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 Enviroment
  - Unlimited number of cases
  - Local and Remote Db
  - Synchronization Module
- Automated Reporting Features
- Total logging

DFLabs
Managing Infosecurity Risks

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

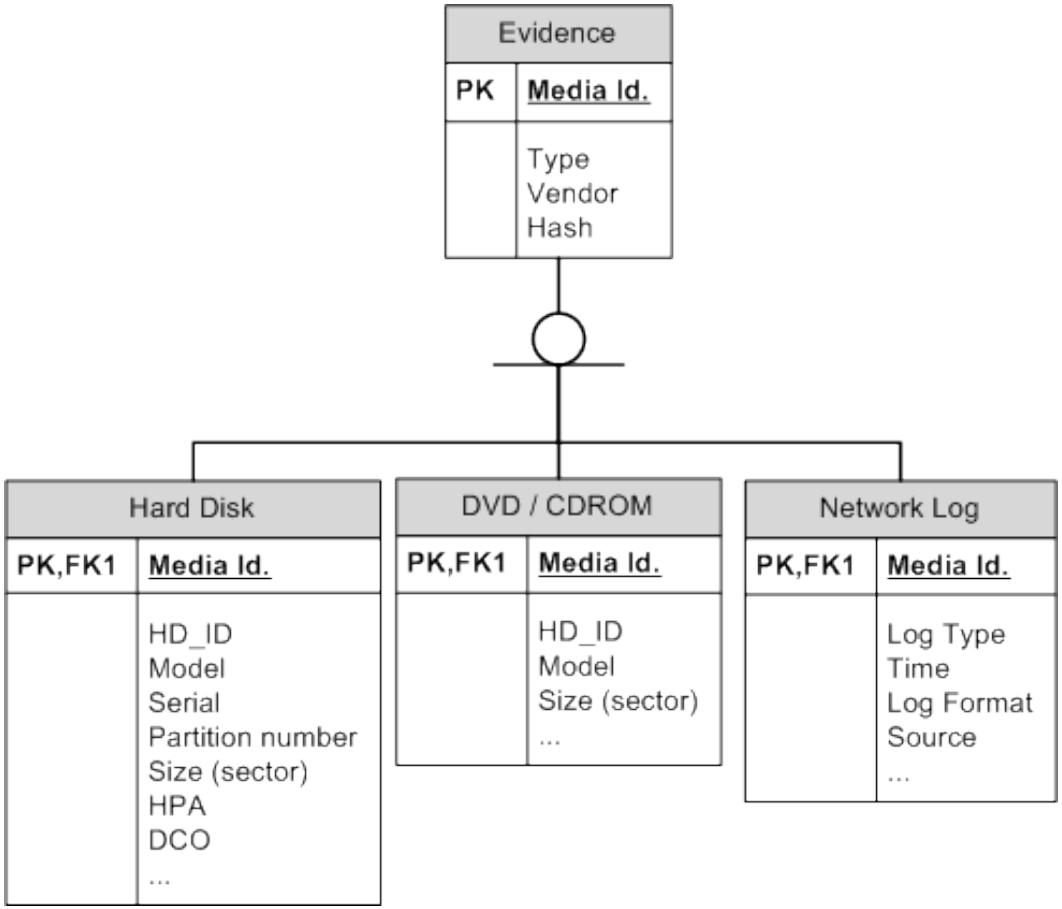
CASE

CASE	
PK	**Case_ID**
	Info Company Contacts Type Date Investigator Note State ...

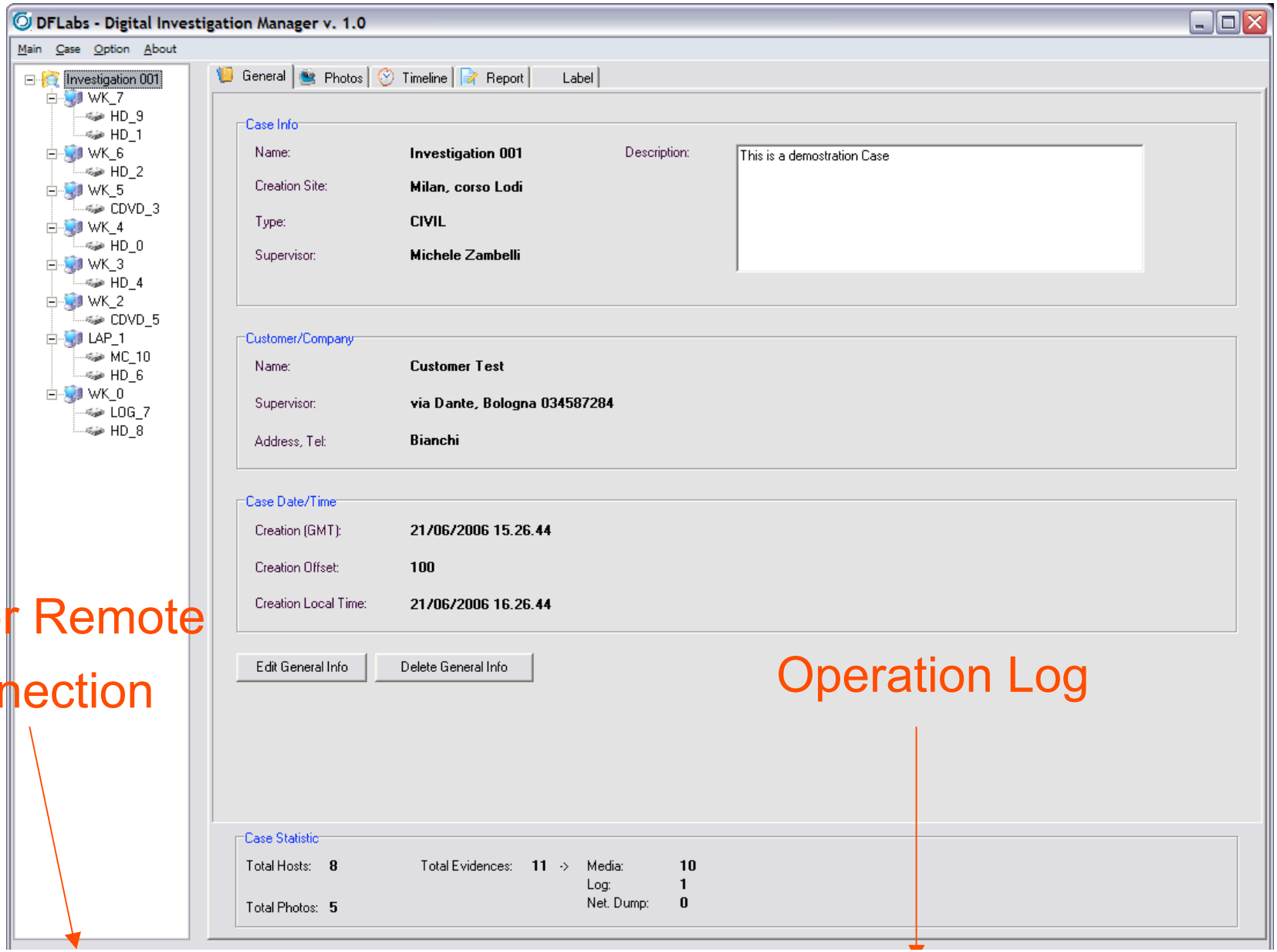
HOST

HOST	
PK	**Host_ID**
	Model Serial CompanyID Owner Photo Bios ....

