# *Ethernet/Data Link frame capture (Evesdropping Lab)*

**i310 Lab 1/12/2016:**

## JF (Network Protocols/Protocol Analyzers) – *attached related slides*

***Lab Exercise*** **– Class/individuals will do a live capture of Ethernet frames, then decode and analyze the frames.**

**The lab requires a wired interface into a shared Ethernet hub where all lab devices will connect.**

**As an alternative – you can load Wireshark on your device. It does require you install the software on your machine – it is free. I will be providing at least several laptops with wired interfaces and Wireshark loaded as a lab resource, important hands-on skill for you to have and be aware of. There should also be a copy posted to Canvas library/share.**

***Deliverable*****: email (to Canvas site) lab write-up detailing your explanation of the lab, how to capture and Ethernet frame, and how this tool would prove useful in network troubleshooting and other cases *(please state at least one scenario besides networking troubleshooting, how it would be used)***

**Wireshark Website: the website contains information on the tool, and also the software for people that want to directly download the tool to their personal device.**

**http://www.wireshark.org/**

# *Ethernet/Data Link frame capture/evesdropping Lab*

***Deliverable*: write-up detailing *your* explanation of the lab – approx. 1 page email (to Canvas site):** ***Due 1/19/2016 8pm* PST**

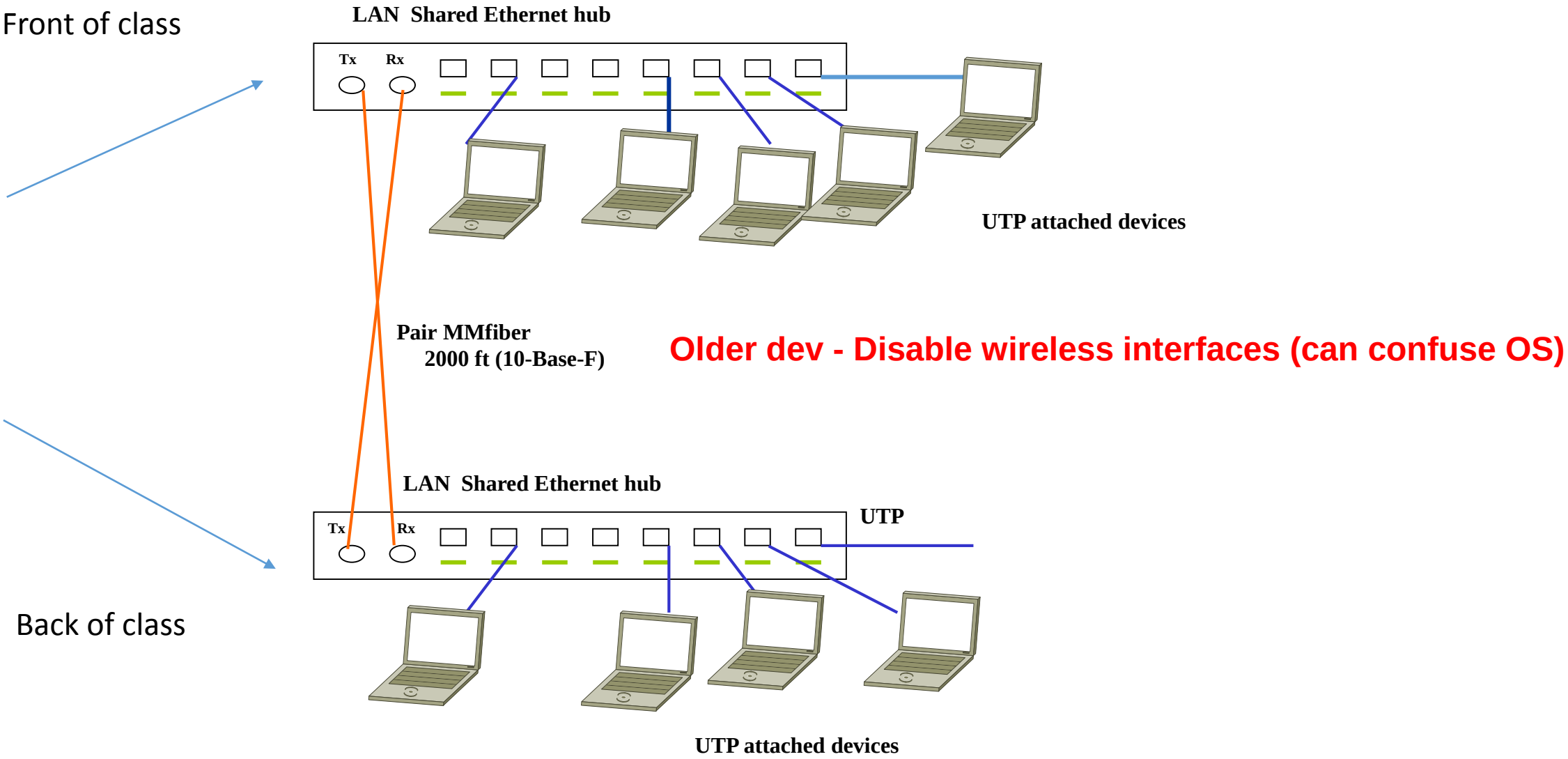
**1. Brief description of how to capture an Ethernet frame (30 %)**

**2. Briefly describe one recommendation how you might use a similar tool to troubleshoot a technical issue or possibly provide analysis and/or forensics in IA/Cyber Security (30 %)**

**4. Summary of what you learned in lab (and how you may apply this knowledge in future (40 %)**

# Lab Topology (Ethernet hub to hub)

Front of class




Older dev - Disable wireless interfaces (can confuse OS)

