OpenSUSE 13.1 Reporting Wireshark Packet Captures

The presentation shows how to set the time parameter in Wireshark for class purposes. The presentation shows how to properly capture a packet in text format for lab assignments.

Preuss
4/22/2104

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

Desktop

Firefox

KInfoCenter

Office

Online Help

openSUSE

Start OpenSUSE or whatever host is running Wireshark.

09:01 PM

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

Desktop

The Wireshark Network Analyzer [Wireshark 1.10.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

WIRESHARK

The World's Most Popular Network Protocol Analyzer
Version 1.10.6 (Git Rev Unknown from unknown)

Capture

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

Start
Choose one or more interfaces to capture from, then **Start**

- eth0
- nflog
- any
- Loopback: 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/wireshark_documentation_net_03212014.pcapng (1,572 kB)

Sample Captures
A rich assortment of example capture files on the wiki

Online

Website
Visit the project's website

User's Guide
The User's Guide (online versi

Security
Work with Wireshark as secure

Make sure you have permission to capture packets on this network. Select the interface and capture packets.

Ready to load or capture | No Packets | Profile: Default

The Wireshark Network Analyzer

09:01 PM

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

Desktop

*eth0 [Wireshark 1.10.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protoco	Length	Info
26	10.382974000	Nortel_c9:10:01	Nortel-autodiscovery	NDP	60	FlatNet Hello
27	10.652566000	Nortel_c9:10:01	Spanning-tree-(for-br:	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Po
28	11.605429000	192.168.65.218	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
29	12.652618000	Nortel_c9:10:01	Spanning-tree-(for-br:	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Po
30	12.755616000	Vmware_c9:4e:51	Broadcast	ARP	60	Who has 192.168.64.2? Tell 192.168.66.10
31	13.757972000	Vmware_c9:4e:51	Broadcast	ARP	60	Who has 192.168.64.2? Tell 192.168.66.10
32	14.606040000	192.168.65.218	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
33	14.652508000	Nortel_c9:10:01	Spanning-tree-(for-br:	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Po
34	14.760598000	Vmware_c9:4e:51	Broadcast	ARP	60	Who has 192.168.64.2? Tell 192.168.66.10
35	16.652463000	Nortel_c9:10:01	Spanning-tree-(for-br:	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Po

> Frame 1: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface 0
> Ethernet II, Src: Hewlett-_16:48:79 (10:1f:74:16:48:79), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.65.44 (192.168.65.44), Dst: 239.255.255.250 (239.255.255.250)
> User Datagram Protocol, Src Port: 58380 (58380), Dst Port: ssdp (1900)
> Hypertext Transfer Protocol

The time configuration is not correct. The capture is stopped.

```
0000  01 00 5e 7f ff fa 10 1f  74 16 48 79 08 00 45 00   ..^..... t.Hy..E.
0010  00 a1 11 38 00 00 01 11  b6 45 c0 a8 41 2c ef ff   ...8.... .E..A,..
0020  ff fa e4 0c 07 6c 00 8d  7b a2 4d 2d 53 45 41 52   .....l.. {.M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1..H
0040  6f 73 74 3a 32 33 39 2e  32 35 35 2e 32 35 35 2e   ost:239. 255.255.
```

File: "/tmp/wireshark_pcapng_eth0_2... Packets: 35 · Displayed: 35 (100.0%) ... Profile: Default

*eth0 [Wireshark 1.10.6 (Git

09:02 PM

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

Desktop

*eth0 [Wireshark 1.10.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Destination	Protoco	Length	Info
27	Spanning-tree-(for-br:	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10
28	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
29	Spanning-tree-(for-br:	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10
30	Broadcast	ARP	60	Who has 192.168.64.2? Tell 192.168
31	Broadcast	ARP	60	Who has 192.168.64.2? Tell 192.168

Frame 1
Etherne
Interne
User Da
Hyperte

0000 01 00 5e 7f ff fa 10 1f 74 16 48 79 08 00 45 00 ..^..... t.Hy..E.
0010 00 a1 11 38 00 00 01 11 b6 45 c0 a8 41 2c ef ff ...8.... .E..A,..
0020 ff fa e4 0c 07 6c 00 8d 7b a2 4d 2d 53 45 41 52 .....l.. {.M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 6f 73 74 3a 32 33 39 2e 32 35 35 2e 32 35 35 2e ost:239. 255.255.

