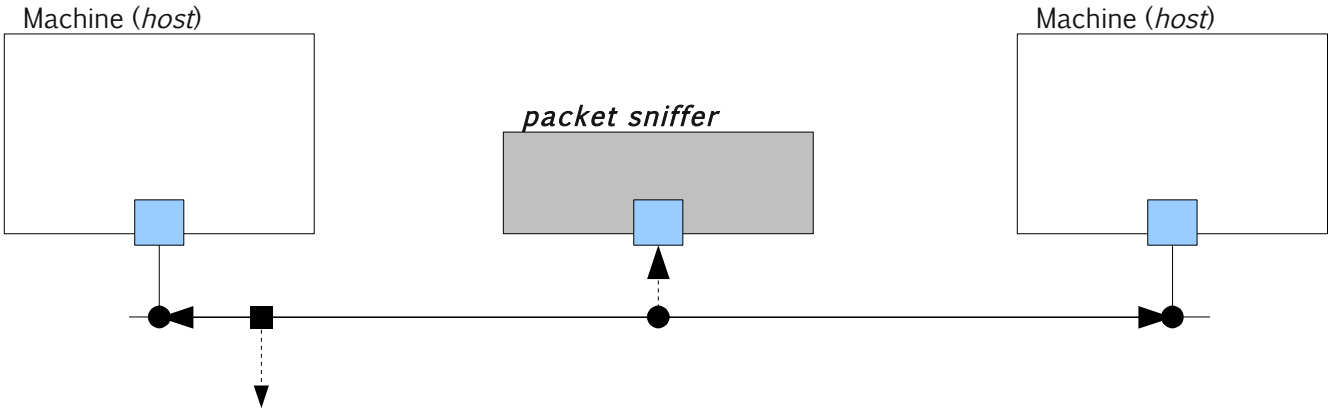
Wireshark

Wireshark (anciennement Ethereal) est un logiciel libre d'**analyse de protocole**, ou « **packet sniffer** », utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie, mais aussi le piratage. Wireshark est multi-plates-formes, il fonctionne sous Windows, Mac OS X, Linux, Solaris, ainsi que sous FreeBSD. Wireshark reconnait actuellement 759 protocoles.

Wireshark dispose d'une interface graphique (GUI – *Graphic User Interface*).

