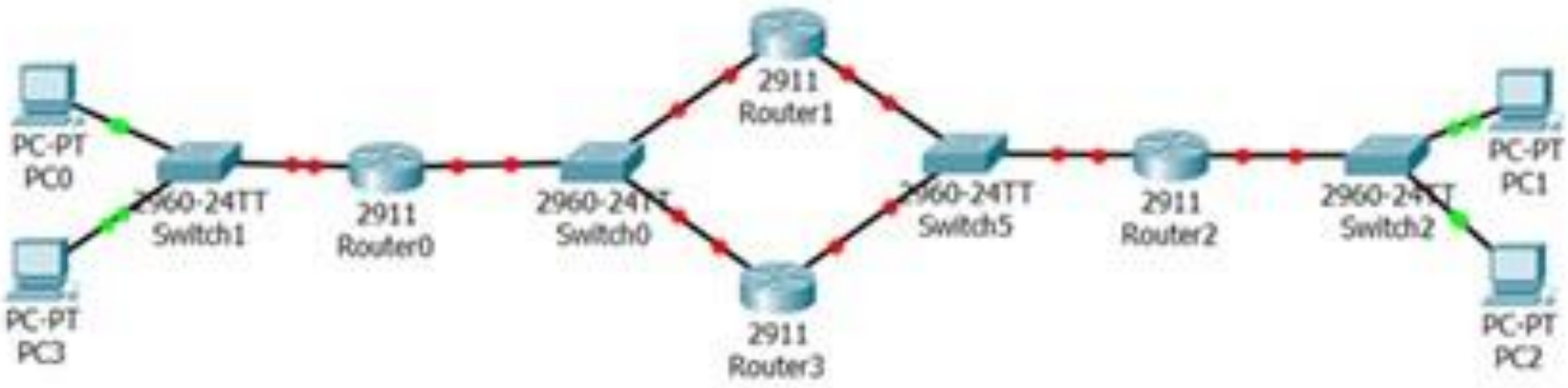

University of Colorado Boulder

Fundamentals of Data Communications

Network Analysis: Packet and Protocol Analyzers (Wireshark)

Levi Perigo, Ph.D.
University of Colorado Boulder
Department of Computer Science
Network Engineering

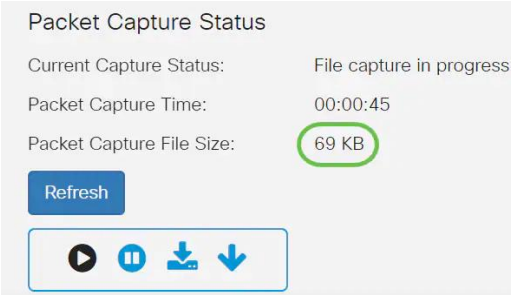
Review


PC-PT
PC0
PC-PT
PC3
2960-24TT
Switch1
2911
Router0
2960-24TT
Switch0
2911
Router1
2911
Router3
2960-24TT
Switch5
2911
Router2
2960-24TT
Switch2
PC-PT
PC1
PC-PT
PC2

```
Router(config-subif)#do show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES unset  up                    up
GigabitEthernet0/0.1       10.1.1.1        YES manual up                    up
GigabitEthernet0/0.2       10.1.10.1       YES manual up                    up
GigabitEthernet0/0.3       10.1.20.1       YES manual up                    up
GigabitEthernet0/1         unassigned      YES unset  administratively down down
Serial1/0                  unassigned      YES unset  administratively down down
Serial1/1                  unassigned      YES unset  administratively down down
Serial1/2                  unassigned      YES unset  administratively down down
Serial1/3                  unassigned      YES unset  administratively down down
FastEthernet2/0            unassigned      YES unset  administratively down down
```

```
interface GigabitEthernet0/0.1
 description VLAN1
 encapsulation dot1Q 1 native
 ip address 10.1.1.1 255.255.255.0
 no snmp trap link-status
!
interface GigabitEthernet0/0.2
 description VLAN10
 encapsulation dot1Q 10
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
!
interface GigabitEthernet0/0.3
 description VLAN20
 encapsulation dot1Q 20
 ip address 10.1.20.1 255.255.255.0
 no snmp trap link-status
```

Packet Analysis



- A packet analyzer or packet sniffer is a computer program (or hardware) that can *intercept* and *log* traffic that passes over a computer network or part of a network.
  - ***Packet capture is the process of intercepting and logging traffic***

