

Wireshark Tutorial

Chris Neasbitt

UGA Dept. of Computer Science

Contents

- Introduction
 - What is a network trace?
 - What is Wireshark?
- Basic UI
 - Some of the most useful parts of the UI.
- Packet Capture
 - How do we capture packets?
- Trace Analysis
- Individual Packet Analysis
- Filters
- Exercises

Introduction

- Network Traffic Trace

- A recording of the network packets both received by and transmitted from a network interface.

- What is a pcap file?

- pcap = Packet Capture
- File format originally designed for tcpdump/libpcap.
- Most widely used packet capture format.

Introduction

- What is Wireshark?
 - A graphical network packet analyser.
 - Found at <http://www.wireshark.org>
 - The complete manual is located [here](#).
- What some are it's uses?
 - Troubleshoot network problems.
 - Learn network protocol internals.
 - Debug protocol/program implementation.
 - Examine network-related security issues.

Basic UI

Menu

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	Broadcast	ARP	42	Gratuitous ARP for 192.168.0.2 (F
2	0.299139	192.168.0.1	192.168.0.2	NBNS	92	Name query NBSTAT *<00><00><00><0
3	0.299214	192.168.0.2	192.168.0.1	ICMP	70	Destination unreachable (Port un
4	1.025659	192.168.0.2	224.0.0.22	IGMP	54	v3 Membership Report / Join group
5	1.044366	192.168.0.2	192.168.0.1	DNS	110	Standard query SRV _ldap._tcp.nbc
6	1.048652	192.168.0.2	239.255.255.250	SSDP	175	M-SEARCH
7	1.050784	192.168.0.2	192.168.0.1	DNS	87	Standard query SOA nb10061d.ww004
8	1.055053	192.168.0.1	192.168.0.2	SSDP	32	HTTP/1.1 200 OK
9	1.082038	192.168.0.2	192.168.0.255	NBNS	110	Registration NB NB10061D<00>
10	1.111945	192.168.0.2	192.168.0.1	DNS	87	Standard query A proxyconf.ww004.
11	1.226156	192.168.0.2	192.168.0.1	TCP	62	ncu-2 > http [SYN] Seq=0 win=6424
12	1.227282	192.168.0.1	192.168.0.2	TCP	60	http > ncu-2 [SYN, ACK] Seq=0 Ack

Packet List

Packet Details

- Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
- Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
- Internet Protocol, src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
- Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0
 - Source port: ncu-2 (3196)
 - Destination port: http (80)
 - [Stream index: 5]
 - Sequence number: 0 (relative sequence number)
 - Header length: 28 bytes
 - Flags: 0x02 (SYN)
 - window size value: 64240

Packet Bytes

```
0000  00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00  ..[-u... ] .....F.
0010  00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8  .0.H@... a...
0020  00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02  ...|.P<6
0030  fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02  .....
```

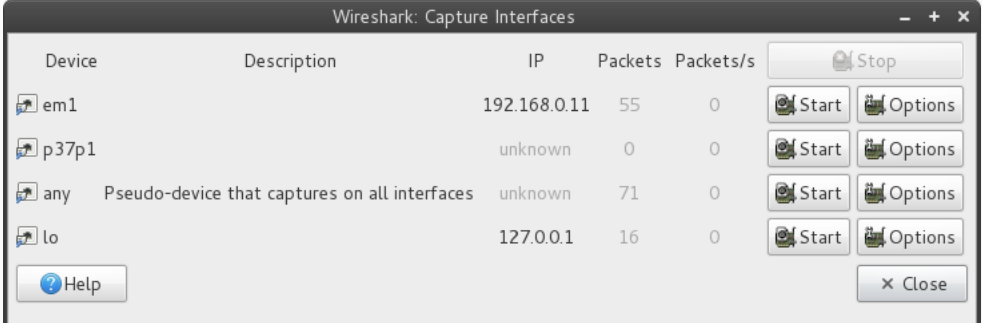
File: "C:/test.cap" 14 KB 00:00:02 Packets: 120 Displayed: 120 Marked: 0 Load time: 0:00.000 Profile: Default

Basic UI

- File -> Open
 - Opens a packet capture file.
- View -> Time Display Format
 - Change the format of the packet timestamps in the packet list pane.
 - Switch between absolute and relative timestamps.
 - Change level of precision.
- View -> Name Resolution
 - Allow wireshark to resolve names from addresses at different protocol layers.

