

This pdf shows basic Wireshark install, operation, and file saving for OpenSUSE. You must have permission to run this program from the network owner. Remember nonrepudiation!

YaST Control Center @ linux-msctc

Search

- Software
- Hardware
- System
- Network Devices
- Network Services
- Novell AppArmor
- Security and Users
- Virtualization
- Support
- Miscellaneous

Ready

Software

- Add-On Products
Install or remove add-on products
- FACTORY Update
- Media Check
- Online Update
- Online Update Configuration
- Package Search (webpin)
- Software Management

YaST Control Center @ linux-msctc

Software

Add-On Products

Search

- Software
- Hardware
- System
- Network Devices
- Network Services
- Novell AppArmor
- Security and Use
- Virtualization
- Support
- Miscellaneous

YaST2

Starting the Software Manager

- ✓ Initialize the Target System
- ✓ Load the Configured Repositories

100%

Help Abort Back Next

YaST2

File Package Configuration Dependencies Options Extras Help

View Search RPM Groups Installation Summary Package Groups

wireshark Search

Search in

- Name
- Keywords
- Summary
- Description
- RPM "Provides"
- RPM "Requires"
- File list

Search Mode:

Contains

Case Sensitive

Package	Summary	Installed (Availab	Size

Description Technical Data Dependencies Versions File

Cancel Accept

YaST2

File Package Configuration Dependencies Options Extras Help

View Search RPM Groups Installation Summary Package Groups

wireshark Search

Search in

- Name
- Keywords
- Summary
- Description
- RPM "Provides"
- RPM "Requires"
- File list

Search Mode: Contains

Case Sensitive

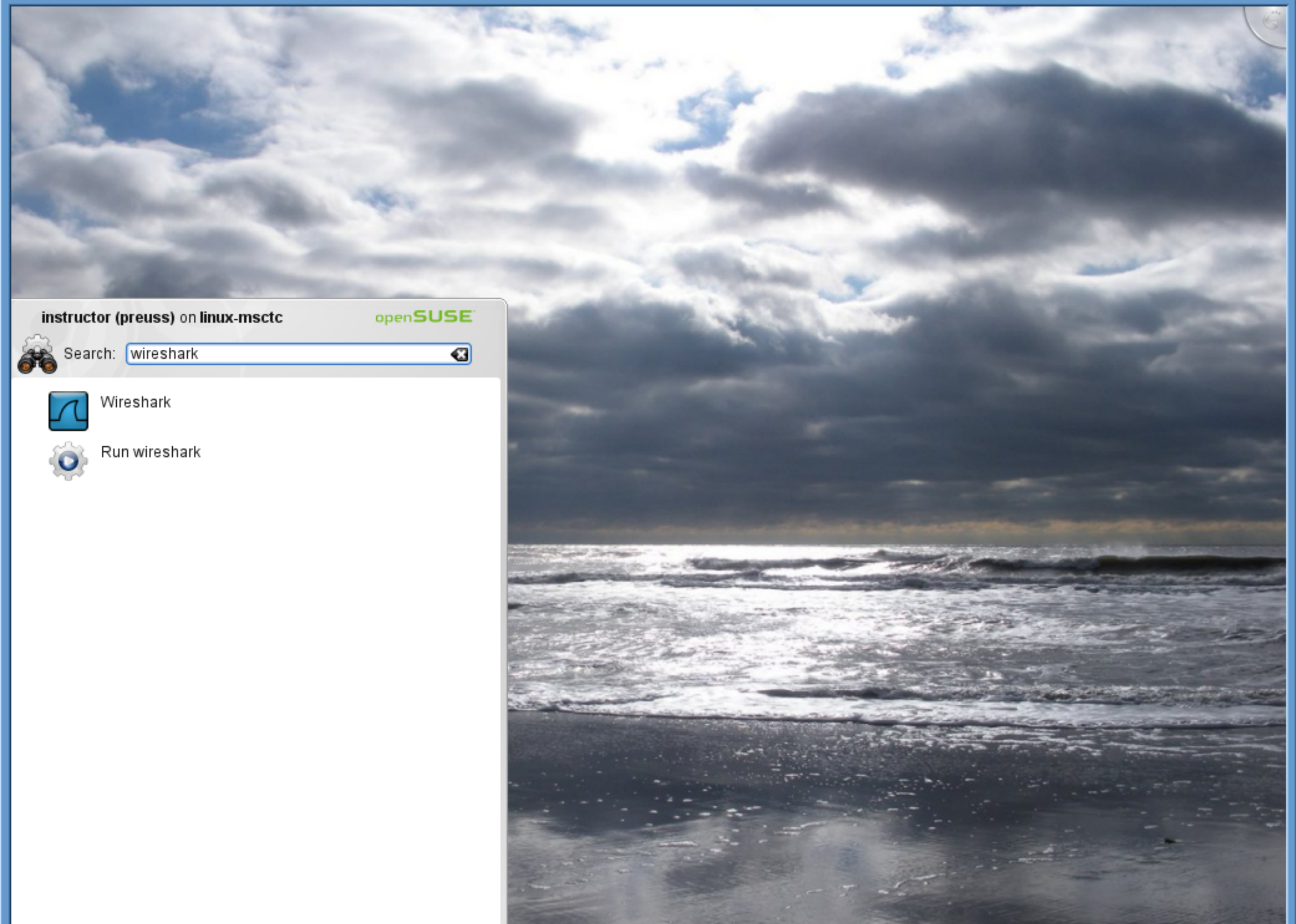
Package	Summary	Installed	Av. Size
<input checked="" type="checkbox"/> wireshark	A Network Traffic An...	1.4.2-1.1.2	52.6 MiB
<input type="checkbox"/> wireshark-devel	A Network Traffic An...	(1.4.2-1.1...	598.0 ...

