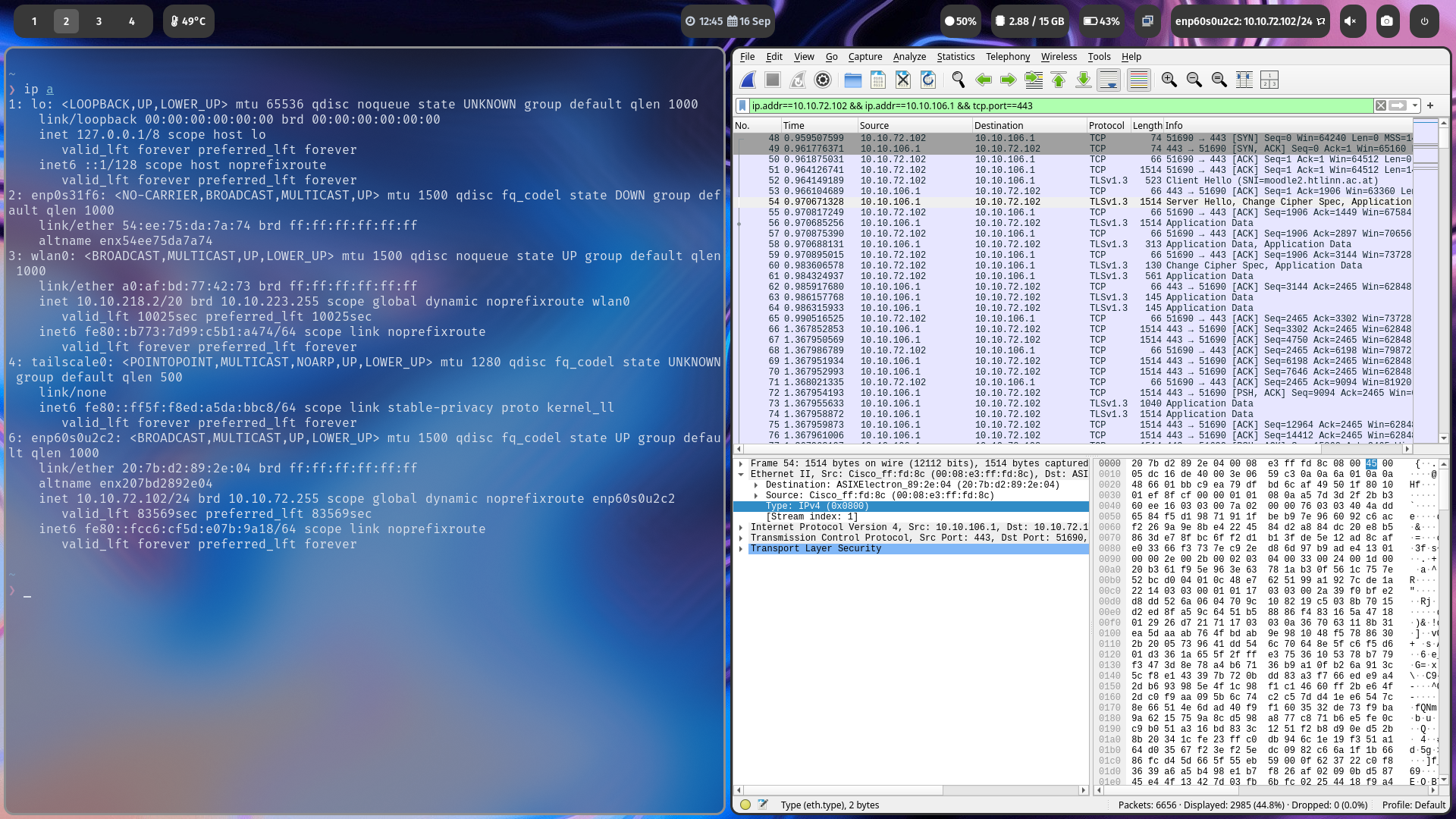
##### Samuel Fronthaler + Samuel Falkner

NWL1 Frame\_Packets\_Wireshark

4AHEL, 16. September



NWL1 – Frames & Packets, Wireshark v1.7b

#### Arbeitsform:

Bildet Zweiergruppen für den Praktischen Teil.

Jede Schülerin und jeder Schüler muss einen **eigenständigen** Laborbericht abgeben. Ein Laborbericht beinhaltet auch ein passendes Deckblatt mit Autor, Datum, Bezeichnung der Laborübung, …. !