EVIDENCE



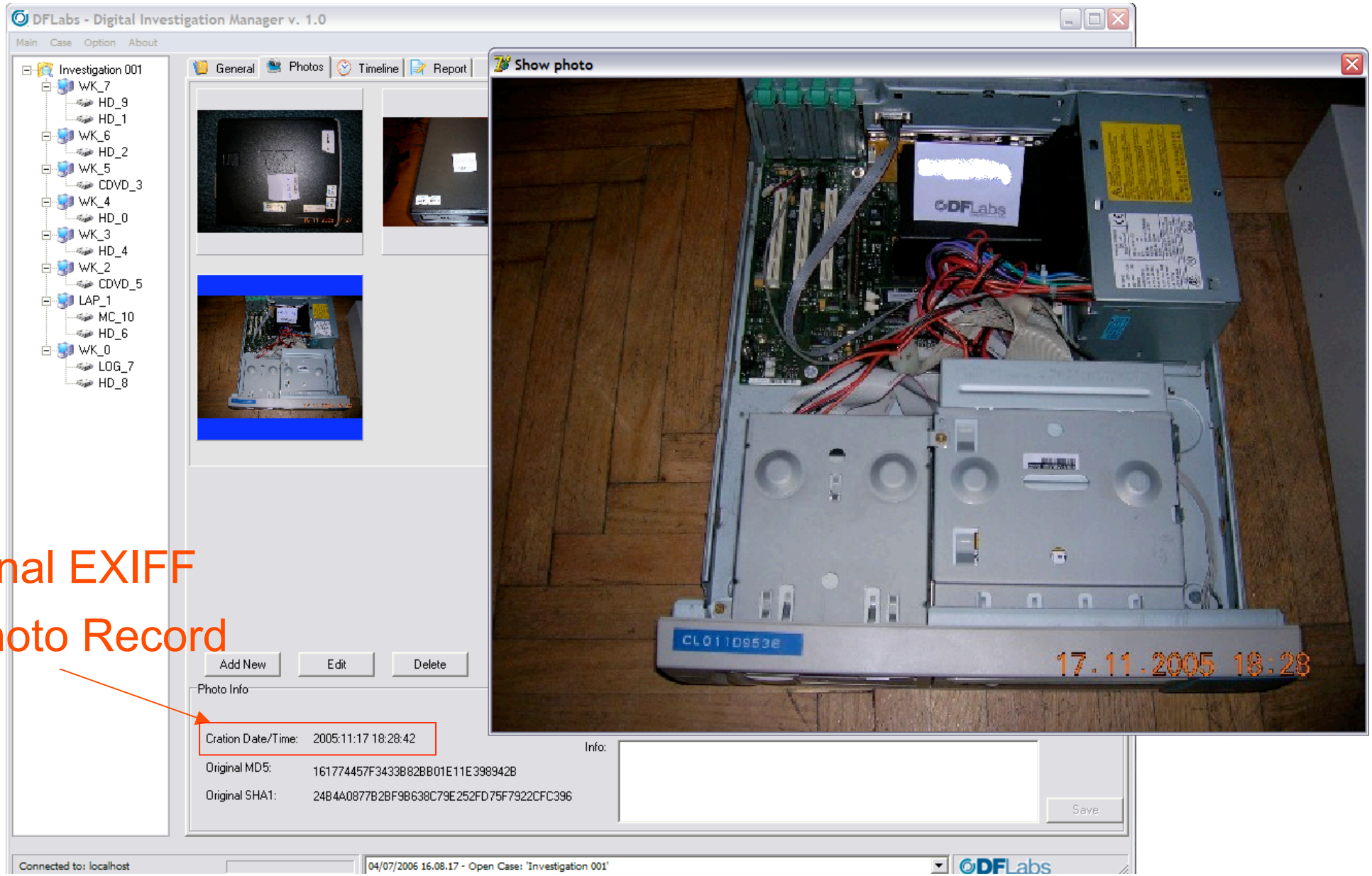
Case Information



Local or Remote Connection

Operation Log

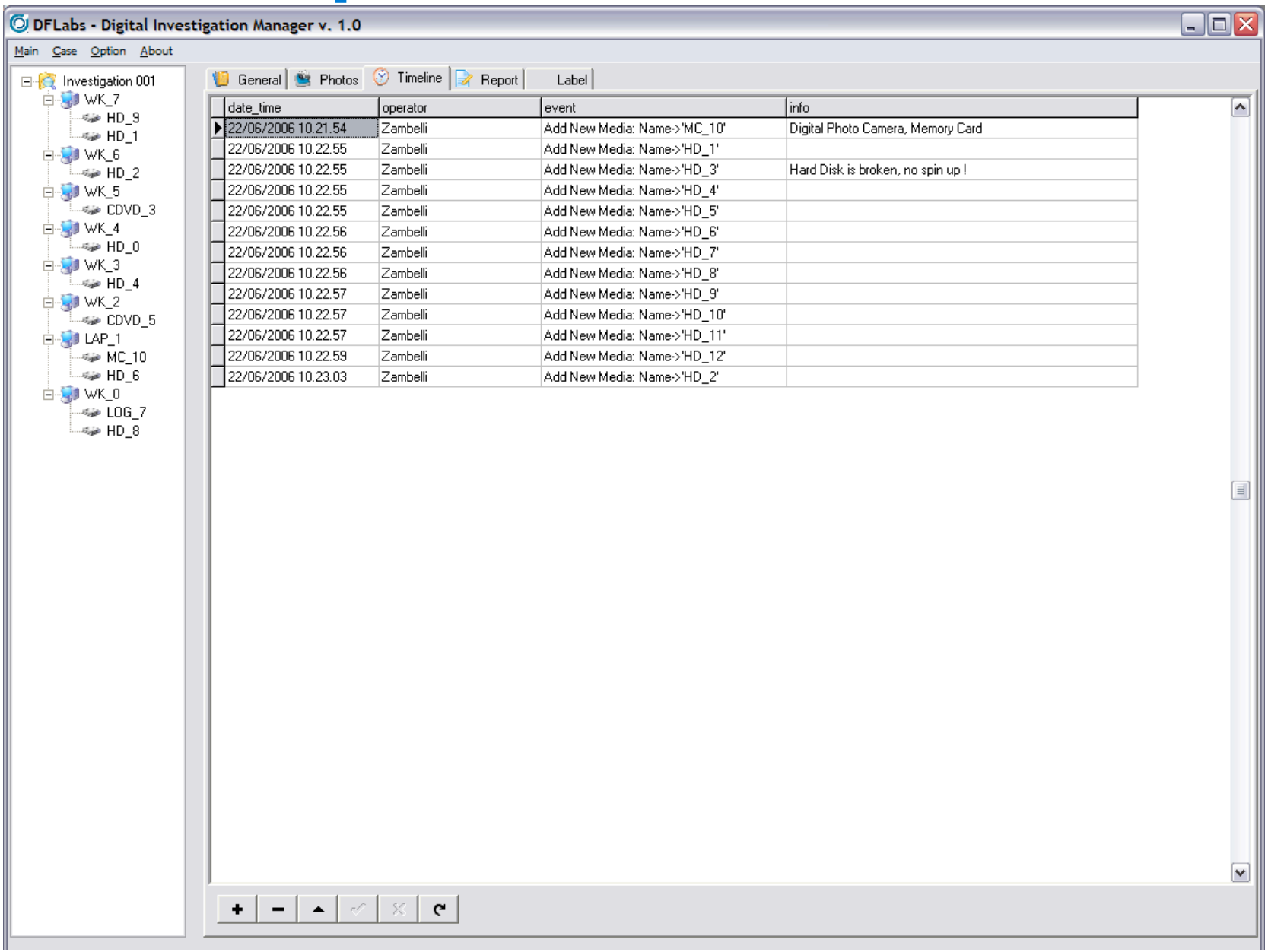
Photographic Documentation



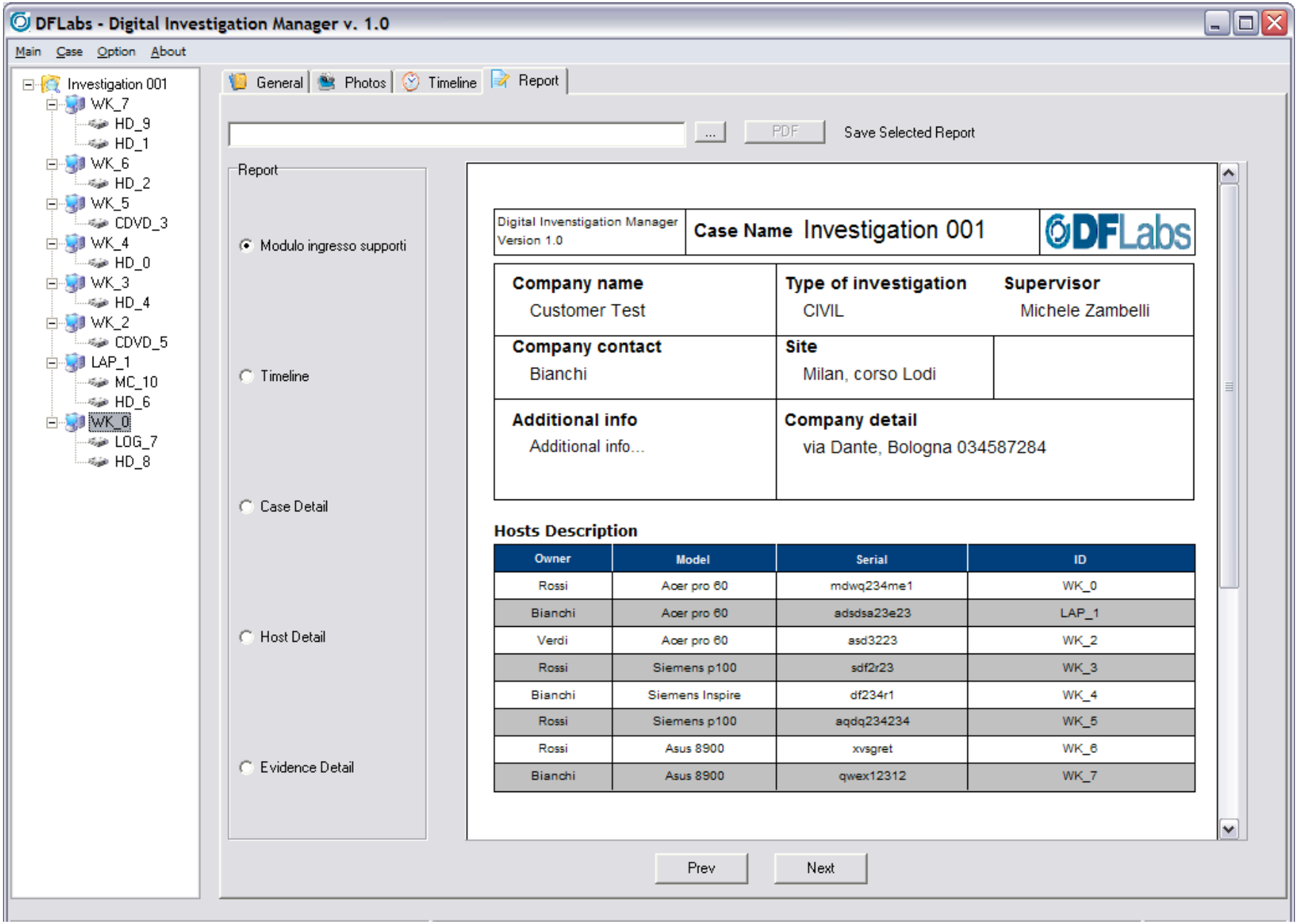
Original EXIFF

Photo Record

Operation Timeline



Report Generation



D.I.M Vs. IODEF

