Web Sockets

WebSockets

Last time we saw how to establish a WebSocket connection

Today, we'll parse and send messages over the socket

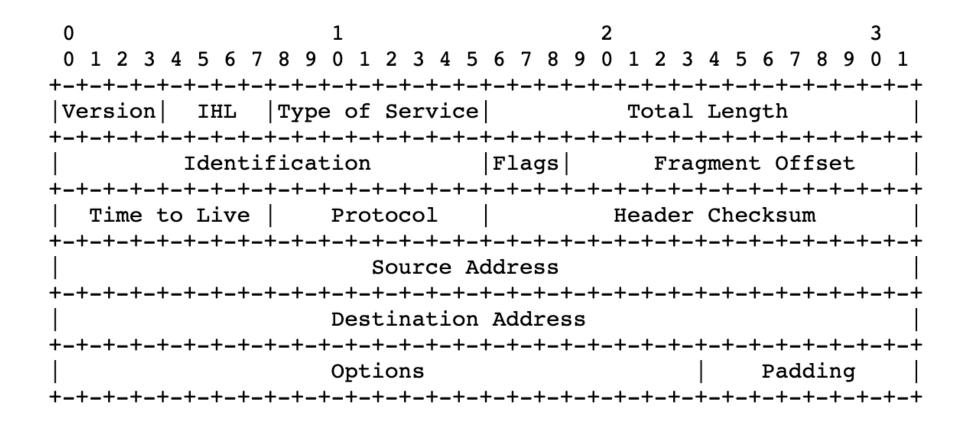
0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
+-	+	+-+	- -+					+-+	+- -							- -															+
F	R	R	R	c	ogo	00	de	M	1	Pay	710	oac	1 :	lei	n			Ex	ĸtε	enc	lec	ı i	pay	710	oac	d 1	Ler	ngt	th		
I	S	S	s		(4	l)		A				(7))									((16	5/6	64)					ĺ
N	v	v	v					S									((if	E 1	pay	710	oac	1	Lei	n==	=12	26/	/12	27))	ĺ
ĺ	1	2	3					K	ĺ																						ĺ
+-	+	+-+	+					+-+	- -																						- +
		I	Ext	er	nde	ed	pa	ay]	Loa	ad	16	enç	gtl	h d	cor	nti	lηι	ied	d,	if	Ę	pay	710	oac	d I	ler	1 =	==	12	27	
<u> </u>																Ma	sk	cir	ıg-	-k∈	у,	, j	Lf	MZ	ASI	Χ :	set	: 1	to	1	
1 1	Mas	ski	ing	j—}	cey	7	(C	ont		nue	ed))									Pá	ay]	Loa	ad	Da	ata	a				
: :	Payload Data continued								- T																						
 +									- •	E	ay	,1c	oa o	d I	Dat	a	cc	nt	ir	iue	ed	•	•	- •	- •		- -	- •	- •		- 1 4

Protocols Sidenote

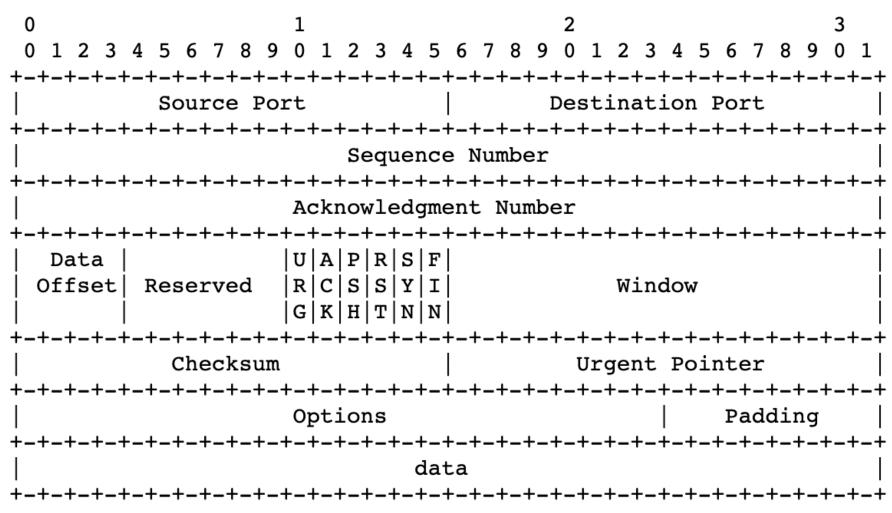
- Many of the protocols used in the Internet define the order and meaning of bits that are sent
 - Sender assembles the bits of a message following the protocol
 - Send the bits through the Internet
 - Receiver interprets the bits following the same protocol to extract meaning from the bits
- Protocols enable communication using only 1's and 0's

Protocols Sidenote

- TCP/IP protocol headers shown hear
- Routers read the IP header following this protocol to know how to route a packet
- Endpoints follow the TCP protocol to assemble a sequence of packets and send it to the process using the given port



Example Internet Datagram Header



- The WebSocket protocol functions the same way
- Client and server agree to follow this protocol
- Send bits in this specific order
 - We can rely on the client following this protocol

	2 3 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-++-+	+
	continued, if payload len == 127
	Masking-key, if MASK set to 1
Masking-key (continued)	Payload Data
: Payload	Data continued
Payload	Data continued

Network Stack

 An IP packet containing a WebSocket frame looks like this

	8	9 0 1 2 3 4 5 6 7 8		0 1 2 3 +-+-+-
	Total Length	pe of Service	on IHL	Version
		ation Flags	Identif	
IP	Header Checksum -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+	Protocol	e to Live	Time t
		Source Address		
		Destination Addre		
	Padding	Options		
	-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Destination Port	Port	Source	i
		Sequence Numb		1
		Acknowledgment Nu		
TOD	-+-+-+-+-+-+-+-+-+-	+-+-+-+-+-+-+-+- U A P R S F		+-+-+-+- Data
ICP	Window	R C S S Y I G K H T N N	j	Offset
	Urgent Pointer	ım	Check	Ī
	-+-+-+-+-+-+-+-+-+-+-+ Padding	Options		Ì
	-+-+-+-+-+-+-	data		
<u>.</u> -	Extended navload length		T-T	T-T-T-T
	Extended payload length (16/64)	(7)	S (4)	F R R R I S S S N V V V
	if payload len==126/127)	(1		1 1 2 3
	ed, if payload len == 127	oad length continue	Extended pa	Ext
WebSocket	ing-key, if MASK set to 1	Maski		
_	Payload Data	inued)	ing-key (co	Masking
- -	ntinued	Payload Data con		: +
-	ntinued	Payload Data con		 +

Parsing Bits

- We will have to read frames at the bit level
 - It's already in a byte array when we receive it
 - We can access any byte and extract the bits we need
 - Helpful to recall that bytes are represented as 8-bit integer values in most languages (0-255)

0	1	2	3
0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7	8 9 0 1
+-+-+-+-		+	+
F R R R opcode $ M $	Payload len	Extended payload len	igth
I S S S (4) $ A $	(7)	(16/64)	
$ \mathbf{N} \mathbf{V} \mathbf{V} \mathbf{V} $		(if payload len==126/	127)
1 2 3 K			İ
+-+-+-+-		+	· +
Extended paylo	ad length co	ntinued, if payload len =	= 127
+			+
		Masking-key, if MASK set	to I
Magking kow (conti		Pauload Data	+
Masking-key (conti	nueu)	Payload Data	
•	Pauload Dat	ta continued	+
• +			· +
	Pavload Dat	ta continued	- +
 +			ا +

