From Zero to Hero

Digital Forensics 1.0.1

Michael Hamm - CIRCL

TLP:CLEAR

Exercises 1.0.1

2.3 Interpreting binary data: Signed Integer

```
  1 1 0 1 0 0 0 0
  ---------------

+
-----------------
```

Two's complement of 108:

1. Invert all single bits
2. Add the value 00000001

3. Convert to Decimal:

2.4 Challenge: 1 byte signed Integer

- Biggest possible positive number

  —>

- Smalest possible positive number

  —>

- Biggest possible negative number

  _____

  _____ —>

- Smalest possible negative number

  _____

  _____ —>

2.5 From Bin to Hex

Example:

0001 1000	0101 0101	0000 1111	1010 0110
1 8	5 5	0 F	A 6

Exercise:

1001 0110	1010 0101	0000 1111	1100 0011

2.6 Exercise: Little Endian

Read and interpret this little endian 2 byte 'word'

```
          -------------
0x96A5 | 9 6 | A 5 |
          -------------
```

```
          -------------
0x        |     |     | =
          -------------
```

2.6 Exercise: Little Endian

Read and interpret this little endian 'double word'

```
                 -------------------------
0xF41B0201       | F 4 | 1 B | 0 2 | 0 1 |
                 -------------------------
```

```
                 -------------------------
0x               |     |     |     |     | =
                 -------------------------
```

2.8 Data structures: Exercise: Your turn

```
 0                               8                               16
|44|46|45|41|08|0E|00|FF|74|65|73|74|2E|74|78|74|22|48|65|6C|6C|6F|20|57|
| D  F  E  A| 8|  14 |-1| t  e  s  t  .  t  x  t |"  H  e  l  l  o     W

 24                              32                              40
|6F|72|6C|64|22|0D|44|46|45|41|07|11|00|00|64|66|69|72|2E|36|34|52|45|5A|
  o  r  l  d  " CR|

 48                              56                              64
|4A|55|69|42|79|64|57|78|6C|65|69|34|4B|0A|FF|FF|FF|FF|  |  |  |  |  |  |
```

```
Offset  Size  Description
     0     4  Header signature (ASCII: DFEA - Digital Forensics EDU Archive)
     4     1  Lenght of file name (Integer)
     5     2  Lenght of data (Little Endian)
     7     1  Type of data (Signed Integer)    (-1 = ASCII; 0 = base64 encoded)
     8   --   Variable file name (ASCII)
    9++  --   Data (Binary)
_    EOF   4  EOF signature (Binary: FF FF FF FF)
```

3.2 Master Boot Record & Partitioned Disk

```
00000000: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
...
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001b0: 0000 0000 0000 0000 ce69 d7db 0000 00f5  .........i......
000001c0: 2e08 0751 0110 8032 0200 80cd 0100 0000  ...Q...2........
000001d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

```
Partitiontable:
  Offset: 0      Size: 1 Value: 0x80      --> Bootable
  Offset: 1      Size: 3 Value:           --> Starting CHS address
  Offset: 4      Size: 1 Value: 0x0b      --> FAT32
                                0x07      --> NTFS
  Offset: 5      Size: 3 Value:           --> Ending CHS address
  Offset: 8      Size: 4 Value:           --> Starting LBA address (Little Endian)
  Offset:12      Size: 4 Value:           --> LBA size in sectors  (Little Endian)
```

Exercise: Calculate partition Start and Size: