DIGITAL FORENSICS E SUA APPLICAZIONE AD APPARECCHIATURE DI BORDO

Paolo Gubian[1], *Mario Piccinelli*[1]

[1] Dipartimento di Ingegneria dell'Informazione, Università di Brescia
Via Branze, 38 - 25123 Brescia, e-mail paolo.gubian@unibs.it

Parole chiave: Digital, Systems, Forensics

La Digital Forensics è la disciplina che si occupa della analisi, con lo scopo di accertare fatti di interesse in indagini e procedimenti giudiziari, di apparecchiature digitali in genere, e in particolare di computer tradizionali, nelle loro varie accezioni. Il processo di Digital Forensics passa per le fasi di individuazione, estrazione, protezione, conservazione e documentazione dei dati. Fa parte della discipline della Digital Forensics anche la attività di sviluppo degli strumenti, hardware e/o software, di uso generale o specifico, per supportare l'analista forense nello svolgimento delle varie fasi della sua attività.

L'attività di ricerca locale sulla Digital Forensics, fin dall'inizio si è orientata verso i dispositivi digitali più moderni, diversi dai tradizionali personal computer per i quali la letteratura è decisamente più ricca: i dispositivi portatili in genere, e in particolare gli smartphone, le smartcard e le SIM, i dispositivi embedded in generale e, recentemente, anche più specificamente alle apparecchiature di bordo di una nave. Il coivolgimento di ricercatori dell'Unità nel procedimento giudiziario relativo al naufragio della Costa Concordia del gennaio 2012 ha portato allo sviluppo di metodologie e strumenti ad-hoc per l'analisi dei dati presenti nelle decine di sottosistemi digitali a bordo di una grande nave, al fine di rispondere a "quesiti" posti dalla Autorità Giudiziaria, secondo i canoni e le pratiche della Digital Forensics.

A bordo di una grande nave da crociera decine di sottosistemi digitali collegati a migliaia di sensori, e tra loro interconnessi. I principali sono il VDR (Voyage Data Recorder), la Ship Automation, il sistema di monitoraggio di tutte le parti della nave a fini di sicurezza e il sistema per il mantenimento della stabilità in navigazione. Questi sistemi sono costituiti da computer tradizionali, computer industriali, microcontrollori, sensori e attuatori, tra loro collegati con reti e protocolli standard, protocolli industriali e link di comunicazione di basso livello (in genere link seriali). L'estrazione dei dati, la loro analisi e presentazione ai fini dell'utilizzo in un evento che comprende un incidente richiede un mix di metodi ad-hoc, strumenti di analisi tradizionali e strumenti sviluppati appositamente per l'applicazione, ma suscettibili di essere estesi ad altri casi di navi di vario genere.

Un primo insieme di risultati rilevanti si è ottenuto con la analisi del VDR (Voyage Data Recorder) della Costa Concordia, un sottosistema costituito da sensori intelligenti, link seriali, un computer industriale, collegamenti con altri sottosistemi di bordo e un modulo di registrazione dati a prova di incidente, colloquialmente ed impropriamente chiamato "scatola nera". L'estrazione e l'analisi dei dati del VDR, oltre a dare conferma di fatti importanti nella evoluzione dell'incidente, come l'ormai noto presunto errore del timoniere oppure i problemi dovuti al malfunzionamento del generatore elettrico di emergenza, ha portato allo sviluppo e alla codifica di una metodologia strutturata di approccio alla analisi di questi sistemi, presenti su tutte le navi medio/grandi, e allo sviluppo di strumenti software ad-hoc, ma facilmente riconvertibili ad altre situazioni, per la analisi e la presentazione sintetica dei dati del VDR. Tali strumenti sono stati utilizzati nell'incidente probatorio istituito appena dopo il naufragio e nel procedimento penale in corso, e mostrati su diversi mezzi di comunicazione incluse le principali reti televisive nazionali.

I dati estratti dal VDR, combinati con altri dati raccolti da altre fonti tra cui diversi altri sottosistemi di bordo, hanno poi consentito di sviluppare un modello matematico short-term del movimento della nave, basato su un insieme di equazioni differenziali ordinarie di tipo "black box", cioè con coefficienti da determinare conuna procedura di fitting che fa uso proprio dei dati di navigazione. Il modello è stato validato su dati reali di navigazione e poi applicato alla simulazione degli ultimi minuti prima dell'incidente e ad uno studio "what-if" dell'effetto del presunto errore del marinaio timoniere sulle conseguenze dell'incidente (danni alla nave).

BIBLIOGRAFIA

[1] M.Piccinelli, P. Gubian (2013), "Modern Ships Voyage Data Recorders: a Forensics Perspective on the Costa Concordia Shipwreck", *Proc. DFRWS Digital Forensics Research Workshop*, Monterey CA (USA), 4-7 agosto 2013, also published in Digital Investigations, Special Issue: DFRWS 2013, Elsevier.

[2] P.Neri, M.Piccinelli, P.Gubian, B.Neri (2014); " A Ship Motion Short Term Time Domain Simulator and its Application to Costa Concordia Emergency Manoeuvres Just Before the Shipwreck at Giglio Island ". *Proc. ECMS European Conference on Modelling and Simulation 2014*, Brescia, Italy, May 27-30 2014 [Best Paper Award].