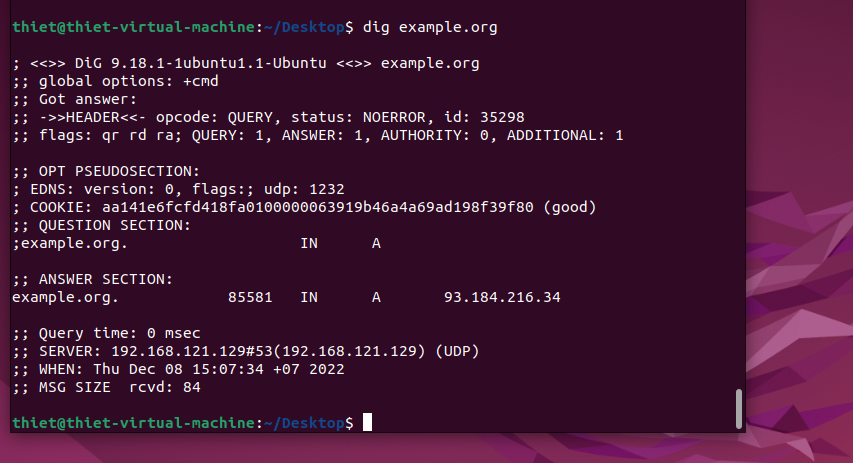
5. Tại sao khi thiết lập spoofip với giá trị raw, tỉ lệ thành công khi thực hiện hình thức tấn công này sẽ cao hơn?



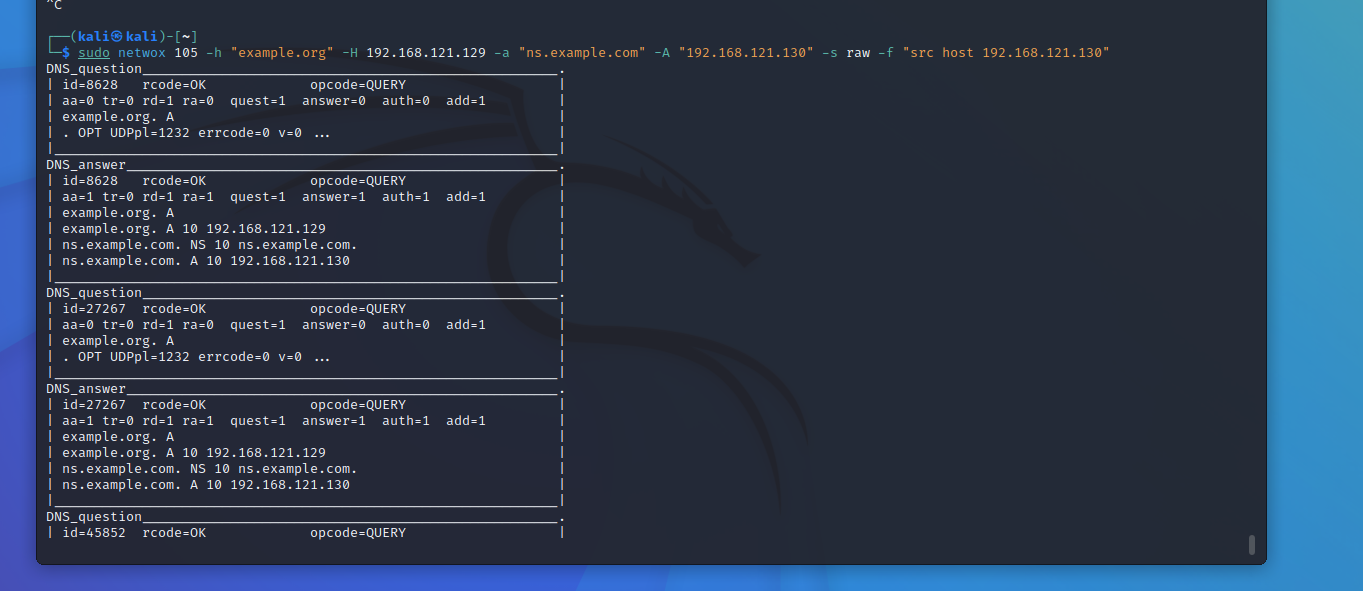
* Xóa rỗng DNS cache tại DNS server



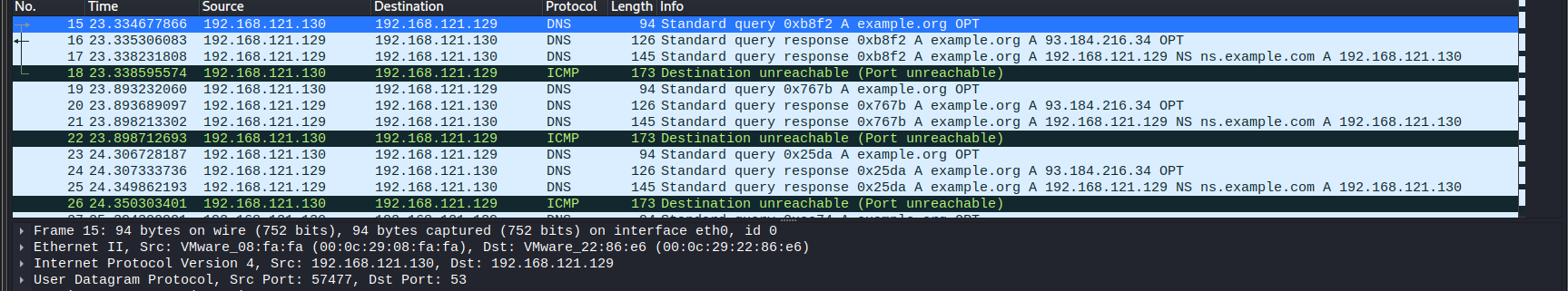
* Tại máy tấn công, sử dụng Netwox 105 như trong bài trước để thực hiện tấn công. Sử dụng filter với nội dung “src host 10.0.2.6” (sử dụng địa chỉ IP của DNS server). Có thể sử dụng thêm ttl (time-to-live) để chỉ định thời gian tồn tại trong bộ nhớ cache.



