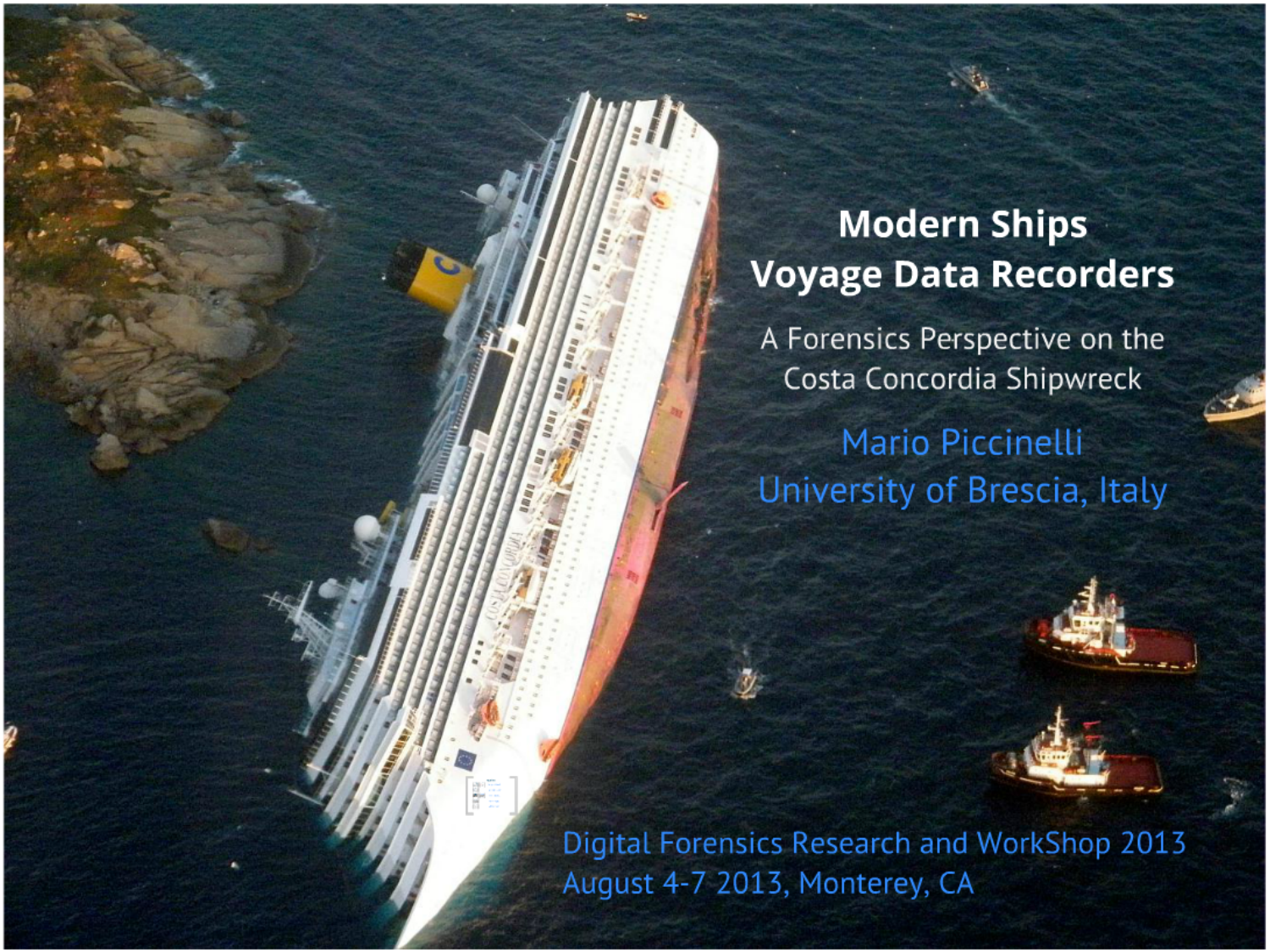


The authors wish to thank the Italian Consumers' Rights Association CODACONS and the other members of the CODACONS consulting team in the Costa Concordia Shipwreck trial.

ANY QUESTIONS?

Thanks for listening!

mario.piccinelli@ing.unibs.it

Modern Ships Voyage Data Recorders

A Forensics Perspective on the Costa Concordia Shipwreck

Mario Piccinelli
University of Brescia, Italy

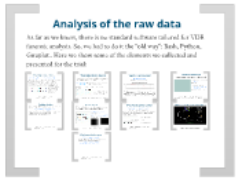
Digital Forensics Research and WorkShop 2013
August 4-7 2013, Monterey, CA

Outline

Why am I here?

What is a VDR?

Data retrieval



Data analysis

What's next?

The Costa Concordia disaster

MS Costa Concordia was a cruise ship built in 2004 and launched in 2006 in Italy. She was operated by Costa Crociere (subsidiary of Carnival Corporation). On January 13th, 2012, during a cruise on the Mediterranean sea, it ran aground and partially sank near the "Isola del Giglio", off the western coast of Italy, claiming 32 lives.

The ship

Concordia-class cruise ship.
Overall length: ~290 m. (~950 ft.)
Max width: ~35 m (~116 ft.)
17 decks, 2 of them underwater.
Power plant: six 12-cilinders diesel generating sets, combined power output of ~75 megawatts.
Propulsion: 2 electrical motors, 21 MW each.
Service speed: 19.6 knots (23 mph)
Capacity: 3,780 passengers, 1,100 crew.

The disaster

January 13th, 2012 21:45 local time: the ship was on the first leg of a 7-days cruise on the Mediterranean sea, sailing from Civitavecchia to Savona (both on the west coast of Italy).

During an unofficial near-shore passage, the ship hit an underwater reef near "Isola del Giglio", about 300 ft from the main land. The impact caused a massive flooding and the loss of electrical power. The ship, progressively listing on the right side, was then pushed by winds and currents to her final resting place.

At that time, the ship was carrying 4,252 people. The disaster claimed 32 lives (2 of the victims are still unaccounted for).

The ship

Concordia-class cruise ship.

Overall length: ~290 m. (~950 ft.)

Max width: ~35 m (~116 ft.)

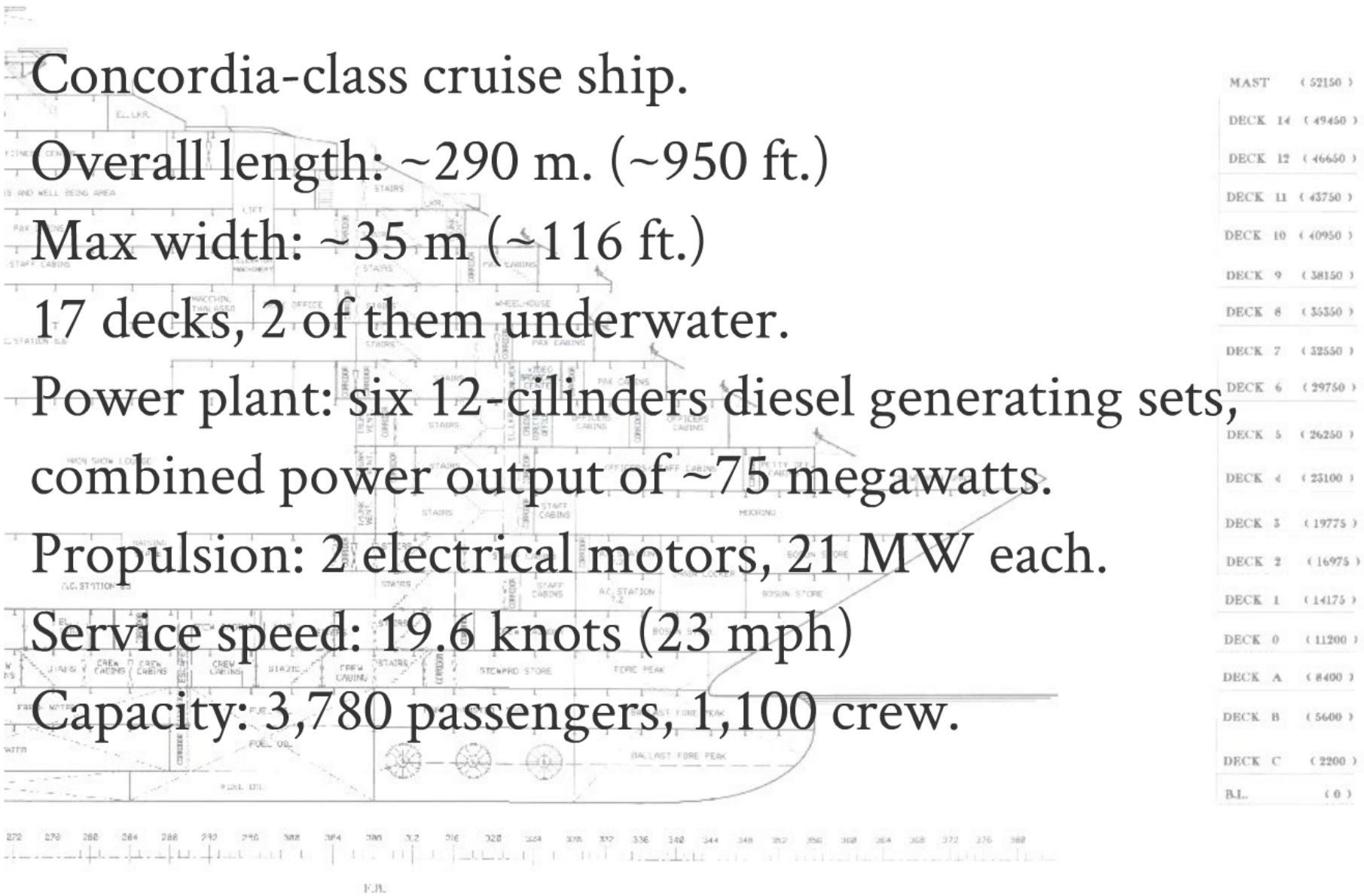
17 decks, 2 of them underwater.