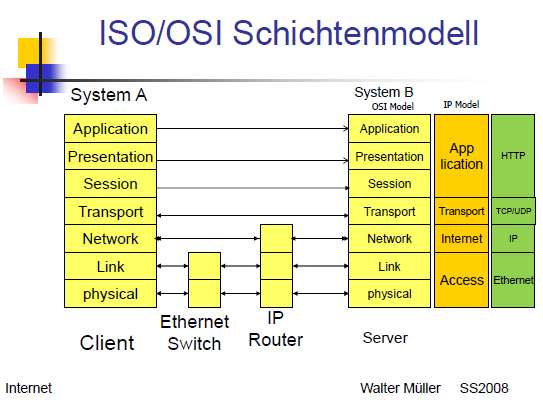
Duplikate bzw. weitreichende Kopien werden nicht akzeptiert und damit negativ beurteilt.   
Dokumentiert im Bericht auch die Namen Eurer ArbeitskollegInnen in der Gruppe.

#### Dauer:

3 Schulstunden.

#### Grundlagen Basiswissen:

* Cisco Kurs ITN, Kapitel 03 Protocols and Models
* IP- und ISO/OSI Schichtenmodell.

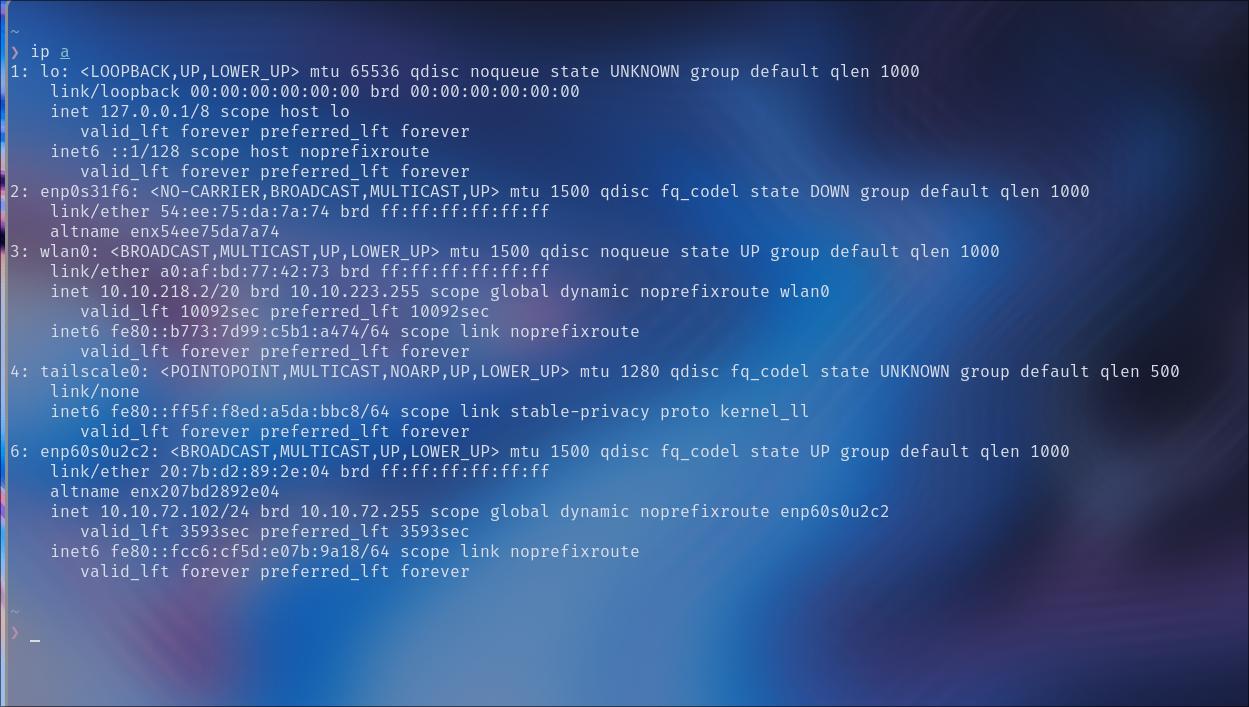


#### Fragestellungen Labor – PCs im Schulnetz:

Hängt den eigenen Laptop bzw. die Labor-PCs an das Labornetz (B-Dosen).

