

## Ethereal

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>

## Ethereal: présentation

- ethereal est un analyseur de trame.
- outil libre en constante évolution
- de nombreux greffons lui permettent de décoder de nombreux protocoles
- livré avec les outils suivants :
  - tethereal: ~ d'ethereal en ligne de commande
  - mergecap: fusionne des fichiers de capture
  - editcap: conversion/modification en ligne de commande de fichier de capture
  - text2pcap: convertit un dump hexa en fichier pcap

## Ethereal: 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
- tethereal: outil de capture en mode texte

## •architecture en couche

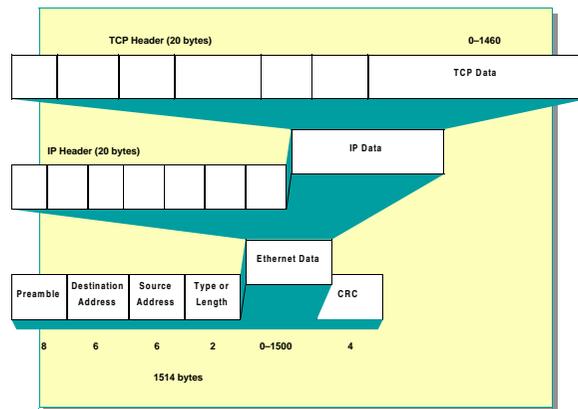


schéma: M. Besson

## Ethereal: écran

The screenshot shows the Ethereal network protocol analyzer interface. It displays a list of captured frames, a detailed view of a selected frame, and the corresponding hex dump.

**Liste des trames:** A table showing the list of captured frames with columns for No., Time, Source, Destination, Protocol, and Info.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction
2	0.095000	131.107.2.100	255.255.255.255	DHCP	DHCP Offer - Transaction
3	0.098000	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction
4	0.189000	131.107.2.100	255.255.255.255	DHCP	DHCP ACK - Transaction
5	0.187000	131.107.2.217	Broadcast	ARP	who has 131.107.2.217? grat
6	2.953000	131.107.2.217	Broadcast	ARP	who has 131.107.2.100? Te11
7	2.954000	131.107.2.100	131.107.2.217	ARP	131.107.2.100 is at 02:60:8c
8	2.961000	131.107.2.217	131.107.2.100	NENS	Registration NB WIN95-03s
9	3.017000	131.107.2.100	131.107.2.217	NENS	Registration response NB 131.
10	4.472000	131.107.2.217	131.107.2.100	NENS	Registration NB WIN95-00s
11	4.474000	131.107.2.217	131.107.2.100	NENS	Registration NB DOMAIN-00s
12	4.515000	131.107.2.100	131.107.2.217	NENS	Registration response NB 131.

**détail d'une trame:** A detailed view of a selected frame, showing the frame structure and the corresponding hex dump.

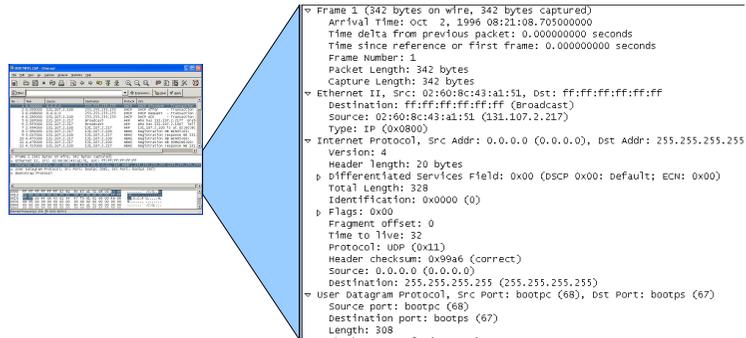
**contenu hexa:** The hex dump of the selected frame, showing the raw data in hexadecimal and ASCII.

Dans la fenêtre « détail d'une trame », on retrouve une section par couche:

- physique
- ethernet
- IP
- UDP
- dhcp

Lorsque l'on sélectionne une section, la zone correspondante est mise en évidence dans la fenêtre HEXA.

