결과 파일: 0731_analysis.txt

---

1. 프로토콜/응답 포트별 연결 수 Top 10 (Protocol/Resp_Port)

```
 372249 tcp       443
      7 udp       443
      4 tcp      9200
      1 tcp       143
```

---

2. 서버 이름별 연결 수 Top 10 (SSL/TLS Server Name)

```
  92273 www.muni.cz
  88886 cdn.muni.cz
  12548 www.econ.muni.cz
  12154 www.fss.muni.cz
   8126 poradna.fss.muni.cz
   7127 it.muni.cz
   6961 www.ics.muni.cz
   6161 www.recetox.muni.cz
   4866 perun-aai.org
   4202 www.skm.muni.cz
```

---

3. 시간대별 활동량 시각화 (Hour vs. Count)

```
[00]     17515 **********
[01]     18782 **********
[02]     16629 **********
[03]     17785 **********
[04]     16390 **********
[05]     19007 **********
[06]     15286 **********
[07]     12938 **********
[08]     11222 **********
[09]     12119 **********
[10]     11380 **********
[11]     11573 **********
[12]     11169 **********
[13]     13954 **********
[14]     13693 **********
[15]     16358 **********
[16]     17629 **********
[17]     16018 **********
[18]     16955 **********
[19]     16847 **********
```

[20] 15758 **********
[21] 16772 **********
[22] 18847 **********
[23] 17635 **********

---

4. 비정상 종료 연결 상태 Top (SF: 정상 종료 제외)

 125309 RSTR
  38991 RSTO
  26090 OTH
  11998 SH
   1452 S1
    450 RSTRH
    358 SHR
    182 S0
     42 REJ
     38 S2
      2 S3

---

5. 데이터 전송량 Top 10 (Total/Client Tx/Server Tx - 단위 자동 변환)

Total Size	Resp_IP	Client Tx (Orig)	Server Tx (Resp)	TS (Timestamp)
4.04GB	10.0.0.1	4.00GB	44.80MB	1627754301.266073
1.57GB	10.0.0.1	1.57GB	131.96KB	1627713710.649055
1.50GB	10.0.0.2	1.50GB	3.06KB	1627738130.193924
1.40GB	10.0.0.2	517B	1.40GB	1627710851.052193
600.45MB	10.0.0.3	1.05KB	600.45MB	1627705394.786482
505.59MB	10.0.0.2	1.15MB	504.44MB	1627735897.250384
379.01MB	10.0.0.2	186.31KB	378.83MB	1627700783.042054
359.12MB	10.0.0.2	517B	359.12MB	1627710851.385442
142.24MB	10.0.0.1	517B	142.24MB	1627732762.875411
80.20MB	10.0.0.2	1.66KB	80.20MB	1627748738.660308

---

6. 서버 응답량 분포 Top 10 (MB 단위)

 367830 0MB
   2552 1MB
    777 2MB
    401 3MB
    175 4MB
    139 5MB
    104 6MB
     75 7MB

44 10MB
31 8MB
---
7. 평균 연결 지속 시간 (Average Duration)
평균 연결 지속 시간: 15.6306 초
==========

1. 트래픽 환경 및 기본 특징

- **주요 프로토콜**: 전체 37만 2261건 중 372,249건이 TCP 443 포트(HTTPS) 사용 (99.99%)
  - 소량의 UDP 443 연결 7건, TCP 9200 포트 4건(Elasticsearch/Kibana 관련) 확인됨
- **주요 접속 대상**: muni.cz 도메인 계열
  - www.muni.cz: 92,273건 (메인 웹사이트)
  - cdn.muni.cz: 88,886건 (CDN 서버)
  - www.econ.muni.cz, www.fss.muni.cz 등 서브 도메인도 높은 순위 차지

2. 시간대별 활동 패턴

- **피크 시간대**: 05시(19,007건), 22시(18,847건), 01시(18,782건)에 최고치 기록
- **활동 집중 시간**: 00~05시, 16~23시의 야간/새벽 시간대에 집중
- **특징**: 일반 업무 시간(09~17시)보다 새벽/심야에 트래픽 활발
  → 자동화 작업(백업, 데이터 동기화, 크롤링)이나 타 지역 시차 사용량으로 추정

3. 연결 상태 및 실패율

- **비정상 연결 다수 발생**
  - RSTR (클라이언트 측 강제 종료): 125,309건
  - RSTO (서버 측 강제 종료/타임아웃): 38,991건
  - OTH (기타 상태): 26,090건
- **원인 추정**: 클라이언트 요청 중단 또는 서버 과부하로 인한 강제 종료
- **평균 연결 지속 시간**: 15.6초로 비교적 긴 편

4. 데이터 전송 부하 분석 (Top 10)

- **전송량 규모**: 80.20MB~4.04GB의 대규모 데이터 전송 발생
- **전송 방향별 특징**
  - 클라이언트 → 서버: 4.00GB, 1.57GB, 1.50GB의 대용량 업로드 3건 발생
    → 대규모 파일 업로드나 백업 작업으로 확인됨
  - 서버 → 클라이언트: 1.40GB, 600.45MB 등 대용량 다운로드 확인
    (예: 10.0.0.2에서 1.40GB 다운로드)