

Ethereal/Wireshark

un analyseur de protocoles réseau

Licence GFDL

Ce document est soumis à la Gnu Free Documentation Licence. C'est à dire que :

toute personne a le droit d'utiliser, diffuser et modifier ces documents

à condition d'indiquer la provenance du document original

à condition que les documents modifiés ou diffusés soient eux aussi soumis à la Gnu Free Documentation Licence et accessibles en ligne

j'apprécie d'avoir des retours sur les utilisations de ce document et/ou sur d'éventuelles erreurs/typo/màj/...

GFDL: <http://cesarx.free.fr/gfdlf.html>

wireshark: présentation

wireshark est un analyseur de trame.

outil libre en constante évolution

de nombreux greffons lui permettent de décoder
de nombreux protocoles

livré avec des outils en lignes de commande
permettant la capture de trame, la conversion
de formats, ...

wireshark: fonctionnalités

analyse de protocol réseau

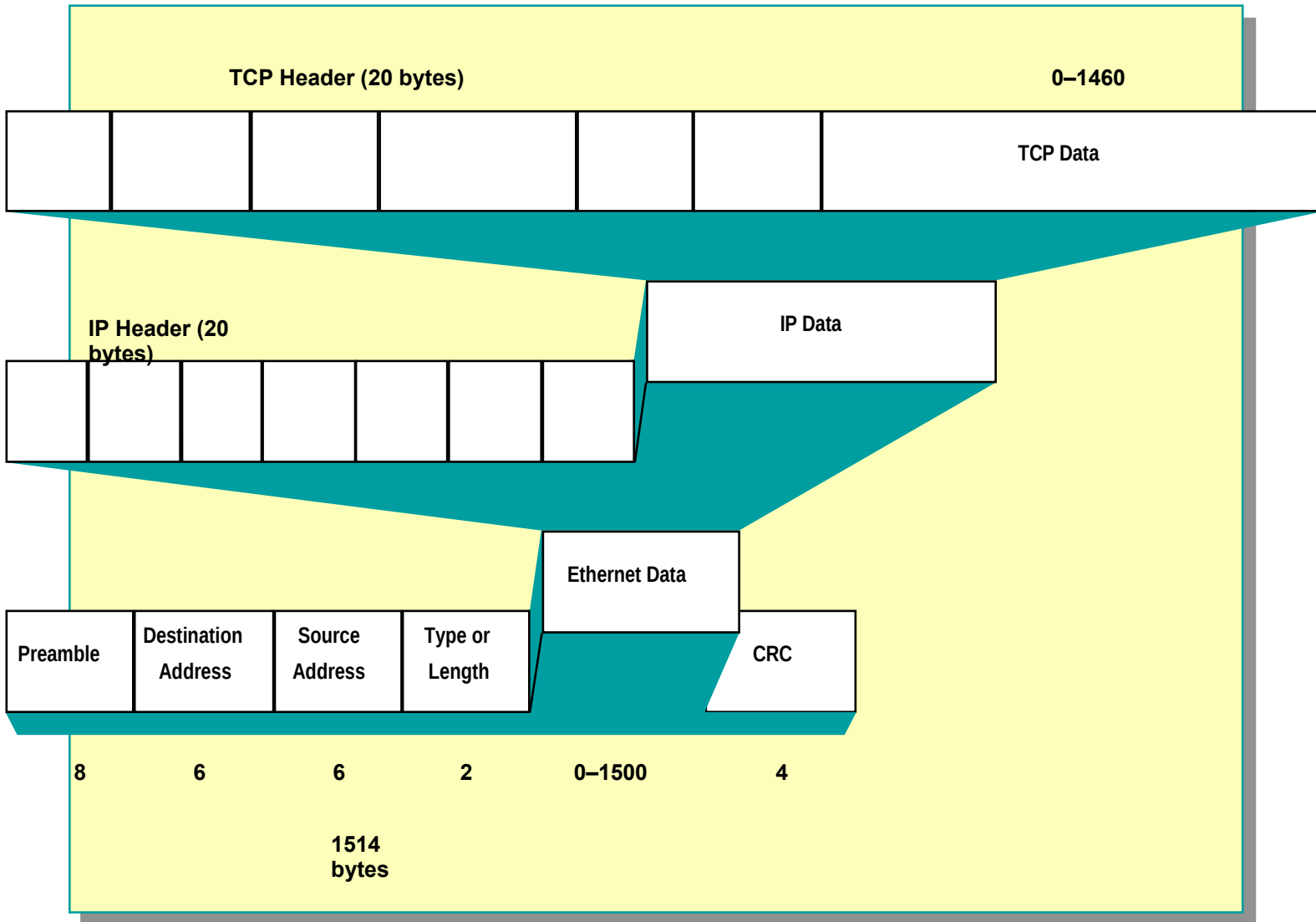
capture et analyse de trames

sauvegarde/lecture de capture précédemment
sauvegardées

décompose les différentes couches réseaux
présentes dans une trame

compatible avec les formats de sauvegardes de
nombreux logiciels

architecture en couche



wireshark: écran

Liste des trames

détail d'une trame

contenu hexa

The screenshot shows the Wireshark 1.8.2 interface with a capture file named 'dns-pp.cap'. The main pane displays a list of 13 network frames. The details pane for the first frame (No. 1) is expanded, showing the Ethernet II and Address Resolution Protocol (request) layers. The hex dump pane at the bottom shows the raw data of the first frame.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-------------------|-----------------|----------|--------|---|
