



D.I.M. – Digital Investigation Manager
IODEF Implementation Report
66th IETF Meeting

Dario Forte

Cristiano Maruti

Thomas Orlandi

Michele Zambelli

Who we are

- Dflabs is a company founded in 2002 by Prof. Dario Forte
- All the employees are former/contemporary University of Milano at Crema Graduate students
- We are also part of the IRItaly Project (Incident Response Italy) born at University of Milano at Crema and part of the Honeynet Project.
- Prof Forte is also part of the DFRWS Tech comm.

Why D.I.M.

- Digital Investigation Manager born to Support incident response.
 - Global Reports
 - Operation Timeline
 - Digital Forensic Support
 - Preservation Phase Support
- Multi-User Environment
 - Unlimited number of cases
 - Local and Remote Db
 - Synchronization Module
- Automated Reporting Features
- Total logging

Procedure Support

- D.I.M. can support both documental and operating procedures; i,e,
 - Incident Reports
 - Media acquisition
 - Chain of custody of media, log etc,
- All the evidence collecting process can be managed, including pictures, and external documents
- The Database allows multiple queries

Database Scheme, main tables

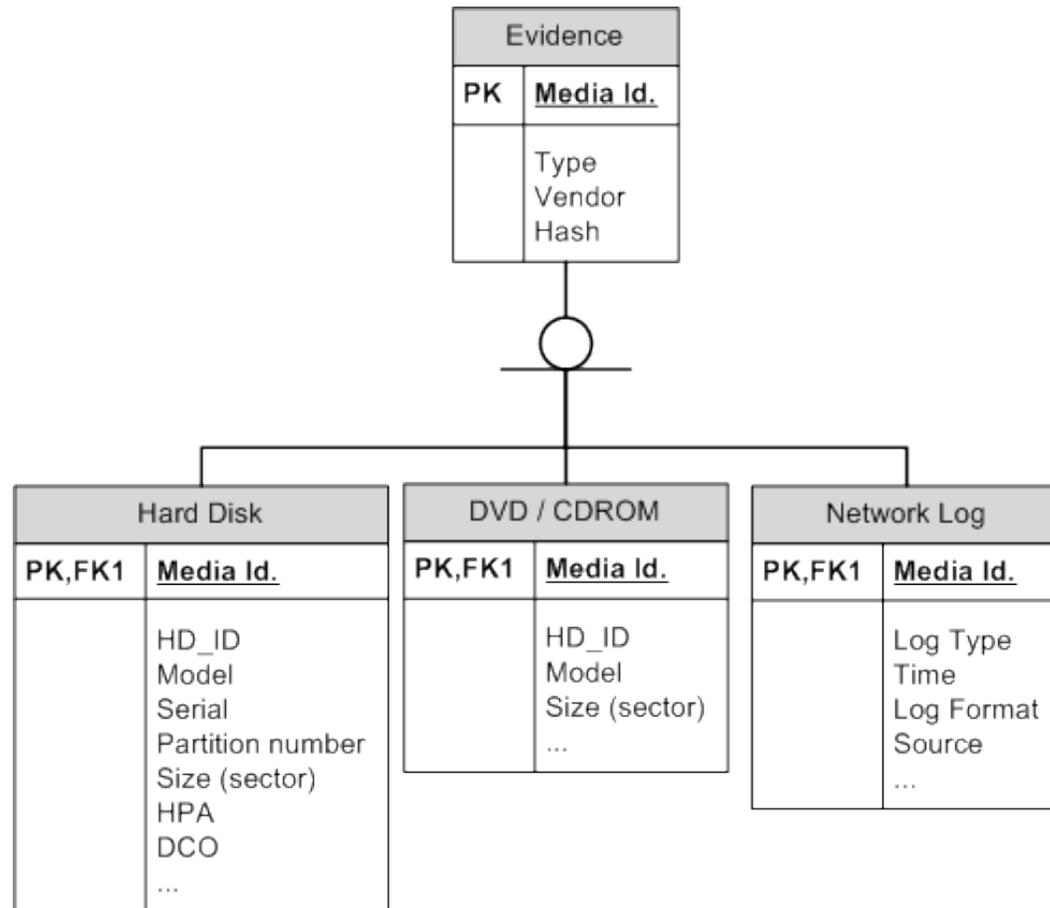
CASE

CASE	
PK	<u>Case ID</u>
	Info Company Contacts Type Date Investigator Note State ...

HOST

HOST	
PK	<u>Host ID</u>
	Model Serial CompanyID Owner Photo Bios

EVIDENCE



Case Information

The screenshot displays the DFLabs - Digital Investigation Manager v. 1.0 interface. The left sidebar shows a tree view of the case structure, including Investigation 001 and its sub-items: WK_7, WK_6, WK_5, WK_4, WK_3, WK_2, LAP_1, and WK_0, each with associated HD, CDVD, MC, LOG, and HD files. The main panel shows the 'General' tab with the following case information:

Case Info

Name:	Investigation 001	Description:	This is a demonstration Case
Creation Site:	Milan, corso Lodi		
Type:	CIVIL		
Supervisor:	Michele Zambelli		

Customer/Company

Name:	Customer Test
Supervisor:	via Dante, Bologna 034587284
Address, Tel:	Bianchi

Case Date/Time

Creation (GMT):	21/06/2006 15.26.44
Creation Offset:	100
Creation Local Time:	21/06/2006 16.26.44

Buttons: Edit General Info, Delete General Info

Case Statistic

Total Hosts:	8	Total Evidences:	11	Media:	10
Total Photos:	5			Log:	1
				Net. Dump:	0

Annotations: An orange arrow points from the text 'Local or Remote Connection' to the bottom of the left sidebar. Another orange arrow points from the text 'Operation Log' to the bottom of the main panel.

Local or Remote
Connection

Operation Log

Photographic Documentation

DF Labs - Digital Investigation Manager v. 1.0

Main Case Option About

Investigation 001

- Wk_7
 - HD_9
 - HD_1
- Wk_6
 - HD_2
- Wk_5
 - CDVD_3
- Wk_4
 - HD_0
- Wk_3
 - HD_4
- Wk_2
 - CDVD_5
- LAP_1
 - MC_10
 - HD_6
- Wk_0
 - LOG_7
 - HD_8

General Photos Timeline Report

Show photo

Original EXIFF
Photo Record

Add New Edit Delete

Photo Info

Creation Date/Time: 2005.11.17 18:28:42

Original MD5: 161774457F3433B82BB01E11E398942B

Original SHA1: 24B4A0877B2BF98638C79E252FD75F7922CFC396

Info:

Save

Connected to: localhost 04/07/2006 16.08.17 - Open Case: 'Investigation 001' DFLabs

Operation Timeline

DFLabs - Digital Investigation Manager v. 1.0

Main Case Option About

General Photos Timeline Report Label

Investigation 001

- Wk_7
 - HD_9
 - HD_1
- Wk_6
 - HD_2
- Wk_5
 - CDVD_3
- Wk_4
 - HD_0
- Wk_3
 - HD_4
- Wk_2
 - CDVD_5
- LAP_1
 - MC_10
 - HD_6
- Wk_0
 - LOG_7
 - HD_8

date_time	operator	event	info
22/06/2006 10.21.54	Zambelli	Add New Media: Name->'MC_10'	Digital Photo Camera, Memory Card
22/06/2006 10.22.55	Zambelli	Add New Media: Name->'HD_1'	
22/06/2006 10.22.55	Zambelli	Add New Media: Name->'HD_3'	Hard Disk is broken, no spin up !
22/06/2006 10.22.55	Zambelli	Add New Media: Name->'HD_4'	
22/06/2006 10.22.55	Zambelli	Add New Media: Name->'HD_5'	
22/06/2006 10.22.56	Zambelli	Add New Media: Name->'HD_6'	
22/06/2006 10.22.56	Zambelli	Add New Media: Name->'HD_7'	
22/06/2006 10.22.56	Zambelli	Add New Media: Name->'HD_8'	
22/06/2006 10.22.57	Zambelli	Add New Media: Name->'HD_9'	
22/06/2006 10.22.57	Zambelli	Add New Media: Name->'HD_10'	
22/06/2006 10.22.57	Zambelli	Add New Media: Name->'HD_11'	
22/06/2006 10.22.59	Zambelli	Add New Media: Name->'HD_12'	
22/06/2006 10.23.03	Zambelli	Add New Media: Name->'HD_2'	

