

Report on Digital Evidence

**Prepared by:
Mark M. Pollitt, BS**

**Unit Chief
Computer Analysis Response Team
Federal Bureau of Investigation Laboratory
Washington, DC, USA**

SUMMARY REPORT ON DIGITAL EVIDENCE

This is the third report to this body concerning digital evidence. The first, in 1995, explored the possibilities for a forensic discipline based on electronically stored digital information. There was clearly enough interest to warrant the inclusion of a report on these matters during the 1998 meeting. In that report, the evidence clearly demonstrated that the potential for forensic examination of digital evidence would likely be realized. The amount of scientific and technical work being done merely whetted the appetite of the few agencies that were fortunate to have such services available. In anticipation of even more significant changes, the committee asked that digital evidence be presented as one of the principle evidence types. That faith was not unfounded.

Where, a few years ago, there were a few lone wolves howling in the desolate wilderness, now we have an entire forensic community, complete with its own professional, scientific bodies. We have robust digital evidence units and laboratories that are well funded and produce forensically sound work. Where once laboratory managers asked the question "should we do this kind of work?" now the question is "how are we going to conduct digital forensic examinations".

This report will focus on two areas that have seen significant change during the last three years. These are: standards and workload. In the standards arena, the existence, composition and contributions of a number of digital evidence forensic groups will be reported. In preparation for this report, a survey was created and distributed to over 70 agencies. The results of that survey will be reported along with some commentary.

DIGITAL EVIDENCE GROUPS – A QUEST FOR STANDARDS

The rapid development of a number of national and regional bodies has been a major factor in the rapid maturity of this nascent discipline. As the following demonstrates, many countries and agencies are working in concert to build a strong foundation for forensic practice.

Forensic Computing Group, United Kingdom

Perhaps the oldest national group dedicated to computer evidence is the Forensic Computing Group in the United Kingdom. This group is made up of various investigative agencies and forensic science units involved in computer evidence. It also has representation from the Association of Chief Police Officers (ACPO) Computer Crime Working Group. The ACPO Computer Crime Working Group was, in fact, the first to draft Good Practice "guidelines" for the search, seizure and examination of computer evidence. This proved very successful, not only from a technical perspective, but also because the document was produced by an ACPO Working Group this ensured that the guidelines would be promulgated and adopted by virtually all of the police agencies in the United Kingdom. The ACPO Working Group has published a second edition of the guidelines and together with the FCG is working with the International Organization on Computer Evidence to develop a generic good practice guide for international use.

ACPO has recently reported that they are at work on a third version that will concentrate on the investigative aspects of computer evidence. It is their belief that there is sufficient documentation available for “first responders”. For further information contact the National High Tech Crime Unit.

European Network of Forensic Science Institutes – Forensic Information Technology Working Group (FIT-WG)

In 1998, the Forensic Information Technology Working Group was established under the auspices of the European Network of Forensic Science Institutes. This group initially met to exchange information concerning information technology forensics. Subsequently, the group has joined with other national and regional groups to pursue the development and acceptance of guidelines, good practices, best practices and standards. Subsequent to hosting the 2000 meeting of IOCE, this group has agreed to specifically focus on quality issues.

In September 2001, the FIT-WG hosted a training conference in Oslo, Norway, which was hosted by the Norway’s Okorim. This meeting concentrated on investigative and forensic information technology training issues. (see <http://www.enfsi.org>)

National Institute of Justice, United States Department of Justice (NIJ)

For the last three years, the National Institute of Justice has been attempting to develop a series of documents focused on different elements of high technology crime. The first of these, which should be published by the date of this symposium, is focused on assisting the “first responder” to a crime scene involving digital evidence. The second volume, which is in work, deals with developing a digital evidence laboratory. Updates on this series may be obtained from <http://www.ojp.usdoj.gov/nij/pubs.htm>.

Scientific Working Group on Digital Evidence (SWGDE)

At the last INTERPOL Forensic Science Symposium, I reported on the establishment of a Technical Working Group on Digital Evidence. This group, which was initially formed from representatives of the Federal crime laboratories in the United States, has been renamed and its membership extended to include representatives from state and local law enforcement agencies from not only the United States, but also Canada. This organization has been extremely busy during the last three years. In 1999, this group produced a document called “Proposed Standards for the Exchange of Digital Evidence”. This document consists of a set of definitions and principles for handling digital evidence. It was presented for discussion at the 1999 International Organization on Digital Evidence (IOCE) meeting. A copy of this document is included in the appendices.

Scientific Working Group for Imaging Technologies (SWGIT)

Working very closely with SWGDE, the Imaging Technologies SWG has developed guidelines that address a number of aspects of digital evidence as related to the examination of the content of digitally stored images. This close association will continue, as more and more “wet” photography is being replaced by digital imaging. Commonly used terms and definitions applied in the imaging discipline often have completely different meanings in computer forensics. A copy of the SWGIT Guidelines is included in the Appendices.

International Organization on Computer Evidence (IOCE)

One of the oldest international organizations to deal with digital evidence is the IOCE. Formed in 1995, it has served as both a forum for the exchange of information and a leader in the development of standards. Merely two months after the last INTERPOL Forensic Science Symposium, the High Tech Crime Sub-Group of the G-8 asked IOCE to undertake the development of standards that would allow for the exchange of digital evidence across national boundaries. Recognizing that it would be difficult to accomplish this from yearly meetings, the IOCE reached out to regional and national digital forensic groups to further the work on a year-round basis while allowing for greater participation.

During the October 1999, meeting of the IOCE (hosted by ACPO/FCG), a set of five principles and accompanying definitions was developed and agreed upon. These were then submitted to the G-8 Sub-Group on High Tech Crime and with minor editing were adopted by the Lyon Group of the G-8. In connection with the 2000 meeting of IOCE (hosted by ENSFI-FIT), a number of draft documents were developed including generic good practice guides for different kinds of digital evidence, an inventory of the required knowledge, skills, and abilities required by forensic practitioners and a template for a “first responders” guide. These draft documents will be further refined during this year by the various national and regional groups. These documents can be found at <http://www.ioce.org/iocedraftdoc.htm>.

High Tech Crime Sub-Group of the G-8

While the High Tech Crime Sub-Group of the G-8 is not strictly a forensic group, it has played a vital role in the rapid progress in the digital evidence area. This group has several mandates from the G-8 ministers that directly impact the practice of information technology forensics. It is fortuitous that representatives from all the national and regional groups are active participants in the G-8 meetings. These meetings occur frequently enough to allow for a great deal of coordination between IOCE meetings. The quest for digital evidence standards would not be as far along were it not for the support of this group.

In December 1997, the High Tech Crime Sub-Group tasked IOCE to develop international standards for the exchange of digital evidence. By November 1999, the first product was ratified by IOCE. During 2000, the IOCE proposal was substantially accepted and a copy is included in the appendices.

Council of Europe

The European Committee on Crime Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), has finished a draft Convention on Cyber-Crime. This convention makes numerous references to the collection and exchange of electronic evidence. This convention is currently undergoing ministerial review and approval. Should this document be approved, it is likely that additional discussion will follow concerning how to implement the digital evidence provisions. (See <http://conventions.coe.int/>)

DIGITAL EVIDENCE QUESTIONNAIRE

In preparation for this conference the FBI Laboratory, as the Coordinating Laboratory for Digital Evidence, sent out a questionnaire to over two hundred laboratories and law enforcement agencies throughout the world. The purpose of this study was to assess the current levels of activity and practices in four specific areas of digital evidence: computer forensics, electronic devices, digital audio/video media examinations, and digital image examinations.

In early 2001, the following questionnaire was mailed to over 200 organizations. The list of organizations was developed from attendance lists from previous INTERPOL Forensic Science Symposia, IOCE meetings and from the American Society of Crime Laboratory Directors (ASCLD). Seventy-three questionnaires were returned representing 73 distinct units and 68 separate agencies from 19 countries.

The following instructions were provided, and an identification section followed:

Questionnaire on Digital Evidence

This questionnaire is designed to elicit information concerning the forensic services and practices of your unit/laboratory involving evidence stored in digital form. With respect to these questions, the following definitions are utilized:

Digital Evidence: Information of probative values stored or transmitted in digital form.

Forensic Examination: A scientific process of developing and/or analyzing media, file systems, devices or content for information of probative value.

Digital Image Examinations: Scientific examinations of digitally stored images for authenticity or content. This includes such examinations as photogrammetry but does not include the taking of crime scene photographs.

Discussion:

This study attempted to gather information concerning the practice of forensic science in three digital domains: computer forensics, electronic devices, audio/video media and digital images. An attempt was made to provide some definition to some of the types of examinations under review in this study. Special emphasis was made on the digital imagery definition, as it was anticipated that there are many different ways to define the forensic examination of digitally stored images. Despite the included definition, we received more inquiries concerning this area than any other. Further, the number of examinations reported for this category exceeds the other three categories. As a result, we recommend further study to refine the data from the category "digital evidence examinations." This also points out the convergent nature of this type of evidence and the difficulties in separating evidence from examination.

The following section will list the questions, the raw data and any discussion:

QUESTIONS AND RESPONSES

1. *Which of the following kinds of forensic examinations are conducted in your laboratory/unit?*

<u>37</u>	computer evidence
<u>23</u>	electronic devices
<u>42</u>	audio/video media
<u>40</u>	digital images

Discussion:

Fifty-four percent of the reporting agencies (37 of 68) report having a computer forensic program while thirty-four percent (23 of 68) perform forensic examinations of electronic devices. Over sixty-one percent (61.7%) of the agencies reported performing audio/video media examinations while just under fifty-nine percent (58.8%) do examinations of digital images.

2. *How many forensic examinations were conducted by your laboratory/unit during your most recent reporting year?*

computer evidence	<u>11142</u>
electronic devices	<u>576</u>
audio/video media	<u>15346</u>
digital images	<u>24226</u>

Discussion:

The high level of case work reported was surprising as was the proportions of the different types of examinations. When compared to the number of units reporting within each discipline, the workload is remarkable for such young programs. In the computer forensic area, the total number of cases, divided by the number of units, reveals an average of over three hundred cases per unit (11142 ÷ 37). Similarly, audio/video and digital imagery have 365 and 605 respectively. Only the electronic devices category had a more modest caseload of 25.

3. *How many full time/part time employees do you have dedicated to the examination of the following media types?*

	Full Time	Part Time
computer evidence	<u>267</u>	<u>71</u>
electronic devices	<u>22</u>	<u>9</u>
audio/video media	<u>101</u>	<u>12</u>
digital images	<u>85</u>	<u>27</u>

Discussion:

While averages could be computed relative to the number of cases per examiner and number of examiners per unit, it is clear that that data would not be definitive. As an example, there are fewer full time electronic device examiners than there are units doing these examinations. It is considered likely that individual examiners are being utilized in multiple functions within single organizations. It is recommended that a study of caseloads, controlled for the multiple variables be conducted.

4. *How many of your forensic examiners are sworn law enforcement officers or civilians?*

	Sworn officers	Civilians
computer evidence	<u>234</u>	<u>83</u>
electronic devices	<u>15</u>	<u>10</u>
audio/video media	<u>48</u>	<u>64</u>
digital images	<u>31</u>	<u>80</u>

Discussion:

It is interesting to note that digital imagery employs substantially more civilians than any of the other disciplines. This may be the result of traditionally civilian photographers evolving into the role of examiners, but we do not have any data to support that conclusion. Conversely, sworn officers outnumber civilian computer forensic examiners by almost three to one. Two possible reasons for this may be that 1) the computer data is more integral to the case and 2) traditional forensic science laboratories have been slow to provide adequate and timely services. Again, we have no data to support that hypothesis, but believe that it is a fertile area of study.

5. *Does your laboratory/unit have written protocols with respect to the following evidence types?*

	Yes	No	Not
Applicable			
computer evidence	<u>19</u>	_____	_____
electronic devices	<u>12</u>	_____	_____
audio/video media	<u>25</u>	_____	_____
digital images	<u>30</u>	_____	_____

Discussion:

Data was only considered from the “Yes” column, as respondents inconsistently marked responses in the “No” and “Not Applicable” fields. As a result, there would not have been referential integrity of the data. We have presumed that those who responded to the “Yes” column were indicating affirmatively that their organization had written protocols.

The results show that the use of written protocols is fairly common. Over seventy-seven percent of the digital imagery units reported using written protocols. Almost sixty percent (25 of 42) audio/video units, sixty-five percent (12 of 23) of electronic devices units and fifty-one percent (19 of 37) computer evidence units reported using written protocols.

6(a). *Does your laboratory/unit have a Quality Assurance Program?*

36 Yes _____ No (*If "NO" then proceed to Question 7*)

Discussion:

Virtually half (36 of 73) of all the responding units indicated that they had a quality assurance program in place. As QA programs tend to be implemented by agency rather than unit, the number would then increase slightly to almost 53% (36 of 68).

6(b). *Does your Quality Assurance Program apply to the following evidence types?*

	Yes	No	Not
Applicable			
computer evidence	<u>13</u>	_____	_____
electronic devices	<u>10</u>	_____	_____
audio/video media	<u>16</u>	_____	_____
digital images	<u>18</u>	_____	_____

Discussion:

For the same reasons presented for Question 5, only affirmative answers were tallied. In agencies where a QA program is in place, it is applied to the digital disciplines over a majority of the time. Taking the information from both Question

5 and Question 6(a), it would appear that in agencies where a QA program is in place and written protocols are in place, that the QA program has been applied to units that perform digital examinations.

7. *Is your laboratory/unit planning on adding or expanding its service offerings with respect to the following evidence types?*

	Add services	Expand services
computer evidence	_____	<u>31</u>
electronic devices	_____	<u>23</u>
audio/video media	_____	<u>32</u>
digital images	_____	<u>36</u>

Discussion:

Given the number of questions concerning what constituted adding versus expanding services, it was decided to combine all the affirmative responses. It is clear that almost half of the respondents intend to increase or add digital forensic services in all but the electronic devices area. Only about a third of the units or agencies intend to increase their services in that arena.

8. *Please use the following space (or attach a narrative) to provide a synopsis of how digital evidence is currently being handled in your jurisdiction. We are interested in any plans or projections for the course of digital evidence in your agency. You are also free to provide any additional information that you would like included in this study.*

The Federal Bureau of Investigation Laboratory Division appreciates your taking the time to participate in this survey. The information that you have provided will be included in the Proceedings of the INTERPOL 13th International Forensic Science Symposium.

Discussion:

Reporting agencies were generous in the amount of information that they provided in the narrative section. A number of themes emerged. Rapid change was reported so often as to be the norm. Many agencies report that they are evolving their organizations to not merely expand, but to improve quality.

Quite a few agencies report that investigative needs are driving the growth of computer forensic work. As a result, there are a number of agencies that report that their computer forensic program is located in their investigative program, rather than in the laboratory. However, a high percentage of them report either a move to bring the program under the supervision of the agency's laboratory or that the investigators performing computer forensics are required to operate under the laboratory's regulations.

In the area of digital imaging, there were a number of comments indicating that all of their photography, including crime scene, was going digital.

Sharing and partnering was another theme reflected in the comments. Many agencies that did not perform one or more of the digital disciplines, pointed to either another laboratory, usually associated with the next superior level of jurisdiction, or a task force. This has some significant ramifications on maintaining multi-jurisdictional standards of quality.

Appendix A
SWGDE Proposed Standards

Proposed Standards for the Exchange of Digital Evidence
As proposed by the Scientific Working Group on Digital Evidence
(United States)

INTRODUCTION:

This document contains a proposal for the establishment of standards for the exchange of digital evidence between sovereign entities. It was drafted by the Scientific Working Group on Digital Evidence and presented to the International Organization on Computer Evidence (IOCE) at the International Hi-tech Crimes Conference held in London, United Kingdom October 4-7, 1999. It is intended to elicit constructive discussion on the topic of digital evidence.

PURPOSE:

The last part of the twentieth century has been marked by the rise of the electronic transistor and all of the machines and ideas made possible by it. As a result, the world has changed from analog to digital. At the turn of the millennium, the computer reigns supreme over the digital domain. But it is, by no means, the only digital device. Indeed, an entire constellation of devices, from audio to video, communications to photographic, are becoming so closely associated with the computer as to have converged.

From a law enforcement perspective, more and more of the information that comprises the currency of the judicial process is being stored, transmitted or processed in digital form. Because of the tremendous connectivity that exists, criminals have the ability to act trans-jurisdictionally with ease. The world has become a single economy and companies providing goods and services are truly international. As a result, a perpetrator may be brought to justice in one jurisdiction, while the digital evidence required to successfully prosecute the case may only reside in other jurisdictions.

This situation requires that all nations have the ability to collect and preserve digital evidence not only for their own interest, but also in the interests of other sovereigns. Each jurisdiction is entitled to their own system of government and administration of justice. In order for one country to protect itself and its citizens, it must be able to make use of evidence collected by other countries.

It is not reasonable to expect all nations to know about and abide by the precise laws and rules of every other country. A way has to be found that will allow exchanges to be conducted. This document is the first attempt to define some basic landmarks for the technical aspects of these exchanges. If we can define the request, then we can deal with its fulfillment.

ORGANIZATION:

This document consists of three parts: an Introduction, Definitions and Standards. The Standards section is organized into principles. Under each Principle, there are two sub-sections: Standards and Criteria section and a Discussion section. This format was adopted so as to conform with the format of the American Society of Crime Laboratory Directors/Laboratory Accreditation Board manual.

DEFINITIONS:

Acquisition of Digital Evidence - The acquisition of digital evidence begins when information and/or physical items are collected or stored for examination purposes. (The term "evidence" implies that the collector of the evidence is one who is recognized by the courts. The process of collecting is also assumed to be a legal process and appropriate for rules of evidence in that locality. A data object or physical item only becomes evidence when so deemed by a law enforcement official or designee.)

Data Objects - Data objects are (information) associated with physical items, (and have potential probative value. Data objects may occur in different formats without altering the original information.)

Digital evidence - Is information of probative value stored or transmitted in digital form.

Physical Items - Physical items are those items on which data objects/information may be stored and/or through which data objects are transferred.

Original Digital Evidence - Original digital evidence is physical items and those data objects (which are) associated with those items at the time of acquisition.

Duplicate Digital Evidence - A duplicate is an accurate reproduction of all data objects contained on the original physical item.

Copy - A copy is an accurate reproduction of information contained in the data objects independent of the original physical item.

PRINCIPLES

Principle 1

In order to ensure that digital evidence is collected, preserved, examined or transferred in a manner that ensures the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system. This system will be referred to as Standard Operating Procedures (SOPs). These SOPs must be documented and use broadly accepted procedures, equipment and materials. Proper case records must support the use of SOPs.

STANDARDS AND CRITERIA

All agencies that seize and/or examine digital evidence must maintain an appropriate Standard Operating Procedures document. All elements of an agency's policies and procedures concerning digital evidence must be clearly set forth in this SOP document. The SOP document must be issued under the agency's management authority.

Discussion:

The use of SOPs is fundamental to both law enforcement and forensic science. Having written guidance that is consistent with scientific and legal principles is essential to the acceptance of results and conclusions by courts and other agencies. The development and implementation of these SOPs must be under an agency's management authority.

Standards and Criteria 1.2

Agency management must review the Standard Operating Procedures on an annual basis to ensure their continued suitability and effectiveness.

Discussion:

Rapid technological changes have been the hallmark of digital evidence. The types, formats, and methods for seizing and examining digital evidence are changing rapidly. In order to ensure that personnel, training, equipment and procedures continue to be appropriate and effective, management needs to review and update as necessary the SOP document on an annual basis.

