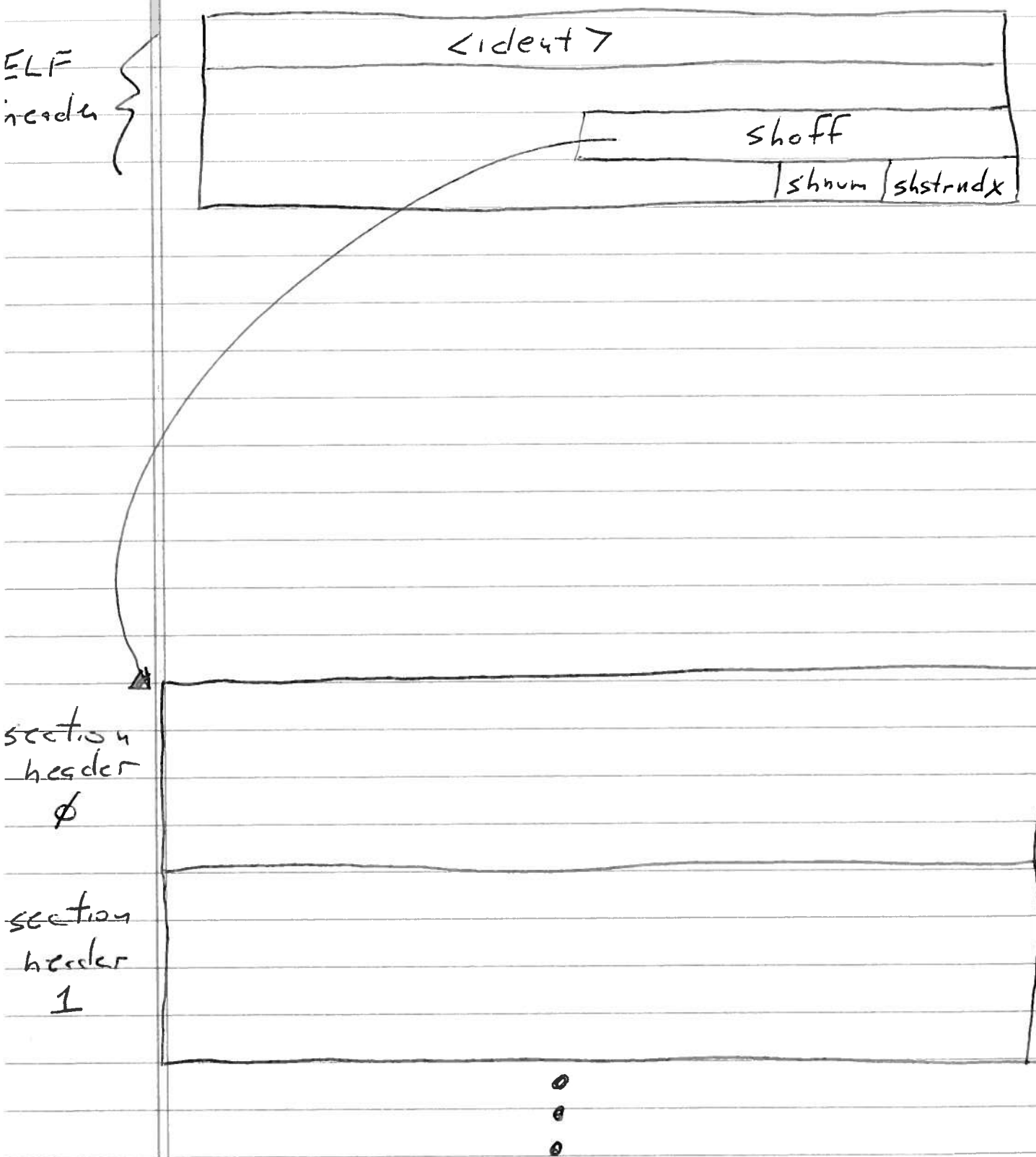
