UEMF
الجامعة الأورومتوسطية بفاس
EUROMED UNIVERSITY OF FES
UNIVERSITÉ EUROMED DE FÈS

EIDIA
École d'Ingénierie Digitale et d'Intelligence Artificielle

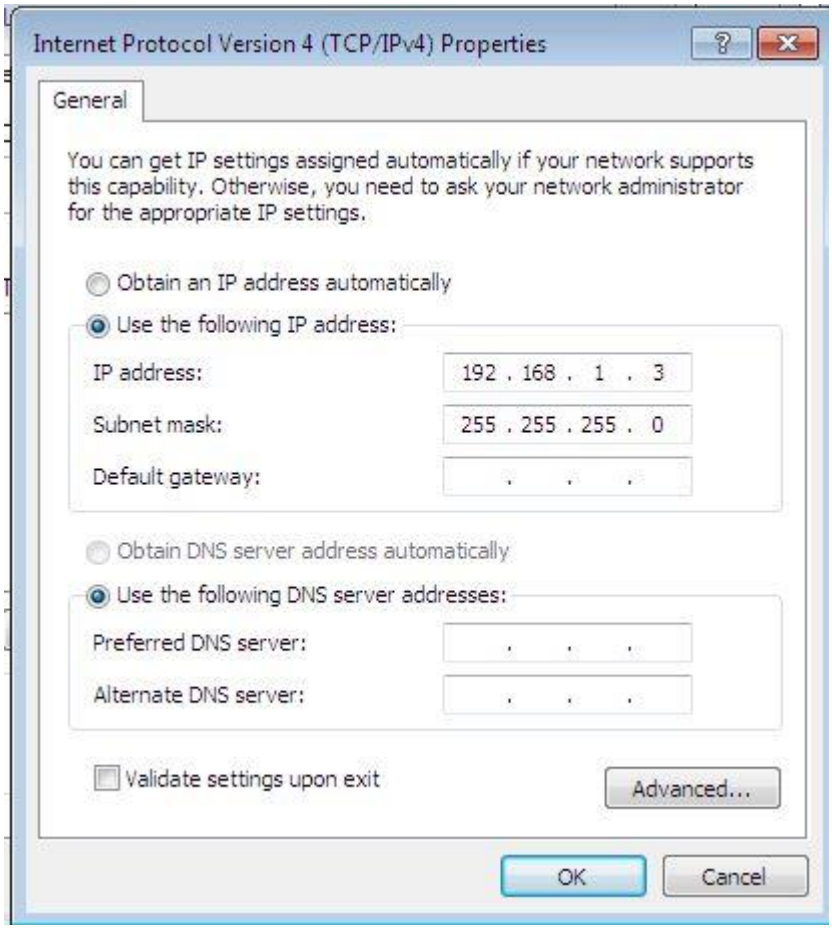
Base de

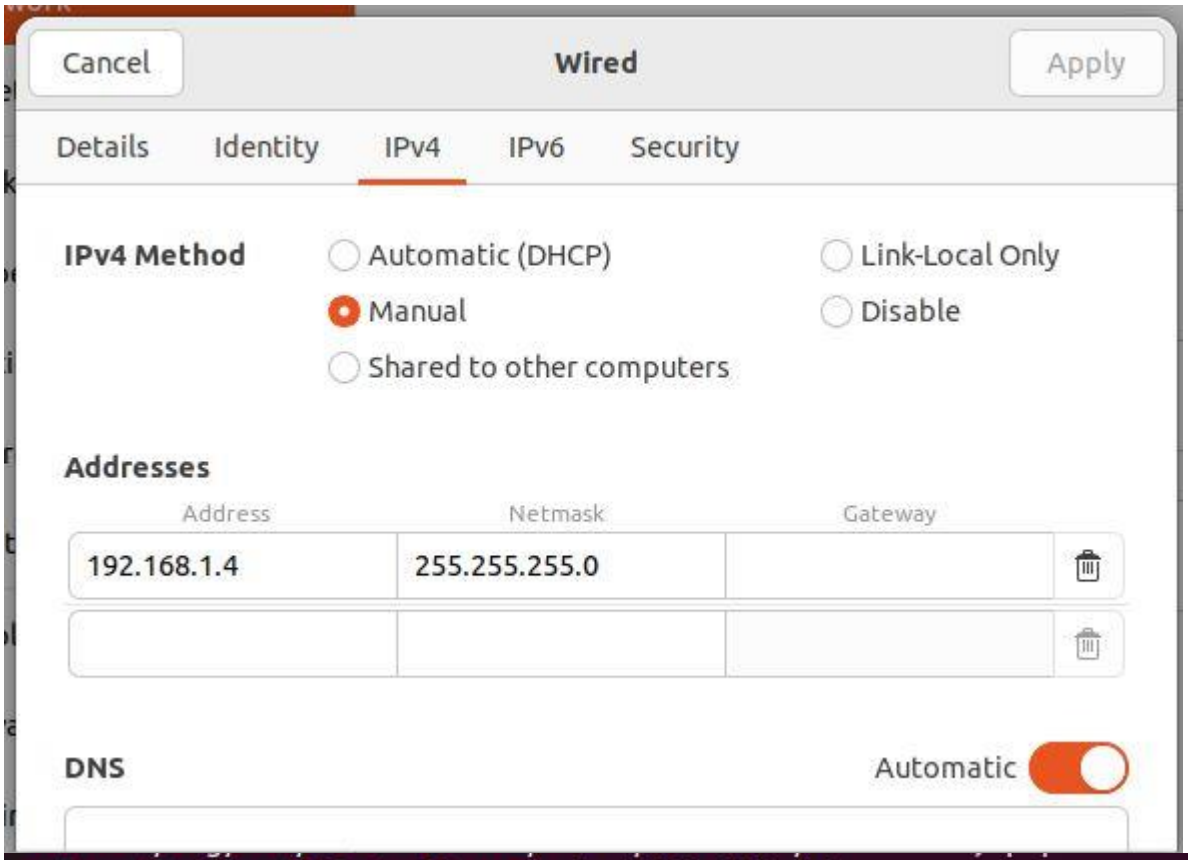
CYBERSECURITE TP1:

Attaques passives :sniffing passif

Mohamed Alaoui Mhamdi && Naoufal amallah

Partie1:Préparation d’environnement du TP






```
mohamed@mohamed-VirtualBox:~$ ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=128 time=0.693 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=128 time=0.255 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=128 time=0.382 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=128 time=0.253 ms
64 bytes from 192.168.1.3: icmp_seq=5 ttl=128 time=0.501 ms
64 bytes from 192.168.1.3: icmp_seq=6 ttl=128 time=0.257 ms
64 bytes from 192.168.1.3: icmp_seq=7 ttl=128 time=0.477 ms
64 bytes from 192.168.1.3: icmp_seq=8 ttl=128 time=0.410 ms
64 bytes from 192.168.1.3: icmp_seq=9 ttl=128 time=0.460 ms
64 bytes from 192.168.1.3: icmp_seq=10 ttl=128 time=0.410 ms
64 bytes from 192.168.1.3: icmp_seq=11 ttl=128 time=0.282 ms
64 bytes from 192.168.1.3: icmp_seq=12 ttl=128 time=0.393 ms
64 bytes from 192.168.1.3: icmp_seq=13 ttl=128 time=0.491 ms
64 bytes from 192.168.1.3: icmp_seq=14 ttl=128 time=0.372 ms
64 bytes from 192.168.1.3: icmp_seq=15 ttl=128 time=0.466 ms
64 bytes from 192.168.1.3: icmp_seq=16 ttl=128 time=0.465 ms
^C
--- 192.168.1.3 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15356ms
rtt min/avg/max/mdev = 0.253/0.410/0.693/0.111 ms
mohamed@mohamed-VirtualBox:~$
```

```
Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time<1ms TTL=64
Reply from 192.168.1.4: bytes=32 time<1ms TTL=64
Reply from 192.168.1.4: bytes=32 time<1ms TTL=64
Reply from 192.168.1.4: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\mohamed>
```

