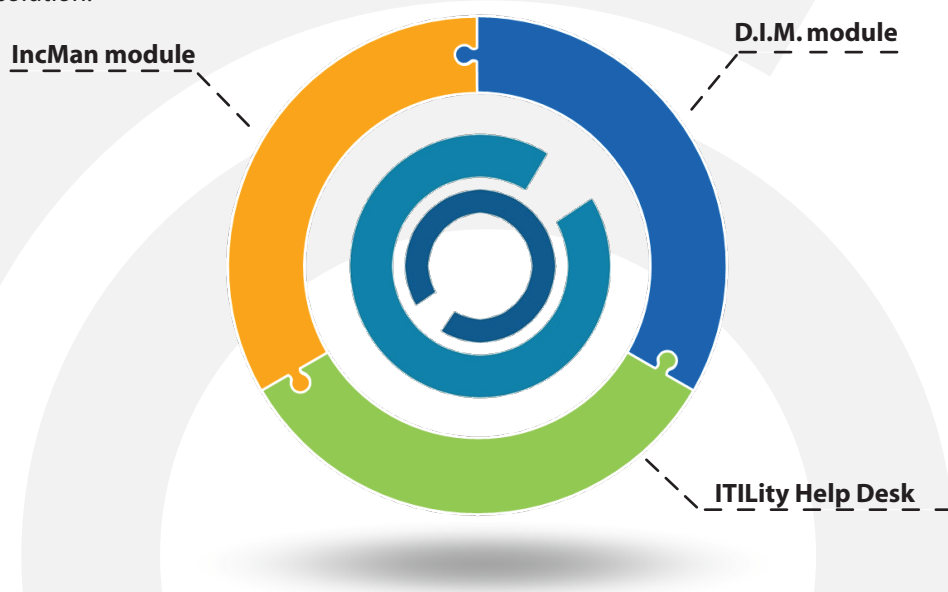


IncMan Suite

Incident Management Suite

DF Labs is proud to present the Incident Management Suite enabling the management, in a unique solution, of every kind of information security incidents. DFLabs IncMan Suite supports the entire incident management process from troubleshooting to security, including digital forensics.

The IncMan Suite comprises three modules that can operate autonomously or collaborate in order to obtain an incident management centralized solution.



INCMAN SUITE - Modules

IncMan Suite enables the development, through the combination of the three modules, of a tool focused on its own needs.

INCMAN MODULE	D.I.M. MODULE	ITILity HELP DESK
Incident Manager (IncMan) is the integrated solution for the complete management of security incidents, IT and Corporate.	D.I.M. is a Digital Evidence Tracker Software used in digital investigations. D.I.M. has been designed and developed to be used as Digital Evidence process Support during computer Forensics and Incident response Operations	ITILity is a framework of best practices to manage IT operations and services. It is designed to provide a complete support solution, to streamline helpdesk processes

IncMan Suite is the first IODEF compliant suite.

The data gathered during an incident are organized according to the IODEF standard (Incident Object Description and Exchange Format) RFC 3067 and RFC 5070. In order to enable the exchange of information through IODEF, **IncMan suite** offers an integrated system of import/export of XML files.

The interface contains an integrated XML Viewer in order to visualize and analyze the incident report in XML.

DF Labs collaborated with IETF (Internet Engineering Task Force) during the implementation of the IODEF standard.

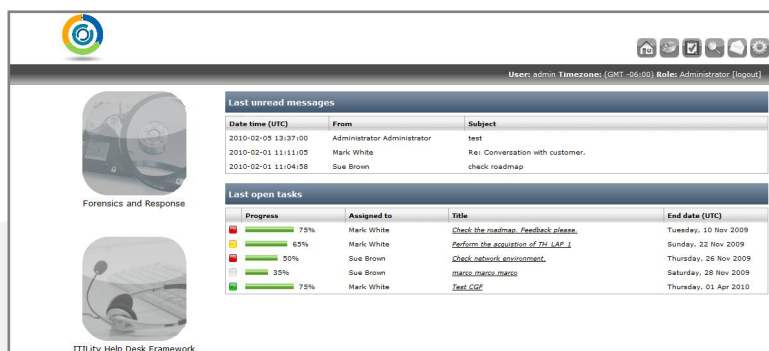
This module enables the total control of the artifacts:

- Artifact analysis
- Artifact response
- Artifact response coordination

D.I.M. enables to divide operations into cases. Every case can contain an unlimited number of Hosts (Workstation, Server, Laptop, Handled); one or several evidence (Hard Disk, CD/DVD-ROM, Memory Card, Log File, Network Dump) are linked to every host.

Photographic documentation can be associated with every host or evidence. Every photo is analyzed and, if it was taken with a digital camera, D.I.M is able to reveal the content of the EXIFF section (Time Stamp)

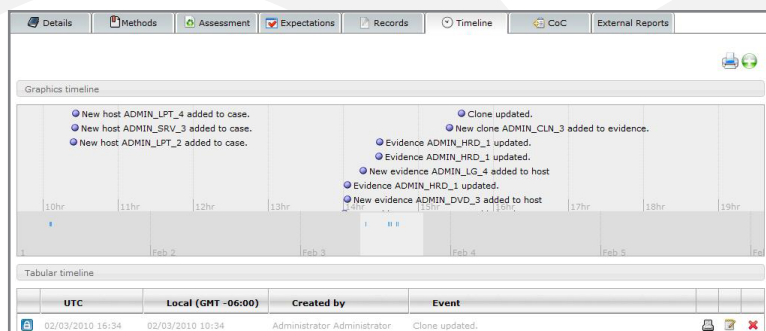
The D.I.M module enables the synchronization between the local database of the forensic laboratory and that the investigators.



INCMAN MODULE

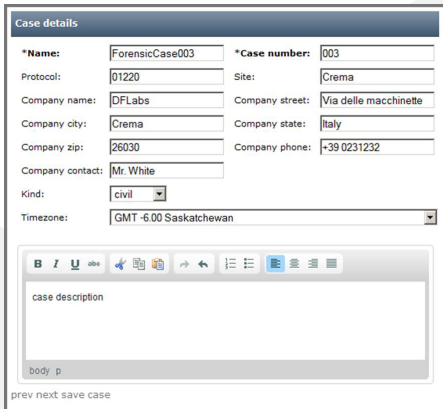
IncMan is the module for managing information security incidents in a company and offers the possibility to generate incident reports compliant with the most strict international standards. It also makes possible a careful economic analysis of direct and indirect damage caused by the incident:

- Company assets involved in the incident
- Work days
- Other costs

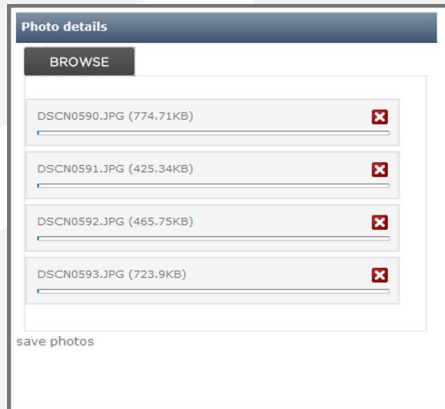


D.I.M. MODULE

Digital Investigation Manager (D.I.M) is a digital evidence management designed and developed in order to be used in IT environments during Incident Response and Forensic Acquisition. The application enables the user to catalog all the relevant information gathered and to generate reports.



The screenshot shows the 'Case details' form in the D.I.M. application. The form contains fields for Case Name, Case number, Protocol, Site, Company name, Company street, Company city, Company state, Company zip, Company phone, Company contact, Kind, and Timezone. There is also a section for 'case description' and 'body p'.



The screenshot shows the 'Photo details' form in the D.I.M. application. The form contains a 'BROWSE' button and a list of photo files with their sizes and a 'save photos' button.

The D.I.M module offers investigators the possibility to print a barcode and apply it to a host and/or media, avoiding thus to accidentally release information. Besides, the user can read the barcode generated by the D.I.M Barcode and very easily recover all the information about the evidence under investigation.