Basic UI

- Capture -> Interfaces
 - Available network interfaces for capture.
 - Total packets per interface.
 - Packet rate per interface.

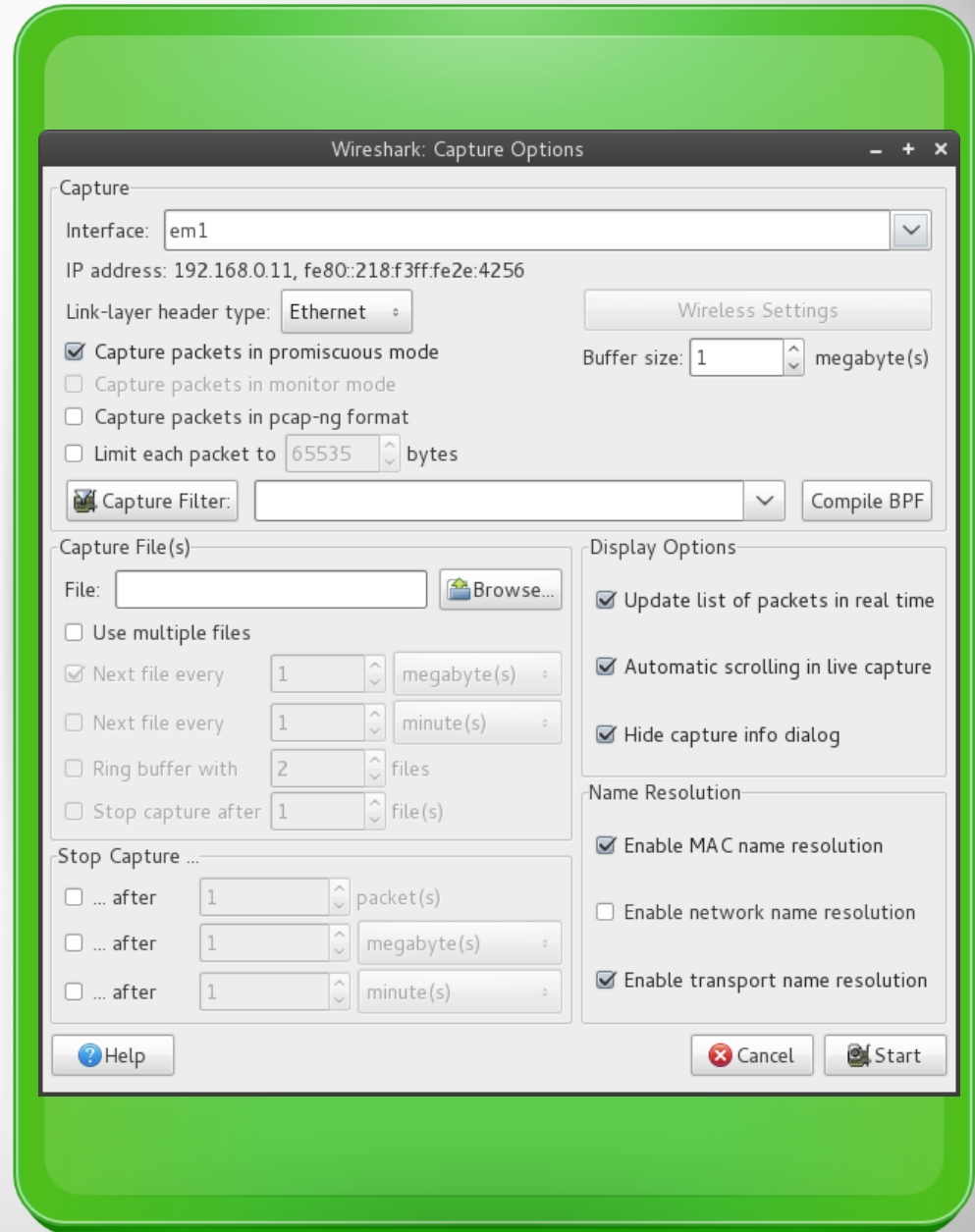


The screenshot shows the 'Wireshark: Capture Interfaces' window. It contains a table with columns for Device, Description, IP, Packets, and Packets/s. Each row has a 'Start' button and an 'Options' button. There is also a 'Stop' button at the top right and a 'Close' button at the bottom right. A 'Help' button is located at the bottom left of the table area.