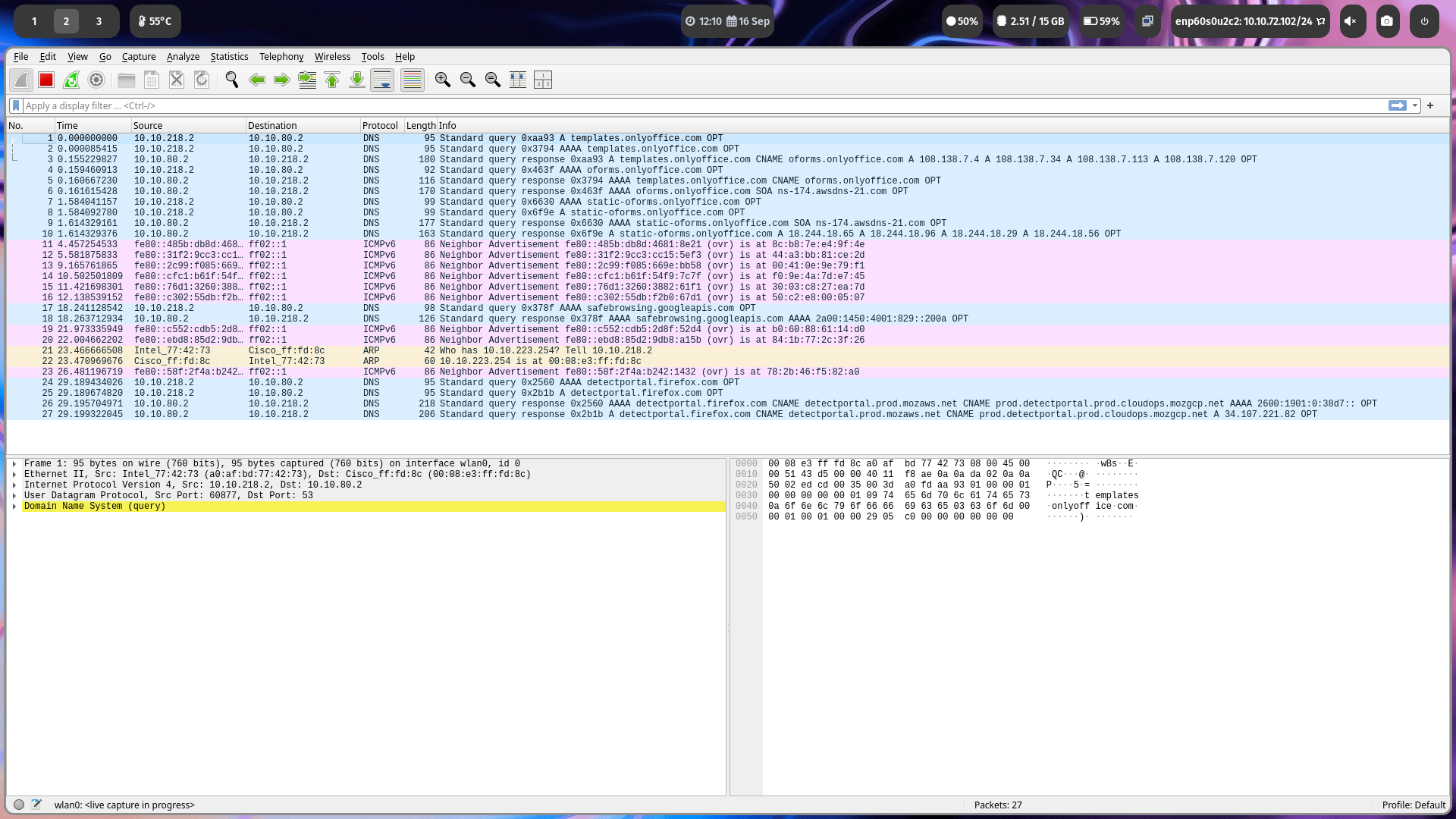
Der Lehrer hat alle PCs über einen Laborswitch mit dem Schulnetz verbunden. So können die PCs untereinander kommunizieren, was auf Grund von Sicherheitseinstellungen zwischen verschiedenen Ports des Switches im A-Netz unterbunden ist.  
  
Stellt den Laptop so ein, dass sie Ihre IP-Adresse und sonstigen Einstellungen vom DHCP-Server der Schule bezieht.  
Systemsteuerung / Netzwerk und Freigabecenter/ Adaptereinstellungen / LAN/Ethernet / Internet Protokoll v4 (bzw. v6) bzw. auf den Labor-PC mit Linux: Netzwerksteuerung im TaskTray / DHCP-Profil aktivieren

1. Dokumentiere mit ipconfig /all in einer CMD Box die IP-Einstellungen Deines PCs.  
   Welche Layer2-Adresse hat der PC am LAN-Interface, welche Layer3-Adresse.  
   Dokumentiert die weiteren Layer3 Einstellungen und erklärt Ihre Bedeutung.  
   (Subnetmask, Default-Gateway, DHCP-Server, DNS-Server)  
   Am Labor-PC (Linux) könnt Ihr die Netzwerkeinstellungen in einer shell mit ifconfig -a ausgeben.

