UNIVERSITÉ Concordia UNIVERSITY

GINA CODY
SCHOOL OF ENGINEERING
AND COMPUTER SCIENCE

Wireshark

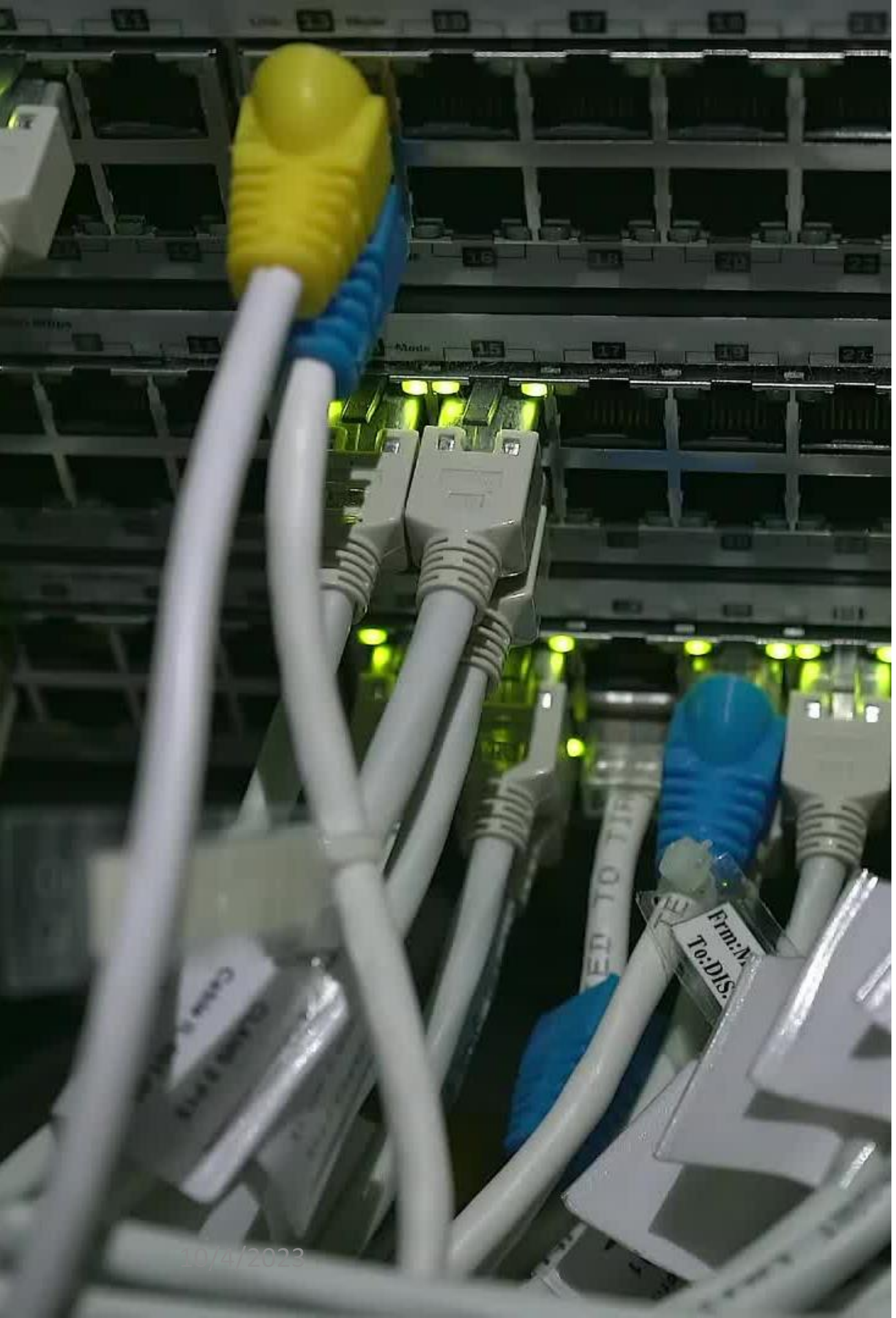
COEN 366

Instructor: Prof. Chadi Assi

What is Wireshark ?

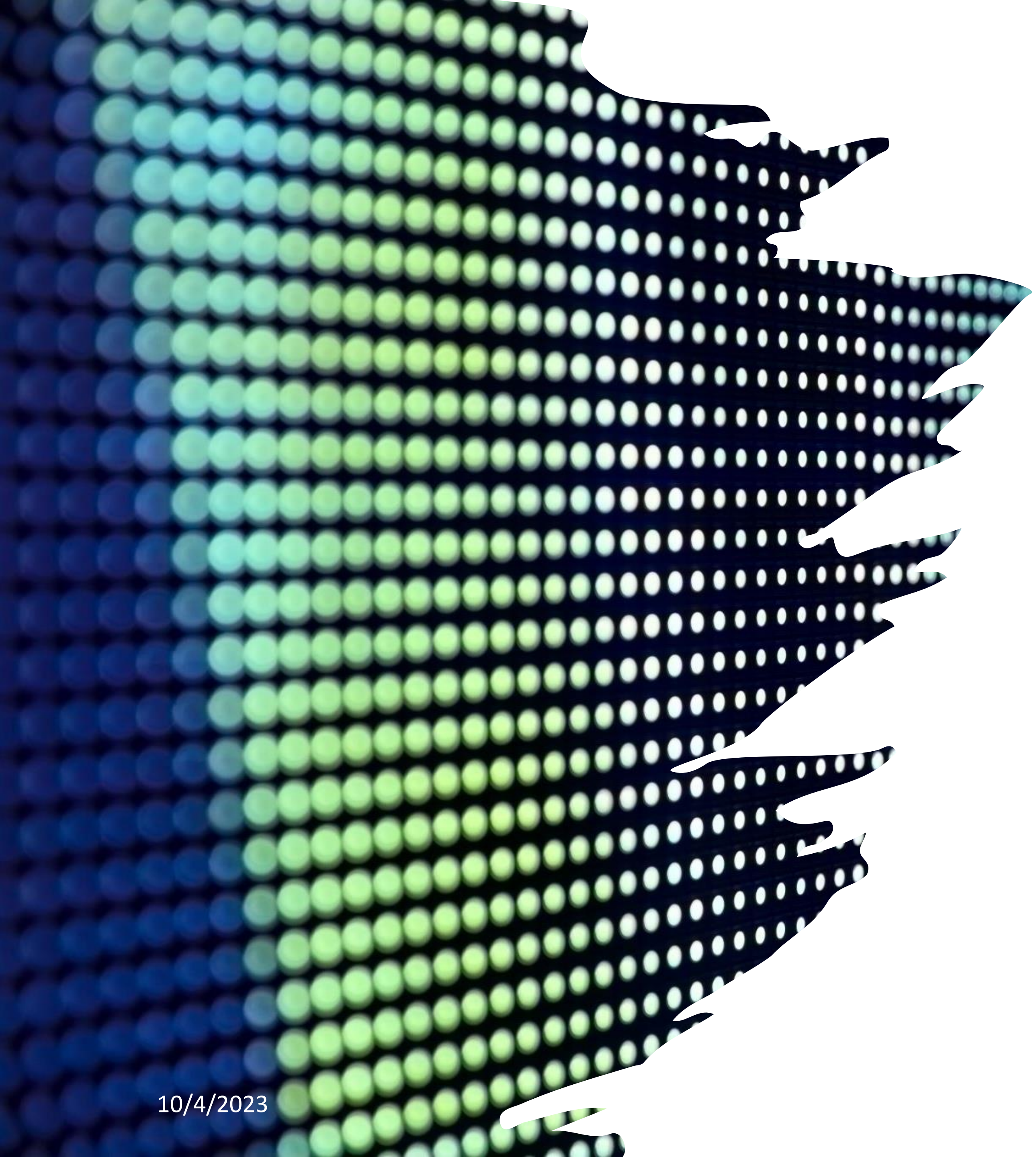
- Wireshark is a **network packet/protocol analyzer**.
- A network packet analyzer will try to capture network packets and try to display that packet data as detailed as possible.
- Wireshark is one of the **best open-source** packet analyzers available today for UNIX and Windows.
- Downlink link:

https://www.wireshark.org/#download



Purpose of using Wireshark

- Network administrators use it to troubleshoot network problems.
- Network security engineers use it to examine security problems.
- Developers use it to debug protocol implementations.
- People use it to learn network protocol internals.
- It should be noted that Wireshark will not manipulate things on the networks, it will only “measure” things from it.



Features

- “Understands” the structure of different network protocols.
- Displays encapsulation and single fields and interprets their meaning.
- It can only capture on networks supported by pcap.
- It is cross-platform running on various OS (Linux, Mac OS X, Microsoft windows)

WinPCap

- Industries – standard tool for link-layer network access in windows environment.
- Allows an application to capture and transmit network packets bypassing the protocol stack.
- Consists of a driver-extends OS to provide low-level network access.
- Consists of the library for easy access to low-level network layers.
- Also contains windows version of libPCap Unix API
- Download link:
- https://nmap.org/npcap