Device	Description	IP	Packets	Packets/s	Start	Options
em1		192.168.0.11	55	0	Start	Options
p37p1		unknown	0	0	Start	Options
any	Pseudo-device that captures on all interfaces	unknown	71	0	Start	Options
lo		127.0.0.1	16	0	Start	Options

Basic UI

- Capture -> Options
 - Set various capture parameters.
- Promiscuous mode
 - On – record all packets reaching the interface.
 - Off – record only those packets directed to the host.

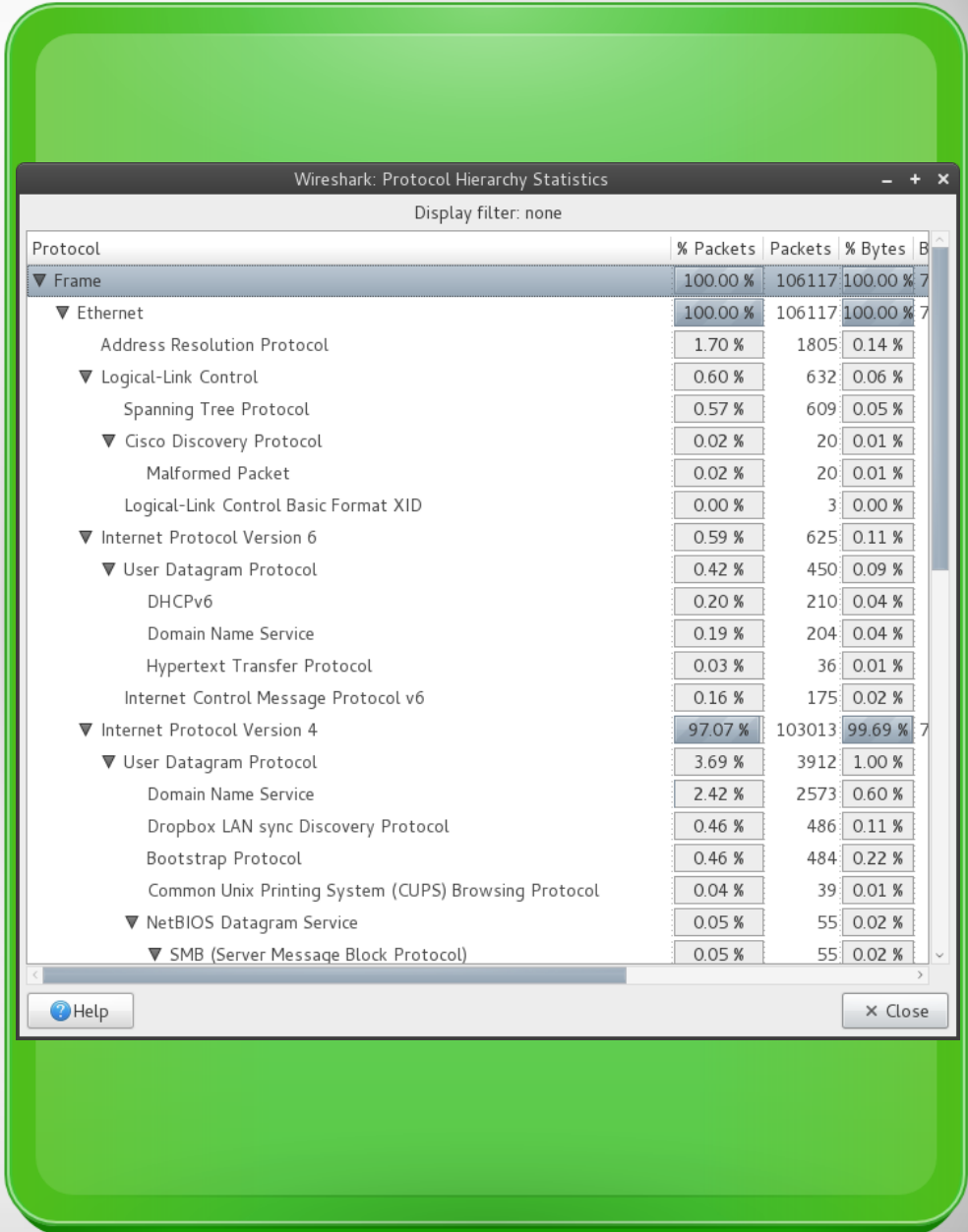


Basic UI

- Analyze -> Follow TCP Stream
 - Applies a filter to follow a single tcp conversation within the trace.
 - Displays the reassembled data section of each packet in the conversation.
 - Useful for debugging or analyzing any TCP based application layer protocol.
 - HTTP, FTP, SSH, LDAP, SMTP, etc.

Basic UI

- Statistics -> Protocol Hierarchy
 - Presents descriptive statistics per protocol.
 - Useful for determining the types, amounts, and relative proportions of protocols within a trace.



Wireshark: Protocol Hierarchy Statistics

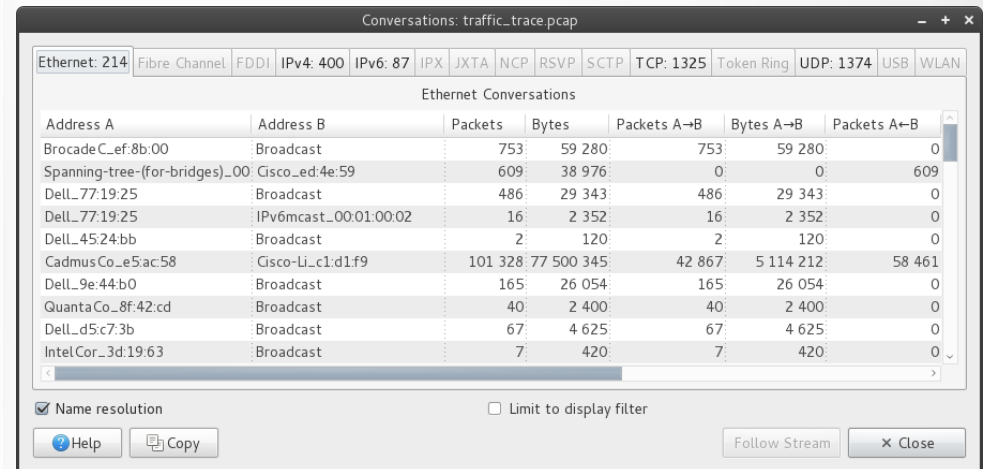
Display filter: none

Protocol	% Packets	Packets	% Bytes	B
