THE GEEK STUFF
Linux | DB | Open Source | Web

≡ Menu

- Home
- Free eBook
- Start Here
- Contact
- About

Packet Analyzer: 15 TCPDUMP Command Examples

by Sasikala on August 25, 2010

tcpdump command is also called as packet analyzer.

tcpdump command will work on most flavors of unix operating system. tcpdump allows us to save the packets that are captured, so that we can use it for future analysis. The saved file can be viewed by the same tcpdump command. We can also use open source software like wireshark to read the tcpdump pcap files.

In this tcpdump tutorial, let us discuss some practical examples on how to use the tcpdump command.

1. Capture packets from a particular ethernet interface using tcpdump -i

When you execute tcpdump command without any option, it will capture all the packets flowing through all the interfaces. -i option with tcpdump command, allows you to filter on a particular ethernet interface.

```
$ tcpdump -i eth1
14:59:26.608728 IP xx.domain.netbcp.net.52497 > valh4.lell.net.ssh: . ack 540 win 16554
14:59:26.610602 IP resolver.lell.net.domain > valh4.lell.net.24151:  4278 1/0/0 (73)
14:59:26.611262 IP valh4.lell.net.38527 > resolver.lell.net.domain:  26364+ PTR? 244.207.104.10.in-addr.arpa. (45)
```

In this example, tcpdump captured all the packets flows in the interface eth1 and displays in the standard output.

Note: Editcap utility is used to select or remove specific packets from dump file and translate them into a given format.

2. Capture only N number of packets using tcpdump -c

When you execute tcpdump command it gives packets until you cancel the tcpdump command. Using -c option you can specify the number of packets to capture.

```
$ tcpdump -c 2 -i eth0
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
14:38:38.184913 IP valh4.lell.net.ssh > yy.domain.innetbcp.net.11006: P 1457255642:1457255758(116) ack 1561463966 win 63652
14:38:38.690919 IP valh4.lell.net.ssh > yy.domain.innetbcp.net.11006: P 116:232(116) ack 1 win 63652
```

```
2 packets captured
13 packets received by filter
0 packets dropped by kernel
```

The above tcpdump command captured only 2 packets from interface eth0.

Note: Mergecap and TShark: Mergecap is a packet dump combining tool, which will combine multiple dumps into a single dump file. Tshark is a powerful tool to capture network packets, which can be used to analyze the network traffic. It comes with wireshark network analyzer distribution.

3. Display Captured Packets in ASCII using tcpdump -A

The following tcpdump syntax prints the packet in ASCII.

```
$ tcpdump -A -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
14:34:50.913995 IP valh4.lell.net.ssh > yy.domain.innetbcp.net.11006: P 1457239478:1457239594(116) ack 1561461262 win 63652
E.....@.@..]..i...9...*.V...]...P....h....E...>{..U=...g.
......G..7\+KA....A...L.
14:34:51.423640 IP valh4.lell.net.ssh > yy.domain.innetbcp.net.11006: P 116:232(116) ack 1 win 63652
E.....@.@..\..i...9...*.V..*]...P....h....7......X..!....Im.S.g.u:*..O&....^#Ba...
E..(R.@.|.....9...i.*...]...V..*P..OWp........
```

Note: Ifconfig command is used to configure network interfaces

4. Display Captured Packets in HEX and ASCII using tcpdump -XX

Some users might want to analyse the packets in hex values. tcpdump provides a way to print packets in both ASCII and HEX format.

```
$tcpdump -XX -i eth0
18:52:54.859697 IP zz.domain.innetbcp.net.63897 > valh4.lell.net.ssh: . ack 232 win 16511
        0x0000:  0050 569c 35a3 0019 bb1c 0c00 0800 4500  .PV.5.........E.
        0x0010:  0028 042a 4000 7906 c89c 10b5 aaf6 0f9a  .(.*@.y.........
        0x0020:  69c4 f999 0016 57db 6e08 c712 ea2e 5010  i.....W.n.....P.
        0x0030:  407f c976 0000 0000 0000 0000            @..v........
18:52:54.877713 IP 10.0.0.0 > all-systems.mcast.net: igmp query v3 [max resp time 1s]
        0x0000:  0050 569c 35a3 0000 0000 0000 0800 4600  .PV.5.........F.
        0x0010:  0024 0000 0000 0102 3ad3 0a00 0000 e000  .$......:.......
        0x0020:  0001 9404 0000 1101 ebfe 0000 0000 0300  ................
        0x0030:  0000 0000 0000 0000 0000 0000            ............
```

