

מטלה 2 רשתות תקשורת

Ping Request and Reply – In Protocol ICMP:

תוכן העניינים :

הקדמה	עמוד 2
תיאור הקוד והוראות ההרצה	עמוד 3
הסבר הקוד לפי צילומי הטרמינל	עמודים 4-5
הסבר הקוד לפי צילומי wireshark	עמודים 6-8

הקדמה:

מטלה זו מחולקת לשני חלקים: חלק א' וחלק ב'.

חלק א:

בחלק זה נתבקשנו לכתוב קוד המממש בקשת ping משרת כלשהו ברשת האינטרנט והמקבל ממנו תשובה לבקשה זו באמצעות פרוטוקול ICMP, כאשר בקשה זו למעשה נשלחת ללא הפסקה כלל.

בקשת ping - הינה יישום השולחת חבילת נתונים בפרוטוקול ICMP ממקור מסוים ליעד מסוים ברשת לפי כתובתו. המטרה העיקרית לה היא משמשת היא בחינת תקינות התקשורת בין נקודת המקור לנקודת היעד.

פרוטוקול ICMP : בראשי התיבות- "Internet Control Message Protocol", הינו פרוטוקול המשמש לבחינת תקינות תקשורת באינטרנט ופועל על פי כתובות IP באופן ישיר. פרוטוקול זה פועל בשכבת הרשת, שהיא למעשה השכבה השלישית על פי מודל ה OSI.

חלק ב:

בחלק זה נתבקשנו להשתמש בקוד אותו מימשנו בחלק א' ולשדרג אותו ע"י קיום קשר באמצעות פרוטוקול tcp בין socket הנמצא בקובץ המבצע שליחת הודעות מסוג ping ללא הפסקה (client), לבין socket הנמצא בקובץ אחר המכונה "watchdog" (server).

ה "watchdog" למעשה אמור להחזיק בתוכו timer המתחיל את פעולתו לאחר שליחת בקשת ה Ping, והמסתיים לאחר עשר שניות מרגע התנעתו או בהישלח הודעה חוזרת מטעם השרת אליו מתבצעת בקשת ה Ping.

במקרה שבו עברו 10 שניות מרגע ההתנעה, וטרם התקבלה הודעה חוזרת מטעם השרת אליו נשלחה הודעת ה ping, הוא אמור לשלוח הודעה ל socket הנמצא בקובץ המבצע את שליחת בקשות ה ping, בדרישה להפסיק את פעולתו, וכתוצאה מכך לסיים את הרצת התוכנית.

תיאור הקוד והוראות ההרצה:

הקוד אותו נתבקשנו לכתוב מורכב למעשה מ 3 קבצי c שונים, וכן מקובץ makefile המשמש לצורך ביצוע ההרצה.

הקובץ ping.c :

בקובץ זה אנו למעשה יוצרים raw-socket המשתמש בפרוטוקול icmp לצורך שליחת בקשות ping מהשרת, שכתובת ה ip שלו היא הכתובת המתקבלת כקלט בפונקציית main של הקובץ. כמו כן, נעשה בקובץ זה שימוש בפונקציית העזר "calculate checksum", לצורך חישוב השדה checksum שבפקטות ה ICMP. פקודת ההרצה לקובץ זה המממש את חלק א' במטלה היא "sudo ./parta 8.8.8.8".

הקבצים better_ping.c + watchdog :

בדומה ל ping.c, גם בקובץ זה אנו יוצרים raw-socket, השולח בקשות ping לשרת המתקבל כקלט בפונקציית ה main על ידי פרוטוקול ICMP. לצורך הידור פקטות ה ICMP נשתמש בפונקציית העזר "calculate checksum". לצורך תקשורת בין ה socket הנמצא בקובץ זה בתור "tcp-client" לבין ה watchdog המשמש כ "tcp-server" אנו משתמשים בפורט מספר 3000, ובאמצעותו הם מתקשרים אחד עם השני. כאשר הודעת ping נשלחת מה "better_ping" אל השרת המתקבל בפונקציית main, תישלח הודעת "start" ל watchdog, ועל הודעה זו הוא יענה "accept". מייד לאחר מכן ייכנס ה watchdog אל לולאת while, הטיפסק בתום 10 שניות, או באמצעות קבלת ההודעה "success" מה better_ping. כאשר תתקבל הודעת ping בחזרה מהשרת אליו נשלחה ההודעה מקודם, תישלח הודעת "success" מה "better_ping" אל ה "watchdog", כאשר גם על הודעה זו הוא ישיב "accept". במקרה שבו לא התקבלה הודעת "success" מה better_ping בתוך 10 שניות מרגע שליחת ההודעה "start", תישלח הודעת "bye" מה watchdog אל ה better_ping, והתוכנית תיפסק. פקודת ההרצה לקובץ זה המממש את חלק ב' במטלה היא "sudo ./partb 8.8.8.8".