▼ Frame	100.00 %	106117	100.00 %	7
▼ Ethernet	100.00 %	106117	100.00 %	7
Address Resolution Protocol	1.70 %	1805	0.14 %	
▼ Logical-Link Control	0.60 %	632	0.06 %	
Spanning Tree Protocol	0.57 %	609	0.05 %	
▼ Cisco Discovery Protocol	0.02 %	20	0.01 %	
Malformed Packet	0.02 %	20	0.01 %	
Logical-Link Control Basic Format XID	0.00 %	3	0.00 %	
▼ Internet Protocol Version 6	0.59 %	625	0.11 %	
▼ User Datagram Protocol	0.42 %	450	0.09 %	
DHCPv6	0.20 %	210	0.04 %	
Domain Name Service	0.19 %	204	0.04 %	
Hypertext Transfer Protocol	0.03 %	36	0.01 %	
Internet Control Message Protocol v6	0.16 %	175	0.02 %	
▼ Internet Protocol Version 4	97.07 %	103013	99.69 %	7
▼ User Datagram Protocol	3.69 %	3912	1.00 %	
Domain Name Service	2.42 %	2573	0.60 %	
Dropbox LAN sync Discovery Protocol	0.46 %	486	0.11 %	
Bootstrap Protocol	0.46 %	484	0.22 %	
Common Unix Printing System (CUPS) Browsing Protocol	0.04 %	39	0.01 %	
▼ NetBIOS Datagram Service	0.05 %	55	0.02 %	
▼ SMB (Server Message Block Protocol)	0.05 %	55	0.02 %	

Help Close

Basic UI

- Statistics -> Conversations
 - Generates descriptive statistics about each conversation for each protocol in the trace.