| 1 | 0.000000 | Vmware_f1:80:77 | Broadcast | ARP | 60 | Who has 192.168.0.237? Tell 192.168.0.15 |
| 2 | 0.001942 | Vmware_82:49:ae | Vmware_f1:80:77 | ARP | 42 | 192.168.0.237 is at 00:0c:29:82:49:ae |
| 3 | 0.004443 | 192.168.0.15 | 192.168.0.237 | DNS | 71 | Standard query 0x3caa A ftp.lip6.fr |
| 4 | 0.010110 | Vmware_82:49:ae | Broadcast | ARP | 42 | Who has 192.168.0.254? Tell 192.168.0.237 |
| 5 | 0.015128 | FreeboxS 06:43:61 | Vmware_82:49:ae | ARP | 60 | 192.168.0.254 is at 00:07:cb:06:43:61 |
| 6 | 0.015461 | 192.168.0.237 | 192.33.4.12 | DNS | 71 | Standard query 0x2012 A ftp.lip6.fr |
| 7 | 0.157223 | 192.33.4.12 | 192.168.0.237 | DNS | 419 | Standard query response 0x2012 |
| 8 | 0.175277 | 192.168.0.237 | 192.93.0.1 | DNS | 71 | Standard query 0x2012 A ftp.lip6.fr |
| 9 | 0.223109 | 192.93.0.1 | 192.168.0.237 | DNS | 185 | Standard query response 0x2012 |
| 10 | 0.223424 | 192.168.0.237 | 132.227.60.30 | DNS | 71 | Standard query 0x2012 A ftp.lip6.fr |
| 11 | 0.282135 | 132.227.60.30 | 192.168.0.237 | DNS | 207 | Standard query response 0x2012 CNAME nephtys.lip6.fr A 195.83.118.1 |
| 12 | 0.283049 | 192.168.0.237 | 192.168.0.15 | DNS | 207 | Standard query response 0x3caa CNAME nephtys.lip6.fr A 195.83.118.1 |
| 13 | 0.329064 | 192.168.0.15 | 195.83.118.1 | ICMP | 74 | Echo (ping) request id=0x0200 seq=756/1 ttl=128 |

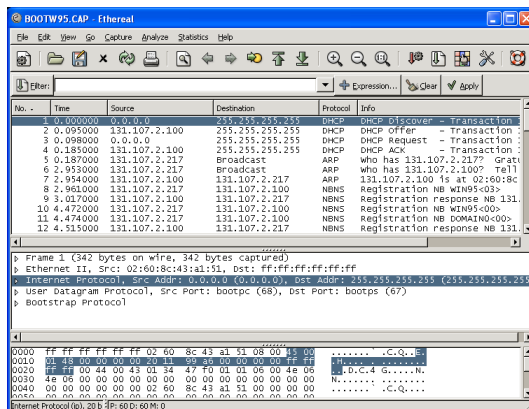
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
 Ethernet II, Src: Vmware_f1:80:77 (00:0c:29:f1:80:77), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (request)

```

0000 ff ff ff ff ff ff 00 0c 29 f1 80 77 08 06 00 01  ....w...
0010 08 00 06 04 00 01 00 0c 29 f1 80 77 c0 a8 00 0f  ....w...
0020 00 00 00 00 00 00 c0 a8 00 ed 64 fb 8c 21 50 14  ....d..!P.
0030 00 00 31 dc 00 00 51 2c b1 78 c0 a8  ....1..Q, .x..
  