הסבר הקוד לפי צילומי הטרמינל:

צילום מספר 1:

```
Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 202
RTT: 66.386002 milliseconds (66386 microseconds)
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 203
RTT: 46.207001 milliseconds (46207 microseconds)
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 204
RTT: 59.323002 milliseconds (59323 microseconds)
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 205
RTT: 45.245998 milliseconds (45246 microseconds)
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 206
RTT: 109.716003 milliseconds (109716 microseconds)
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 207
RTT: 177.638000 milliseconds (177638 microseconds)
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 208
RTT: 188.692993 milliseconds (188693 microseconds)
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 209
RTT: 275.893982 milliseconds (-723106 microseconds)
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 210
RTT: 52.224998 milliseconds (52225 microseconds)
The packet came from 8.8.8.8 all the way to 10.0.2.15
```

בצילום זה ניתן לראות את קבלת פקטות ICMP מהשרת של גוגל שהוא "8.8.8.8".

צילום מספר 2:

```
hamad@hamad-VirtualBox:~/Desktop/EX4_Final$ sudo ./partb 8.8.8.8
[sudo] password for hamad:
in child
create tcp_socket
bind
listen
sucess create icmp
sucess create tcp
accept
Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 1
RTT: 40.409000 milliseconds 40409 microseconds
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 2
RTT: 119.410004 milliseconds 119410 microseconds
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 3
RTT: 658.072998 milliseconds -340927 microseconds
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 4
RTT: 172.119995 milliseconds 172120 microseconds
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 5
RTT: 166.244995 milliseconds 166245 microseconds
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 6
RTT: 531.273010 milliseconds 531273 microseconds
The packet came from 8.8.8.8 all the way to 10.0.2.15

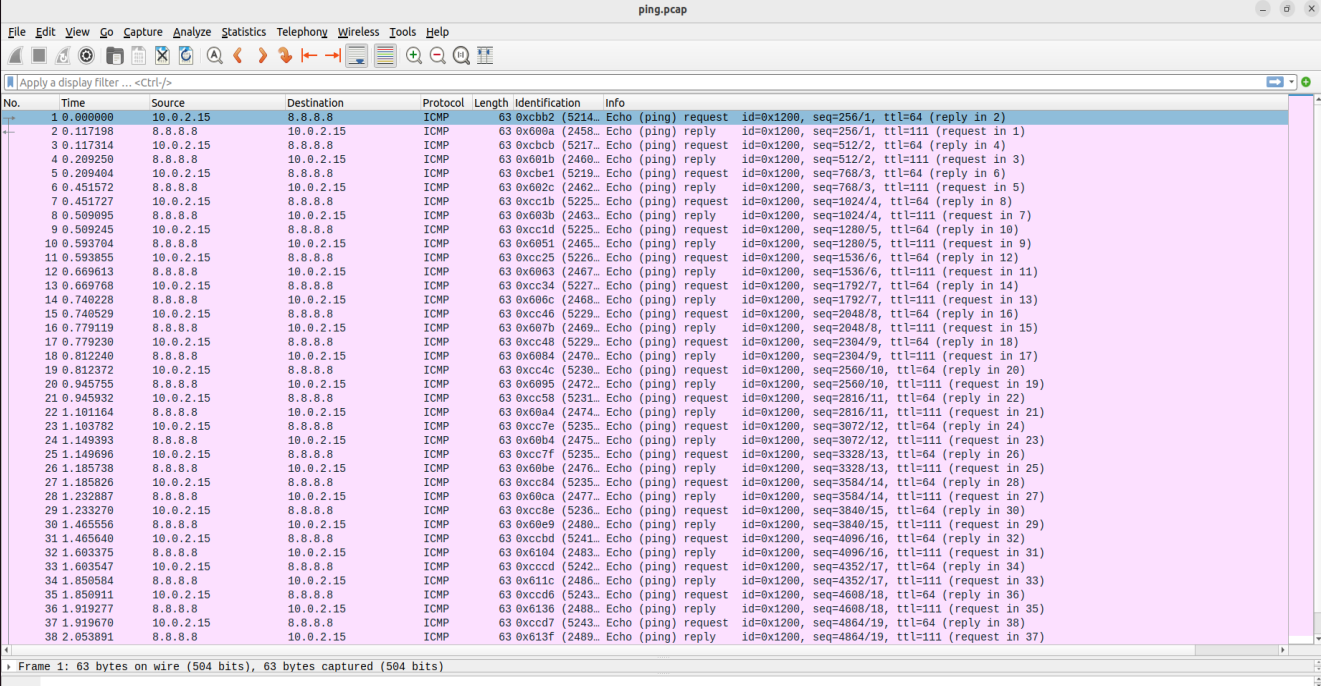
Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 7
RTT: 277.166016 milliseconds -721834 microseconds
The packet came from 8.8.8.8 all the way to 10.0.2.15

Successfully received one packet with 47 bytes : data length : 19 , icmp header : 8 , ip header : 20
The sequence number is: 8
RTT: 70.761002 milliseconds 70761 microseconds
The packet came from 8.8.8.8 all the way to 10.0.2.15
```