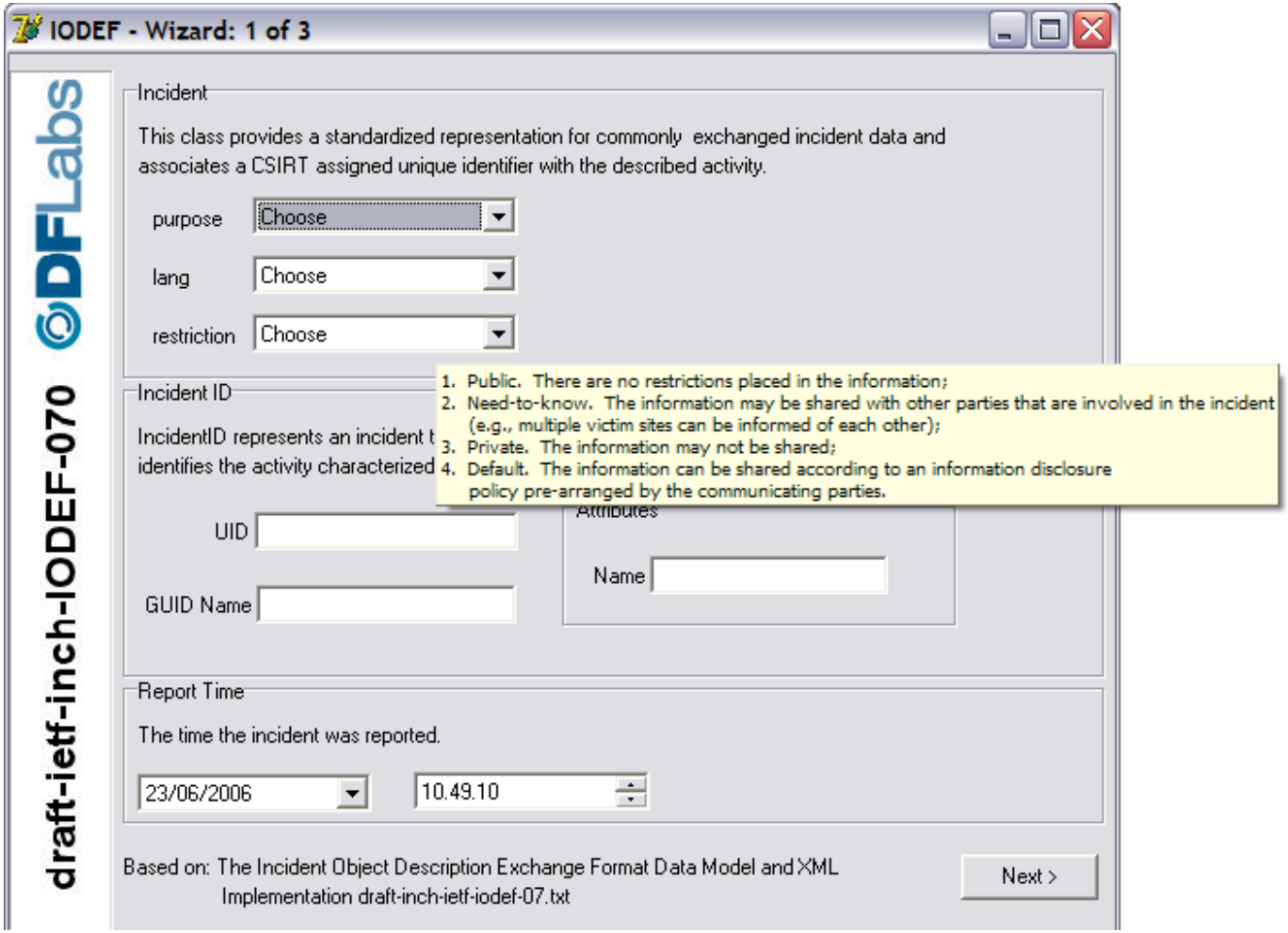
- Each single case can be associated with an XML IODEF compliant documents.
- The validation scheme is based upon **iodef-07** del **draft ietf**
- The initial XML file generation is Wizard driven
- The structure of the document is a tree totally upgradable
- External XML Documents can be imported