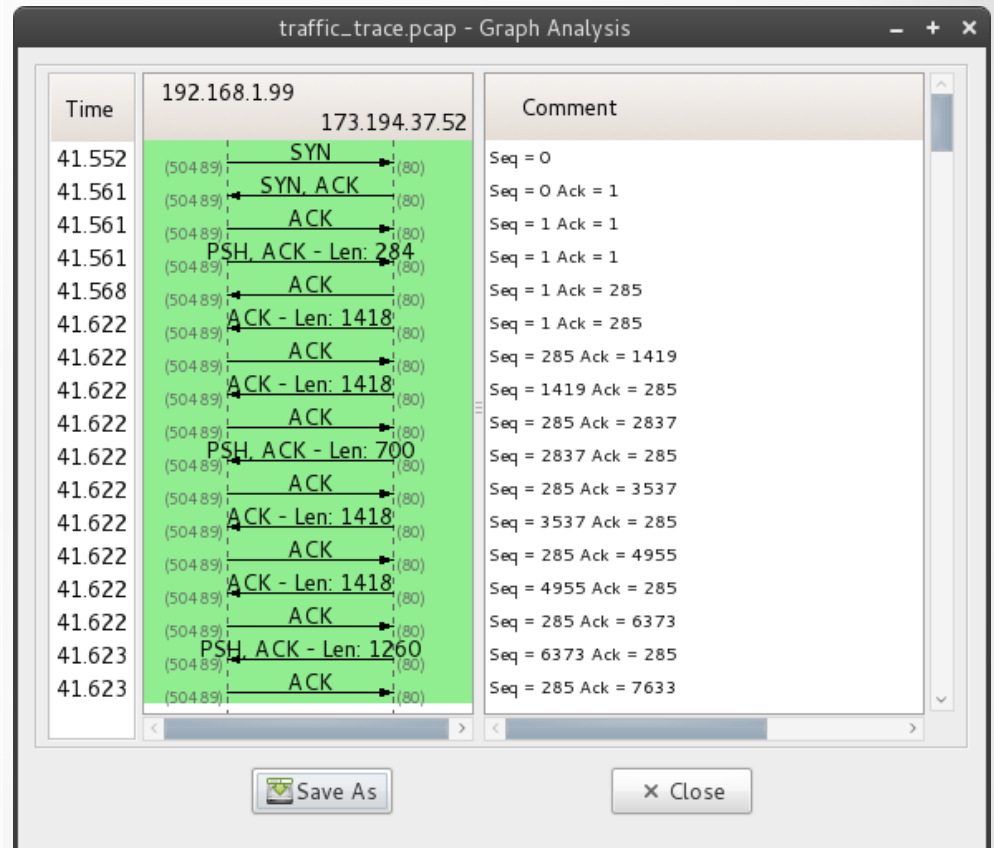
The screenshot shows a window titled "Conversations: traffic_trace.pcap" with a tab for "Ethernet: 214". Below the tab is a table of "Ethernet Conversations". The table has columns for Address A, Address B, Packets, Bytes, Packets A→B, Bytes A→B, and Packets A←B. The data is as follows:

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B
Brocade_C_ef:8b:00	Broadcast	753	59 280	753	59 280	0
Spanning-tree-(for-bridges)_00: Cisco_ed:4e:59		609	38 976	0	0	609
Dell_77:19:25	Broadcast	486	29 343	486	29 343	0
Dell_77:19:25	IPv6mcast_00:01:00:02	16	2 352	16	2 352	0
Dell_45:24:bb	Broadcast	2	120	2	120	0
CadmusCo_e5:ac:58	Cisco-Li_c1:d1:f9	101 328	77 500 345	42 867	5 114 212	58 461
Dell_9e:44:b0	Broadcast	165	26 054	165	26 054	0
QuantaCo_8f:42:cd	Broadcast	40	2 400	40	2 400	0
Dell_d5:c7:3b	Broadcast	67	4 625	67	4 625	0
IntelCor_3d:19:63	Broadcast	7	420	7	420	0

Below the table, there are checkboxes for "Name resolution" (checked) and "Limit to display filter" (unchecked). At the bottom, there are buttons for "Help", "Copy", "Follow Stream", and "Close".