Back of class

** Any significance to the Topology ? Why such old hubs and not new switches ?*

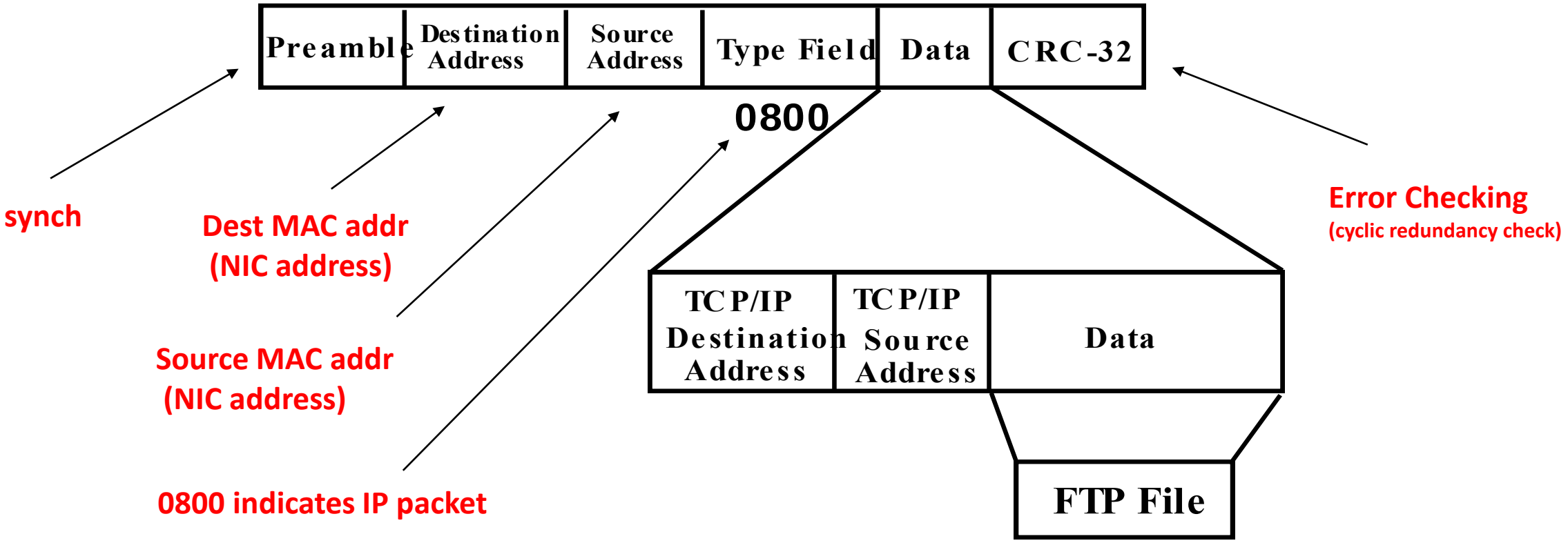
# Ethernet frames and TCP/IP Packets

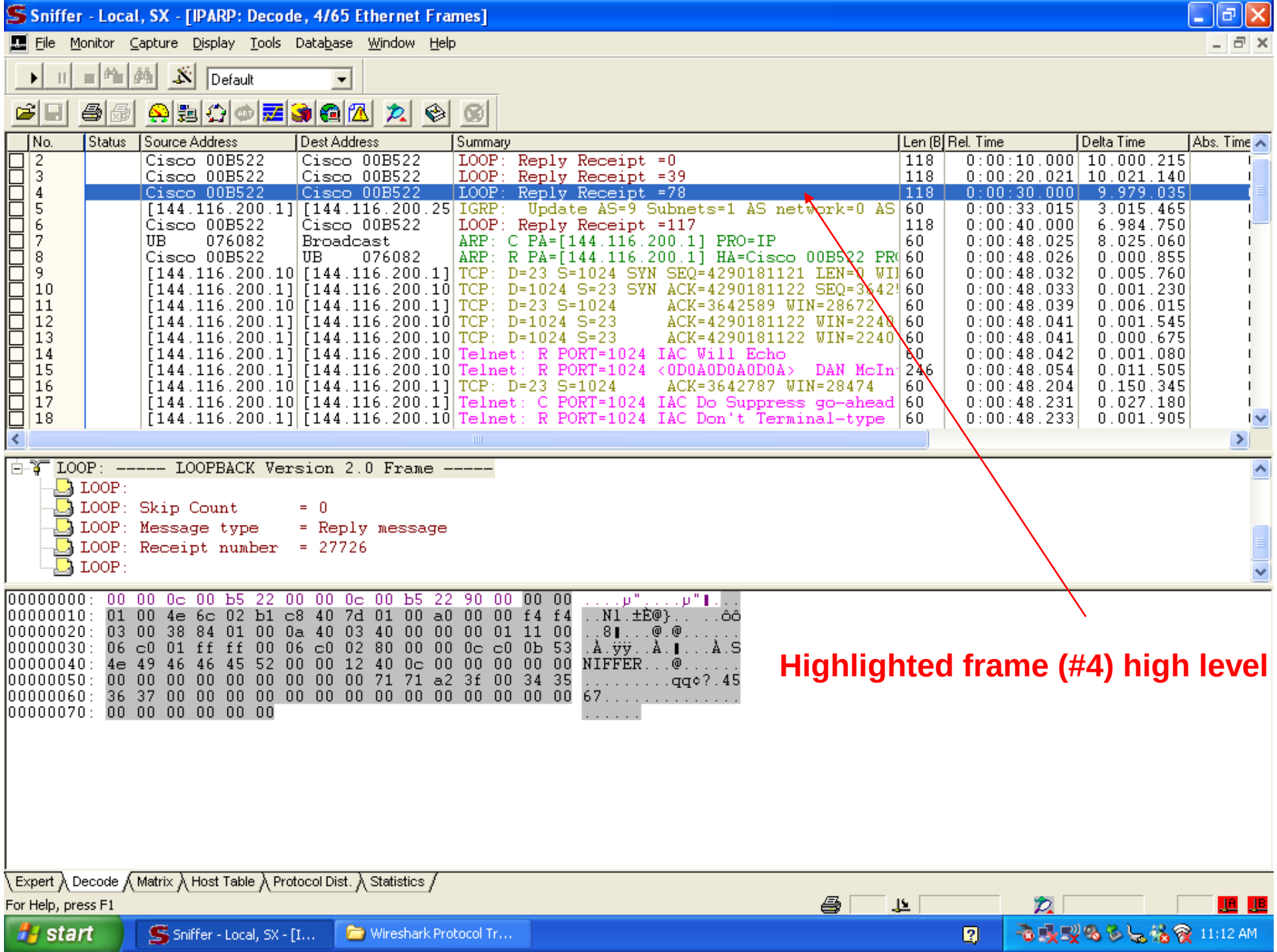
**The following group of slides is intended to provide background information on Ethernet frame and TCP/IP packet structure/content. Additionally, there are slides that demonstrate how to filter (to display only desired traffic) – as well as discovery telnet/http data (i.e. passwords sent in clear)**