* Bên máy user ta thực hiện phân giải tên miền



* Kết quả sau khi thực hiện tấn công
* Để nguyên trường spoofip; nếu không, Netwox 105 sẽ cố gắng giả mạo địa chỉ MAC cho địa chỉ IP giả mạo. Để có được địa chỉ MAC, tool sẽ gửi một yêu cầu ARP, yêu cầu địa chỉ MAC của IP giả mạo. Địa chỉ IP giả mạo này thường là địa chỉ IP của một máy chủ DNS bên ngoài, không nằm trên cùng một mạng LAN. Do đó sẽ không có trả lời cho yêu cầu ARP. Tool sẽ đợi trả lời ARP một lúc trước khi tiếp tục mà không có địa chỉ MAC. Việc chờ đợi sẽ trì hoãn tool gửi phản hồi giả mạo. Nếu phản hồi DNS chính chủ trả sớm hơn phản hồi giả mạo thì cuộc tấn công sẽ thất bại.



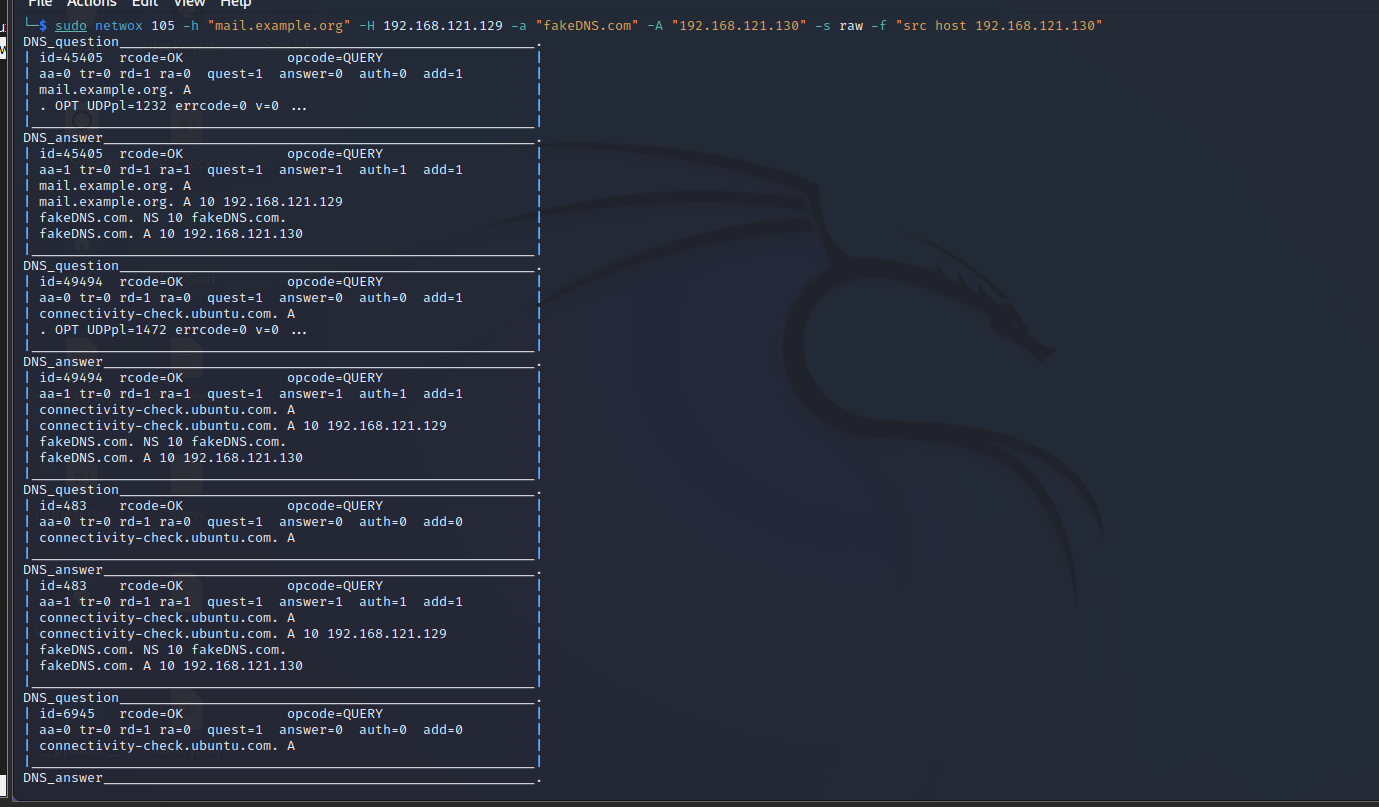
* Sử dụng wireshark để bắt quá trình phân giải tên miền

6. Cách thức tấn công này có nhược điểm chỉ áp dụng trên các hostname cụ thể đã xác định trước (example.org). Nếu người dùng truy cập vào hostname khác (mail.example.org) thì không thể tấn công được. Sinh viên thực hiện tìm hiểu và thực hiện tấn công Authority Section để DNS servers lưu cache thông tin nameserver giả mạo

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Trước khi bị đầu độc



* Thực hiện poisoning



* Kết quả poisoning