트래픽 환경 및 기본 특징:

cat conn.log | zeek-cut proto id.resp_p | sort | uniq -c | sort -nr | head -n 10

```
(venv) knu@h20:~/pcap_data/0730$ cat conn.log | zeek-cut proto id.resp_p | sort | uniq -c | sort -nr | head -n 10
 277293 tcp     443
     12 udp     443
```

요청 목적지 (Target URL) 분포:

cat ssl.log | zeek-cut server_name | sort | uniq -c | sort -nr | head -n 10

```
(venv) knu@h20:~/pcap_data/0730$ cat ssl.log | zeek-cut server_name | sort | uniq -c | sort -nr | head -n 10
  77139 cdn.muni.cz
  68324 www.muni.cz
   8668 www.econ.muni.cz
   8461 www.fss.muni.cz
   5188 poradna.fss.muni.cz
   4649 www.ics.muni.cz
   4643 it.muni.cz
   4433 webcentrum.muni.cz
   4086 www.recetox.muni.cz
   3286 www.skm.muni.cz
```

시간대별 활동 패턴 분석: [09] => 9시, [18] => 오후 6시로 계산.

cat conn.log | zeek-cut ts | awk '{print strftime("%H", $1)}' | sort | uniq -c | sort -nr

```
[00]    18816 ******************
[01]    21270 ********************
[02]    17878 ******************
[03]    18657 ******************
[04]    17653 ******************
[05]    17354 ******************
[06]    14925 **************
[07]    13645 *************
[08]    12058 ************
[18]    20802 ********************
[19]    21626 ********************
[20]    22167 *********************
[21]    20304 ********************
[22]    20248 ********************
[23]    19902 ********************
```

비정상 연결 상태 분석:

cat conn.log | zeek-cut conn_state | grep -v 'SF' | sort | uniq -c | sort -nr

```
(venv) knu@h20:~/pcap_data/0730$ cat conn.log | zeek-cut conn_state | grep -v 'SF' | sort | uniq -c | sort -nr
 100536 RSTR
  26802 RSTO
  17777 OTH
   7292 SH
   1530 S1
    563 RSTRH
    377 SHR
    267 S0
     29 S2
     28 REJ
      5 S3
```

데이터 전송량 및 크기 분석: (단위/정보는 사진 참고)

cat conn.log | zeek-cut id.resp_h orig_bytes resp_bytes ts | awk 'NR>1 {print $1, $2, $3, $4, $2 + $3}' | sort -k5 -nr | head -n 10

```
Total Size   Resp_IP    Client Tx (Orig)   Server Tx (Resp) TS (Timestamp)
-------------------------------------------------------------------------
3.81GB       10.0.0.1   3.81GB             0B               1627653851.089745
2.34GB       10.0.0.1   2.34GB             0B               1627653846.070743
1.69GB       10.0.0.2   467B               1.69GB           1627651622.105732
1.62GB       10.0.0.1   1.62GB             0B               1627653843.870425
1.07GB       10.0.0.1   1.07GB             17.51KB          1627661571.571735
910.61MB     10.0.0.1   910.61MB           0B               1627653844.309924
74.96MB      10.0.0.1   23.70KB            74.94MB          1627648448.258095
51.58MB      10.0.0.1   132.05KB           51.46MB          1627668028.143438
51.30MB      10.0.0.1   3.65KB             51.30MB          1627643131.093694
50.53MB      10.0.0.4   1.27KB
```

서버 응답 크기:

cat conn.log | zeek-cut resp_bytes | awk 'NR>1 {print int($1 / 1024 / 1024) "MB"}' | sort | uniq -c | sort -nr | head -n 10

평균 연결 지속 시간:

cat conn.log | zeek-cut duration | awk '
NR>1 {sum += $1; count++}
END {print "평균 연결 지속 시간:", sum/count, "초"}'

```
(venv) knu@h20:~/pcap_data/0730$ cat conn.log | zeek-cut duration | awk '
NR>1 {sum += $1; count++}
END {print "평균 연결 지속 시간:", sum/count, "초"}'
평균 연결 지속 시간: 18.4145 초
```

(나머지 정보는 위의 이미지 데이터 참고 바람.)
1. 트래픽 환경 및 기본 특징

- **주요 프로토콜**: 전체 27만 7천 건 중 99.9%가 TCP 443 포트 사용 (HTTPS 암호화 트래픽), 소량의 UDP 443 연결(12건)도 확인됨
- **주요 접속 대상**: muni.cz 도메인 계열이 주된 목적지
  - cdn.muni.cz: 77,139건 (CDN 서버)
  - www.muni.cz: 68,324건 (메인 웹사이트)

2. 시간대별 활동 패턴

- **피크 시간대**: 20시(22,167건), 19시(21,626건)에 최고치 기록
- **활동 집중 시간**: 00~08시, 18~23시의 야간/새벽 시간대에 집중
- **특징**: 자동화된 작업(스크립트, 백업)이거나 시차가 있는 타 지역 사용량일 가능성 높음

3. 연결 상태 및 실패율

- **비정상 연결 다수 발생**
  - RSTR (클라이언트 측 강제 종료): 100,536건
  - RSTO (서버 측 강제 종료/타임아웃): 26,802건
- **원인 추정**: 클라이언트 요청 중단, 서버 과부하로 인한 응답 지연 및 타임아웃
- **평균 연결 지속 시간**: 18.4초로 비교적 긴 편

4. 데이터 전송 부하 분석 (Top 10)

- **전송량 규모**: 910MB~3.81GB의 대규모 전송 발생
- **전송 방향별 특징**
  - 클라이언트 → 서버: 3GB 이상 대용량 업로드 4건 발생 (최대 3.81GB)
    → 대규모 파일 업로드나 백업 작업으로 추정
  - 서버 → 클라이언트: 일부 연결에서 대용량 다운로드 확인 (예: 1.69GB)