Parsing Bits

- Bit Example To read the opcode:
 - get the byte at index 0
 - Bitwise AND (& in most languages) this byte with a "bit mask" of 15
 - Since 15 == 00001111 as a byte this will 0 out the 4 higher order bits
 - We now have an int from 0-15 representing the opcode

0 1 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 +-+-+-+	2 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 -+								
F R R R opcode M Payload len I S S S (4) A (7) N V V V S 1 2 3 K	Extended payload length (16/64) (if payload len==126/127)								
Extended payload length c	ontinued, if payload len == 127								
	Masking-key, if MASK set to 1								
Masking-key (continued)	Payload Data								
Payload Data continued									
Payload Data continued									

- FIN: The finish bit
 - 1 This is the last frame for this message
 - 0 There will be continuation frames containing more data for the same message
- [You can assume this is always 1 for the HW]

0	1	2	3								
0 1 2 3 4 5 6 7 8	9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7	8 9 0 1								
+-+-+-+-	+	+	+								
F R R R opcode M	Payload len	Extended payload len	gth								
	i (7)	(16/64)	į								
$ \mathbf{N} \mathbf{V} \mathbf{V} \mathbf{V} $	İ	(if payload len==126/	127)								
1 2 3 K	İ	j `	ĺ								
+-+-+-+-	+	+	÷								
Extended pay	load length co	ntinued, if payload len =	= 127								
+		+									
]		Masking-key, if MASK set	to 1								
Macking kow (con	 +inuod\	Tavload Data	+								
Masking-key (con	cinued)	Payload Data									
•	Pavload Da	ta continued	+								
· +			· +								
·	Pavload Da	ta continued	- +								
I ∔	rayioad Da	ca concinued	<u> </u>								

- RSV: Reserved bits
 - Used to specify any extensions being used
- [You can assume these are always 000 for the HW]

0 1	2 3								
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5	5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1								
+-+-+-+	-++								
F R R R opcode M Payload len	Extended payload length								
I S S S (4) $ A $ (7)	(16/64)								
N V V V S	(if payload len==126/127)								
1 2 3 K									
+-+-+-+	-+ +								
Extended payload length co	ontinued, if payload len == 127								
+	++								
	Masking-key, if MASK set to 1								
Masking-key (continued)	Payload Data								
+	+								
: Pavload Da	ata continued								
+	+								
Payload Da	ata continued								
<u> </u>	<u> </u>								

- opcode: Operation code
 - Specifies the type of information contained in the payload
 - Ex: 0001 for text, 0010 for binary, 1000 to close the connection
- You can assume this is always 0001 for the HW]

0	1	2	3								
0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7	8 9 0 1								
+-+-+-+	+-+	+	+								
F R R R opcode I S S S (4) N V V V 1 2 3 +-+-+-+	e M Payload len A (7) S K	Extended payload ler (16/64) (if payload len==126/	į								
Extended p	ayload length co	ontinued, if payload len == 127									
		Masking-key, if MASK set	to 1								
Masking-key (c	ontinued)	Payload Data									
Payload Data continued											
	Payload Dat	ta continued									

- MASK: Mask bit
 - Set to 1 if a mask is being used
 - Set to 0 if no mask is being used
- This will be 1 when receiving messages from a client

0	1	2 6 7 8 9 0 1 2 3 4 5 6 7	3							
+-+-+-+	+-+	+	t							
I S S S (4) N V V V 1 2 3 +-+-+-+	s K +-+	Extended payload len (16/64) (if payload len==126/ +	127) 							
		Masking-key, if MASK set	to 1							
Masking-key (c	ontinued)	Payload Data	 							
: +	Payload Data continued									
+	Payload Da	ta continued	₋							

- The next bits will represent payload length in bytes
 - Similar to Content-Length
- The length can be represented in 7, 16, or 64 bits

