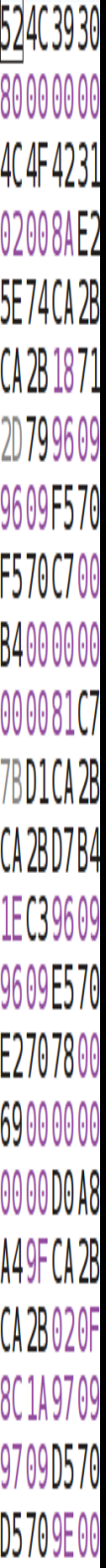
REVERSE-ENGINEERING FILE FORMATS

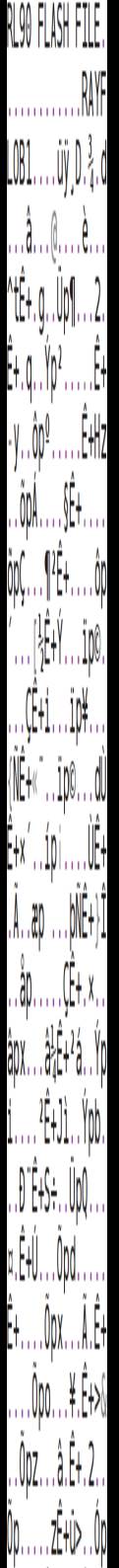
BERNHARD R. FISCHER

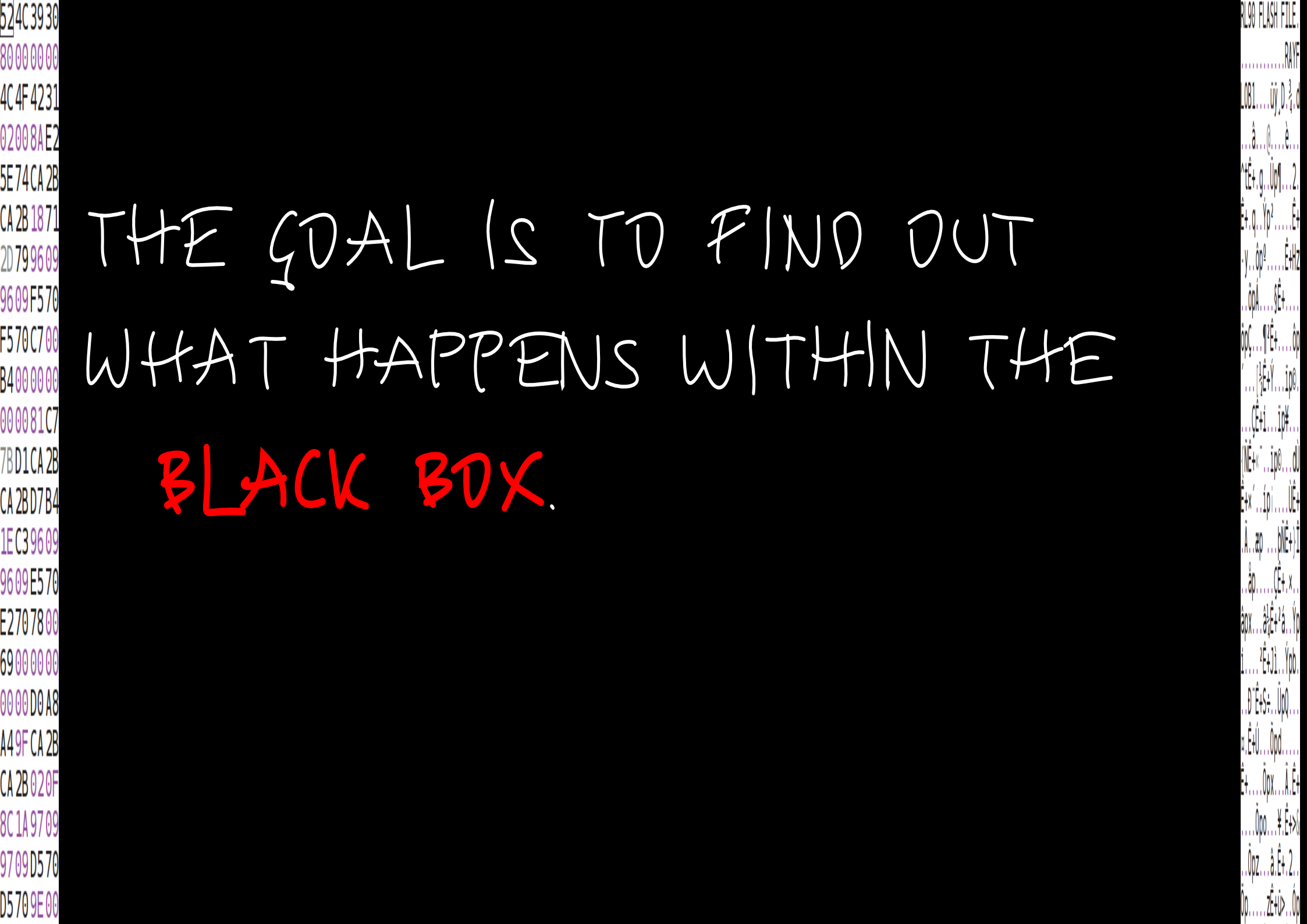
1024D/6202946 <BERNHARD.FISCHER@FHSTP.AC.AT>