# PDU (Protocol Data Unit) - the contents of an Ethernet frame

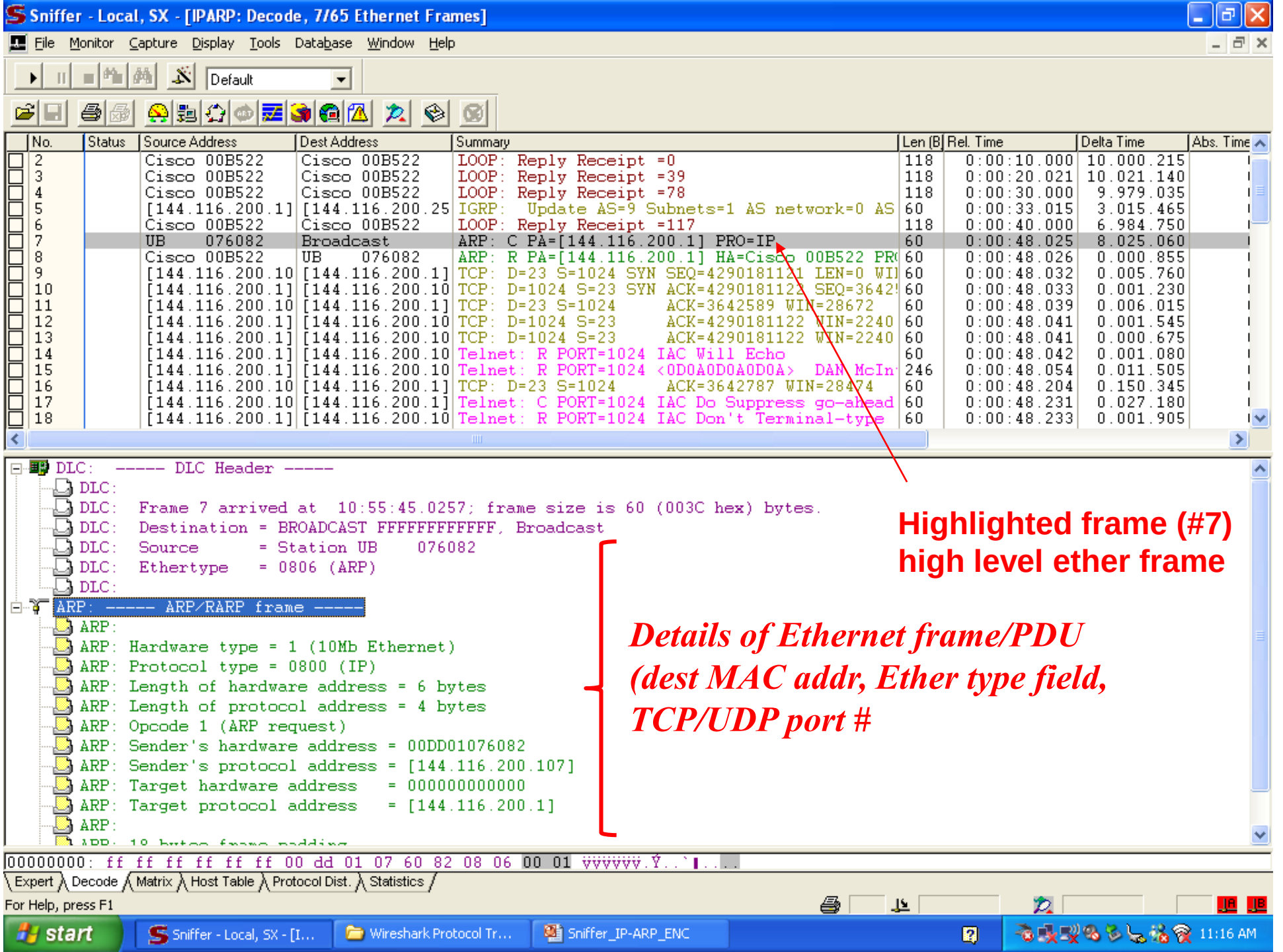
**An Ethernet frame may contain about anything in any format. Ethernet does not interpret the data section, except to look at the protocol type field or length. The data section must be a minimum length of 46 bytes, even if there is only 1 byte to send, and may be as large as 1500 bytes. Typically the data section would contain the protocol packet used by upper layer software such as TCP/IP, XNS, IPX, AppleTalk, SNA,MOP, LAT....)**

**The following diagram illustrates a FTP (file transfer) request from an end user in a TCP/IP packet inside an Ethernet frame.**



