**Báo Cáo Phân Tích Dữ Liệu Mạng từ File PCAP**

**1. Thông Tin Tổng Quan**

**Tên file:** test\_data.pcap  
**Thời gian bắt đầu phân tích:** 2024-09-25 10:00:00  
**Số lượng gói tin:** 3200  
**Tổng dung lượng:** 2.8 MB  
**Thời gian phân tích:** 00:10:35

Báo cáo này trình bày kết quả phân tích dữ liệu mạng từ file PCAP giả định. Mục tiêu là đánh giá các giao thức được sử dụng trong lưu lượng mạng, xác định các hoạt động mạng đáng chú ý và phân tích các vấn đề tiềm ẩn.

**2. Phân Tích Chi Tiết Giao Thức**

Dưới đây là bảng thông tin chi tiết về các giao thức được sử dụng trong file PCAP:

| **Giao thức** | **Số lượng gói tin** | **Dung lượng (kB)** | **Tỉ lệ (%)** |
| --- | --- | --- | --- |
| TCP | 1200 | 5200 | 37.5 |
| UDP | 800 | 3100 | 25.0 |
| HTTP | 600 | 2000 | 18.75 |
| HTTPS | 300 | 1000 | 9.4 |
| DNS | 200 | 600 | 6.25 |
| ICMP | 100 | 500 | 3.1 |