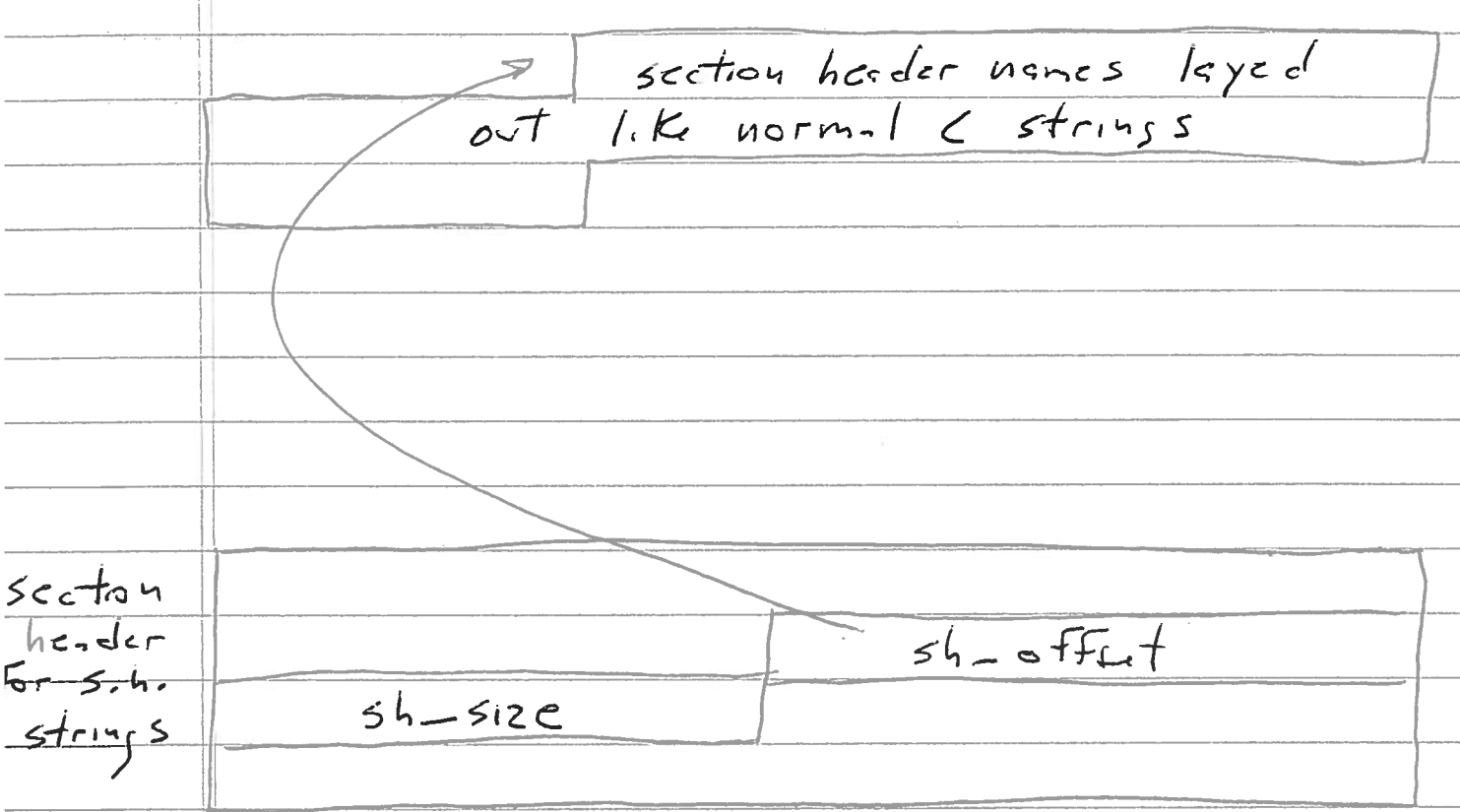