## détail d'une trame

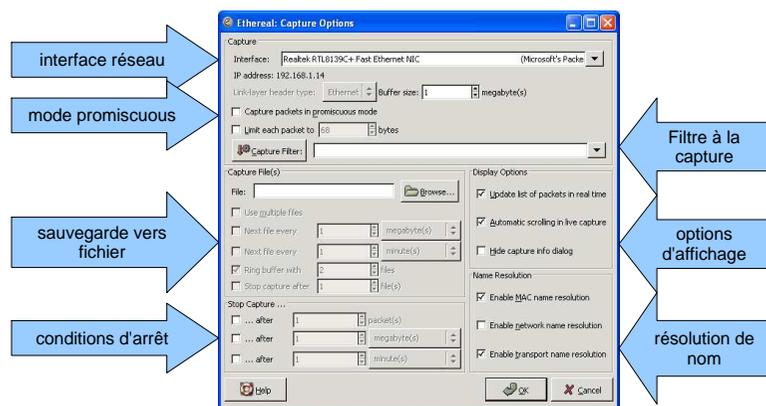


En dépliant une section donnée, on peut consulter son contenu qui est lui-même composé de sections qui peuvent elles-mêmes être déployées.

## 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



## 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](http://www.tcpdump.org/tcpdump_man.html) pour une descriptions complète

## Politique suggérée concernant les filtres à la capture :

- Il peut être utile d'utiliser des filtres à la capture pour limiter la quantité de trafic récupéré. Dans ce cas, en général, des filtres simples suffisent
- La compatibilité du langage de filtre avec celui d'outil usuels sous unix comme tcpdump permet de factoriser l'effort d'apprentissage et justifie que l'on sache faire des filtres minimaux
- il ne faut cependant pas perdre de vue que si l'on élimine trop de trames, elles seront définitivement perdues. c'est la raison pour laquelle l'affinage doit se faire avec les filtres à l'affichage (qui ont en plus l'avantage d'être plus faciles d'accès grâce à l'assistant).

## 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 host 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 égal » ou « supérieur ou égal »
ip ether proto <protocol>	sélection du protocole soit de la couche IP soit de la couche ethernet
ether ip broadcast multicast	sélection des paquets diffusés ou multidiffusés de la couche IP ou ethernet.

Exemples: ràf

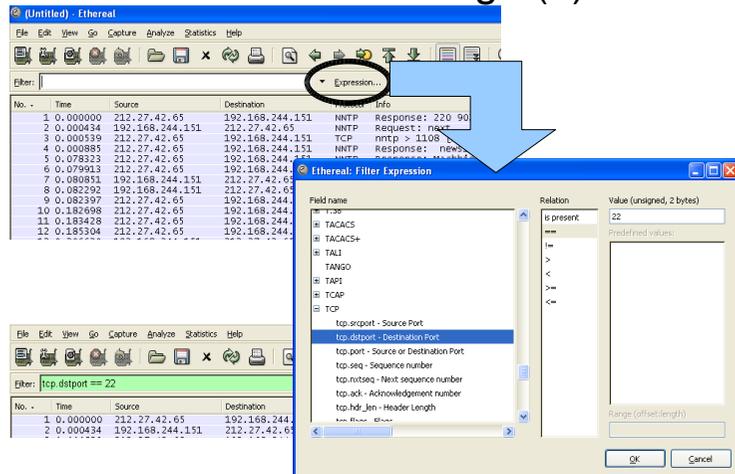
## Filtres à l'affichage

- 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

Politique suggérée concernant les filtres à la capture :

- Il peut être utile d'utiliser des filtres à la capture pour limiter la quantité de trafic récupéré. Dans ce cas, en général, des filtres simples suffisent
- La compatibilité du langage de filtre avec celui d'outil usuels sous unix comme tcpdump permet de factoriser l'effort d'apprentissage et justifie que l'on sache faire des filtres minimaux
- il ne faut cependant pas perdre de vue que si l'on élimine trop de trames, elles seront définitivement perdues. c'est la raison pour laquelle l'affinage doit se faire avec les filtres à l'affichage (qui ont en plus l'avantage d'être plus faciles d'accès grâce à l'assistant).

