

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 عملاً بسته ای که تحویل داده میشود سالم است(درستی بسته در جای دیگری قبلاً 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 ما هم به همین میرسیم. بریا محاسبه چکسام خود فیلد 0 میشود.

Wireshark packet capture showing ICMP Echo (ping) request and reply. The packet list shows a request from 172.17.13.75 to 8.8.8.8 and a reply from 8.8.8.8 to 172.17.13.75. The packet details show the ICMP Echo (ping) request with ID 0x0001, sequence 1/256, and TTL 128. The packet bytes show the raw data of the ICMP Echo request.

No.	Time	Source	Destination	Protocol	Length	Info
1215	40.784815	172.17.13.75	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 1217)
1217	40.881568	8.8.8.8	172.17.13.75	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=49 (request in 1215)
1286	41.798131	172.17.13.75	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 1331)
1331	41.898385	8.8.8.8	172.17.13.75	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=49 (request in 1286)
1338	42.814424	172.17.13.75	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 1339)
1339	42.908749	8.8.8.8	172.17.13.75	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=49 (request in 1338)
1343	43.828932	172.17.13.75	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 1346)
1346	43.931894	8.8.8.8	172.17.13.75	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=49 (request in 1343)

Frame 1217: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{01A960CF-3B0C-4822-928B-9A1CC55B7F84}, id 0
Ethernet II, Src: CiscoGb:00:00 (00:12:44:6b:d0:00), Dst: IntelCor_c4:de:75 (f4:c8:8a:c4:de:75)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.17.13.75
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x0000 (0)
> Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 49
Protocol: ICMP (1)
Header Checksum: 0xc055 [validation disabled]
[Header checksum status: Unverified]
Source Address: 8.8.8.8
Destination Address: 172.17.13.75
> Internet Control Message Protocol

0000 f4 c8 8a c4 de 75 00 12 44 6b d0 00 08 00 45 00Dk....
0010 00 3c 00 00 00 00 31 01 c0 55 08 08 08 08 ac 111..U....
0020 0d 4b 00 00 55 5a 00 01 00 01 61 62 63 64 65 66 ..k-UZ...abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklm opqrstu
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Internet Protocol Version 4 (ip), 20 bytes Packets: 450298 - Displayed: 8 (0.0%) Profile: Default

-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 کاملاً معادل و یکسان باشند پس منطقی است که checksum آنها 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.