בצילום זה ניתן לראות כיצד בהרצת חלק ב' שה-Watchdog יצר תקשורת עם ה-better_ping באמצעות tcp-socket וגם במקביל נוצר raw-socket המשתמש בפרוטוקול ICMP לצורך שליחת הודעת ה-ping .

הסבר הקוד לפי צילומי ה-wireshark:

לפי הקלטות ה-ping :



No.	Time	Source	Destination	Protocol	Length	Identification	Info
1	0.000000	10.0.2.15	8.8.8.8	ICMP	63	0xcbb2 (5214)	Echo (ping) request id=0x1200, seq=256/1, ttl=64 (reply in 2)
2	0.117198	8.8.8.8	10.0.2.15	ICMP	63	0x600a (2458)	Echo (ping) reply id=0x1200, seq=256/1, ttl=111 (request in 1)
3	0.117314	10.0.2.15	8.8.8.8	ICMP	63	0xcbb2 (5217)	Echo (ping) request id=0x1200, seq=512/2, ttl=64 (reply in 4)
4	0.209250	8.8.8.8	10.0.2.15	ICMP	63	0x601b (2460)	Echo (ping) reply id=0x1200, seq=512/2, ttl=111 (request in 3)
5	0.209404	10.0.2.15	8.8.8.8	ICMP	63	0xcbe1 (5219)	Echo (ping) request id=0x1200, seq=768/3, ttl=64 (reply in 6)
6	0.451572	8.8.8.8	10.0.2.15	ICMP	63	0x602c (2462)	Echo (ping) reply id=0x1200, seq=768/3, ttl=111 (request in 5)
7	0.451727	10.0.2.15	8.8.8.8	ICMP	63	0xc0c1b (5225)	Echo (ping) request id=0x1200, seq=1024/4, ttl=64 (reply in 8)
8	0.509095	8.8.8.8	10.0.2.15	ICMP	63	0x603b (2463)	Echo (ping) reply id=0x1200, seq=1024/4, ttl=111 (request in 7)
9	0.509245	10.0.2.15	8.8.8.8	ICMP	63	0xc0c1d (5225)	Echo (ping) request id=0x1200, seq=1280/5, ttl=64 (reply in 10)
10	0.593704	8.8.8.8	10.0.2.15	ICMP	63	0x6051 (2465)	Echo (ping) reply id=0x1200, seq=1280/5, ttl=111 (request in 9)
11	0.593855	10.0.2.15	8.8.8.8	ICMP	63	0xc0c25 (5226)	Echo (ping) request id=0x1200, seq=1536/6, ttl=64 (reply in 12)
12	0.669613	8.8.8.8	10.0.2.15	ICMP	63	0x6063 (2467)	Echo (ping) reply id=0x1200, seq=1536/6, ttl=111 (request in 11)
13	0.669768	10.0.2.15	8.8.8.8	ICMP	63	0xc0c34 (5227)	Echo (ping) request id=0x1200, seq=1792/7, ttl=64 (reply in 14)
14	0.740228	8.8.8.8	10.0.2.15	ICMP	63	0x606c (2468)	Echo (ping) reply id=0x1200, seq=1792/7, ttl=111 (request in 13)
15	0.740529	10.0.2.15	8.8.8.8	ICMP	63	0xc0c46 (5229)	Echo (ping) request id=0x1200, seq=2048/8, ttl=64 (reply in 16)
16	0.779119	8.8.8.8	10.0.2.15	ICMP	63	0x607b (2469)	Echo (ping) reply id=0x1200, seq=2048/8, ttl=111 (request in 15)
17	0.779230	10.0.2.15	8.8.8.8	ICMP	63	0xc0c48 (5229)	Echo (ping) request id=0x1200, seq=2304/9, ttl=64 (reply in 18)
18	0.812240	8.8.8.8	10.0.2.15	ICMP	63	0x6084 (2470)	Echo (ping) reply id=0x1200, seq=2304/9, ttl=111 (request in 17)
19	0.812372	10.0.2.15	8.8.8.8	ICMP	63	0xc0c4c (5230)	Echo (ping) request id=0x1200, seq=2560/10, ttl=64 (reply in 20)
20	0.945755	8.8.8.8	10.0.2.15	ICMP	63	0x6095 (2472)	Echo (ping) reply id=0x1200, seq=2560/10, ttl=111 (request in 19)
21	0.945932	10.0.2.15	8.8.8.8	ICMP	63	0xc0c58 (5231)	Echo (ping) request id=0x1200, seq=2816/11, ttl=64 (reply in 22)
22	1.101164	8.8.8.8	10.0.2.15	ICMP	63	0x60a4 (2474)	Echo (ping) reply id=0x1200, seq=2816/11, ttl=111 (request in 21)
23	1.103782	10.0.2.15	8.8.8.8	ICMP	63	0xc0c7e (5235)	Echo (ping) request id=0x1200, seq=3072/12, ttl=64 (reply in 24)
24	1.149393	8.8.8.8	10.0.2.15	ICMP	63	0x60b4 (2475)	Echo (ping) reply id=0x1200, seq=3072/12, ttl=111 (request in 23)
25	1.149696	10.0.2.15	8.8.8.8	ICMP	63	0xc0c7f (5235)	Echo (ping) request id=0x1200, seq=3328/13, ttl=64 (reply in 26)
26	1.185738	8.8.8.8	10.0.2.15	ICMP	63	0x60be (2476)	Echo (ping) reply id=0x1200, seq=3328/13, ttl=111 (request in 25)
27	1.185826	10.0.2.15	8.8.8.8	ICMP	63	0xc0c84 (5235)	Echo (ping) request id=0x1200, seq=3584/14, ttl=64 (reply in 28)
28	1.232887	8.8.8.8	10.0.2.15	ICMP	63	0x60ca (2477)	Echo (ping) reply id=0x1200, seq=3584/14, ttl=111 (request in 27)
29	1.233270	10.0.2.15	8.8.8.8	ICMP	63	0xc0c8e (5236)	Echo (ping) request id=0x1200, seq=3840/15, ttl=64 (reply in 30)
30	1.465556	8.8.8.8	10.0.2.15	ICMP	63	0x60e9 (2480)	Echo (ping) reply id=0x1200, seq=3840/15, ttl=111 (request in 29)
31	1.465640	10.0.2.15	8.8.8.8	ICMP	63	0xc0cbd (5241)	Echo (ping) request id=0x1200, seq=4096/16, ttl=64 (reply in 32)
32	1.603375	8.8.8.8	10.0.2.15	ICMP	63	0x6104 (2483)	Echo (ping) reply id=0x1200, seq=4096/16, ttl=111 (request in 31)
33	1.603547	10.0.2.15	8.8.8.8	ICMP	63	0xc0ccd (5242)	Echo (ping) request id=0x1200, seq=4352/17, ttl=64 (reply in 34)
34	1.859584	8.8.8.8	10.0.2.15	ICMP	63	0x611c (2486)	Echo (ping) reply id=0x1200, seq=4352/17, ttl=111 (request in 33)
35	1.859911	10.0.2.15	8.8.8.8	ICMP	63	0xc0cd6 (5243)	Echo (ping) request id=0x1200, seq=4608/18, ttl=64 (reply in 36)
36	1.919277	8.8.8.8	10.0.2.15	ICMP	63	0x6136 (2488)	Echo (ping) reply id=0x1200, seq=4608/18, ttl=111 (request in 35)
37	1.919670	10.0.2.15	8.8.8.8	ICMP	63	0xc0cd7 (5243)	Echo (ping) request id=0x1200, seq=4864/19, ttl=64 (reply in 38)
38	2.053891	8.8.8.8	10.0.2.15	ICMP	63	0x613f (2489)	Echo (ping) reply id=0x1200, seq=4864/19, ttl=111 (request in 37)