0	1	2	3								
0 1 2 3 4 5 6 7 8	9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7	8 9 0 1								
+-+-+-+-		+	+								
F R R R opcode $ M $	Payload len	Extended payload len	igth								
I S S S (4) $ A $	(7)	(16/64)									
$ \mathbf{N} \mathbf{V} \mathbf{V} \mathbf{V} $ S		(if payload len==126/	127)								
1 2 3 K											
+-+-+-+-		+	· +								
Extended pay	oad length co	ontinued, if payload len == 127 \mid									
+		+									
 		Masking-key, if MASK set to 1									
Masking-key (cont	inued)	Payload Data									
+			· +								
•	Payload Da	ata continued									
+			+								
	Payload Da	ata continued									
+			·+								

- If the length is <126 bytes
 - The length is represented in 7 bits, sharing a byte with the MASK bit
 - The next bit after the length is either the mask or payload

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
+	+-+		+-+	 -				+ –+	- -						1																-+
F	R	R	R	c	opo	00	de	M	:	Pa	yl	oac	1 :	lei	n			Εz	κte	enc	ded	ı b	pay	710	oac	1	Ler	ıgt	:h		
I	s	S	s		(4	!)		A				(7))									((16	5/6	64)					
N	V	V	V					s									((i1	E	pay	710	oac	ı i	Lei	n==	=12	26/	/12	27)		
	1	2	3					K																							
+	+-+		+-+	- - -				+ –+	- - -						1	- -															- +
		I	Ext	er	nde	ed	рā	ay]	Lo	ad	1	enç	jtl	n o	cor	ıti	Ĺηι	iec	ı,	ií	f 1	pay	γlo	oac	d I	Ler	n =	==	12	27	
+ -															- +																+
																Ma	ısl	cir	ıg-	-k€	ЭУ.	, :	Ĺf	M	ASI	Χ 5	set	t t	co	1	
+															+																+
1	4as	k:	inç	j-k	сеу	7	(C	ont	i	nu	ed)									Pä	ау:	Loa	ad	Da	ata	a				
+																															- +
:										_]	Pay	ylc	oac	d I	at	a	CC	ont	cir	nue	ed	•	• •								:
	_		_	_	_	•		_		_ :	Pay	ylc	oa o	d I	oat	a	c	ont		nue	ed	•		-				-		_	
Τ																															+

- If the length is >=126 and <65536 bytes
 - The 7 bit length will be exactly 126 (1111110)
 - The next 16 bits represents the payload length

0	1	2 3									
0 1 2 3 4 5 6 7 8	9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1									
+-+-+-+-		+									
F R R R opcode $ M $	Payload len	Extended payload length									
I S S S (4) $ A $	(7)	(16/64)									
N V V V S		(if payload len==126/127)									
1 2 3 K											
+-+-+-+-		+									
Extended pay	oad length co	ontinued, if payload len == 127									
+		+									
		Masking-key, if MASK set to 1									
Masking-key (cont	inued)	Payload Data									
+											
•	Pavload Da	ta continued									
· +											
	Pavload Da	ata continued									
+											

- If the length is >=65536 bytes
 - The 7 bit length will be exactly 127 (1111111)
 - The next 64 bits represents the payload length
 - 18,446,744,073,709,551,615 max length
 - 16 exabytes / 16,000,000 terabytes

0	1	2	3
	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7	8 9 0 1
I S S S (4)	•	Extended payload len (16/64) (if payload len==126/	127) +
+	ayload length cor	ntinued, if payload len == +	= 127 +
		Masking-key, if MASK set	to 1
Masking-key (co	ontinued)	Payload Data	 +
Payload Data continued			
·	Payload Dat	ta continued	

- To read the frame length, read the 7 bit length
 - If the value is 126, read the next 16 bits as the length
 - If the value is 127, read the next 64 bits as the length
 - Else, the value itself is the length

