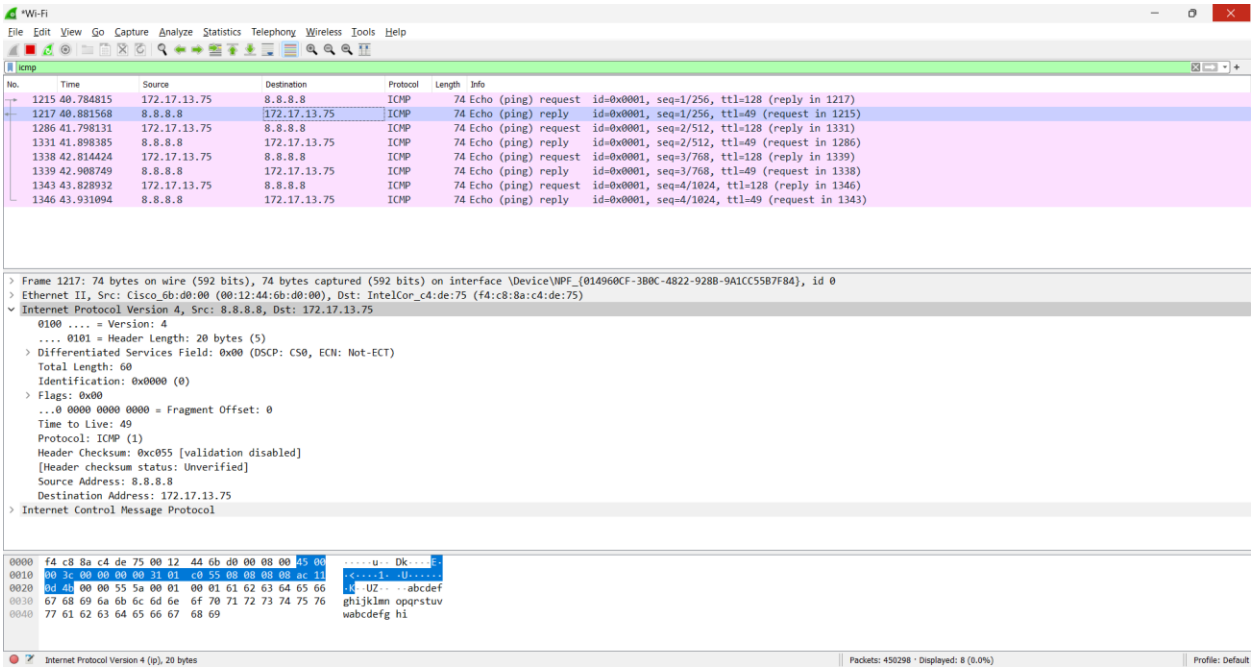
Practical Wireshark Homework

-1

نداشتن checksum یا [validation disabled] به این معنی است که router نیازی به محاسبه و تعیین صحت بسته ندارد. دلیلش هم این است که این به نوعی کار اضافه حساب میشود چون پروتکل های link-layer مانند Ethernet یا Wifi خودشان روش های صحت سنجی خودشان را دارند و عملا بسته ای که تحویل داده میشود سالم است(درستی بسته در جای دیگری قبلا چک شده یا میشود). مگر اینکه اشکال منطقی داشته باشد که این با checksum هم قابل تشخیص نیست. پس با حساب نکردن و به نوعی در نظر نگرفتن checksum در پردازش بسته ها سرعت بیشتری ایجاد میشود و محاسبات کمتر میشود.

-2 چکسام در این بسته 0xC055 تعیین شده که در انتها ماهم به همین میرسیم. برپا محاسبه چکسام خود فیلد 0 میشود.



-3	Bit-1	Bit-2	Bit-3	Bit-4	Bit-5	Bit-6	Bit-7	Bit-8	Bit-9	Bit-10	Bit-11	Bit-12	Bit-13	Bit-14	Bit-15	Bit-16	Hex Result
No.1	0	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	4500
No.2	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	3C
No.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
No.2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
No.3	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	1	3101
No.4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
No.5	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0808
No.6	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0808
No.7	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	1	AC11
No.8	0	0	0	0	1	1	0	1	0	1	0	0	1	0	1	1	0D4B
No.9 Result	0	0	1	1	1	1	1	1	1	0	1	0	1	0	1	0	13FA9=3FFA
No.10 Not Result	1	1	0	0	0	0	0	0	0	1	0	1	0	1	0	1	C055

3- بله. با اینکه احتمال رخ دادن این اتفاق کم است ولی ممکن است دو بسته دارای checksum یکسان باشند. یک احتمال این است که دو بسته کاملا معادل و یکسان باشند پس منطقی است که checksum انها هم مساوی باشد. ولی با احتمال خیلی کمتر ممکن است به طور اتفاقی checksum دو بسته یکسان باشد. برای اینکه از یکسان بودن یا نبودن این دو بسته اطمینان حاصل کنیم میتوانیم راه های دیگری برای مقایسه دو بسته در نظر بگیریم. به عنوان مثال طول دو بسته نیز مقایسه شود و اگر نابرابر بود معلوم میشود که به طور اتفاقی checksum این دو بسته یکسان شده. اگر از این هم بگذریم میتوان برای اطمینان بیشتر چند بخش دیگر را هم چک کرد به همین روش.