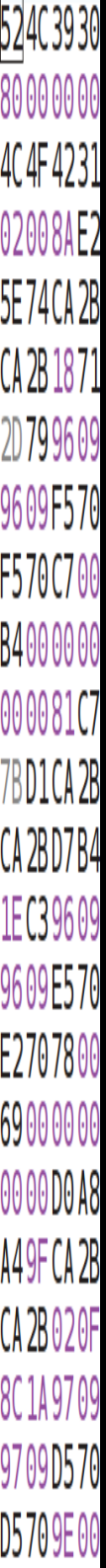


MORE SPECIFICALLY...

REVERSE-ENGINEERING BINARY FILE FORMATS AND THE RAYMARINE ARCHIVE.FSH FORMAT.



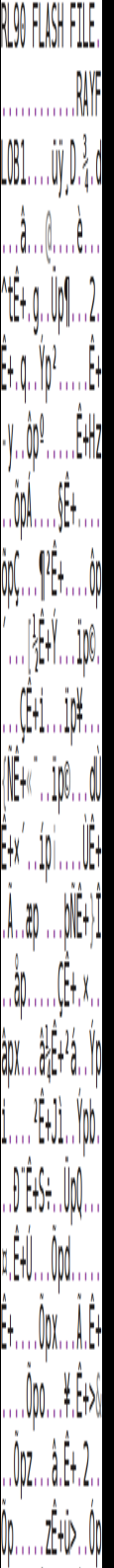

THE GOAL IS TO FIND OUT
WHAT HAPPENS WITHIN THE
BLACK BOX.



- EXECUTABLES ARE DYNAMIC.
  THEY CAN BE EXECUTED.

- DATA IS STATIC!
  IT DOESN'T DO ANYTHING.

-> THIS CHANGES THE METHOD OF REVERSE-ENGINEERING!



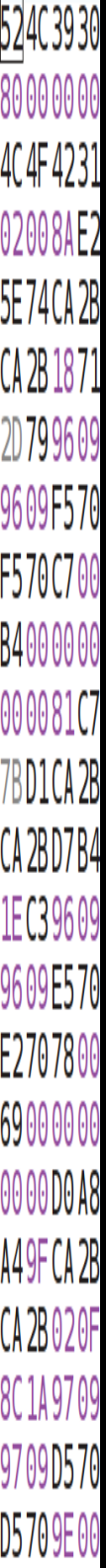
WHY REVERSE-ENGINEERING?

- VALUABLE DATA MAY BE STORED WITHIN FILES.
- COMMERCIAL SOFTWARE MAY BE UNSUITABLE.

CLASSES OF ATTACK

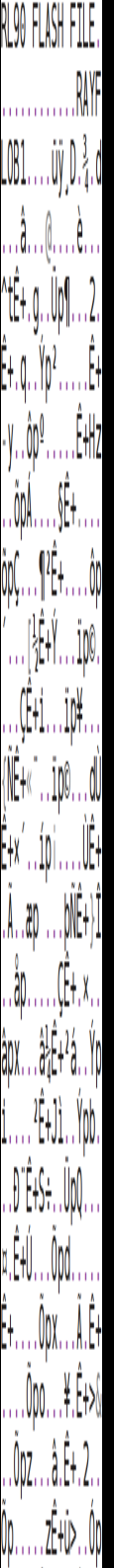
CRYPTOGRAPHY KNOWS ABOUT

- CIPHERTEXT ONLY
- KNOWN PLAINTEXT
- CHOSEN CIPHERTEXT
- CHOSEN PLAINTEXT



DON'T BLINDLY START STARING AT THE HEX CODE!

TURN IT INTO A CHOSEN PLAINTEXT ATTACK!