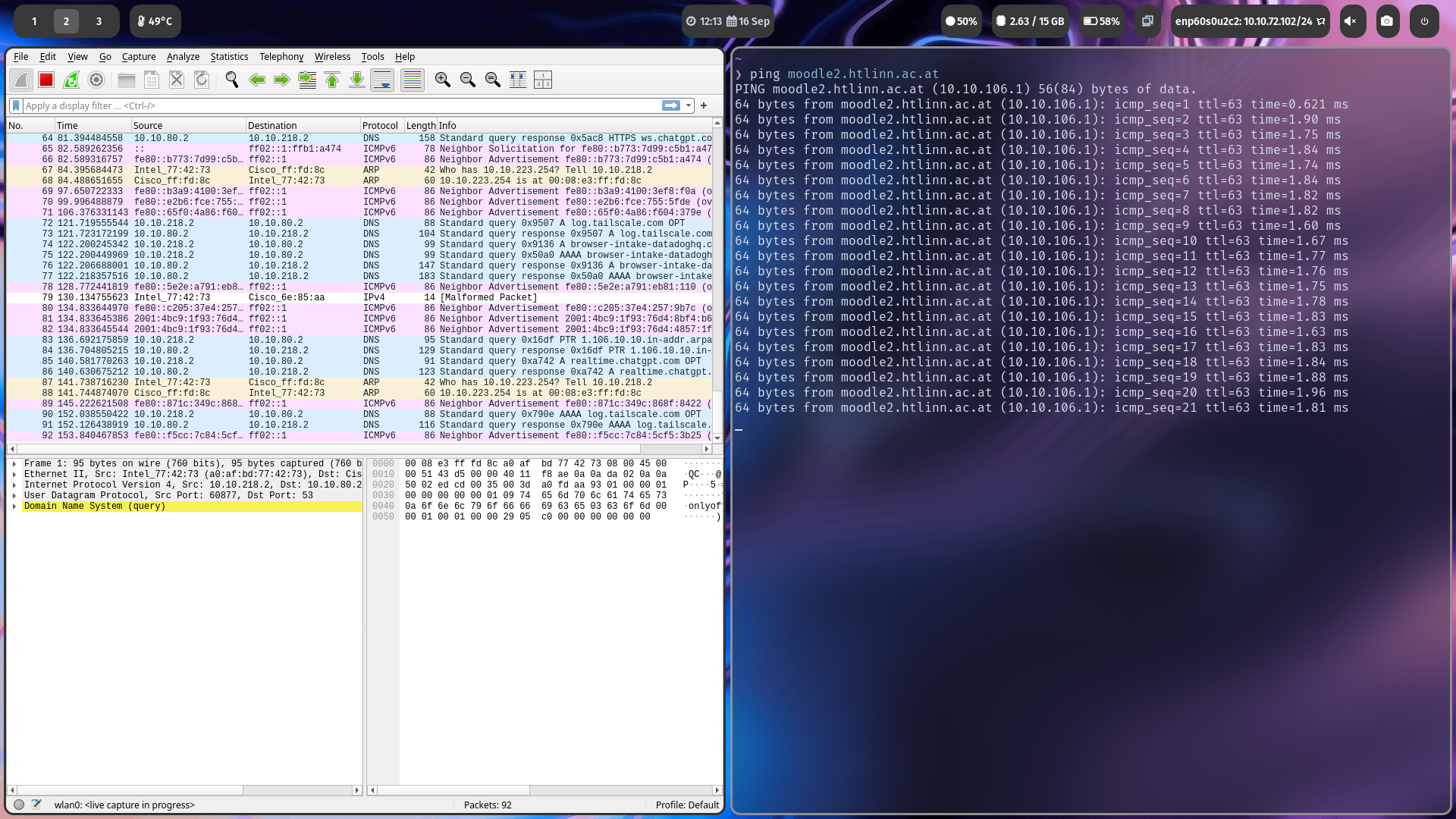


Mein LAN-Interface hat die MAC-Adresse 20:7b:d2:89:2e:04 und die IP-Adresse 10.10.72.102/24, die vom DHCP-Server zugewiesen wurde. Die Subnetzmaske ist 255.255.255.0, das Default-Gateway leitet den Verkehr außerhalb meines Netzwerks und der DNS-Server löst Domainnamen in IP-Adressen auf.