tcpdump

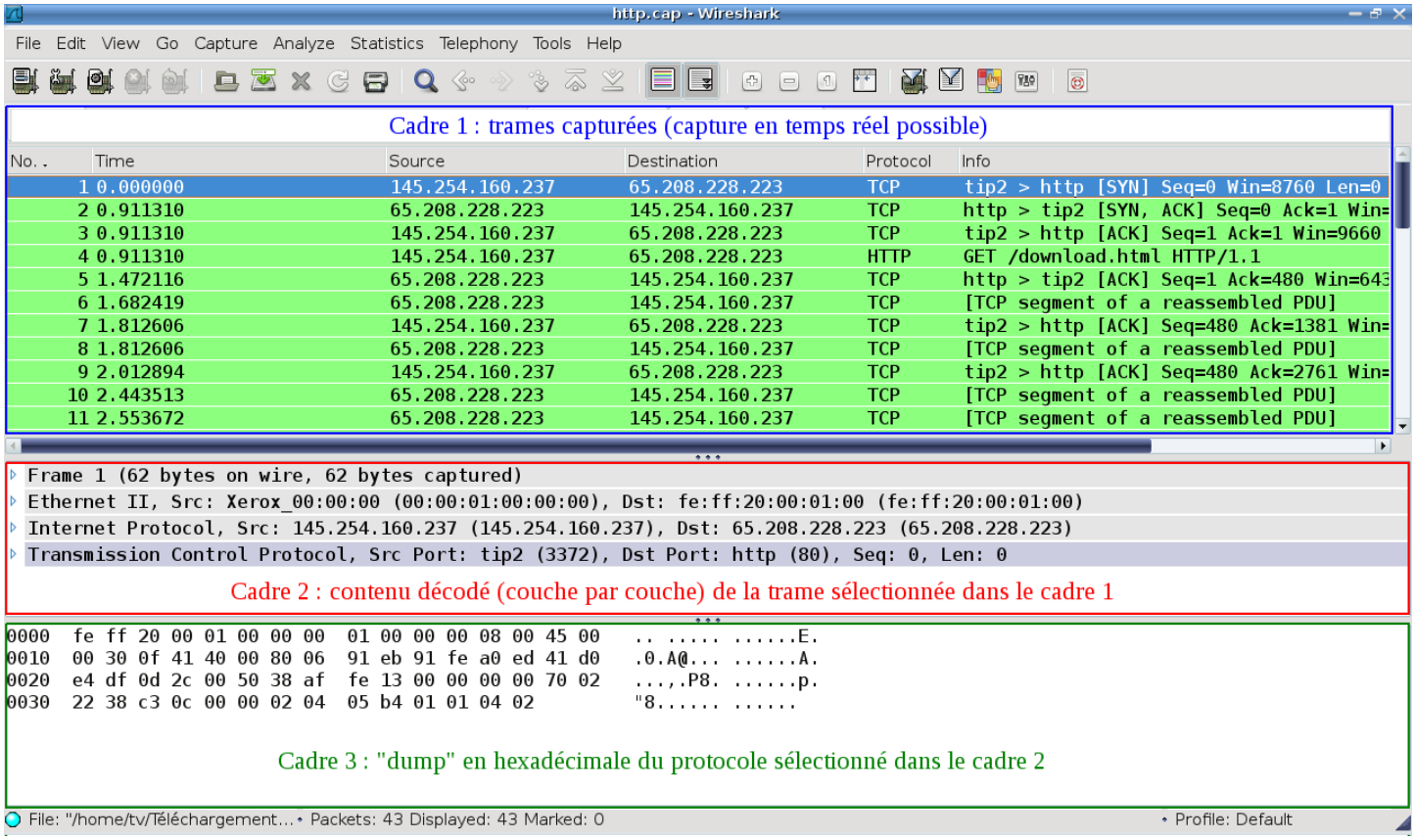
tcpdump est un « ***packet sniffer*** » en ligne de commande. Il permet d'obtenir le détail du trafic visible depuis une interface réseau. C'est un outil de mise au point apprécié pour sa puissance.



Les **trames** échangées sur le réseau physique seront **capturées** par la machine équipée d'un logiciel du type « ***packet sniffer*** ».

Principe

L'affichage dans Wireshark se décompose en trois cadres :



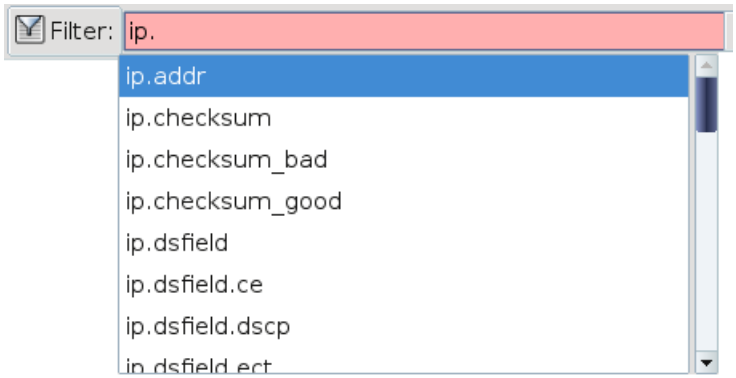
Filtrage

Il est possible (indispensable !) de créer des filtres d'affichage qui ne montrent que les trames conformes à la règle de filtrage. Cela permettra d'isoler un échange en particulier ou l'analyse d'un protocole spécifique.
On renseignera alors le cadre **Filter** dans la barre du haut du cadre 1 :

On peut créer des règles de filtrage en combinant plusieurs expressions avec des opérateurs && (ET), || (OU) et ! (INVERSEUR).

Par exemple, toutes les trames dont l'adresse ip destination est égale à 145.254.160.237 et dont le port source ou destination n'est pas 80 : ip.dst == 145.254.160.237 && !tcp.port == 80

*Remarque : en tapant directement dans la zone de saisie « **Filter** », Wireshark propose une complétion bien pratique.*



Encapsulation

Le cadre 2 illustre le principe de l'encapsulation des protocoles utilisées dans l'échange d'une trame. On fait souvent référence à un modèle pour représenter cette communication.