- 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

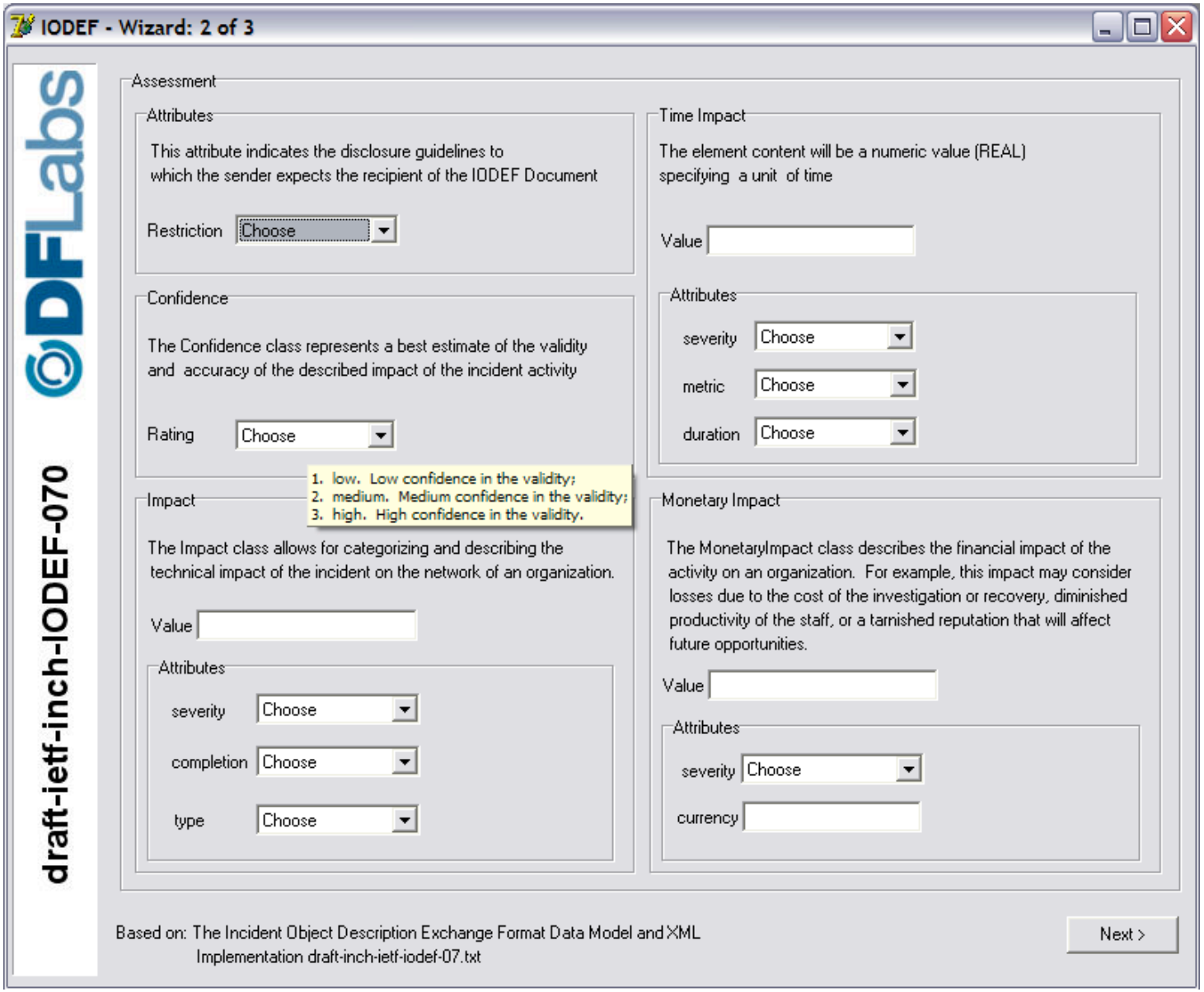
- 1st part: we worked on our files and external files to validate them reciprocely;
- 2nd part: after Brian Trammel's review we have added more programming and re-tested the application
- Tests were positive

