Modern Ships Voyage Data Recorders: a Forensics Perspective on the Costa Concordia Shipwreck

By

Mario Piccinelli and Paolo Gubian

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2013 USA

Monterey, CA (Aug 4th - 7th)

Contents lists available at SciVerse ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Modern ships Voyage Data Recorders: A forensics perspective on the Costa Concordia shipwreck

Mario Piccinelli*, Paolo Gubian

University of Brescia, Dept. of Information Engineering, Via Branze 38, 25123 Brescia, Italy

Keywords:
VDR
Voyage Data Recorder
Shipwreck
Costa Concordia
Digital forensics

ABSTRACT

International regulations about the safety of ships at sea require every modern vessel to be equipped with a Voyage Data Recorder to assist investigations in the event of an accident. As such, these devices are the primary means for acquiring reliable data about an accident involving a ship, and so they must be the first targets in an investigation. Although regulations describe the sources and amount of data to be recorded, they say nothing about the format of the recording. Because of this, nowadays investigators are forced to rely solely on the help of the builder of the system, which provides proprietary software to “replay” the voyage recordings. This paper delves into the examination of data found in the VDR from the actual Costa Concordia accident in 2012, and describes the recovery of information useful for the investigation, both by deduction and by reverse engineering of the data, some of which were not even shown by the official replay software.

1. Introduction

Voyage Data Recorders (VDRs) are 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. While the ongoing data collection is performed by various devices, such as analog and digital sensors or dedicated computer systems, the actual recording of this information is entrusted to an industrial grade computer. This paper describes how these systems work and how they store data related to ship navigation, focusing on details that could prove more useful for investigating an accident. In addition, this paper highlights how technical difficulties related to VDRs have slowed down or hampered investigations into naval accidents, demonstrating the need for digital forensic investigators to support naval investigators in recovering and analyzing data from these recording devices.

Using a real world case, the sinking of the ship Costa Concordia, we will describe the specific challenges that digital forensic investigators faced while trying to understand data extracted from the ship’s VDR. One of the primary challenges involved translating recorded data from non-standard formats into a form that could be used to reconstruct events surrounding the accident.

This description of a complete VDR forensics analysis and insights into information that was recovered is the first of its kind. Although specific data formats covered in this work may differ from other manufacturers’ devices, the overall process and methods presented in this paper can be applied to any VDR. As such, this work is a valuable first source for any practitioner approaching this kind of problem for the first time.

2. Motivation

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.

* Corresponding author.
E-mail addresses: mario.piccinelli@ing.unibs.it, mario.piccinelli@gmail.com (M. Piccinelli).

1742-2876/$ – see front matter © 2013 Mario Piccinelli and Paolo Gubian. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.diin.2013.06.005

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. Although some general purpose digital forensic processes which are commonly applied to standard computers can also be applied to VDRs, including hard disk imaging, the specialized, proprietary, and non-standard formats of data in these systems present unique challenges from a digital forensic perspective.

3. Regulations governing use of VDRs

The use of VDRs on ships is subjected to the regulations contained in chapter V on "Safety of Navigation" of the "International Convention for the Safety of Life at Sea" (SOLAS) (International Maritime Organization, 1974). This chapter has been amended in 1999 to adopt the IMO (International Maritime Organization) resolution A.861(20) "Performance Standards for Shipborne Voyage Data Recorders (VDRs)" (International Maritime Organization, 1997). These regulations, entered into force on July 1st, 2002, specify the kinds of ships that are required to carry Voyage Data Recorders, which include passenger ships, roll on-roll off passenger ships built before July 1st, 2002 (designed to carry wheeled cargo such as automobiles and trucks and thus provided with built-in ramps), and other ships over 3000 gross tonnage built on or after July 1, 2002.

The IMO resolution also sets requirements about the operation of the VDR. For example, it states that the device should be entirely automatic in normal operation and should continuously store sequential records of preselected data items related to status, command, and control of the ship. The recording medium should be installed in a brightly colored protective capsule and fitted with a beaconing device to help its localization. A further IMO resolution, MSC.163(78) adopted on 17 May 2004 (International Maritime Organization, 2004), creates a new category of VDR, called "Simplified VDR" or S-VDR, with lesser requirements to be fitted on older vessels.

According to the aforementioned regulations, a standard VDR is required to store at least the following data items: date and time referenced to Coordinated Universal Time (UTC), ship's position (latitude, longitude, coordinate reference), speed, heading, bridge audio (acquired by one or more microphones placed as to record conversations and audible alarms), Very High Frequency (VHF) radio communications, radar data (such as to record a faithful replica of the radar display that was on view at the time of recording), depth under keel, main alarms, rudder order and response, engine order and response, hull openings status, watertight and fire doors status and, where available, accelerations and hull stresses.

