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: 2024-10-01 11:31:00

Số lượng gói tin: 1251

Tổng dung lượng: 660.58 KB

# 2. Phân Tích Chi Tiết Giao Thức

|  |  |  |  |
| --- | --- | --- | --- |
| Giao thức | Số lượng gói tin | Dung lượng (KB) | Tỉ lệ (%) |
| ARP | 16 | 0.80 | 1.28 |
| DATA | 161 | 41.93 | 12.87 |
| TCP | 540 | 241.89 | 43.17 |
| TLS | 404 | 307.09 | 32.29 |
| HTTP | 1 | 0.71 | 0.08 |
| DATA-TEXT-LINES | 1 | 1.00 | 0.08 |
| URLENCODED-FORM | 2 | 1.59 | 0.16 |
| JSON | 2 | 1.38 | 0.16 |
| ICMPV6 | 2 | 0.17 | 0.16 |
| QUIC | 116 | 60.81 | 9.27 |
| \_WS.MALFORMED | 2 | 2.52 | 0.16 |
| DNS | 4 | 0.68 | 0.32 |

## Nhận xét:

• ARP: Giao thức ARP chiếm tỷ lệ 1.28% trong tổng số lượng gói tin.

• DATA: Giao thức DATA chiếm tỷ lệ 12.87% trong tổng số lượng gói tin.

• TCP: Giao thức TCP chiếm tỷ lệ 43.17% trong tổng số lượng gói tin.

• TLS: Giao thức TLS chiếm tỷ lệ 32.29% trong tổng số lượng gói tin.

• HTTP: Giao thức HTTP chiếm tỷ lệ 0.08% trong tổng số lượng gói tin.

• DATA-TEXT-LINES: Giao thức DATA-TEXT-LINES chiếm tỷ lệ 0.08% trong tổng số lượng gói tin.

• URLENCODED-FORM: Giao thức URLENCODED-FORM chiếm tỷ lệ 0.16% trong tổng số lượng gói tin.

• JSON: Giao thức JSON chiếm tỷ lệ 0.16% trong tổng số lượng gói tin.

• ICMPV6: Giao thức ICMPV6 chiếm tỷ lệ 0.16% trong tổng số lượng gói tin.

• QUIC: Giao thức QUIC chiếm tỷ lệ 9.27% trong tổng số lượng gói tin.

• \_WS.MALFORMED: Giao thức \_WS.MALFORMED chiếm tỷ lệ 0.16% trong tổng số lượng gói tin.

• DNS: Giao thức DNS chiếm tỷ lệ 0.32% trong tổng số lượng gói tin.

# 4. Phân Tích Lưu Lượng TCP

Tổng số lượng gói tin TCP: 540

Tổng dung lượng: 241.89 KB

## Phân loại gói tin TCP:

|  |  |  |  |
| --- | --- | --- | --- |
| Loại gói tin | Số lượng | Dung lượng (kB) | Tỉ lệ (%) |
| SYN | 24 | 1.73 | 4.44 |
| ACK | 0 | 0.00 | 0.00 |
| FIN | 0 | 0.00 | 0.00 |
| PSH | 0 | 0.00 | 0.00 |

## Nhận xét:

• Gói SYN: Chiếm tỷ lệ 4.44% trong tổng số gói tin TCP, cho thấy nhiều kết nối TCP mới được thiết lập.

• Gói ACK: Chiếm 0.00%, 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 (0.00%), cho thấy một số kết nối TCP đã được kết thúc.

• Gói PSH: Chiếm 0.00%, chỉ ra rằng có sự truyền tải dữ liệu giữa các máy.

# 5. Phân Tích Lưu Lượng UDP

Tổng số lượng gói tin UDP: 0

Tổng dung lượng: 0.00 KB

Các dịch vụ UDP phổ biến:

Nhận xét: