**International Federation for Information Processing**

**TC-11**  **Security and Protection in Information Processing Systems**

# Factsheet

# WG 11.9

# Digital Forensics

Version: 22 May 2006

## *Introduction*

*(Strategic issues / questions: Introduction and mission statement)*

IFIP Working Group 11.9 on Digital Forensics was founded in 2004.

At the outer fringes of the Internet, usage is increasingly driven by devices beyond the computer. A plethora of audio, video and communication devices are becoming closely associated with the computer and are gradually converging with it. This has resulted in more and more information being stored, transmitted and processed in digital form than ever before. At the same time this connectivity is also enabling criminals to act trans-jurisdictionally with ease. Increasingly we are witnessing that a perpetrator of a crime is being brought to justice in one jurisdiction while the digital evidence needed to prosecute the perpetrator residing in other jurisdictions. This requires that all nations have the ability to collect, preserve and examine digital evidence for their own needs as well as for the potential needs of other nations. Digital Forensics is the scientific study of the processes involved in the recovery, preservation and examination of digital evidence, including audio, imaging and communication devices. The efforts of the working group in digital forensics strive to discover, define and foster fundamental scientific principles that support the investigation of digital wrongdoings from all perspectives, legal, business and military.

Mission statement: working group 11.9 is an active international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics – the scientific study of the processes involved in extracting, analyzing, preserving and presenting all forms of electronic evidence.

## *Aims and scope (last revised / reconfirmed August 2004)*

*(Strategic issues / questions: What does the TC address, what does it want to achieve, what are the groups of people the working group focuses on, what are the boundaries of the work area)*

The aim of the IFIP WG 11.9 group is to promote through education, research and outreach, the awareness and understanding of (i) the scientific methods and techniques that help to tell about a computer related security incident (including those that involve converging digital technology), what occurred, when it occurred, how it occurred, what resources were affected and who initiated the incident, in a manner that will support a legal action, and (ii) the operational and legal aspects of new and emerging digital technology so as to help develop such methods and techniques.

The scope of the WG 11.9 group is
1. To establish and expand a common digital forensics lexicon so that international community speaks the same language.
2. To propose, define and evaluate core technologies that assist in the discovery, explanation and presentation of conclusive and persuasive digital evidence that will meet the heightened scrutiny of the courts and other decision-makers in military and civilian environments.
3. To promote through education, research and outreach, a wider understanding of the legal, social and operational issues related to digital forensics.
4. To foster cooperation between international communities so as to promote scholarly discussion related to digital forensic research and its application.

## Products, services and activities *(last revised / reconfirmed August 2004)*
*(Strategic issues / questions: What are the products and activities the working group will deliver)*

IFIP WG 11.9 hosts an annual international conference that provides a forum for presenting original, unpublished research results and innovative ideas related to the extraction, analysis and preservation of all forms of digital evidence.

In addition, it hosts technology transfer workshops to showcase advances in digital forensics research and practice, and to solicit input on research trends and needs.

Research results from the annual IFIP WG 11.9 conferences are published by Springer (New York) as books in the series, Research Advances in Digital Forensics. In addition, selected papers from IFIP WG 11.9 conferences will be published in special issues of Digital Investigations (Elsevier) and other technical journals.

## Membership rules *(last revised / reconfirmed August 2004)*
*(Strategic issues / questions: Membership rules)*

IFIP Working Group 11.9 has two membership categories.
• Members: IFIP WG 11.9 members are expected to be qualified researchers, practitioners and/or educators in digital forensics. Members are nominated by the Working Group Chair, subject to IFIP approval. Members are expected to participate in Working Group activities. At a minimum, members must present a paper at a WG 11.9 conference or workshop, or take an active role in the organization of a conference or workshop at least once every three years. A three-year period of inactivity is taken to indicate that a member is no longer interested in the technical area.

• Observers: IFIP WG 11.9 observers are expected to be qualified researchers, practitioners and/or educators in digital forensics. Observers are nominated by the Working Group Chair, subject to IFIP approval. Individuals attending or presenting papers at WG 11.9 conferences or workshops will be offered observer or member status. Observers who do not attend at least one WG 11.9 event every three years will lose their status. A three-year period of inactivity is taken to indicate that an observer is no longer interested in the technical area.

## *Contact details*

Contact of working group chair:

- xx
  Telephone:
  Fax:
  E-mail:

Home page and mailing address of the group:

- http://

## *Annex a. Membership*

- **Officers, current**

| | | |
|---|---|---|
| Chair: | Indrajit Ray, USA | first three-year term, August 2004 – August 2007 |
| Vice-chair: | Mark Pollitt, USA | first three-year term, August 2004 – August 2007 |
| Treasurer: | Sujeet Shenoi, USA | first three-year term, August 2004 – August 2007 |

(Note that the 11.9 website says the following:
**Indrajit Ray, Chair,** Colorado State University
**Gavin Manes, Vice Chair,** University of Tulsa
**Mark Pollitt, Secretary,** Digital Evidence Professional Services
**Sujeet Shenoi, Treasurer,** University of Tulsa)

- **Membershiplist, confirmed in TC-11 meeting of May 2005**

IFIP WG 11.9 has 50 members as of February 18, 2006. The majority of the members (35) are from the United States; the others are from Australia (1), France (2), Japan (1), Norway (1), South Africa (9), and the United Kingdom (1).
IFIP WG 11.9 has 25 observers as of February 18, 2006. Most of the observers (17) are from the United States; the others are from Japan (4), South Africa (1), Taiwan (2) and the United Kingdom (1).

