

524C3930
80000000
4C4F4231
02008AE2
5E74CA2B
CA2B1871
2D799609
9609F570
F570C700
B4000000
000081C7
7BD1CA2B
CA2BD7B4
1EC39609
9609E570
E2707800
69000000
0000D0A8
A49FCA2B
CA2B020F
8C1A9709
9709D570
D5709E00

REVERSE-ENGINEERING FILE FORMATS

BERNHARD R. FISCHER

1024D/62029468 <BERNHARD.FISCHER@FHSTP.AC.AT>

RL90 FLASH FILE
.....RAYF
LOB1...üýD,¿,0
â...@...è
*É+ q, úpñ...2
É+ q, Yp²...É+
y, ópº...É+Hz
...ôpá...SÉ+...
ôç...ñÉ+...ôp
'...É+ý...ipº
...CÉ+i...ip+
...ñÉ+...ipº...ú
É+x'...ipº...úÉ+
...Ä...ap...ñÉ+...í
...âp...CÉ+x...
âpx...âÉ+â...Yp
i...?É+ñ...Ypº
...D'É+S=...ipº...
...É+ú...ôpº...
É+...ôpx...ÄÉ+
...ôoo...*É+>
...ôpz...âÉ+2...
ôp...zÉ+ú>...ôp

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

FILE HEADER

DATA BLOCK 1

DATA BLOCK 2

....

DATA BLOCK N

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

RAYMARINE'S FSH FORMAT

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



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

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 FLASH FORMAT

FILE HEADER

FLASH OBJECT 1

FLASH OBJECT 2

.....

FLASH OBJECT N

FLOB FORMAT

EVERY FLOB HAS THE SAME FIXED SIZE OF 0X10000 BYTES

DATA BLOCK

DATA BLOCK

DATA BLOCK

.....

BLOCK FORMAT:

IS IT HEADER PLUS DATA?

DATA BLOCKS HAVE A VARIABLE LENGTH

-> LENGTH ENCODED?

-> END MARKER?

SEVERAL KINDS OF DATA CAN BE STORED:

• TRACKS, WAYPOINTS, ROUTES, GROUPS OF WAYPOINTS, ...

-> TRACK TYPE?

524C3930
80000000
4C4F4231
02008AE2
5E74CA2B
CA2B1871
2D799609
9609F570
F570C700
B4000000
000081C7
7BD1CA2B
CA2BD7B4
1E C39609
9609E570
E2707800
69000000
0000D0A8
A49FCA2B
CA2B020F
8C1A9709
9709D570
D5709E00

YES, IT IS :)

RL90 FLASH FILE.
.....RAYF
LOB1...üý D, 3, 0
â...@...è
*É+ q, ÜpM...Z
É+ q, Yp²...É+
y, ôpº...É+Hz
...ôpá...\$É+...
ôç...¶É+...ôp
'...§É+ý...ipº.
...CÉ+í...ip+...
(NÉ+...ipº...Ü
É+x'...ip) ...ÜÉ+
Ä...ap...NÉ+) I
...âp...CÉ+x...
âpx...âÉ+²á...Yp
i...²É+í)...Ypº.
...D'É+S=...ÜpQ...
...É+Ü...Ôpº...
É+...Ôpx...ÄÉ+
...Ôpº...¥É+>ö
...Ôpz...âÉ+2...
Ôp...zÉ+ü>...Ôp