5. Capture the packets and write into a file using tcpdump -w

tcpdump allows you to save the packets to a file, and later you can use the packet file for further analysis.

```
$ tcpdump -w 08232010.pcap -i eth0
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
32 packets captured
32 packets received by filter
0 packets dropped by kernel
```

-w option writes the packets into a given file. The file extension should be .pcap, which can be read by any network protocol
analyzer.

6. Reading the packets from a saved file using tcpdump -r

You can read the captured pcap file and view the packets for analysis, as shown below.

```
$tcpdump -tttt -r data.pcap
2010-08-22 21:35:26.571793 00:50:56:9c:69:38 (oui Unknown) > Broadcast, ethertype Unknown (0xcafe), length 74:
        0x0000:  0200 000a ffff 0000 ffff 0c00 3c00 0000  ............<...
        0x0010:  0000 0000 0100 0080 3e9e 2900 0000 0000  ........>.).....
        0x0020:  0000 0000 ffff ffff ad00 996b 0600 0050  ...........k...P
        0x0030:  569c 6938 0000 0000 8e07 0000            V.i8........
2010-08-22 21:35:26.571797 IP valh4.lell.net.ssh > zz.domain.innetbcp.net.50570: P 800464396:800464448(52) ack 203316566 win 71
2010-08-22 21:35:26.571800 IP valh4.lell.net.ssh > zz.domain.innetbcp.net.50570: P 52:168(116) ack 1 win 71
2010-08-22 21:35:26.584865 IP valh5.lell.net.ssh > 11.154.12.255.netbios-ns: NBT UDP PACKET(137): QUERY; REQUEST; BROADC
```

7. Capture packets with IP address using tcpdump -n

In all the above examples, it prints packets with the DNS address, but not the ip address. The following example captures the packets and it will display the IP address of the machines involved.

```
$ tcpdump -n -i eth0
15:01:35.170763 IP 10.0.19.121.52497 > 11.154.12.121.ssh: P 105:157(52) ack 18060 win 16549
15:01:35.170776 IP 11.154.12.121.ssh > 10.0.19.121.52497: P 23988:24136(148) ack 157 win 113
15:01:35.170894 IP 11.154.12.121.ssh > 10.0.19.121.52497: P 24136:24380(244) ack 157 win 113
```

8. Capture packets with proper readable timestamp using tcpdump -tttt

```
$ tcpdump -n -tttt -i eth0

2010-08-22 15:10:39.162830 IP 10.0.19.121.52497 > 11.154.12.121.ssh: . ack 49800 win 16390
2010-08-22 15:10:39.162833 IP 10.0.19.121.52497 > 11.154.12.121.ssh: . ack 50288 win 16660
2010-08-22 15:10:39.162867 IP 10.0.19.121.52497 > 11.154.12.121.ssh: . ack 50584 win 16586
```

9. Read packets longer than N bytes

You can receive only the packets greater than n number of bytes using a filter ‘greater’ through tcpdump command

```
$ tcpdump -w g_1024.pcap greater 1024
```

10. Receive only the packets of a specific protocol type

You can receive the packets based on the protocol type. You can specify one of these protocols — fddi, tr, wlan, ip, ip6, arp, rarp, decnet, tcp and udp. The following example captures only arp packets flowing through the eth0 interface.

```
$ tcpdump -i eth0 arp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
19:41:52.809642 arp who-has valh5.lell.net tell valh9.lell.net
19:41:52.863689 arp who-has 11.154.12.1 tell valh6.lell.net
19:41:53.024769 arp who-has 11.154.12.1 tell valh7.lell.net
```

11. Read packets lesser than N bytes

You can receive only the packets lesser than n number of bytes using a filter ‘less’ through tcpdump command

```
$ tcpdump -w l_1024.pcap  less 1024
```

12. Receive packets flows on a particular port using tcpdump port

If you want to know all the packets received by a particular port on a machine, you can use tcpdump command as shown below.

```
$ tcpdump -i eth0 port 22
19:44:44.934459 IP valh4.lell.net.ssh > zz.domain.innetbcp.net.63897: P 18932:19096(164) ack 105 win 71
19:44:44.934533 IP valh4.lell.net.ssh > zz.domain.innetbcp.net.63897: P 19096:19260(164) ack 105 win 71
19:44:44.934612 IP valh4.lell.net.ssh > zz.domain.innetbcp.net.63897: P 19260:19424(164) ack 105 win 71
```

13. Capture packets for particular destination IP and Port

The packets will have source and destination IP and port numbers. Using tcpdump we can apply filters on source or destination IP and port number. The following command captures packets flows in eth0, with a particular destination ip and port number 22.

```
$ tcpdump -w xpackets.pcap -i eth0 dst 10.181.140.216 and port 22
```

14. Capture TCP communication packets between two hosts

If two different process from two different machines are communicating through tcp protocol, we can capture those packets using tcpdump as shown below.

```
$tcpdump -w comm.pcap -i eth0 dst 16.181.170.246 and port 22
```

You can open the file comm.pcap using any network protocol analyzer tool to debug any potential issues.

15. tcpdump Filter Packets – Capture all the packets other than arp and rarp

In tcpdump command, you can give “and”, “or” and “not” condition to filter the packets accordingly.

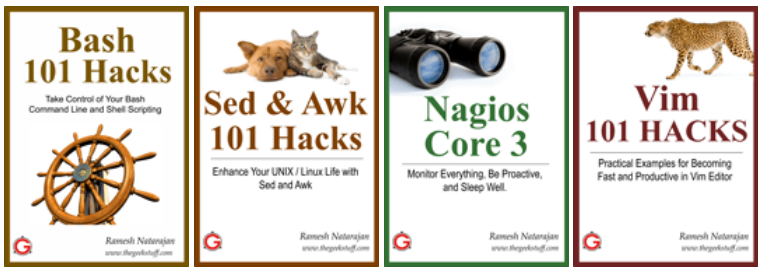
```
$ tcpdump -i eth0 not arp and not rarp
20:33:15.479278 IP resolver.lell.net.domain > valh4.lell.net.64639:  26929 1/0/0 (73)
20:33:15.479890 IP valh4.lell.net.16053 > resolver.lell.net.domain:  56556+ PTR? 255.107.154.15.in-addr.arpa. (45)
20:33:15.480197 IP valh4.lell.net.ssh > zz.domain.innetbcp.net.63897: P 540:1504(964) ack 1 win 96
20:33:15.487118 IP zz.domain.innetbcp.net.63897 > valh4.lell.net.ssh: . ack 540 win 16486
```

```
20:33:15.668599 IP 10.0.0.0 > all-systems.mcast.net: igmp query v3 [max resp time 1s]
```


If you enjoyed this article, you might also like..

1. 50 Linux Sysadmin Tutorials
2. 50 Most Frequently Used Linux Commands (With Examples)
3. Top 25 Best Linux Performance Monitoring and Debugging Tools
4. Mommy, I found it! – 15 Practical Linux Find Command Examples
5. Linux 101 Hacks 2nd Edition eBook Free

- Awk Introduction – 7 Awk Print Examples
- Advanced Sed Substitution Examples
- 8 Essential Vim Editor Navigation Fundamentals
- 25 Most Frequently Used Linux IPTables Rules Examples
- Turbocharge PuTTY with 12 Powerful Add-Ons



Tagged as: aix tcpdump, dhcp tcpdump, FreeBSD tcpdump, TCP Dump, tcpdump command, tcpdump DNS, tcpdump for Windows, tcpdump format, tcpdump how to, tcpdump icmp, tcpdump ip, tcpdump not, tcpdump windows, tcpdump wireshark

{ 38 comments… add one }

- Jeffrey August 25, 2010, 2:50 am

  Why not use wireshark?

  Link
- Zigor Alcañiz Eiguren August 25, 2010, 2:57 am

  Hi!

  Nice tips, good work.

  I think there is a glitch in number 14.

  It should be something like:
  $tcpdump -w comm.pcap -i eth0 tcp host 16.181.170.246 or host 10.181.140.216.

  You specify that you just want TCP traffic and you don't specify whether you want those hosts as src or dst, so it captures traffic in both directions.

  Bye…

  Link
- Zigor Alcañiz Eiguren August 25, 2010, 3:05 am

  Sorry,… I correct myself (this happens for no trying the command prior to writting it):

  There is a lacking "and":
  $tcpdump -w comm.pcap -i eth0 tcp and \(host 16.181.170.246 or host 10.181.140.216\)

  Bye…

  Link
- Tanmay Joshi August 25, 2010, 6:30 am

  Nice article. Good for me to get started. Just had one suggestion, point 8 should have came before point 6. I got bit

confused with -tttt option and was solved at point 8.

But thanks for this. Would really help me getting me ahead into linux world.

Thanks,
Tanmay

Link

- Diggy August 25, 2010, 10:48 am

  Number 14 should be:

  tcpdump -w comm.pcap -i eth0 src xxx.xxx.xxx.xxx and port 22 and dst xxx.xxx.xxx.xxx and port 22

  That captures all ssh packets flowing between the source and destination addresses.

  Regarding an earlier Comment suggesting the use of Wireshark, while i use it and find it an excellent tool: 1) it requires a desktop environment and, on servers at least, that's usually not desirable, and; 2) it has some overhead, and may not capture all packets on a busy network; tcpdump is very light weight, and has no problem capturing all packets. .BTW, as the OP and others probably know, a tcpdump output file can be read/rendered by Wireshark

  Link
- Anwar August 25, 2010, 3:58 pm

  why not whireshark..??? yea… this command runs on all Unix OS.
  But wireshark is best if you want to capture the Network packets and use them for analyzing..

  Link
- Ivan Carrasco Q. August 27, 2010, 9:25 am

  Wireshark works only in graphical interface, tcpdump on CLI.

  Regards,
  Iván

  Link
- b-rad September 1, 2010, 3:58 pm

  @Ivan, Wireshark, as mentioned in the article, also ships with its CLI tool tshark. Which can be used on servers in a CLI only environment. Although, I don't know if it has any advantages over tcpdump.

  Link
- IMFerret January 14, 2011, 9:01 am

  Hello I am using the following command:
  tcpdump -i eth0 -n
  This yields all traffic seen. A great deal HTTP traffic from our 10.11.76.x subnet.
  However if I try to filter, no matter what I use, I get no results.
  tcpdump -i eth0 -n port 80
  Yields NO traffic?!
  Similarly, attempts to filter for source or destination IPs yeilds no traffic. Even when I use IPs that I know are chatty I get nothing.
  Any ideas why? Thanks in advance.

  Link
- Diggy January 14, 2011, 10:53 am

  I believe that should be "tcpdump -i eth0 -n dst port 80″ (" added for clarity)

  Link
- Rajnish Pankaj January 28, 2011, 8:17 am

  Hi,

  Quite interesting but i want to see dscp marking value and other details.Is there any option for looking that in tcpdump analyzer?

  Link
- Mullaiselvan. M March 28, 2011, 7:04 am

  Nice….

I tried tcpdump/tshark/ tethereal to capture port 80 packet in ab -n 1000 http://fedora9/ and grep only source IP and SYN packet. But most of the time these tools didn't capture 1000 SYN request. Do any one know why. please reply.

Thanks…

Link

- Prasad March 28, 2011, 7:15 am

  Hi

  Thank you very much to all in this forum. the information provided here is very much helpful to me…

  The below command will capture the udp network packets(to and fro) between the two IPs.

  command: tcpdump -w -s -i udp and \(host and host \)

  Example: tcpdump -w comm.pcap -s 1000 -i bond0 udp and \(host 172.20.68.176 and host 172.24.173.9\)

  Thanks & Regards,
  Prasad.