4. VDR system

The VDR is the complete system for processing, encoding and recording the data required by the IMO regulations.

The elements in this system, as seen in Fig. 1, are:

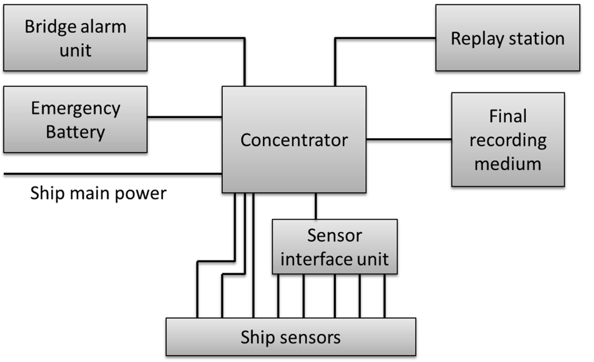


Fig. 1. VDR system schematic.

- **Concentrator**: usually an industrial grade computer which receives data from the sensors, processes and encodes them, and then records the stream to the final recording medium.
- **Sensors**: all the external devices from which the VDR receives data.
- **Sensor interface unit**: optional device providing additional input lines to the concentrator.
- **Final recording medium (FRM)**: the capsule used to store the data, designed to survive an accident and thus enable the recovery of the voyage data even in the event of a catastrophic loss of the ship.
- **Dedicated power source**: an external battery exclusively used to power the VDR for at least 2 h in the event of loss of main and backup power source of the ship.
- **Bridge alarm unit**: a remote interface to manage the VDR and acknowledge system alarms and warnings.
- **Replay stations**: one or more optional personal computers used to download and review voyage data from the concentrator.

In case of accident and subsequent investigation, both the final recording medium and, if they survived, the concentrator and the replay stations can serve as sources of data. The final recording medium is required to store at least the last 12 h of data (older records can be overwritten). Recording is required to continue 2 h after the loss of ship power, to allow archiving of data from before, during and after the accident. In case of non-catastrophic accidents, various manufacturers provide a way to backup data to another medium, usually placed near the concentrator, to prevent them from being overwritten and thus allowing their use for investigations. At last, the concentrator itself usually stores a larger amount of data, so its recovery can provide data which, even if not required by the regulations, can also be useful in an investigation.

4.1. How the VDR collects data

The VDR concentrator is wired to all the devices in the ship providing required data for it to store. The sources of data can be split into categories, depending on the interface involved:

- **Microphones**: the analog signals from bridge microphones, bridge telephones and VHFs are usually directly fed into the concentrator via dedicated input ports. The concentrator itself then manages to sample and record them.
- **Digital signals**: state signals (on/off) which usually carry information about ship alarms and warnings.
- **Analog signals**: signals acquired from analog transducers connected to parts of the ship. They can carry, for example, information about the position of the rudders or the speed of the main engines' shafts.
- **Video signals**: signals from analog video cameras. These are usually required to record the radar display for ships fitted with traditional analog radar devices.
- **Serial data**: complex data generated by smart devices such as the weather station, the ship's radar, the AIS and so on. The communication is usually done by NMEA strings (which will be discussed in the following sections). Also, the VDR sensor interface units usually convert their input (analog/digital/serial) into NMEA strings which are then fed to the main unit, so it is not uncommon for VDRs to store analog and digital inputs as NMEA strings too (especially for larger ships, where the acquisition must be performed on data sources placed far from the bridge).
- **Complex data**: bidirectional data connection (usually Ethernet) to autonomous devices able to provide complex data for the VDR to store. For example, modern ships are fitted with radar stations which are in fact industrial computers and concentrate all the information available on the bridge; these stations are able to provide the VDR with, for example, screenshots of the radar display, a task which previously required the use of a video camera to acquire an analog video feed.

On modern ships these data feeds are, in fact, stored in three formats: images (screenshots from the radar display/displays, provided by the radar station itself already in digital format), audio files (for the microphone inputs) and text (the NMEA strings representing serial, analog and digital inputs).

4.2. NMEA strings format

The preferred format for storing data on a VDR is using NMEA strings. NMEA 0183 (National Marine Electronics Association (NMEA), 2013) is a combined electrical and data specification for communication between marine electronic devices such as echo sounder, sonars, anemometer, gyrocompass, autopilot, GPS receivers and many other kinds of instruments. The NMEA standard is administered by the National Marine Electronics Association and, in marine applications, is gradually being replaced by the newer NMEA 2000 standard.

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. Through the use of intermediate expanders, a talker can have a unidirectional conversation with a nearly unlimited number of listeners and, using multiplexers, multiple sensors can talk to a single computer port. At the application layer, the standard also defines the contents of each sentence (message) type so that all listeners can parse messages accurately. The VDR is usually a listener, while all sensors and interface units are talkers.