PREPARATORY WORK

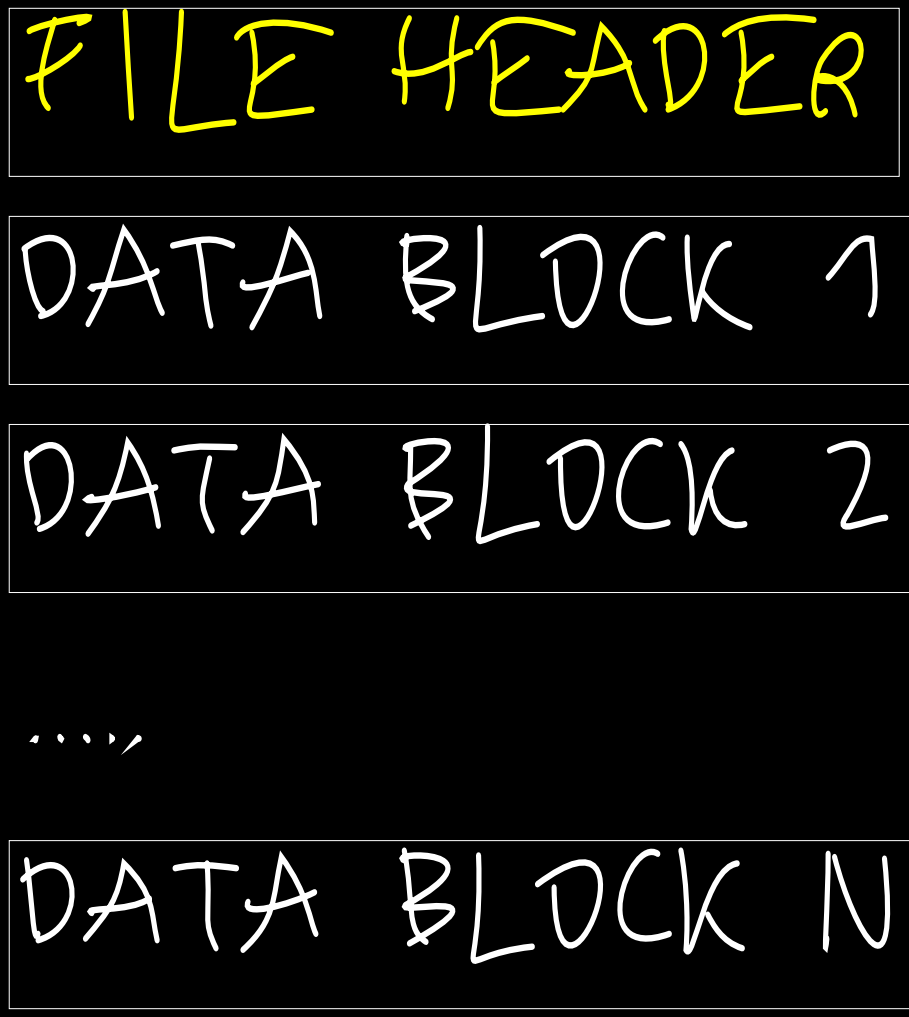
1.) UNDERSTAND THE CONTEXT!

2.) SEARCH FOR

RELATED WORK!

3.) SEARCH FOR TOOLS

GENERAL FILE STRUCTURE



GENERAL HINTS

PEOPLE ARE GOOD IN PATTERN RECOGNITION!

- FIND A GLOBAL FILE STRUCTURE
- LOOK FOR REPEATING PATTERNS
- REFINE STRUCTURE ITERATIVELY
- FIND LENGTH OF GLOBAL STRUCTURES
- COLLECT FILES, TEST YOUR FORMAT HYPOTHESIS

MORE HINTS

- FIND LENGTH OF LOCAL STRUCTURES
- FIND BEGINNING/END OF STRUCTURES
- FIND ENDIANESS
- FIND FIELDS OF STRUCTURES
- VARIABLE LENGTH FIELDS HAVE
  - -> A LENGTH FIELD
  - -> OR A DELIMITER