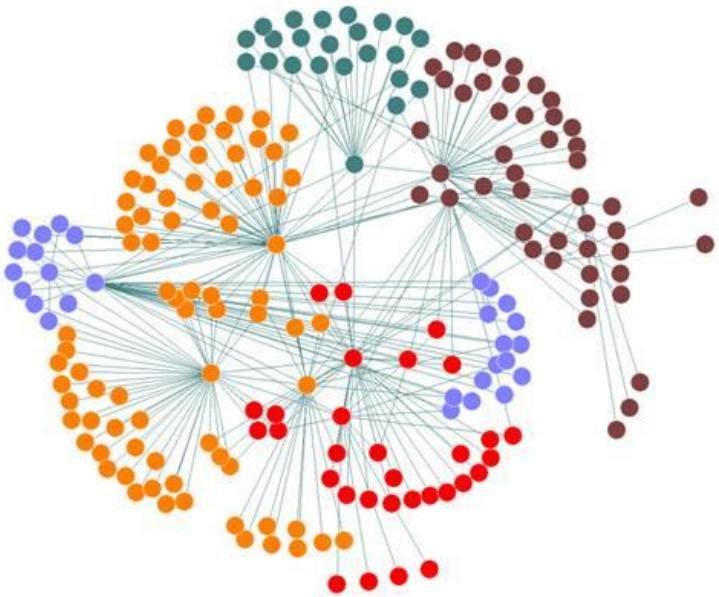
- One of the most important tools for a network engineer!

Network Analysis

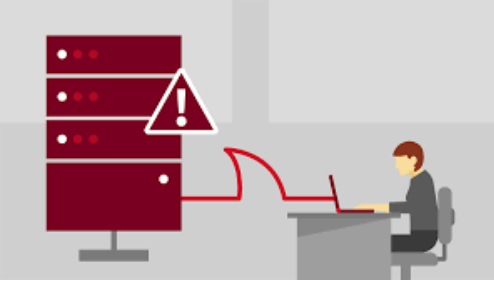
- **The process of listening to and analyzing network traffic**
- **Passive and non-intrusive**
- **Requires strong knowledge of network data flows**
  - Switch, Router, Firewall
- **Requires strong knowledge of TCP/IP and protocol communications (IPv6, UDP, ICMP, DHCP, etc.)**
  - Know the technology, figure out what's wrong

Purpose of Network Analysis

1. **Troubleshooting**
2. **Security**
3. **Network Optimization**
4. **Application Analysis**



Troubleshooting Tasks



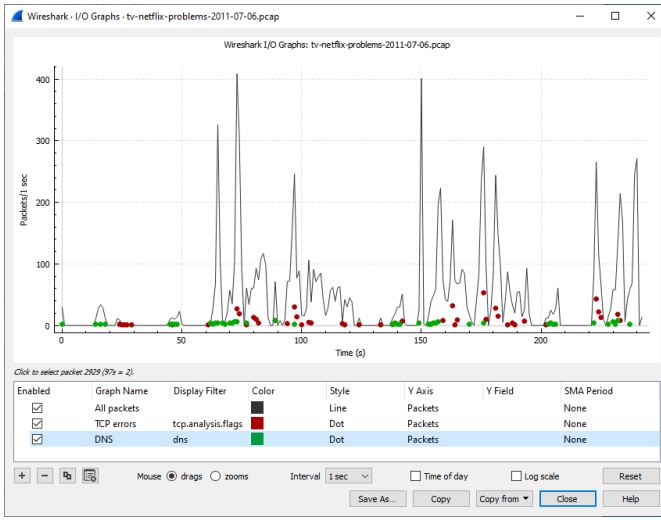
- **Locate faulty network devices**
- **Identify device or software misconfigurations**
  - DNS, DHCP, Rogue Access Point, IPSec
- **Measure high delays along a path**
  - Latency via “time” field
  - Server TCP SYN/ACK/RST and Slowstart

Troubleshooting Tasks Cont.

- **Locate the point of packet loss**
  - Almost always hardware device

- **Identify network errors and service refusals**

- **Graph queuing delays**



Security Tasks

- **Perform intrusion detection (IDS)**
  - Packets match filter
  - Can we perform IPS? What's the difference?
- **Identify and define malicious traffic signatures**
- **Passively discover hosts, OS, and services**
  - Where would we place analyzer?

Security Tasks Cont.

- **Log traffic for forensics examination**
  - Hash files (capinfos)

- **Capture traffic as evidence**

- **Test firewall blocking**
  - Outside and inside (make it through?)

- **Validate secure login and data traversal**
  - Is traffic encrypted as it should?

Legal Issues of Listening to Network Traffic (Telecom Policy)

- **ECPA (Electronic Communications and Privacy Act) "Wiretap Act"**
  - Prohibits the intentional, actual, or attempted interception, use…electronic communication

- **Security Issues to Consider**
  - Define policies regarding use of a traffic capture tool
  - Secure files containing network traffic
    - ***PII (Personally Identifiable Information)***
    - ***HIPPA & CMI***
  - Protect against unwanted sniffers
    - ***Block ports***
    - ***Wireless passwords***
    - ***Top 5 recommendations***

Network Optimization Tasks

- **Analyze current bandwidth usage**
- **Evaluate efficient use of packet sizes in data transfer applications**
- **Evaluate response times across a network**
  - Troubleshooting the time between TCP SYN/SYNACK
- **Validate proper system configurations**
  - How? Why?

Application Analysis

- **Why are applications important to the network?**

- **Analyze application bandwidth requirements**
  - Get a general summary of bandwidth usage and requirements
  - Ports? Time of day?