1. Startet als Administrator das Programm Wireshark (WS) (ein Netzwerksniffer/-analyse-programm).  
   und beginnt mit Capture / Interface / auswählen / Start die Aufzeichnung von Paketen.  
   Es sollten Netzwerkpakete angezeigt werden.

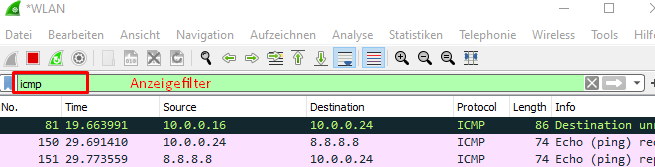


1. Kopiert einen Screenshot in dieses Dokument.  
   Welche Fenster gibt es – Beschreibt die drei horizontal unterteilten Fensterabschnitte im WS!  
   Paketliste, Paktedetails, Paketbytes
2. Startet im Wireshark die Aufzeichnung und   
   gebt in einem CMD-Fenster bzw. einer shell unter Linux das Kommando  
   ping moodle2.htlinn.ac.at   
   ein.  
   Was macht ping? Ping schickt ein packet an den moodle server und wartet auf eine antwort dass es angekommen ist



1. Welche Ausgabe seht Ihr im CMD Fenster?  
   Welche im Wireshark?  
   Stoppt die Aufzeichnung im WS.
2. Dokumentiert einen Ping-Request, also einen Ethernet-Frame bzw. ein IP-Paket im Wireshark.

Welche Quell- und Zieladressen erkennt Ihr auf Layer3 (IP) und auf Layer2(Ethernet)?  
Dokumentiert im WS welche Teile des Pakets zum Layer2 und welche zum Layer 3 gehören.  
Was bezeichnet man als Frame, was als Packet?  
Tipp: Zum Auswählen der Ping Pakete bei Anzeigefilter ICMP eingeben:



Destination: Cisco\_ff:fd:8c (00:08:e3:ff:fd:8c)

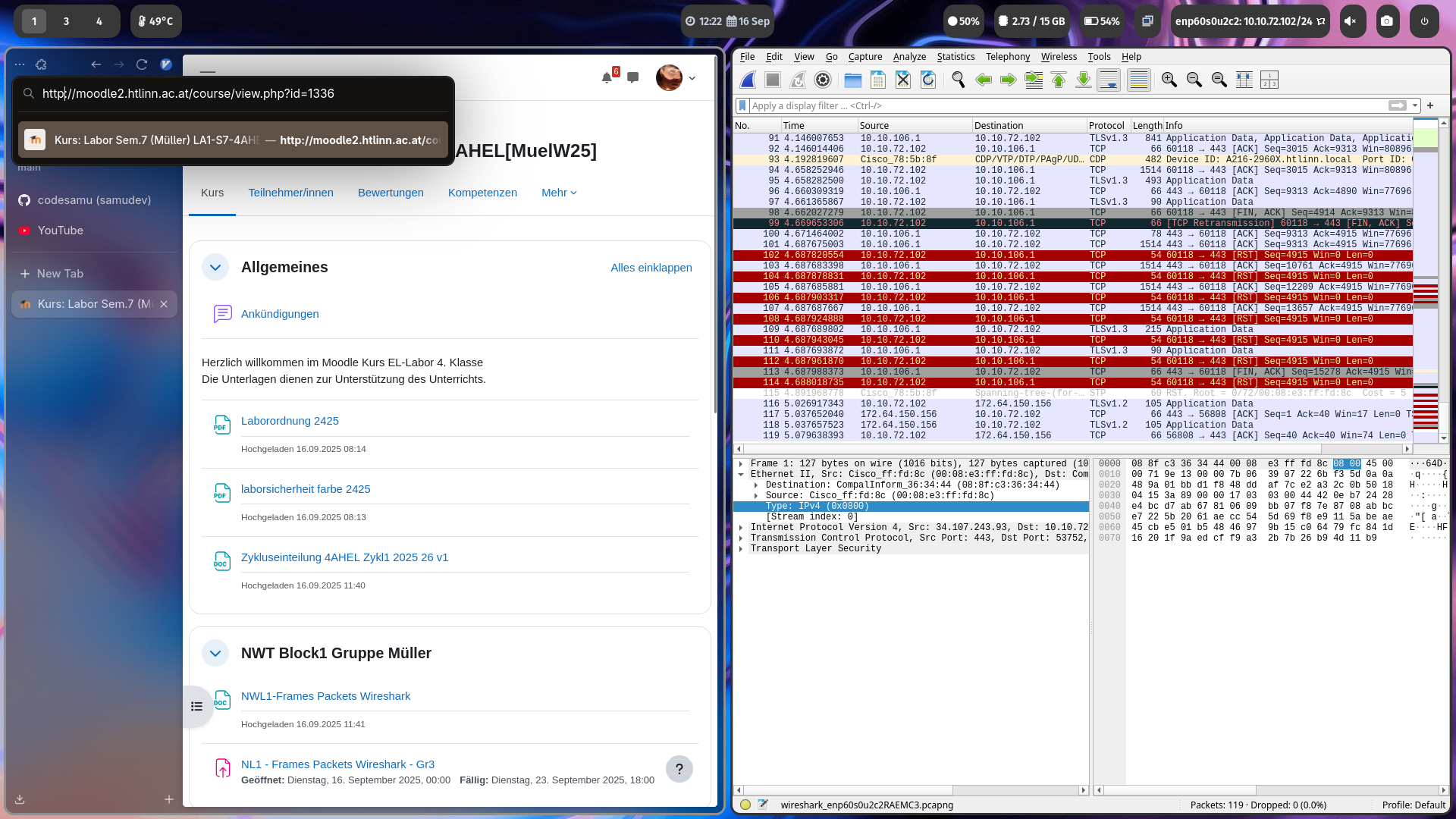
Source: ASIXElectron\_89:2e:04 (20:7b:d2:89:2e:04)