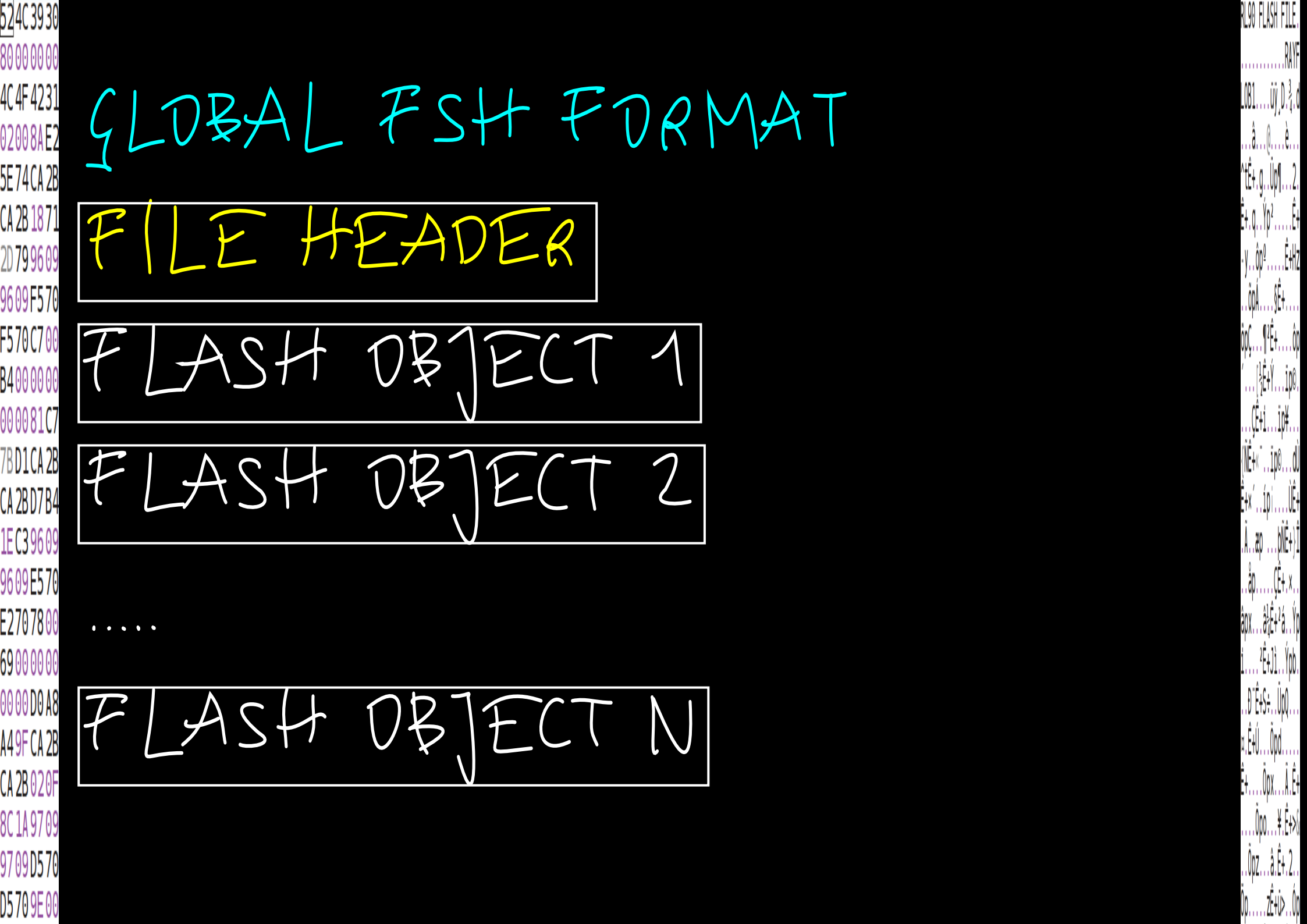
RAYMARINES FSH FORMAT

- SAVES MARINE GPS TRACKS.
- CREATED WITH CHART PLOTTERS.

PEOPLE WANT TO SEE THEIR TRACKS IN GOOGLE EARTH AND OSM.