- **Identify application protocols and ports in use**

- **Validate secure application data traversal**

Analysis Review - Checklist

- **Find the top talkers**
  - Allocate bandwidth appropriately
- **Identify the protocols and applications used on the network**
  - Security – IDS
  - Baseline
- **Determine the throughput of applications or network traffic on a link**
  - Web server, FTP, Mail, etc.
- **List all hosts communicating on link**
  - Hosts you don't recognize or abnormal?
- **Learn the most common connection problems**
- **Latency and delays**

Analysis Review - Checklist Cont.

- **Identify and locate misconfigured hosts - How?**
  - DHCP
  - DNS
  - Gateway

- **Recognize segment/network or host that is slowing down traffic**
  - Top Talkers
    - ***What do you do?***

- **Locate asymmetric traffic prioritization**

- **Graph HTTP flows**
  - Examine website rates

- **Identify errors for specific protocol (HTTP, SIP, FTP, etc.)**

- **Build graphs to compare traffic: good, normal, poor**

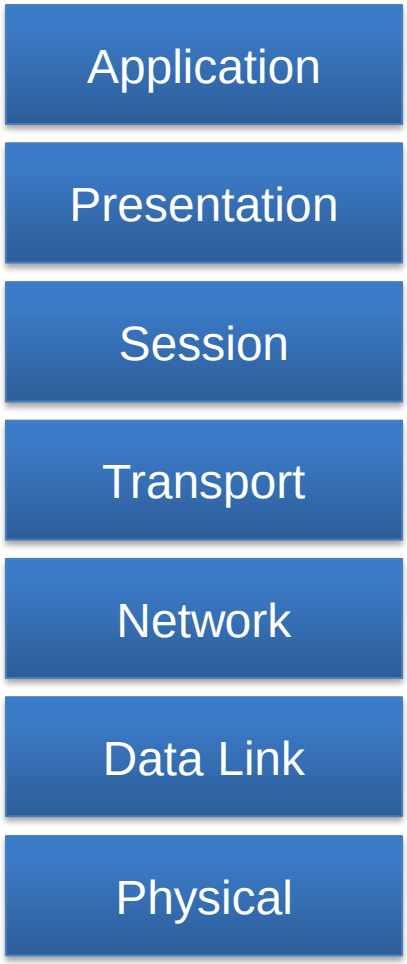
Analysis Review - Checklist Cont.

- **Identify applications that do not encrypt traffic**
- **Detect and analyze OS use on network**
- **Replay VoIP conversations to listen to quality**
  - VoIP Lab
  - What else could you do with this information?

Understand Network Traffic Flows

- **Switch**
  - Layer 2 device
  - MAC addresses
  - Collision domain
  - Can’t tell if it has gone through switch (transparent)
- **Router**
  - Layer 3 device
  - IP addresses
  - Broadcast domain
  - MAC
  - TTL
- **Firewall, Proxy, NAT/PAT**
  - Proxy = Layer 4
  - PAT = Layer 3 and ”4”
  - IP address modifications

OSI Model Review



What is Wireshark?

- **Packet and Protocol Analyzer**
  - Analyzing Traffic
  - Troubleshooting Tasks
  - Security Analysis
  - Application Analysis

- **Rated the #1 Open-Source App of all time**
  - #1 Network Protocol Analyzer
  - #1 Network Security Tool

Wireshark

- **Typical Uses**
  - First responder tool!
  - Determine Bugs – How?
  - Top Talkers
  - Slow Response Times and Delayed Traffic
  - Network Traffic
  - **What is on the wire!

- **Name changed from Ethereal to Wireshark in 2006 for copyright reasons.**

- **Certification – Wireshark Certified Network Analyst (WCNA) (*not recommended*)**

How to get it?

- **You can download for computer FREE at www.wireshark.org.**

- **All Wireshark files are .pcap or .pcapng**
  - TShark = .pcapng

- **What version to get?**
  - Upgrade occasionally
  - Stick with what works

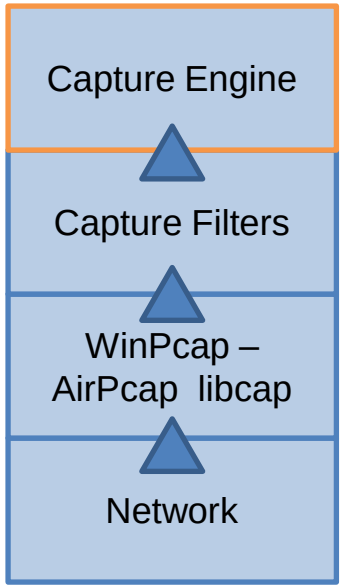
- **Help**
  - ask.wireshark.org

Why Wireshark?

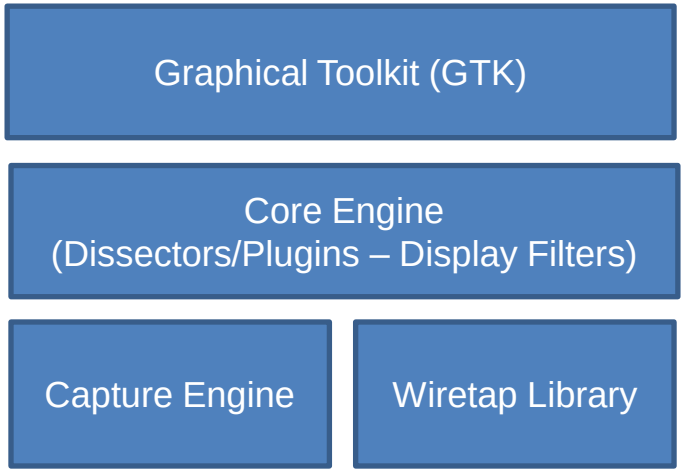
- **Persistent**
  - Remote/Left on Site
- **Standardization**
  - Anyone can read Wireshark
    - ***Vendor specific logs/debugs***
- **Logs/Debugs vs. .pcap**
  - Logs can be misleading, or they do not capture the whole story
  - Debugs can be wrong
    - ***Why?***
  - .pcap = packets do not lie!

Wireshark Elements

- **Capturing Traffic**
  - Drivers
    - ***NIC – Wireless – Open File***
  - Capture Filters
    - ***Use Sparingly***
      - Example: Only capture DNS traffic
    - ***Can't get that traffic back!***
    - ***Use <u>Display</u> Filters instead of Capture Filters***
  - Wiretap library
    - ***Can open almost any file (not only .pcap)***



Processing Packets



Place the Analyzer Appropriately

- **Placement is Key!**
  - General Rule / Best Practice
    - ***Place Analyzer as close to the complaining user/suspecting unit as possible – Why?***
  - See from the client's perspective
    - ***If errors coming from server; then move or add another analyzer to the sever location***
  - Multiple Locations
    - ***(Problems with this?)***

Where to implement it?

- Depends on the problem and the network configuration

- If you suspect or know that between the client and the server there are some devices that can ‘’mangle’’ the network communications (NAT/Websense appliances, IPSec, firewalls, etc.)
  - ***Capture in multiple places***

Capture Appropriate Traffic

- **Where do we place it?**
  - Connecting Analyzer to Switches
    - ***Forward based on target MAC address; doesn't reach analyzer***
    - ***Analyzer Receives Four Types of Traffic***
      - Broadcast
      - Multicast (if configured to pass MCAST)
      - Unknown MAC
      - Analyzer MAC

Capture Appropriate Traffic - Options

- **Install on host machine**
  - Security Issues
    - ***Individual***
  - Unavailable
  - May be unreliable
    - ***CPU Usage***
- **Tap Device**

- **Port Span/Port Mirror**
  - Switch Capable
  - Administrator Capable
- **Install Hub**
  - Half-duplex
  - Move Device to Hub too!

Capture Appropriate Traffic

- **What about a wireless network?**
  - Promiscuous and/or Monitor Mode
    - ***All traffic***
  - Need to see Control and Management Frames
  - Physically stand by the person/device
    - ***Stand by AP (if all users)***
  - WISpy adapter and/or AirPCAP adapters

Wireshark - Tips and Tricks

- **Display Filters**
- **Statistics**
- **Coloring Rules**
- **Filter, Graph, Analyze**

Display Filters

- **Error Detection = Green vs. Red**
  - Keep Typing example:
  - ip.addr==255.255.2 (not green)
    ip.addr==255.255.255.255 (green)
  - Just because it is a valid filter doesn't mean it is appropriate
    - ***Example: HTTP vs. HTTPS***

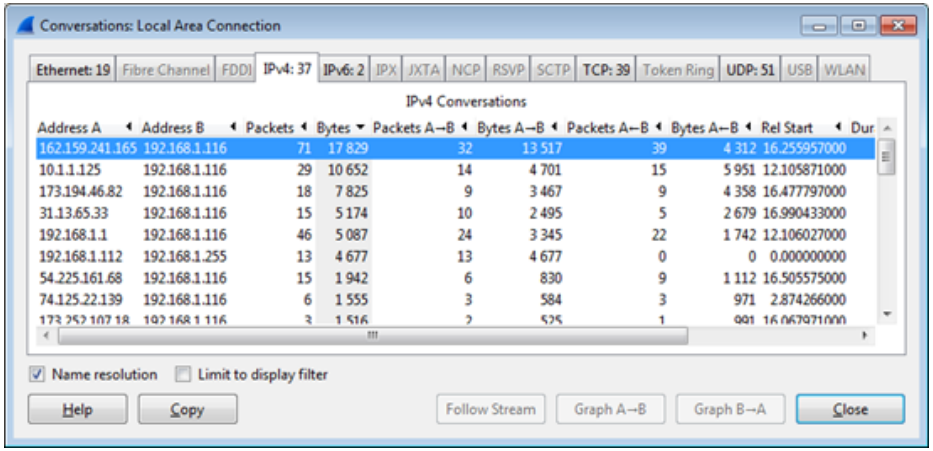
Display Filters Cont.

