TP 3: Wireshark

1. Lisez la description de Wireshark (à voir: le PDF joint).
2. Pour capturer le trafic dans le réseau avec Wireshark il vous faut d'avoir des droits d'administrateur. Alors, cela va marcher bien sur vos ordis personnels, mais je ne suis pas certaine de réussir de faire marcher ceci sur les ordis à l'université.
3. Essayez d'installer Wireshark sur vos ordis.
4. Lisez la description dans le pdf joint. L'interface de Wireshark a beaucoup changé pendant le temps écoulé depuis lors que la description dans le pdf joint a été écrite. Par contre, la description de l'interface graphique (à voir les volets) n'a pas trop changé.
5. On va maintenant s'occuper de la Tâche 1. Comme c'est difficile à installer Wireshark sans avoir permission d'admin, on va faire cela sur papier pour l'instant et je vais mettre en-ligne les fichiers pour vous donner l'opportunité de tester Wireshark chez vous également.
   Dans la figure 1 vous trouverez la capture de Wireshark sur un protocole de ping. Régardez en particulier les paquets 51, 53, 54, 55, et puis 63, 65, 66, 68, 69 et 71. Quel protocole a été utilisé ?
   En utilisant vos connaissances et l'internet donnez quelques indications sur le protocole utilisé : son rôle, ses spécifications, etc. Quel est le format d'une requête ping ?
6. En utilisant les informations dans les Figures 2 et 3, répondez aux questions suivantes : (a) quel est l'envoyeur de la requête ping ? (b) quel est le destinataire ? (c) est-ce que vous pouvez retrouver le format standard du protocole (que vous avez donné dans la question précédente) dans le message ?
7. Continuez regarder les informations données dans la figure 4. Notez les détails que vous reconnaissez. Notez les adresses de la source et de la destination dans le volet Ethernet II, puis les mêmes infos dans le volet Internet Protocol version 4. Pourquoi est-ce que les deux sont différentes ? Il y a une ligne en bas – dans le volet avec le contenu du message – qui est marqué en bleu. Cette ligne corresponde à la partie sélectionnée en haut : Ethernet II. Quelles sont les informations données dans la ligne en bleu ?
8. Voilà l'effet de faire le ping sur mon ordinateur :

   ```
   PING printer (192.168.0.14) 56(84) bytes of data.
   64 bytes from printer (192.168.0.14): icmp_seq=1 ttl=255 time=13.4 ms
   64 bytes from printer (192.168.0.14): icmp_seq=2 ttl=255 time=6.36 ms
   64 bytes from printer (192.168.0.14): icmp_seq=3 ttl=255 time=5.48 ms
   64 bytes from printer (192.168.0.14): icmp_seq=4 ttl=255 time=7.04 ms
   64 bytes from printer (192.168.0.14): icmp_seq=5 ttl=255 time=6.29 ms
   64 bytes from printer (192.168.0.14): icmp_seq=6 ttl=255 time=5.41 ms
   64 bytes from printer (192.168.0.14): icmp_seq=7 ttl=255 time=6.63 ms
   64 bytes from printer (192.168.0.14): icmp_seq=8 ttl=255 time=5.90 ms
   64 bytes from printer (192.168.0.14): icmp_seq=9 ttl=255 time=4.43 ms
   ```

   Faites le lien entre ces messages-ci et la liste de paquets dans la Figure 1.

9. On continue avec la tâche 2 dans le fichier pdf : capturer une connexion ftp. En faisant cela j'ai le prochain résultat.

```
$ ftp ftp.gnu.org
Connected to ftp.gnu.org.
220 GNU FTP server ready.
Name (ftp.gnu.org:vegard): cristina
530 This FTP server is anonymous only.
Login failed.
ftp> 221 Goodbye.

$ ftp ftp.gnu.org
Connected to ftp.gnu.org.
220 GNU FTP server ready.
Name (ftp.gnu.org:vegard): anonymous
230-Due to U.S. Export Regulations, all cryptographic software on this
230-site is subject to the following legal notice:
230-
230-    This site includes publicly available encryption source code
230-    which, together with object code resulting from the compiling of
230-    publicly available source code, may be exported from the United
230-    States under License Exception "TSU" pursuant to 15 C.F.R. Section
230-    740.13(e).
230-
230-This legal notice applies to cryptographic software only. Please see
230-the Bureau of Industry and Security (www.bxa.doc.gov) for more
230-information about current U.S. regulations.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
lrwxrwxrwx    1 0        0               8 Aug 20  2004 CRYPTO.README
-> .message
-rw-r--r--    1 0        0           17864 Oct 23  2003 MISSING-FILES
-rw-r--r--    2 0        0            4178 Aug 13  2003 MISSING-FILES.README
-rw-r--r--    1 0        0            1962 Nov 15  2012 README
-rw-r--r--    1 0        0          405121 Oct 23  2003
before-2003-08-01.md5sums.asc
-rw-r--r--    1 0        0          198738 Nov 09 11:25 find.txt.gz
drwxrwxr-x  305 0        3003        12288 Sep 06 13:30 gnu
drwxrwxr-x    3 0        3003        4096 Mar 10  2011 gnu+linux-distros
-rw-r--r--    1 0        0          384444 Nov 09 11:25 ls-lrRt.txt.gz
drwxr-xr-x    3 0        0           4096 Apr 20  2005 mirrors
lrwxrwxrwx    1 0        0             11 Apr 15  2004 non-gnu -> gnu/non-gnu
drwxr-xr-x   88 0        0           4096 May 30  2013 old-gnu
lrwxrwxrwx    1 0        0              1 Aug 05  2003 pub -> .
drwxr-xr-x    2 0        0           4096 Nov 08  2007 savannah
drwxr-xr-x    2 0        0           4096 Aug 02  2003 third-party
drwxr-xr-x    2 0        0           4096 Apr 07  2009 tmp
drwxr-xr-x    2 0        0           4096 May 07  2013 video
-rw-r--r--    1 0        0            954 Aug 13  2003 welcome.msg
226 Directory send OK.
ftp> cd tmp
250 Directory successfully changed.
```

```
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> get README
local: README remote: README
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for README (1962 bytes).
226 Transfer complete.
1962 bytes received in 0.00 secs (7018.4 kB/s)
ftp> 221 Goodbye.
```

Essayez de comprendre ce qui s'est passé.

10. Regardez la Fig. 5. À quelle partie du log dans l'exercice précèdent correspondent les paquets 16 – 39 ? C'est quoi, un DNS ? Quel est le rôle de la partie capturée entre les paquets 16 et 22 ?
11. Regardez la Fig. 6. À quelle partie du log dans l'exercice 9 correspondent les paquets 45 – 75 ? Quels sont les caractéristiques du protocole FTP ?
12. Les paquets 74 – 76 sont affichés plus en détail dans les Fig. 7 – 9. Notez les détails les plus signifiants dans ces figures. Reconnaissez-vous le texte marqué en bleu dans le volet en bas dans la figure 8 ?
13. Regardez les paquets 183 – 192 (Fig. 10). Reconnaissez-vous le paquet dont les détails sont affiches en bas ? Maintenant regardez la Fig. 11. Est-ce que le fichier a été bien transféré ? Comment est-ce que vous pouvez savoir cela ?