File: "/tmp/wireshark_pcapng_eth0_2... Packets: 35 · Displayed: 35 (100.0%) ... Profile: Default

*eth0 [Wireshark 1.10.6 (Git

09:03 PM

View menu:

- Main Toolbar
- Filter Toolbar
- Wireless Toolbar
- Status Bar
- Packet List
- Packet Details
- Packet Bytes
- Time Display Format
- Name Resolution
- Colorize Packet List
- Auto Scroll in Live Capture
- Zoom In Ctrl++
- Zoom Out Ctrl+-
- Normal Size Ctrl+=
- Resize All Columns Shift+Ctrl+R
- Displayed Columns
- Expand Subtrees Shift+Right
- Expand All Ctrl+Right
- Collapse All Ctrl+Left
- Colorize Conversation
- Reset Coloring 1-10 Ctrl+Space
- Coloring Rules...
- Show Packet in New Window
- Reload Ctrl+R

Time Display Format:

- Date and Time of Day: 1970-01-01 01:02:03.123456 Ctrl+Alt+1
- Time of Day: 01:02:03.123456 Ctrl+Alt+2
- Seconds Since Epoch (1970-01-01): 1234567890.123456 Ctrl+Alt+3
- Seconds Since Beginning of Capture: 123.123456 Ctrl+Alt+4
- Seconds Since Previous Captured Packet: 1.123456 Ctrl+Alt+5
- Seconds Since Previous Displayed Packet: 1.123456 Ctrl+Alt+6
- UTC Date and Time of Day: 1970-01-01 01:02:03.123456 Ctrl+Alt+7
- UTC Time of Day: 01:02:03.123456 Ctrl+Alt+7
- Automatic (File Format Precision)
- Seconds: 0
- Deciseconds: 0.1
- Centiseconds: 0.12
- Milliseconds: 0.123
- Microseconds: 0.123456
- Nanoseconds: 0.123456789
- Display Seconds with hours and minutes

The lab assignments require the time settings shown. You will need to make sure the date/time is correct for the system.

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

Desktop

*eth0 [Wireshark 1.10.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protoco	Length	Info
142	2014-04-22 21:04:08.330457000	fe80::211:43ff:fee7:f	ff02::1:ff37:67c3	ICMPv6	86	Neighbor Solicitation for 2001:470:
143	2014-04-22 21:04:09.329570000	fe80::211:43ff:fee7:f	ff02::1:ff37:67c3	ICMPv6	86	Neighbor Solicitation for 2001:470:
144	2014-04-22 21:04:10.300873000	Nortel_c9:10:01	Spanning-tree-(for-br:	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10
145	2014-04-22 21:04:10.329557000	fe80::211:43ff:fee7:f	ff02::1:ff37:67c3	ICMPv6	86	Neighbor Solicitation for 2001:470:
146	2014-04-22 21:04:11.325548000	192.168.65.122	192.168.67.255	NBNS	92	Name query NB WPAD<00>
147	2014-04-22 21:04:12.074158000	192.168.65.122	192.168.67.255	NBNS	92	Name query NB WPAD<00>
148	2014-04-22 21:04:12.300825000	Nortel_c9:10:01	Spanning-tree-(for-br:	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10
149	2014-04-22 21:04:12.823991000	192.168.65.122	192.168.67.255	NBNS	92	Name query NB WPAD<00>
150	2014-04-22 21:04:14.300815000	Nortel_c9:10:01	Spanning-tree-(for-br:	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10

> Frame 145: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Ethernet II, Src: Dell_e7:f1:95 (00:11:43:e7:f1:95), Dst: IPv6mcast_ff:37:67:c3 (33:33:ff:37:67:c3)
> Internet Protocol Version 6, Src: fe80::211:43ff:fee7:f195 (fe80::211:43ff:fee7:f195), Dst: ff02::1:ff37:67c3 (ff02::1:ff37:67c3)
> Internet Control Message Protocol v6