The following example describes a NMEA string carrying information about the location of a generic GPS receiver:

```
    $GPGGA,123519,4807.038,N,01131.000,E,1,
08,0.9,545.4,M,46.9,M,,*47
```

The elements composing the string are the following:

- **$**: start symbol (can be an exclamation mark for some specific cases).
- **GP**: first two characters of the string preamble, they identify the source of the data (GP stands for a GPS receiver).
- **GGA**: last three characters of the preamble, a standard description of the following data (GGA stands for global positioning fix data).
- **123519**: time of when the fix was taken (12:35:19 UTC).
- **4807.038,N**: latitude (48 deg. 07.038′ North).
- **01131.000,E**: longitude (11 deg. 31.00′ East).
- **1**: fix quality (1 stands for GPS fix).
- **08**: number of satellites being tracked.
- **0.9**: horizontal dilution of precision (index of the precision of the satellite positioning)
- **545.4,M**: height above mean sea level (545.4 m).
- **46.9,M**: height of mean sea level above WGS84 ellipsoid.
- **Empty field**: time in seconds since last update.
- **Empty field**: DGPS station ID number.
- ***47**: checksum data (always begins with *).

The checksum data consists of two hexadecimal digits representing an 8 bit exclusive OR of the entire sequence from the $ to the * ($ and * are not used for the calculation).

The NMEA standard defines many fixed-form sequences, identified by the last three characters of the preamble. Also, the manufacturers of NMEA talkers are allowed to create proprietary sentences for specific purposes. These non-standard sentences are usually named by combining the P character, a single character manufacturer's code and additional characters to define the sentence type.

One of the biggest problems in VDR forensics is trying to find the meaning of the data contained in non-standard sequences. This goal can be accomplished by deduction, by combining data from other similar sources, or with the help of the manufacturer. For example, while working on the Costa Concordia shipwreck investigation, the authors happened to find sentences generated by the control systems of the watertight doors of the ship. The sentences were something like this:

```
$PSWTD,01,O——,*XX
$PSWTD,24,OFV-,*XX
```

These are non-standard sequences (starting with $P), from a device created by a manufacturer identified by the letter S (subsequent investigation determined that this was in fact the first letter of the manufacturer's name, Seanet). The sentence itself is described by the characters WTD, which could mean “Water Tight Doors”. This preamble was followed by an integer value, ranging from 1 to 25. Knowing that the ship under analysis had 25 watertight doors, it was initially hypothesized, and later verified through other means, that this was the number of the door the sentence was generated from. After this value was a string of 5 symbols. The first character is always O or C, which was initially assumed to mean “open” or “close” and was later confirmed through other evidence. The meaning of the other elements was resolved later with help from the manufacturer, but just by using the data identified by deduction (and later confirmed) it was possible to draw an accurate picture of a single aspect of the accident under investigation.

5. Issues in VDR forensics analysis

One of the most significant challenges in digital forensic investigations on VDRs is that the data is not supposed to be readily available to the investigators in the native format they have been recorded in on the medium. Standard protocols provide that the FRM is opened by a technician sent by the manufacturer, who then extracts the data with proprietary software and gives the investigators processed data in form of a video replay of the accident, sound files or text files with timestamps and values from the sensors. As of now, the procedure itself cannot be validated by third parties because of the intermediate elaboration of data by proprietary software. The current IMO Performance Standards for VDR/S-VDR do not specify a recording format for VDR data. Consequently VDR manufacturers have adopted various approaches and methods. While widely accepted, this procedure is far from being forensically sound. Even though the International Marine Organization prescribes that the manufacturer has to provide the owner of the ship all the means to download data from the VDR to an ordinary laptop, it allows the use of proprietary formats and software (International Maritime Organization, 2005). Another issue is that the elements which will then be brought in front of a court are not the ones acquired during preliminary investigations, but instead something else which is thought to be a faithful representation of them. In fact the court is watching at the data through an unknown (to the end user) abstraction layer, which could be lossy and lead to abstraction errors (Carrier, 2003). Moreover, each ship provides a different set of sensors and thus electrical signals to store and replay, so different versions of the replay software are needed to show data from different ships equipped with the same VDR system. In the real world case that is detailed in the following sections, the VDR manufacturer provided the authors with a generic version of the replay software, which did not show some values that were needed for the investigation such as the status of the watertight doors, making it necessary to work around this issue by writing customized replay software. At the same time, the investigators appointed by the court received full support by the manufacturer and were thus provided with the more complete software. This inconsistency raises questions of fairness when defendants are completely reliant upon the VDR manufacturer in order to retrieve data for analysis.