Partie2:Implémentation d’un sniffer passif

```
mohamed@mohamed-VirtualBox:~/Desktop$ cc -c sniffer_eth_ip_tcp_data.c
mohamed@mohamed-VirtualBox:~/Desktop$ cc  sniffer_eth_ip_tcp_data.c -o
 sniffer
```

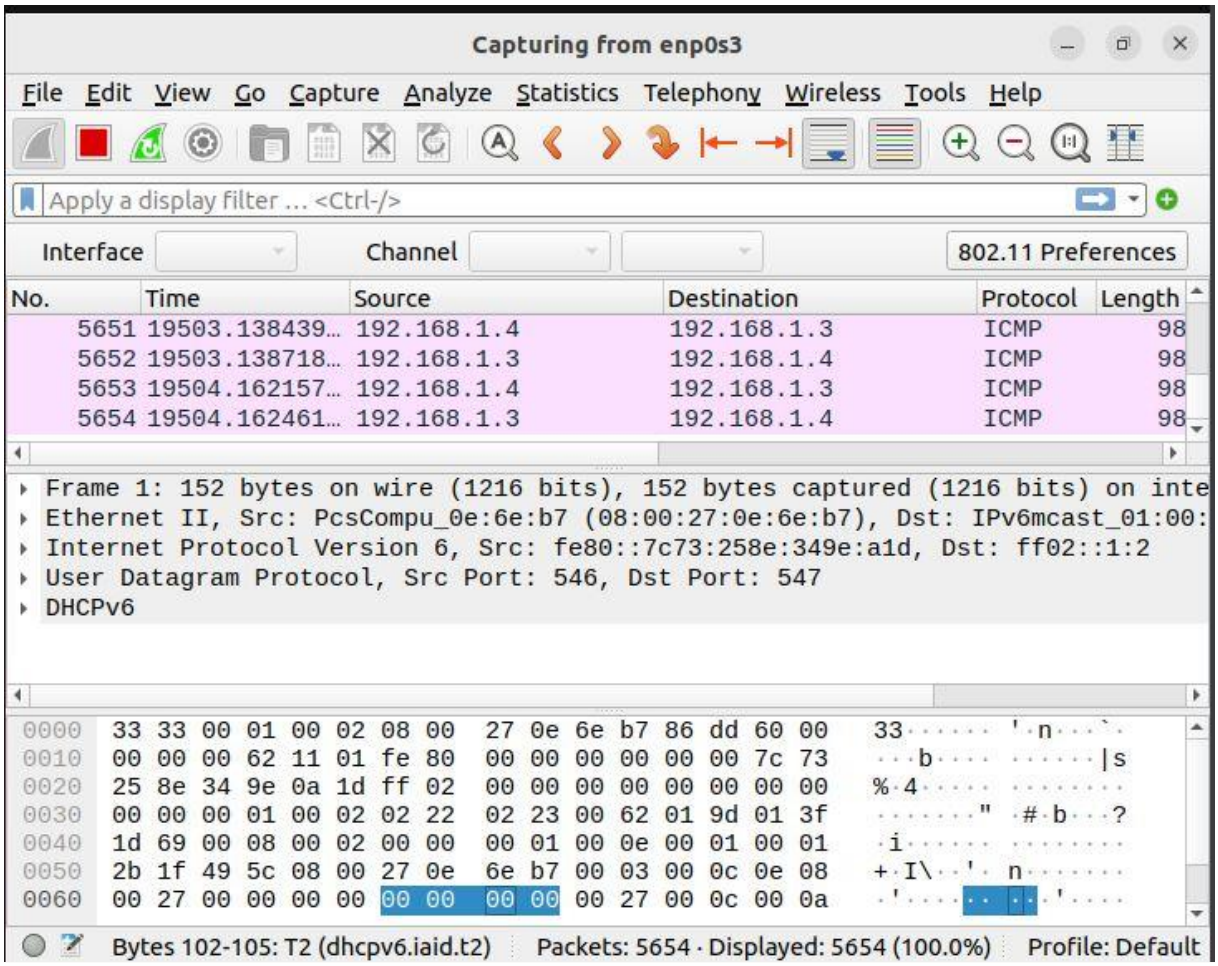
```
mohamed@mohamed-VirtualBox:~/Desktop$ nmcli device status
DEVICE  TYPE      STATE      CONNECTION
enp0s3  ethernet  connected  Wired connection 1
lo      loopback  unmanaged  --
mohamed@mohamed-VirtualBox:~/Desktop$ sudo ./sniffer enp0s3 1
```