Wizard 1, General Info

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

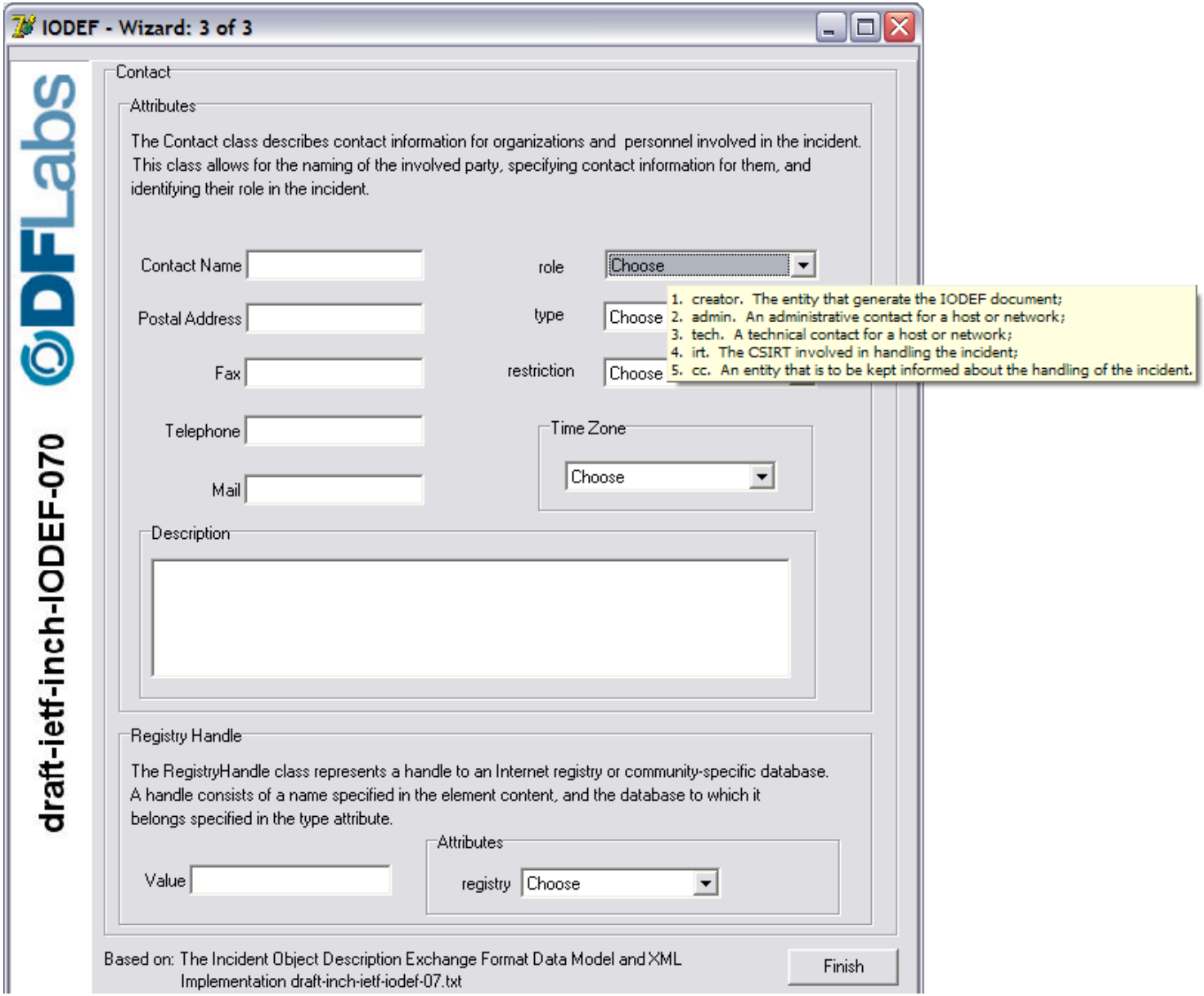


Wizard 2, Assessment section



DFLabs
Managing Infosecurity Risks

Wizard 3, Contact Section

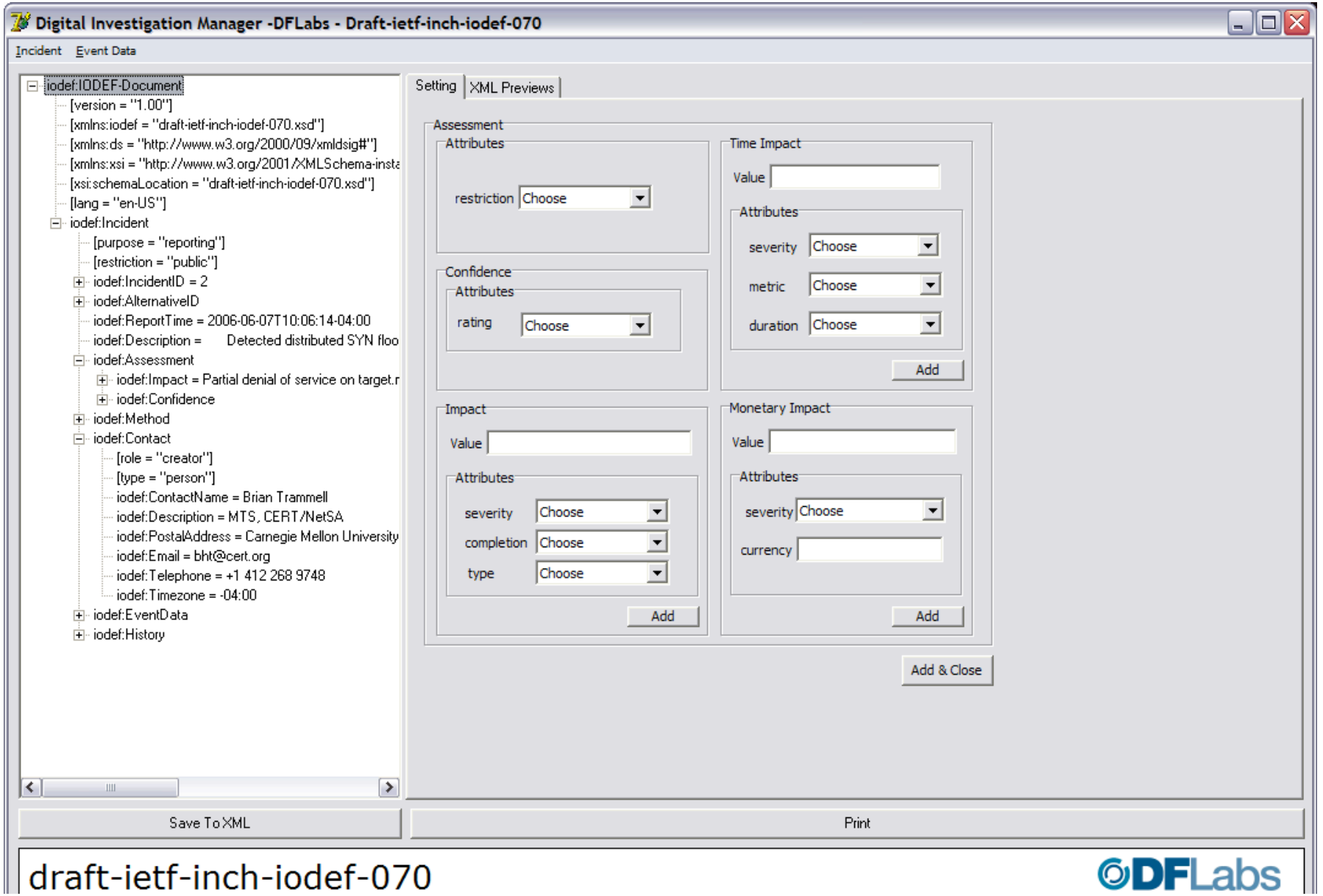


DFLabs
Managing Infosecurity Risks

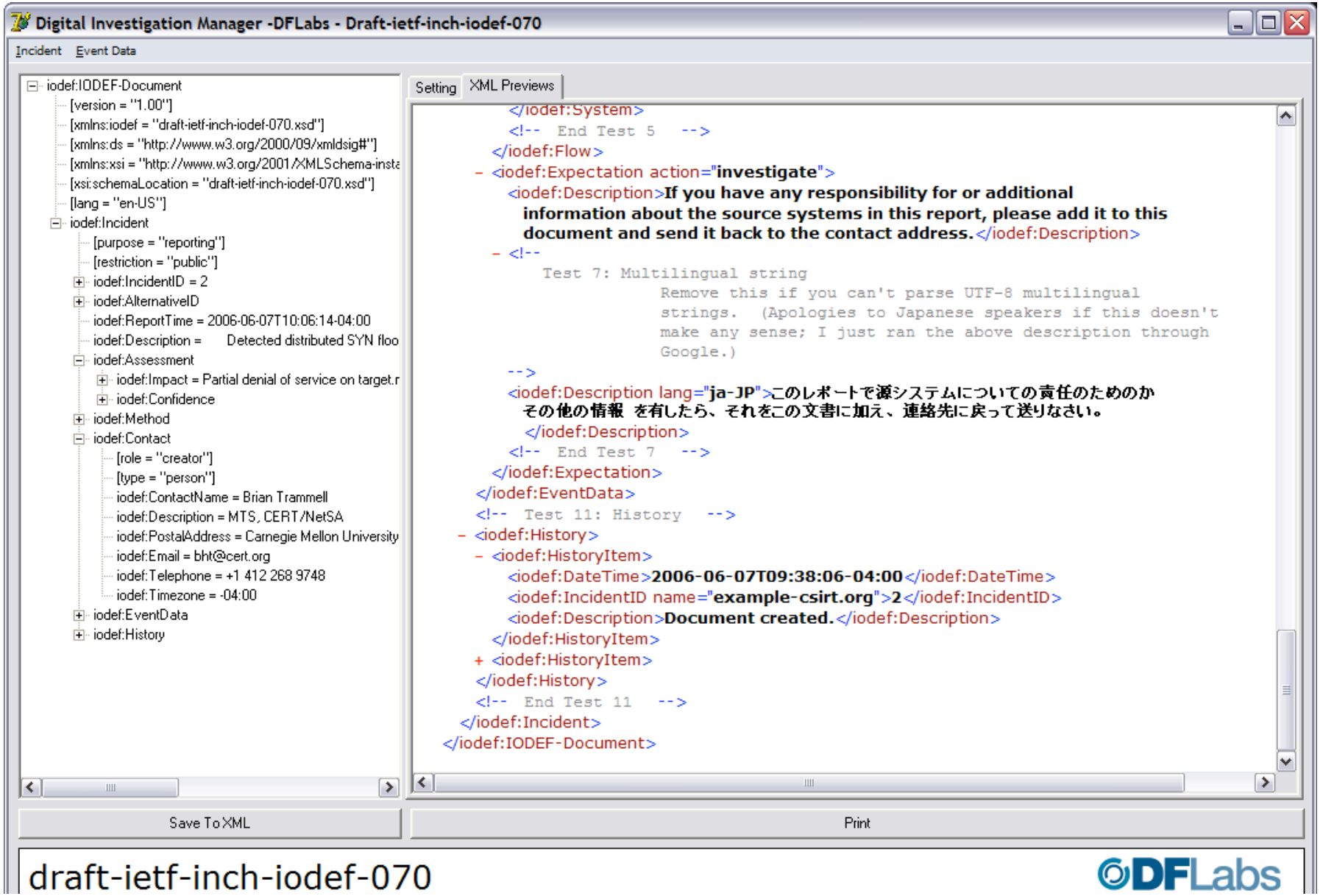
Tree view Section, features

- 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



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