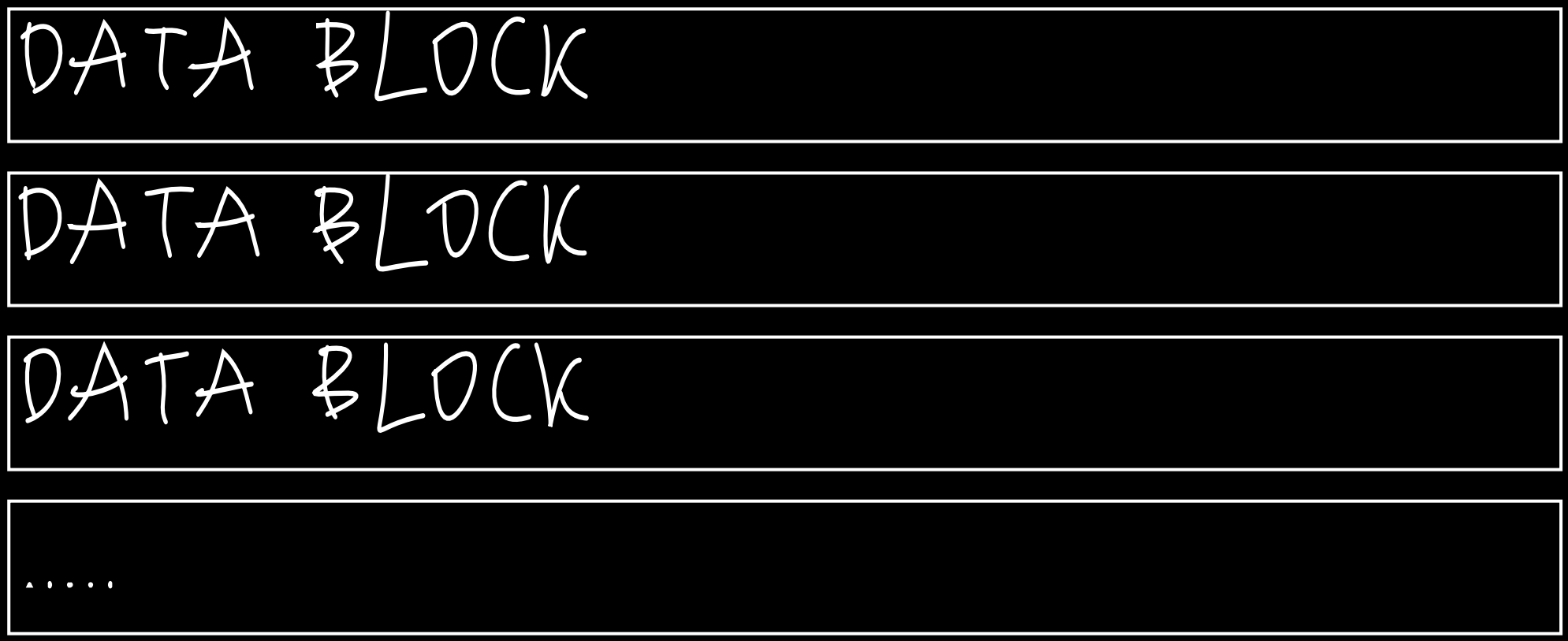
ABOUT THE ARCHIVE.FSH

- THE FORMAT CONTAINS GEOGRAPHIC DATA.
- A GUY IN THE USA WROTE A PYTHON SCRIPT.
- RAYMARINE'S SOFTWARE CAN READ/WRITE IT (OF COURSE...).
- CLOSED SOURCE GPS-UTILITY CAN READ/WRITE IT.
  -> BETA VERSION FOR DOWNLOAD.


GLOBAL FSH FORMAT
FILE HEADER
FLASH OBJECT 1
FLASH OBJECT 2
.....
FLASH OBJECT N

FLOB FORMAT

EVERY FLOB HAS THE SAME FIXED SIZE OF 0X10000 BYTES



BLOCK FORMAT:

IS IT HEADER PLUS DATA?

DATA BLOCKS HAVE A VARIABLE LENGTH

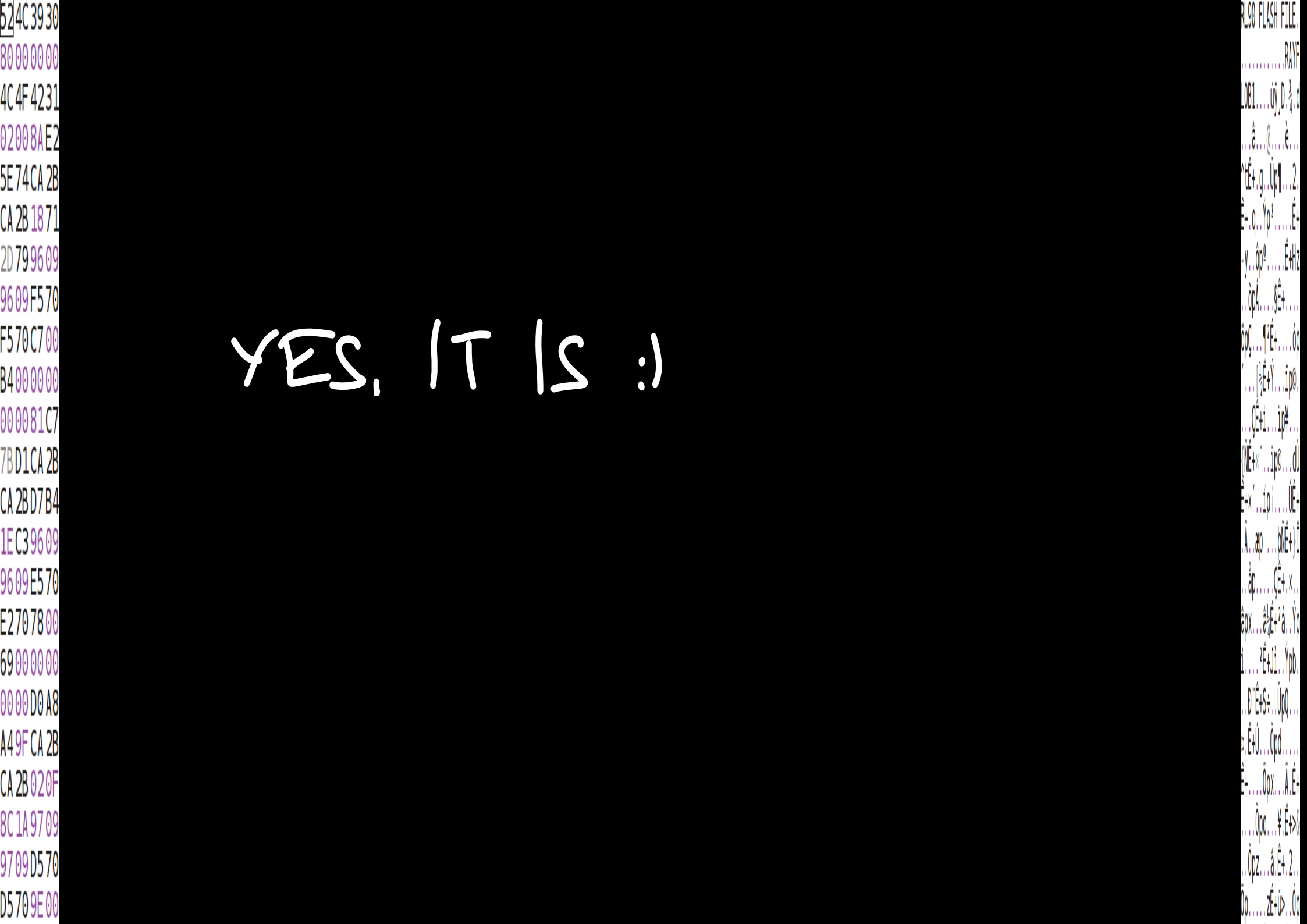
-> LENGTH ENCODED?

-> END MARKER?

SERVERAL KINDS OF DATA CAN BE STORED:

- TRACKS, WAYPOINTS, ROUTES, GROUPS OF WAYPOINTS, ...

-> TRACK TYPE?


YES, IT IS :)

THE TRACK FORMAT 1

- FIND THE RECORD LENGTH
- FIND THE BEGINNING AND THE END!
- IS THERE A HEADER?
- FIND THE FIELDS OF EACH RECORD

THE TRACK FORMAT 2

- FIND THE RECORD LENGTH
  - -> FOUND EASY IN THE HEXCODE
- FIND THE BEGINNING AND THE END!
- IS THERE A HEADER?
- FIND THE FIELDS OF EACH RECORD

THE TRACK FORMAT 3

- FIND THE RECORD LENGTH
- FIND THE BEGINNING AND THE END!
  -> SUPPORTED BY A NIFTY TOOL
- IS THERE A HEADER?
- FIND THE FIELDS OF EACH RECORD

THE TRACK FORMAT 4

- FIND THE RECORD LENGTH
- FIND THE BEGINNING AND THE END!
- IS THERE A HEADER?
  -> THERE ARE BYTES BETWEEN BLOCK HEADER AND TRACK POINTS
- FIND THE FIELDS OF EACH RECORD

THE TRACK FORMAT 5

- FIND THE RECORD LENGTH
- FIND THE BEGINNING AND THE END!
- IS THERE A HEADER?
- FIND THE FIELDS OF EACH RECORD
  -> THERE MUST BE AT LEAST LATITUDE AND LONGITUDE