Another issue to consider when approaching such an investigation is that the VDR stores a huge amount of data, both in terms of number of different sources and in terms of number of readings for each source. This leads to the need to:

- Define a subset of the data which could prove useful in the investigation.
- Define a temporal filter that limits the reading to the time span of interest.
- Define a presentation strategy for presenting data (charts, single values, animations, etc.)

Nowadays, VDR forensics is almost non-existent in the literature and in the industry, so how these goals can be accomplished is left to the experience of the digital forensic investigator.

Furthermore, the experience of a forensic practitioner could prove valuable in cases involving damaged storage medium or when the stored data is corrupted or lost due to technical failures or human errors. For example, after the grounding of the ship “Maersk Kendal” on September 2009 the Master failed to stop the VDR and the data related to the accident was overwritten (Maritime Accident Casebook, 2013). It may be possible to recover such deleted data from storage media using digital forensic method. In another case, after an accident occurred to the “Chicago Express” container ship in September 2008, the VDR was not working but the investigation was delayed when the inquirers were falsely led to believe that the data could be retrieved (Guest, 2013). In such cases, digital forensic practitioners have the necessary experience to resolve such questions in an efficient and reliable manner.

6. Case example: VDR forensics in the Costa Concordia investigation

The Costa Concordia is the perfect example of a modern cruise ship with state-of-the-art electronic aids to navigation, security and resources management.

The ship was built in 2004/2005 by Fincantieri Sestri Ponente, an Italian shipbuilder, and entered service in July 2006. On January 2012, in calm seas and with clear visibility, she struck a rock in the Tyrrhenian Sea, near the shore of Isola del Giglio, on the west coast of Italy. The ship began to flood and immediately lost power to her propulsion and electrical systems. She finally grounded north of the village of Giglio Porto, lying on her starboard (right) side in shallow water with most of her right side under water. She is now considered a complete loss and she is waiting to be refloated and consequently moved to a dock for being dismantled. Of the 3229 passengers and 1023 crew members known to have been aboard, 30 bodies have been located, and two more passengers are missing and presumed dead (Wikipedia, 2012).

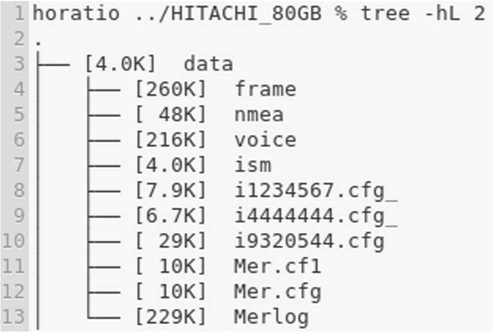
The ongoing investigation of the accident, which is just at the beginning, focused mainly on the evidence extracted from the VDR. While the FRM unit was found to be not working (allegedly a fault of the owner), luckily the concentrator survived the accident and enabled investigators to retrieve all required data.

6.1. Collection and preservation

The hard disk inside the concentrator was recovered and acquired by the Italian police, and the forensic duplicate was made available to all the parties involved in the trial. The data on this hard disk was not immediately useful because it was structured in a way that was difficult to read without the proprietary software. So, the first step in the investigation was to discover the format of the elements stored and then build a series of software tools to automate the recovery process.

6.2. Survey and examination

The hard disk in the VDR concentrator was an 80 GB device with a single non-bootable partition formatted in QNX 4.0 file system. The content is depicted in Fig. 3:



```
horatio ../HITACHI_80GB % tree -hL 2
.
├── [4.0K]  data
│   ├── [260K]  frame
│   ├── [ 48K]  nmea
│   ├── [216K]  voice
│   ├── [4.0K]  ism
│   ├── [7.9K]  i1234567.cfg_
│   ├── [6.7K]  i4444444.cfg_
│   ├── [ 29K]  i9320544.cfg
│   ├── [ 10K]  Mer.cf1
│   ├── [ 10K]  Mer.cfg
│   └── [229K]  Merlog
```

Fig. 3. Content of VDR concentrator hard disk under analysis.

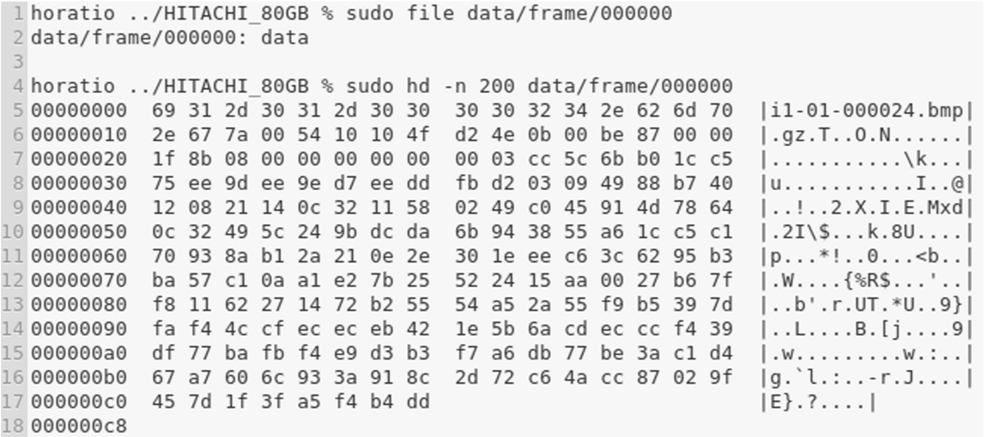
Forensic analysis began from the “frame” and “NMEA” directories, which contain the files related to the radar screenshots and to the NMEA sequences archive.