Description Technical Data Dependencies Versions File < >

wireshark - A Network Traffic Analyser

Wireshark is a free network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Wireshark has several powerful features, including a rich display filter language and the ability to view the

Cancel Accept



instructor (preuss) on linux-msctc

openSUSE



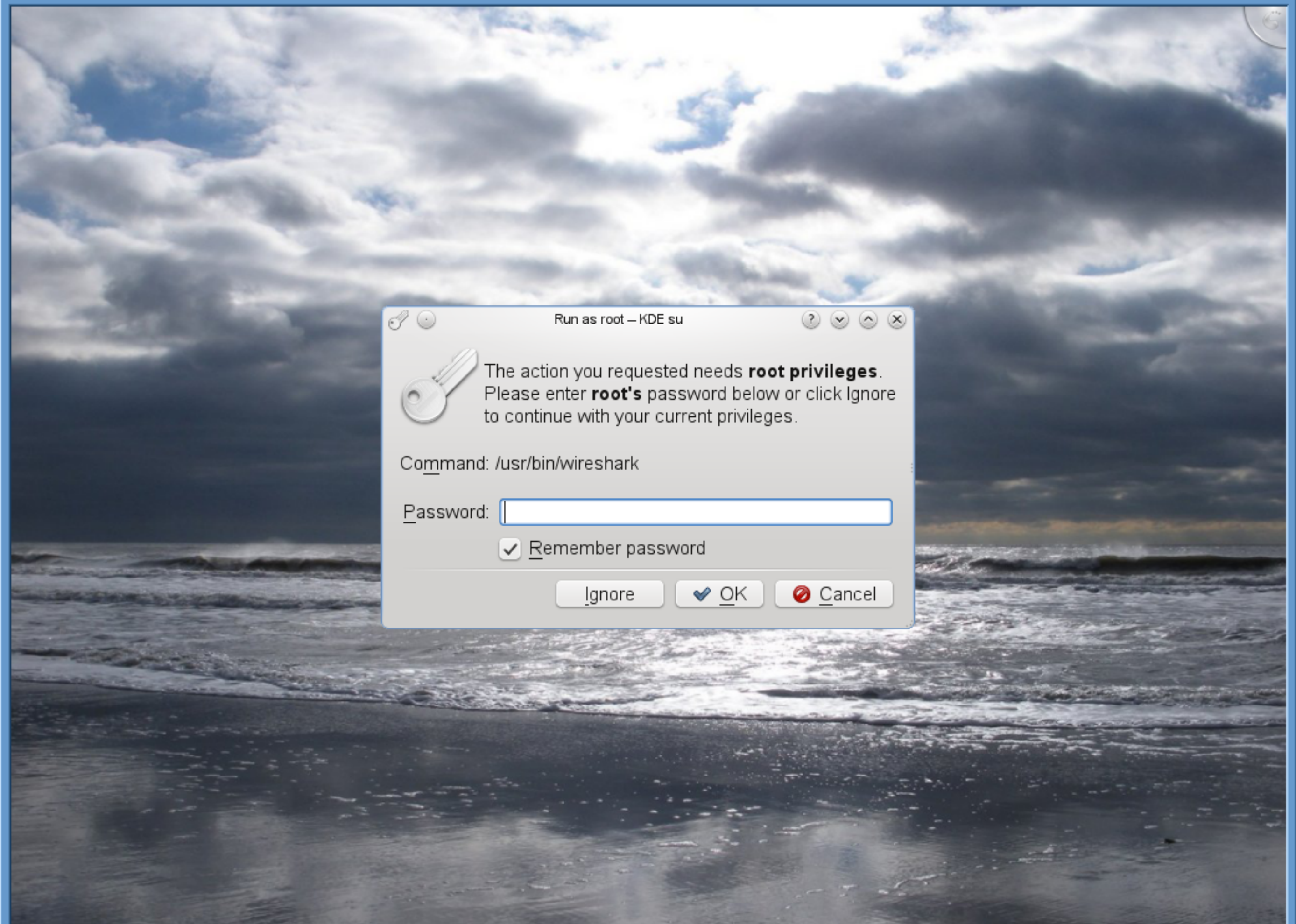
Search:




Wireshark



Run wireshark



Run as root – KDE su

 The action you requested needs **root privileges**. Please enter **root's** password below or click Ignore to continue with your current privileges.

Command: /usr/bin/wireshark

Password:

Remember password

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply



The World's Most Popular Network Protocol Analyzer

Capture

Interface List
Live list of the capture interfaces (counts incoming packets)

Start capture on interface:

- eth0
- Pseudo-device that captures on all interfaces
- lo

Capture Options
Start a capture with detailed options

Capture Help

How to Capture
Step by step to a successful capture setup

Network Media
Specific information for capturing on: Ethernet, WLAN, ...

Files

Open
Open a previously captured file

Open Recent:

- /home/preuss/Documents/dragon02_02252011_hub (2382 KB)
- /home/preuss/Documents/dragon01_02252011 (230 KB)

Sample Captures
A rich assortment of...

Your ethernet card may have another name.

Webs
Visit the p...

User'
The User'