NUMERIC FIELDS

- HAVE AN ENDIANESS
- USUALLY A FIXED SIZE
  -> 1, 2, 4, & BYTES

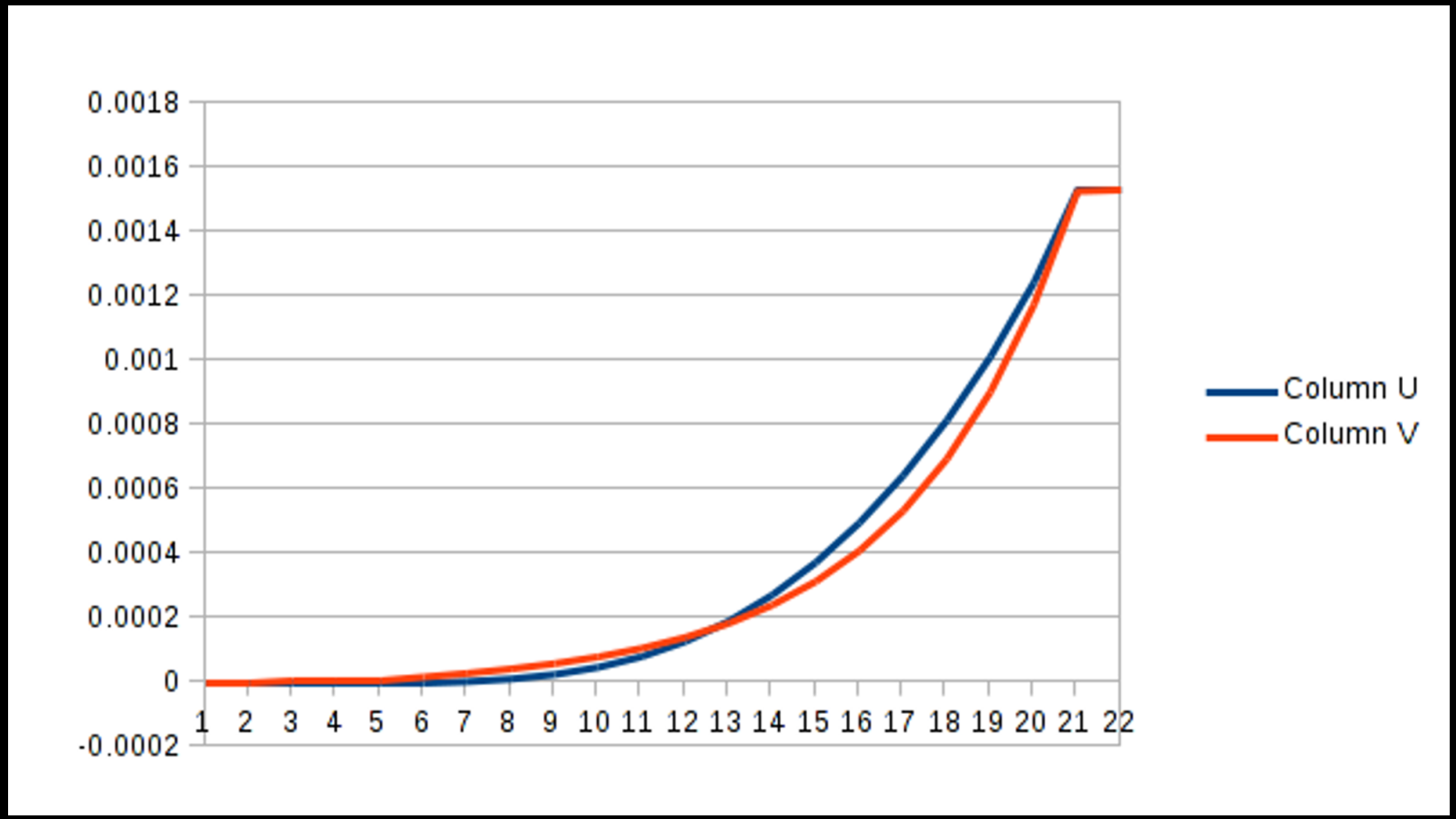
STRAWBERRY FIELDS ARE RED AND GREEN :)

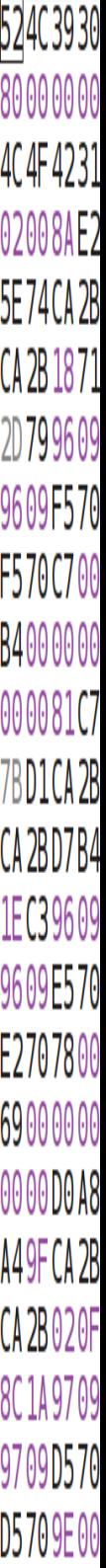
INTERPRET FIELDS

- CHOSEN PLAINTEXT ATTACK!
- GRAPHICAL DATA ANALYSIS
  (-> E.G. EXCEL)

INTERPRET FIELDS 2

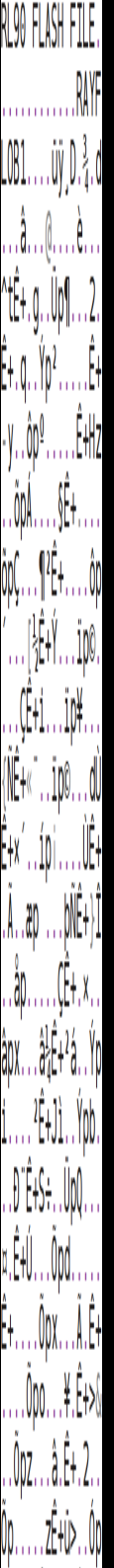
- LONGITUDE IS SCALED LINEARLY
  0X7FFFFFFF -> 180 DEGREES EAST
- LATITUDE IS PROJECTED USING MERCATOR





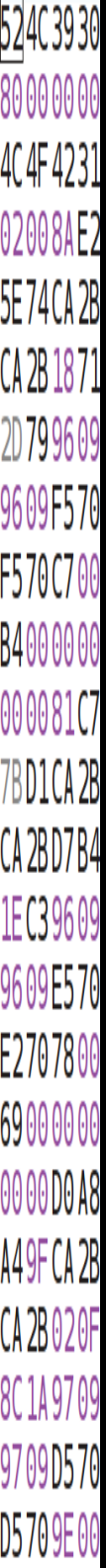
WRITE A TOOL

- CONVERT DATA INTO SOMETHING USEFUL
- AND VERIFY IF IT MAKES SENSE :)
- ... AND STARE AT IT :))



FINAL FSH TRACK FORMAT

```
INT32 NORTH   // NORTHING
INT32 EAST    // EASTING
UINT16 TEMPR  // TEMP IN KELVIN X 100
INT16 DEPTH   // DEPTH IN CM
INT16 C       // UNKNOWN. ALWAYS 0
```

