

1

Ethereal

un analyseur de protocoles réseau

2

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/...

3

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
 - merg pcap: fusionne des fichiers de capture
 - editcap: conversion/modification en ligne de commande de fichier de capture
 - text2pcap: convertit un dump hexa en fichier pcap

4

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

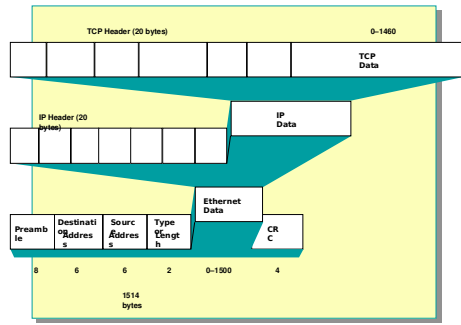


schéma: M. Besson

Ethereal: écran

The screenshot shows the Wireshark interface with three main sections: a list of frames, a detailed view of a selected frame, and the raw hex data. Three blue arrows point from the text labels to these sections.

- Liste des trames:** Points to the packet list pane showing a table of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info.
- détail d'une trame:** Points to the packet details pane showing the hierarchical structure of the selected packet (Ethernet II, Internet Protocol Version 4, Hypertext Transfer Protocol).
- contenu hexa:** Points to the packet bytes pane showing the raw hexadecimal and ASCII data of the selected packet.

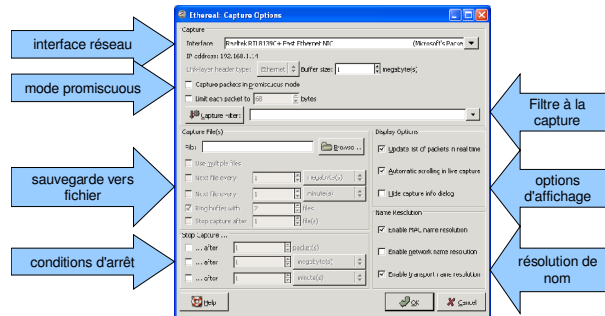
détail d'une trame

The screenshot shows the detailed view of a selected frame in Wireshark. The tree view on the left shows the protocol hierarchy: Ethernet II, Internet Protocol, and Hypertext Transfer Protocol. The right pane shows the specific details for each protocol, such as source and destination addresses, flags, and content length.

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 (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
length > <length>	filtrage sur la taille du paquet: « inférieur ou égal » ou « supérieur ou égal »
p[ether proto <protocol>	sélection du protocole soit de la couche IP soit de la couche ethernet

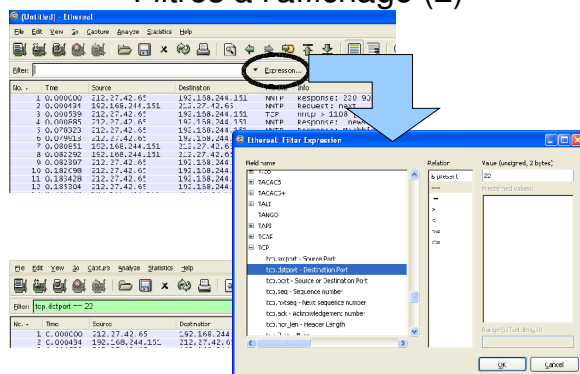
Filtres à la capture

- 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 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

Filtres à l'affichage (2)



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 suyvants se fait en référence à cette trame
- « Edit/mark Packet »: marquer la trame pour la repérer

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
-

Statistiques: protocol hierarchy

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

Protocol	% Packets	Packets	Bytes	Mbits	End Packets	End Bytes	End Mbits
Frame	100.00%	52	8213	0.002	0	0	0.000
Internet	100.00%	52	8213	0.002	0	0	0.000
Address Resolution Protocol	11.54%	6	1960	0.000	6	308	0.001
Internet Protocol	88.46%	46	6253	0.001	0	0	0.000
User Datagram Protocol	11.54%	6	1044	0.000	0	0	0.000
Network Name Service	7.69%	4	292	0.000	4	392	0.000
Network Discovery Service	3.85%	2	652	0.000	0	0	0.000
Simple Message Block Protocol	3.85%	2	652	0.000	0	0	0.000
Simple Mailbox Protocol	3.85%	2	652	0.000	0	0	0.000
Microsoft Windows Stream Protocol	1.92%	1	550	0.000	1	260	0.000
Microsoft Windows Logon Protocol (OLD)	1.92%	1	292	0.000	1	392	0.000
Transmission Control Protocol	7.69%	4	609	0.001	12	720	0.000
Network Session Service	63.85%	34	6299	0.001	4	372	0.000
Simple Message Block Protocol	6.15%	3	6117	0.001	14	1057	0.000
Simple File Protocol	19.23%	10	3560	0.001	0	0	0.000
Microsoft Windows Lanman Remote API Protocol	11.54%	6	1052	0.000	6	852	0.000
DC:RPC	7.69%	4	1538	0.000	2	396	0.000
Microsoft Network Logon	3.85%	2	1112	0.000	2	112	0.000

Statistiques: conversations

- qui cause à qui: résumés par couche
- chaque onglet peut s'obtenir séparément via « conversation lists »

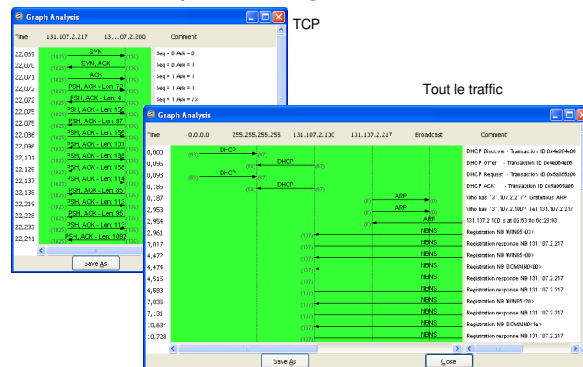
Adresse A	Adresse B	Packets	Bytes	Packets A->B	Bytes A->B	Packets B->A	Bytes B->A
131.107.2.200	131.107.2.217	25	14	10	235	15	1465
131.107.2.200	131.107.2.216	13	308	0	204	13	1465
131.107.2.217	BroadCast	3	360	3	360	0	0
131.107.2.217	131.107.2.200	3	16	2	84	1	164
131.107.2.200	131.107.2.200	2	106	1	92	1	104

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 »

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	krpp	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