Frame 1: 63 bytes on wire (504 bits), 63 bytes captured (504 bits)

בצילום זה ניתן לראות את שליחת הודעות ה-ping מה-raw-socket שייצרנו ממקור "10.0.2.15" אל גוגל "8.8.8.8" ומגוגל אלינו בחזרה דרך הפרוטוקול ICMP.

צילומי הקלטות ה-wireshark של חלק ב':

betterping_watchdog.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl>/>

No.	Time	Source	Destination	Protocol	Length	Identification	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	74	0x67ed (2686)	50726 → 3000 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=3298707071 TSecr=0 WS=128
2	0.000015	127.0.0.1	127.0.0.1	TCP	74	0x0090 (0)	3000 → 50726 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=3298707071 TSecr=3298707071
3	0.000025	127.0.0.1	127.0.0.1	TCP	66	0x67ee (2686)	50726 → 3000 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3298707071 TSecr=3298707071
4	0.000064	127.0.0.1	127.0.0.1	TCP	72	0x67ef (2686)	50726 → 3000 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=6 TSval=3298707071 TSecr=3298707071
5	0.000067	127.0.0.1	127.0.0.1	TCP	66	0x62f0 (9744)	3000 → 50726 [ACK] Seq=1 Ack=7 Win=65536 Len=0 TSval=3298707071 TSecr=3298707071
6	0.000096	127.0.0.1	127.0.0.1	TCP	73	0x62f1 (9745)	3000 → 50726 [PSH, ACK] Seq=1 Ack=7 Win=65536 Len=7 TSval=3298707071 TSecr=3298707071
7	0.000115	127.0.0.1	127.0.0.1	TCP	66	0x67f9 (2686)	50726 → 3000 [ACK] Seq=7 Ack=8 Win=65536 Len=0 TSval=3298707071 TSecr=3298707071
8	0.457291	127.0.0.1	127.0.0.1	TCP	73	0x67f1 (2686)	50726 → 3000 [PSH, ACK] Seq=7 Ack=8 Win=65536 Len=7 TSval=3298707528 TSecr=3298707071
9	0.457307	127.0.0.1	127.0.0.1	TCP	73	0x62f2 (9746)	3000 → 50726 [PSH, ACK] Seq=8 Ack=14 Win=65536 Len=7 TSval=3298707528 TSecr=3298707528
10	0.457314	127.0.0.1	127.0.0.1	TCP	66	0x67f2 (2686)	50726 → 3000 [ACK] Seq=14 Ack=15 Win=65536 Len=0 TSval=3298707528 TSecr=3298707528
11	0.457405	127.0.0.1	127.0.0.1	TCP	66	0x67f3 (2686)	50726 → 3000 [PSH, ACK] Seq=14 Ack=15 Win=65536 Len=6 TSval=3298707528 TSecr=3298707528
12	0.457431	127.0.0.1	127.0.0.1	TCP	73	0x62f3 (9747)	3000 → 50726 [PSH, ACK] Seq=15 Ack=20 Win=65536 Len=7 TSval=3298707528 TSecr=3298707528
13	0.497837	127.0.0.1	127.0.0.1	TCP	66	0x67f4 (2686)	50726 → 3000 [ACK] Seq=20 Ack=22 Win=65536 Len=0 TSval=3298707528 TSecr=3298707528
14	0.001011	127.0.0.1	127.0.0.1	TCP	73	0x67f5 (2686)	50726 → 3000 [PSH, ACK] Seq=20 Ack=22 Win=65536 Len=7 TSval=3298707673 TSecr=3298707528
15	0.001030	127.0.0.1	127.0.0.1	TCP	73	0x62f4 (9748)	3000 → 50726 [PSH, ACK] Seq=22 Ack=27 Win=65536 Len=7 TSval=3298707673 TSecr=3298707673
16	0.001038	127.0.0.1	127.0.0.1	TCP	66	0x67f6 (2686)	50726 → 3000 [ACK] Seq=27 Ack=29 Win=65536 Len=0 TSval=3298707673 TSecr=3298707673
17	0.001949	127.0.0.1	127.0.0.1	TCP	72	0x67f7 (2686)	50726 → 3000 [PSH, ACK] Seq=27 Ack=29 Win=65536 Len=6 TSval=3298707673 TSecr=3298707673