Power plant: six 12-cilinders diesel generating sets, combined power output of ~75 megawatts.

Propulsion: 2 electrical motors, 21 MW each.

Service speed: 19.6 knots (23 mph)

Capacity: 3,780 passengers, 1,100 crew.

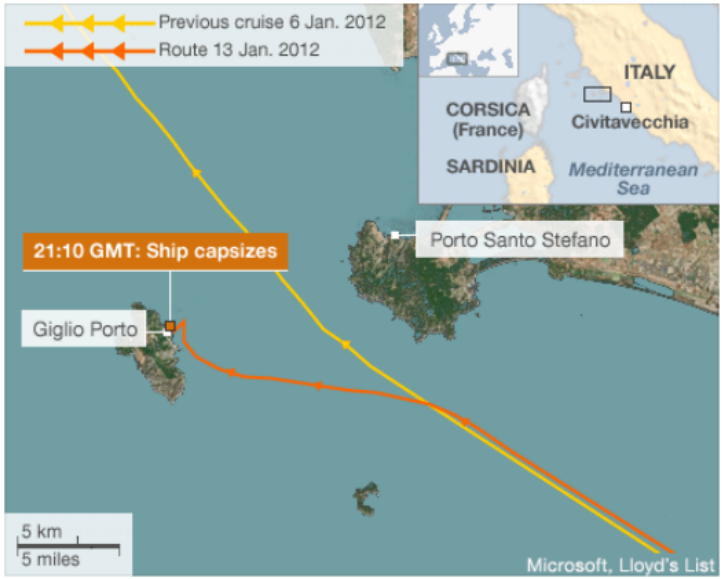


The disaster

January 13th, 2012 21:45 local time: the ship was on the first leg of a 7-days cruise on the Mediterranean sea, sailing from Civitavecchia to Savona (both on the west coast of Italy).

During an unofficial near-shore passage, the ship hit an underwater reef near "Isola del Giglio", about 300 ft from the main land. The impact caused a massive flooding and the loss of electrical power. The ship, progressively listing on the right side, was then pushed by winds and currents to her final resting place.

At that time, the ship was carrying 4,252 people. The disaster claimed 32 lives (2 of the victims are still unaccounted for).



Why this work?

International resolutions state which kind of data must be recorded on the "black box" of a ship, but they say nothing about how. In fact, the investigation on an accident must rely on the builder of the system, which is in charge of:

- opening the "black box"
- retrieving the data in proprietary format
- use a proprietary software to cook the data into a more useful format
- prepare the data to be shown in court.

There are many things in this list which are not really "forensically sound"..

"A forensically sound duplicate is obtained in a manner that does not materially alter the source evidence, except to the minimum extent necessary to obtain the evidence. The manner used to obtain the evidence must be documented, and should be justified to the extent applicable."

Harlan Carvey

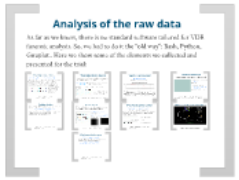
Why don't we try a REAL forensic examination of this "black box" with open source tools and standard techniques?

Outline

Why am I here?

What is a VDR?

Data retrieval



Data analysis

What's next?

VDRs (Voyage Data Recorders)

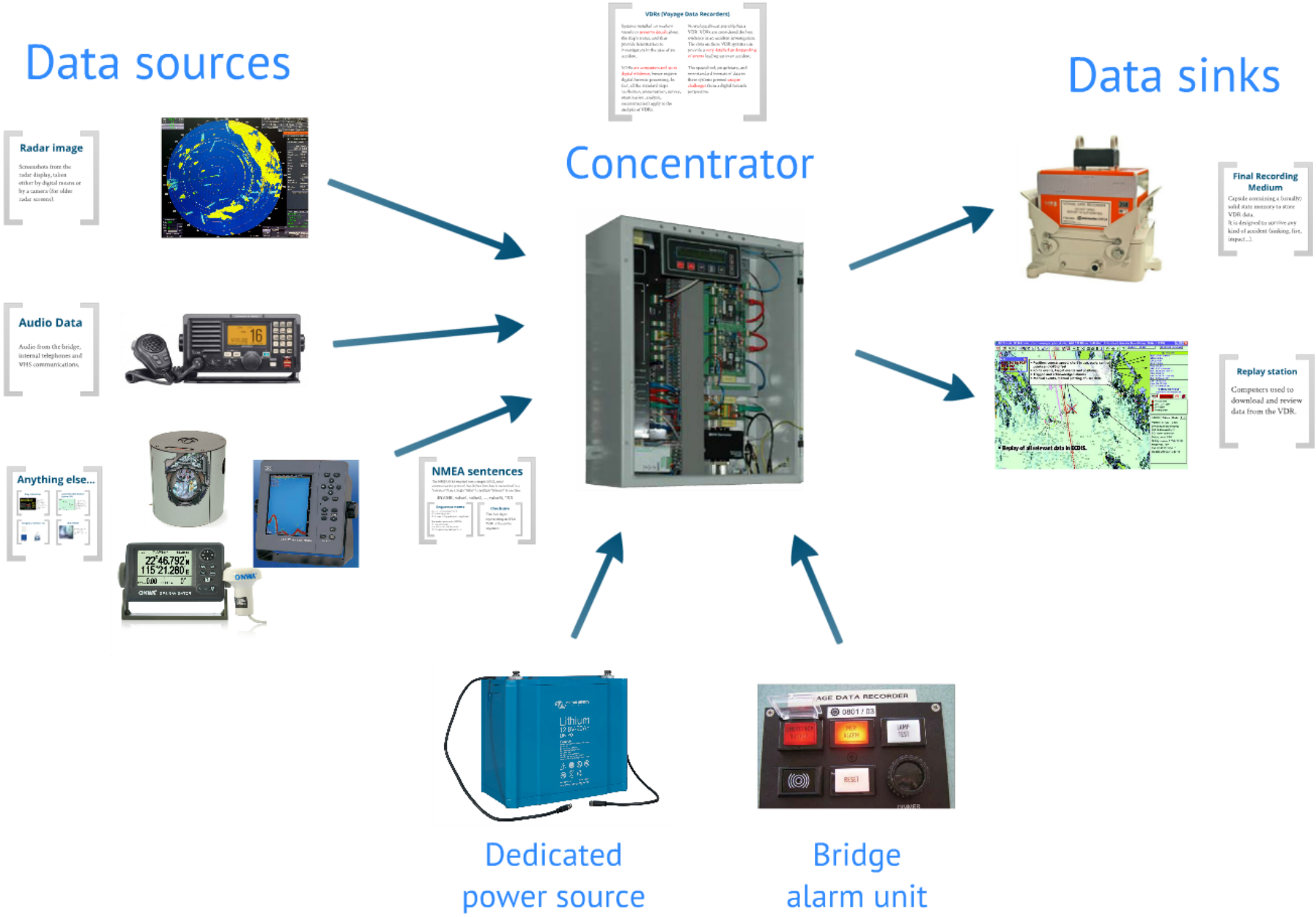
Systems installed on modern vessels to preserve details about the ship's status, and thus provide information to investigators in the case of an accident.

VDRs are computers and store digital evidence, hence require digital forensic processing. In fact, all the standard steps (collection, preservation, survey, examination, analysis, reconstruction) apply to the analysis of VDRs.

Nowadays almost any ship has a VDR. VDRs are considered the best evidence in an accident investigation. The data on these VDR systems can provide a very detailed understanding of events leading up to an accident.

The specialized, proprietary, and non-standard formats of data in these systems present unique challenges from a digital forensic perspective.