```

File: "/home/petit/petit.old/Ensei... Packets: 111 Displayed: 111 Marked: 0 Load time: 0:00.088 Profile: Default

détail d'une trame



- ▾ Frame 1 (342 bytes on wire, 342 bytes captured)
 - Arrival Time: oct 2, 1996 08:21:08.705000000
 - Time delta from previous packet: 0.000000000 seconds
 - Time since reference or first frame: 0.000000000 seconds
 - Frame Number: 1
 - Packet Length: 342 bytes
 - Capture Length: 342 bytes
- ▾ Ethernet II, Src: 02:60:8c:43:a1:51, Dst: ff:ff:ff:ff:ff:ff
 - Destination: ff:ff:ff:ff:ff:ff (Broadcast)
 - Source: 02:60:8c:43:a1:51 (131.107.2.217)
 - Type: IP (0x0800)
- ▾ Internet Protocol, Src Addr: 0.0.0.0 (0.0.0.0), Dst Addr: 255.255.255.255
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 - Total Length: 328
 - Identification: 0x0000 (0)
 - Flags: 0x00
 - Fragment offset: 0
 - Time to live: 32
 - Protocol: UDP (0x11)
 - Header checksum: 0x99a6 (correct)
 - source: 0.0.0.0 (0.0.0.0)
 - destination: 255.255.255.255 (255.255.255.255)
- ▾ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
 - Source port: bootpc (68)
 - Destination port: bootps (67)
 - Length: 308

Ethereal: deux types de filtres

filtres à la capture:

- sélectionner les trames à capturer

- moins pratique et convivial que les filtres d'affichage

- réduit le nombre de trames à capturer

filtres d'affichage:

- langage simple, création avec un assistant

- sélectionner les trames à afficher

- colorier les trames affichées

Lancement d'une capture

The screenshot shows the 'Ethereal: Capture Options' dialog box. The 'Capture' section is highlighted with a blue arrow pointing to the 'Interface' dropdown menu, which is labeled 'interface réseau'. Another blue arrow points to the 'Capture Filter' text box, labeled 'Filtre à la capture'. The 'Capture File(s)' section is highlighted with a blue arrow pointing to the 'File' text box and the 'Browse...' button, labeled 'sauvegarde vers fichier'. The 'Stop Capture ...' section is highlighted with a blue arrow pointing to the '... after' dropdown menus, labeled 'conditions d'arrêt'. The 'Display Options' section is highlighted with a blue arrow pointing to the 'Update list of packets in real time' checkbox, labeled 'options d'affichage'. The 'Name Resolution' section is highlighted with a blue arrow pointing to the 'Enable MAC name resolution' checkbox, labeled 'résolution de nom'.

interface réseau

mode promiscuous

Filtre à la capture

sauvegarde vers fichier

conditions d'arrêt

options d'affichage

résolution de nom

Filtres à la capture

langage de filtre de libpcap, utilisable avec
tcpdump

forme générale d'un filtre à la capture :

[not] primitive [and|or] [not] primitive ...]

Exemple :

tcp port 23 and host 10.0.0.5

cf http://www.tcpdump.org/tcpdump_man.html
pour une descriptions complète

Filtres à la capture (2)

| | |
|---|---|
| [src dst] host <host> | sélection des paquets selon l'adresse ip source (src) ou destination (dst) ou les deux si on ne précise pas src ou dst. « |
| ether [src dst] host <ehost> | idem selon l'adresse ethernet source ou destination |
| gateway host <host> | paquet utilisant <i>host</i> comme routeur: routeur est source ou destination au niveau ethernet mais pas IP. |
| [src dst] net <net> [{mask <mask>}]{len <len>}} | sélection des paquets ayant un sous-réseau comme source ou destination. le masque peut être indiqué explicitement ou en notation CIDR |
| [tcp udp] [src dst] port <port> | sélection de paquets selon le port source/destination et le protocole tcp/udp |
| less greater <length> | filtrage sur la taille du paquet: « inférieur ou égaux » ou « supérieur ou égaux » |
| ip ether proto <protocol> | sélection du protocole soit de la couche IP soit de la couche ethernet |

Filtres à l'affichage

langage de filtre différent de celui des filtres à la capture: &&, ||, (,) et des expressions

sert à la sélection des trames affichés et à la colorisation des trames

dépend des routines de décodage de chaque protocole

=> évolue beaucoup d'une version à l'autre

guide de référence du filtre d'affichage:

<http://www.ethereal.com/docs/dfref/>

ne pas oublier de cliquer sur « Apply » pour appliquer le filtre courant

Filtres à l'affichage (2)

The screenshot illustrates the process of creating a display filter in Wireshark. The main window shows a list of captured packets. A blue arrow points from the 'Expression...' dropdown in the filter bar to the 'Ethereal: Filter Expression' dialog box. In this dialog, the 'Field name' list includes 'tcp.dstport - Destination Port', which is selected. The 'Relation' is set to 'is present', and the 'Value' is '22'. The 'Predefined values' section is empty. The 'Range (offset:length)' field is also empty. The 'OK' and 'Cancel' buttons are at the bottom.

Below the dialog, the main window's filter bar is updated to show the filter: `tcp.dstport == 22`. The packet list below the filter shows only two packets:

| No. | Time | Source | Destination | Protocol | Info |
|-----|----------|-----------------|-----------------|----------|---|
| 1 | 0.000000 | 212.27.42.65 | 192.168.244.151 | TCP | 65535 → 1108 [RST] Seq=3392288088 Win=0 Len=0 |
| 2 | 0.000434 | 192.168.244.151 | 212.27.42.65 | TCP | 1108 → 65535 [RST] Seq=3392288088 Win=0 Len=0 |

Filtres à l'affichage (3)

dns-pp.cap [Wireshark 1.8.2]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter:

| No. | Time | Source | Len | Info |
|-----|----------|-------------------|----------------------|--------------------------------|
| 1 | 0.000000 | Vmware_f1:80:77 | 60 | Who has 192.168.0.237? Tell 1 |
| 2 | 0.001942 | Vmware_82:49:ae | 42 | 192.168.0.237 is at 00:0c:29:8 |
| 3 | 0.004443 | 192.168.0.15 | Selected | 0x3caa A ftp.l |
| 4 | 0.010110 | Vmware_82:49:ae | Not Selected | 3.0.254? Tell 1 |
| 5 | 0.015128 | FreeboxS_06:43:61 | ... and Selected | is at 00:07:cb:0 |
| 6 | 0.015461 | 192.168.0.237 | ... or Selected | 0x2012 A ftp.l |
| 7 | 0.157223 | 192.33.4.12 | ... and not Selected | response 0x2012 |
| 8 | 0.175277 | 192.168.0.237 | ... or not Selected | 0x2012 A ftp.l |
| 9 | 0.223109 | 192.93.0.1 | 71 | Standard query 0x2012 A ftp.l |
| 10 | 0.223424 | 192.168.0.237 | 207 | Standard query response 0x2012 |
| 11 | 0.282135 | 132.227.60.30 | 207 | Standard query response 0x3caa |
| 12 | 0.283049 | 192.168.0.237 | 74 | Echo (ping) request id=0x0200 |
| 13 | 0.329064 | 192.168.0.15 | | |

Version: 4
Header length: 20 bytes
⊕ Differentiated Services Field: 0x00
Total Length: 57
Identification: 0x00f8 (248)
⊕ Flags: 0x00
Fragment offset: 0
Time to live: 128
Protocol: UDP (17)
⊕ Header checksum: 0xb3f9 [correct]
Source: 192.168.0.237 (192.168.0.237)
Destination: 192.33.4.12 (192.33.4.12)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
⊕ User Datagram Protocol, Src Port: 1028 (1028), Dst Port: domain (53)
⊖ Domain Name System (query)

Filtres à l'affichage (4)

- il est possible de sélectionner les paquets ayant le même critère qu'un paquet existant grâce au menu contextuel
- cf diapo précédente

Exercices

charger « bootw95.cap » situé dans
captures_base

sélectionner les trames tcp

sélectionner les trames dhcp (voir Bootp/Dhcp)

les trames dont l'adresse ip destination est
255.255.255.255

coloriage et divers

coloriage: colorier les trames vérifiant certains filtres

couleur de la trame = celle du premier filtre auquel correspond elle correspond

via « View/coloring rules »

« set time reference » (menu edit): l'horodatage des trames suivants se fait en référence à cette trame