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:

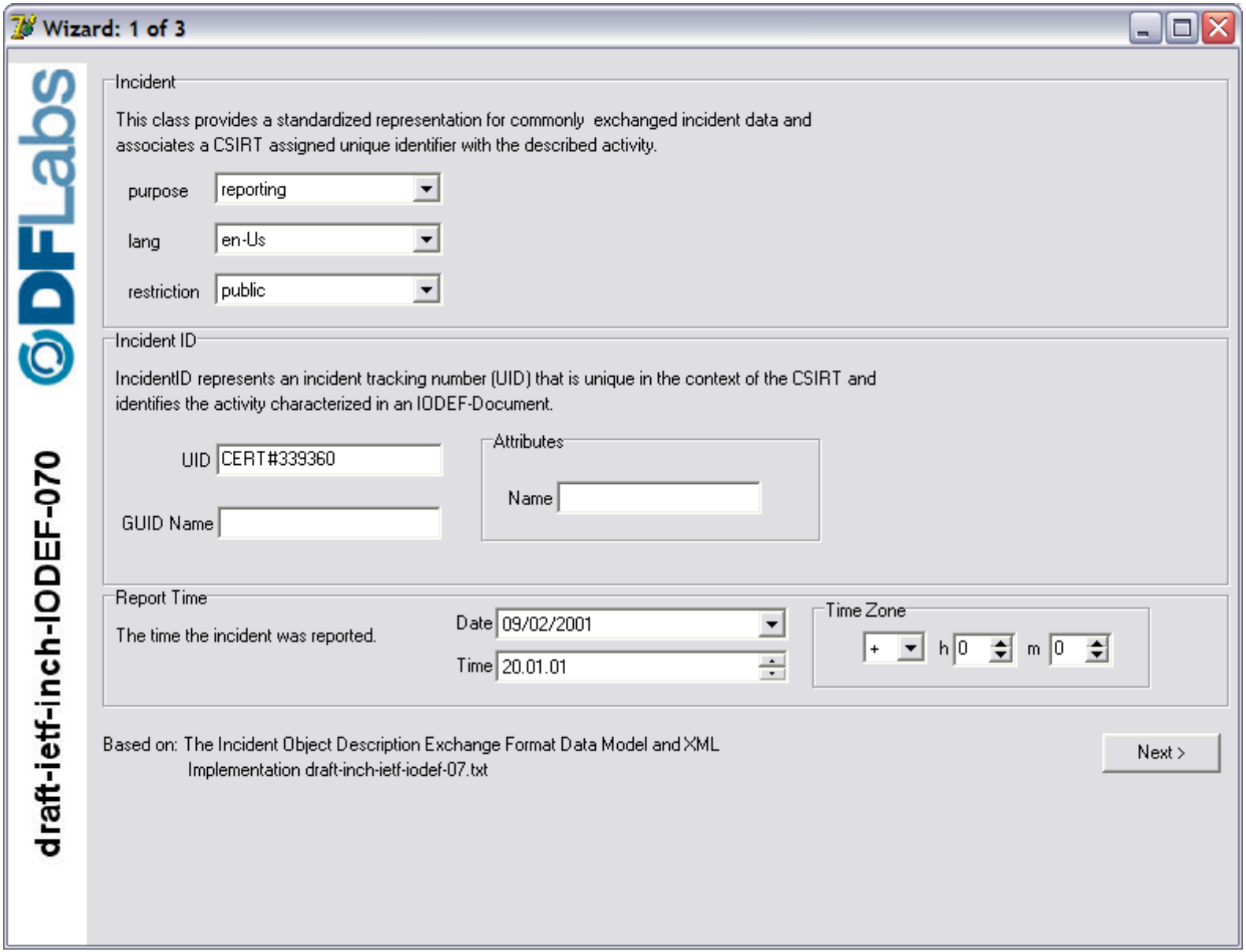
1. for dim-iodef-test1.xml : nearly validates against -070. There appears to be a problem with your ISO8601 (DateTime) representation (one-digit months and days always need leading zeroes). Also, the value of the MonetaryImpact element should not contain digit separators (12.000) to avoid locale issues. 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/doc01-simple-event.xml FIXED