+ - ▲ ↶ ✕ ↷

Report Generation

DF Labs - Digital Investigation Manager v. 1.0

Main Case Option About

General Photos Timeline Report

Investigation 001

- Wk_7
 - HD_9
 - HD_1
- Wk_6
 - HD_2
- Wk_5
 - CDVD_3
- Wk_4
 - HD_0
- Wk_3
 - HD_4
- Wk_2
 - CDVD_5
- LAP_1
 - MC_10
 - HD_6
- Wk_0
 - LOG_7
 - HD_8

Report

Modulo ingresso supporti

Timeline

Case Detail

Host Detail

Evidence Detail

Save Selected Report

Digital Investigation Manager Version 1.0	Case Name Investigation 001	
Company name Customer Test	Type of investigation CIVIL	Supervisor Michele Zambelli
Company contact Bianchi	Site Milan, corso Lodi	
Additional info Additional info...	Company detail via Dante, Bologna 034587284	

Hosts Description

Owner	Model	Serial	ID
Rossi	Acer pro 60	mdwq234me1	WK_0
Bianchi	Acer pro 60	adsdsa23e23	LAP_1
Verdi	Acer pro 60	asd3223	WK_2
Rossi	Siemens p100	sdf2r23	WK_3
Bianchi	Siemens Inspire	df234r1	WK_4
Rossi	Siemens p100	aqdq234234	WK_5
Rossi	Asus 8900	xvsgret	WK_6
Bianchi	Asus 8900	qwex12312	WK_7

Prev Next

D.I.M Vs. IODEF

- Each single case can be associated with an XML IODEF compliant documents.
- The validation scheme is based upon **iodef-07 del draft ietf**
- The initial XML file generation is Wizard driven
- The structure of the document is a tree totally upgradable
- External XML Documents can be imported
- Two Way Synchronization of IODEF files with the remote DB
- The IODEF Infos will be part of the final report

How we conducted the test

- 1st part: we worked on our files and external files to validate them reciprocely;
- 2nd part: after Brian Trammel's review we have added more programming and re-tested the application
- Tests were positive

Wizard 1, General Info

- Users are required to fill the **mandatory** IODEF infos

IODEF - Wizard: 1 of 3

DFLabs

draft-ietf-inch-iodef-070

Incident
This class provides a standardized representation for commonly exchanged incident data and associates a CSIRT assigned unique identifier with the described activity.

purpose: Choose

lang: Choose

restriction: Choose

Incident ID
IncidentID represents an incident that identifies the activity characterized by the incident.

UID:

GUID Name:

Name:

Report Time
The time the incident was reported.

23/06/2006 10.49.10

Based on: The Incident Object Description Exchange Format Data Model and XML Implementation draft-inch-ietf-iodef-07.txt

Next >

1. Public. There are no restrictions placed in the information;
2. Need-to-know. The information may be shared with other parties that are involved in the incident (e.g., multiple victim sites can be informed of each other);
3. Private. The information may not be shared;
4. Default. The information can be shared according to an information disclosure policy pre-arranged by the communicating parties.

Wizard 2, Assessment section

IODEF - Wizard: 2 of 3

DF Labs

draft-ietf-inch-IODEF-070

Assessment

Attributes
This attribute indicates the disclosure guidelines to which the sender expects the recipient of the IODEF Document

Restriction

Confidence
The Confidence class represents a best estimate of the validity and accuracy of the described impact of the incident activity

Rating

Impact
The Impact class allows for categorizing and describing the technical impact of the incident on the network of an organization.

Value

Attributes

severity

completion

type

Time Impact
The element content will be a numeric value (REAL) specifying a unit of time

Value

Attributes

severity

metric

duration

Monetary Impact
The MonetaryImpact class describes the financial impact of the activity on an organization. For example, this impact may consider losses due to the cost of the investigation or recovery, diminished productivity of the staff, or a tarnished reputation that will affect future opportunities.

Value

Attributes

severity

currency

Based on: The Incident Object Description Exchange Format Data Model and XML Implementation draft-inch-ietf-iodef-07.txt

Next >

1. low. Low confidence in the validity;
2. medium. Medium confidence in the validity;
3. high. High confidence in the validity.

Wizard 3, Contact Section

IODEF - Wizard: 3 of 3

DF Labs
draft-ietf-inch-iodef-070

Contact

Attributes

The Contact class describes contact information for organizations and personnel involved in the incident. This class allows for the naming of the involved party, specifying contact information for them, and identifying their role in the incident.