The presentation selects a packet to report. After highlighting the packet, the presentation uses the Ctrl + M combination to select the packet. Several packets may be selected using Ctrl + M combination.

```
0000  33 33 ff 37 67 c3 00 11  43 e7 f1 95 86 dd 60 00   33.7g... C.....`.
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 02 11   ... :... ........
0020  43 ff fe e7 f1 95 ff 02  00 00 00 00 00 00 00 00   C....... ........
0030  00 01 ff 37 67 c3 87 00  9f e5 00 00 00 00 20 01   ...7g... ...... .
0040  04 70 1f 11 04 55 02 50  56 ff fe 37 67 c3 01 01   .p...U.P V..7g...
```

File: "/tmp/wireshark_pcapng_eth0_2... Packets: 150 · Displayed: 150 (100.0... Profile: Default

*eth0 [Wireshark 1.10.6 (Git

09:04 PM

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

Desktop

*eth0 [Wireshark 1.10.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Open... Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Shift+Ctrl+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Selected Packet Bytes... Ctrl+H
Export SSL Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q

Expression... Clear Apply Save

ce	Destination	Protoco	Length	Info
el_c9:10:01	Spanning-tree-(for-br:	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10
::211:43ff:fee7:f	ff02::1:ff37:67c3	ICMPv6	86	Neighbor Solicitation for 2001:470:
::211:43ff:fee7:f	ff02::1:ff37:67c3	ICMPv6	86	Neighbor Solicitation for 2001:470:
el_c9:10:01	Spanning-tree-(for-br:	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10
::211:43ff:fee7:f	ff02::1:ff37:67c3	ICMPv6	86	Neighbor Solicitation for 2001:470:
168.65.122	192.168.67.255	NBNS	92	Name query NB WPAD<00>
168.65.122	192.168.67.255	NBNS	92	Name query NB WPAD<00>
el_c9:10:01	Spanning-tree-(for-br:	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10
168.65.122	192.168.67.255	NBNS	92	Name query NB WPAD<00>
el_c9:10:01	Spanning-tree-(for-br:	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10

6 bytes captured (688 bits) on interface 0
:e7:f1:95), Dst: IPv6mcast_ff:37:67:c3 (33:33:ff:37:67:c3)
11:43ff:fee7:f195 (fe80::211:43ff:fee7:f195), Dst: ff02::1:ff37:67c3 (ff02::1:ff37:67c3)

The presentation opens the File Menu to "print" or save the packet. The presentation selects the Print option.

```
0000  33 33 ff 37 67 c3 00 11  43 e7 f1 95 86 dd 60 00   33.7g... C.....`.
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 02 11   ... :... ........
0020  43 ff fe e7 f1 95 ff 02  00 00 00 00 00 00 00 00   C....... ........
0030  00 01 ff 37 67 c3 87 00  9f e5 00 00 00 00 20 01   ...7g... ...... .
0040  04 70 1f 11 04 55 02 50  56 ff fe 37 67 c3 01 01   .p...U.P V..7g...
```

File: "/tmp/wireshark_pcapng_eth0_2... Packets: 150 · Displayed: 150 (100.0... Profile: Default

*eth0 [Wireshark 1.10.6 (Git

09:04 PM

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

*eth0 [Wireshark 1.10.6

File Edit View Go Capture Analyze Statistics Telephony Tools Inter

Filter: Expressior

No.	Time	Source	Dest
142	2014-04-22 21:04:08.330457000	fe80::211:43ff:fee7:f	ff02
143	2014-04-22 21:04:09.329570000	fe80::211:43ff:fee7:f	ff02
144	2014-04-22 21:04:10.300873000	Nortel_c9:10:01	Span
145	2014-04-22 21:04:10.329557000	fe80::211:43ff:fee7:f	ff02
146	2014-04-22 21:04:11.325548000	192.168.65.122	192.
147	2014-04-22 21:04:12.074158000	192.168.65.122	192.
148	2014-04-22 21:04:12.300825000	Nortel_c9:10:01	Span
149	2014-04-22 21:04:12.823991000	192.168.65.122	192.
150	2014-04-22 21:04:14.300815000	Nortel_c9:10:01	Span

```
> Frame 145: 86 bytes on wire (688 bits), 86 bytes captured (688
> Ethernet II, Src: Dell_e7:f1:95 (00:11:43:e7:f1:95), Dst: IPv6
> Internet Protocol Version 6, Src: fe80::211:43ff:fee7:f195 (fe
> Internet Control Message Protocol v6
```

