracting streams, credentials, and objects.

**Task 2 – Case: Teamwork!**

* Scenario: Multiple team members analyzing the same **PCAP**.
* Goal: Use **TShark commands** to quickly gather needed data and share results.
* Steps generally involve:
  1. **Load pcap**:

tshark -r file.pcap

* 1. **Apply display filters** to isolate relevant traffic:

tshark -r file.pcap -Y "http"

* 1. **Extract fields**:

tshark -r file.pcap -T fields -e ip.src -e ip.dst

* 1. **Count and summarize**:

tshark -r file.pcap -q -z io,phs

* 1. **Export** to share:
     + Redirect output to .txt or .csv

tshark -r file.pcap -T fields -e ip.src -e ip.dst > teamwork\_results.csv

* Benefit: Everyone works with **consistent, filtered, and summarized** data → faster joint investigation.

