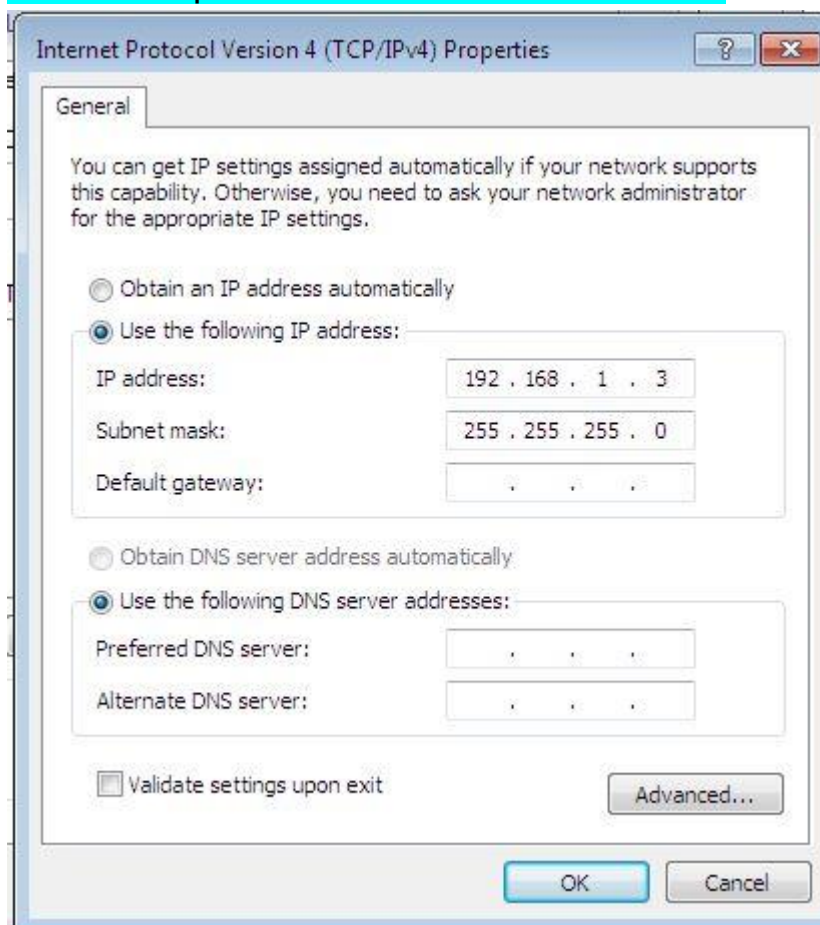
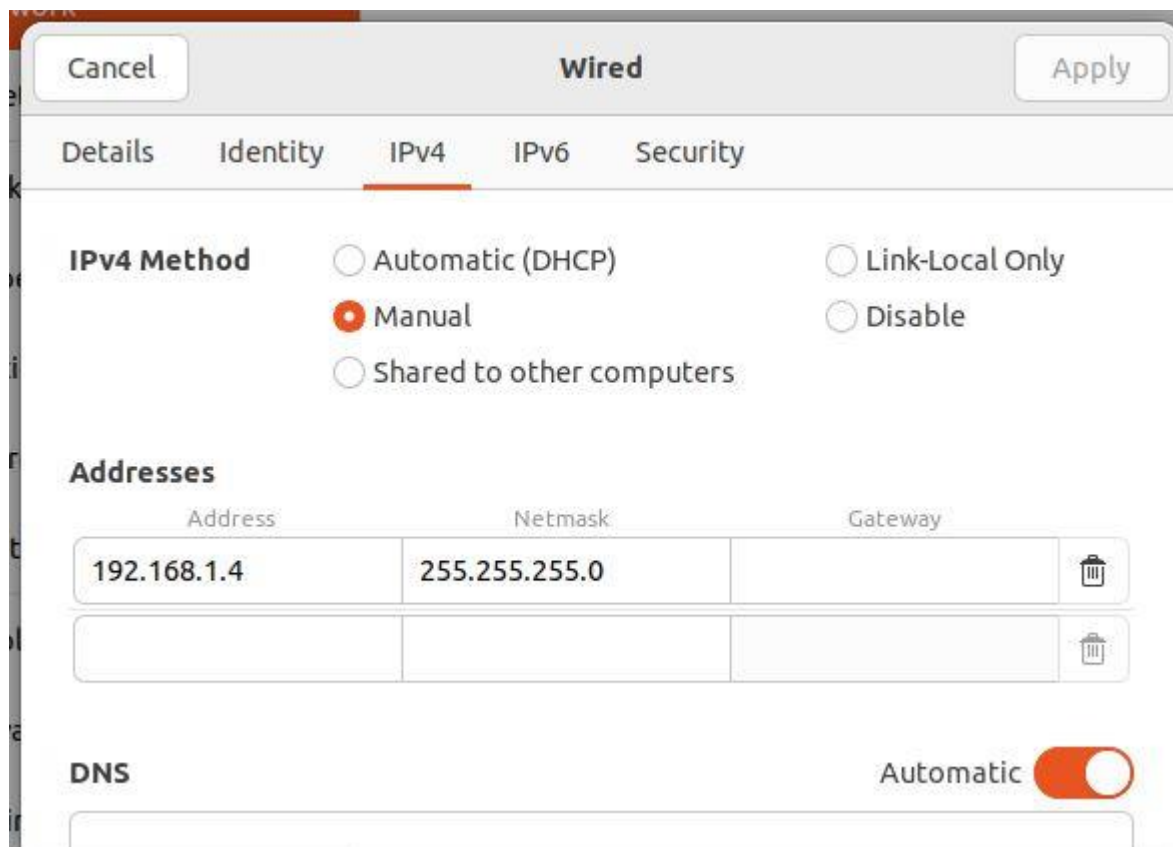