Secu
Work with

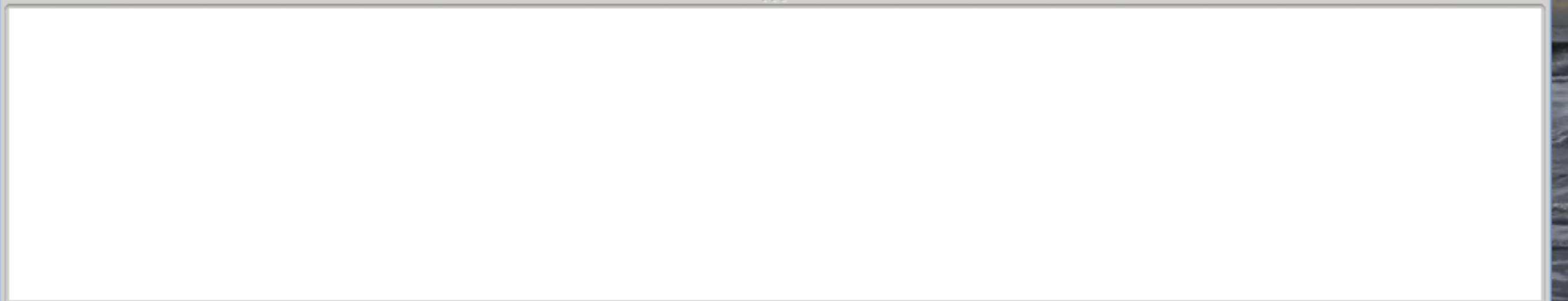
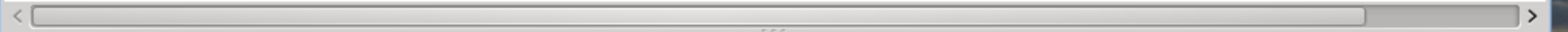
Ready to load or capture No Packets Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Tools Help



Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info



eth0: <live capture in progress> to... No Packets Profile: Default

Capturing from eth0 - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Open... Ctrl+O
 Open Recent >
 Merge...
 Close Ctrl+W
 Save Ctrl+S
 Save As... Shift+Ctrl+S
 File Set >
 Export >
 Print... Ctrl+P
 Quit Ctrl+Q

No.	Time	Destination	Protocol	Info
3	0.00000	192.168.5.255	RIPv2	Response
7	0.00000	192.168.5.1	DNS	Standard query A www.opensuse.org
7	0.00000	192.168.5.1	DNS	Standard query AAAA www.opensuse.org
1	0.00000	192.168.5.7	DNS	Standard query response A 130.57.4.24
1	0.00000	192.168.5.7	DNS	Standard query response
7	0.00000	130.57.4.24	TCP	46684 > http [SYN] Seq=0 Win=5840 Len=0
4	0.00000	192.168.5.7	TCP	http > 46684 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
7	0.00000	130.57.4.24	TCP	46684 > http [ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.00000	130.57.4.24	HTTP	GET / HTTP/1.1
10	0.490522	130.57.4.24	TCP	http > 46684 [ACK] Seq=1 Ack=534 Win=0 Len=0

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 Ethernet II, Src: Cisco-Li_71:97:f4 (00:14:bf:71:97:f4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Internet Protocol, Src: 192.168.5.3 (192.168.5.3), Dst: 192.168.5.255 (192.168.5.255)
 User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
 Routing Information Protocol

```

0000  ff ff ff ff ff ff 00 14 bf 71 97 f4 08 00 45 00  .....q....E.
0010  00 34 e1 50 00 00 40 11 0d 16 c0 a8 05 03 c0 a8  .4.P..@. ....
0020  05 ff 02 08 02 08 00 20 a3 9c 02 02 00 00 00 02  .....
0030  00 00 00 00 00 00 ff ff ff 00 00 00 00 00 00 00  .....
  
```

eth0: <live capture in progress> Fi... Packets: 588 Displayed: 588 Marked: 0 Profile: Default

Capturing from eth0 - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.5.7	130.57.4	RIPv2	Response
2	0.227001	192.168.5.7	130.57.4	DNS	Standard query A www.opensuse.org
3	0.231336	192.168.5.7	130.57.4	DNS	Standard query AAAA www.opensuse.org
4	0.312662	192.168.5.7	130.57.4	DNS	Standard query response A 130.57.4
5	0.312673	192.168.5.7	130.57.4	DNS	Standard query response
6	0.313639	192.168.5.7	130.57.4	TCP	46684 > http [SYN] Seq=0 Win=5840
7	0.400435	130.57.4	192.168.5.7	TCP	http > 46684 [SYN, ACK] Seq=0 Ack=
8	0.400490	192.168.5.7	130.57.4	TCP	46684 > http [ACK] Seq=1 Ack=1 Win=
9	0.400674	192.168.5.7	130.57.4	HTTP	GET / HTTP/1.1
10	0.490522	130.57.4	192.168.5.7	TCP	http > 46684 [ACK] Seq=1 Ack=534 W