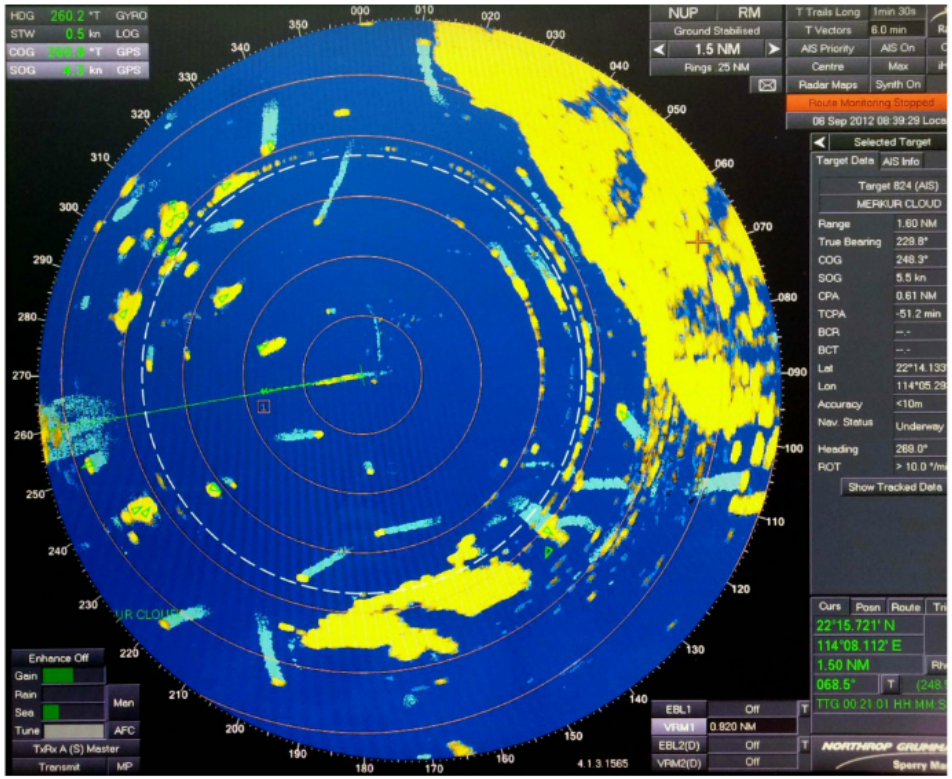
Voyage Data Recorder

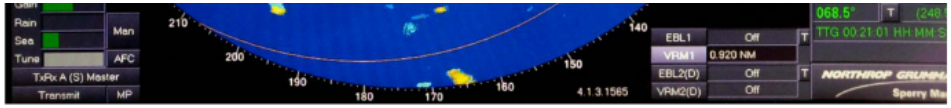


Data sources

Radar image

Screenshots from the radar display, taken either by digital means or by a camera (for older radar screens).



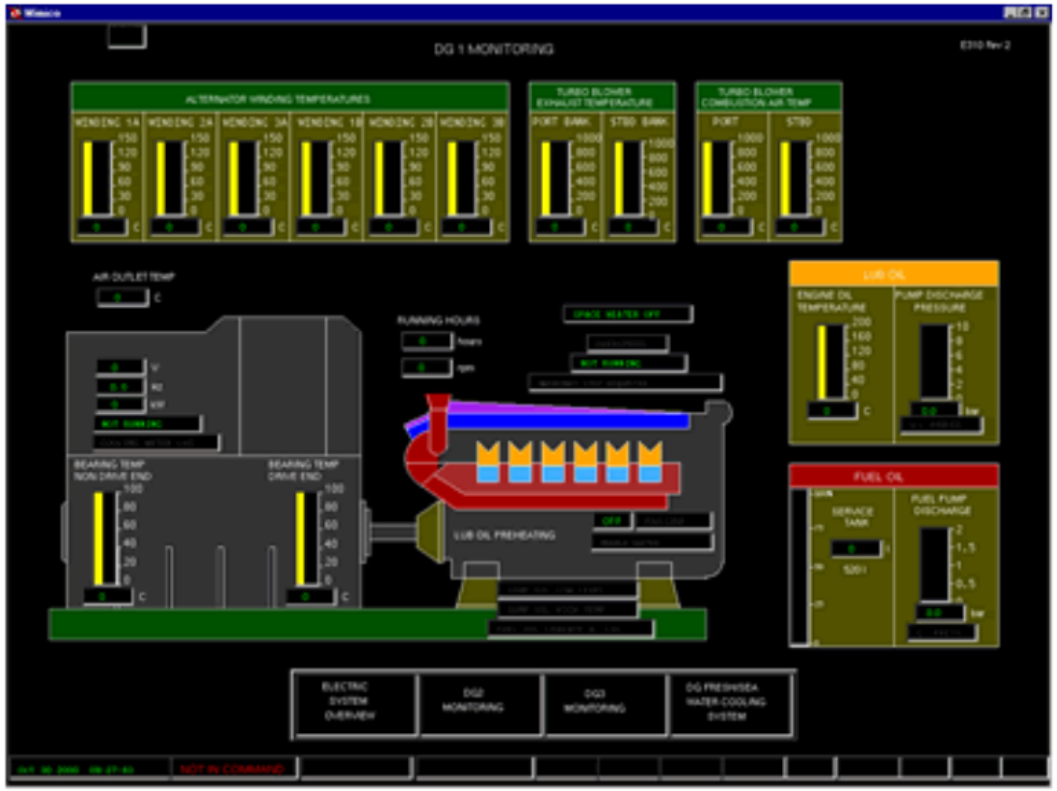


Audio Data

Audio from the bridge, internal telephones and VHS communications.

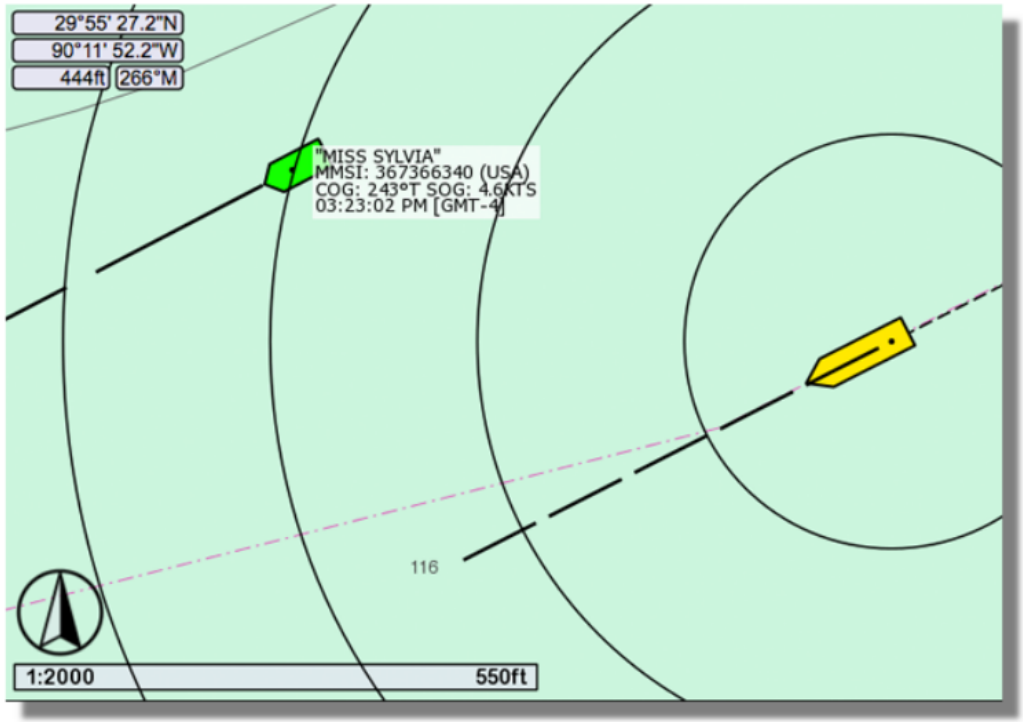
Anything else...

Ship automation



Status of engines, propellers, side propellers, main generator, emergency generators, ordered and actual position of rudders, ordered and actual speed of engines, and much more...

Automatic Identification System (AIS)



Each ship passing by transmits over radio broadcast some information such as its name and caller sign, speed, position, course, destination, and much more. The received signals are shown on the ECDIS (Electronic Chart DISplay).

Navigation instruments

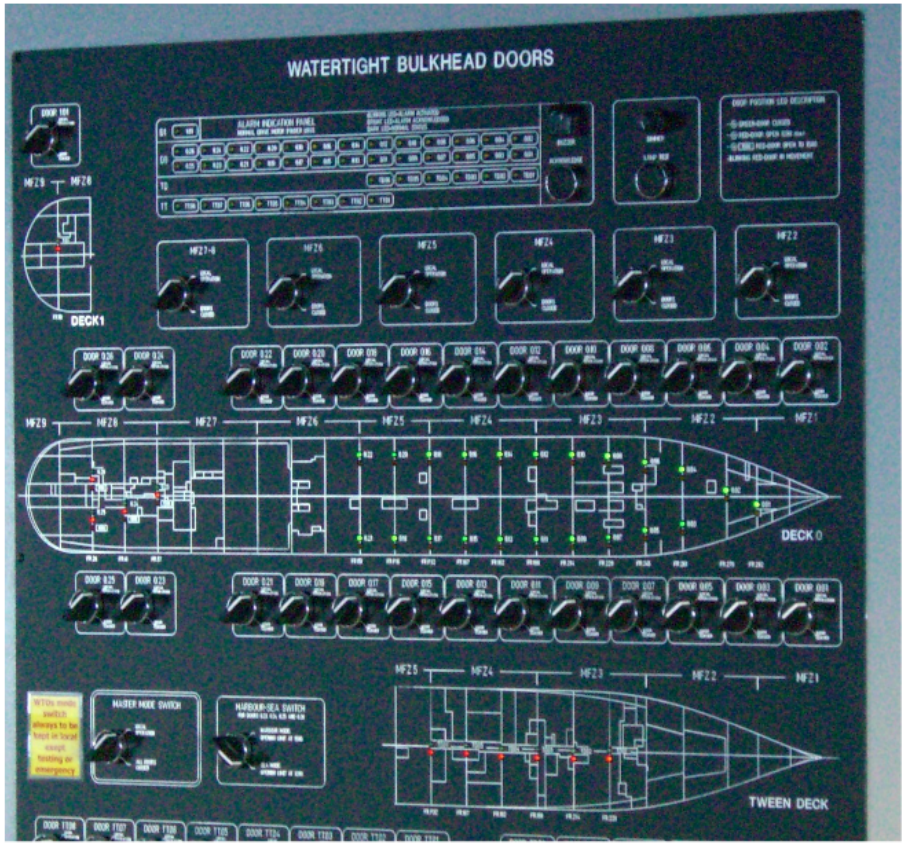
Compass

GPS

Echo sounder

Meteo station

Ship status



Fire alarms, flooding alarms, fireproof doors status, watertight doors status, hull doors status, hull stress, water tanks, and much more.

Audio Data

Audio from the bridge, internal telephones and VHS communications.

Anything else...

NMEA sentences

The NMEA 0183 standard uses a simple ASCII, serial communication protocol that defines how data is transmitted in a "sentence" from a single "talker" to multiple "listeners" at one time.

$NAME, value1, value2, ..., valueN, *XX

Sequence name

Standard sentences (e.g. GPGGA)
GP: talker (e.g. gps unit)
GGA: sequence (e.g. global positioning fix data)

Non standard sentences (e.g. PRWTD6)
P: non-standard sequence
T: manufacturer's code (e.g. Furuno)
WTD: sequence (e.g. waypoint data)

Checksum

Two hex digits representing an 8-bit XOR of the entire sequence.

NMEA sentences

The NMEA 0183 standard uses a simple ASCII, serial communication protocol that defines how data is transmitted in a "sentence" from a single "talker" to multiple "listeners" at one time.

$NAME, value1, value2, ..., valueN, *XX

Sequence name

Standard sentences (eg: GPGGA)
GP: source (eg: gps unit)
GGA: sequence (eg: global positioning fix data)

Non standard sentences (eg: PSWTD):
P: nonstandard sequence
S: manufacturer's code (eg: Seanet)
WTD: sequence (eg: watertight door)

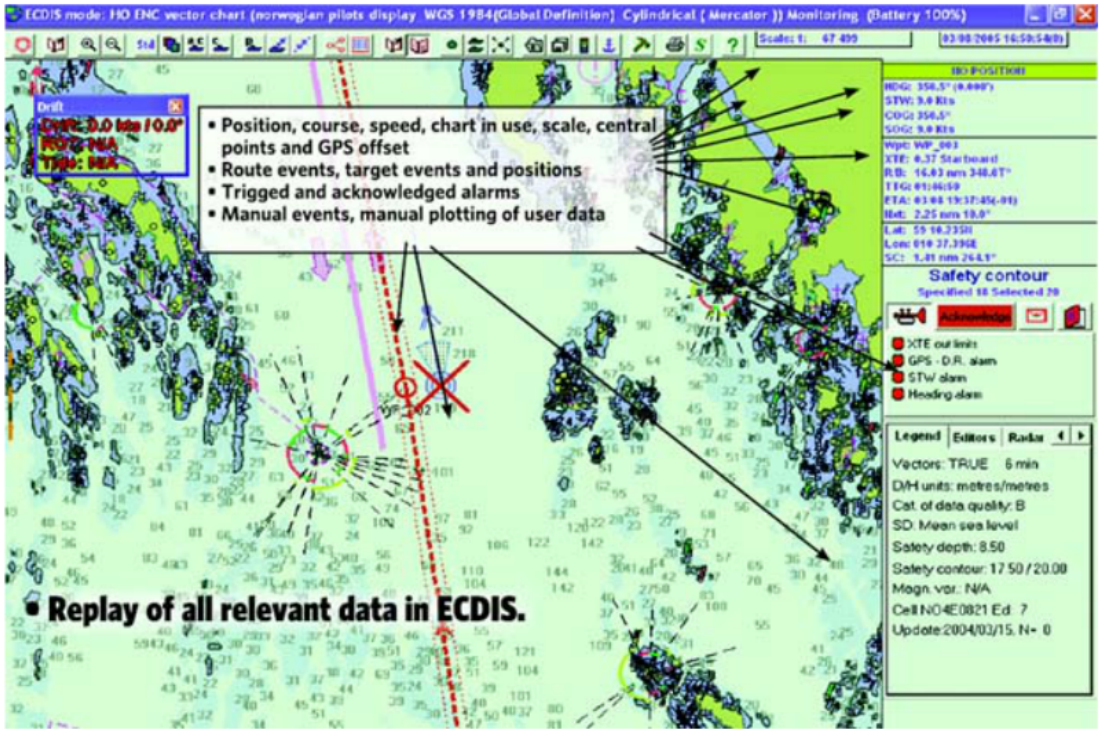
Checksum

Two hex digits representing an 8-bit XOR of the entire sequence.

Data Sinks

Final Recording Medium

Capsule containing a (usually) solid state memory to store VDR data.
It is designed to survive any kind of accident (sinking, fire, impact...).



Replay station

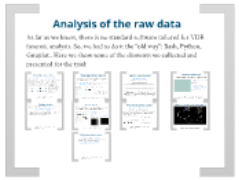
Computers used to download and review data from the VDR.

Outline

Why am I here?

What is a VDR?

Data retrieval



Data analysis

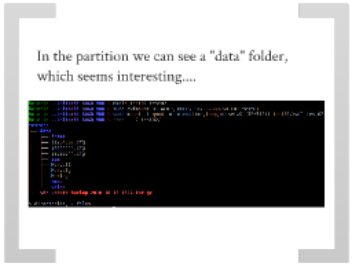
What's next?

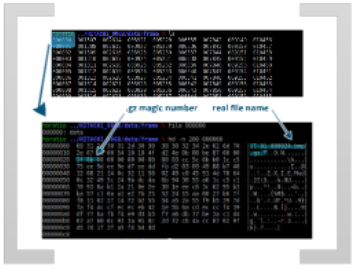
Disclaimer: the authors never climbed on the shipwreck...

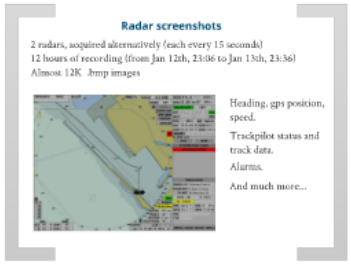
FRM being recovered by italian Coast Guard

We worked on a COPY of the FRM data, found in the concentrator which survived the accident.

We approached the disk recovered from the concentrator with standard forensics techniques...







We started from a copy of the disk of the "Data Collecting Unit" (concentrator) in EWF format, acquired by the Italian Police.

```
horatio ../Hitachi 80GB VDR % ewfinfo HITACHI\ 80GB\ SN\ FZG8976B.E01
ewfinfo 20120603

Acquiry information
        Case number:            P.P. 117.12 GIP GROSSETO
        Description:            HITACHI 80GB SN FZG8976B
        Examiner name:          GAT
        Evidence number:        HITACHI 80GB SN FZG8976B
        Notes:                  HD INTERNO DATA COLELCTING UNIT
        Acquisition date:       Wed Apr  4 11:22:16 2012
        System date:            Wed Apr  4 11:22:16 2012
        Operating system used:  Windows 7
        Software version used:  6.15
        Password:               N/A
        Model:                  HEJ421080G9AT00
        Extents:                0

EWF information
        File format:            EnCase 6
        Sectors per chunk:      64
        Error granularity:      64
        Compression level:      no compression
        GUID:                   e3371cf3-d842-4706-a18b-fda7fe8921f7

Media information
        Media type:             fixed disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      156301488
        Media size:             74 GiB (80026361856 bytes)

Digest hash information
        MD5:                    4e897ad39ea8ae1cede38cc4c36aea48
        SHA1:                   295ceb449b4a5a5c5ec6496e29b45e6bfc601828
```

Looking at the partition table we found a QNX (Unix) system.

```
horatio ../Hitachi 80GB VDR % mmls HITACHI\ 80GB\ SN\ FZG8976B.E01
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000000031   0000000032   Unallocated
02:  00:00   0000000032   0156296639   0156296608   QNX 4.x (0x4D)
03:  -----   0156296640   0156301487   0000004848   Unallocated
```

In the partition we can see a "data" folder, which seems interesting....

```
horatio ../Hitachi 80GB VDR % mkdir test01 test02
horatio ../Hitachi 80GB VDR % sudo ewfmount HITACHI\ 80GB\ SN\ FZG8976B.E01 test01
horatio ../Hitachi 80GB VDR % sudo mount -t qnx4 -o ro,noatime,loop,offset=$((32*512)) test01/ewf1 test02
horatio ../Hitachi 80GB VDR % tree -L 2 test02/
test02/
├── data
│   ├── frame
│   ├── i1234567.cfg
│   ├── i4444444.cfg
│   ├── i9320544.cfg
│   ├── ism
│   ├── Mer.cf1
│   ├── Mer.cfg
│   ├── Merlog
│   ├── nmea
│   └── voice
└── vdr_update-backup-2010-10-12-1327.tar.gz

5 directories, 7 files
```

```
horatio ../HITACHI_80GB/data/frame % ls
000000  001307  002614  003921  005228  006535  007842  009149  010456
000001  001308  002615  003922  005229  006536  007843  009150  010457
000002  001309  002616  003923  005230  006537  007844  009151  010458
000003  001310  002617  003924  005231  006538  007845  009152  010459
000004  001311  002618  003925  005232  006539  007846  009153  010460
000005  001312  002619  003926  005233  006540  007847  009154  010461
000006  001313  002620  003927  005234  006541  007848  009155  010462
000007  001314  002621  003928  005235  006542  007849  009156  010463
000008  001315  002622  003929  005236  006543  007850  009157  010464
000009  001316  002623  003930  005237  006544  007851  009158  010465
```