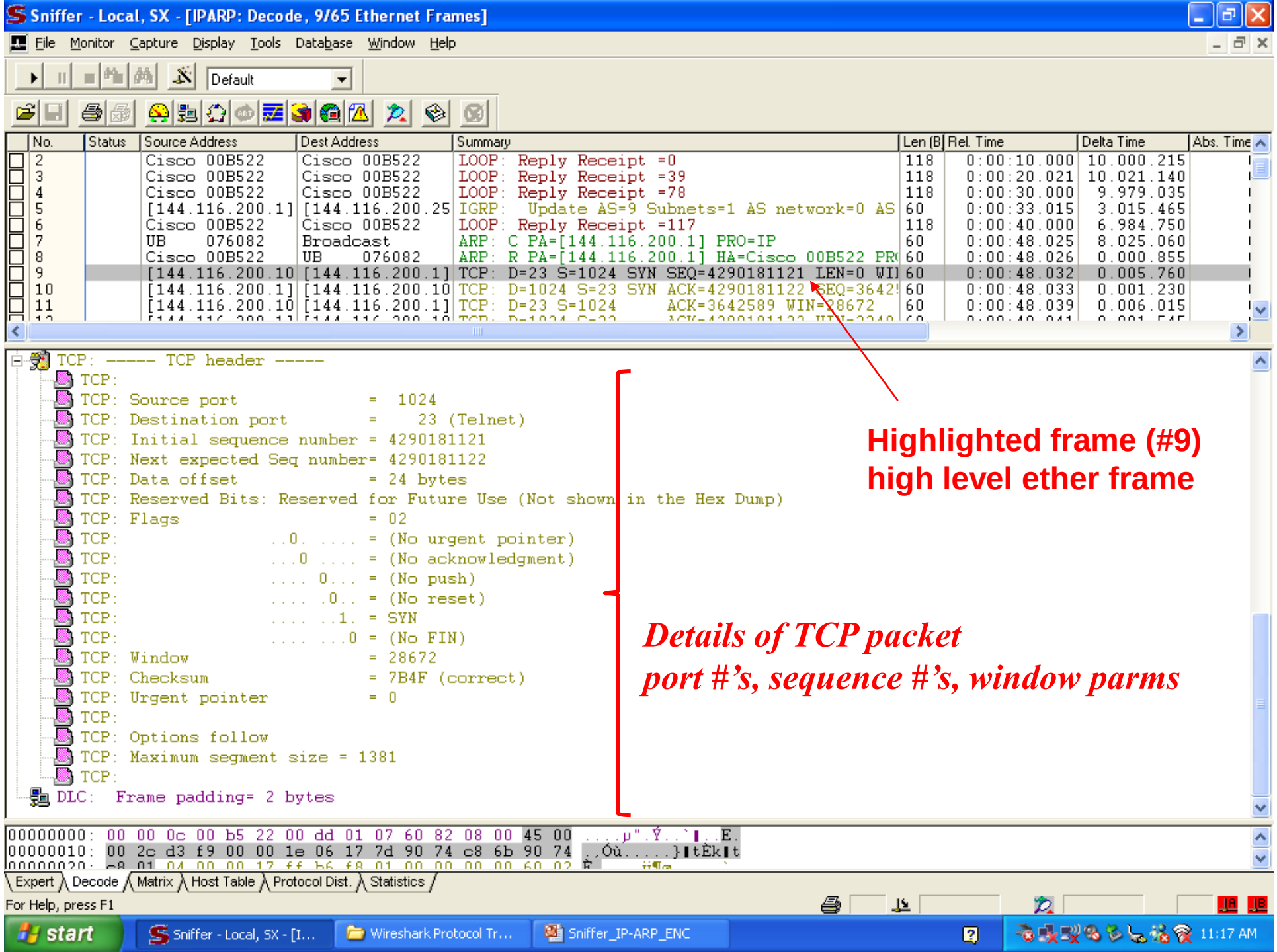



**Highlighted frame (#4) high level ether frame**




**Highlighted frame (#7)**
**high level ether frame**

***Details of Ethernet frame/PDU (dest MAC addr, Ether type field, TCP/UDP port #***

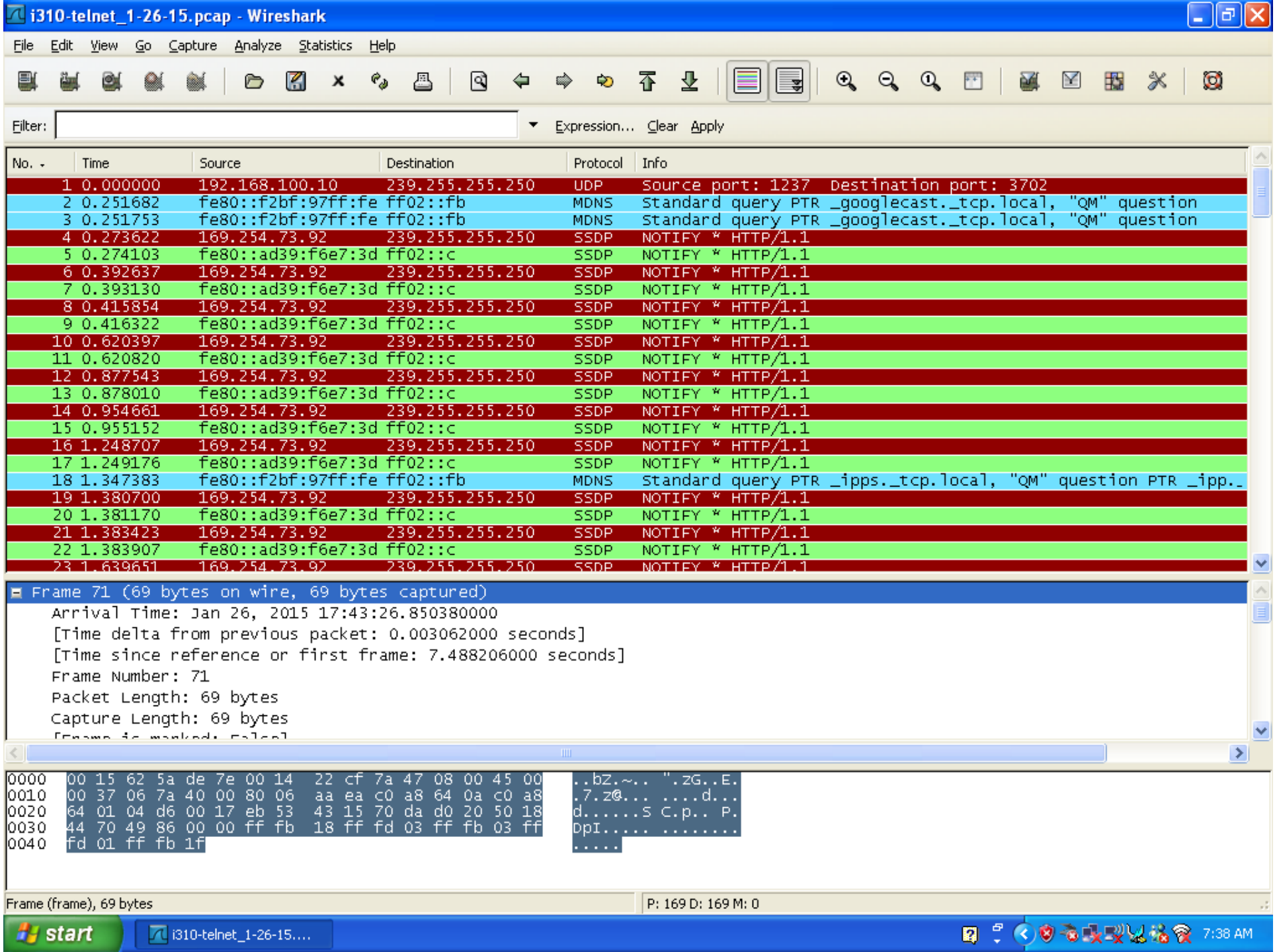



**Highlighted frame (#9)**
**high level ether frame**

***Details of TCP packet***
***port #'s, sequence #'s, window parms***

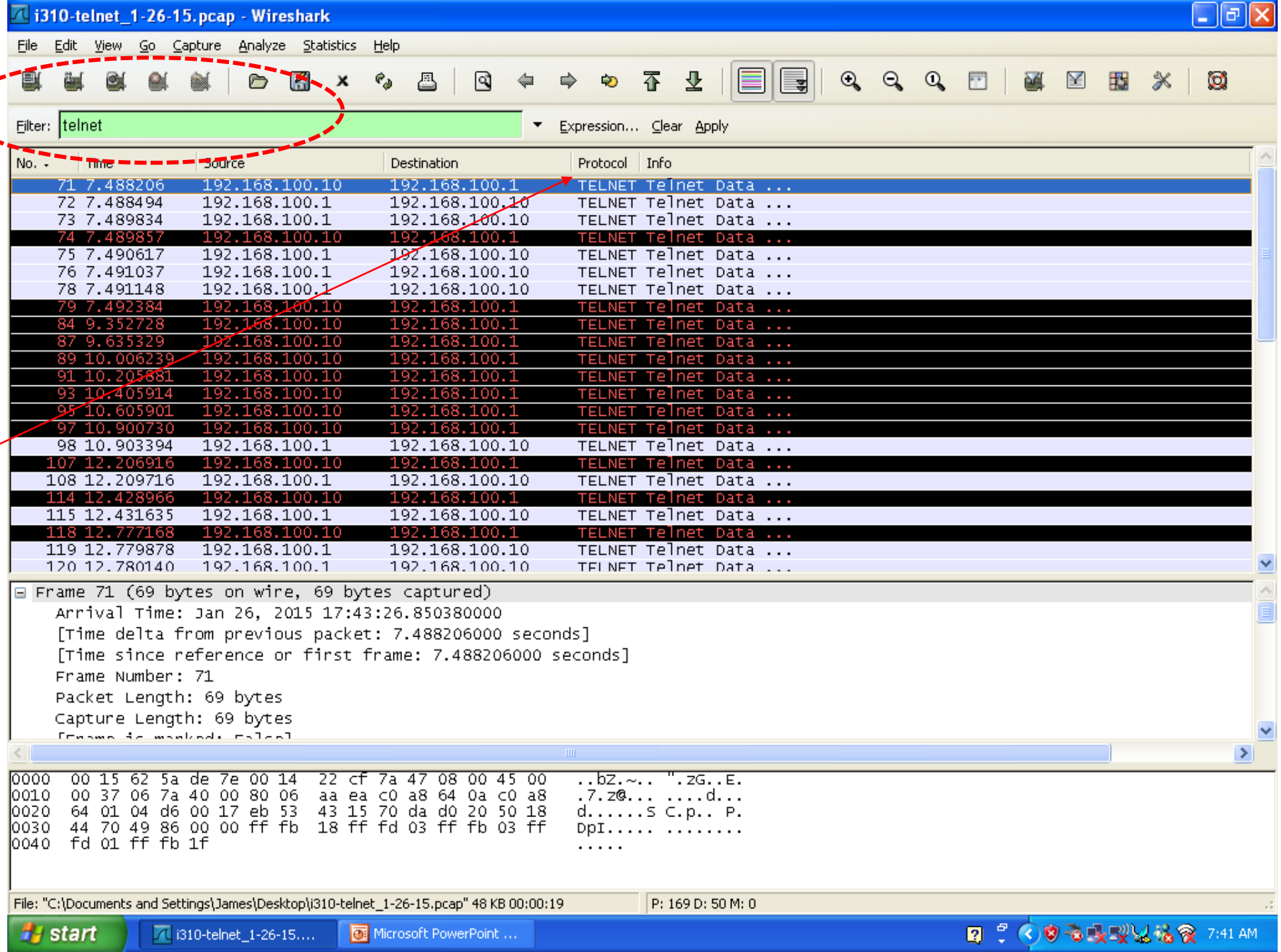
## Sample Capture:

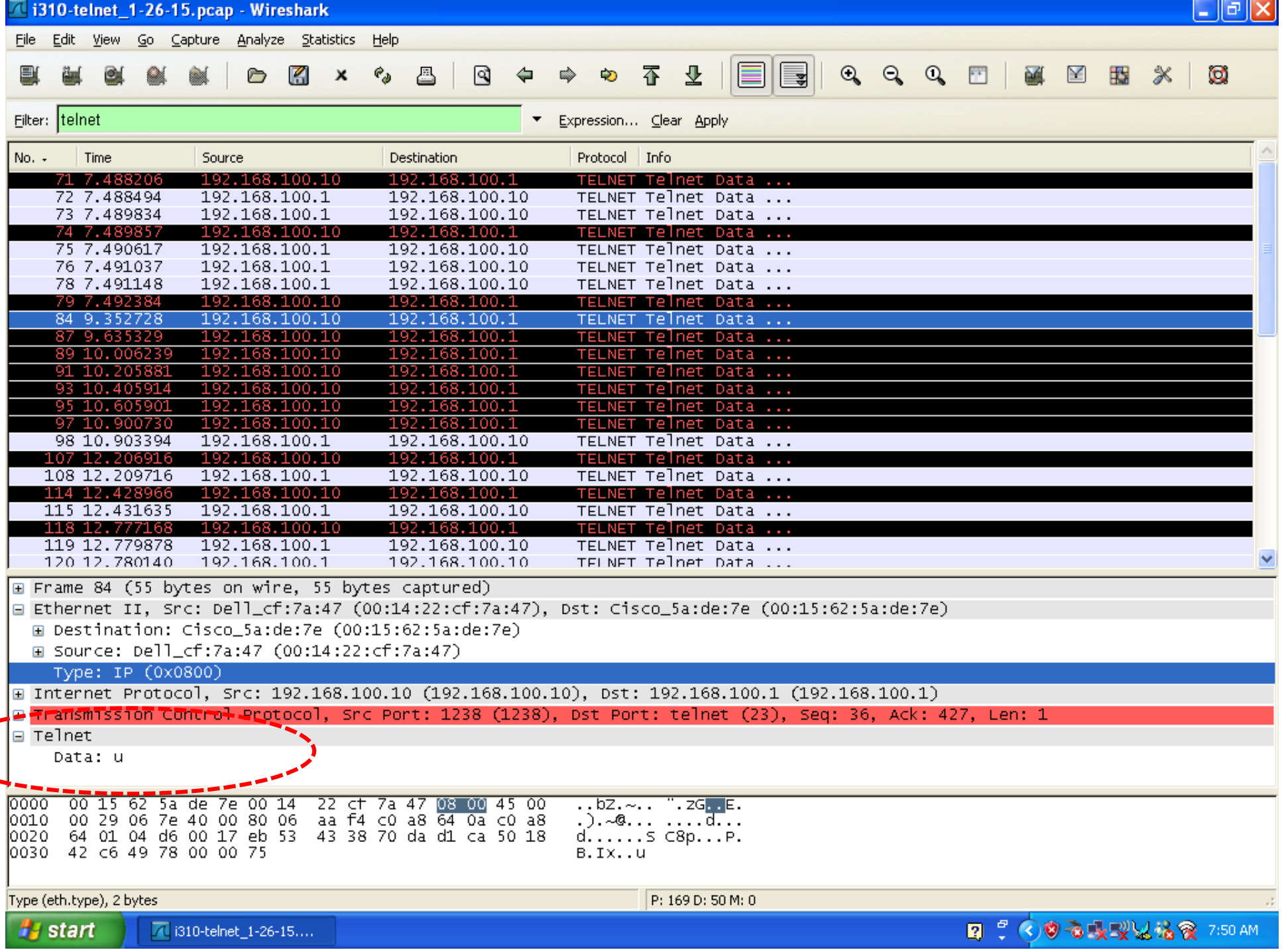
***Telnet app capture (multiple frames)***