Type: IPv4 (0x0800)

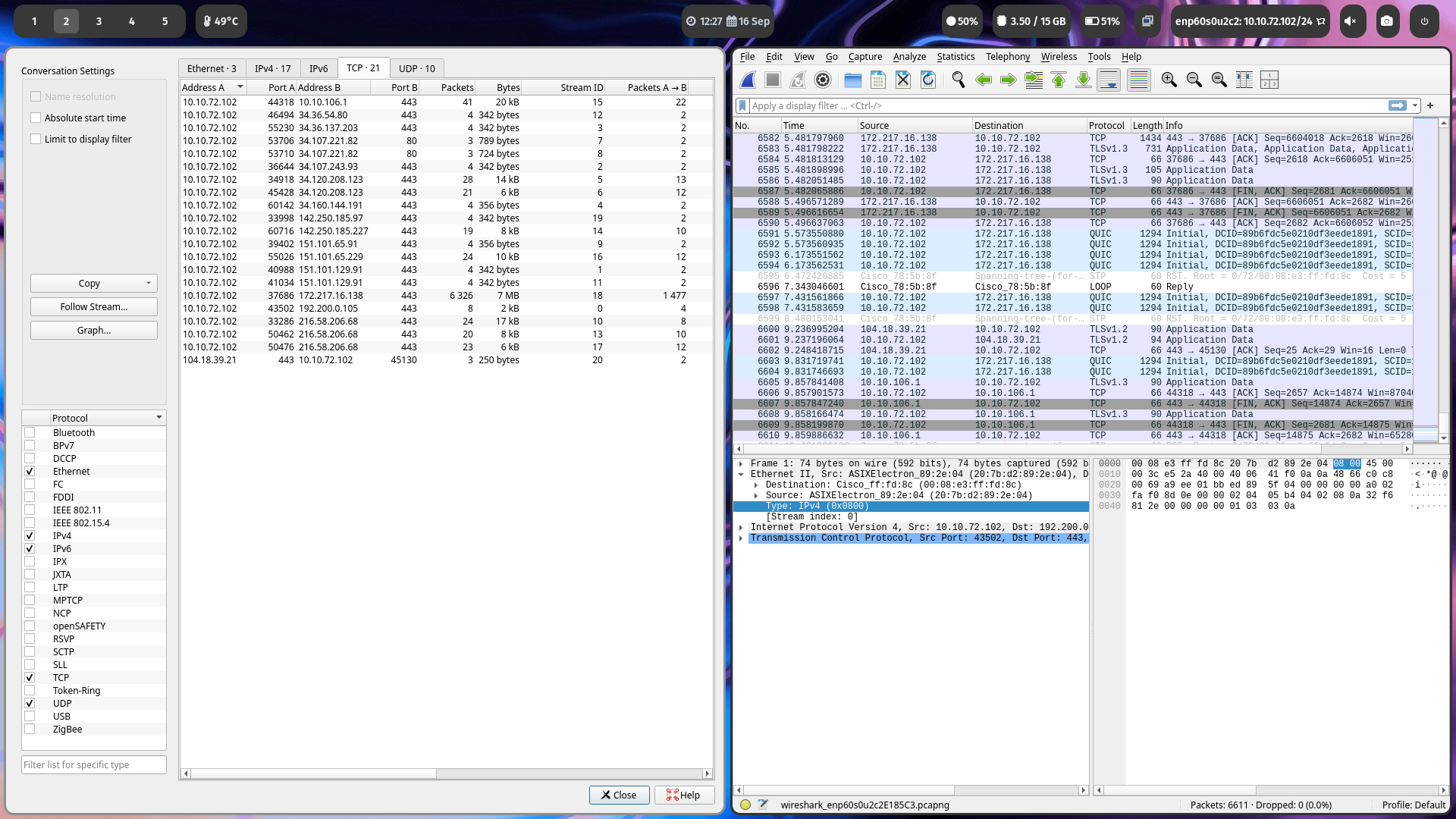
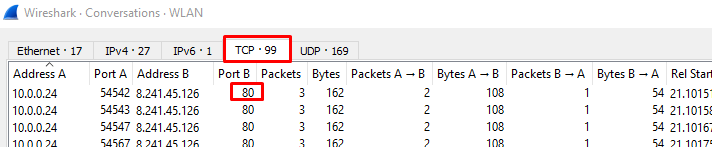
Layer2 ethernet (mac adressen), Layer 3 (IP adressen)