Basic UI

- Statistics -> Flow Graph
 - Generates a sequence graph for the selected traffic.
 - Useful for understanding seq. and ack. calculations.



Packet Capture

- Interface selection

- Capture -> Interfaces

- Select the interface from which to capture packets.

- any – captures from all interfaces

- lo – captures from the loopback interface (i.e. from localhost)

- Set the desired capture parameters under the options menu.

- Start Capture

- Click the start button next to the desired interface.

- Captured traffic will be displayed in the packet list pane.

Packet Capture

- Stop Capture
 - Select Capture -> Stop
- Saving Capture
 - Once the capture has been stopped select File -> Save As.
 - From the save dialog you can specify file type and which packets to save via the packet range menu.

Trace Analysis

The screenshot displays the Wireshark interface for a file named 'test.cap'. The interface is divided into several sections:

- Menu:** Located at the top, it includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help) and a toolbar with various icons. A red arrow points to the menu bar.
- Filter:** A text box for entering filter expressions, with a dropdown menu and 'Clear' and 'Apply' buttons.
- Packet List:** A table showing a list of captured packets. A red arrow points to this section. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info.
- Packet Details:** A pane showing the hierarchical structure of the selected packet (Frame 11). A red arrow points to this section. It includes details for Ethernet II, Internet Protocol, and Transmission Control Protocol (TCP).
- Packet Bytes:** A pane showing the raw bytes of the selected packet in hexadecimal and ASCII. A red arrow points to this section.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	Broadcast	ARP	42	Gratuitous ARP for 192.168.0.2 (F
2	0.299139	192.168.0.1	192.168.0.2	NBNS	92	Name query NBSTAT *<00><00><00><0
3	0.299214	192.168.0.2	192.168.0.1	ICMP	70	Destination unreachable (Port un
4	1.025659	192.168.0.2	224.0.0.22	IGMP	54	v3 Membership Report / Join group
5	1.044366	192.168.0.2	192.168.0.1	DNS	110	Standard query SRV _ldap._tcp.nbc
6	1.048652	192.168.0.2	239.255.255.250	SSDP	175	M-SEARCH
7	1.050784	192.168.0.2	192.168.0.1	DNS	87	Standard query SOA nb10061d.ww004
8	1.055053	192.168.0.1	192.168.0.2	SSDP	32	HTTP/1.1 200 OK
9	1.082038	192.168.0.2	192.168.0.255	NBNS	110	Registration NB NB10061D<00>
10	1.111945	192.168.0.2	192.168.0.1	DNS	87	Standard query A proxyconf.ww004.
11	1.226156	192.168.0.2	192.168.0.1	TCP	62	ncu-2 > http [SYN] Seq=0 win=6424
12	1.227282	192.168.0.1	192.168.0.2	TCP	60	http > ncu-2 [SYN, ACK] Seq=0 Ack

Frame 11 details:

- Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
- Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
- Internet Protocol, src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
- Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0
 - Source port: ncu-2 (3196)
 - Destination port: http (80)
 - [Stream index: 5]
 - Sequence number: 0 (relative sequence number)
 - Header length: 28 bytes
 - Flags: 0x02 (SYN)
 - window size value: 64240

Packet Bytes:

```
0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00  ..[-u... ] .....F.
0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8  .0.H@... a...
0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02  ...|.P<6
0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02  .....
```

Trace Analysis

- Packet list

- Displays all of the packets in the trace in the order they were recorded.
- Columns
 - Time – the timestamp at which the packet crossed the interface.
 - Source – the originating host of the packet.
 - Destination – the host to which the packet was sent.
 - Protocol – the highest level protocol that Wireshark can detect.
 - Length – the length in bytes of the packet on the wire.
 - Info – an informational message pertaining to the protocol in the protocol column.

