

Flex

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

Skaner po wczytaniu prawidłowego logu ma wypisywać informację o godzinie, adresie hostów między którymi przesyłane są pakiety oraz o liczbie ewentualnie przesłanych danych, czyli dla wejścia:

```
11:57:13.923781 IP 149.156.99.111.1791 > 66.102.9.99.80: P 1560712269:1560712573(304)...
11:57:13.980726 IP 66.102.9.99.80 > 149.156.99.111.1791: . ack 304 win 7886
11:57:13.981908 IP 66.102.9.99.80 > 149.156.99.111.1791: . ack 304 win 6432
11:57:13.986793 IP 66.102.9.99.80 > 149.156.99.111.1791: P 1431:1636(205) ack 304 win...
11:57:13.987073 IP 149.156.99.111.1791 > 66.102.9.99.80: . ack 1 win 65535
```

ma dawać na wyjściu:

```
11:57:13 from 149.156.99.111 to 66.102.9.99 304 bytes
11:57:13 from 66.102.9.99 to 149.156.99.111
11:57:13 from 66.102.9.99 to 149.156.99.111
11:57:13 from 66.102.9.99 to 149.156.99.111 205 bytes
11:57:13 from 149.156.99.111 to 66.102.9.99
```

Proszę obsłużyć sytuację, gdy wejście nie jest w formacie tcpdump (np. pominięcie niepoprawnej linii i/lub komunikat o błędzie).

W zadaniu należy wykorzystać generator skanerów flex ([flex manual](#))

Przykładowy log tcpdump: [test-log](#)

Inne materiały

[monitoring with tcpdump](#)

[tools: tcpdump](#)

[Lex - A Lexical Analyzer Generator, M. E. Lesk](#)