**Please provide the membership list for approval at the May 2006 meeting.**

- **Officers, history**

WG 11.9 was established in 2004, the current team of officers are the first officers for this working group.

## *Annex b. Workplan*

- Past events / products / achievements

Annual Conference
The Second Annual IFIP WG 11.9 International Conference on Digital Forensics was held in conjunction with the annual meeting of IFIP Working Group 11.9 at the National Center for Forensic Science in Orlando, Florida on January 29 – February 1, 2006. The purposes of the three-day conference were: (i) To provide a forum for the international digital forensics community to discuss the current state of research and practice in the discipline, (ii) To enable participants to expand their knowledge in digital forensics through personal contact with other researchers and practitioners, and (iii) To disseminate widely the results of the conference and accompanying discussions, including original research, practical experiences and innovative ideas in digital forensics.
Martin Olivier (University of Pretoria, South Africa) and Sujeet Shenoi (University of Tulsa, USA) served as the program chairs for the conference. A total of 49 papers from seven countries were received by the program chairs. After a formal review process, 30 papers were accepted for presentation at the conference along with two invited papers. The strong conference program was organized around ten sessions: Evidence Collection and Handling, Portable Electronic Device Forensics, Network Forensics I, Legal Issues and Knowledge Management, Advanced Forensic Techniques, Evidence Attribution, Network Forensics II, Forensic Techniques and Applications, Multimedia Forensics, and Digital Forensic Processes and Training. In addition, two keynote lectures were delivered by stalwarts in the field: Research Challenges in Digital Forensics by Professor Eugene Spafford, Director, CERIAS, Purdue University, West Lafayette, Indiana and A Law Enforcement Challenge to the Digital Forensics Research Community by James Christy, Director, Defense Cyber Crime Institute, Linthicum, Maryland. Revised versions of the papers presented at the conference will be published as a book: Research Advances in Digital Forensics – II, M. Olivier and S. Shenoi (Eds.), Springer, New York, 2006.
The conference program generated considerable interest in the digital forensics community. To maintain the working group atmosphere and promote intense interactions between researchers, attendance was limited to 64 individuals ranging from undergraduate students to senior researchers. As expected, most of the participants were from the United States (43). Nevertheless, the conference had strong international participation – 21 attendees, corresponding to nearly 33% of the total participation. The countries represented included Australia (1), Japan (6), South Africa (11), Taiwan (2) and the United Kingdom (1).
The conference program and the accompanying discussions of research issues in digital forensics were enhanced by a good mix of researchers from academia, industry, research organizations and the public sector. In addition to 45 university researchers (including 15 students), there were three private sector participants, three from research organizations, and 13 from government or law enforcement agencies.

Technology Transfer Workshops
IFIP WG 11.9 periodically organizes technology transfer workshops to showcase advances in digital forensics research and practice to the law enforcement, inspector general and intelligence communities, and to solicit input on research trends and needs. The workshops provide important

visibility for IFIP WG 11.9. To allow for effective interactions between attendees, workshop attendance is typically limited to 60 invited participants.

The 2005 Technology Transfer Workshop on Digital Forensics was held at Johns Hopkins University (Columbia, Maryland) on June 9-10, 2005. The workshop program included seven presentations delivered by IFIP WG 11.9 members. The topics included: Storage Area Networks, Defeating Hostile Forensic Techniques and Tools, Recovering Digital Evidence from Hand-Held Devices, Acquiring Evidence from Telecommunications Networks, Forensic Analysis of Digital Images, Attribution of Digital Media, and New Technologies and Tools for Digital Forensics Education and Training. In addition, a moderated discussion on Research Needs and Technology Transfer was organized.

IFIP WG 11.9 Publications

Refereed papers, keynote presentations and details of panel discussions at the annual IFIP WG 11.9 conferences are by Springer (New York) as books in the series, Research Advances in Digital Forensics. The first book in the series, edited by Mark Pollitt and Sujeet Shenoi, was published in November 2005. The second book, Research Advances in Digital Forensics – II (Martin Olivier and Sujeet Shenoi (Eds.)), is scheduled to be published during the summer of 2006. In addition, revised and/or extended versions of selected papers from IFIP WG 11.9 conferences will be published in special issues of Digital Investigations and other technical journals.

- Planned events / activities

Due to the success of the first and second conferences, and continued interest in the Orlando venue, the Third Annual IFIP WG 11.9 International Conference on Digital Forensics will also be held at the National Center for Forensic Science in Orlando, Florida in January 2007. The working group ambience will be maintained by restricting attendance to no more than 70 participants. Plans are underway to hold the Fourth Annual IFIP WG 11.9 International Conference on Digital Forensics at a location in Asia or Europe during the spring of 2008.

Building on the success of the 2005 event, plans are underway to hold the 2006 Technology Transfer Workshop on Digital Forensics at Johns Hopkins University (Columbia, Maryland) during the summer of 2006.