Incident management and problem management offer the user a simple and immediate interface in order to fully support the following:

- Problem logging
- Categorization
- Prioritization
- Investigation and diagnosis
- Solution
- User Satisfaction

The ITILity Help Desk allows the introduction of the concept of IT incident in the **IncMan Suite**. Enabling this module triggers the addition of sections such as:

- Ticket management
- Solution management

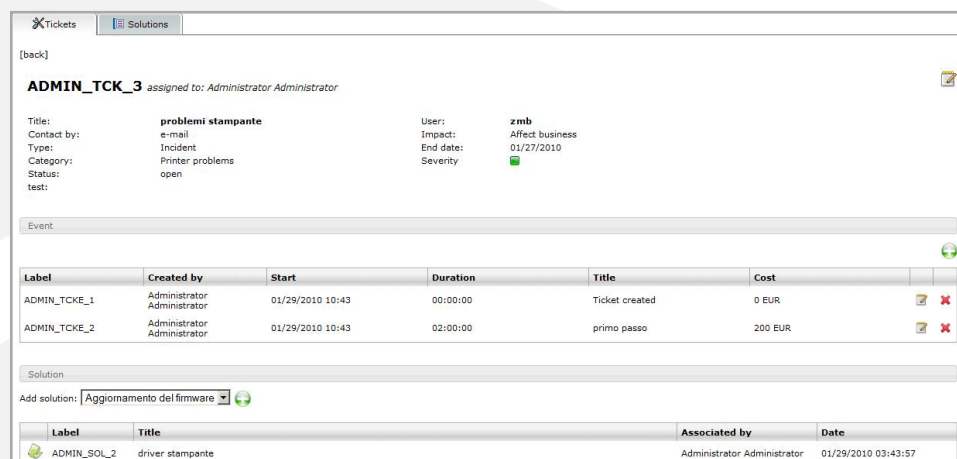
The **IncMan Suite** dashboard is designed in order to render the maximum visual impact in a format studied for the immediate comprehension of data using a combination of graphics, scales and visual indicators. The dashboard supplies other data related to all cases and incidents managed. This information is largely used by roles such as administrators, supervisors, in order to have a summarizing overview from which to derive strategic information.

A powerful and flexible profiling system in order to enable the operators involved in the security incident specific access to the case /incidents data as to the different features of the product.

ITILity HELP DESK

The ITILity Help Desk process is intended to reduce the number and severity of incidents, and report it in documentation to be available for the first-line and second line of the help desk. The ITILity Help Desk module:

- Allows to thoroughly and systematically manage tickets
- Allows to completely track all activities linked to a single ticket
- Allows to recover all essential information through immediate interface.



ADMIN_TCK_3 assigned to: Administrator Administrator

Title: **problemi stampante** User: **zmb**
 Contact by: e-mail Impact: Affect business
 Type: Incident End date: 01/27/2010
 Category: Printer problems Severity: ■
 Status: open
 test:

Event:

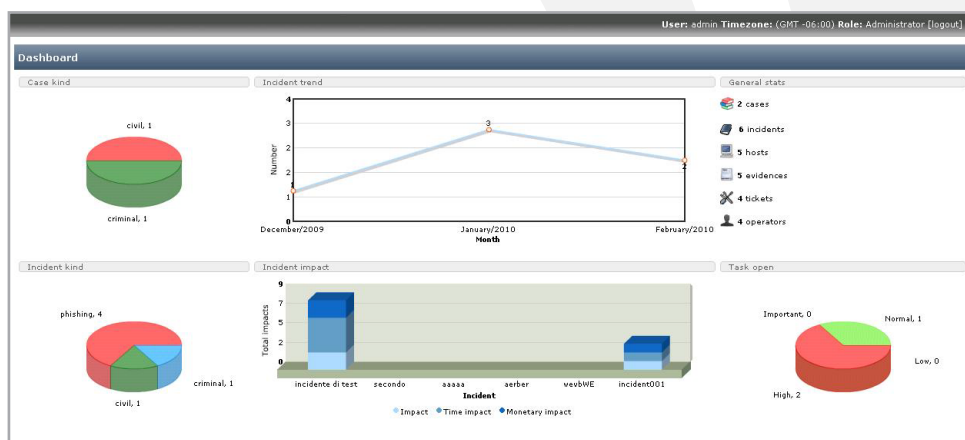
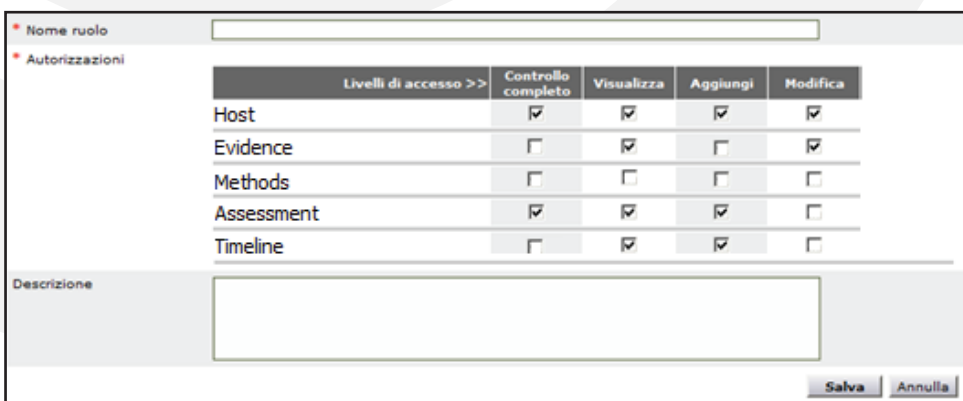
Label	Created by	Start	Duration	Title	Cost
ADMIN_TCKE_1	Administrator	01/29/2010 10:43	00:00:00	Ticket created	0 EUR
ADMIN_TCKE_2	Administrator	01/29/2010 10:43	02:00:00	primo passo	200 EUR