Trace Analysis

- Packet list
 - Default Coloring
 - Gray – TCP packets
 - Black with red letters – TCP Packets with errors
 - Green – HTTP Packets
 - Light Blue – UDP Packets
 - Pale Blue – ARP Packets
 - Lavender – ICMP Packets
 - Black with green letters – ICMP Packets with errors
 - Colorings can be changed under View -> Coloring Rules

Individual Packet Analysis

The screenshot displays the Wireshark network protocol analyzer interface. The main window is titled "test.cap". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu bar is a toolbar with various icons. A filter field is present with the text "Filter:" and a dropdown menu. The main display area is divided into four panes:

- Packet List:** A table showing a list of captured packets. The columns are No., Time, Source, Destination, Protocol, Length, and Info. Packet 3 is highlighted in black, and packet 11 is highlighted in blue. A red arrow points to this pane with the label "Packet List".
- Packet Details:** A pane showing the hierarchical structure of the selected packet (packet 11). It includes Ethernet II, Internet Protocol, and Transmission Control Protocol (TCP) details. The TCP section is expanded, showing source and destination ports, sequence number, and flags. A red arrow points to this pane with the label "Packet Details".
- Packet Bytes:** A pane showing the raw bytes of the selected packet in hexadecimal and ASCII. A red arrow points to this pane with the label "Packet Bytes".
- Status Bar:** Located at the bottom, it shows "File: 'C:/test.cap' 14 KB 00:00:02", "Packets: 120 Displayed: 120 Marked: 0 Load time: 0:00.000", and "Profile: Default".

Individual Packet Analysis

- Packet Details

- Detailed information about the currently selected packet is displayed in the packet details pane.
- All packet layers are displayed in the tree menu.
- Any portion of any layer can be exported via a right click and selecting Export Selected Packet Bytes

- Packet Bytes

- Displays the raw packet bytes.
- The selected packet layer is highlighted.