Standards and Criteria 1.3

Procedures used must be generally accepted in the field or supported by data gathered and recorded in a scientific manner.

Discussion:

Since a variety of scientific procedures may validly be applied to a given problem, standards and criteria for assessing procedures need to remain flexible. The validity of a procedure may be established by demonstrating the accuracy and reliability of specific techniques. In the digital evidence area, peer review of SOPs by other agencies may be useful.

Standards and Criteria 1.4

The agency must maintain written copies of appropriate technical procedures.

Discussion:

Procedures should set forth their purpose and appropriate application. Required elements such as hardware and software must be listed. The proper steps for successful use should be listed or discussed. Any limitations on either the use of the procedure or in the use or interpretation of the results should be set forth. Personnel who utilize these procedures must be familiar with them and have them available for reference.

Standards and Criteria 1.5

The agency must utilize hardware and software that is appropriate and effective for the seizure/examination procedure intended.

Discussion:

Although many acceptable procedures may exist to perform a particular task, considerable variations in cases require that personnel have the flexibility to exercise discretion in selecting a method appropriate to the problem at hand.

Hardware used in the seizure and/or examination of digital evidence should be in good operating condition and be tested to ensure that it operates correctly. Software utilized must be tested to ensure it produces reliable results for use in examination and/or seizure purposes.

Standards and Criteria 1.6

All activity relating to the seizure, storage, examination or transfer of digital evidence must be recorded in written form and be available for review and testimony.

Discussion:

In general, documentation to support conclusions must be such, that in the absence of the originator, another competent person could evaluate what was done, interpret the data and come to the same conclusions as the originator.

The requirement for the reliability of evidence usually requires that a solid chain of custody be maintained concerning items of evidence. Documentation clearly establishing this must be maintained for all digital evidence.

Case notes and records of observations must be of a permanent nature. Handwritten notes and observations must be in ink, not pencil. Pencil (including color) may be appropriate for diagrams or making tracings. Any corrections to notes must be made by an initialled single strikeout. Nothing in the handwritten information should be obliterated or erased. A means of authentication of notes and records should be employed. Handwritten signatures, initials or digital signatures may be utilized for this purpose.

Standards and Criteria 1.7

Any action, which has the potential to alter, damage or destroy any aspect of original evidence, must be performed by qualified persons in a forensically sound manner.

Discussion:

As outlined in the preceding standards and criteria, evidence only has value if it can be shown to be accurate, reliable, and controlled. A quality forensic program consists of properly trained people, appropriate equipment, software and procedures that collectively ensure these three attributes.

Appendix B
IOCE Principles and Definitions

SECOND MEETING (7th October 1999), Marriott Hotel, London

PURPOSE OF MEETING

The IOCE Chairman, Mark Pollitt wished to seek ratification of a set of Principles that had been produced by the Forensic Computing, International Principles Workshop, and for which he wished to submit to the next G8 Meeting to be held in Berlin during November 1999.

WORKSHOP – TERMS OF REFERENCE

Guidelines used by the workshop for the production of International Principles. The G-8, the IOCE and the delegates to the International Hi-Tech Crime and Forensics Conference have recognised the necessity of relying on the exchange of digital evidence in trans-national law enforcement matters. It is hoped that the following developed Principles and definitions will form the basis for the establishment of universal practices, which will ensure the continuity, and reliability of evidence that will be exchanged between legal entities.

In order to be most effective, Principles must have certain characteristics.

Principles must:

be consistent with all legal systems

allow for the use of a common language

be durable

cross international boundaries

lead to the confidence in the integrity of evidence

be applicable to all forensic evidence.

Be applicable at all levels, from the individual, through agencies to countries.

Principles are not implementation plans. They are designed to allow each legal entity to design a programme that is appropriate to their situation. But by applying these Principles, digital evidence collected will be useful across national boundaries.

THE PRINCIPLES

The following Principles were established in the Workshop:

- 4# Upon seizing digital evidence, actions taken should not change that evidence.
- 4# When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- 4# All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
- 4# An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.

- 4# Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles

ACCOMPANYING DEFINITIONS

A number of accompanying definitions were produced during the workshop that are directly associated with the agreed Principles. These are:

- 4# *Digital Evidence*-Information stored or transmitted in binary form that may be relied upon in court.
- 4# *Original Digital Evidence*-Physical items and those data objects, which are associated with those items at the time.
- 4# *Duplicate Digital Evidence*-A duplicate is an accurate digital reproduction of the original evidence continued on the original physical item.
- 4# *Copy*-A copy is an accurate reproduction of information contained in the data objects independent of the original physical item.

PROPOSAL

The Chairman proposed that the items detailed in sections 3 & 4 should be ratified by the membership of IOCE and submitted to G8 for future actions.

The IOCE membership unanimously voted in favour of the proposal.

The Chairman agreed to ensure that these items were presented to G8 along with other items arising from the IHCFC Conference and that he would support that submission on behalf of IOCE.

It was agreed that further discussion was required on the 'granularity' arising from the Principles. For example the issue of 'forensic competency', a term used in the third Principle, is an issue for further debate with an aim to perhaps provide agreed international accreditation and validation of tools, techniques and training. Further work is required on issues relating to practices and procedures for the examination of digital evidence. In addition, the sharing of information relating to hi-tech crime and forensic computing, such as events, tools and techniques, should be further facilitated.

It was recommended that a workshop of practitioners from all the G8 nations be formed to develop further detailed guidelines to accompany the Principles.

Appendix C
SWGIT Definitions and Guidelines Scientific Working Group
for Imaging Technologies (SWGIT)

**Definitions and guidelines for the use of Imaging Technologies in the Criminal
Justice System**

(VERSION 2.1 - June 8, 1999)

BACKGROUND:

While digital imaging technologies have been used in a variety of scientific fields for decades, their application within the Criminal Justice System is relatively recent. Therefore, there is a need to gather and disseminate accurate information regarding the proper application of this and other imaging technologies (including silver-based film and video) in the Criminal Justice System.

MISSION STATEMENT:

The mission of the Scientific Working Group on Imaging Technologies (SWGIT) is to facilitate the integration of imaging technologies and systems within the Criminal Justice System (CJS) by providing definitions and recommendations for the capture, storage, processing, analysis, transmission, and output of images.

PURPOSE OF THIS DOCUMENT:

This document is intended to serve two purposes:

- 4# Provide a set of definitions for use by members of the CJS when discussing imaging and imaging technologies.
- 4# Provide a preliminary set of general guidelines for use by members of the CJS as they develop specific standard operating procedures for their respective agencies.