.gz magic number

real file name

```
horatio ../HITACHI_80GB/data/frame % file 000000
000000: data
horatio ../HITACHI_80GB/data/frame % hd -n 200 000000
00000000  69 31 2d 30 31 2d 30 30  30 30 32 34 2e 62 6d 70  |i1-01-000024.bmp|
00000010  2e 67 7a 00 54 10 10 4f  d2 4e 0b 00 be 87 00 00  |.gz.T..O.N......|
00000020  1f 8b 08 00 00 00 00 00  00 03 cc 5c 6b b0 1c c5  |...........\k...|
00000030  75 ee 9d ee 9e d7 ee dd  fb d2 03 09 49 88 b7 40  |u...........I..@|
00000040  12 08 21 14 0c 32 11 58  02 49 c0 45 91 4d 78 64  |..!..2.X.I.E.Mxd|
00000050  0c 32 49 5c 24 9b dc da  6b 94 38 55 a6 1c c5 c1  |.2I\$...k.8U....|
00000060  70 93 8a b1 2a 21 0e 2e  30 1e ee c6 3c 62 95 b3  |p...*!..0...<b..|
00000070  ba 57 c1 0a a1 e2 7b 25  52 24 15 aa 00 27 b6 7f  |.W....{%R$...'..|
00000080  f8 11 62 27 14 72 b2 55  54 a5 2a 55 f9 b5 39 7d  |..b'.r.UT.*U..9}|
00000090  fa f4 4c cf ec ec eb 42  1e 5b 6a cd ec cc f4 39  |..L....B.[j....9|
000000a0  df 77 ba fb f4 e9 d3 b3  f7 a6 db 77 be 3a c1 d4  |.w.........w.:..|
000000b0  67 a7 60 6c 93 3a 91 8c  2d 72 c6 4a cc 87 02 9f  |g.`l.:..-r.J....|
000000c0  45 7d 1f 3f a5 f4 b4 dd                           |E}.?....|
000000c8
```

A little bit of Python to extract and rename the images...

```
import gzip
import sys,os
import StringIO

inputDir = "/data/Concordia/Immagini_dischi/HITACHI_80GB/prova2/data/frame/"
fileNames = range(0,11759)

containedFileOffset = 32
print "Contained file offset: %i"%containedFileOffset

for fileIndex in fileNames:

        initialPath = os.path.join(inputDir, "%06i"%fileIndex)
        print "Acquiring: %s"%initialPath

        # remove first N offset bytes, find in them the real file name
        file = open(initialPath, 'rb')
        data = StringIO.StringIO(file.read())
        file.close()

        nameData = data.read(containedFileOffset)
        realFileName = nameData[0:19]
        print "Real file name: %s"%realFileName
```

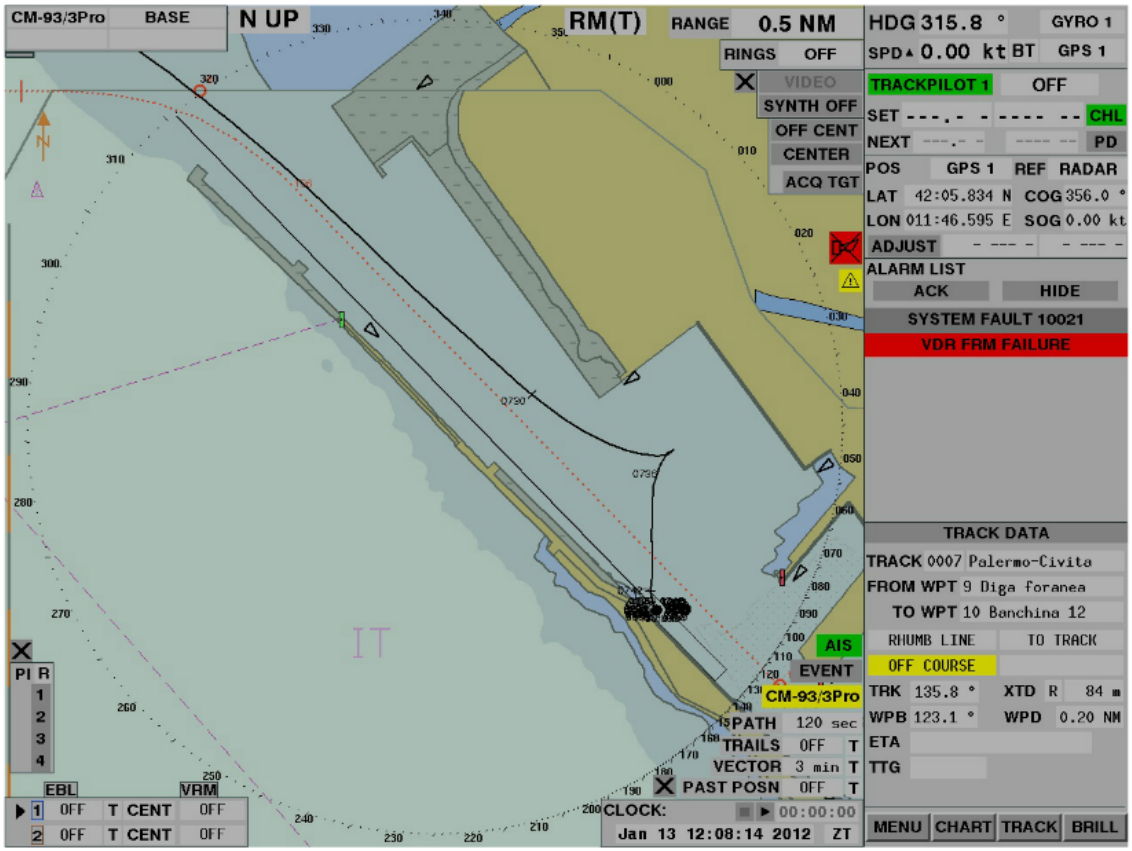
ex_images.py

Radar screenshots

2 radars, acquired alternatively (each every 15 seconds)

12 hours of recording (from Jan 12th, 23:06 to Jan 13th, 23:36)

Almost 12K .bmp images



Heading, gps position, speed.

Trackpilot status and track data.

Alarms.

And much more...

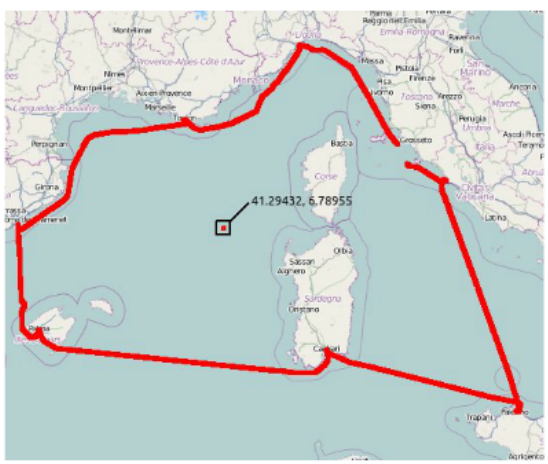
The same goes for the NMEA folder

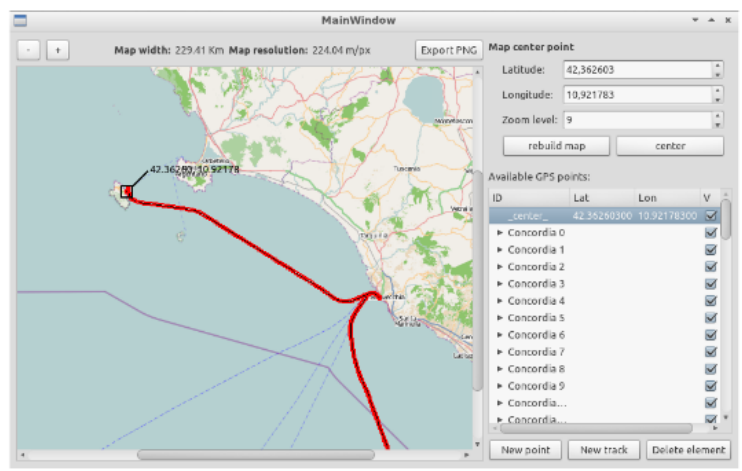
About 2K ASCII files with long lines.

Each line contains a timestamp (UTC Unix time written in hex) followed by some NMEA sentences. By concatenating the files we obtained a single ASCII file of 798 MB detailing one whole week of the cruise.

```
horatio ../Concordia/prove/nmea % head nmea
4F108AE8:76$RAZDA,195001.00,13,01,2012,-01,*40~14$HEHDT,303.6,T*29~14$RAROT,-0.0
1,A*29~14$GPGLL,4217.0357,N,01113.7944,E,195001.00,A,A*68~14$GPVTG,302.0,T,,M,16
.1,N,,K,A*14~14$RADTM,W84,,,,,,,*15~14$GPVBW,,,V,16.1,-0.4,A,,,,*5C~14$WIMWV,055
.0,R,22.7,N,A*14~14$PSWTD,14,C----,*32~0A$PSWTD,15,C----,*33~0A
4F108AE8:76!AIVDM,1,1,,B,13cmld002l0k3H8H=3SL6ad400Rq,0*1A~03!AIVDM,1,1,,A,402Fh
cQuhFkj10k82NH@@T700@14,0*16~03!AIVDO,1,1,,,13ceFq002Q0kJ1dH<NqclIP20000,0*1E~03
$GPGLL,4217.0342,N,01113.7974,E,195001.00,A,A*6F~04$GPVTG,302.0,T,,M,16.1,N,,K,A
*14~04$HEHDT,303.6,T*29~04$RAOSD,303.6,A,302.0,P,16.1,P,,,N*77~04$RAZDA,195001.0
0,13,01,2012,-01,00*40~04$RAROT,-0.02,A*2A~04$GPVBW,,,V,16.1,-0.4,A,,,,*5C~04
4F108AE8:76$GPGLL,4217.0372,N,01113.7914,E,195002.00,A,A*69~04$GPVTG,302.0,T,,M,
16.1,N,,K,A*14~04$HEHDT,303.6,T*29~04$RAOSD,303.6,A,302.0,P,16.1,P,,,N*77~04$GPG
```

Data from all the sensors onboard (from GPS position to meteo station, from watertight doors status to engines rpm and much more...) for a whole week.. plenty of data!