Filters

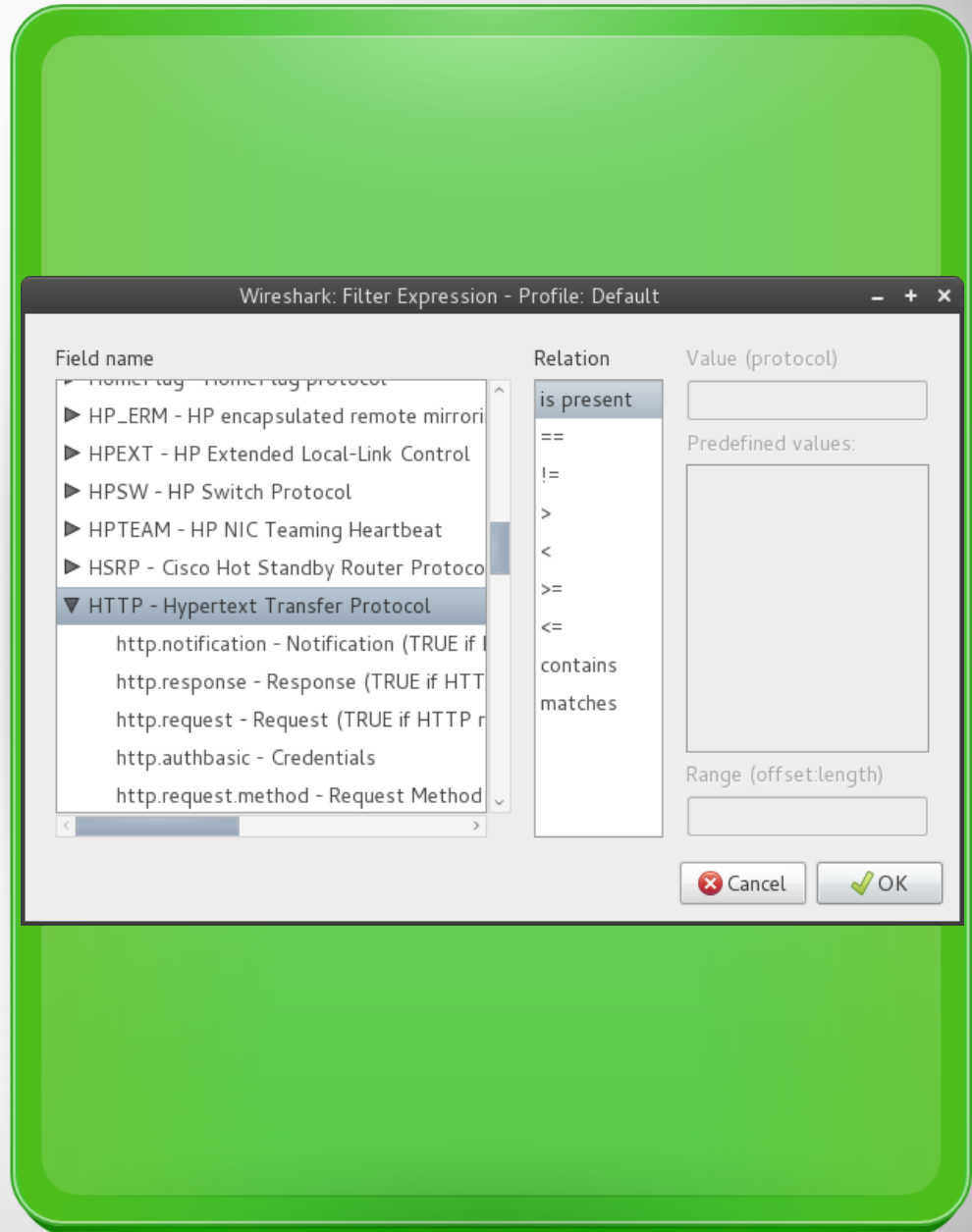
- Filters

- Packets captures usually contain many packets irrelevant to the specific analysis task.
- To remove these packets from display or from the capture Wireshark provides the ability to create filters.
- Filters are evaluated against each individual packet.
- Boolean expressions dealing with packet properties.
- Supports regular expressions.
- Can either be manually constructed, composed via the Expressions menu or composed based on a selected packet's properties.

Filters

- Expressions Menu

- Field name - selects the packet property.
- Relation - selects the boolean test.
- Predefined values - common values against which the selected packet property is tested.
- Value - Arbitrary Textual or Numeric value against which the selected packet property is tested.



Filters

- Compound Filters

- Filters can be composed of multiple tests joined with boolean connectives.
 - && - logical conjunction (i.e. AND)
 - || - logical disjunction (i.e OR)
 - ! - logical negation (i.e. NOT)
- Supports the order of operations.

- Regular Expressions

- Fields can be evaluated against a regular expression using the “matches” test.
- Uses [Perl regex syntax](#).

Filters

- Filter Text Box
 - Green – valid filter
 - Red – invalid filter
 - Yellow – may produce unexpected results
- Packet based filters
 - Filters can be constructed on the basis of individual packets by right clicking on a packet and selecting either:
 - Prepare as filter – creates a filter.
 - Apply as filter – creates a filter and applies it to the trace.
 - Follow TCP Stream – creates a filter from a TCP packet's stream number and applies it to the trace.

Filters

- Filter examples

- `http.request` – Display all HTTP requests.
- `http.request || http.response` – Display all HTTP request and responses.
- `ip.addr == 127.0.0.1` – Display all IP packets whose source or destination is localhost.
- `tcp.len < 100` – Display all TCP packets whose data length is less than 100 bytes.
- `http.request.uri matches "(gif)$"` – Display all HTTP requests in which the uri ends with "gif".
- `dns.query.name == "www.google.com"` – Display all DNS queries for "www.google.com".

Questions

Any Questions?

Thank you for your attention!

Exercises

- Work in groups of 2.
- Download the trace at http://cs.uga.edu/~neasbitt/files/user1_tcpdump.pcap
- Answer the following questions on a sheet of paper.
 - What is the total number of HTTP Post requests in the trace?
 - What is the status code for the last HTTP response in TCP stream 17?
 - What is the total size in bytes for all packets containing JavaScript Object Notation (JSON) data?
 - Between which two IP address where the most IP packets sent?
 - What is pictured in the image bostonmusic-promo.jpg?

Exercises

- Work in groups of 2.
- Download the trace at http://cs.uga.edu/~neasbitt/files/user1_tcpdump.pcap
- Answer the following questions on a sheet of paper.
 - What is the total number of HTTP Post requests in the trace?
 - What is the status code for the last HTTP response in TCP stream 17?
 - What is the total size in bytes for all packets containing JavaScript Object Notation (JSON) data?
 - Between which two IP addresses were the most IP packets sent?
 - What is pictured in the image `bostonmusic-promo.jpg`?

Question Answers

1. 8
2. 302
3. 2253
4. 10.0.2.15 – 123.125.114.18
5. A stereo system.