- **Right Click is Easy Method**
  - Note: Not Selected is Good Option

- **Apply vs. Prepare**
  - Apply - takes affect immediately
  - Prepare - enters syntax to be changed/modified if needed
    - ***HTTP Errors are 399 and above***
    - ***http.response.code == 404 change to http.response.code > 399***

Stats

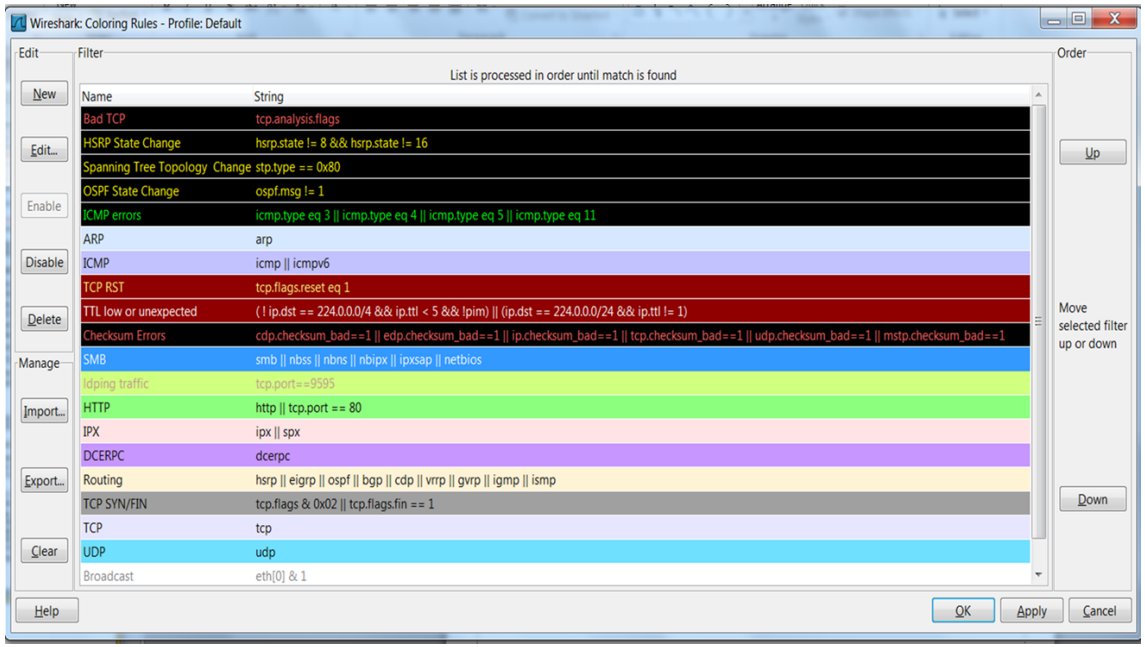
- **Statistics**
  - Top Talker
    - ***Statistics > Conversations > Bytes > Apply as Filter***
    - ***Statistics > Endpoints > IPv4 TX bytes > Apply as Filter***



Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Dur
162.159.241.165	192.168.1.116	71	17 829	32	13 517	39	4 312	16.255957000	
10.1.1.125	192.168.1.116	29	10 652	14	4 701	15	5 951	12.105871000	
173.194.46.82	192.168.1.116	18	7 825	9	3 467	9	4 358	16.477797000	
31.13.65.33	192.168.1.116	15	5 174	10	2 495	5	2 679	16.990433000	
192.168.1.1	192.168.1.116	46	5 087	24	3 345	22	1 742	12.106027000	
192.168.1.112	192.168.1.255	13	4 677	13	4 677	0	0	0.000000000	
54.225.161.68	192.168.1.116	15	1 942	6	830	9	1 112	16.505575000	
74.125.22.139	192.168.1.116	6	1 555	3	584	3	971	2.874266000	
173.252.107.18	192.168.1.116	3	1 516	2	525	1	991	16.067971000	

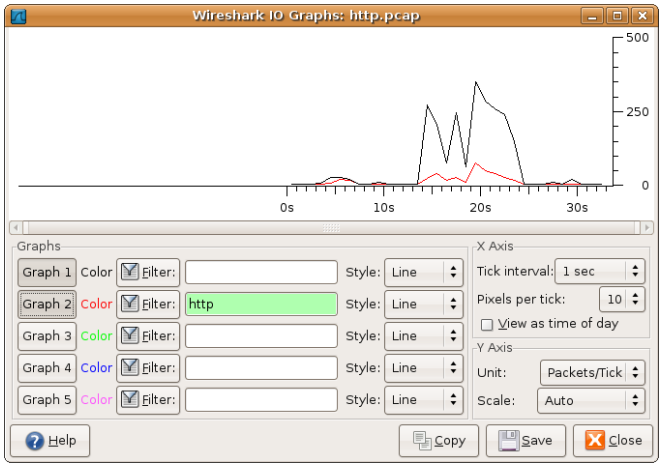
Coloring Rules

- Great to add to different Profiles
- Note: Work in “Top Down” fashion, similar to ACLs