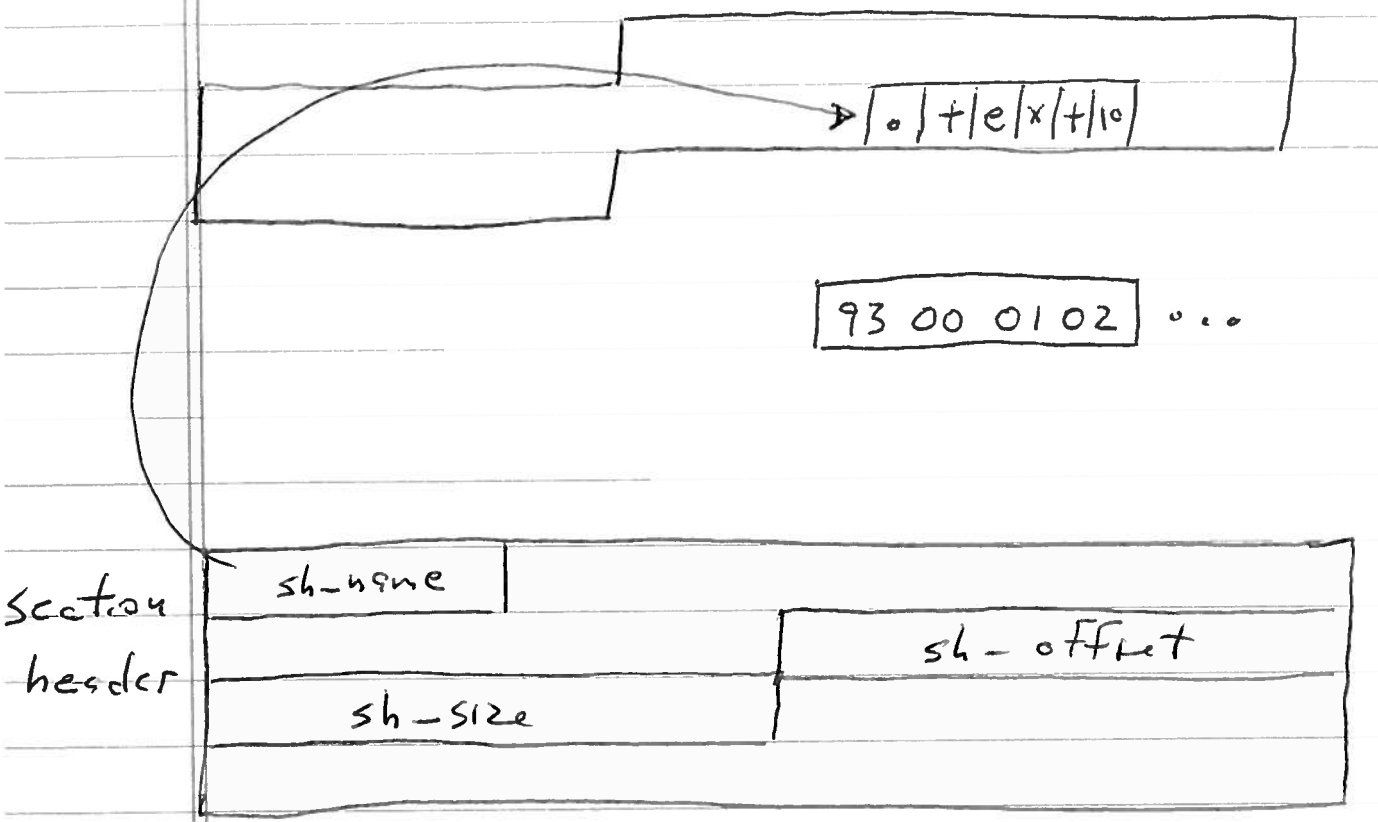
How To Find The Code