  Link

- Johnny August 25, 2011, 9:41 am

  I wanted to learn basic tcpdump and came across this site. Great Job and many thanks!

  Link

- vikas September 15, 2011, 1:56 am

  Nice article Ramesh!! Thanks.

  Link

- imkapps September 25, 2011, 4:11 pm

  Thanks for the post, I'm trying to do the following and was hoping to use tip 14 for that.
  I have an iPhone, that can control my TV.
  The iPhone is connected via the WLAN of my router, the TV is connected via LAN to router.
  I want to capture the data between iPhone and TV, by using TCPDump on a PC (via LAN) or laptop (WLAN).

  Is this possible?

  Link

- Stat November 3, 2011, 6:26 am

  Could anybody please help with the tcpdump command format in case I need all the messages flow (source and destination) for the specific IP?

  Link

- MH November 23, 2011, 12:47 pm

  can someone please tell me the IP protocol number, the source and destination IP addresses being used on this capturing packet command please 🙁

  [student@centos-R9-Group1-R10-Group1 ~]$ sudo tcpdump -v -X -i eth1 -l | tee lo
  g16.txt
  tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
  11:57:24.580138 IP (tos 0xc0, ttl 64, id 65248, offset 0, flags [none], proto:
  UDP (17), length: 192) 200.0.9.10.router > 200.0.9.255.router:
  RIPv2, Response, length: 164, routes: 8
  AFI: IPv4: 200.0.5.0/24, tag 0x0000, metric: 1, next-hop: self
  AFI: IPv4: 200.0.7.0/24, tag 0x0000, metric: 1, next-hop: self[|

  Link

- Anshuman Goyal November 29, 2011, 8:59 am

  What if I want to filter the packets from tcpdump with Content-Type.

  I want to capture all packets which have content type Video. Will it be possible with tcpdump?

  Link

- M.Tahir December 14, 2011, 12:02 am

Very nice & precise tutorial.
Help a lot.
Good work keep it up!

Thanks a bundle.

Link

- Anant Agarwal March 11, 2012, 7:19 am

  Hey, how do i get tcpdump to generate –

  1. Flow duration
  2. Flow volume in bytes and packets
  3. Packet length
  4. Inter-arrival time between packet

  any help would be appreciated. thanks.

  Link
- yehuda June 6, 2012, 6:56 pm

  I'm looking for linux commands to be able to measure network speed on linux box at customer sites. Do you think tcpdump could be used to measure the speed. We cannot use tools such as ipef as it requires to be installed on a client and a server. Can one run the following command, compute the speed by parsing the time and length.
  "tcpdump -c 50 -i eth0 -n -tttt"

  Link
- Pavan June 15, 2012, 1:38 am

  good to read.Please publish more articles about this quite helpful for every one

  Link
- Peluso August 20, 2012, 6:21 pm

  Hi, Does anyone knows if via tcpdump is there a way to know if the packet was translated when using NAT or if the packet goes redirected to a different IP?

  Link
- jamuna August 31, 2012, 3:45 am

  how do i get tcpdump to generate –
  1. Packets
  2. Bytes
  3. Packet size
  4. Inter packet time

  Link
- jamuna August 31, 2012, 6:54 am

  Is there a way to get the size of a packet on the network with tcpdump (or other program)? Or can you calculate it?

  Link
- Naveen September 11, 2012, 4:02 pm

  –to see what packets are sent to destination xx.yy.c.d from port 8021
  tcpdump -s0 -A -n -tttt -i eth0:1 dst xx.yy.c.d and port 8021

  –to see what packets are received from source xx.yy.c.d to port 8021
  tcpdump -s0 -A -n -tttt -i eth0:1 src xx.yy.c.d and port 8021

  Link
- bob February 12, 2013, 10:21 pm

  small bug: eth0 will never exist as there is no 'eth' driver. Perhaps you mean re0, rl0, wlan0, en0, lagg0, etc?