Base de
CYBERSECURITE TP1:
Attaques passives :sniffing passif

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

```

```

-----

```



```

1  int ParseUdpHeader(unsigned char *packet , int len)
2  {
3      struct ethhdr *ethernet_header;
4      struct iphdr *ip_header;
5      struct udphdr *udp_header;
6
7      /* Check if enough bytes are there for TCP Header */
8
9      if(len >= (sizeof(struct ethhdr) + sizeof(struct iphdr) +
10 sizeof(struct udphdr)))
11 {
12     /* Do all the checks: 1. Is it an IP pkt ? 2. is it TCP ? */
13
14     ethernet_header = (struct ethhdr *)packet;
15
16     if(ntohs(ethernet_header->h_proto) == ETH_P_IP)
17     {
18         ip_header = (struct iphdr *)(packet + sizeof(struct
19 ethhdr));
20
21         if(ip_header->protocol == IPPROTO_UDP)
22         {
23             printf("UDP datagram (UDP num=%d)\n",
24 ip_header->protocol);
25             udp_header = (struct udphdr*)(packet +
26 sizeof(struct ethhdr) + ip_header->ihl*4 );
27             udp_header = (struct udphdr*)(packet +
28 sizeof(struct ethhdr) + ip_header->ihl*4 );
29             /* Print the Dest and Src ports */
30
31             printf("Source Port: %d\n",
32 ntohs(udp_header->source));
33             printf("Dest Port: %d\n", ntohs(udp_header->
34 >dest));
35
36             }
37             else
38             {
39                 printf("Not a UDP packet\n");
40             }
41         }
42         else
43         {
44             printf("Not an IP packet\n");
45         }
46     }
47     else
48     {
49         printf("UDP Header not present \n");
50     }
51 }
52 }

```

Partie3:manipulation des niffers

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

Capturing from enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Interface Channel 802.11 Preferences

No.	Time	Source	Destination	Protocol	Length
5651	19503.138439...	192.168.1.4	192.168.1.3	ICMP	98
5652	19503.138718...	192.168.1.3	192.168.1.4	ICMP	98
5653	19504.162157...	192.168.1.4	192.168.1.3	ICMP	98
5654	19504.162461...	192.168.1.3	192.168.1.4	ICMP	98

Frame 1: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface enp0s3

- Ethernet II, Src: PcsCompu_0e:6e:b7 (08:00:27:0e:6e:b7), Dst: IPv6mcast_01:00:00:00:00:00
- Internet Protocol Version 6, Src: fe80::7c73:258e:349e:a1d, Dst: ff02::1:2
- User Datagram Protocol, Src Port: 546, Dst Port: 547
- DHCPv6

0000 33 33 00 01 00 02 08 00 27 0e 6e b7 86 dd 60 00 33 ' . n
0010 00 00 00 62 11 01 fe 80 00 00 00 00 00 00 7c 73 . . . b | s
0020 25 8e 34 9e 0a 1d ff 02 00 00 00 00 00 00 00 00 % 4
0030 00 00 00 01 00 02 02 22 02 23 00 62 01 9d 01 3f " . # . b . . ?
0040 1d 69 00 08 00 02 00 00 00 01 00 0e 00 01 00 01 . i
0050 2b 1f 49 5c 08 00 27 0e 6e b7 00 03 00 0c 0e 08 + . I \ . . ' . n
0060 00 27 00 00 00 00 00 00 00 00 00 00 00 00 0a . ' '

Bytes 102-105: T2 (dhcpv6.iaid.t2) Packets: 5654 · Displayed: 5654 (100.0%) Profile: Default

*enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.3 && ip.addr == 192.168.1.4

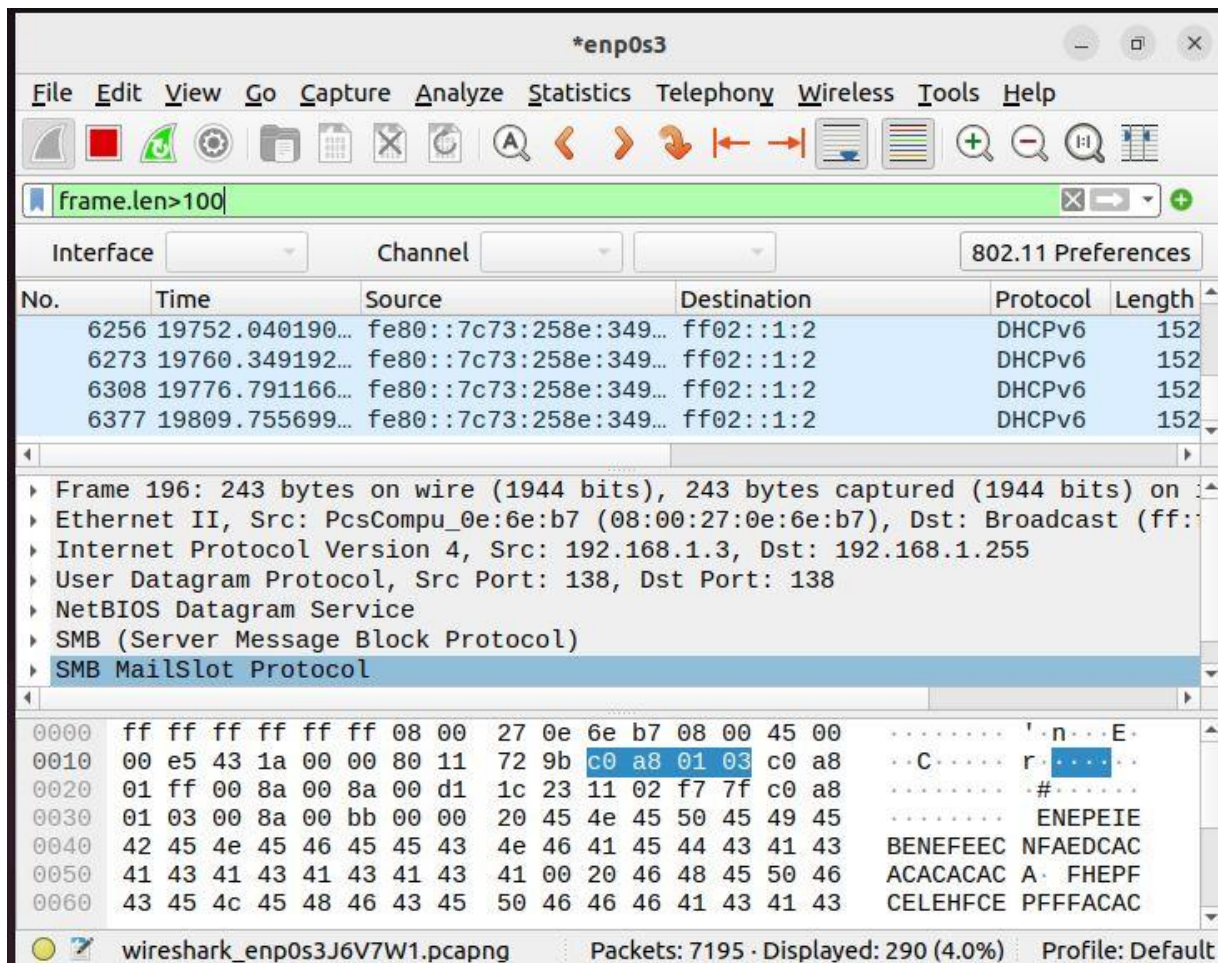
Interface Channel 802.11 Preferences

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 interface
 Ethernet II, Src: PcsCompu_0e:6e:b7 (08:00:27:0e:6e:b7), Dst: PcsCompu_a7:ae:c8
 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	..'....n...E..
0010	00 3c 43 1b 00 00 80 01 74 4e c0 a8 01 03 c0 a8	..<C...tN.....
0020	01 04 08 00 4b 89 00 01 01 d2 61 62 63 64 65 66	...K...abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcedfg 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]
```



```
(orig: 0) WpdPack C
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
checking for u_int64_t using gcc... yes
```

```

mohamed@moahmed-VirtualBox:~$ cd Desktop/wincap/wpcap/libpcap
mohamed@moahmed-VirtualBox:~/Desktop/wincap/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]