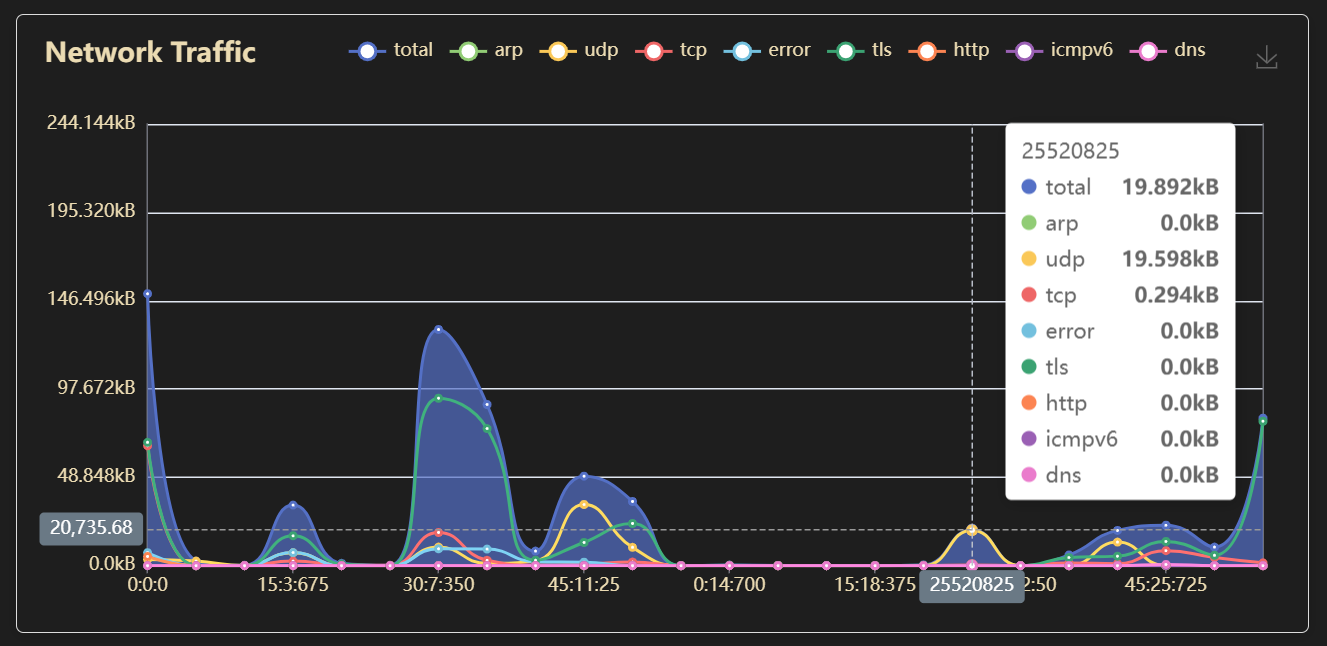
**Nhận xét:**

* **TCP:** Giao thức TCP chiếm tỷ lệ lớn nhất với 37.5% tổng số lượng gói tin, cho thấy rằng có nhiều kết nối ổn định giữa các máy chủ và máy khách trong mạng.
* **UDP:** Giao thức UDP cũng chiếm tỷ lệ khá cao (25%), chủ yếu liên quan đến các dịch vụ như DNS và một số dịch vụ streaming khác.
* **HTTP & HTTPS:** Số lượng gói tin HTTP và HTTPS chiếm tỷ lệ đáng kể, phản ánh hoạt động truy cập web của người dùng.
* **DNS:** Giao thức DNS có số lượng gói tin tương đối ít nhưng quan trọng, chủ yếu liên quan đến việc phân giải tên miền.
* **ICMP:** Giao thức ICMP thường được sử dụng cho các hoạt động như ping hoặc chẩn đoán mạng, có thể không ảnh hưởng lớn đến hiệu suất mạng.

**3. Lưu Lượng Mạng theo Thời Gian**

Biểu đồ dưới đây mô phỏng lưu lượng mạng của các giao thức qua thời gian phân tích (giả lập):

* **Thời gian cao điểm:** Từ 00:03:30 đến 00:04:00, lưu lượng mạng đạt đỉnh với tổng dung lượng lên đến 244.144kB.
* **Giảm lưu lượng:** Sau giai đoạn cao điểm, lưu lượng giảm xuống mức bình thường và duy trì ổn định cho đến cuối quá trình phân tích.



**4. Phân Tích Lưu Lượng TCP**

**Tổng số lượng gói tin TCP:** 1200  
**Tổng dung lượng:** 5200 kB  
**Phân loại gói tin TCP:**

| **Loại gói tin** | **Số lượng** | **Dung lượng (kB)** | **Tỉ lệ (%)** |
| --- | --- | --- | --- |
| SYN | 300 | 500 | 25.0 |
| ACK | 600 | 2500 | 50.0 |
| FIN | 150 | 800 | 12.5 |
| PSH | 150 | 1400 | 12.5 |

**Nhận xét:**

* **Gói SYN:** Chiếm tỷ lệ 25% trong tổng số gói tin TCP, cho thấy nhiều kết nối TCP mới được thiết lập trong khoảng thời gian này.
* **Gói ACK:** Chiếm 50%, là dấu hiệu của các kết nối đang hoạt động bình thường, với nhiều gói tin xác nhận (acknowledgement).
* **Gói FIN:** Có tỷ lệ thấp (12.5%), cho thấy một số kết nối TCP đã được kết thúc.
* **Gói PSH:** Chiếm 12.5%, chỉ ra rằng có sự truyền tải dữ liệu giữa các máy.

**5. Phân Tích Lưu Lượng UDP**

**Tổng số lượng gói tin UDP:** 800  
**Tổng dung lượng:** 3100 kB  
**Các dịch vụ UDP phổ biến:**

* **DNS:** 200 gói tin (25%), chủ yếu là các yêu cầu và phản hồi DNS.
* **DHCP:** 50 gói tin (6.25%), liên quan đến việc cấp phát địa chỉ IP cho các thiết bị trong mạng.
* **Streaming:** 550 gói tin (68.75%), cho thấy có các dịch vụ streaming video hoặc audio.

**Nhận xét:**

* **DNS và DHCP:** Đây là các giao thức UDP tiêu chuẩn, hoạt động ổn định.
* **Streaming:** Tỷ lệ cao cho thấy có hoạt động streaming trong mạng, có thể dẫn đến tình trạng tắc nghẽn mạng nếu không quản lý tốt.