  Link
- Anonymous April 28, 2013, 7:09 pm

  Wireshark is a great analysis tool. But one reason not to use it when sifting through a capture that is suspected of containing illicit traffic is that Wireshark has had many security flaws. I believe these flaws are most attributed to the many plugins available.

In essence, Wireshark could be compromised merely by reading packets intended to compromise the flaws in some versions.

Link

- Abdul Majeed LArdhi July 4, 2013, 6:40 am

  how can i get red of the SSAP and DSAP !!?
  Is there any options in tcpdump to sniff inline traffic comming from tap device ?

  # tcpdump -c 20 -tttt -i eth2
  tcpdump: WARNING: eth2: no IPv4 address assigned
  tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
  listening on eth2, link-type EN10MB (Ethernet), capture size 96 bytes
  2013-07-04 15:37:00.362454 00:12:1e:2d:45:00 (oui Unknown) OSI > 00:18:74:17:fb:40 (oui Unknown) Unknown DSAP 0x62 Information, send seq 0, rcv seq 0, Flags [Command, Poll], length 576
  2013-07-04 15:37:00.362537 00:12:1e:2d:45:00 (oui Unknown) OSI > 00:18:74:17:fb:40 (oui Unknown) Unknown DSAP 0x62 Information, send seq 0, rcv seq 0, Flags [Command, Poll], length 93
  2013-07-04 15:37:00.362554 00:12:1e:2d:45:00 (oui Unknown) OSI > 00:18:74:17:fb:40 (oui Unknown) Unknown DSAP 0x62 Information, send seq 0, rcv seq 0, Flags [Command, Poll], length 576
  2013-07-04 15:37:00.362569 00:18:74:17:45:00 (oui Unknown) Unknown SSAP 0x16 > 00:12:1e:2d:04:1f (oui Unknown) Unknown DSAP 0x1c Information, send seq 32, rcv seq 0, Flags [Command, Poll], length 46
  2013-07-04 15:37:00.362555 00:18:74:17:45:00 (oui Unknown) Unknown SSAP 0x62 > 00:12:1e:2d:04:1f (oui Unknown) Unknown DSAP 0x5a Information, send seq 32, rcv seq 0, Flags [Command], length 46
  2013-07-04 15:37:00.362877 00:18:74:17:45:00 (oui Unknown) Unknown SSAP 0x08 > 00:12:1e:2d:04:1f (oui Unknown) Unknown DSAP 0x6a Information, send seq 32, rcv seq 0, Flags [Command], length 46
  2013-07-04 15:37:00.363100 00:12:1e:2d:45:00 (oui Unknown) Unknown SSAP 0x8a > 00:18:74:17:fb:40 (oui Unknown) Unknown DSAP 0x30 Information, send seq 32, rcv seq 0, Flags [Command], length 1440

  Link

- Momin July 6, 2013, 4:50 pm

  Excellent article to start using tcpdump; simple and precise. Thank you.

  Link

- Dinesh Venkatasubramanian February 25, 2014, 4:33 am

  Hi

  If i need to run tcp dump between a host and a destination server on 20th of previous month what is the syntax for that. Please let me know

  Thanks
  Dinesh

  Link

- Majid March 17, 2014, 2:38 am

  Hi,
  what is the option -s0 use for, is this to specify the host, what if i don't use -s0?
  Is there any option to capture the TCP dump based on time duration rather than packets?

  tcpdump -c 60 -i eth1 -s0 host XXX.XXX.XXX.XXX -w test.cap

  bye

  Link

- Bill N. November 5, 2014, 4:06 pm

  when tcpdump displays the 'capture size', does that include any TCP header-like information. E.g., my application expects to read 800 to 100 bytes on a particular port each time. Frequently I see 40 to 60 bytes in the 'capture size'. Also, I cannot make heads or tails out of the hex/ascii output (-A option or -XX option).

  Link

- shashikumar H R November 28, 2014, 2:58 am

  How to capture the packets in pcap-ng format using tcpdump?

  Link

- Bilal April 2, 2015, 10:10 am

Hi,

Can you please tell tcpdump command to capture packets on particular destination number(for eg 923333333333) for sip call ?
Also how to capture packets for sip call flow between two IPs ?