PART I: DEFINITIONS

Main Definitions pertaining to *Image*:

Image - (Webster's New World Dictionary, Third College Edition) 1 a) An imitation or representation of a person or thing, drawn, painted, photographed, etc.

Imaging Technologies - Any systems and/or methods used to capture, store, process, analyze, transmit, or produce an image. Such systems include (but are not limited to): film, electronic sensors, cameras, video devices, scanners, printers, computers, etc.

Archive Image - Either the primary or original image stored on media suitable for long-term storage.

Copy Image - A reproduction of information contained in a primary or original image.

Digital Image - An image that is stored in numerical form.

Duplicate Image - An accurate and complete replica of an original image, irrespective of media.

Primary Image - Refers to the first instance in which an image is recorded onto any media that is a separate, identifiable object or objects. Examples include: a digital image recorded on a flash card or a digital image downloaded from the Internet.

Original Image - An accurate and complete replica of the primary image, irrespective of media. For film and analog video, the primary image is the original image.

Processed Image - An output image (see *Image Processing*)

Working Image - Any image subjected to processing.

Other Definitions (alphabetically):

Archiving - Long-term storage of an image.

Artifact - Any information not present in the primary or original image inadvertently introduced by image processing.

Capture - The process of recording an image.

Capture Device - A device used in the recording of an image.

Compression - The process of reducing the size of a data file.

Digital Image File - A record that includes image data and related data objects.

File Format - The structure by which data is organized in a file.

Image Analysis - The extraction of information from an image beyond that which is readily apparent through visual examination.

Image Enhancement - Any process intended to improve the visual appearance of an image.

Image Output - The means by which an image is presented for examination or observation.

Image Processing - Any activity which transforms an input image into an output image.

Image Processing Log - A record of the steps used in the processing of an image.

Image Transmission - The act of moving images from one location to another.

Image Verification - A process by which an individual identifies an image as being an accurate representation.

Intermediate Storage - Any media or device on which an image is temporarily stored for transfer to permanent or archival storage.

Legacy File Management - A methodology for preserving data and images so that they are retrievable as technology changes.

Lossless Compression - Compression in which no image data is lost and the image can be retrieved in its original form.

Lossy Compression - Compression in which image data is lost and the image cannot be retrieved in its original form.

Native File Format - The file format of the primary image.

Source Code - The list of instructions written in a standard programming language used to construct a computer program. This information is not usually provided absent a court order or prior contractual agreement.

Storage - The act of preserving an image.

Storage Media - Any object on which an image is preserved.

PART II: GUIDELINES

Documented Procedures:

Organizations and individuals engaged in the capture, storage, processing, analysis, transmission, or output of imagery in the criminal justice system should ensure that their use of images and imaging technologies are governed by documented policies and procedures.

Preserving Original – storage:

The original image should be stored and maintained in an unaltered state. This includes maintaining original digital images in their native file formats. Duplicates or copies should be used for working images when applicable (see *Post-Capture Processing*).

The following media are recommended for the preservation of original images because of their quality, durability, permanence, and reliability:

- Silver-based film with the exception of instant film
- Write-once Compact Disk Recordable (CDR)
- Digital Versatile Disk Recordable (DVD-R)

The following are acceptable for the preservation of original images but care must be taken to avoid loss of data:

- Instant film separately fixed
- Photographic prints
- Diskettes
- Magnetic tape
- Fixed hard drives
- Removable magnetic media
- Compact flash cards
- PC cards
- Smart media
- Removable magneto-optical drives
- Write-once magneto-optical drives

The following are not considered to be acceptable for the preservation of original images:

- Instant film packs
- Inkjet prints
- Solid ink prints
- Thermal wax paper prints
- Dye-sublimation prints
- Dry-silver prints
- Laser prints
- Electro-static prints

Preserving Original - Post-Capture Processing:

Film - Can process the original if the processing is non-destructive.

Analog Video - Recommend minimal processing of original to avoid degradation of signal. If original is to be used, copy should be made prior to processing and analysis.

Digital - Make duplicate image and use this as the working image.

Documentation of Image Processing:

Techniques common to traditional darkrooms and digital imaging stations, such as cropping, dodging, burning, color balancing, and contrast adjustment, that are used to achieve an accurate recording of an event or object, are standard processing steps.

When the results of these steps are visually verifiable, documentation of such steps is not considered mandatory except when the image is subjected to image analysis.

Techniques, such as unsharp masking, multi-image averaging or integration, and Fourier analysis, that are used to increase the visibility of specific details in an image at the expense of other image details are standard processing steps. However, the use of such steps should be documented in the case notes in sufficient detail that another comparably trained individual can repeat these steps and produce the same output when the image is subjected to image analysis.

Verification of Original and Processed Images:

An individual who captured the original image or was present at the time the original image was captured can verify that the image is *a true and accurate representation*.

Any processed image subjected to image analysis should be documented with an image processing log. An image not subjected to image analysis does not need a log.

It is recommended that the image processing log document steps such as: dodging, burning, color balancing, contrast adjustment, unsharp masking, multi-image averaging or integration, and Fourier analysis, etc. The use of such steps should be documented in the case notes in sufficient detail that another comparably trained individual can repeat these steps and produce a similar output.

Preserving Original - Chain of Custody:

A chain of custody must be maintained for the film or video tape upon which original images are recorded.

For digital images, the chain of custody should document the identity of the individuals who had custody and control of the digital image file from the point of capture to archiving. Once the file has been archived, the chain of custody should document the identity of the individuals who had custody and control of the archived image.

Guidelines for Software:

Software used in the processing and analysis of digital images should produce consistent results, permitting another comparably trained individual to achieve similar results.

LEGAL NOTE: Manufacturers of software used for image processing may be required to make the software source code available to litigants, subject to an appropriate protective order designed to protect the manufacturer's proprietary interests. Failure on the part of the manufacturer to provide this information to litigants could result in the exclusion of imaging evidence in court proceedings. This should be considered when selecting software.

Guidelines for Compression:

Original images and images expected to undergo image analysis should not be subjected to lossy compression. If compression is necessary, lossless compression is strongly recommended. If lossy compression must be used, then the highest quality option is recommended. Note that if lossy compression is used, critical image information could be lost and artifacts introduced as a result of the compression process. Repeated saving of a file using lossy compression may exacerbate the loss of image information.

Guidelines for Image Capture:

Image capture devices should be capable of rendering an accurate representation of the item(s) of interest. Different applications will dictate different standards of accuracy. At a minimum, the following should be considered when selecting appropriate devices:

- Characteristics (size, movement, location, etc.) of the scene/item(s) of interest
- Lighting of the items of interest
- Dynamic range of the scene
- Time constraints
- Required end product(s).

It is strongly recommended that conventional silver-based film be the primary media for documenting crime scenes. This documentation may be supplemented by analog video and/or digital imaging.

Guidelines for Image Output

An output device should be capable of producing an accurate representation of the input image. The following should be considered in the selection of output devices:

- Final use of image
- Time constraints
- Longevity/permanence of output image
- Spatial resolution required
- Range of colors and brightness to be produced

Guidelines for Image Transmission:

Received images should accurately reflect the transmitted images. The following should be considered in the selection of transmission methods and devices:

- Final use of image
- Time constraints
- File size
- Security of transmission
- Integrity of transmission
- Hardware and software compatibility of transmitters and receivers
- File format compatibility

PART III: ELEMENTS OF STANDARD OPERATING PROCEDURES (SOPS)

The following elements should be considered when formulating standard operating procedures:

Title - The title should be a descriptive name for the procedure.

Purpose - Why, when, and by whom the procedure is used.

Equipment/Materials/Standards/Controls - Identifies what items are required to perform the procedure. This may include protective equipment, hardware, software, and configurations.

Procedures - A step-by-step description of how the procedure is conducted. If appropriate, instructions should include precautions to be taken to minimize degradation.

Calibration - Describes any steps required to ensure the accuracy and reliability of the procedure. Where applicable, instrumentation setup and calibration procedures should be documented.

Calculation - Describes any mathematical operations that are applicable to the procedure.

Limitations - Describes any actions, interpretations, or equipment that are not appropriate for the procedure.

Safety - Identifies and addresses potential hazards in the use of the procedure.

References - Identifies documents both internal and external to the user agency regarding the procedure, related procedures, and principles behind them.

PART IV: QUALITY ASSURANCE

Organizations which utilize images and imaging technologies in the criminal justice system should implement quality assurance programs to ensure that results achieved are repeatable and valid. As part of these programs, performance checks and corrective actions should be documented.

Equipment:

Where applicable, equipment utilized in imaging should be checked regularly for proper performance and calibration, and findings documented. Where applicable, an end-to-end system check for consistency within specified system parameters should be performed on a regular basis and whenever modifications are made to the system. All equipment should be maintained according to the manufacturers' specifications and recommendations as contained in the operating manuals.

When a piece of equipment or a system falls outside the specifications and recommendations, the equipment or system should be taken out of service until such time as it has been corrected. Evaluation of equipment and system checks should be documented inclusive of corrective actions.

Software:

If software errors that significantly affect the results of a processing step are detected, then corrective actions should be taken. If the manufacturer identifies software errors and provides corrective remedies for them, the remedies should be implemented before the software is used again. Once corrective actions have been taken, an end-to-end system check should be performed prior to putting the system back into operation.

Personnel:

All personnel utilizing imaging technologies shall be trained and tested for competency and proficiency in the agency's standard operating procedures and the operation of the relevant imaging technologies. A formal training program should be documented and maintained, with the results of competency and proficiency tests documented. Proficiency testing should be repeated on a regular basis or when significant changes in hardware or software are made.

PART V: TRAINING, QUALIFICATIONS AND PROFICIENCY

Awareness Training - Photographers/Imaging Scientists:

Individuals and organizations within the law enforcement community engaged in the production or use of images should be aware of the standard procedures commonly utilized within the community and should strive to conform to or exceed these standards. These individuals should also endeavor to maintain awareness of new developments as they arise.

Organizations and/or individuals engaged in the production of images should define and implement quality assurance programs to ensure the following: reliable services; implementation of recognized standards for good practice; and use of valid, reliable procedures adequate for the task. Individuals should receive training in these quality systems.

Individuals engaged in the production of images should maintain proficiency in their field by pursuing continuing education courses in imaging.

Individuals engaged in the production of images should maintain awareness of legal developments relating to the use of imaging technologies by the criminal justice system.

Technical Skills Training:

Personnel responsible for operating imaging technologies should be trained in the operation of those technologies and should be able to explain their operation to a lay jury. Individuals should receive training in the following categories based on their specific applications:

Image Acquisition and Storage:

- a. Capture (multiple sub-categories: field/studio/ scanner/camera/media)**
- b. Transfer**
- c. Storage**

Image Processing:

- a. Intermediate storage/working images**
- b. Image enhancement processes**
- c. Application specific processes**

Output:

- a. Printers**
- b. Papers**
- c. Film recorders**
- d. Monitors**
- e. Video**
- f. Other devices and media Transmission**

Awareness Training - End Users:

Individuals and organizations within the criminal justice system who utilize images must also be aware of the capabilities and limitations of specific imaging technologies available. The following individuals would benefit from training in imaging technologies:

- 1. Investigators**
- 2. Managers**
- 3. Court Officials**

This document is identified as Version 2.1. Information referenced to this document can be identified as Version 2.1, 6/8/99.

Appendix D
G8 Proposed Principles

High Tech Crime Sub-Group, G8
G8 Proposed Principles for the Procedures Relating to Digital Evidence

In March 1998, IOCE was appointed to draw international principles for the procedures relating to digital evidence, to ensure the harmonization of methods and practices among nations and guarantee the ability to use digital evidence collected by one state in the courts of another state.

In March 2000, the first report of IOCE was presented to the subgroup, proposing a series of definitions and principles, following the International high-tech crimes and forensics conference in London in October 1999.

After review by the experts of the subgroup, the following recommendations are made:

Each member State is encouraged to consider the following principles when establishing procedures for the collection, preservation and use of digital evidence, according to its national law and standards bodies, and to be aware of potential differences when collecting evidence at the request of other States.

These principles should be submitted by IOCE to other national, regional and international standards making bodies and organizations responsible for the promotion of procedures relating to digital evidence for review.

IOCE should develop in consultation with the above-mentioned bodies, a generic good practice guide for the collection, preservation and use of digital evidence, encompassing the range of existing sources of digital evidence.

The high-tech crime subgroup should review regularly the work of IOCE.

Principles:

- 4# When dealing with digital evidence, all of the general forensic and procedural principles must be applied.**
- 4# Upon seizing digital evidence, actions taken should not change that evidence.**
- 4# When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.**
- 4# All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.**
- 4# An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.**
- 4# Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles**

General Definitions relating to digital evidence

Digital Evidence

Information stored or transmitted in binary form that may be relied upon in court.

Original Digital Evidence

Physical items and those data objects, which are associated with those items at the time of seizure.

Duplicate Digital Evidence

A duplicate is an accurate digital reproduction of all data objects contained on the original physical item.

Copy

A copy is an accurate reproduction of information contained in the data objects independent of the original physical item.

Appendix E
Bibliography

Bibliography

The following documents are of fairly recent publication and may provide useful information to forensic practitioners.

Barrett, Neil. *Digital Crime – Policing the Cybernation*. Kogan Page Limited. 1997

Icove, David, Seger, Karl, VonStorch, William. *Computer Crime – A Crimefighter’s Handbook*. O’Reilly & Associates, Inc. 1995

National Institute of Justice. *Electronic Crime Needs Assessment for State and Local Law Enforcement*, by Hollis Stambaugh, David S. Beaupre, David J. Icove, Richard Baker, Wayne Cassaday, and Wayne P. Williams, March 2001

Stephenson, Peter. *Investigating Computer-Related Crime*. CRC Press. 2000.

Sammes, Tony, Jenkinson, Brian. *Forensic Computing – A Practitioner’s Guide*. 2000.

Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press 2000

United States Department of Justice. *Searching and Seizing Computers And Obtaining Electronic Evidence in Criminal Investigations*.
<http://www.usdoj.gov/criminal/cybercrime/searching.html>

Appendix F
Survey Respondents

**UC Mark Pollitt
FBI Laboratory
Computer Analysis Response Team
935 Pennsylvania Ave NW
Washington, DC 20535
USA**

**S/Sgt. Peter Frasier
Audio/Visual Analysis Section
Royal Canadian Mounted Police
1426 St. Joseph Blvd. Rm 1330
Ottawa, Ontario KIA 0R2
Canada**

**Inspector PA. Macaulay
High Tech Crime Forensics
Royal Canadian Mounted Police
1426 St. Joseph Blvd.
Ottawa, Ontario KIA 0R2
Canada**

**Professor Kostadin Bobev, Dir.
Document Exams/ Forensic Photography/
Voice Analysis Section
Research Institute of
Forensic Science & Criminology
P.O. Box 934
1000 Sofia, Bulgaria**

**Inv. Joseph Hennehey
Computer Crime Unit
Monroe County Sheriffs Office
130 S. Plymouth Ave
Rochester, NY 14614
USA**

**DSFC Dan Herley
High Tech Crimes & Investigations Support Unit
New Jersey State Police
1 River Road
West Trenton, NJ 08628
USA**

**Karen L. Irish/
Sgt. Robert Derbyshire
Forensic Services Section
Baltimore County Police Department
700 East Joppa Rd.
Towson, MD 21286
USA**

**Patricia Sempels
DJT - Audio
DGJ
Rue du Royale, 211
B - 1000- Bruxelles
Belgium**

**Daniel C. Nippes
Regional Crime Lab at IRCC
3209 Virginia Avenue
Ft. Pierce, FL 34981
USA**

**Joseph Henre
Regional Computer Crime Enforcement Group
St. Charles Co. Sheriffs Dept.
301 N. Second Street
St. Charles, MO 63301
USA**

**Karen Smith
Pensacola Regional Operations Center
Florida Dept. of Law Enforcement
1301 N. Palafox Street
Pensacola, FL 32501
USA**

**Sgt. Jon Pacewicz
High Tech Crime Detail
San Bernardino Co. Sheriff's Dept.
655 E. Third St.
San Bernardino, CA 92415
USA**

**Chester W. Ubowski, Agent-in-Charge
Denver Forensic Laboratory
Colorado Bureau of Investigation
690 Kipling Street
Denver, CO 80215
USA**

**Kenneth H. Michau
Arkansas State Crime Laboratory
#3 Natural Resources Drive
Little Rock, AR 72023
USA**

**Det. Scergeant Paul Gillen
Garda Computer Crime Investigation Unit
An Garda Siochana
Harcoute, Sq., Harcourt St.
Dublin 2
Ireland**

**Deputy Director Kathleen Barch
Computer Crime Unit
Ohio Bureau of Criminal Investigation
1560 St. Route 56
London, OH 43140
USA**

**Charles M. Pruitt
Forensic Imaging Section
Division of Forensic Science
Central Lab
300 N. 5th Street
Richmond, VA 23219
USA**

**Pierre D. Bernier
Ministere de La Securite Publique
1701 Parthenais
Montreal H21 3S7
Canada**

**Detective Chris Duque
White Collar Crime Unit
801 S. Beretania St.
Honolulu, HI 96813
USA**

**J. Lauridson
Alabama Department of Forensic Sciences
P.O. Box 240591
Montgomery, AL 36124-0591
USA**

**Mike Allen
Mississippi Crime Laboratory
Main Lab
1700 E. Woodrow Wilson Avc.
Jackson, MS 39216
USA**

**Lori Bates Wilson
Regional Crime Lab
Jefferson Co. Sheriffs Office
5030 Hwy. 69 South, Suite 500
Beaumont, TX 77705
USA**

**Sonja L. Rawn
Forensic Laboratory
Div. of State Fire Marshal
Ohio State Dept. of Commerce
8895 East Main Street
Reynoldsburg, OH 43068
USA**

**Roger Thompson/Ray Nance
Police Crime Laboratory
Charlotte/Mecklenburg Police Department
601 E. Trade St.
Charlotte, NC 28202
USA**

**James Hamby, Director
Indianapolis-Marion County Forensic Services
40 5. Alabama St.
Indianapolis, IN 46204
USA**

**Mark Huntzinger
City/County Crime Laboratory
Tucson Police Department
270 South Stone Avenue
Tucson, AZ 85701-1917
USA**

**Sergeant R.A. Theis
Forensic Laboratory
West Virginia State Police
725 Jefferson Road
S. Charleston, WV 25309-1698
USA**

**Verlin Cross
National Fish & Wildlife Forensics Laboratory
U.S. Fish & Wildlife Service
1490 E. Main St.
Ashland, OR 97520
USA**

**William J. Darby III
TBI Crime Laboratory
Tennessee Bureau of Investigation
901 R. S. Gass Blvd.
Nashville, TN 37216
USA**

**Elizabeth K. Balraj, M.D.
Cuyahoga County Coroner's Office
11001 Cedar Ave.
Cleveland, OH 44106
USA**

**Lt. Chip Johnson
Computer Crimes Unit
South Carolina Law Enforcement Div.
P.O. Box 21398
Columbia, SC 29221-1398
USA**

**Captain Richard Lowthian
MSP Laboratory System
Michigan State Police
714 S. Harrison Rd.
East Lansing, MI 48823
USA**

**Harold R. Messler
St. Louis Metropolitan Police
1200 Clark Avenue
St. Louis, MO 63103
USA**

**F/Sgt. Shannon Spreckelmeyer
Identification Unit
Indiana State Police Laboratory
8500E. 21st. St.
Indianapolis. IN 46219
USA**