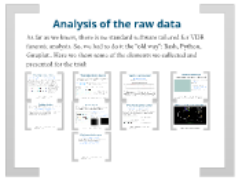
https://github.com/PicciMario/UiMapper

Outline

Why am I here?

What is a VDR?

Data retrieval

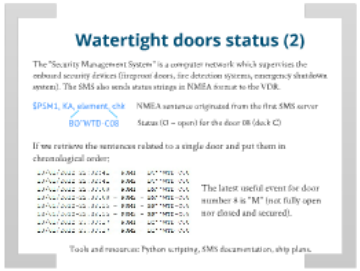


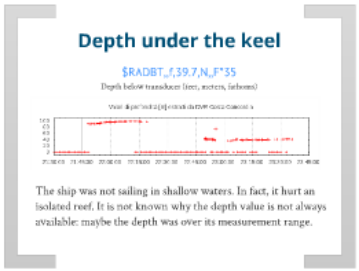
Data analysis

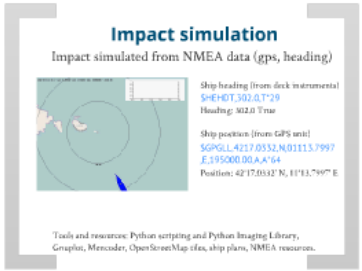
What's next?

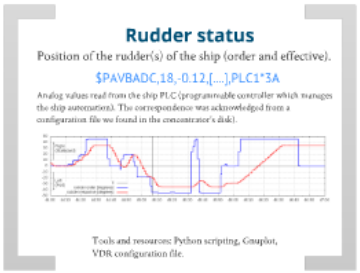
Analysis of the raw data

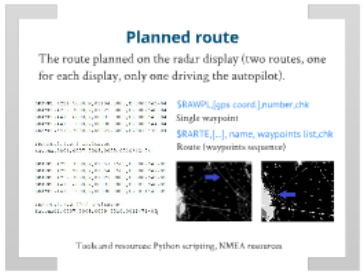
As far as we know, there is no standard software tailored for VDR forensic analysis. So, we had to do it the "old way": Bash, Python, Gnuplot.. Here we show some of the elements we collected and presented for the trial:

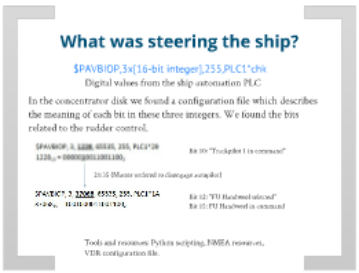


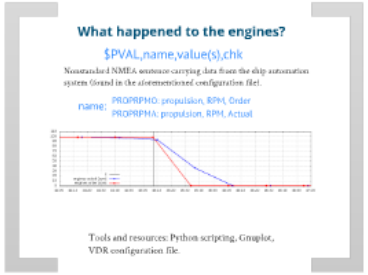












Watertight doors status

$PSWTD,17,C---,*35

Door number 17 closed.

$PSWTD,6,OF--P,*3B

Door number 6 open with fault (low pressure).

If we retrieve the sentences related to a single door, put them in chronological order and filter them to show only the status changes:

```
2012/01/13-21:26:17 - $PSWTD,08,C----,*35~0A
2012/01/13-21:42:45 - $PSWTD,08,O----,*31~0A
2012/01/13-21:43:01 - $PSWTD,08,C----,*35~0A
2012/01/13-21:46:56 - $PSWTD,08,CFV--,*37~0A
2012/01/13-22:32:26 - $PSWTD,08,CFV-P,*3A~0A
2012/01/13-22:32:41 - $PSWTD,08,CFV--,*37~0A
2012/01/13-22:33:13 - $PSWTD,08,OFV--,*33~0A
2012/01/13-22:33:28 - $PSWTD,08,?????,*39~0A
```

Last useful status for door number 8 is "open with electrical fault" (due to loss of the main generator after the flooding of the lower decks). Was the door closed after the loss of communications?

Tools and resources: Python scripting, Seanet documentation, ship plans.

Watertight doors status (2)

The "Security Management System" is a computer network which supervises the onboard security devices (fireproof doors, fire detection systems, emergency shutdown system). The SMS also sends status strings in NMEA format to the VDR.

$PSM1, KA, element, chk — NMEA sentence originated from the first SMS server

BO''WTD-C08 — Status (O = open) for the door 08 (deck C)

If we retrieve the sentences related to a single door and put them in chronological order:

```
13/01/2012-22:32:41 - PSM1 - BC''WTD-C08
13/01/2012-22:32:41 - PSM2 - BC''WTD-C08
13/01/2012-22:33:08 - PSM1 - BM''WTD-C08
13/01/2012-22:33:08 - PSM2 - BM''WTD-C08
13/01/2012-22:33:15 - PSM1 - BF''WTD-C08
13/01/2012-22:33:15 - PSM2 - BF''WTD-C08
13/01/2012-23:33:17 - PSM1 - Bf''WTD-C08
13/01/2012-23:33:17 - PSM2 - Bf''WTD-C08
```

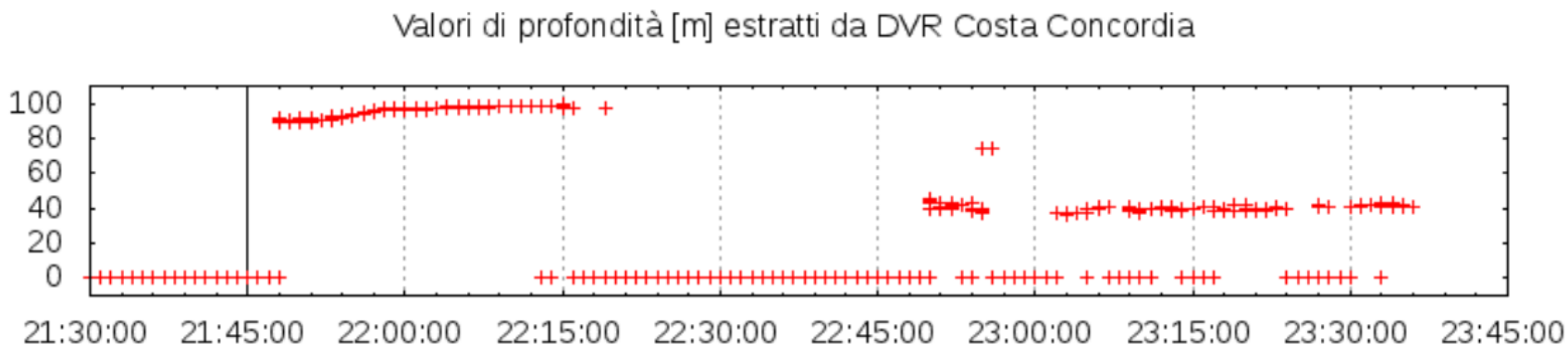
The latest useful event for door number 8 is "M" (not fully open nor closed and secured).

Tools and resources: Python scripting, SMS documentation, ship plans.

Depth under the keel

$RADBT,,f,39.7,N,,F*35

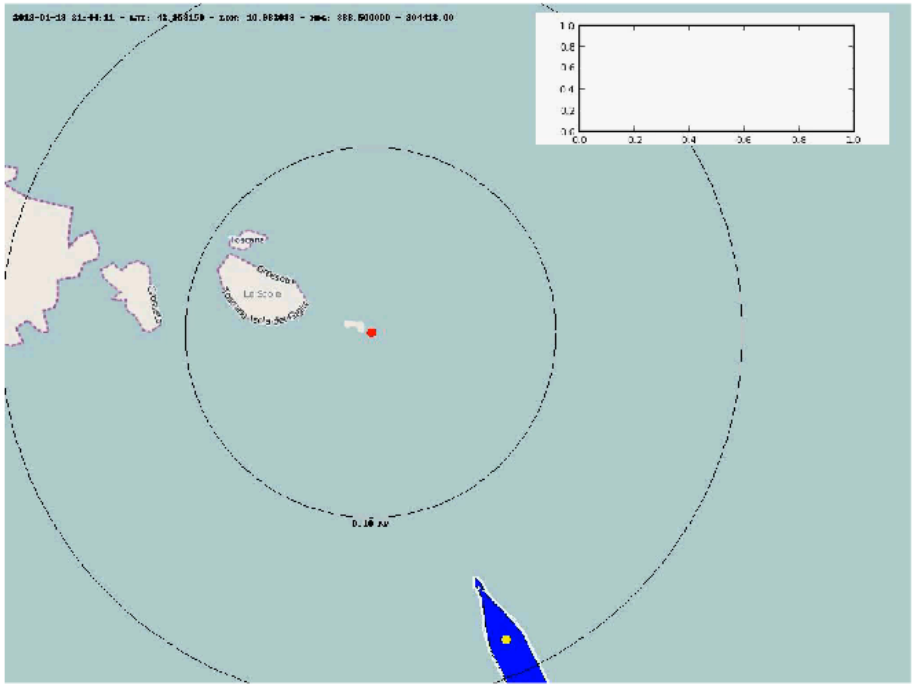
Depth below transducer (feet, meters, fathoms)



The ship was not sailing in shallow waters. In fact, it hurt an isolated reef. It is not known why the depth value is not always available: maybe the depth was over its measurement range.

