Flex

Zadanie polega na stworzeniu **skanera do analizy logów w formacie tcpdump** (tcpdump manual).

Skaner po wczytaniu logu ma wypisywać informację o połączeniach z/na port 80 w formacie: godzina, adres hosta źródłowego, port, adres hosta docelowego, port, liczba ewentualnie przesłanych bajtów danych; czyli dla wejścia:

```
13:14:26.356390 IP (tos 0x8,...) 149.156.99.9.22 > 149.156.99.182.1128: . [tcp sum ok]...
13:14:26.356651 IP (tos 0x0,...) 149.156.99.182.1128 > 149.156.99.9.22: P [tcp sum ok]...
13:13:34.874424 IP (tos 0x0,...) 217.74.65.55.80 > 149.156.99.182.1096: S [tcp sum ok]...
13:13:34.874821 IP (tos 0x0,...) 149.156.99.182.1096 > 217.74.65.55.80: . [tcp sum ok]...
13:13:34.892791 IP (tos 0x0,...) 149.156.99.182.1096 > 217.74.65.55.80: P 1:685(684)...
13:13:35.278346 arp who-has 149.156.99.89 tell 149.156.99.51
13:13:35.976915 IP (tos 0x0,...) 130.203.133.50.80 > 149.156.99.182.1118: S [tcp sum ok]...
13:13:40.849502 IP (tos 0x0,...) 149.156.99.182.1096 > 217.74.65.55.80: P 1:685(684)...
13:13:41.977473 IP (tos 0x0,...) 130.203.133.50.80 > 149.156.99.182.1118: S [tcp sum ok]...
13:13:45.393437 IP (tos 0x0,...) 217.74.64.234.80 > 149.156.99.182.1100: F [tcp sum ok]...
13:13:45.393901 IP (tos 0x0,...) 149.156.99.182.1100 > 217.74.64.234.80: . [tcp sum ok]...
13:13:46.493062 IP (tos 0x0,...) 149.156.99.182 > 216.239.59.104: icmp 72: echo request
13:13:46.493598 IP (tos 0xc0,...) 149.156.99.17 > 149.156.99.182: icmp 120: time exceeded
```

ma dawać na wyjściu:

```
13:13:34 from 217.74.65.55:80 to 149.156.99.182:1096
13:13:34 from 149.156.99.182:1096 to 217.74.65.55:80
13:13:34 from 149.156.99.182:1096 to 217.74.65.55:80 684 bytes
13:13:35 from 130.203.133.50:80 to 149.156.99.182:1118
13:13:40 from 149.156.99.182:1096 to 217.74.65.55:80 684 bytes
13:13:41 from 130.203.133.50:80 to 149.156.99.182:1118
13:13:45 from 217.74.64.234:80 to 149.156.99.182:1100
13:13:45 from 149.156.99.182:1100 to 217.74.64.234:80
```

Linie w nieprawidłowym formacie powinny być pominięte.

W zadaniu należy wykorzystać generator skanerów flex (flex manual)

Przyładowy log tcpdump: tcpdump-log

Inne materiały

monitoring with tcpdump
tools: tcpdump
Lex - A Lexical Analyzer Generator, M. E. Lesk