The presentation configures the Printer file as shown. This configuration will report the entire packet.

The presentation selects the Browse button on the output to file: line.

Wireshark: Print

Printer

- (•) Plain text
- ( ) PostScript
- [x] Output to file: wireshark.out — Browse...
- Print command: lpr

Packet Range

	Captured	Displayed
( ) All packets	150	150
(•) Selected packet only	1	1
( ) Marked packets only	0	0
( ) From first to last marked packet	0	0
( ) Specify a packet range:	0	0
[ ] Remove Ignored packets	0	0

Packet Format

- [x] Packet summary line
- [x] Packet details:
  - ( ) All collapsed
  - ( ) As displayed
  - (•) All expanded
- [x] Packet bytes
- [x] Each packet on a new page

Help Cancel Print

```
0000  33 33 ff 37 67 c3 00 11  43 e7 f1 95 86 dd 60 00   33.7g... C.....`.
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 02 11   ... :... ........
0020  43 ff fe e7 f1 95 ff 02  00 00 00 00 00 00 00 00   C....... ........
0030  00 01 ff 37 67 c3 87 00  9f e5 00 00 00 00 20 01   ...7g... ...... .
0040  04 70 1f 11 04 55 02 50  56 ff fe 37 67 c3 01 01   .p...U.P V..7g...
```

File: "/tmp/wireshark_pcapng_eth0_2... Packets: 150 · Displayed: 150 (100.0... Profile: Default

*eth0 [Wireshark 1.10.6 (Git

09:05 PM

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

*eth0

File Edit View Go Capture Analyze Statistics Telephc

Filter:

No.	Time	Source
142	2014-04-22 21:04:08.330457000	fe80::211:43
143	2014-04-22 21:04:09.329570000	fe80::211:43
144	2014-04-22 21:04:10.300873000	Nortel_c9:1(
145	2014-04-22 21:04:10.329557000	fe80::211:43
146	2014-04-22 21:04:11.325548000	192.168.65.1
147	2014-04-22 21:04:12.074158000	192.168.65.1
148	2014-04-22 21:04:12.300825000	Nortel_c9:1(
149	2014-04-22 21:04:12.823991000	192.168.65.1
150	2014-04-22 21:04:14.300815000	Nortel_c9:1(

> Frame 145: 86 bytes on wire (688 bits), 86 bytes
> Ethernet II, Src: Dell_e7:f1:95 (00:11:43:e7:f1:9
> Internet Protocol Version 6, Src: fe80::211:43ff
> Internet Control Message Protocol v6

The presentation types the name demo_01.txt in the top name line. You may choose any name. The presentation selected the login name, so the captures will be put in the login's home directory.

```
0000  33 33 ff 37 67 c3 00 11  43 e7 f1 95 86 dd 6
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 0
0020  43 ff fe e7 f1 95 ff 02  00 00 00 00 00 00 0
0030  00 01 ff 37 67 c3 87 00  9f e5 00 00 00 00 2
0040  04 70 1f 11 04 55 02 50  56 ff fe 37 67 c3 0
```