Impact simulation

Impact simulated from NMEA data (gps, heading)



Ship heading (from deck instruments)

$HEHDT,302.0,T*29

Heading: 302.0 True

Ship position (from GPS unit)

$GPGLL,4217.0332,N,01113.7997,E,195000.00,A,A*64

Position: 42°17.0332' N, 11°13.7997' E

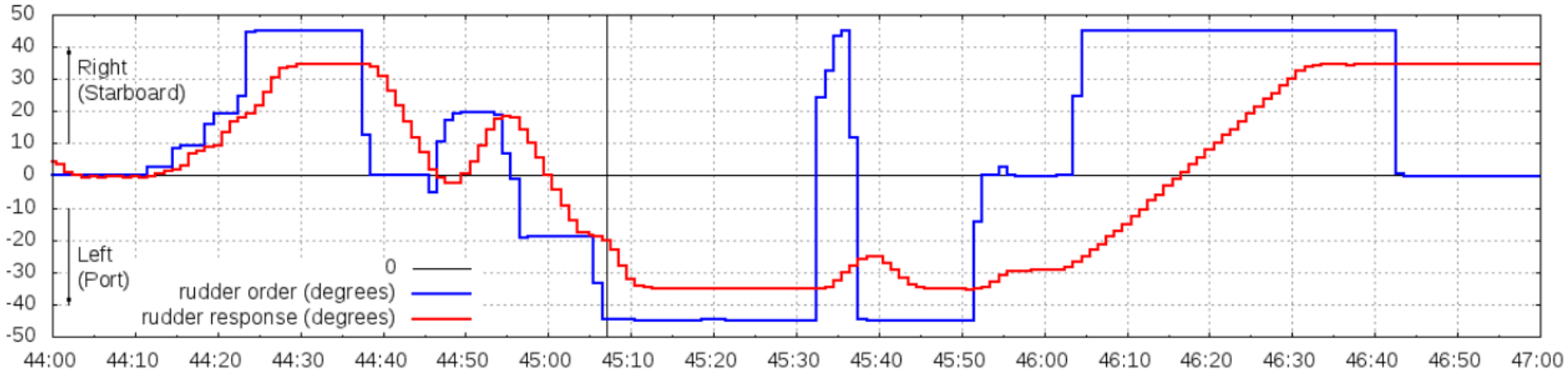
Tools and resources: Python scripting and Python Imaging Library, Gnuplot, Mencoder, OpenStreetMap tiles, ship plans, NMEA resources.

Rudder status

Position of the rudder(s) of the ship (order and effective).

$PAVBADC,18,-0.12,[....],PLC1*3A

Analog values read from the ship PLC (programmable controller which manages the ship automation). The correspondence was acknowledged from a configuration file we found in the concentrator's disk).



Tools and resources: Python scripting, Gnuplot, VDR configuration file.

Planned route

The route planned on the radar display (two routes, one for each display, only one driving the autopilot).

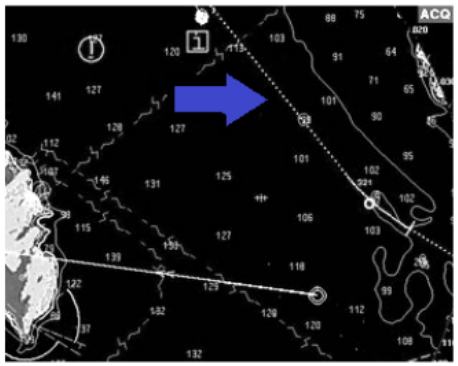
```
$RAWPL,4221.5000,N,01104.0000,E,0006*4D~04
$RAWPL,4252.7000,N,01029.8000,E,0007*4C~04
$RAWPL,4418.6000,N,00831.7000,E,0008*45~04
$RAWPL,4419.1000,N,00830.0000,E,0009*44~04
$RAWPL,4418.7000,N,00829.3000,E,0010*40~04

$RARTE,1,1,w,1 Civitavec-
Savona,0006,0007,0008,0009,0010*42~04

$RAWPL,4220.3500,N,01057.1500,E,0007*4D~05
$RAWPL,4223.9200,N,01054.7500,E,0008*49~05
$RAWPL,4252.7000,N,01029.8000,E,0009*42~05
$RAWPL,4418.6000,N,00831.7000,E,0010*4C~05
$RAWPL,4419.1000,N,00830.0000,E,0011*4D~05

$RARTE,1,1,w,9012 Civitavec-
SavonaGI,0007,0008,0009,0010,0011*71~05
```

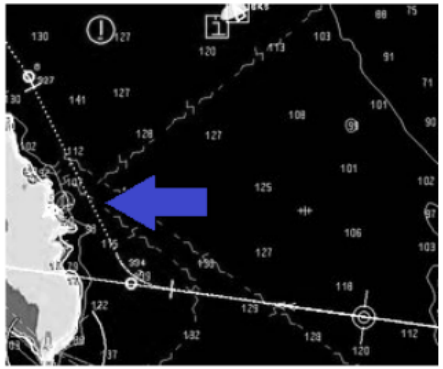
$RAWPL,[gps coord.],number,chk

Single waypoint

$RARTE,[...], name, waypoints list,chk

Route (waypoints sequence)





Tools and resources: Python scripting, NMEA resources

What was steering the ship?

$PAVBIOP,3x[16-bit integer],255,PLC1*chk

Digital values from the ship automation PLC

In the concentrator disk we found a configuration file which describes the meaning of each bit in these three integers. We found the bits related to the rudder control.

$PAVBIOP, 3, **1228**, 65535, 255, PLC1*29

$1228_{10} = 0000010011001100_2$

Bit 10: "Trackpilot 1 in command"

21:35 (Master ordered to disengage autopilot)

$PAVBIOP, 3, **37068**, 65535, 255, PLC1*1A

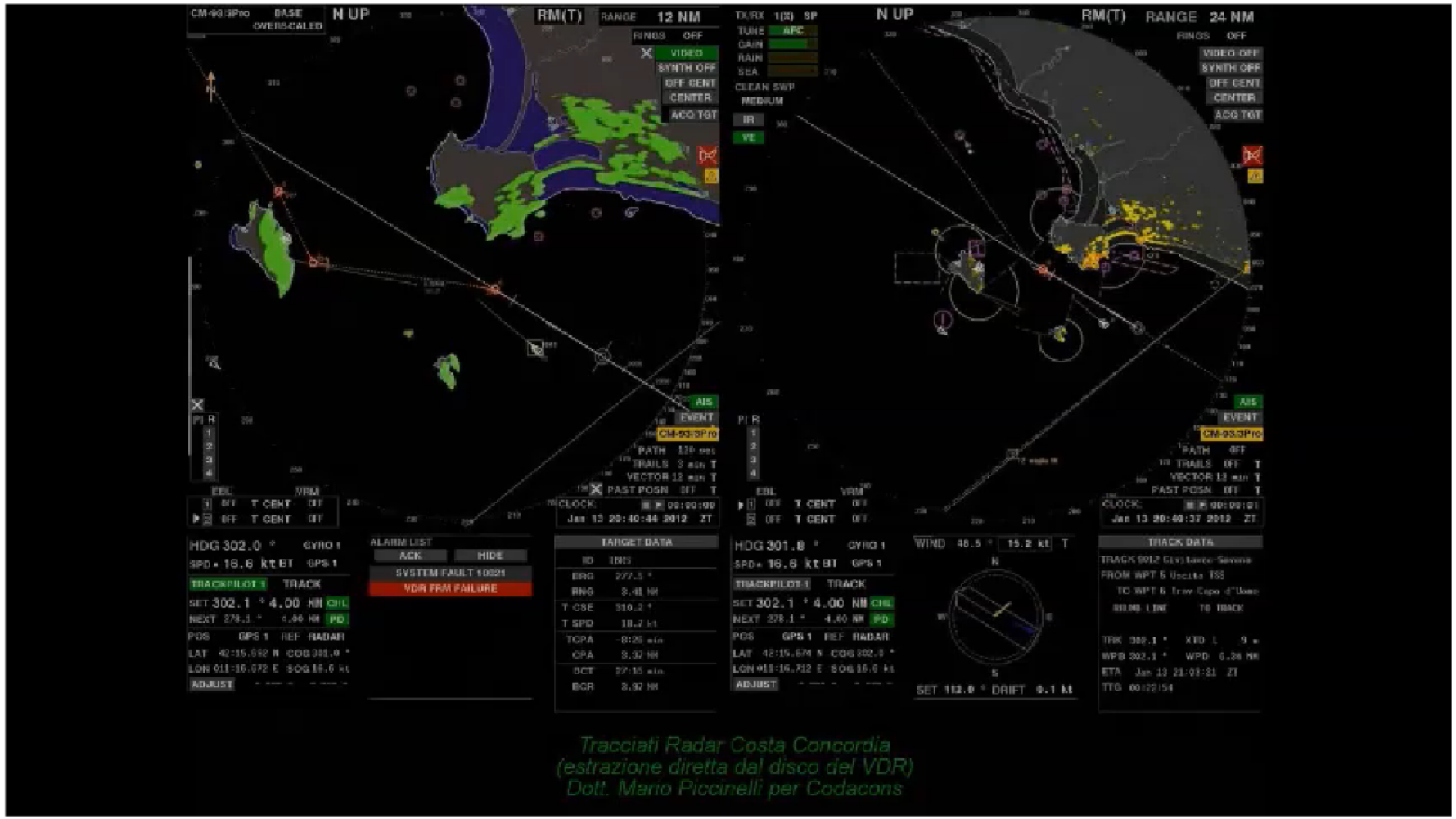
$37068_{10} = 1001000011001100_2$

Bit 12: "FU Handweel selected"

Bit 15: FU Handweel in command

Tools and resources: Python scripting, NMEA resources, VDR configuration file.