« Edit/mark Packet »: marquer la trame pour la repérer

Statistiques: protocol hierarchy

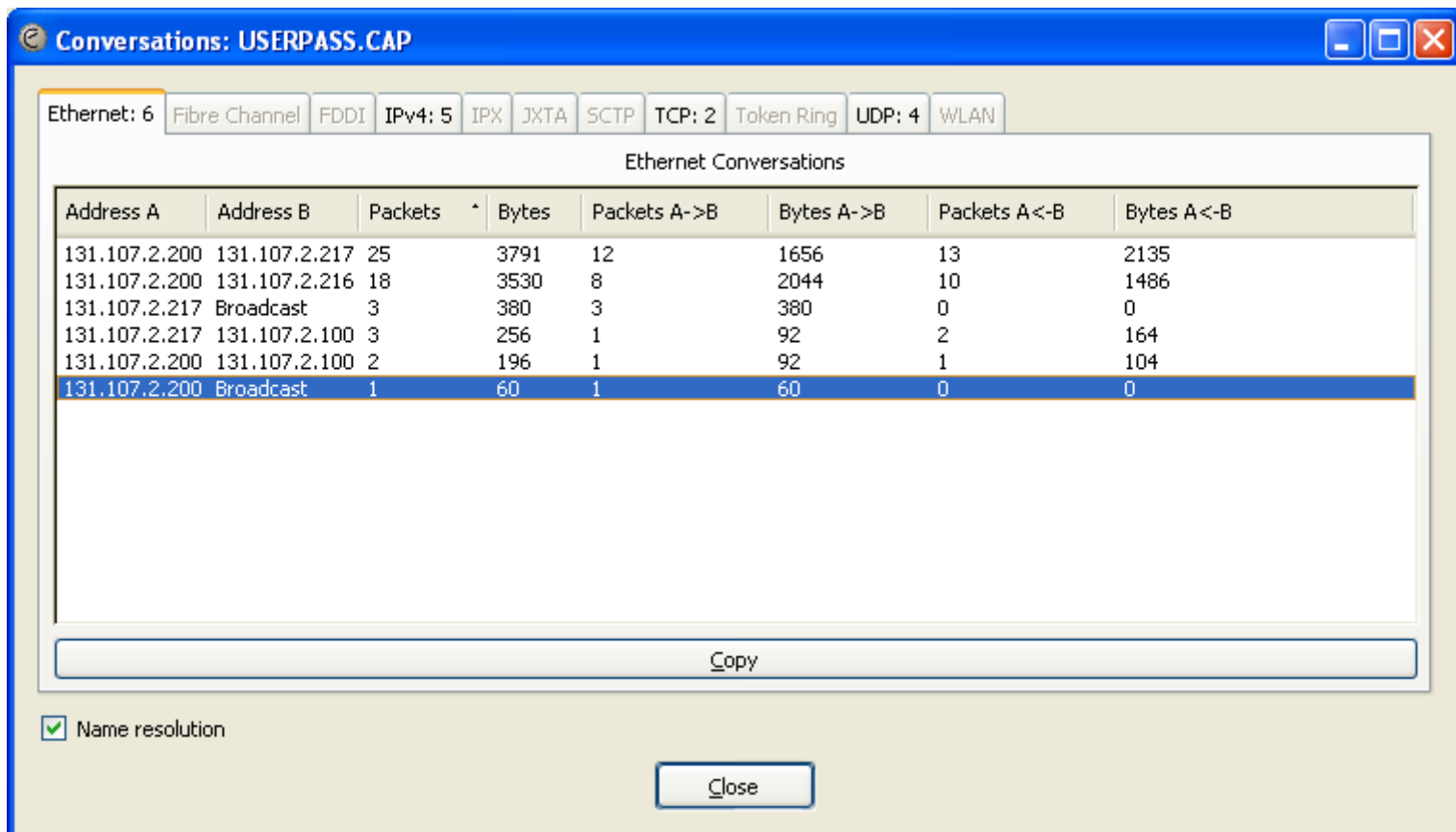
« protocol hierarchy »: nombre de trames, débit, ... présenté hiérarchiquement selon le modèle en couche