Clear Apply

Display Filters...
 Display Filter Macros...
 Apply as Column
 Apply as Filter >
 Prepare a Filter >
 Enabled Protocols... Shift+Ctrl+E
 Decode As...
 User Specified Decodes...
 Follow TCP Stream
 Follow UDP Stream
 Follow SSL Stream
 Expert Info
 Expert Info Composite
 Conversation Filter >

Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0

Ethernet II, Src: Vmware_21:f8:df (00:0c:29:21:f8:df), Dst: 130.57.4:1 (08:00:45:00:3c:1f)

Internet Protocol, Src: 192.168.5.7 (192.168.5.7), Dst: 130.57.4 (130.57.4)

Transmission Control Protocol, Src Port: 46684 (46684), Dst Port: 80 (80)

0000 00 14 6c 40 fa b0 00 0c 29 21 f8 df 08 00 45 00 ..1
 0010 00 3c 1f bd 40 00 40 06 ce fe c0 a8 05 07 82 39 <
 0020 04 18 b6 5c 00 50 f1 4f 5d 3a 00 00 00 00 a0 02 ...\.P.O].....
 0030 1c 40 0e fb 00 00 02 04 05 b4 04 02 08 0e 01 17 [

Frame (frame), 74 bytes Packets: 592 Displayed: 592 Marked: 0 Profile: Default

The example selects a tcp packet and chooses the Follow TCP Stream

Follow TCP Stream

Stream Content

```

GET / HTTP/1.1
Host: brazil.minnesota.edu
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.15) Gecko/20110303 SUSE/3.6.15-0.2.1
Firefox/3.6.15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive

HTTP/1.1 200 OK
Content-Type: text/html
Content-Encoding: gzip
Last-Modified: Tue, 22 Mar 2011 18:20:29 GMT
Accept-Ranges: bytes
ETag: "e19cbbd2bde8cb1:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Wed, 23 Mar 2011 21:22:15 GMT

```

ASCII
 EBCDIC
 Hex Dump
 C Arrays
 Raw

0000	00	14	6c	40	fa	b0	00	0c	29	21	f8	df	08	00	45	00	..l@....)!....E.
0010	00	3c	2a	19	40	00	40	06	e0	70	c0	a8	05	07	86	1d	.<*.@.@. .p.....
0020	e4	65	ab	08	00	50	f9	f2	4d	43	00	00	00	00	a0	02	.e...P.. MC.....
0030	1c	d0	e5	fa	00	00	00	04	05	b4	04	00	08	00	01	17	

eth0: <live capture in progress> Fi... Packets: 618 Displayed: 435 Marked: 0 Profile: Default



Filter: tcp.stream eq 20 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
111	9.740221	192.168.5.7	134.29.228.101	TCP	43784 > http [SYN] Seq=0 Win=5840
112	9.817413	134.29.228.101	192.168.5.7	TCP	http > 43784 [SYN, ACK] Seq=0 Ack=1
113	9.817438	192.168.5.7	134.29.228.101	TCP	43784 > http [ACK] Seq=1 Ack=1 Win=
114	9.817563	192.168.5.7	134.29.228.101	HTTP	GET / HTTP/1.1
115	9.901146	134.29.228.101	192.168.5.7	TCP	[TCP segment of a reassembled PDU]
116	9.901164	192.168.5.7	134.29.228.101	TCP	43784 > http [ACK] Seq=387 Ack=1369
117	9.901305	134.29.228.101	192.168.5.7	TCP	[TCP segment of a reassembled PDU]
118	9.901310	192.168.5.7	134.29.228.101	TCP	43784 > http [ACK] Seq=387 Ack=2737
119	9.979780	134.29.228.101	192.168.5.7	TCP	[TCP segment of a reassembled PDU]
120	9.979795	192.168.5.7	134.29.228.101	TCP	43784 > http [ACK] Seq=387 Ack=4109