Contact Name role

Postal Address type

Fax restriction

Telephone Time Zone

Mail

Description

Registry Handle

The RegistryHandle class represents a handle to an Internet registry or community-specific database. A handle consists of a name specified in the element content, and the database to which it belongs specified in the type attribute.

Value registry

1. creator. The entity that generate the IODEF document;
2. admin. An administrative contact for a host or network;
3. tech. A technical contact for a host or network;
4. irt. The CSIRT involved in handling the incident;
5. cc. An entity that is to be kept informed about the handling of the incident.

Based on: The Incident Object Description Exchange Format Data Model and XML Implementation draft-inch-ietf-iodef-07.txt

Finish

Tree view Section, features

- Tree View visualization of the XML document generated by the wizard
- External XML Documents can be imported
- Further elements can be added/modified
- Editing , via wizard/form, of the document
- Integrated browser XML structure

Tree Section, Setting Tab

The screenshot displays the Digital Investigation Manager (DFLabs) interface for a draft document titled "draft-ietf-inch-iodef-070". The interface is divided into two main sections: a Tree Section on the left and a Setting Tab on the right.

Tree Section: This section shows a hierarchical tree view of the document structure. The root node is "iodef:IODEF-Document", which contains several attributes such as "version", "xmlns:iodef", "xmlns:ds", "xmlns:xsi", "xsi:schemaLocation", and "lang". Below this is the "iodef:Incident" node, which includes attributes like "purpose", "restriction", and "iodef:IncidentID". The "iodef:Incident" node is expanded to show its children: "iodef:AlternativeID", "iodef:ReportTime", "iodef:Description", "iodef:Assessment", "iodef:Method", "iodef:Contact", "iodef:EventData", and "iodef:History". The "iodef:Contact" node is further expanded to show its attributes, including "role", "type", "iodef:ContactName", "iodef:Description", "iodef:PostalAddress", "iodef:Email", "iodef:Telephone", and "iodef:Timezone".

Setting Tab: This section is titled "Setting" and "XML Previews". It contains four main configuration panels, each with an "Add" button:

- Assessment:** Contains an "Attributes" section with a "restriction" dropdown menu.
- Confidence:** Contains an "Attributes" section with a "rating" dropdown menu.
- Impact:** Contains a "Value" text input field and an "Attributes" section with "severity", "completion", and "type" dropdown menus.
- Time Impact:** Contains a "Value" text input field and an "Attributes" section with "severity", "metric", and "duration" dropdown menus.
- Monetary Impact:** Contains a "Value" text input field and an "Attributes" section with "severity" and "currency" dropdown menus.

At the bottom of the Setting Tab, there is an "Add & Close" button. The interface also features a "Save To XML" button and a "Print" button at the bottom.

Footer: The text "draft-ietf-inch-iodef-070" is displayed at the bottom left, and the "DFLabs" logo is at the bottom right.

Tree Section, XML Tab (based upon: doc01-simple-event.xml)

The screenshot displays the Digital Investigation Manager (DF Labs) interface. The window title is "Digital Investigation Manager -DFLabs - Draft-ietf-inch-iodef-070". The interface is split into two main panes.

Left Pane (Tree View): Shows a hierarchical tree structure of the XML document. The root is `iodef:IODEF-Document`, which contains several child elements: `[version = "1.00"]`, `[xmlns:iodef = "draft-ietf-inch-iodef-070.xsd"]`, `[xmlns:ds = "http://www.w3.org/2000/09/xmldsig#"]`, `[xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance"]`, `[xsi:schemaLocation = "draft-ietf-inch-iodef-070.xsd"]`, `[lang = "en-US"]`, `iodef:Incident`, `iodef:Assessment`, `iodef:Method`, `iodef:Contact`, `iodef:EventData`, and `iodef:History`. The `iodef:Incident` element is expanded, showing sub-elements like `[purpose = "reporting"]`, `[restriction = "public"]`, `iodef:IncidentID = 2`, `iodef:AlternativeID`, `iodef:ReportTime = 2006-06-07T10:06:14-04:00`, `iodef:Description = Detected distributed SYN flood`, `iodef:Assessment`, `iodef:Impact = Partial denial of service on target`, `iodef:Confidence`, `iodef:Method`, `iodef:Contact` (with details like `[role = "creator"]`, `[type = "person"]`, `iodef:ContactName = Brian Trammell`, `iodef:Description = MTS, CERT/NetSA`, `iodef:PostalAddress = Carnegie Mellon University`, `iodef:Email = bht@cert.org`, `iodef:Telephone = +1 412 268 9748`, `iodef:Timezone = -04:00`), `iodef:EventData`, and `iodef:History`.