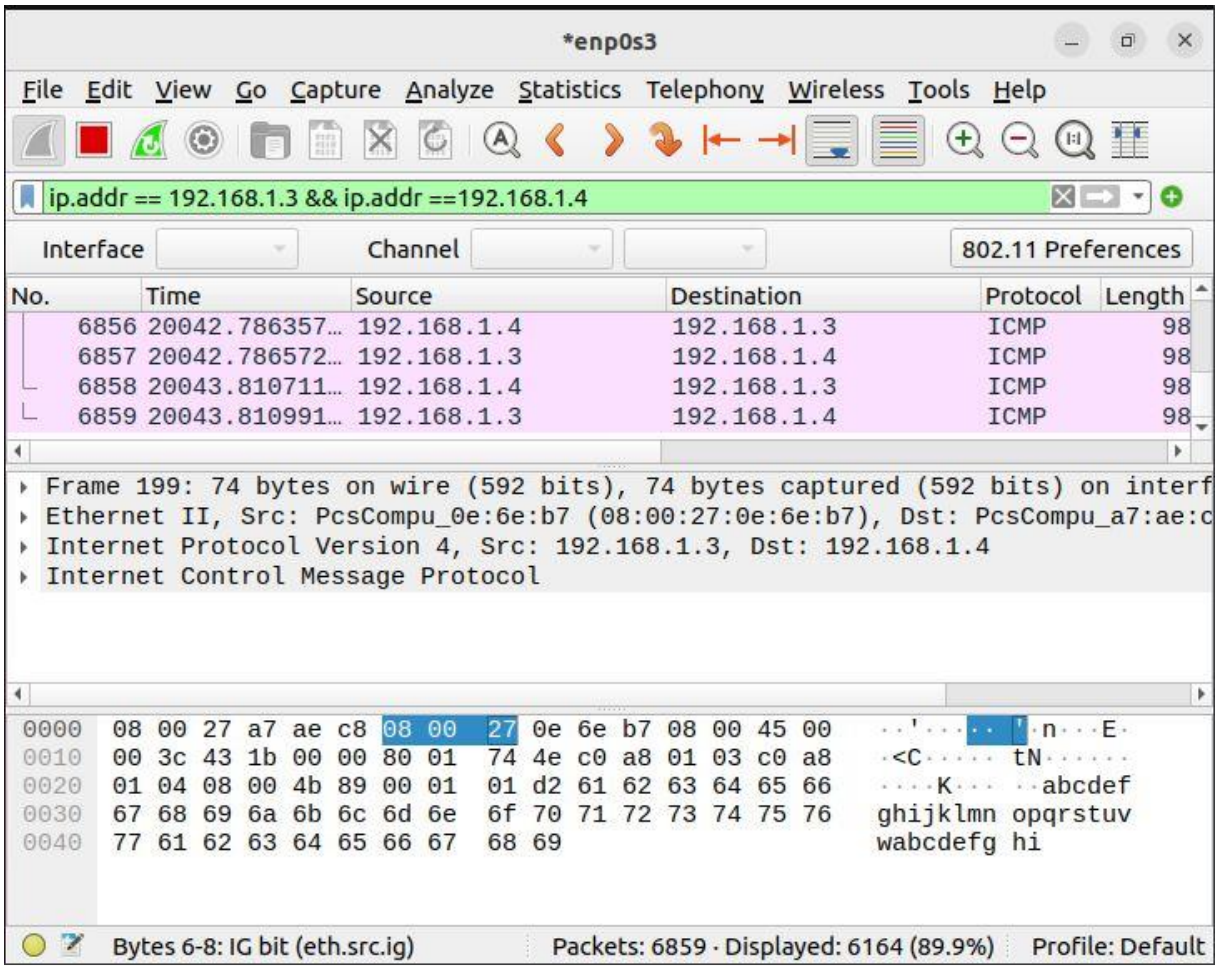
```
[sudo] password for mohamed:


---------Packet---Starts----

08 00 27 a7 ae c8 08 00 27 0e 6e b7 08 00 45 00 00 54 0c 2a 00 00 80 0
1 ab 27 c0 a8 01 03 c0 a8 01 04 00 00 bc 63 00 08 00 17 ef 7a 91 63 00
 00 00 00 f7 cb 0c 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 3
3 34 35 36 37

--------Packet---Ends-----

Destination MAC: 08 00 27 A7 AE C8
Source MAC: 08 00 27 0E 6E B7
Protocol: 08 00
TTL: 128
Dest IP address: 192.168.1.4
Source IP address: 192.168.1.3
Not a TCP packet
Not a UDP packet
Data Len : 44
------------------
```