0 1	2 3		
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1		
+-+-+	++		
F R R R opcode M Payload len	Extended payload length		
I S S S (4) $ A $ (7)	(16/64)		
N V V V S	(if payload len==126/127)		
1 2 3 K			
+-+-+	+ +		
Extended payload length continued, if payload len == 127			
+	Magking kov if MACK got to 1		
 +	Masking-key, if MASK set to 1		
Masking-key (continued)	Payload Data		
Masking-key (Continued)			
: Payload Da	ta continued :		
+	+		
Pavload Da	ta continued		
i ajiouu bu			

- After all the length bits:
 - If the MASK bit == 1, the next 4 bytes (32 bits) is the mask
 - If the MASK bit == 0, the payload begins

0	1	2	3
0 1 2 3 4 5 6 7 8	9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7	8 9 0 1
+-+-+-+-		+	+
F R R R opcode $ M $	Payload len	Extended payload len	gth
I S S S (4) $ A $	(7)	(16/64)	
N V V V S		(if payload len==126/	127)
1 2 3 K			
+-+-+-+-		+	+
Extended pay	oad length co	ntinued, if payload len =	= 127
+		+	+
		Masking-key, if MASK set	to 1
Masking-key (conf	inued)	Pavload Data	+
Masking-key (continued) Payload Data			
Payload Data continued			
· +			+
· 	Pavload Da	ta continued	i
+			, ++

- If there is a mask, read these 4 bytes
- The mask will be randomly generated by the client for each message
 - You must parse this each time a message is received

0 1		2	3	
0 1 2 3 4 5 6 7 8 9 0	1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7	8 9 0 1	
+-+-+-+		+	+	
F R R R opcode M Pay:	load len	Extended payload len	gth	
I S S S (4) $ A $	(7)	(16/64)		
N V V V S		(if payload len==126/	127)	
1 2 3 K				
+-+-+-+		+	+	
Extended payload	length co	ntinued, if payload len =	= 127	
+		Magking kow if MACK got	+ +0 1	
 +		Masking-key, if MASK set	+	
Masking-key (continued	۲) ۲۱	Payload Data		
+	., 		+	
• P:	Payload Data continued			
+			+	
Pa	avload Dat	ta continued	i	
+			 ++	

- Each 4 bytes of the payload has been XORed with the mask by the client
- Read the payload 4 bytes at a time and XOR the bytes with the mask
- If the length is not a multiple of 4, use only the bytes of the mask that are needed
 - le. Always reading 4 bytes will cause an index out of bounds error

0 1		2	3	
0 1 2 3 4 5 6 7 8 9 0	1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7	8 9 0 1	
+-+-+-+		+	+	
F R R R opcode M Pay:	load len	Extended payload len	gth	
I S S S (4) $ A $	(7)	(16/64)		
N V V V S		(if payload len==126/	127)	
1 2 3 K				
+-+-+-+		+	+	
Extended payload	length co	ntinued, if payload len =	= 127	
+		Magking kow if MACK got	+ +0 1	
 +		Masking-key, if MASK set	+	
Masking-key (continued	۲) ۲۱	Payload Data		
+	., 		+	
• P:	Payload Data continued			
+			+	
Pa	avload Dat	ta continued	i	
+			 ++	

XOR Example

- If 4 bytes of the message are:
 - 01001001_01000011_01010101_00100001
- And the random mask is:
 - 01111011_00100010_01110101_01110011
- This part of the payload will be "message XOR mask":
 - 00110010_01100001_00100000_01010010
- When we receive these bits and XOR it with the mask again we get the original message bits:
 - 01001001_01000011_01010101_00100001

- Once the payload is XORed with the mask 4 bytes at time we get the entire message
- Then process the message

0	1	2	3
0 1 2 3 4 5 6	7 8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8	9 0 1
+-+-+-+-	+-+	+	+
F R R R opcod	de M Payload len	Extended payload lengt	:h
I S S S (4)	A (7)	(16/64)	
N V V V	s	(if payload len==126/12	27)
1 2 3	K		
+-+-+-+	+-+	+	. – – +
Extended	payload length com	ntinued, if payload len ==	127
+		+	+
		Masking-key, if MASK set t	:o 1
+		+	+
Masking-key ((continued)	Payload Data	
+			
Payload Data continued			
	Payload Da	ta continued	+
+			+