Filter, Graph, and Analyze Traffic

- **Expert Info Window**
  - Button in Bottom Left = Gray vs. Yellow
  - Click on Yellow Button; then focus on errors
    - ***Details and Charts are rarely used***



- **Charts and Graphs**
  - Security
    - ***What protocols clients are using?***
    - ***Statistics > Protocol Hierarchy***
    - ***Statistics > Conversations***
      - Check box for Limit to Display Filter
  - Graphs
    - ***Statistics > IO Graphs***
      - Maps throughput download in graph format
      - Can alter multiple graphs overlapping to see when/why throughput drops
    - ***Statistics > TCP Steam Graph > Throughput Graph***
      - Must contain data in packet
    - ***Statistics > TCP Steam Graph > Round Trip Time Graph***
    - ***Statistics > HTTP > Requests***

CLI Access

- **Terminal-based Wireshark**
  - TShark

- **TCPDump**

The “Needle in the Haystack” Issue

- **The #1 reason network engineers shy away from analysis tools**
- **Capture close to client first**
- **Rarely use *capture filters***
  - Okay if you are in the middle of the enterprise – Why?
- **Use *display filters* to exclude “good” traffic or focus on “bad” traffic**
- **Colorize “bad” or “questionable” traffic**
- **Add filter expression buttons or specific profiles to quickly find network problems**
  - Lab
- **Reassemble for clarity/easy understanding**
  - “Follow the stream”
- **Graph for visibility**

Troubleshooting

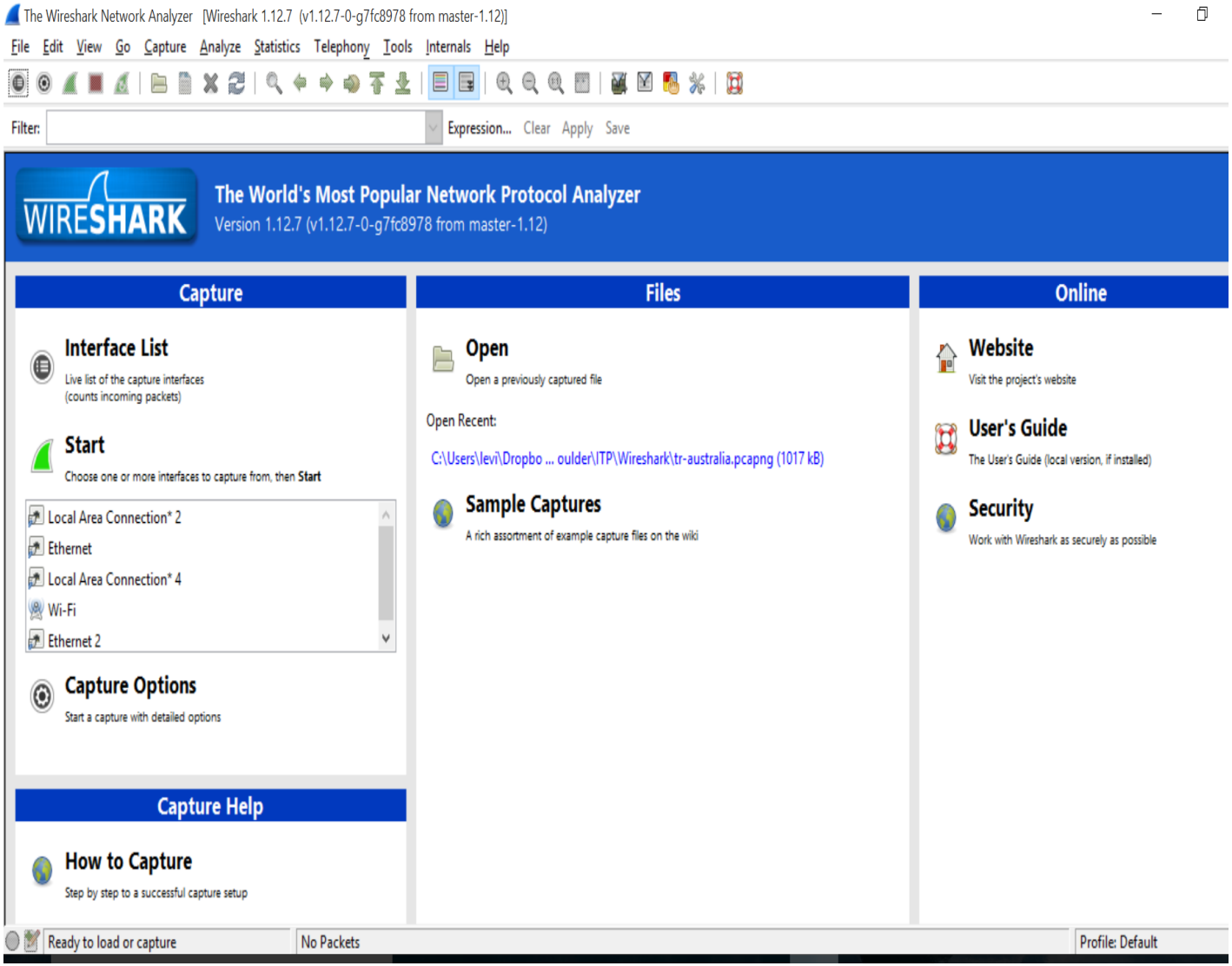
Questions?