**Enter telnet on filter line to only view telnet frames (app used in lab) <enter>**

**Notice how now only see telnet frames** *(easier to decode/view)*



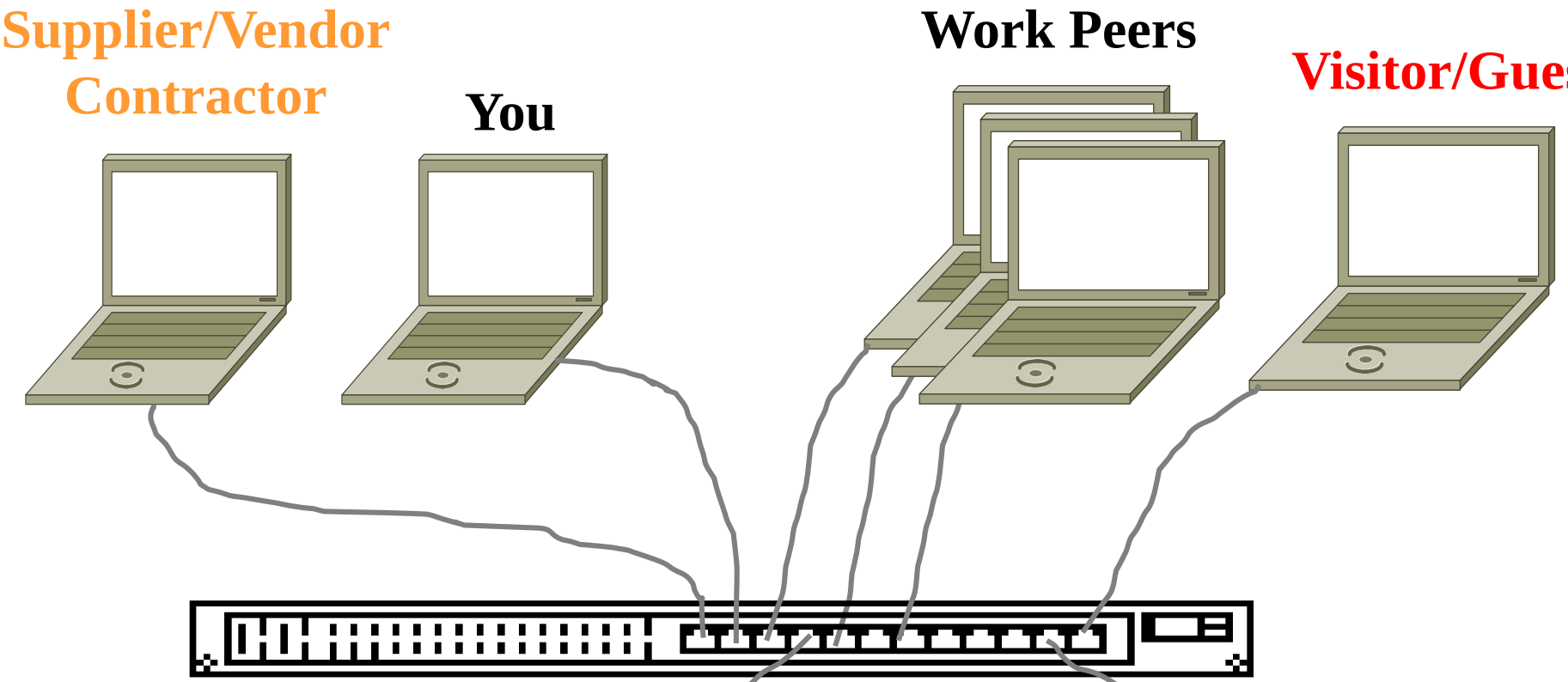



**telnet frame & detailed data view should first letter of password as sent asynch (1 char at a time)**

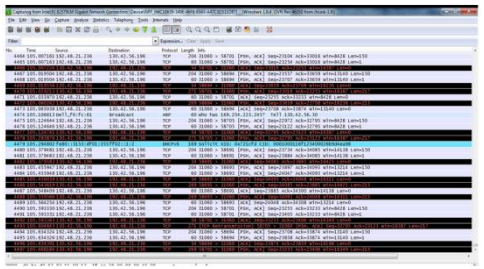
**Why 1 char at a time ?**

**VT100 protocol**

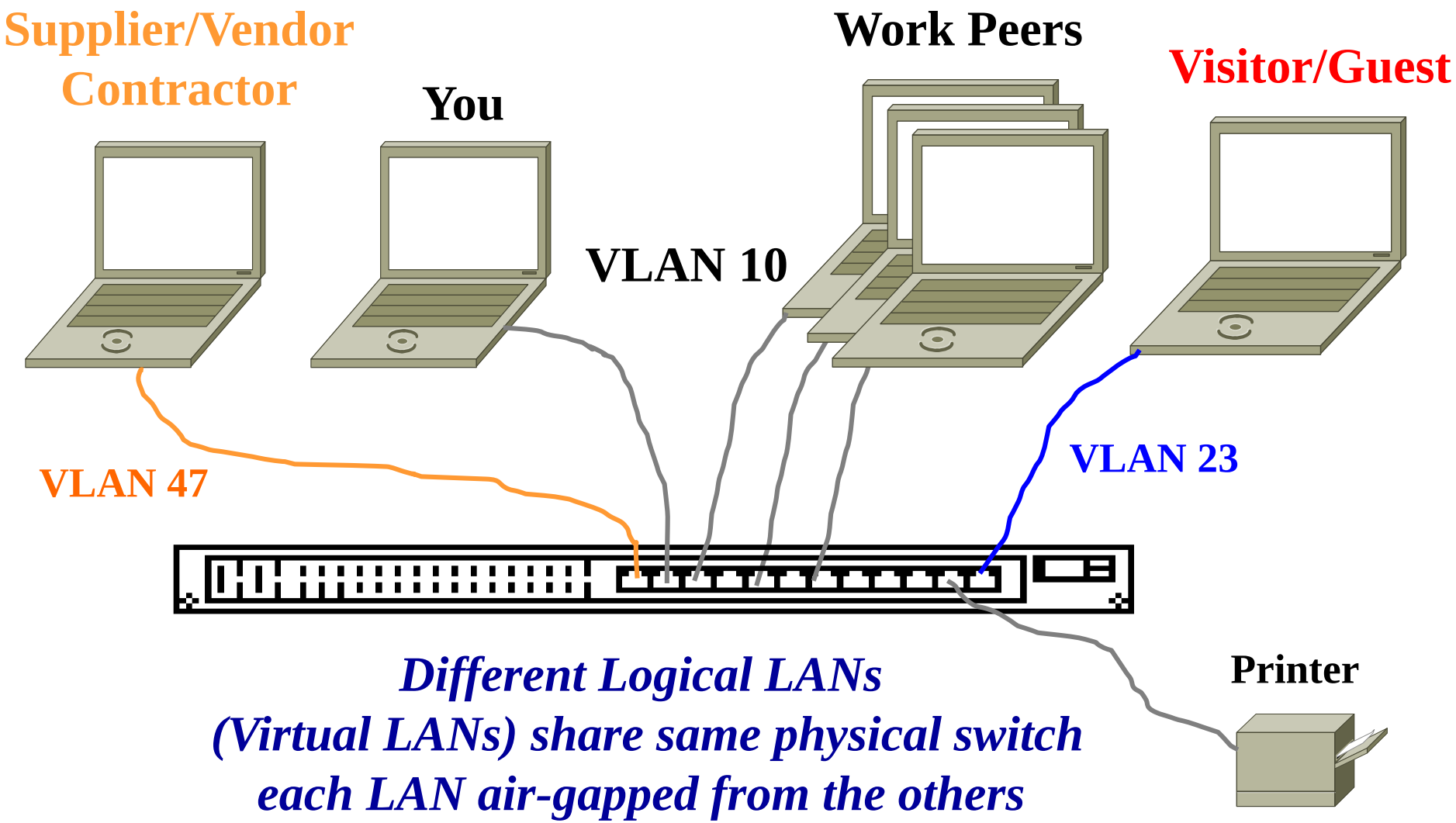
# VLANs (Virtual LANs)