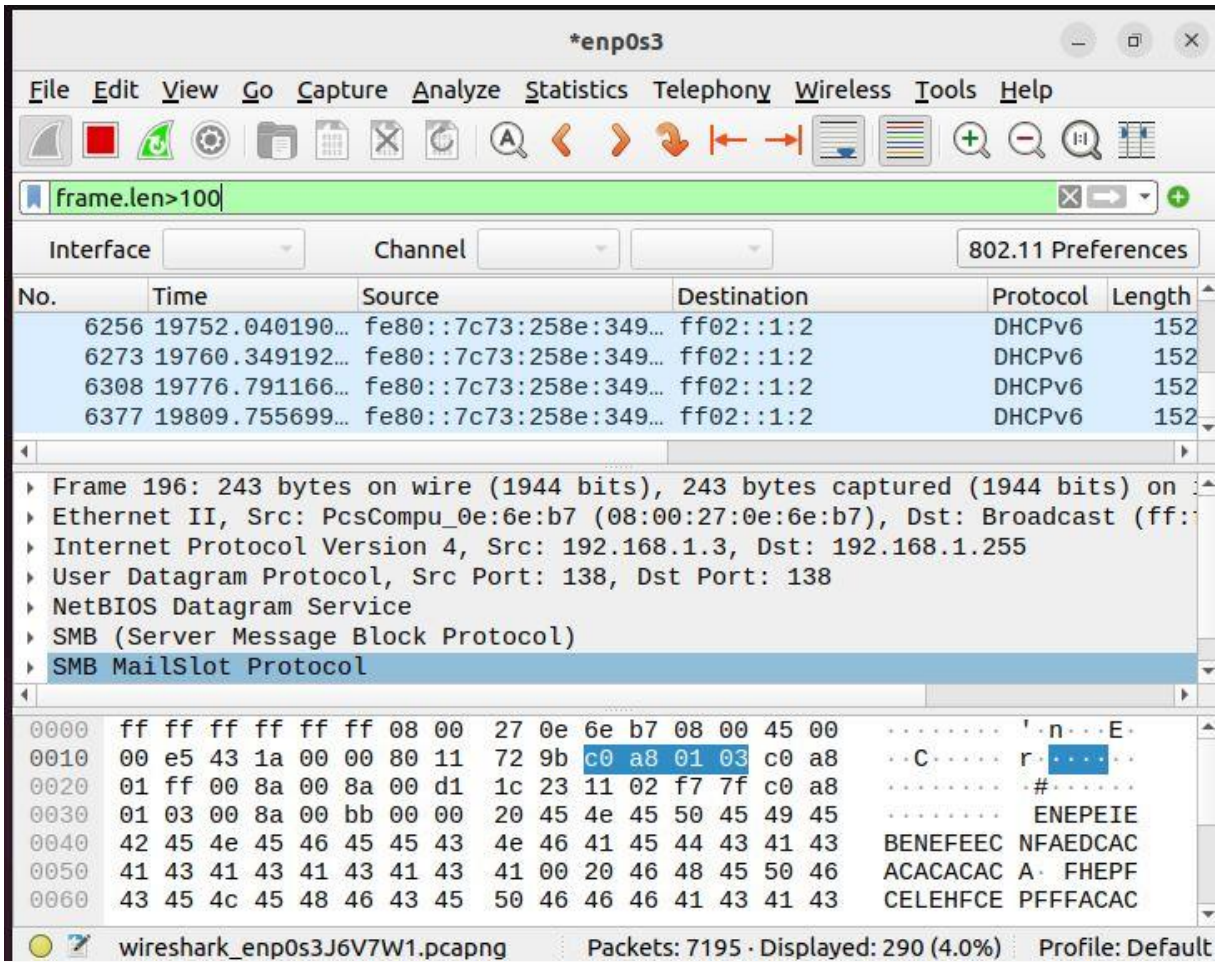
```
int ParseUdpHeader(unsigned char *packet , int len)
{
        struct ethhdr *ethernet_header;
        struct iphdr *ip_header;
        struct udphdr *udp_header;

        /* Check if enough bytes are there for TCP Header */

        if(len >= (sizeof(struct ethhdr) + sizeof(struct iphdr) +
sizeof(struct udphdr)))
        {
                /* Do all the checks: 1. Is it an IP pkt ? 2. is it TCP ? */

                ethernet_header = (struct ethhdr *)packet;

xt Editor       if(ntohs(ethernet_header->h_proto) == ETH_P_IP)
                {
                        ip_header = (struct iphdr *)(packet + sizeof(struct
ethhdr));


                        if(ip_header->protocol == IPPROTO_UDP)
                        {
                                printf("UDP datagram (UDP num=%d)\n",
ip_header->protocol);
                                udp_header = (struct udphdr*)(packet +
sizeof(struct ethhdr) + ip_header->ihl*4 );
                                /* Print the Dest and Src ports */

                                printf("Source Port: %d\n",
ntohs(udp_header->source));
                                printf("Dest Port: %d\n", ntohs(udp_header-
>dest));

                        }
                        else
                        {
                                printf("Not a UDP packet\n");
                        }
                }
                else
                {
                        printf("Not an IP packet\n");
                }

        }
        else
        {
                printf("UDP Header not present \n");

        }
}
```