Right Pane (XML Previews): Shows the XML code corresponding to the tree view. The code is color-coded and includes comments like `<!-- End Test 5 -->` and `<!-- End Test 7 -->`. Key elements visible include `<iodef:System>`, `<iodef:Flow>`, `<iodef:Expectation action="investigate">`, `<iodef:Description>` (with a description in English and a description in Japanese: `<iodef:Description lang="ja-JP">`), `<iodef:HistoryItem>`, and `<iodef:History>` (with a description: `<iodef:Description>Document created.</iodef:Description>`). The code ends with `</iodef:IODEF-Document>`.

At the bottom of the window, there are two buttons: "Save To XML" and "Print".

Below the screenshot, the text "draft-ietf-inch-iodef-070" is displayed on the left, and the "DF Labs" logo is on the right.

Implementation report: Our Files respect the IODEF after Trammel's Review (1)

- The files generated by DIM were validated via XSD Scheme (IETF). At this moment we used an external tool (Altova XMLSpy) to validate the XML structure
- INCH Interoperability Test - IETF 66: all the files were correctly imported.
- We submitted 2 files for evaluation and we received the following feedback:
 1. for dim-iodef-test1.xml : nearly validates against -070. There appears to be a problem with your ISO8601 (DateTime) representation (one-digit months and days always need leading zeroes). Also, the value of the MonetaryImpact element should not contain digit separators (12.000) to avoid locale issues. **FIXED**
 2. for dim-iodef-test2.xml : Same ISO8601 issues with validation. Also, PostalAddress should contain \$-separated lines of a full postal address, as in <http://www.cert.org/ietf/inch/interop-ietf66/001-simple-event.xml> **FIXED**

Implementation report: Our Files respect the IODEF after Trammel's Review (2) Based Upon rep02-scan.txt

- **Issue:** Reviewer referred to us that we needed to integrate our test using the incident report supplied by the interoperability test.
- **Action:** We integrated the test as required. The results are in the next slides:
`rep02-scan.txt`
- **Methodology:** We integrated our wizard and tested it against the CERT#339360 based report.

Wizard screenshot (1)

Wizard: 1 of 3

DF Labs
draft-ietf-inch-IODEF-070

Incident
This class provides a standardized representation for commonly exchanged incident data and associates a CSIRT assigned unique identifier with the described activity.

purpose: reporting
lang: en-US
restriction: public

Incident ID
IncidentID represents an incident tracking number (UID) that is unique in the context of the CSIRT and identifies the activity characterized in an IODEF-Document.

UID: CERT#339360
GUID Name:
Attributes: Name:

Report Time
The time the incident was reported.

Date: 09/02/2001
Time: 20.01.01
Time Zone: + h 0 m 0

Based on: The Incident Object Description Exchange Format Data Model and XML Implementation draft-inch-ietf-iodef-07.txt

Next >

Wizard screenshot (2)

IODEF - Wizard: 2 of 3

DF Labs

draft-ietf-inch-iodef-070

Assessment

Attributes
This attribute indicates the disclosure guidelines to which the sender expects the recipient of the IODEF Document

Restriction: public

Confidence
The Confidence class represents a best estimate of the validity and accuracy of the described impact of the incident activity

Rating: numeric

Time Impact
The element content will be a numeric value (REAL) specifying a unit of time

Value: []

Attributes

severity: Choose
metric: Choose
duration: Choose

Impact
The Impact class allows for categorizing and describing the technical impact of the incident on the network of an organization.

Value: Successful Root Compromise

Attributes

severity: high
completion: succeeded
type: admin

Monetary Impact
The MonetaryImpact class describes the financial impact of the activity on an organization. For example, this impact may consider losses due to the cost of the investigation or recovery, diminished productivity of the staff, or a tarnished reputation that will affect future opportunities.

