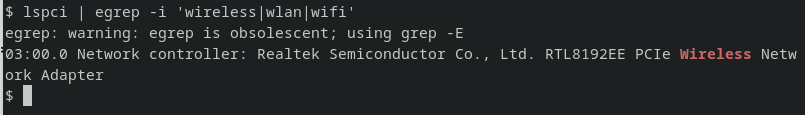
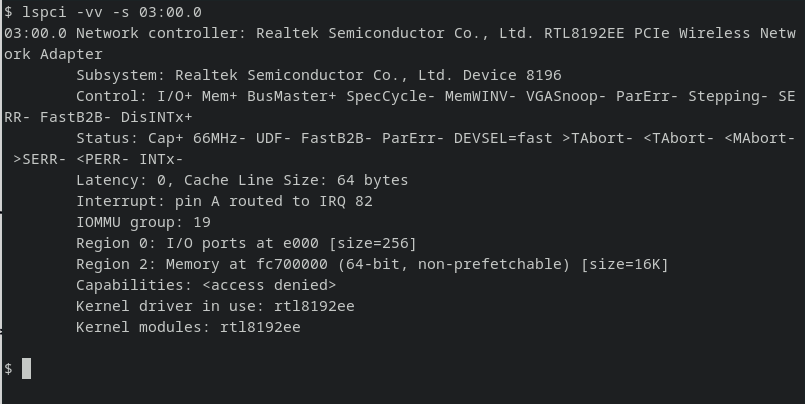
***به نام خدا***

سوال 1:

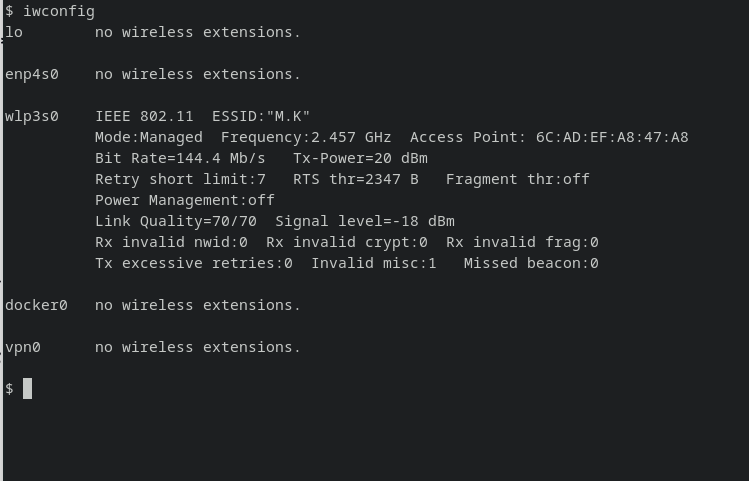




سوال 2:

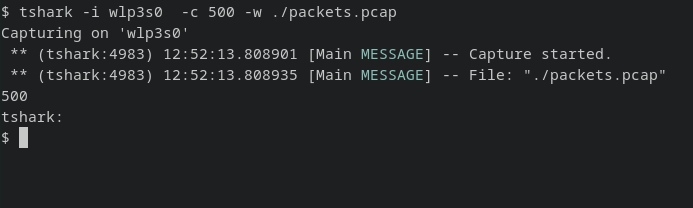
rssi قدرت سیگنال دریافتی را نشان میدهد و تقریبی از قدرت سیگنال دریافتی است.

snr رابطه مستقیمی با rssi دارد. rssi سیگنال قوی‌تر را نشان میدهد و snr نیز بیشتر خواهد شد .

سوال 3:

تغییر مکان باعث تغییر rssi می‌شود.

سوال 4:



سوال 5:

الف)



ب)



سوال 6:

Management:برای مدیریت سرویس‌ها (اتصال، قطع ارتباط و …) استفاده میشوند. سه نمونه زیر مجموعه دارد که شامل موارد زیر است:

association request

reassociation request

probe request

Control:برای کمک به تحویل بسته‌های داده به مقصد موردنظر بین station‌ها استفاده میشود. سه نمونه زیر مجموعه دارد که شامل موارد زیر است:

trigger

ack

tack

Data: داده‌ها همچون صفحات وب را درون شبکه حمل می‌کنند. سه زیر مجموعه دارد که شامل موارد زیر است:

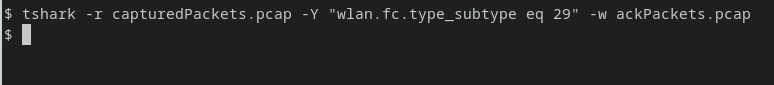
data

null

QoS data

سوال 7:

الف)

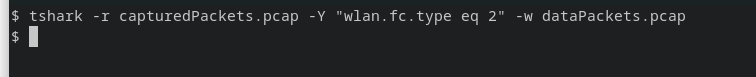


ب)

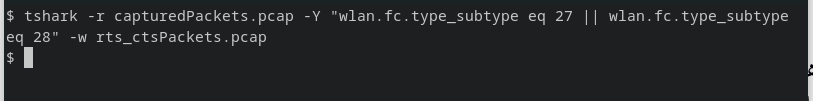
اطلاعات مربوط به شبکه را در فواصل زمانی مشخص به نقاط دیگر می‌فرستند.



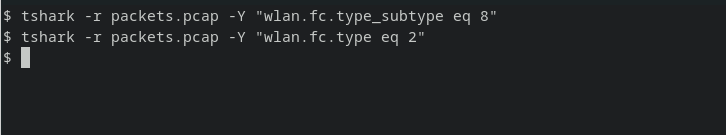
ج)



د)



سوال 8:



خیر. چون واسط شبکه‌ی مورد استفاده در حالت Managed می‌باشد، برای دریافت و ارسال بسته‌ها از MAC آدرس استفاده می‌کند. بنابراین بسته‌های دیگر قابل ردیابی از طریق این واسط نیستند.

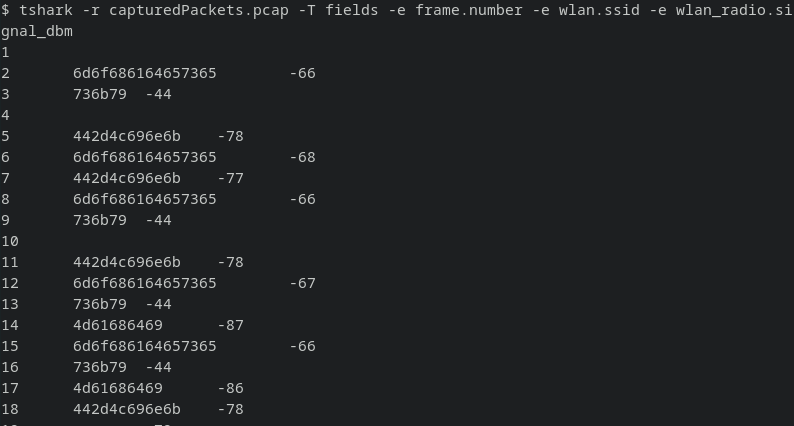
سوال 9:

در این دو مود واسط شبکه تمامی بسته‌هایی که می‌گیرد را به cpu گزارش می‌دهد، در نتیجه تمامی بسته‌ها قابل ردیابی می‌شوند. در حالت promiscuous فقط بسته‌هایی که مربوط به شبکه متصل می‌باشد و در حالت monitor هر بسته‌ دریافت شده (حتی از شبکه‌های غیر متصل) گزارش می‌شود

سوال 10:

برای این کار ابتدا حالت واسط را به مانیتور می‌بریم، سپس مثل بخش ۴ عمل می‌کنیم.

سوال 11:



ستون اول برابر با شماره‌ی بسته بوده، ستون دوم ssid شبکه wifi (هر شبکه‌ wifi یک ssid مخصوص به خود دارد که با آن شناخته می‌شود) و ستون سوم rssi می‌باشد.

سوال 12:

در مرحله گرفتن بسته‌ها، می‌توان فیلترهایی استفاده کرد (capture filters) که این فیلتر‌ها باعث می‌شوند فقط بسته‌های متناظر گرفته شوند و در نتیجه دسترسی به بسته‌های فیلتر نشده نداریم. اما فیلترهای نمایش (display filter) فیلتری روی گرفتن بسته‌ها اعمال نمی‌کنند (تمامی بسته‌ها گرفته می‌شود) ولی فقط برخی از بسته‌ها را متناسبا نمایش می‌دهد.

فیلتر capture روی فایل‌های .pcap نمی‌توان اعمال کرد، چراکه این اطلاعات قبلاً گرفته‌شده‌اند و صرفاً می‌توانیم نمایش آن‌ها را در نرم‌افزار فیلتر کنیم.

برای پیداکردن بسته‌ها به شکل زیر عمل می‌کنیم.

tshark -i wlp3s0 -f “icmp && src host 192.168.1.51 && dst host 192.168.1.52”

tshark -i wlp3s0 -Y “icmp && ip.src==192.168.1.51 && ip.dst==192.168.1.52”