▶ Frame 115: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits)
 ▶ Ethernet II, Src: Netgear_40:fa:b0 (00:14:6c:40:fa:b0), Dst: Vmware_21:f8:df (00:0c:29:21:f8:df)
 ▶ Internet Protocol, Src: 134.29.228.101 (134.29.228.101), Dst: 192.168.5.7 (192.168.5.7)
 ▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 43784 (43784), Seq: 1, Ack: 387, Len:

Use Ctrl M to select the packets requested by the lab.

```

0000  00 0c 29 21 f8 df 00 14 6c 40 fa b0 08 00 45 00  ...
0010  05 8c 2b 0c 40 00 6e 06 ac 2d 86 1d e4 65 c0 a8  ...
0020  05 07 00 50 ab 08 bc 17 96 b6 f9 f2 4e c6 80 10  ...
0030  01 00 08 00 00 00 01 01 08 00 07 78 00 f8 01 17  ...
  
```

eth0: <live capture in progress> Fi... Packets: 659 Displayed: 435 Marked: 5



Filter: tcp.stream eq 20 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
126	9.980478	192.168.5.7	134.29.228.101	TCP	43784 > http [ACK] Seq=507 Ack=757
127	9.984935	192.168.5.7	134.29.228.101	HTTP	GET /default_html_m2b0c4566.jpg HT
128	10.088268	134.29.228.101	192.168.5.7	TCP	[TCP segment of a reassembled PDU]
129	10.088345	134.29.228.101	192.168.5.7	TCP	[TCP segment of a reassembled PDU]
130	10.088353	192.168.5.7	134.29.228.101	TCP	43784 > http [ACK] Seq=808 Ack=101
131	10.088846	134.29.228.101	192.168.5.7	TCP	[TCP segment of a reassembled PDU]
132	10.090141	134.29.228.101	192.168.5.7	TCP	[TCP segment of a reassembled PDU]
133	10.090145	192.168.5.7	134.29.228.101	TCP	43784 > http [ACK] Seq=808 Ack=1284
134	10.092195	134.29.228.101	192.168.5.7	TCP	[TCP segment of a reassembled PDU]
135	10.094187	134.29.228.101	192.168.5.7	TCP	[TCP segment of a reassembled PDU]
136	10.094194	192.168.5.7	134.29.228.101	TCP	[TCP segment of a reassembled PDU]

▶ Frame 133: 66 bytes on wire (528 bits), 66 bytes captured
 ▶ Ethernet II, Src: vmnic3 (08:00:27:00:00:00), Dst: 134.29.228.101 (08:00:27:00:00:00)
 ▶ Internet Protocol Version 4, Src: 192.168.5.7, Dst: 134.29.228.101
 ▶ Transmission Control Protocol, Src Port: 43784 (43784), Dst Port: 80

Export your selected packets as a pdml file for submission.

Wireshark: Export as "PDML" file

Export to file:

Packet Range

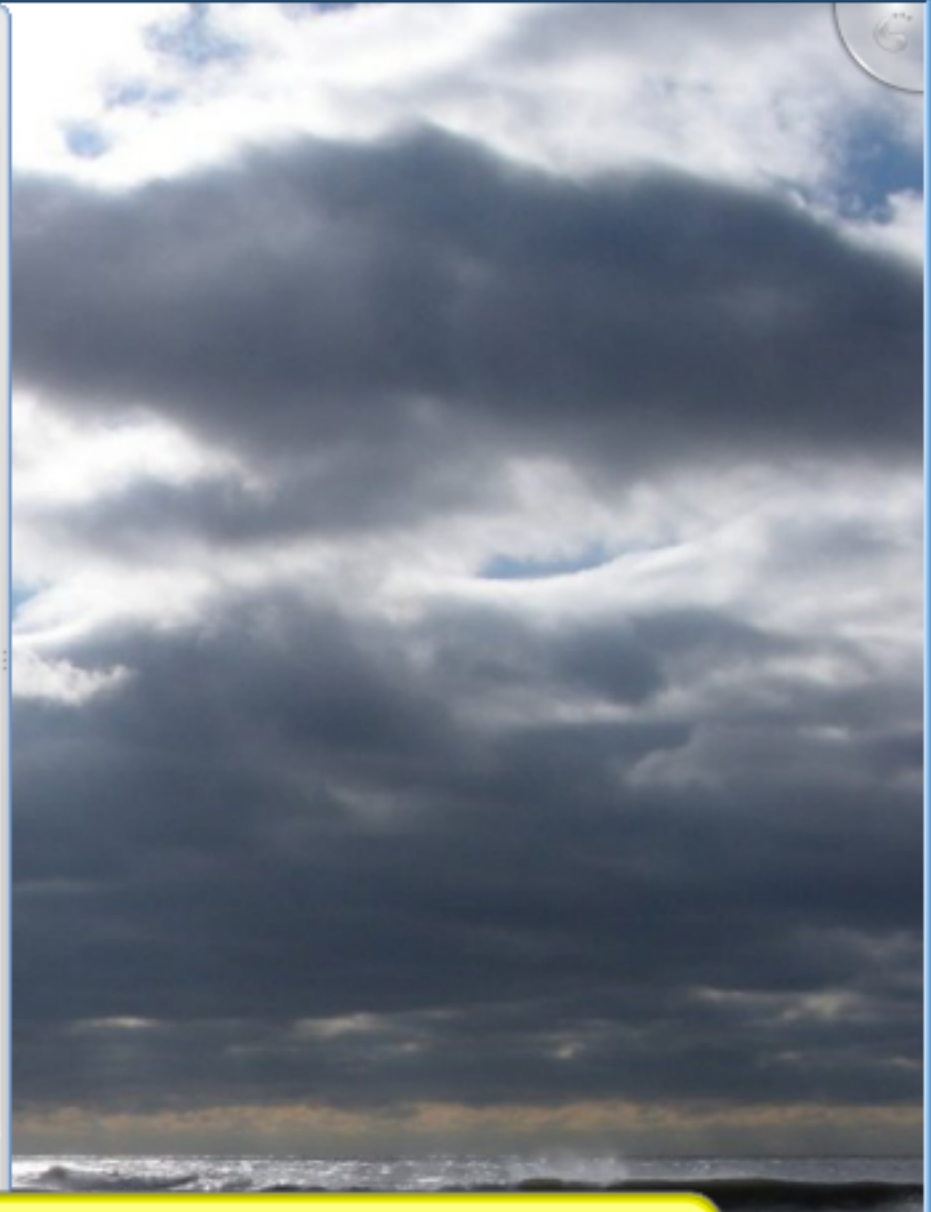
	Captured	Displayed
<input type="radio"/> All packets	673	435
<input type="radio"/> Selected packet only	1	1
<input checked="" type="radio"/> Marked packets only	22	22
<input type="radio"/> From first to last marked packet	22	22
<input type="radio"/> Specify a packet range:	0	0
<input type="text" value=""/>		
<input type="checkbox"/> Remove ignored packets	0	0

eth0: <live capture in progress> Fi... Packets: 675 Displayed: 435 Marked: 22

```

Documents : bash
File Edit View Scrollback Bookmarks Settings Help
preuss@linux-msctc:~/Documents> ls
dragon01_02252011      hosts          New Spreadsheet.ots  stream2  tmp
dragon02_02252011_hub New Document.ott new.txt              test.gz
preuss@linux-msctc:~/Documents> █

```



Documents : bash

You may view the contents of stream2.