- To send a message to a client:
 - Use this same protocol
 - Assemble a byte array with the appropriate values
 - Append your payload as bytes

0	1	2	3
0 1 2 3 4 5 6 7 8	9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8	8 9 0 1
+-+-+-+-+-		+	+
F R R R opcode $ M $	Payload len	Extended payload leng	gth
I S S S (4) $ A $	(7)	(16/64)	
$ \mathbf{N} \mathbf{V} \mathbf{V} \mathbf{V} $ S		(if payload len==126/1	127)
1 2 3 K			j
+-+-+-+-		+	+
Extended payl	oad length co	ntinued, if payload len ==	= 127
		Masking-key, if MASK set	to 1
+			-
Payload Data continued			
	Payload Da	ta continued	

- Do not use a mask when sending frames to a client
 - No caching concerns on server to client frames

0	1	2	3
0 1 2 3 4 5 6 7 8	9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8 9	0 1
+-+-+-+-		+	+
– .	Payload len	Extended payload length	1
I S S S (4) $ A $	(7)	(16/64)	
$ \mathbf{N} \mathbf{V} \mathbf{V} \mathbf{V} $ s		(if payload len==126/127	')
1 2 3 K			
+-+-+-+-		+	+
Extended pay	load length co	ntinued, if payload len == 1	L 2 7
+		+	+
		Masking-key, if MASK set to) 1
Masking-key (con	inued)	Payload Data	+
Masking-key (continued) Payload Data			
· •	Pavload Da	ta continued	:
+			+
	Payload Da	ta continued	- 1
· +			+

- Example: For our purposes in the HW
 - FIN is always 1
 - RSVs are always 0
 - opcode is always 0001 (Sending text)
- Therefore, the first byte is always 10000001 == 129

0 0 1 2 3 4 5 6 7 8 5		2 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0	1
	Payload len (7)	Extended payload length (16/64) (if payload len==126/127)	
Extended payle	oad length co	ntinued, if payload len == 127	
<u>i</u>		Masking-key, if MASK set to 1	
Masking-key (cont	inued)	Payload Data	
Payload Data continued			
	Payload Da	ta continued	- +

- Check the length of your payload to determine how many bits are needed for the length
- Follow the same format for payload length as the received messages

0	1	2	3
0 1 2 3 4 5 6 7 8	9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7	8 9 0 1
+-+-+-+-		+	+
F R R R opcode $ M $	Payload len	Extended payload len	gth
I S S S (4) $ A $	(7)	(16/64)	
N V V V S		(if payload len==126/	127)
1 2 3 K			
+-+-+-+-		+	+
Extended pay	oad length co	ntinued, if payload len =	= 127
+		+	+
		Masking-key, if MASK set	to 1
Masking-key (conf	inued)	Pavload Data	+
Masking-key (continued) Payload Data			
Payload Data continued			
· +			+
· 	Pavload Da	ta continued	i
+			, ++

- MASK bit is 0 and there are not mask bytes
 - After payload length, immediately add the bytes of the payload

0	1	2 3		
0 1 2 3 4 5 6 7 8	9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 3	1	
+-+-+-+-		·+	-+	
F R R R opcode $ M $	Payload len	Extended payload length		
I S S S (4) $ A $	(7)	(16/64)		
N V V V S		(if payload len==126/127)		
1 2 3 K				
+-+-+-+-		.+	+	
Extended pay	oad length co	ntinued, if payload len == 127		
+		+	- +	
		Masking-key, if MASK set to 1		
Masking-key (conf	Magking kov (continued)			
Masking-key (continued) Payload Data				
•	Payload Data continued			
+			+	
	Pavload Da	ta continued	İ	
+			_+	