18	0.002025	127.0.0.1	127.0.0.1	TCP	73	0x62f5 (9749)	3000 → 50726 [PSH, ACK] Seq=29 Ack=33 Win=65536 Len=7 TSval=3298707673 TSecr=3298707673
19	0.646516	127.0.0.1	127.0.0.1	TCP	66	0x67f8 (2686)	50726 → 3000 [ACK] Seq=33 Ack=36 Win=65536 Len=0 TSval=3298707711 TSecr=3298707673
20	0.764828	127.0.0.1	127.0.0.1	TCP	73	0x67f9 (2686)	50726 → 3000 [PSH, ACK] Seq=33 Ack=36 Win=65536 Len=7 TSval=3298707836 TSecr=3298707673
21	0.764846	127.0.0.1	127.0.0.1	TCP	73	0x62f6 (9750)	3000 → 50726 [PSH, ACK] Seq=36 Ack=40 Win=65536 Len=7 TSval=3298707836 TSecr=3298707836
22	0.764854	127.0.0.1	127.0.0.1	TCP	66	0x67fa (2686)	50726 → 3000 [ACK] Seq=40 Ack=43 Win=65536 Len=0 TSval=3298707836 TSecr=3298707836
23	0.764913	127.0.0.1	127.0.0.1	TCP	72	0x67fb (2686)	50726 → 3000 [PSH, ACK] Seq=40 Ack=43 Win=65536 Len=6 TSval=3298707836 TSecr=3298707836
24	0.764942	127.0.0.1	127.0.0.1	TCP	73	0x62f7 (9751)	3000 → 50726 [PSH, ACK] Seq=43 Ack=46 Win=65536 Len=7 TSval=3298707836 TSecr=3298707836
25	0.818451	127.0.0.1	127.0.0.1	TCP	66	0x67fc (2686)	50726 → 3000 [ACK] Seq=46 Ack=50 Win=65536 Len=0 TSval=3298707889 TSecr=3298707836
26	1.113951	127.0.0.1	127.0.0.1	TCP	73	0x67fd (2686)	50726 → 3000 [PSH, ACK] Seq=46 Ack=50 Win=65536 Len=7 TSval=3298708185 TSecr=3298707836
27	1.113997	127.0.0.1	127.0.0.1	TCP	73	0x62f8 (9752)	3000 → 50726 [PSH, ACK] Seq=50 Ack=53 Win=65536 Len=7 TSval=3298708185 TSecr=3298708185
28	1.114005	127.0.0.1	127.0.0.1	TCP	66	0x67fe (2686)	50726 → 3000 [ACK] Seq=53 Ack=57 Win=65536 Len=0 TSval=3298708185 TSecr=3298708185
29	1.114134	127.0.0.1	127.0.0.1	TCP	72	0x67ff (2686)	50726 → 3000 [PSH, ACK] Seq=53 Ack=57 Win=65536 Len=6 TSval=3298708185 TSecr=3298708185
30	1.114218	127.0.0.1	127.0.0.1	TCP	73	0x62f9 (9753)	3000 → 50726 [PSH, ACK] Seq=57 Ack=59 Win=65536 Len=7 TSval=3298708185 TSecr=3298708185
31	1.157513	127.0.0.1	127.0.0.1	TCP	66	0x6080 (2682)	50726 → 3000 [ACK] Seq=59 Ack=64 Win=65536 Len=0 TSval=3298708228 TSecr=3298708185
32	1.408747	127.0.0.1	127.0.0.1	TCP	73	0x6081 (2682)	50726 → 3000 [PSH, ACK] Seq=59 Ack=64 Win=65536 Len=7 TSval=3298708479 TSecr=3298708185
33	1.408767	127.0.0.1	127.0.0.1	TCP	73	0x62f1a (9754)	3000 → 50726 [PSH, ACK] Seq=64 Ack=66 Win=65536 Len=7 TSval=3298708480 TSecr=3298708479
34	1.408775	127.0.0.1	127.0.0.1	TCP	66	0x6082 (2682)	50726 → 3000 [ACK] Seq=66 Ack=71 Win=65536 Len=0 TSval=3298708480 TSecr=3298708480
35	1.408897	127.0.0.1	127.0.0.1	TCP	72	0x6083 (2682)	50726 → 3000 [PSH, ACK] Seq=66 Ack=71 Win=65536 Len=6 TSval=3298708480 TSecr=3298708480
36	1.408974	127.0.0.1	127.0.0.1	TCP	73	0x62f1b (9755)	3000 → 50726 [PSH, ACK] Seq=71 Ack=72 Win=65536 Len=7 TSval=3298708480 TSecr=3298708480
37	1.449556	127.0.0.1	127.0.0.1	TCP	66	0x6084 (2682)	50726 → 3000 [ACK] Seq=72 Ack=78 Win=65536 Len=0 TSval=3298708520 TSecr=3298708480
38	1.560919	127.0.0.1	127.0.0.1	TCP	73	0x6085 (2662)	50726 → 3000 [PSH, ACK] Seq=72 Ack=78 Win=65536 Len=7 TSval=3298708632 TSecr=3298708480

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

בצילום זה ניתן לראות כיצד נעשה שימוש באמצעות פרוטוקול TCP לצורך תקשורת בין ה-watchdog ל-better_ping.

Wireshark - Packet 4 - betterping_watchdog.pcap

Frame 4: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)

Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

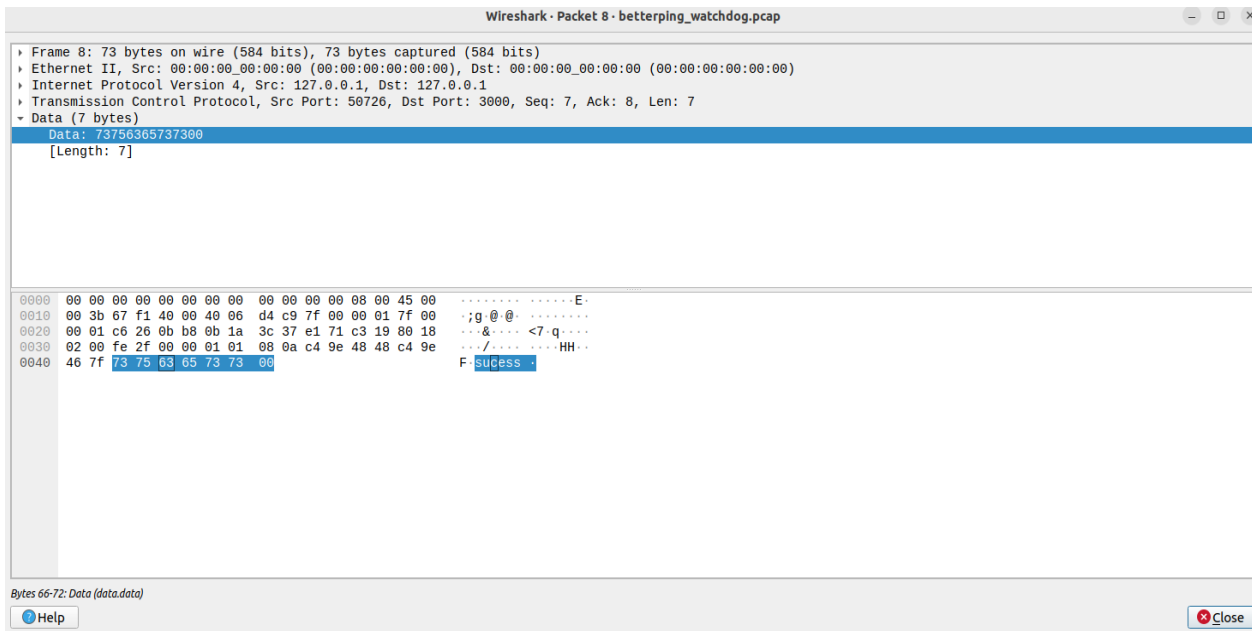
Transmission Control Protocol, Src Port: 50726, Dst Port: 3000, Seq: 1, Ack: 1, Len: 6