| Protocol | % Packets | Packets | Bytes | Mbit/s | End Packets | End Bytes | End Mbit/s |
|--|-----------|---------|-------|--------|-------------|-----------|------------|
| Frame | 100,00% | 52 | 8213 | 0,002 | 0 | 0 | 0,000 |
| Ethernet | 100,00% | 52 | 8213 | 0,002 | 0 | 0 | 0,000 |
| Address Resolution Protocol | 11,54% | 6 | 360 | 0,000 | 6 | 360 | 0,000 |
| Internet Protocol | 88,46% | 46 | 7853 | 0,001 | 0 | 0 | 0,000 |
| User Datagram Protocol | 11,54% | 6 | 1044 | 0,000 | 0 | 0 | 0,000 |
| NetBIOS Name Service | 7,69% | 4 | 392 | 0,000 | 4 | 392 | 0,000 |
| NetBIOS Datagram Service | 3,85% | 2 | 652 | 0,000 | 0 | 0 | 0,000 |
| SMB (Server Message Block Protocol) | 3,85% | 2 | 652 | 0,000 | 0 | 0 | 0,000 |
| SMB MailSlot Protocol | 3,85% | 2 | 652 | 0,000 | 0 | 0 | 0,000 |
| Microsoft Windows Browser Protocol | 1,92% | 1 | 260 | 0,000 | 1 | 260 | 0,000 |
| Microsoft Windows Logon Protocol (Old) | 1,92% | 1 | 392 | 0,000 | 1 | 392 | 0,000 |
| Transmission Control Protocol | 76,92% | 40 | 6809 | 0,001 | 12 | 720 | 0,000 |
| NetBIOS Session Service | 53,85% | 28 | 6089 | 0,001 | 4 | 372 | 0,000 |
| SMB (Server Message Block Protocol) | 46,15% | 24 | 5717 | 0,001 | 14 | 2357 | 0,000 |
| SMB Pipe Protocol | 19,23% | 10 | 3360 | 0,001 | 0 | 0 | 0,000 |
| Microsoft Windows Lanman Remote API Protocol | 11,54% | 6 | 1852 | 0,000 | 6 | 1852 | 0,000 |
| DCE RPC | 7,69% | 4 | 1508 | 0,000 | 2 | 396 | 0,000 |
| Microsoft Network Logon | 3,85% | 2 | 1112 | 0,000 | 2 | 1112 | 0,000 |

Statistiques: conversations

qui cause à qui: résumés par couche

chaque onglet peut s'obtenir séparément via
« conversation lists »



The screenshot shows a window titled "Conversations: USERPASS.CAP" with a blue title bar. Below the title bar, there are several tabs: "Ethernet: 6", "Fibre Channel", "FDDI", "IPv4: 5", "IPX", "JXTA", "SCTP", "TCP: 2", "Token Ring", "UDP: 4", and "WLAN". The "Ethernet: 6" tab is selected, and the window displays "Ethernet Conversations".

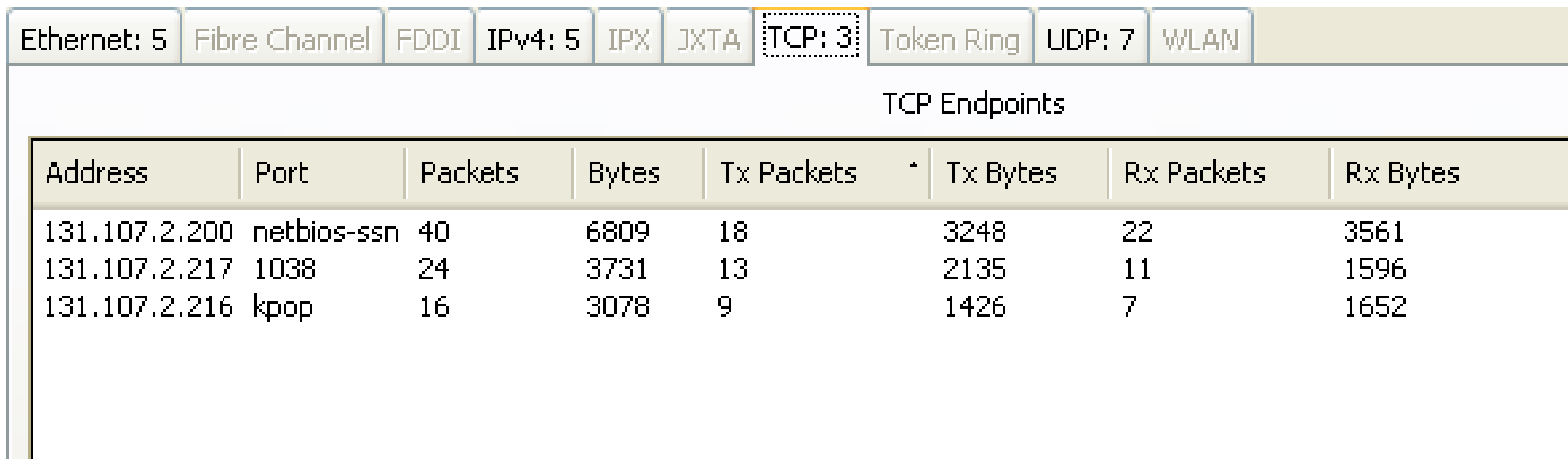
| Address A | Address B | Packets | Bytes | Packets A->B | Bytes A->B | Packets A<-B | Bytes A<-B |
|---------------|---------------|---------|-------|--------------|------------|--------------|------------|
| 131.107.2.200 | 131.107.2.217 | 25 | 3791 | 12 | 1656 | 13 | 2135 |
| 131.107.2.200 | 131.107.2.216 | 18 | 3530 | 8 | 2044 | 10 | 1486 |
| 131.107.2.217 | Broadcast | 3 | 380 | 3 | 380 | 0 | 0 |
| 131.107.2.217 | 131.107.2.100 | 3 | 256 | 1 | 92 | 2 | 164 |
| 131.107.2.200 | 131.107.2.100 | 2 | 196 | 1 | 92 | 1 | 104 |
| 131.107.2.200 | Broadcast | 1 | 60 | 1 | 60 | 0 | 0 |

Below the table, there is a "Copy" button. At the bottom left, there is a checked checkbox labeled "Name resolution". At the bottom center, there is a "Close" button.

Statistiques: EndPoints

indique les destinations des divers traffic. La notion dépend de la couche considérée: adresse MAC pour ethernet, adresse IP pour IP, adresse IP+port pour tcp ou udp, ...

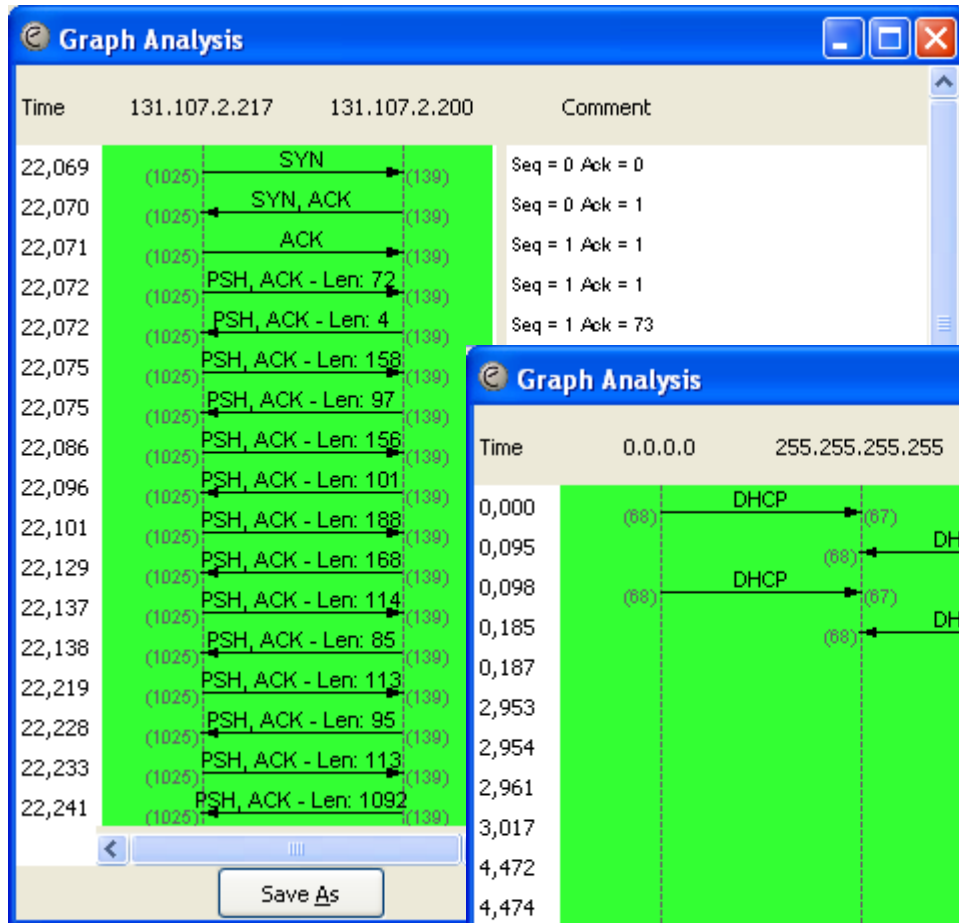
chaque onglet peut s'obtenir séparément via « EndPoints lists »



The screenshot shows a network monitoring interface with a tabbed menu at the top. The tabs include: Ethernet: 5, Fibre Channel, FDDI, IPv4: 5, IPX, JXTA, TCP: 3 (highlighted with a dashed border), Token Ring, UDP: 7, and WLAN. Below the tabs, the title 'TCP Endpoints' is centered. A table displays the following data:

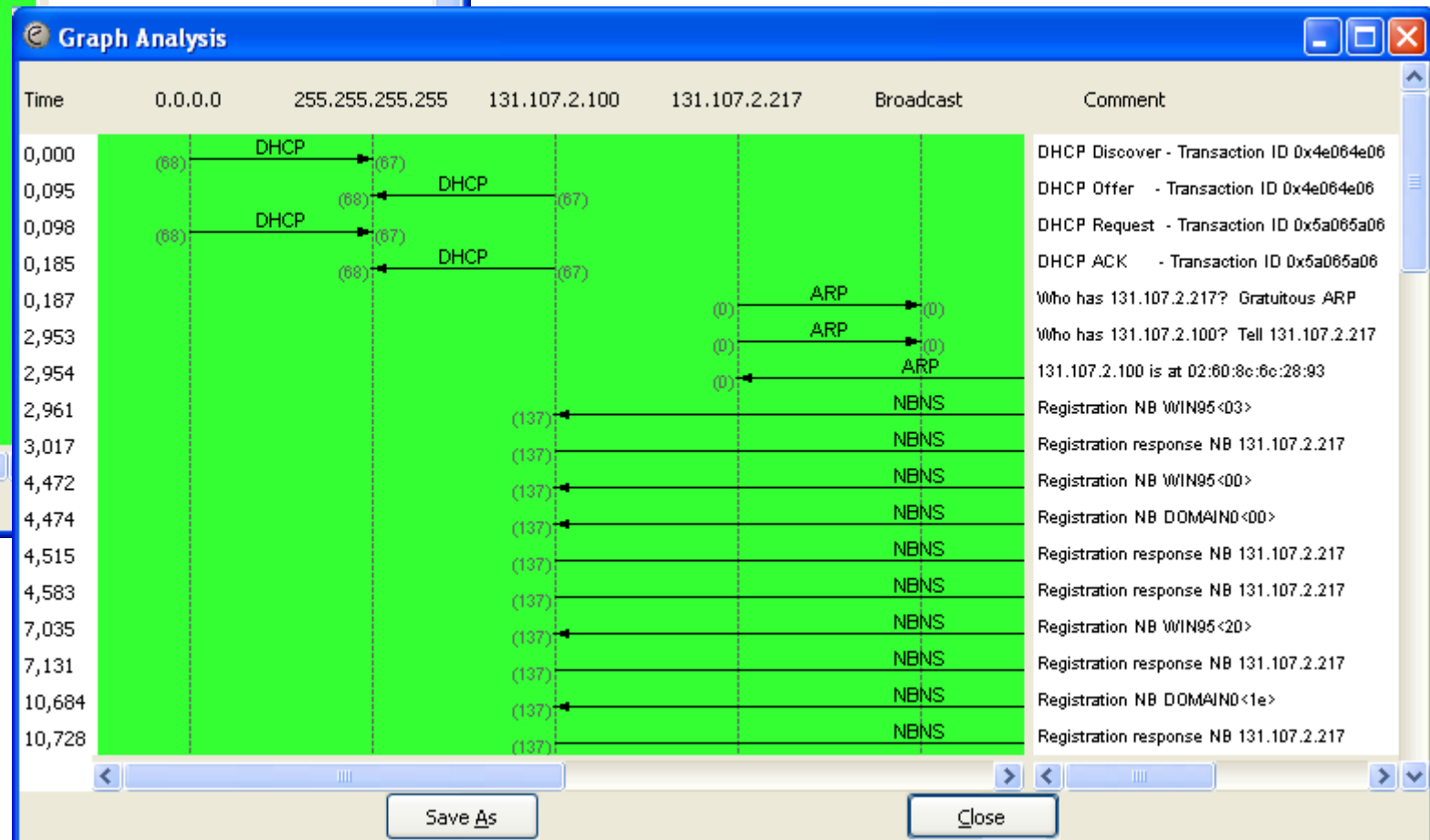
| Address | Port | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes |
|---------------|-------------|---------|-------|------------|----------|------------|----------|
| 131.107.2.200 | netbios-ssn | 40 | 6809 | 18 | 3248 | 22 | 3561 |
| 131.107.2.217 | 1038 | 24 | 3731 | 13 | 2135 | 11 | 1596 |
| 131.107.2.216 | kpop | 16 | 3078 | 9 | 1426 | 7 | 1652 |

Statistiques: diagramme de flot



TCP

Tout le trafic



Ethereal: performances

perte de trames: ethereal n'arrive plus à suivre

Solutions possibles

- désactiver l'affichage en temps réel des trames

- désactiver les filtres à la capture si la quantité capturée est grande

- activer les filtres à la capture si seule une faible part des trames est utile

- arrêter les autres programmes (antivirus, daemon chargés, ...)

- utiliser un outil dédié à la capture (tethereal, tcpdump, ...) puis analyser le fichier sauvé avec ethereal