Frame ist Datenpacket layer2, Packet is Datenpacket layer3

1. Vergleicht die L2- und L3-Adressen im Wireshark mit den zuvor mit ipconfig bzw. ifconfig (Linux) ermittelten Adressen am PC.  
   layer3 ist gleich wie davor, layer2(mac) hat sich verändert, ip a: 54:ee:75:da:7a:74 , wireshark 20:7b:d2:89:2e:04
2. Startet die WS Aufzeichnung wieder.  
   Startet eine Web-Browser (z.B. Firefox) und „besucht“ die Seite   
   [**http**://moodle2.htlinn.ac.at](http://moodle2.htlinn.ac.at) (http ist wichtig, da von den Browsern ansonsten sofort die verschlüsselte Variante HTTPS verwendet wird)

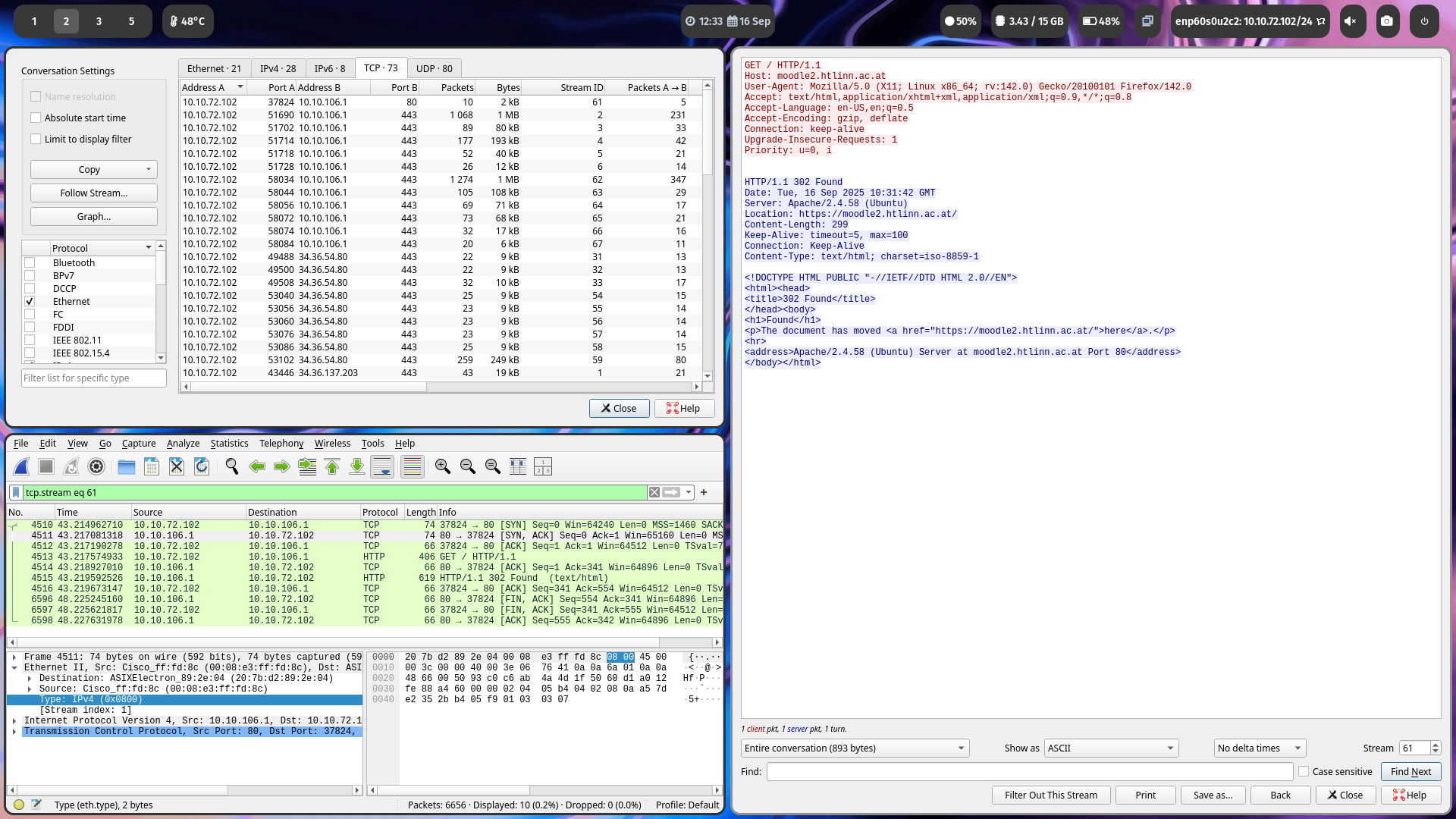


1. Mit „Statistiken / Verbindungen“ könnt ihr euch einen Überblick über das Kommunikationsgeschehen verschaffen. Wer spricht mit wem auf welcher Protokollebene.  
     
   Fügt hier Eure Verbindungsstatistik ein.



Solltet Ihr keine http-Verbindungen zum moodle-Server entdecken:  
Euer Browser scheint sich den „sicheren“ moodle-Server zu merken und baut Verbindungen prinzipiell mit HTTPS auf.  
Beendet also die Aufzeichnung und probiert mit einem alternativen Browser wie Chrome oder Edge erneut euer Glück.

1. Wählt eine Verbindung (Zeile) mit der Zieladresse moodle-Server und dem Ziel Port 80 und mehr als 3 Paketen aus.  
   Mit der rechten Maustaste / Als Filter anwenden / ausgewählt / A <-> B wird im Wireshark der Anzeigefilter so gesetzt, dass nur mehr diese Verbindung angezeigt wird.  
   (screenshot)



1. Wählt ein Paket der Verbindung aus und startet „Analyze/Follow TCP stream“.  