Solution

Add solution: **Aggiornamento del firmware**

Label	Title	Associated by	Date
ADMIN_SOL_2	driver stampante	Administrator Administrator	01/29/2010 03:43:57

DASHBOARD

*** Nome ruolo**

*** Autorizzazioni**

	Livelli di accesso >>	Controllo completo	Visualizza	Aggiungi	Modifica
Host	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Evidence	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Methods	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Assessment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Timeline	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Descrizione

Salva **Annulla**

Compatible and standard compliant

Complying with the standard is not just the requisite for incident management but specific to every section of the suite. The entire design of the interface is compliant with the directives delineated by the **W3C** consortium. The **IncMan Suite** supports the most common browsers.

IncMan Suite promotes the **LAMP** technology; through the combination of the best-known technologies on the market (webserver, DBMS and script language). The use of this solution enables us to have a totally platform independent tool.

* Technical specification

Processor Quad Core Xeon X3323,
2.5GHz;
4GB DDR2 667MHz Memory
2 Hard Disk 500 GB SATA 7.2k 3.5"
HD Hot Plug SAS 6iR internal RAID
controller, PCI-e 1 S
Rack Chassis
Hot-Plug HD Cage
Internal SATA DVD-ROM Drive
2 Broadcom Gigabit Ethernet NIC
4 USB 2.0 Port

The first step for incident management is prevention, the **IncMan Suite** integrates an automated backup system that besides database dump, encrypts it with PGP.

IncMan Suite offers the user a centralized configuration system enabling him to personalize different aspects of the tool such as:

- Report (details regarding the heading of the reports generated)
- International settings (currency, timezone)
- SMTP configuration (enabling the possibility to automatically send emails following specific conditions)
- LDAP support
- User management
- Company information
- Automatic backup of the database, database management fields
- Automatic events notification

The **IncMan Suite** offers also a set of very interesting features such as the following:

Internal messaging system that guarantees a continuous and immediate messages exchange between investigators.

Integrated system for the management of tasks assigned to every investigator. The administrator can monitor the progress of every operation assigned and eventually communicate new details.

new section dedicated to **reports** that allows to **generate PDF** files in order to exchange documents. Besides it is important to set up periodic reports in order to constantly monitor incident management.

APPLIANCE

The **IncMan Suite HW Appliance** is a highly professional, multi-user and handy solution for Incident Handling, Digital Forensics and e-discovery solutions. The solution, available also in virtual machine, is completely configured and secured by qualified personnel.



DFLABS INCMAN SUITE COMPRISES THE FOLLOWING:

- High performance hardware appliance *
- Automatic backup of the database
- **2 days training** (onsite, local, online)
- 24h support NBD (Next Business Day)