These directories contained a large number of files, named in numerical order (0000001, 0000002, etc.) without a file extension. Further analysis with an hex editor revealed that these files were GZip compressed files (starting with the standard hex header 0x1F8B), which was preceded by a non-standard header containing what was presumed to be the real name of the file, with extension .BMP.GZ for radar frames and .LOG.GZ for NMEA files (as seen in Fig. 2).

Using this knowledge, several scripts were developed in Bourne Shell and Python to extract and decompress the embedded files and rename them with their real name, found in the header. As a result of this process, the following information was obtained:

- The radar screenshots, stored as bitmap images. These screenshots have been collected from the two main radar displays of the bridge, alternating in intervals of about 7 s. The real names of the files contain an indication to which radar display the image was taken from: the string “i1” for the first one and the string “i3” for the second. In total, the folder contains 11,759 images spanning for about 24 h preceding the VDR shutdown, hence from January 12th at 23:06 to January 13th at 23:36 (in local time, which is UTC + 1). The files namespace is a circular buffer, hence the last image in the recording is the 5,515th and the first one is the following.
- The NMEA strings, stored as ASCII text files. Each text file contains a number of long rows. Each row is made by a timestamp, written in UNIX epoch (number of seconds since January 1st, 1970 at 00.00) in hexadecimal format, followed by some NMEA strings which have supposedly been collected at that time. Each file holds strings related to a 5 min time span, ranging for about a week preceding the VDR shutdown, hence from January 6th at 22:50 to January 13th at 23:35 (in local time UTC + 1). As seen for the radar images, the NMEA log file namespace is also used as a circular buffer.

After being able to retrieve the data in a useful format, the subsequent steps were directed toward finding ways to interpret and concentrate these data to show specific aspects of the incident, deemed useful for the ongoing



```
horatio ../HITACHI_80GB % sudo file data/frame/000000
data/frame/000000: data

horatio ../HITACHI_80GB % sudo hd -n 200 data/frame/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
```

Fig. 2. Hex dump of a file in the “frame” directory.

investigation. Some of the work performed to analyze the data and reconstruct events surrounding the Costa Concordia accident is presented in the following sections.

6.3. Rudder status

One of the first elements that emerged from the ongoing investigation (Carpinteri et al., 2012) is that, in the critical moments before the impact, the helmsman (the member of the crew who steers the ship) apparently failed to follow the directions of the master by turning the rudders in a wrong direction for some seconds. To investigate this matter it was necessary to determine the real positions of the rudders and of the control wheel. The rudder control, as with many other parameters related to the control of the ship such as the main engines and side thrusters, is managed by an integrated automation system which sends information to the VDR for recording purposes. The automation system builds non-standard NMEA strings, which contain analog and digital values from the actual sensors and actuators, in a format similar to:

`$PAVBADC, a, xx.xxx,[a times xx.xxx], name *hh`where:

- a is the number of values following (1–8)
- xx.xxx: analog value
- name: source description
- hh: checksum

During this research into data from the VDR in this case, a configuration file was recovered from the concentrator hard disk which describes the meaning of these analog values, providing the information needed to build a graph showing the following values:

- Rudder order: the position of the control wheel on the bridge, managed by the helmsman.
- Rudder response: the effective position of the rudders, which follows the rudder order after some latency.

Because the ship had two rudders, both of the elements described above had two distinct values, one for each rudder. These two values were very similar to each other, and so it was decided to analyze on only one of them. As a result of this decision, the remainder of this discussion refers to a single value for each parameter.

The graph of rudder order and status around the time of the Costa Concordia accident is shown in Fig. 4. The time scale ranges from about 1 min before the impact (marked on the graph with a black vertical line) to about 2 min afterward. By studying the graph while listening to the voice recordings from the bridge, it was confirmed that until about 21:44:40 the helmsman correctly fulfilled the orders (starboard 10, starboard 20, hard to starboard, mid ship). Then, while the ship's Master voice could be clearly heard delivering the order to bring the rudders to the port side (left), the helmsman instead brought them back to the starboard (right) side and kept them there for about 10 s, before correcting at about 21:44:55. Whether this error influenced the accident or not is an important subject for the ongoing investigation.