## Filtres à l'affichage (2)



le bouton « Expression » permet d'ajouter une expression à un filtre via un assistant. Lorsque la syntaxe du filtre est bonne, le fond est vert (comme sur le bas de la diapo). Quand le fond est rouge, c'est que le filtre n'est pas bon. L'utilisation des filtres suppose de comprendre finement ce que l'on fait et a des effets de bord non voulus.

Exemple:

- filtrer sur adresses ip et port suppose d'aller dans IP (adresse) et dans tcp/udp pour le port.
- ne garder que les trames ip de/vers une machine élimine les trames arp qui sont pourtant partie intégrantes du dialogue.

## 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

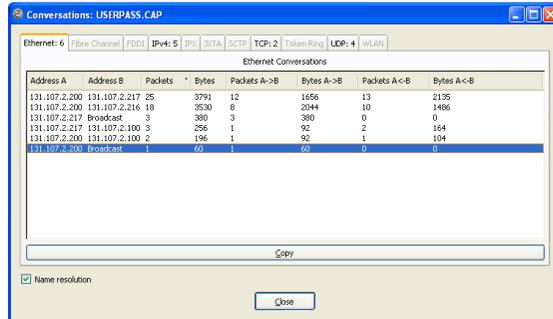
## Statistiques: protocol hierarchy

- « 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 »



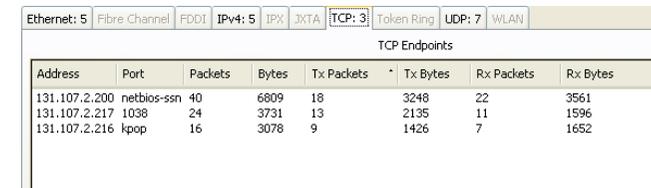
The screenshot shows a window titled 'Conversations: USERPASS.CAP'. It has several tabs: Ethernet: 6, Fibre Channel, FDDI, IPv4: 5, IPX, X25A, TCP: 2, Token Ring, UDP: 4, and WLAN. The 'Ethernet: 6' tab is selected. Below the tabs is a table titled 'Ethernet Conversations' with the following columns: Address A, Address B, Packets, Bytes, Packets A->B, Bytes A->B, Packets A<-B, and Bytes A<-B. The table contains the following data:

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	1655	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

At the bottom of the window, there is a 'Copy' button and a checkbox for 'Name resolution' which is checked. A 'Close' button is also present.

## Statistiques: EndPoints

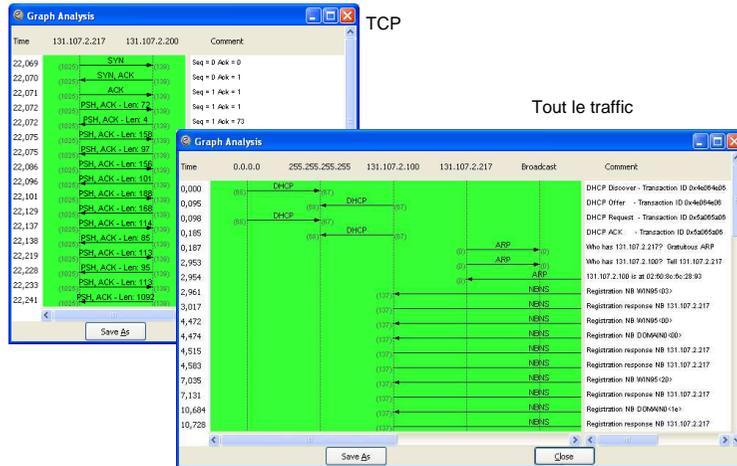
- indique les destinations des divers traffic. La notion dépend de la couche considérée: adresse MAC pour ethernet, adresse IP pour IP, adresse IP+port pour tcp ou udp, ...
- chaque onglet peut s'obtenir séparément via « EndPoints lists »



The screenshot shows a window titled 'TCP Endpoints'. It has several tabs: Ethernet: 5, Fibre Channel, FDDI, IPv4: 5, IPX, X25A, TCP: 3, Token Ring, UDP: 7, and WLAN. The 'TCP: 3' tab is selected. Below the tabs is a table titled 'TCP Endpoints' with the following columns: Address, Port, Packets, Bytes, Tx Packets, Tx Bytes, Rx Packets, and Rx Bytes. The table contains 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



## 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 seul 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