Data (6 bytes)

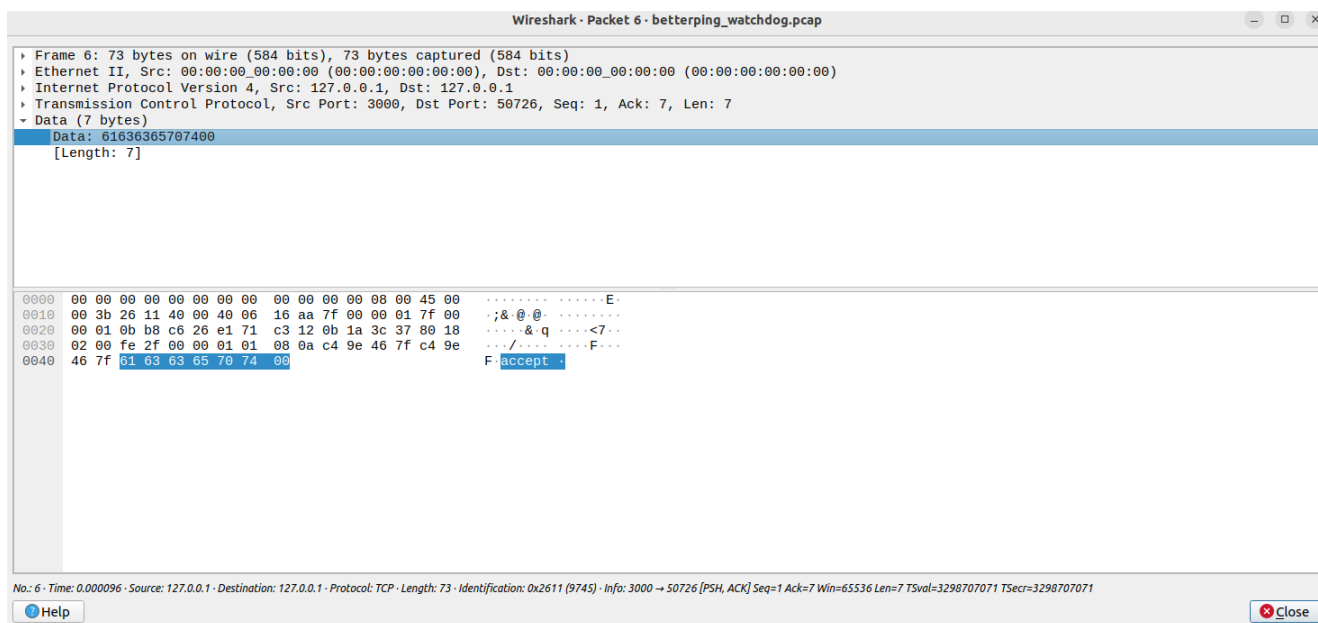
Data: 737461727400
[Length: 6]

0000	00 00 00 00 00 00 00 00	00 00 00 00 08 00 45 00 E..
0010	00 3a 67 ef 40 00 40 06	d4 cc 7f 00 00 01 7f 00	..:g @.
0020	00 01 c6 26 0b b8 0b 1a	3c 31 e1 71 c3 12 80 18	...&... <1 q...
0030	02 00 fe 2e 00 00 01 01	08 0a c4 9e 46 7f c4 9e F...
0040	46 7f 73 74 61 72 74 00		F Start.

בצילום זה ניתן להראות איך כשה-better_ping שולח הודעת start ל-watchdog מייד עם שליחת הודעת ה-ping לגוגל.



בצילום זה ניתן להראות שה – watchdog מקבל הודעת “success” מה-better_ping
הודעה זו אמורה להשלח אליו מייד לאחר קבלת הודעת ה-ping בחזרה מגוגל.



בצילום זה ניתן להראות שה- watchdog שולח הודעת "accept" ל – better_ping
מייד לאחר שהוא מקבל הודעת “start” או “success”.