need to find the .text section

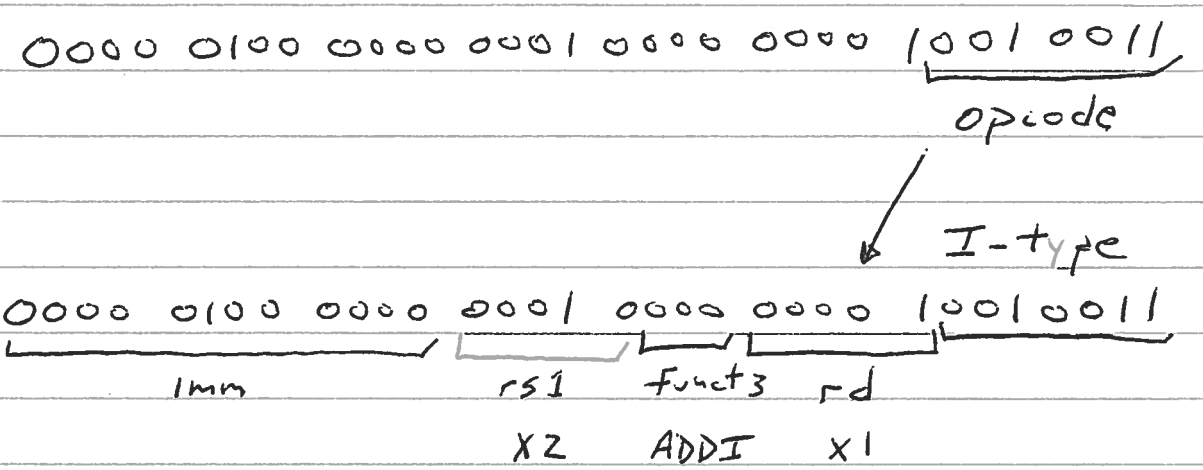



section header names layed
out like normal C strings
section
header
for s.h.
strings
sh_offset
sh_size


.|t|e|x|t|10
93 00 0102 ...
section header
sh_name
sh_offset
sh_size

Decoding Instructions

ex 93 | 00 | 01 | 04 ⇒ 04010093



addi X1 X2, 64

ex

fe588ea3

1111 1110010 1000 1000 1110 1010 0011

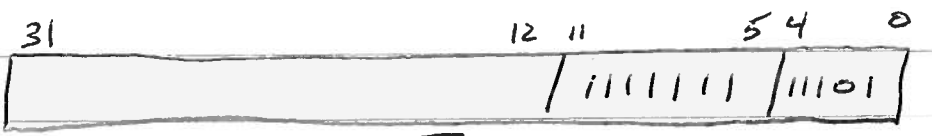
↳ S-type

1111 1110 0101 1000 1000 1110 1010 0011

imm[11:5] rs2 rs1 funct3 imm[4:0]

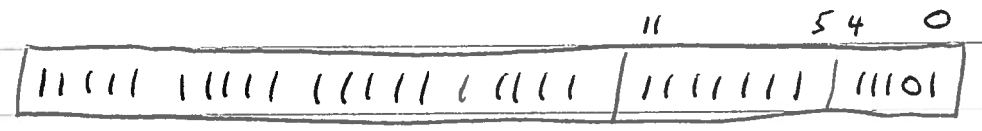
X5 X17 SB

need to put the two pieces together for the immediate constant



what about these?

↳ need to perform sign extension



replicate this bit across the top

sb x17, x5, -3

note in assembly language this is specified:

sb x5, -3(x17)

31 27	26 25	24 20	19 15	14 12	11 7	6 0	
funct7		rs2	rs1	funct3	rd	opcode	R-type
imm[11:0]			rs1	funct3	rd	opcode	I-type
imm[11:5]		rs2	rs1	funct3	imm[4:0]	opcode	S-type
imm[12|10:5]		rs2	rs1	funct3	imm[4:1|11]	opcode	SB-type
imm[31:12]					rd	opcode	U-type
imm[20|10:1|11|19:12]					rd	opcode	UJ-type