*Ethernet Frame Protocol Decodes*

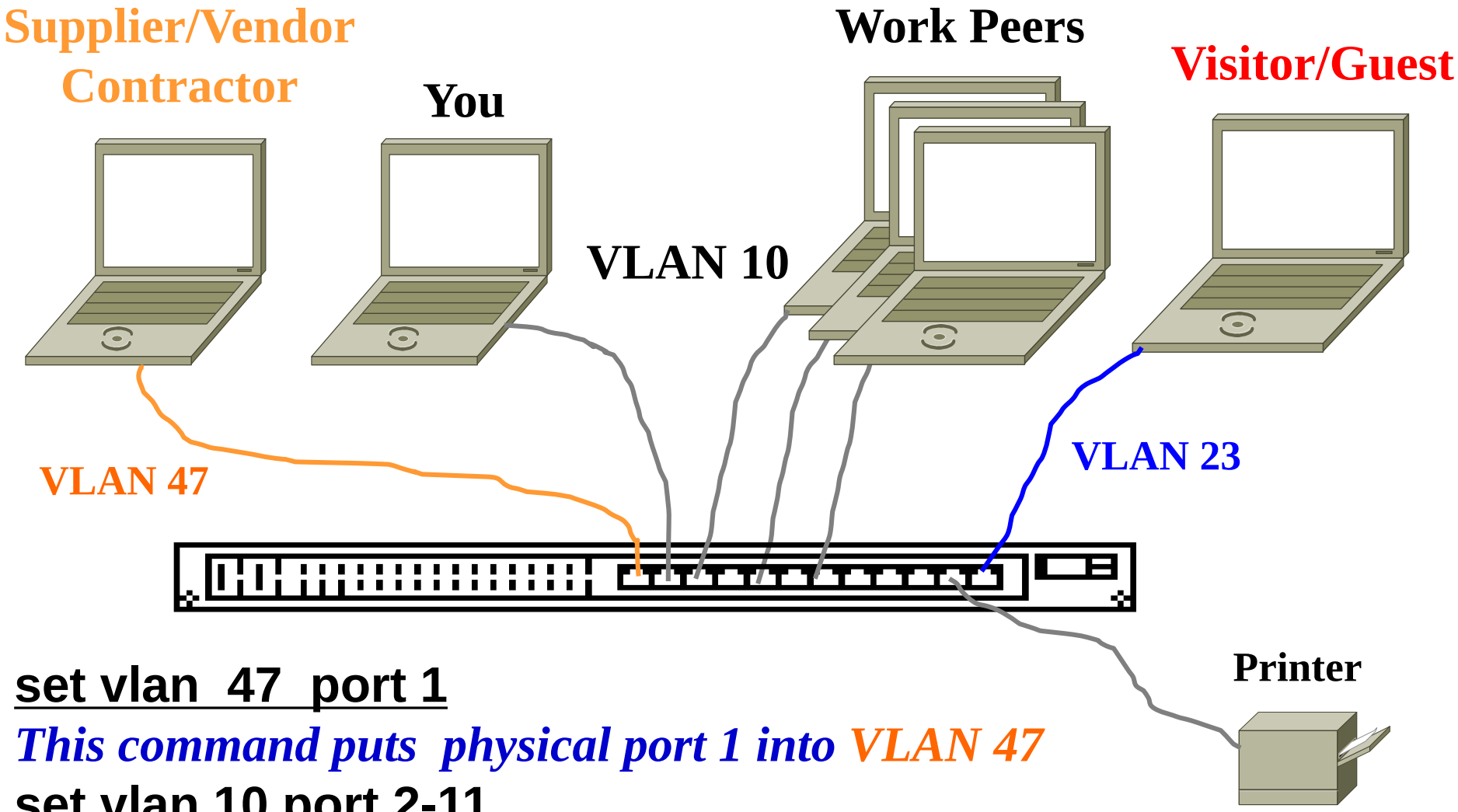


# VLANs (Virtual LANs)




*Different Logical LANs*
*(Virtual LANs) share same physical switch*
*each LAN air-gapped from the others*

# VLANs (Virtual LANs)




**set vlan 47 port 1**

***This command puts physical port 1 into VLAN 47***

**set vlan 10 port 2-11**

***This would put physical ports 2 thru 11 into VLAN 10***

***Question:*** *What command set for Visitor/Guest port into VLAN 23 ?*

**So now you have implemented LANs to segment internal and external traffic as a good security mechanism:**

**what threats/vulnerabilities has this eliminated ?**