6.4. Watertight doors status

Another issue that emerged during the investigations is related to the status of the watertight doors. The watertight doors are hatches located in the lower decks of a ship, separating the lower hull volume into watertight compartments. In this way, when the hull is breached and a compartment is flooded, the other compartments are preserved and the ship is able to survive. The status of these watertight doors play a major role in the dynamics of a maritime accident, because a door left open could allow sea water to enter a non-damaged compartment thus quickening the sinking. To reduce this risk, international rules state that these doors must be shut before departing from a harbor and kept closed through the entire journey.

Watertight doors on board of the Costa Concordia are hydraulic operated devices that carry an autonomous electric power supply capable of performing three closing operations after the loss of external power. The closing operation can be performed manually or by remote command (for example from the so-called "safety room" on the bridge). Each door is fitted with a NMEA transmitter, which at fixed intervals sends its status to the VDR, in the form of a proprietary non-standard string. This information was used to reconstruct the status of watertight doors on the Costa Concordia immediately before and after the accident.

The strings depicting the watertight doors status are built as in the following example:

`$PSWTD, 07, C—, *34`where:

- $PSWTD is the preamble of the string. $ is the start character, P stands for non-standard string, S is the prefix created by the builder (Seanet), WTD stands for "Water Tight Door".

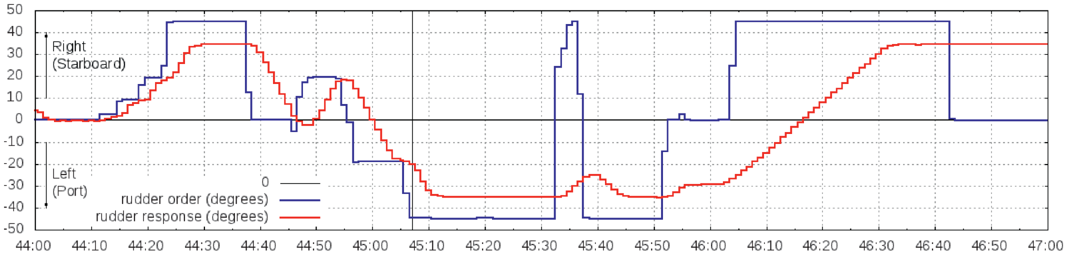


Fig. 4. Rudder order and status (in degrees) versus time (minutes and seconds from 21.00 of January 12th, 2012).

- 07 is the door number (ranging from 1 to 24).
- C—— is the status. The first letter states whether the door is open (O) or closed (C). The second character states whether the door is functioning correctly (−) or there is a fault (F). Other characters describe the kind of fault (L for low level of oil, P for low pressure, V for voltage loss).
- *34 is the checksum.

The doors transmit their status one at a time in a fixed interval, so that each door's status is updated every 16 s, approximately.

In order to ascertain whether the watertight doors were closed before, during and after the accident, a custom Python script was developed as part of this work to filter the doors NMEA statuses, order them chronologically, and report only the status changes. The output of this script revealed that a couple of doors did not declare a clear closed state before signal loss due to progressive flooding of the ship. An example of this behavior is shown in the following output:

```
**** Looking for door 08 ****
2012/01/13-21:00:07 - $PSWTD,08,C——,*35~0A
2012/01/13-21:19:15 - $PSWTD,08,O——,*31~0A
2012/01/13-21:19:30 - $PSWTD,08,C——,*35~0A
2012/01/13-21:22:07 - $PSWTD,08,O——,*31~0A
2012/01/13-21:22:54 - $PSWTD,08,C——,*35~0A
2012/01/13-21:26:01 - $PSWTD,08,O——,*31~0A
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
```

The above data shows that the last useful state of one door was "OFV–", which stands for a faulty open door, the fault being a loss of voltage. Whether this door was then closed after the loss of communication is still unclear.

The Costa Concordia, like many modern ships, has another system, called the Security Management System (SMS), that can provide additional details pertaining to watertight doors and other safety systems. The SMS is a network of computers supervising onboard safety devices such as the fire detection system, watertight doors system, and emergency shutdown system. Using NMEA strings related to the status of watertight doors system that this SMS sent to the VDR system. First, however, it was necessary to figure out the format of the custom NMEA sentences. The format, for the parts useful in this digital forensic investigation, is as follows:

`$PSM[12], K[AB...], {element,} checksum`where PSM1 or PSM2 states the server which originated the sentence, K states this is a descriptive (non-cumulative) sentence, the following letter is used to distinguish between sentences generated in the same time span (the first one is KA, then KB and so on). The field named "element" is the description of a single status. For the watertight doors, the status string is as follows:

`B[status]”WTD-[door_identification]`where *`door_identification`* is a string describing the door such as C08 (C is the deck, 08 is the door number) and *`status`* is a letter from the following list:

- O: open
- C: closed
- M: intermediate
- X: extra open (only for doors which can be more than 1200 mm wide when open).

