Wireshark - tcpdump / Удаленный рабочий снифферер

Задача:

* Мониторинг трафика на удаленной машине.

Требования:

* На удаленной машине, ssh-доступ и пакет tcpdump.
* На локальной машине, wireshark и ssh-клиент.

Процесс:

* Передача информации от удаленного узла производится при помощи стандартных stdout/stdin pipe'ов на локальную машину при помощи запуска через ssh на удалённой машине tcpdump и передачи его трафика локальному wireshark:

$ ssh user@host tcpdump -lni eth0 -s0 -w- http | wireshark -i-

PS - опцию -l в команде вызова tcpdump, которая указывает, чтобы он использовал live-режим вывода в stdout.

http://crimea-karro.blogspot.ru/2015/07/wireshark-tcpdump.html