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

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-cylinders 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 waves and currents to her final resting place.

At that time, the ship was carrying 4,233 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-cylinders 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.

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.

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.

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
- Audio data
- Anything else...
- NMEA sentences

Concentrator

- Final recording medium
- Replay station

Data sinks

- Dedicated power source
- Bridge alarm unit
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.
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 (National Marine Electronics Association) protocol is a standard for serial communication between marine electronic devices. A NMEA sentence is a sequence of fields separated by commas. The general format is:

NMEA field names are case-sensitive.

Example: $GPGGA,111111,123456,01,23456,789012,345678,901234,567890,012345,678901,234567,890123,456789,012345,678901*XX

Sequence name

Several field names are used in NMEA sentences, such as GGA, RMC, and VOR.

Checksum

The checksum is a 2-byte number that is calculated from the data and appended to the end of the message.

Example: 0x1234

Two-line data

NMEA messages are typically two lines long, and the second line is the checksum.
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.

$\textbf{Name}$, 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.
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...

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

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

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

Radar screenshots

The same goes for the NMEA folder

Dataset with the data extracted and renamed.
We started from a copy of the disk of the "Data Collecting Unit" (concentrator) in EWF format, acquired by the Italian Police.
Looking at the partition table we found a QNX (Unix) system.
In the partition we can see a "data" folder, which seems interesting....
A little bit of Python to extract and rename the images...

```python
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.

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**

- Status: Open/Closed
- Time stamps: [Timestamps]
- Conditions: [Cond.]

**Rudder status**

- Position: [Position]
- Time stamps: [Timestamps]

**Planned route**

- Routes: [Routes]
- Time stamps: [Timestamps]

**What happened to the engines?**

- Status: [Status]
- Time stamps: [Timestamps]

**Impact simulation**

- Diagram: [Diagram]
- Time stamps: [Timestamps]

**Depth under the keel**

- Measurements: [Measurements]
- Time stamps: [Timestamps]

**What was steering the ship?**

- Controls: [Controls]
- Time stamps: [Timestamps]
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
BO''WTD-C08

NMEA sentence originated from the first SMS server
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

$\text{RADBT,,f,39.7,N,,F*35}$

Depth below transducer (feet, meters, fathoms)

Valori di profondità [m] estratti da DVR Costa Concordia

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, Mencode, OpenStreetMap tiles, ship plans, NMEA resources.
Rudder status

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

$PAVBADC,18,-0.12,[...],PLC1\times3A$

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).

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

$\text{RARTE}, 1, 1, w, 1 \text{ Civitavec-Savona}, 0006, 0007, 0008, 0009, 0010*42-04$

$\text{RARTE}, [...], \text{name, waypoints list, chk}$

Single waypoint

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,\text{name},\text{value(s)},\text{chk}

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

\text{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.
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?
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

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