As before, custom Python script was developed to extract status strings from the NMEA pool and identify the statuses related to a single door, such as the number 8 seen before. The results are shown below:

```
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
```

As can be seen in the above data, around the time of the accident the last condition of the door is *F*, which describes a fault condition, as was expected. The last status before this fault is *M*, which means "intermediate": a situation where the door is not completely open nor locked in close position. For unknown reasons, the status changes to *f* an hour later. These results are coherent with the analysis on the PSWTD sentences and confirm that the status of the doors cannot be clearly assessed.

6.5. *Check which route was set on the autopilot*

As part of the investigation there was a need to know which route had been planned on the autopilot, to later assess whether the navigation mishap was due to bad planning or to the Master not following the predetermined track. Forensic examination revealed two NMEA sentences that could prove useful to this goal: RAWPL and RARTE. RAWPL stands for "RAdar – Way Points List", and is used to describe a single geographic coordinate associated with an identification number; RARTE stands for "RAdar – RouTE", and describes a pre-planned route with a descriptive name and a list of waypoints. In the NMEA sentences extracted from the VDR we have found two alternate streams of waypoints/route, presumably one for each of the two radar screens. These findings were later confirmed by the radar screenshots also found in the VDR, which confirm that the radars were set on different routes (only one of them being fed to the autopilot, of course). One was the standard route, while the second was a custom one designed to navigate the ship close to Isola del Giglio. As an example, Figs. 5 and 6 show screenshots from the two main radar screens, both taken from the VDR memory and recorded at almost the same time.

The NMEA strings related to the two routes are the following:

```
$RAWPL,4221.5000,N,01104.0000,E,0006*4D~04
$RAWPL,4252.7000,N,01029.8000,E,0007*4C~04
```

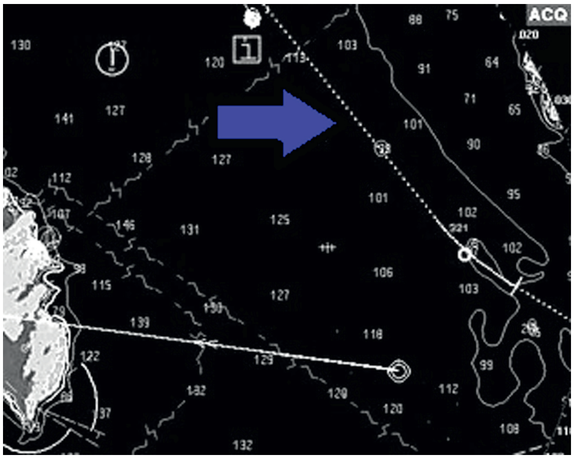


Fig. 5. Radar screenshot from the VDR depicting the standard route (the dotted line pointed at by the arrow).

```
   $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
```

The above output contains two blocks, each bound to one of the radar screens and comprising a list of waypoints (RAWPL sentences) and a route (RARTE sentences). The names assigned to the routes are the following:

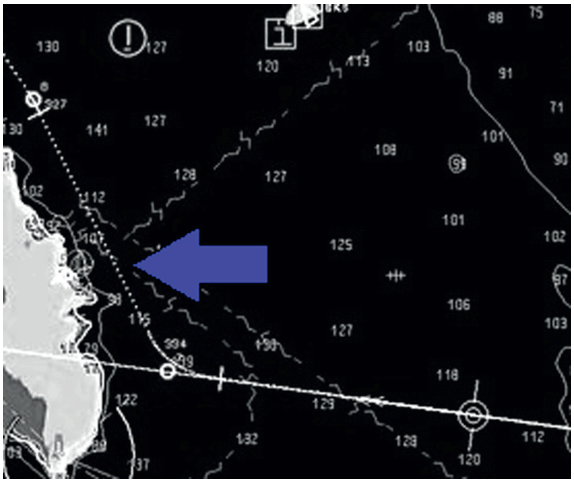


Fig. 6. Radar screenshot from the VDR depicting the custom route to pass close to Isola del Giglio (dotted line pointed at by the arrow).

- 1 Civitavec-Savona
- 9012 Civitavec-SavonaGI

The main content of the names is obviously related to the two ends of the route, the Italian ports of Civitavecchia and Savona. One can speculate that the suffix GI appended to the second route is related to the ship passing close to Isola del Giglio. Regarding the number appended before the names, one can speculate that the number 1 means that route is the standard first leg of the cruise, while the value 9012 could denote a custom route (in simple industrial interfaces, in which lists are alphabetically ordered, it is a common practice to name 9000-something the non-standard elements, so they are always listed after the standard ones).