Value: 400

Attributes

severity: low
currency: usd

Based on: The Incident Object Description Exchange Format Data Model and XML Implementation draft-inch-ietf-iodef-07.txt

Next >

Wizard screenshot (3)

IODEF - Wizard: 3 of 3

DF Labs
draft-ietf-inch-IODEF-070

Contact

Attributes

The Contact class describes contact information for organizations and personnel involved in the incident. This class allows for the naming of the involved party, specifying contact information for them, and identifying their role in the incident.

Contact Name role

Postal Address type

Fax restriction

Telephone Time Zone h m

Mail

Description

Registry Handle

The RegistryHandle class represents a handle to an Internet registry or community-specific database. A handle consists of a name specified in the element content, and the database to which it belongs specified in the type attribute.

Value Attributes registry

Based on: The Incident Object Description Exchange Format Data Model and XML Implementation draft-inch-ietf-iodef-07.txt

Finish

IODEF, xml validation steps

The screenshot displays the Digital Investigation Manager (DF Labs) interface for a draft IODEF document. The left pane shows a tree view of the document structure, and the right pane shows the XML preview of the selected 'Method' element.

Incident Event Data

- IODEF-Document
 - Incident
 - [purpose = "reporting"]
 - [lang = "en-US"]
 - [restriction = "public"]
 - IncidentID
 - [name = "CERT#339360"]
 - ReportTime = 2001-02-09T20:01:01
 - Assessment
 - [restriction = "public"]
 - Impact = Successful Root Compromise and R
 - MonetaryImpact = 400
 - Confidence
 - Contact
 - [role = "tech"]
 - [type = "person"]
 - ContactName = Andrew Jackson
 - RegistryHandle = port.tinycorp.com
 - Email = andrew@tinycorp.com
 - Telephone = 901 555-5232
 - Fax
 - Timezone = +00:00
 - Contact
 - [role = "tech"]
 - [type = "person"]
 - ContactName = John Lafitte
 - Telephone = 901-555-2336
 - Fax
 - EventData
 - Description = It appears that initial entry was c
 - DetectTime = 2001-02-01T20:01:01
 - Method
 - Classification
 - [origin = "certcc"]
 - name = CA-1999-13
 - url = http://www.cert.org/advisories/1

XML Preview

```
accounts were disabled. After that, we replaced the ftpd, disabled anonymous ftp and closed all of the crackers accounts except one non-root account which was fitted with a logging/notifying shell. We restricted telnet access to local machines. rlogin/rshd were already disabled. Merged logs from messages and last that shows his activity is also included as an attachment. It is also possible that there is more than one person involved. That would explain the multiple accounts. Also at least one cracker irc'ed from the cracked host.</Description>
<DetectTime>2001-02-01T20:01:01</DetectTime>
- <Method>
- <Classification origin="certcc">
  <name>CA-1999-13</name>
  <url>http://www.cert.org/advisories/CA-1999-13.html</url>
</Classification>
<Description>Remote and local intruders may be able exploit this vulnerability to execute arbitrary code as the user running the ftpd daemon, usually root.</Description>
</Method>
- <Flow>
- <System restriction="public" category="target" spoofed="no">
  - <Node>
    <name>port.tinycorp.com</name>
    <Address category="ipv4-addr">10.3.0.2</Address>
    <NodeRole category="ftp" />
  </Node>
  - <Service ip_version="4" ip_protocol="4">
    <portlist>21,80,135,139,25,110</portlist>
    <ProtoType>6</ProtoType>
  - <Application vendor="Washington University FTP server" family="" name="wu-ftp"
    version="" patch="">
    <url>http://www.wu-ftp.org/</url>
  </Application>
  </Service>
  <OperatingSystem name="linux" />
</System>
```

Our feedback

- Some potential “localization related issues”
- Enlarge the number of the participant to a further implementation test
- RFC, why not?
- More Involvement of further working groups/vendors for the implementation phase

Further Work

- Implementation of FINE (Format for Incident Information Exchange) interface
- Document XML Signature
- Tuning of the implementation (rif: Flow node)
- Implementation of the draft-ietf-inch-phishingextns extension

- Automated validation of the imported documents

Contact Info

- Dflabs italy, www.dflabs.com
- Prof. Dario Forte, University of Milano at Crema
- Email: dario.forte@acm.org