References

- **Chappell University**
- **Chapell, L. (2013) Wireshark 101**

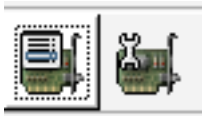
Appendix

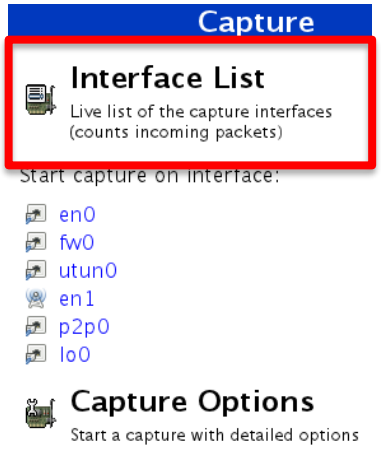
The Interface



How to start a capture

- Starting a capture can be done in multiple ways. The most common are:

1. Select an interface from the interface list: the capture begins immediately with the default option
2. Click on the Interface List
3. Click on the one of the two first icons of the ribbon 



How to start a capture

4. Press Ctrl+E
5. Use the Capture menu

- When you start a capture you can generally choose some options (except when you press CTRL+E or click directly on the interface: In these cases the capture starts immediately).
- The most important options you need to know in the option pane are:
  promiscuous mode, capture filter & enable network name resolution.
- CAVEAT: use the enable network name resolution option sparingly! This option will generate a lot of DNS requests and so DNS replies as well. You may not want to generate this kind of traffic.

Promiscuous mode or not?

- In Promiscuous Mode your network interface is going to receive all the traffic even if it is not directed specifically to it.

  Example: a device (IP 10.14.8.1) is trying to talk with another device (IP 10.14.8.2) on the same network segment.
  If you are in Promiscuous Mode you should be able to see the conversation even if it is not for you.
- There are many factors that may limit your visibility while you are in Promiscuous Mode such as network switches! If your switch is a ‘’proper one’’ should direct the traffic from device A to device B to the switch ports where A and B are physically plugged in.
- There are some solutions to this problem: configure the switch to repeat all the traffic to a SPAN port, use an HUB to connect the devices (if you are still able to find one) or ask budget to buy an Aggregating Network TAP)
- If you are not in Promiscuous Mode you will be able to see all the traffic direct to you, broadcast and multicast traffic.

Capture Filters

Some Common and Capture Filters:

ip	Only IP traffic
tcp	Only TCP traffic
udp	Only UDP traffic
host 192.168.0.1	All the traffic to/for 192.168.0.1
not broadcast and not multicast	Self explanatory
ether src 10:10:EA:11:33:22	All the Ethernet traffic from that MAC address
ether dst 10:10:EA:11:33:22	All the Ethernet traffic to that MAC address
ether host 10:10:EA:11:33:22	All the Ethernet traffic to/for that MAC address
port 80	Udp or Tcp traffic where the source or destination port is the 80
tcp and udp	Only TCP and UDP traffic

Display Filters

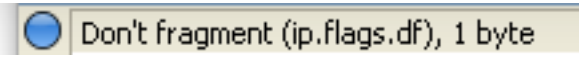
- Display filters: their knowledge is essential to analyze the traffic. They help us to display only the interesting traffic and solve the famous ‘’needle in the haystack” problem
- They can be applied while you are capturing or after the capture is finished.
- Their syntax is used for Columns definition and coloring rules as well.
- Wireshark comes already with a predefined list of filters that can be used as example (starting point)
- Display Filters as the Capture Filters are case sensitive ! HTTP is not the same of http
- Fortunately when you type filters in the filter field you can use Intellisense.

Display Filters

- To create a filter you can simply type it in the filter field and get the advantage of Intellisense.
- Another way to create a filter is to explode a packet in the details section, click on a particular section of it, then right click and choose Prepare Filter or Apply filter.
- The difference between apply and prepare is that Apply will immediately apply the filter instead prepare will only prepare the filter in the filter field and then you will need to press the Apply button. The advantage is that you can have a look to the syntax generated and eventually amend it before to apply it.
- Another way is to press the Expression button that’s near the Filter field: a GUI to help you to formulate the expression will appear.

Display Filters

- But what about if I want to filter a certain field but I do not know its name?
  - The simplest way is to explode the packet and select the field in the Packet Display section and have a look to the Status Bar.