File: "/tmp/wireshark_pcapng_eth0_2... Packets: 150 · Di

Wireshark: Print to File

Name: demo_01.txt

Save in folder: home > preuss

Create Folder

Places	Name	Size	Modified
Search	bin		04/15/2014
Recently Used	Desktop		20:58
preuss	Documents		15:51
root	Downloads		01/17/2014
File System	GNUstep		12/03/2013
	Music		12/03/2013
	pass		03/05/2014
	Pictures		12/03/2013
	Public		12/03/2013
	public_html		12/03/2013
	setup		03/05/2014
	Templates		12/03/2013
	Videos		12/03/2013
	albatross01.txt	155 bytes	02/25/2014
	neigh.txt	203 bytes	02/25/2014
	sha_chk.sha1	52 bytes	02/26/2014
	testtest.pcap.pcapng	3.6 kB	02/25/2014
	trace01.txt	390 bytes	03/21/2014
	wireshark01.out	3.0 kB	20:46
	wireshark02.out	3.6 kB	20:52
	wireshark03.out	3.3 kB	20:56
	wireshark_documentation_net_03212014.pcapng	1.6 MB	03/21/2014

OK Cancel

*eth0 [Wireshark 1.10.6 (Git

09:05 PM

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

*eth0 [Wireshark 1.10.6

File Edit View Go Capture Analyze Statistics Telephony Tools Inter

Filter: Expressior

No.	Time	Source	Dest
142	2014-04-22 21:04:08.330457000	fe80::211:43ff:fee7:f	ff02
143	2014-04-22 21:04:09.329570000	fe80::211:43ff:fee7:f	ff02
144	2014-04-22 21:04:10.300873000	Nortel_c9:10:01	Span
145	2014-04-22 21:04:10.329557000	fe80::211:43ff:fee7:f	ff02
146	2014-04-22 21:04:11.325548000	192.168.65.122	192.
147	2014-04-22 21:04:12.074158000	192.168.65.122	192.
148	2014-04-22 21:04:12.300825000	Nortel_c9:10:01	Span
149	2014-04-22 21:04:12.823991000	192.168.65.122	192.
150	2014-04-22 21:04:14.300815000	Nortel_c9:10:01	Span

> Frame 145: 86 bytes on wire (688 bits), 86 bytes captured (688
> Ethernet II, Src: Dell_e7:f1:95 (00:11:43:e7:f1:95), Dst: IPv6
> Internet Protocol Version 6, Src: fe80::211:43ff:fee7:f195 (fe
> Internet Control Message Protocol v6

The presentation is now ready to press the print button.

Wireshark: Print

Printer

Plain text

PostScript

Output to file: /home/preuss/demo_01.txt Browse...

Print command: lpr

Packet Range

	Captured	Displayed
All packets	150	150
Selected packet only	1	1
Marked packets only	0	0
From first to last marked packet	0	0
Specify a packet range:	0	0
Remove Ignored packets	0	0

Packet Format

Packet summary line

Packet details:

All collapsed

As displayed

All expanded

Packet bytes

Each packet on a new page

Help Cancel Print

```
0000  33 33 ff 37 67 c3 00 11  43 e7 f1 95 86 dd 60 00   33.7g... C.....`.
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 02 11   ... :... ........
0020  43 ff fe e7 f1 95 ff 02  00 00 00 00 00 00 00 00   C....... ........
0030  00 01 ff 37 67 c3 87 00  9f e5 00 00 00 00 20 01   ...7g... ...... .
0040  04 70 1f 11 04 55 02 50  56 ff fe 37 67 c3 01 01   .p...U.P V..7g...
```

File: "/tmp/wireshark_pcapng_eth0_2... Packets: 150 · Displayed: 150 (100.0... Profile: Default

*eth0 [Wireshark 1.10.6 (Git

09:05 PM

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

*eth0 [Wireshark 1.1

File Edit View Go Capture Analyze Statistics Telephony Tools

Filter: Expres

No.	Time	Source
142	2014-04-22 21:04:08.330457000	fe80::211:43ff:fee7:f
143	2014-04-22 21:04:09.329570000	fe80::211:43ff:fee7:f
144	2014-04-22 21:04:10.300873000	Nortel_c9:10:01
145	2014-04-22 21:04:10.329557000	fe80::211:43ff:fee7:f
146	2014-04-22 21:04:11.325548000	192.168.65.122
147	2014-04-22 21:04:12.074158000	192.168.65.122
148	2014-04-22 21:04:12.300825000	Nortel_c9:10:01
149	2014-04-22 21:04:12.823991000	192.168.65.122
150	2014-04-22 21:04:14.300815000	Nor