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

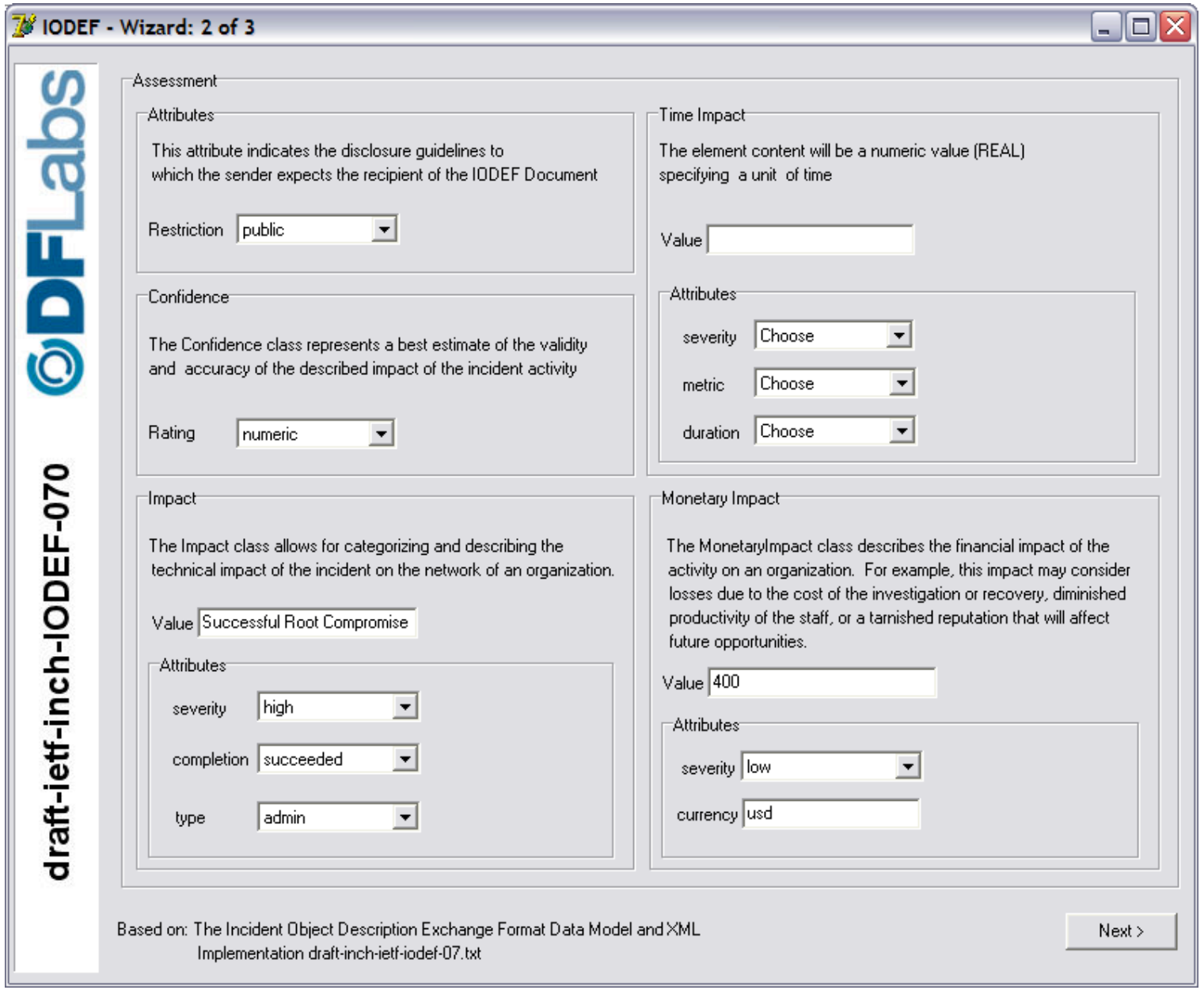
- **Issue**: Reviewer referred to us that we needed to integrate our test using the incident report supplied by the interoperability test.
- **Action:** We integrated the test as required. The results are in the next slides: rep02-scan.txt
- **Methodology:** We integrated our wizard and tested it against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

Wizard screenshot (1)



