결과 파일: 0803_analysis.txt

---

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

```
 426301 tcp       443
      7 udp       443
```

---

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

```
 128635 cdn.muni.cz
 104922 www.muni.cz
  13881 www.econ.muni.cz
  13153 www.fss.muni.cz
   8103 poradna.fss.muni.cz
   7480 it.muni.cz
   6332 webcentrum.muni.cz
   6255 www.ics.muni.cz
   5986 www.skm.muni.cz
   5865 www.recetox.muni.cz
```

---

3. 시간대별 활동량 시각화 (Hour vs. Count)

```
[00]     19594 ******************
[01]     21801 ********************
[02]     19453 ******************
[03]     20245 ********************
[04]     19682 ******************
[05]     18920 ******************
[06]     15301 ***************
[07]     12953 ************
[08]     12039 ************
[09]     10734 **********
[10]     10417 **********
[11]     10533 **********
[12]     11128 ***********
[13]     13893 *************
[14]     16043 ***************
[15]     18204 ******************
[16]     21333 ********************
[17]     22873 *********************
[18]     21316 ********************
[19]     22582 *********************
[20]     23379 **********************
[21]     21209 ********************
```

[22] 21287 **********
[23] 21389 **********
---
4. 비정상 종료 연결 상태 Top (SF: 정상 종료 제외)
 160055 RSTR
  42212 RSTO
  25244 OTH
   4574 SH
   1748 S1
    734 RSTRH
    480 SHR
    183 S0
     46 S2
     42 REJ
      1 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)
2.28GB	10.0.0.1	1.14GB	1.14GB	1627949652.820708
2.00GB	10.0.0.1	1.39GB	620.54MB	1627989118.637186
1.72GB	10.0.0.2	1.72GB	223B	1627949892.224801
1.70GB	10.0.0.2	1.70GB	3.06KB	1627989116.914493
1.70GB	10.0.0.1	1.70GB	2.89KB	1628006859.850227
1.64GB	10.0.0.2	1.64GB	3.06KB	1627949652.710183
1.59GB	10.0.0.2	1.37GB	218.33MB	1627949652.711783
1.41GB	10.0.0.1	279.38MB	1.14GB	1628006859.790684
1.39GB	10.0.0.1	1.39GB	0B	1627989259.995228
1.29GB	10.0.0.1	667B	1.29GB	1627949892.349777

---
6. 서버 응답량 분포 Top 10 (MB 단위)
 420223 0MB
   3376 1MB
   1104 2MB
    519 3MB
    268 4MB
    221 5MB
    153 6MB
    109 7MB
     69 10MB
     59 8MB

---
7. 평균 연결 지속 시간 (Average Duration)
평균 연결 지속 시간: 19.1784 초
==========
1. 트래픽 환경 및 기본 특징
- 전체 42만 6308건 중 426,301건이 TCP 443 포트(HTTPS) 사용 (99.99%), UDP 443 연결 7건
- cdn.muni.cz: 128,635건 (CDN 서버)
- www.muni.cz: 104,922건 (메인 웹사이트)
- www.econ.muni.cz: 13,881건
- www.fss.muni.cz: 13,153건
- 기타 서브 도메인 다수 확인

2. 시간대별 활동 패턴
- 피크 시간대: 20시(23,379건), 17시(22,873건), 19시(22,582건)에 최고치 기록
- 활동 집중 시간: 00~05시 새벽과 16~23시 저녁 시간대에 집중
- 특징: 업무 시간(08~14시)보다 저녁~심야에 트래픽 급증
→ 업무 종료 후 사용량 증가 및 자동화 작업 혼재로 추정

3. 연결 상태 및 실패율
- 비정상 연결 다수 발생
- RSTR (클라이언트 측 강제 종료): 160,055건
- RSTO (서버 측 강제 종료/타임아웃): 42,212건
- OTH (기타 상태): 25,244건
- SH, S1 등 기타 비정상 상태 다수
- 원인 추정: 클라이언트 요청 중단 또는 서버 과부하로 인한 강제 종료
- 평균 연결 지속 시간: 19.2초로 긴 편

4. 데이터 전송 부하 분석 (Top 10)
- 전송량 규모: 1.29GB~2.28GB의 대규모 데이터 전송 발생
- 전송 방향별 특징
- 양방향 대용량: 2.28GB (클라이언트 1.14GB, 서버 1.14GB)
- 클라이언트 → 서버: 1.72GB, 1.70GB, 1.64GB, 1.39GB 등 대용량 업로드 다수
→ 대규모 파일 업로드나 백업 작업으로 추정
- 서버 → 클라이언트: 1.29GB, 1.14GB 등 대용량 다운로드 확인
- 특징: 이전 날짜와 달리 클라이언트→서버 방향 대용량 전송이 두드러짐

5. 서버 응답량 분포
- 대부분 소용량: 420,223건(98.6%)이 0MB대 응답
- 중대용량 응답: 1~10MB 범위 응답이 5,878건 정도 분포
- 특징: 소량의 연결에서 대용량 전송이 집중됨