**David Bicigo
Microtrace
Michigan State Police Forensic Lab
6296 Dixie Hwy., P.O. Box 608
Bridgeport, MI 48722
USA**

**Det. Michael Lee
Laboratory
Anderson Police Department
700 Meridian St.
Anderson, IN 46016
USA**

**Rex Riis
SD Forensic Lab
South Dakota Div. of Criminal Investigation
500 E. Capitol
Pierre, SD 57501
USA**

**Mike Heintzrnan
Salem Forensic Lab
Oregon State Police
3772 Portland Rd. NE
Salem, OR 97303
USA**

**Robert Sanders
State Crime Lab/Forensic Imaging Unit
Wisconsin State Department of Justice
7100 Stewart Ave
Wausau, WI 54401
USA**

**David McGill
Forensic Imaging Unit
Montgomery Co. Department of Police
2350 Research Blvd.
Rockville, MD 20850
USA**

**Acting Detective Sergeant Wisniewski
Computer Crime Investigation
Western Australia Police Service
Lever 7, Eastpoint Plaza, 233 Adelaide Terrace
Perth 6000 W. Australia
Australia**

**Haakan Bergstedt
SKL - National Laboratory of Forensic Science
SKL
S-58 194 Linkoping
Sweden**

**Robert Thibault
US Army Criminal Investigation Laboratory
US Army Criminal Investigation Command
4553 North 2nd. Street
Forest Park, GA 30297-5122
USA**

**Dr. L. W. Russell
Digital Service Group/Metropolitan Lab London
Forensic Science Service
109 Lambeth Road
London SE1 7LP
United Kingdom**

**Oklahoma State Bureau of Investigation
Investigative Division
6600 North Harvey
Oklahoma City, OK 73116
USA**

**Kenneth Zercie, Assistant Director
Division of Scientific Services
Forensic Science Laboratory
Connecticut Department of Public Safety
278 Colony Street
Meriden, CT 06451
USA**

**Antipas O.A. Nyanjwa
Computer Crime & Digital Evidence Recovery Unit
Criminal Investigations Department
P.O. Box 30036
Nairobi
Kenya**

**Zeno Scrads
Netherlands Forensic Institute
Digital Evidence Unit
Ministry of Justice
P.O. Box 3110
2280 GD Rijswijk
Netherlands**

**Chris DeVeth
National Institute of Forensic Science
98-100 vilvoordse Steenweg
1120 Brussels
Belgium**

**Lt. Robert Tavenner
Economic /Cybercrime Investigative Unit
VA State Police
P.O. Box 27472
Richmond, VA 23261-7472
USA**

**Jwonna Rucinska
Central Forensic Laboratory of Polish Police
High Command of Polish Police
Al Ujazdowskie 7
00-583 Warsaw
Poland**

**Sergeant Troy OMalley
Electronic Recording Section
Queensland Police Service
Floor 5, 200 Roma Street
Brisbane, Queensland 4001
Australia**

**Sergeant Peter Lehmann
Communications Center Technical Support Unit
South Australia Police
GPO Box 1539
Adelaide, South Australia 5001
Australia**

**Dusty Clark
Bureau of Forensic Services
California Department of Justice
4949 Broadway
Sacramento, CA 95820
USA**

**Denise Walter/Sgt. David Oldford
Forensic Imaging Services
Royal Canadian Mounted Police
1200 Vanier Parkway
Ottawa, ON KIA 0R2
Canada**

**Dean Catoggio
Victoria Forensic Science Centre
Victoria Police
Forensic Drive
Macleod Victoria 3085
Australia**

**Senior Constable Darren Bails
Photographic Section
Forensic Serv. Branch
South Australia Police
1 Angas Street
Adelaide 5000, So. Australia
Australia**

**Liga Peisniece
Forensic Research Centre
State Police
12 B. Bruninicku Street
Riga, LV 4009
Latvia**

**Dr. Walter Bruschweiler
Scientific Forensic Service
Zurich City Police
Zeughausstrasse I I
CH-8004 Zurich
Switzerland**

**Linda T. Errichetto, Director
LVMPD Forensic Laboratory
Las Vegas Metropolitan Police Dept.
6767 West Charleston Blvd.
Las Vegas, NV 89146
USA**

**Det. Chief Superintendent Frank Jensen
Forensic Technical Department
The National Commissioner/ Dept. A.
Slotsnerrensvej 113
DK-2720 Vaniose
Denmark**

**Agent Superintendent B' Andreas Nikolaides
Police Forensic Laboratory
Cyprus Police
1478 Nicosia, Cyprus
Greece
Dimitrios Agelopoulous**

**Forensic Science Division
Digital Evidence Unit
Hellenic Police
173 Alexandras Ave.
11522 Athens
Greece**

**Gorazd Pezdir
Forensic Science Laboratory
Ministry of the Interior
Stefanova 2
1501 Ljubljana, Slovenia
Yugoslavia**

**Captain Patrick Olvey
Regional Electronics Computer Intelligence Section
Hamilton County Sheriff's Office/Cincinnati PD
1000 Sycamore Street, Rm. 110
Cincinnati, OH 45202
USA**

**Charles M. Richardson
Office of Forensic Sciences
Drug Enforcement Agency
700 Army Navy Dr. Rm. 7320
Arlington, VA 22202
USA**

**Bahadic K. Akcam
KPL- Crim. Police Lab
Voice Video Data Analysis Unit
General Directorate of Security
Kriminal Police Laboratories
06100 Ankara
Turkey**

**Dr. Peter Halicky
Kriminalisticka Informatika (FIT)
Institute Forensic Science of Slovak Police
Sklahinska I
Bratislava 81272
Czech Republic**

**Sam Guttman
Digital Evidence
U.S. Postal inspection Service
22433 Randolph Dr.
Dulles, VA 20104-1000
USA**

**Sergeant Guy Pierce
Criminalistics
Albuquerque Police Department
400 Roma NW
Albuquerque, NM 87102
USA**

**Lt. Barry E. Leese
Computer Crimes Unit
Maryland State Police
7155-C Columbia Gateway Dr.
Colombia, MD 21046
USA**

**Seiji Mineta
Police Communications Research Center
National Police Agency
4-13-1, Nakano
Nakano-ku, Tokyo 164-000 1
Japan**

Toshihiko Kamon
High-Tech Crime Technology Division
National Police Agency
2-1-2, Kasumigaseki, Chiyoda-ku
Tokyo 100-8974
Japan

Masumi Tanimoto
Natl. Research Institute of Police Science
Acoustics Section
National Police Agency
6-3-I, Kashiwanoha, Kashiwa
Chiba, 277-0882
Japan