RV32I Base Instruction Set

imm[31:12]			rd	0110111	LUI rd,imm
imm[31:12]			rd	0010111	AUIPC rd,imm
imm[20|10:1|11|19:12]			rd	1101111	JAL rd,imm
imm[11:0]	rs1	000	rd	1100111	JALR rd,rs1,imm
imm[12|10:5] rs2	rs1	000	imm[4:1|11]	1100011	BEQ rs1,rs2,imm
imm[12|10:5] rs2	rs1	001	imm[4:1|11]	1100011	BNE rs1,rs2,imm
imm[12|10:5] rs2	rs1	100	imm[4:1|11]	1100011	BLT rs1,rs2,imm
imm[12|10:5] rs2	rs1	101	imm[4:1|11]	1100011	BGE rs1,rs2,imm
imm[12|10:5] rs2	rs1	110	imm[4:1|11]	1100011	BLTU rs1,rs2,imm
imm[12|10:5] rs2	rs1	111	imm[4:1|11]	1100011	BGEU rs1,rs2,imm
imm[11:0]	rs1	000	rd	0000011	LB rd,rs1,imm
imm[11:0]	rs1	001	rd	0000011	LH rd,rs1,imm
imm[11:0]	rs1	010	rd	0000011	LW rd,rs1,imm
imm[11:0]	rs1	100	rd	0000011	LBU rd,rs1,imm
imm[11:0]	rs1	101	rd	0000011	LHU rd,rs1,imm
imm[11:5] rs2	rs1	000	imm[4:0]	0100011	SB rs1,rs2,imm
imm[11:5] rs2	rs1	001	imm[4:0]	0100011	SH rs1,rs2,imm
imm[11:5] rs2	rs1	010	imm[4:0]	0100011	SW rs1,rs2,imm
imm[11:0]	rs1	000	rd	0010011	ADDI rd,rs1,imm
imm[11:0]	rs1	010	rd	0010011	SLTI rd,rs1,imm
imm[11:0]	rs1	011	rd	0010011	SLTIU rd,rs1,imm
imm[11:0]	rs1	100	rd	0010011	XORI rd,rs1,imm
imm[11:0]	rs1	110	rd	0010011	ORI rd,rs1,imm
imm[11:0]	rs1	111	rd	0010011	ANDI rd,rs1,imm
0000000 shamt	rs1	001	rd	0010011	SLLI rd,rs1,shamt
0000000 shamt	rs1	101	rd	0010011	SRLI rd,rs1,shamt
0100000 shamt	rs1	101	rd	0010011	SRAI rd,rs1,shamt
0000000 rs2	rs1	000	rd	0110011	ADD rd,rs1,rs2
0100000 rs2	rs1	000	rd	0110011	SUB rd,rs1,rs2
0000000 rs2	rs1	001	rd	0110011	SLL rd,rs1,rs2
0000000 rs2	rs1	010	rd	0110011	SLT rd,rs1,rs2
0000000 rs2	rs1	011	rd	0110011	SLTU rd,rs1,rs2
0000000 rs2	rs1	100	rd	0110011	XOR rd,rs1,rs2
0000000 rs2	rs1	101	rd	0110011	SRL rd,rs1,rs2
0100000 rs2	rs1	101	rd	0110011	SRA rd,rs1,rs2
0000000 rs2	rs1	110	rd	0110011	OR rd,rs1,rs2
0000000 rs2	rs1	111	rd	0110011	AND rd,rs1,rs2
0000 pred succ	00000	000	00000	0001111	FENCE
0000 0000 0000	00000	001	00000	0001111	FENCE.I
000000000000	00000	000	00000	1110011	SCALL
000000000001	00000	000	00000	1110011	SBREAK
110000000000	00000	010	rd	1110011	RDCYCLE rd
110010000000	00000	010	rd	1110011	RDCYCLEH rd
110000000001	00000	010	rd	1110011	RDTIME rd
110010000001	00000	010	rd	1110011	RDTIMEH rd
110000000010	00000	010	rd	1110011	RDINSTRET rd
110010000010	00000	010	rd	1110011	RDINSTRETH rd