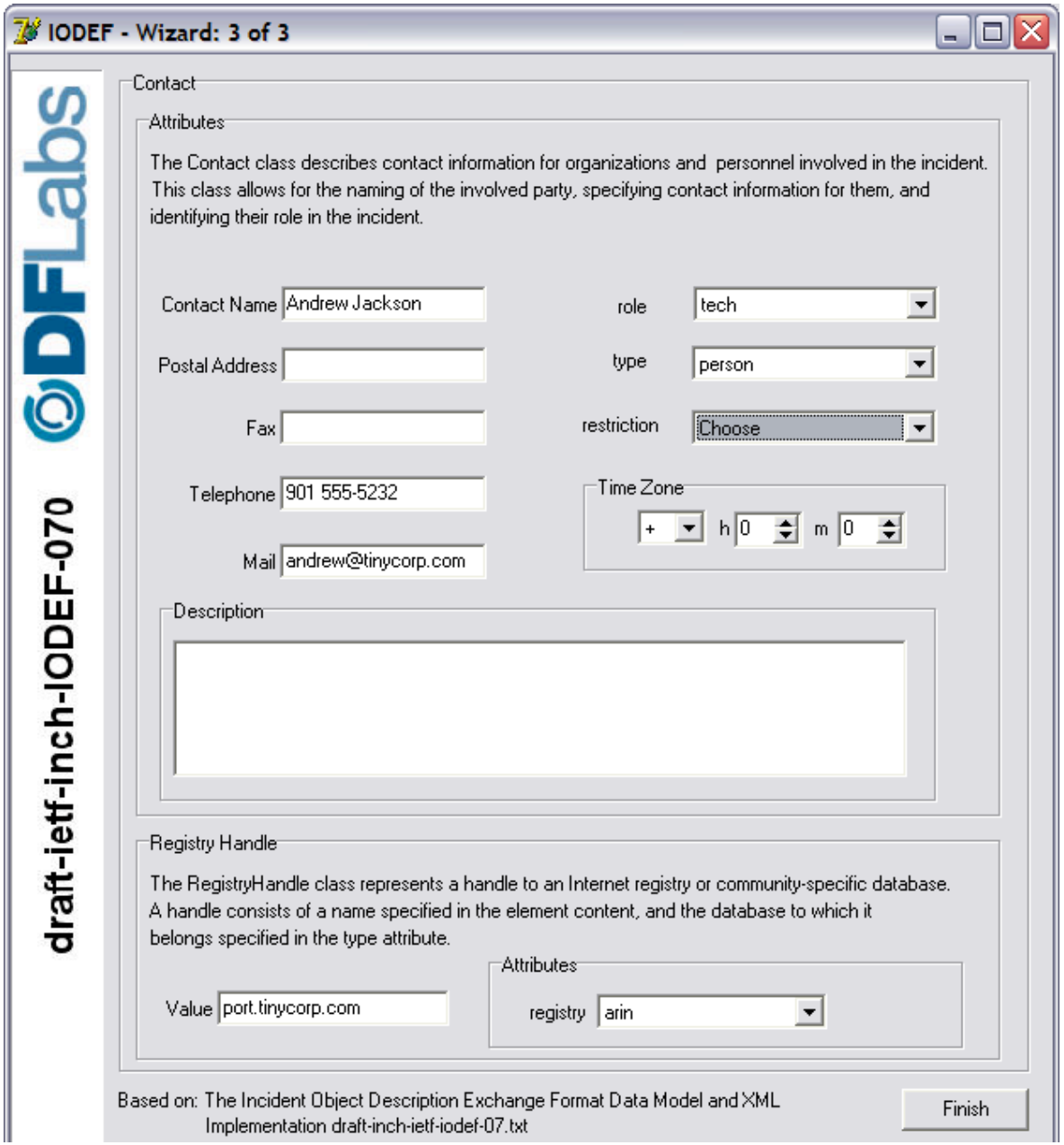
DFLabs
Managing Infosecurity Risks

Wizard screenshot (2)



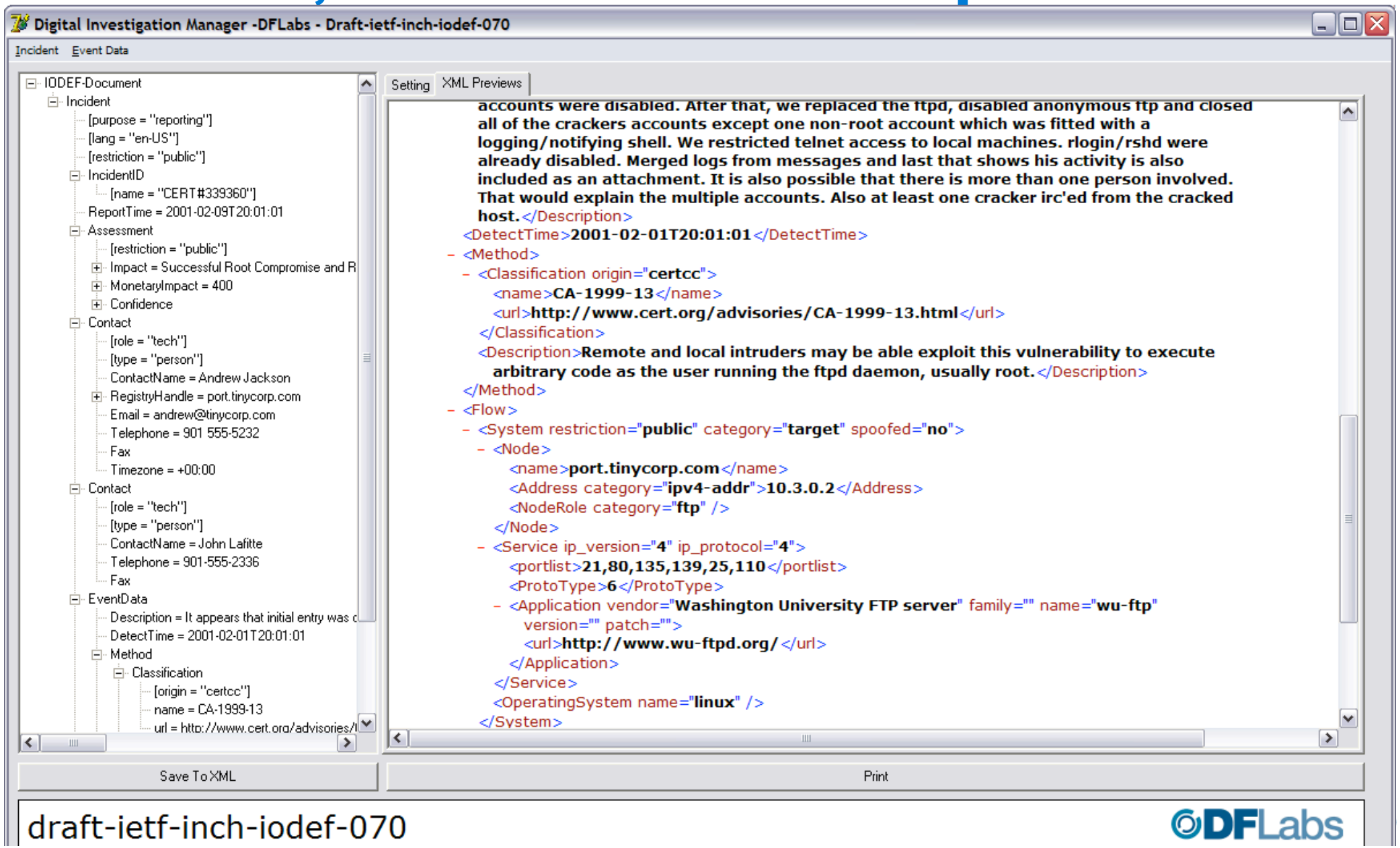
DFLabs
Managing Infosecurity Risks

Wizard screenshot (3)



DFLabs
Managing Infosecurity Risks

IODEF, xml validation steps



Our feedback

- Some potential “localization related issues”
- Enlarge the number of the partecipant 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

DFLabs
Managing Infosecurity Risks

Contact Info

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

DFLabs
Managing Infosecurity Risks