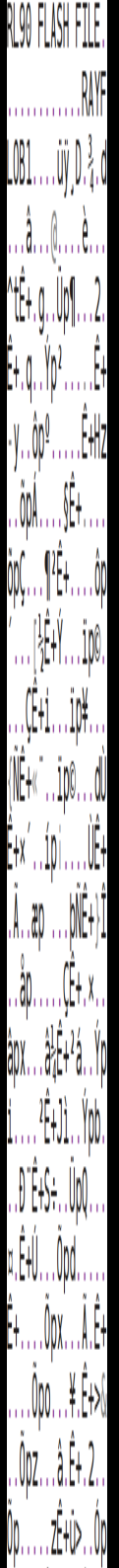


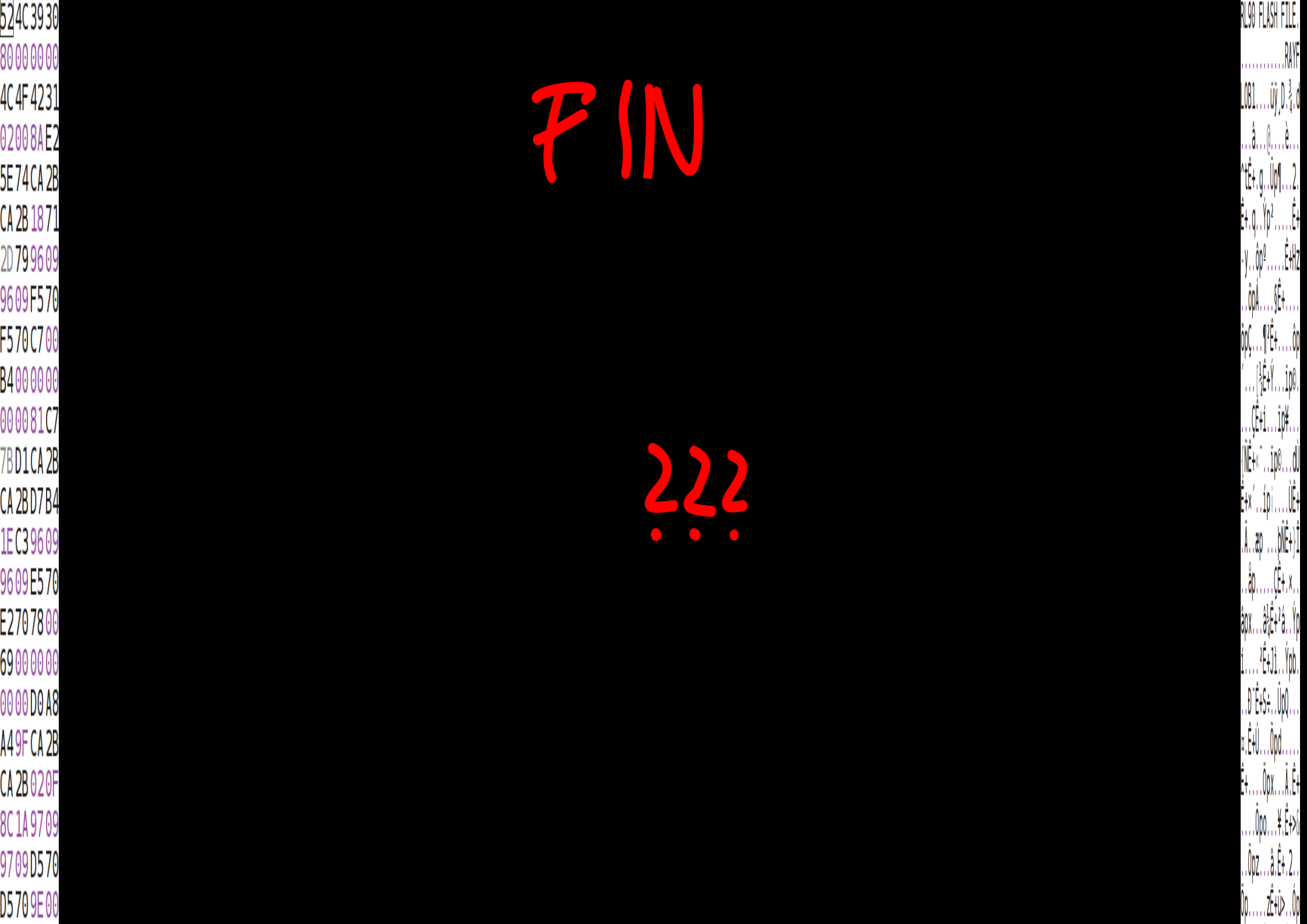
FINALLY

DOCUMENT EVERYTHING

YOU KNOW!

... AND WHAT IS YET UNKNOWN




FIN
???