Please let me know.

Regards,

Link

- Nimesh April 11, 2015, 8:03 am

  Hi All,

  I can not take the pcap below command but i can see the traffic in live so what should be enter the command if need to eth4 filter in below command.

  tcpdump -n host 10.10.3.2 and port 161 | grep -i 'eth4' -w /var/crm12345.pcap -s 4000

  Anyone suggest me.

  Link

- charana June 26, 2015, 5:56 am

  thanks for your tutoriles

  Link

Leave a Comment

Name

Email

Website

Comment

Submit

Notify me of followup comments via e-mail

Next post: Linux cpio Examples: How to Create and Extract cpio Archives (and tar archives)

Previous post: How To Be Productive and Get Things Done Using GTD

RSS | Email | Twitter | Facebook | Google+

Search

POPULAR POSTS

- 12 Amazing and Essential Linux Books To Enrich Your Brain and Library
- 50 UNIX / Linux Sysadmin Tutorials
- 50 Most Frequently Used UNIX / Linux Commands (With Examples)
- How To Be Productive and Get Things Done Using GTD
- 30 Things To Do When you are Bored and have a Computer
- Linux Directory Structure (File System Structure) Explained with Examples
- Linux Crontab: 15 Awesome Cron Job Examples
- Get a Grip on the Grep! – 15 Practical Grep Command Examples
- Unix LS Command: 15 Practical Examples
- 15 Examples To Master Linux Command Line History
- Top 10 Open Source Bug Tracking System
- Vi and Vim Macro Tutorial: How To Record and Play
- Mommy, I found it! -- 15 Practical Linux Find Command Examples
- 15 Awesome Gmail Tips and Tricks
- 15 Awesome Google Search Tips and Tricks
- RAID 0, RAID 1, RAID 5, RAID 10 Explained with Diagrams
- Can You Top This? 15 Practical Linux Top Command Examples
- Top 5 Best System Monitoring Tools
- Top 5 Best Linux OS Distributions
- How To Monitor Remote Linux Host using Nagios 3.0
- Awk Introduction Tutorial – 7 Awk Print Examples
- How to Backup Linux? 15 rsync Command Examples
- The Ultimate Wget Download Guide With 15 Awesome Examples
- Top 5 Best Linux Text Editors
- Packet Analyzer: 15 TCPDUMP Command Examples
- The Ultimate Bash Array Tutorial with 15 Examples
- 3 Steps to Perform SSH Login Without Password Using ssh-keygen & ssh-copy-id
- Unix Sed Tutorial: Advanced Sed Substitution Examples
- UNIX / Linux: 10 Netstat Command Examples
- The Ultimate Guide for Creating Strong Passwords
- 6 Steps to Secure Your Home Wireless Network
- Turbocharge PuTTY with 12 Powerful Add-Ons

CATEGORIES

- Linux Tutorials
- Vim Editor
- Sed Scripting
- Awk Scripting
- Bash Shell Scripting
- Nagios Monitoring
- OpenSSH
- IPTables Firewall
- Apache Web Server
- MySQL Database
- Perl Programming
- Google Tutorials
- Ubuntu Tutorials
- PostgreSQL DB
- Hello World Examples
- C Programming
- C++ Programming

- DELL Server Tutorials
- Oracle Database
- VMware Tutorials

Ramesh Natarajan

Follow

About The Geek Stuff


My name is **Ramesh Natarajan**. I will be posting instruction guides, how-to, troubleshooting tips and tricks on Linux, database, hardware, security and web. My focus is to write articles that will either teach you or help you resolve a problem. Read more about Ramesh Natarajan and the blog.

Contact Us

Email Me : Use this Contact Form to get in touch me with your comments, questions or suggestions about this site. You can also simply drop me a line to say hello!.

Follow us on Google+

Follow us on Twitter

Become a fan on Facebook

Support Us

Support this blog by purchasing one of my ebooks.

Bash 101 Hacks eBook

Sed and Awk 101 Hacks eBook

Vim 101 Hacks eBook

Nagios Core 3 eBook