   Was erkennt Ihr? Klartextprotokoll

Wofür steht http? Hypertext transfer protocol

\*) optionale Aufgaben falls noch Zeit bleibt

1. \*) Findet Ihr im Output auch ein ARP, ein DNS-Paket?  
   Wozu braucht es diese Pakete?

* ARP
  + Übersetzt IP → MAC
  + Lokales Netzwerk
  + Layer2: MAC-Adressen
  + Layer3: IP-Adresse
* DNS
  + Übersetzt Domainname → IP
  + Internet/Hostname-Auflösung
  + Layer2: MAC-Adressen
  + Layer3: IP-Adresse
  + Layer4: UDP, Port 53
* Grund
  + ARP: Geräte im LAN finden
  + DNS: Hostnamen auflösen für Kommunikation

1. \*) Dokumentiere Deine IPv6 Link-Local-Adresse am Ethernet-Interface.  
   Anmerkung zu Win11:  
   Das Betriebssystem scheint per Default nicht auf allen Interfaces IPv6 zu aktivieren.  
   Taucht bei ipconfig /all keine IPv6-Adresse beim entsprechenden Interface auf, muss IPv6 unter „Netzwerk&Internet / WLAN bzw. Ethernet.. / erweiterte Netzwerkeinstellungen / Adaptereinstellungen“ durch Anhaken des IPv6 Kästchens aktiviert werden.



1. \*) Zeichne mit Wireshark einen IPv6 Ping zum PC Deines Arbeitskollegen auf und dokumentiere diesen mit Screenshots.  
   Windows Rechner blockieren per default ICMP-Echo Requests (Ping) und antworten deshalb nicht. „Datei und Druckerfreigabe (ICMPv6)“ ist daher in den eingehenden Firewall Regeln zu aktivieren und unter Erweitert für alle Profile (Domäne, Privat, Öffentlich) frei zu geben.
2. Gebt den Laborbericht als PDF mit dem Namen **NWL1-*Namen*.pdf** im moodle ab!