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, 8 BYTES

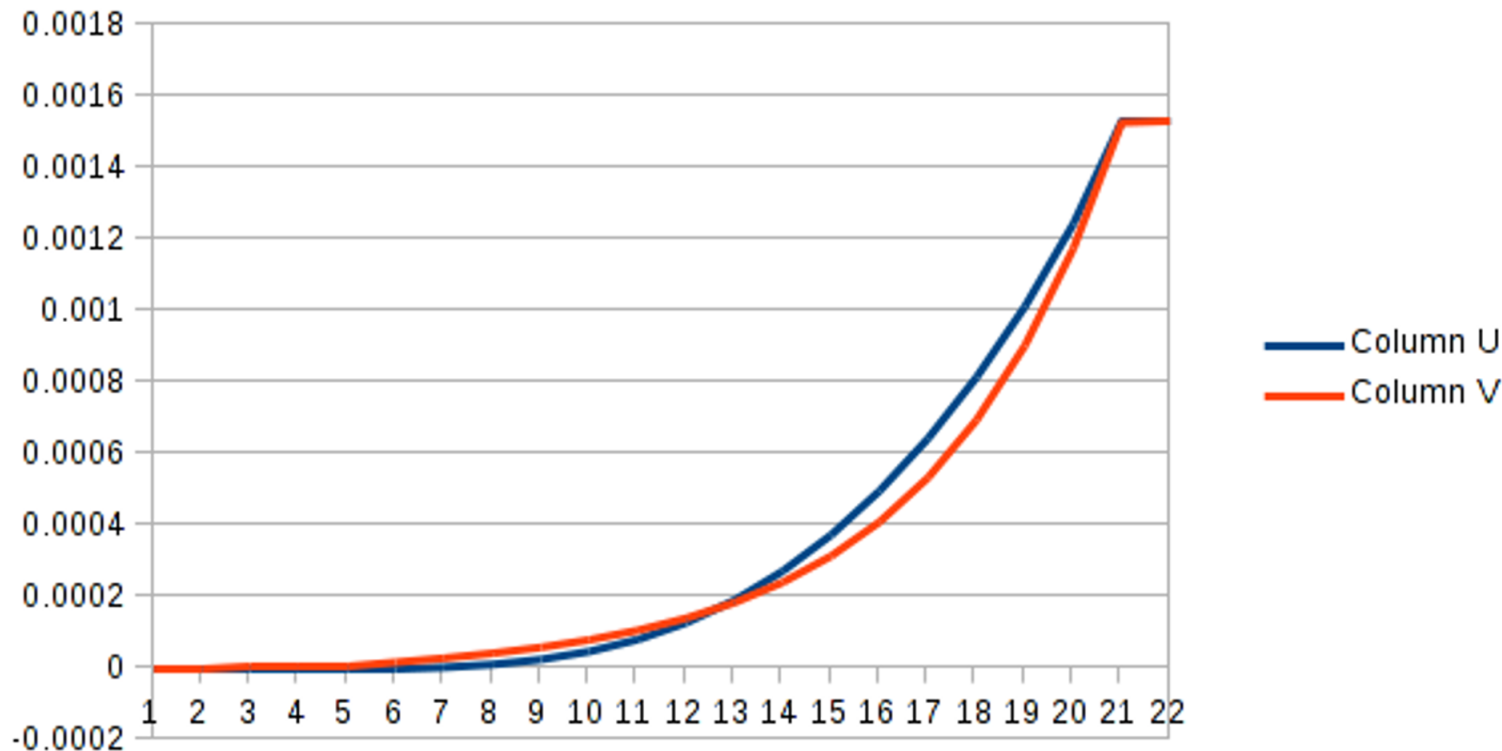
STRAWBERRY FIELDS ARE RED AND GREEN :)

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

524C3930
80000000
4C4F4231
02008AE2
5E74CA2B
CA2B1871
2D799609
9609F570
F570C700
B4000000
000081C7
7BD1CA2B
CA2BD7B4
1EC39609
9609E570
E2707800
69000000
0000D0A8
A49FCA2B
CA2B020F
8C1A9709
9709D570
D5709E00

FINALLY

DOCUMENT EVERYTHING

YOU KNOW!

... AND WHAT IS YET UNKNOWN

524C3930
80000000
4C4F4231
02008AE2
5E74CA2B
CA2B1871
2D799609
9609F570
F570C700
B4000000
000081C7
7BD1CA2B
CA2BD7B4
1E C39609
9609E570
E2707800
69000000
0000D0A8
A49FCA2B
CA2B020F
8C1A9709
9709D570
D5709E00

FIN

???

PL90 FLASH FILE.
.....RAYF
LOB1...üý D, 3, 0
...â...@...è...
...tÊ+ q, ÜpM...2
Ê+ q, Yp²...Ê+
-y, òpº...Ê+Hz
...òpá...\$Ê+...
òç...¶Ê+...òp
...ÿÊ+ý...ipò.
...CÊ+i...ip+...
(NÊ+...ipò...du
Ê+x' ipi...UÊ+
...Ä...ap...NÊ+)i
...âp...CÊ+x...
òpx...âÊ+²á...Yp
i...²Ê+iì...Ypò.
...D'Ê+S=...ùpQ...
...Ê+U...òpò...
Ê+...òpx...ÄÊ+
...òpò...¥Ê+>ò
...òpz...âÊ+2...
òp...zÊ+ù>...òp