```

The image shows the Wireshark network traffic capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window displays a packet capture from the interface 'enp0s3' on IP '192.168.2.3'. The packet list shows several DHCPv6 packets and a BROWSER packet. The selected packet (No. 14723) is expanded in the packet details pane, showing the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, NetBIOS Datagram Service, SMB (Server Message Block Protocol), and SMB MailSlot Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII, with the ASCII column displaying the string 'BENEFEEC NFAEDCAC ACACACAC A FHEPF CELEHFCE PFFACAC'.

No.	Time	Source	Destination	Protocol	Length
14610	58975.675524...	fe80::7c73:258e:349...	ff02::1:2	DHCPv6	152
14643	58991.949493...	fe80::7c73:258e:349...	ff02::1:2	DHCPv6	152
14714	59024.450327...	fe80::7c73:258e:349...	ff02::1:2	DHCPv6	152
14723	59029.121731...	192.168.1.3	192.168.1.255	BROWSER	243

Frame 196: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on enp0s3

Ethernet II, Src: PcsCompu_0e:6e:b7 (08:00:27:0e:6e:b7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.255

User Datagram Protocol, Src Port: 138, Dst Port: 138

NetBIOS Datagram Service

SMB (Server Message Block Protocol)

SMB MailSlot Protocol

Offset	Hex	ASCII
0000	ff ff ff ff ff ff 08 00 27 0e 6e b7 08 00 45 00n...E..
0010	00 e5 43 1a 00 00 80 11 72 9b c0 a8 01 03 c0 a8	..C...r.....
0020	01 ff 00 8a 00 8a 00 d1 1c 23 11 02 f7 7f c0 a8#.....
0030	01 03 00 8a 00 bb 00 00 20 45 4e 45 50 45 49 45ENEPEIE
0040	42 45 4e 45 46 45 45 43 4e 46 41 45 44 43 41 43	BENEFEEC NFAEDCAC
0050	41 43 41 43 41 43 41 43 41 00 20 46 48 45 50 46	ACACACAC A FHEPF
0060	43 45 4c 45 48 46 43 45 50 46 46 46 41 43 41 43	CELEHFCE PFFACAC

":" was unexpected in this context. Packets: 14979 · Displayed: 369 (2.5%) Profile: Default