What was shown on the ship radars?



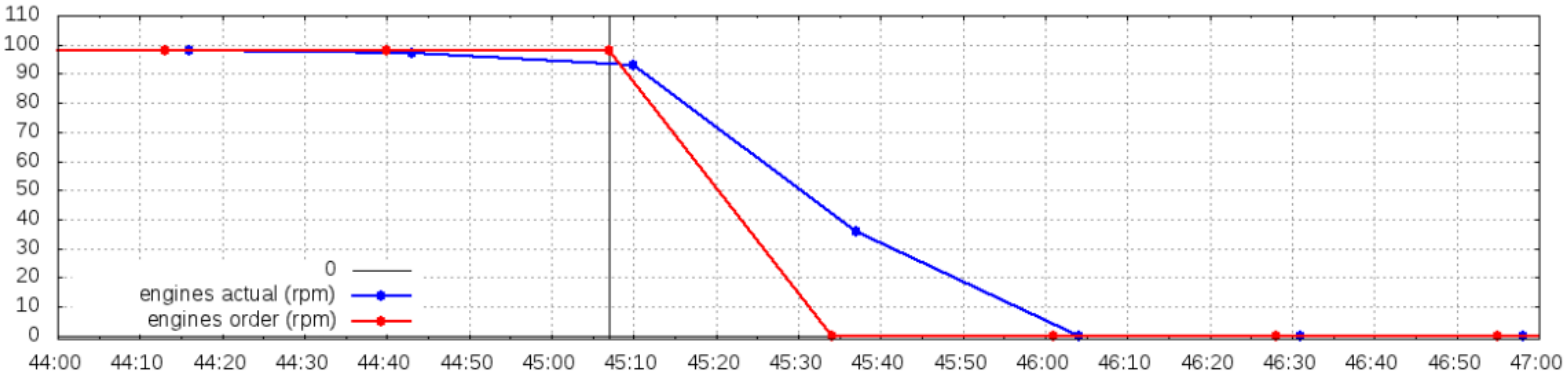
Tools and resources: Bash, ImageMagick suite, Mencoder

What happened to the engines?

$PVAL,name,value(s),chk

Nonstandard NMEA sentence carrying data from the ship automation system (found in the aforementioned configuration file).

name: PROPRPMO: propulsion, RPM, Order
PROPRPMA: propulsion, RPM, Actual



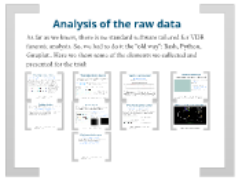
Tools and resources: Python scripting, Gnuplot, VDR configuration file.

Outline

Why am I here?

What is a VDR?

Data retrieval



Data analysis

What's next?

What's next?

What to look for?

Well, almost everything else.. The trial is still in progress and so it will be for a LONG time (trial, appeals, side trials, damages actions and so on). It is also extremely complex and it involves a huge number of people.
For these reasons we can't know which piece of data could be required for the next hearing.
The best thing we can do now is continue exploring the data we have in our hands, to achieve a better awareness about it and about the accident and its aftermaths.

What to do?

The field of computer forensics in ship accidents is almost unexplored. What I tried to do during my research work by hand (and much, much more) could be easily done with the help of specific software.

What to ask for?

VDRs, despite being the best source for accident investigations, still:

- Record data in a proprietary format.
- Require engineers sent by the builder to be opened and downloaded.
- Require proprietary software for extracting useful data and replaying the information.
- Forces investigators and judges to rely on cooked data instead of the raw (unreadable) content.

Can't we think about urging the ship industry towards some kind of standard?

What to look for?

Well, almost everything else.. The trial is still in progress and so it will be for a LONG time (trial, appeals, side trials, damages actions and so on). It is also extremely complex and it involves a huge number of people.

For these reasons we can't know which piece of data could be required for the next hearing.

The best thing we can do now is continue exploring the data we have in our hands, to achieve a better awareness about it and about the accident and its aftermaths.

What to do?

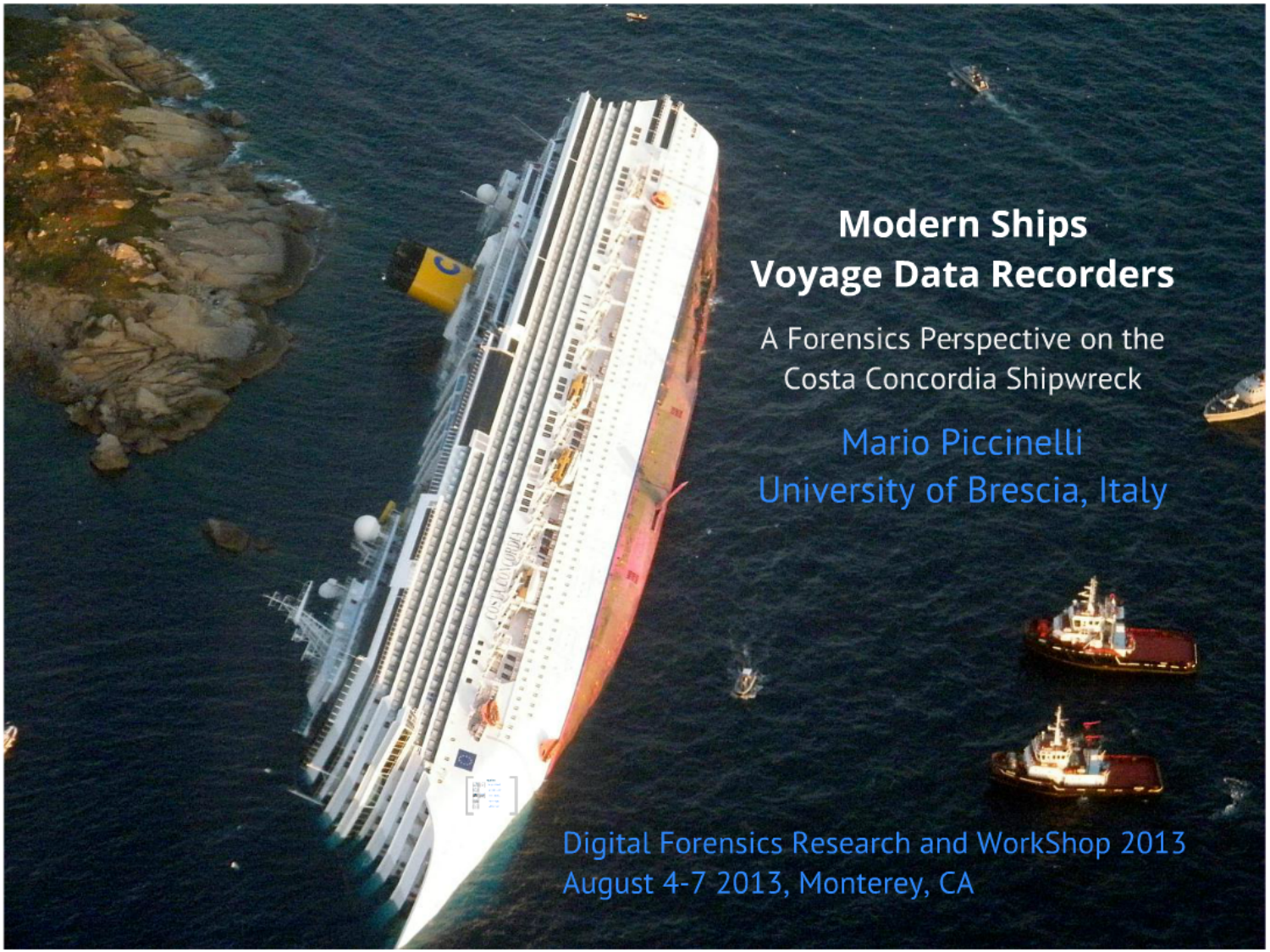
The field of computer forensics in ship accidents is almost unexplored. What I tried to do during my research work by hand (and much, much more) could be easily done with the help of specific software.

What to ask for?

VDRs, despite being the best source for accident investigations, still:

- Record data in a proprietary format.
- Require engineers sent by the builder to be opened and downloaded.
- Require proprietary software for extracting useful data and replaying the information.
- Forces investigators and judges to rely on cooked data instead of the raw (unreadable) content.

Can't we think about urging the ship industry towards some kind of standard?



The authors wish to thank the Italian Consumers' Rights Association CODACONS and the other members of the CODACONS consulting team in the Costa Concordia Shipwreck trial.

ANY QUESTIONS?

Thanks for listening!

mario.piccinelli@ing.unibs.it