- In this case we selected the Do not fragment field and its syntax is ip.flags.df == 1 (1 is set , 0 is not)

- The general structure of a display filter is a sequence of expressions eventually concatenated by logic operators. An expression is a field + comparison operator + value.
  Example: **tcp.dstport == 80**
- The most common comparison operators are:
  ==, ||, &&, >=, !=, <=, >, <, matches, contain. For the nostalgic geek it is possible to use the literals **eq, or, and, ge, ne,le,gt,lt**
- && and || are logic operators
- An example: **tcp.port == 80 || tcp.port == 443**
- As with the display filter we need to be careful of the meaning of them
- For example **tcp && arp** is a syntactically valid filter but, won't match any traffic
- Some popular protocols define some basic filters that help us to speed up the writing of filters.
- For example instead of writing: tcp.port == 53 || udp.port == 53 we can simply write: dns
- Instead of **tcp.port==80 ||tcp.port == 443** we can write: **http**
- Other popular protocols are: arp, bootp, smtp, pop3, smb, ftp, ftp-data, ldap, icmp, imap

Advanced Filters

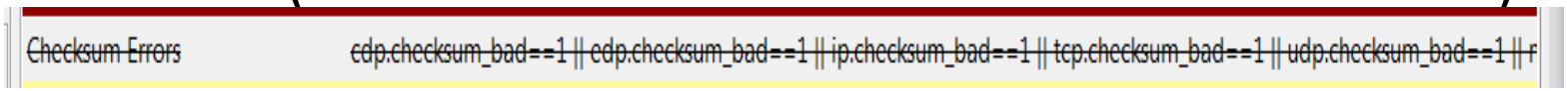
- In some special circumstances we need to match one or more bytes of a packet in specific positions. This type of filter is called offset filter and it is in this form:
  field (or protocol layer)[offset 0 based:length] comparison value
- Example: eth.src[4:2]==22:1f
- Example: ip[14:2] == 90:20
- To formulate this kind of filter you need to know the protocol well and know what you are looking for.

Coloring Rules

- Coloring Rules and Columns: they are defined with the same syntax used for Display Filters.
  - Have you noticed in captures that some packets have a different color from the others?
- The Coloring Rules are a very import tool that will help you to better understand the trace file: you will be able to display different kind of packets in a different color and this will help you a lot to find the “needle in the haystack.”
- You can manage them via the View -> Coloring Rules menu

Coloring Rules

- Coloring rules color a packet if the rule, expressed with Display Filter syntax, is matched.
- Coloring rules can be created, deleted, moved up and down, disabled, imported, exported or reset to default (Cleared).
- Coloring rules are saved in the colorfilters file.
- Rule precedence: the rules are evaluated from the top to the bottom of the list. When a rule is matched the evaluation finishes for that packet.
- How to disable one: Checksum errors*(Most of the time this a false positive error caused by TCP/UDP offloading settings of your network adapter)*
- To disable it simply select it and then press the disable button. A line will appear on it marking that the rule is disabled. (It is better to disable rules than delete them)

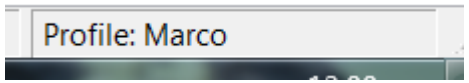


Columns

- Columns are fundamental to view the traffic you captured.
- The default column set is not always appropriate for the analysis of all the problems you want to analyse.
- So it is possible to define custom columns, resize them and re-arrange them as you like.
- Clicking on a column you can sort the data in ascending and descending order: this feature is particularly useful when you order the capture for “Seconds since previous captured/displayed packet”
- Custom Column definition needs the field name you want to display: the same field name you use in the Display Filter syntax.

Creating a New Column

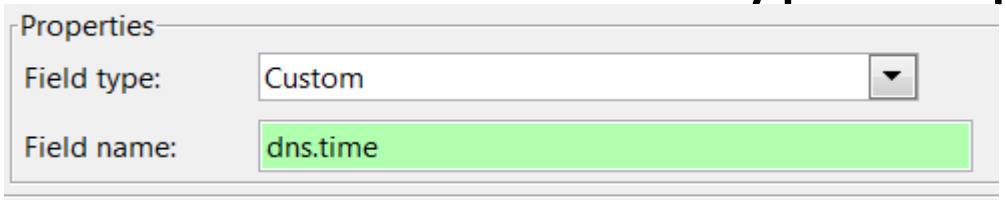
- There are many ways to create a custom column:
  -Edit -> Preferences -> Column section.
  -Right click on a column and select Column Preferences.
  -Right click on a field and choose the option Apply as a column: in this case the column definition is applied immediately. If the column definition created is not what you want you will need to edit or remove it using the Column Preferences menu
- Column definition is saved in your current profile directory in the preferences file(the active profile is displayed in the right down corner of Wireshark Window)



Define a Custom Column

- Example create a new custom column:

1. Click on Edit -> Preferences -> Column section.
2. Click the Add button.
3. Select Custom from the Field Type drop down



4. Enter the field that you want to display in the column in the “Field name” field
5. Click on the title of the column and name it, then press Apply and then OK

Useful Columns to Add

- The columns you add depend on the traffic you are going to analyse. You may want to create different configuration profiles for different situations and define a different column set in every profile.
- You can reposition the columns, delete them or simply hide them.