> Frame 145: 86 bytes on wire (688 bits),
> Ethernet II, Src: Dell_e7:f1:95 (00:11:4
> Internet Protocol Version 6, Src: fe80::
> Internet Control Message Protocol v6

preuss – Dolphin

Find Preview Split Control

Places
- Home
- Network
- Root
- Trash

Devices
- openSUSE-13.1-DVD-i586
- 0 B Removable Media
- 8.0 GiB Hard Drive
- 20.1 GiB Hard Drive
- 399.0 MiB Hard Drive

> Home

bin, Desktop, Documents, Downloads, GNUstep, Music, pass, Pictures, Public, _html, setup, Templates, albatross01.txt, demo_01.txt, sha_chk.sha1, testtest.pcap.pcapng, wireshark01.out, wireshark02.out, wireshark03.out, wireshark_

demo_01.txt (plain text document, 3.5 KiB)

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/kate -b /home/preuss/demo_01.txt

Password:

Remember password

Ignore OK Cancel

The presentation open the file manager Dolphin. The presentation selected the newly printed file. Since Wireshark runs as root, the printed file needs root permission to open.

60 00 33.7g... C.....`.
02 11 ... :... ....
00 00 C..... ....
20 01 ...7g... ..... .
01 01 .p...U.P V..7g...

Displayed: 150 (100.0... Profile: Default

preuss – Dolphin | Run as root – KDE su | *eth0 [Wireshark 1.10.6 (Git | 09:06 PM

msctc-linux-spring2014a - VMware Player (Non-commercial use only)

Player

demo_01.txt - Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

New Open Previous Document Next Document Save Save As Close Undo Redo

Documents Projects

```
No.     Time                           Source                Destination           Protocol Length Info
    145 2014-04-22 21:04:10.329557000 fe80::211:43ff:fee7:f195 ff02::1:ff37:67c3     ICMPv6   86     Neighbor Solicitation for 2001:470:1f11:455:250

Frame 145: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 22, 2014 21:04:10.329557000 CDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1398218650.329557000 seconds
    [Time delta from previous captured frame: 0.028684000 seconds]
    [Time delta from previous displayed frame: 0.028684000 seconds]
    [Time since reference or first frame: 34.027814000 seconds]
    Frame Number: 145
    Frame Length: 86 bytes (688 bits)
    Capture Length: 86 bytes (688 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ipv6:icmpv6]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: Dell_e7:f1:95 (00:11:43:e7:f1:95), Dst: IPv6mcast_ff:37:67:c3 (33:33:ff:37:67:c3)
    Destination: IPv6mcast_ff:37:67:c3 (33:33:ff:37:67:c3)
        Address: IPv6mcast_ff:37:67:c3 (33:33:ff:37:67:c3)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
    Source: Dell_e7:f1:95 (00:11:43:e7:f1:95)
        Address: Dell_e7:f1:95 (00:11:43:e7:f1:95)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: fe80::211:43ff:fee7:f195 (fe80::211:43ff:fee7:f195), Dst: ff02::1:ff37:67c3 (ff02::1:ff37:67c3)
    0110 .... = Version: 6
        [0110 .... = This field makes the filter "ip.version == 6" possible: 6]
    .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
        .... 0000 00.. .... .... .... .... .... = Differentiated Services Field: Default (0x00000000)
        .... .... ..0. .... .... .... .... .... = ECN-Capable Transport (ECT): Not set
        .... .... ...0 .... .... .... .... .... = ECN-CE: Not set
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 32
    Next header: ICMPv6 (58)
    Hop limit: 255
    Source: fe80::211:43ff:fee7:f195 (fe80::211:43ff:fee7:f195)
    [Source SA MAC: Dell_e7:f1:95 (00:11:43:e7:f1:95)]
```

Line: 1 Col: 1 LINE INS demo_01.txt UTF-8

The presentation is ready to add this to the lab pdf answer file.

preuss – Dolphin | demo_01.txt – Kate | *eth0 [Wireshark 1.10.6 (Git | 09:06 PM