Partie3:manipulation des niffers

3-Oui on pout capturer les trafics échangés entre les machines du reste du réseau




*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.3 && ip.addr ==192.168.1.4
Interface
Channel
802.11 Preferences
No. Time Source Destination Protocol Length
6856 20042.786357… 192.168.1.4 192.168.1.3 ICMP 98
6857 20042.786572… 192.168.1.3 192.168.1.4 ICMP 98
6858 20043.810711… 192.168.1.4 192.168.1.3 ICMP 98
6859 20043.810991… 192.168.1.3 192.168.1.4 ICMP 98
Frame 199: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interf
Ethernet II, Src: PcsCompu_0e:6e:b7 (08:00:27:0e:6e:b7), Dst: PcsCompu_a7:ae:c
Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.4
Internet Control Message Protocol
0000 08 00 27 a7 ae c8 08 00 27 0e 6e b7 08 00 45 00
0010 00 3c 43 1b 00 00 80 01 74 4e c0 a8 01 03 c0 a8
0020 01 04 08 00 4b 89 00 01 01 d2 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69
ghijklmn opqrstuv
wabcdefg hi
Bytes 6-8: IG bit (eth.src.ig)
Packets: 6859 · Displayed: 6164 (89.9%)
Profile: Default



Partie4:remotesniffing

```
mohamed@mohamed-VirtualBox:~/Desktop$ unzip -a WpdPack.zip
Archive:  WpdPack.zip
   creating: WpdPack/
   creating: WpdPack/docs/
   creating: WpdPack/docs/html/
  inflating: WpdPack/docs/html/annotated.html  [text]
  inflating: WpdPack/docs/html/classes.html  [text]
  inflating: WpdPack/docs/html/daemon_8h.html  [text]
  inflating: WpdPack/docs/html/daemon_8h_source.html  [text]
  inflating: WpdPack/docs/html/deprecated.html  [text]
  inflating: WpdPack/docs/html/doxygen.png  [binary]
  inflating: WpdPack/docs/html/doxygen__groups_8txt.html  [text]
  inflating: WpdPack/docs/html/dump.gif  [binary]
  inflating: WpdPack/docs/html/encoding.gif  [binary]
  inflating: WpdPack/docs/html/fileconf_8h.html  [text]
  inflating: WpdPack/docs/html/fileconf_8h_source.html  [text]
  inflating: WpdPack/docs/html/files.html  [text]
```

```
mohamed@mohamed-VirtualBox:~/Desktop$ cd WpdPack/wpcap/libpcap
bash: cd: WpdPack/wpcap/libpcap: No such file or directory
mohamed@mohamed-VirtualBox:~/Desktop$ cd WpdPack/wpcap/libpcap
bash: cd: WpdPack/wpcap/libpcap: No such file or directory
mohamed@mohamed-VirtualBox:~/Desktop$ unzip WpcapSrc.zip
Archive:  WpcapSrc.zip
   creating: winpcap/
  inflating: winpcap/build_wpdpack.bat
  inflating: winpcap/build_wpdpack.txt
   creating: winpcap/Common/
  inflating: winpcap/Common/dagc.h
```

```
mohamed@mohamed-VirtualBox:~/Desktop/winpcap/wpcap/libpcap$ chmod +x configure
runlex.sh
mohamed@mohamed-VirtualBox:~/Desktop/winpcap/wpcap/libpcap$ CFLAGS=/.,,,.';][=
> ^C
mohamed@mohamed-VirtualBox:~/Desktop/winpcap/wpcap/libpcap$ CFLAGS=-static ./co
nfigure
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking target system type... x86_64-unknown-linux-gnu
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking gcc version... 11
checking for inline... inline
checking for __attribute__... yes
checking for u_int8_t using gcc... yes
checking for u_int16_t using gcc... yes
checking for u_int32_t using gcc... yes
```

```
mohamed@mohamed-VirtualBox:~$ cd Desktop/winpcap/wpcap/libpcap
mohamed@mohamed-VirtualBox:~/Desktop/winpcap/wpcap/libpcap$ ./configure --help
`configure' configures this package to adapt to many kinds of systems.

Usage: ./configure [OPTION]... [VAR=VALUE]...

To assign environment variables (e.g., CC, CFLAGS...), specify them as
VAR=VALUE.  See below for descriptions of some of the useful variables.

Defaults for the options are specified in brackets.

Configuration:
  -h, --help              display this help and exit
      --help=short        display options specific to this package
      --help=recursive    display the short help of all the included packages
  -V, --version           display version information and exit
  -q, --quiet, --silent   do not print `checking...' messages
      --cache-file=FILE   cache test results in FILE [disabled]
  -C, --config-cache      alias for `--cache-file=config.cache'
  -n, --no-create         do not create output files
      --srcdir=DIR        find the sources in DIR [configure dir or `..']

Installation directories:
  --prefix=PREFIX         install architecture-independent files in PREFIX
                          [/usr/local]
```