6.6. *What was steering the ship*

Another element which could prove useful during the investigation is the assessment of what was in charge of steering the ship. A modern cruise ship such as the Costa Concordia, in fact, can be steered by many drivers, either automatic, such as an autopilot, or man controlled. The operators of the ship can steer it via different devices, different from each other by position (in the main bridge or outside) and by kind. These devices can be split into two different categories: FU, follow-up, and NFU, non-follow-up. In FU mode the rudder stops when the selected position is reached. In the case of NFU tiller steering, the rudder moves in the pre-selected direction as long as the tiller is being actuated. The position of the rudder in this case can be verified by observing the rudder angle indicator. The steering wheel on the bridge is a FU device.

During the forensic analysis the authors were able to discover a non-standard NMEA string, named $PAVBIOP, which carries three decimal integer values as payload. We found in a configuration file hidden in the VDR concentrator hard disk a possible glossary of the meaning of each binary bit in these three numbers, and by intuition and several attempts we were able to confirm this correspondence with a good degree of confidence. Among these values there were alarm bits, mostly related to failures of different pumps (which we supposed to be related to the rudders), and status bits indicating the in-command status of the different steering devices of the ship.

In brief, forensic analysis of this data found that, until about 10 min before the accident, the second value in the payload of the NMEA string $PAVBIOP was in range 1228–1288, which means that among the most significant bits the one which is assessed is the number 10, which, according to the configuration file we found, means: “Trackpilot 1 in command”.

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

$1228_{10} = 0000\mathbf{1}0011001100_2$

This lasts until 21:35:07, when the aforementioned value enters the range 37068–37102, in which among the most significant bits the ones asserted are the number 12 and the number 15, which respectively mean “FU Handweel selected” and “FU Handweel in command”.

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

$37068_{10} = \mathbf{1}00\mathbf{1}000011001100_2$

This confirms what was heard from the voice recordings from the VDR: the ship was being steered by the autopilot until 21:35, when the Master asked to switch it off. From then the helmsman was in charge of steering the ship using his handwheel.

7. Conclusions

Most investigations into ship accidents will have associated data on VDR systems that can be used to reconstruct events in great detail. Digital forensics techniques can be applied to these devices and provide a deeper insight into the data, particularly when problems are encountered either on the hardware or on the software side. In this paper we described how we approached the investigation on the Costa Concordia shipwreck for what it concerned the digital forensic aspects. We talked about the unresolved issues in the digital investigation on maritime accidents due to lack of standardization in data on VDR systems which makes forensics analysis more challenging, but we also demonstrated how we've been able to overcome these obstacles. We provided an in-depth analysis of some of the elements we were able to retrieve to help the ongoing investigation by studying the raw data extracted from the actual VDR of the ship. As future work, we plan to leverage this kind of investigation by designing and proposing forensically-sound standards for recording, storing and interpreting data, and by providing maritime accidents investigators with standard software tools to retrieve the data in the same way we have been able to do.

Acknowledgments

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.

References

Carrier Brian. Defining digital forensic examination and analysis tools using abstraction layers. International Journal of Digital Evidence Winter 2003;1(4).

Carpinteri F, Cavo Dragone G, Dalle Mese E, Mestro M. Relazione tecnica dei consulenti nominati dal GIP del Tribunale di Grosseto [Technical report of the consultants appointed by the judge for preliminary investigations of the Court of Grosseto] September 11, 2012.

Andrew Guest. Feature: black box or black hole? Retrieved on April 2013 from: https://www.bimco.org/News/2010/01/20_Feature_Week_03.aspx.

International Maritime Organization. International convention for the Safety Of Life At Sea SOLAS 1974.

International Maritime Organization. Resolution A.861(20) "Performance standards for shipborne Voyage Data Recorders (VDRs)". Adopted on November 27, 1997.

International Maritime Organization. Resolution MSC.163(78) "Performance standards for shipborne simplified Voyage Data Recorders (S-VDRs)". Adopted on May 17, 2004.

International Maritime Organization. SN/Circ/246 Recommended means for extracting stored data from Voyage Data Recorders (VDRs) and Simplified Voyage Data Recorders (S-VDRs) for investigation authorities 2005.

Maritime Accident Casebook. Maersk Kendal – Complacency, BTM, Culture and VDRs. Retrieved on April 2013 from: http://maritimeaccident.org/?p=7070.

National Marine Electronics Association (NMEA). NMEA 0183 standard. Retrieved on April 2013: http://www.nmea.org/content/nmea_standards/nmea_0183_v_410.asp.

Wikipedia. Costa Concordia disaster. Retrieved on October 2012 from: http://en.wikipedia.org/wiki/Costa_Concordia_disaster.