AFRL-IF-RS-TR-2002-269
Final Technical Report
October 2002

CYBER-FORENSIC RESEARCH EXPERIMENTATION AND TEST ENVIRONMENT (CREATE)

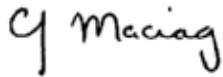**Utica College**

**AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK**

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2002-269 has been reviewed and is approved for publication.

APPROVED:　*CJ Maciag*
　　　　　　CHESTER J. MACIAG
　　　　　　Project Engineer

FOR THE DIRECTOR:　*[signature]*
　　　　　　WARREN H. DEBANY, Technical Advisor
　　　　　　Information Grid Division
　　　　　　Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	October 2002	Final Feb 01 – Feb 02

4. TITLE AND SUBTITLE
CYBER-FORENSIC RESEARCH EXPERIMENTATION AND TEST ENVIRONMENT (CREATE)

5. FUNDING NUMBERS
C - F30602-01-1-0506
PE - 62702F
PR - 01PG
TA - 32
WU - P4

6. AUTHOR(S)
Gary R. Gorden and Chester D. Hosmer

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Prime:
Utica College
CFR&D Center
1600 Burrstone Road
Utica New York 13502

Sub:
Wetstone Technologies
17 Main Street, Ste 237
Cortland New York 13045

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/IFGB
525 Brooks Road
Rome New York 13441-4505

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

AFRL-IF-RS-TR-2002-269

11. SUPPLEMENTARY NOTES

AFRL Project Engineer: Chester J. Maciag/IFGB/(315) 330-3184/ Chester.Maciag@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 Words)*

The objective of this effort was to develop methodologies and standards for cyber forensics methods and tools. The current cyber forensic certification/validation efforts are described along with a best practices model. The potential for an Information Analysis Center (IAC) in computer forensics was explored. Finally, the International Journal of Digital Evidence, an online journal, was established to report the research findings in these areas as well as other cyber forensics research.

14. SUBJECT TERMS
Cyber Forensics, Cyber Forensics Standards, Cyber Forensics Certification and validation, Cyber Forensics Information Analysis Center

15. NUMBER OF PAGES
112

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Table of Contents

1   Background

The Computer Forensics Research & Development Center at Utica College (CFRDC) was established in May 1999 as one of the tasks of the Forensics Information Warfare (FIW) Study (AFRL Contract F30602-98-C-0243). This research project fits the mission of the CFRDC; to advance the state-of-the-art of cyber forensics research and development. The work to date positioned the Center to complete the five tasks in this study. The subcontractor, Wetstone Technologies, Inc., provided significant expertise in the areas of cyber forensics and software development to this project.

1.1 Period of performance

This report reflects work done on the complete effort from 2/27/01 – 2/27/02.

1.2   The Team

Dr. Gary R. Gordon, director of the CFRDC, was the principal investigator and Chet Hosmer, President & CEO of WetStone Technologies, Inc. was the subcontractor on this project. The staff of the CFRDC, Christine Siedsma, Program Manager, and Matt Ward, Research Associate, provided significant support. Dr. Don Rebovich, Associate Professor of Economic Crime Programs at Utica College, was a key contributor.

2   Technical Program

During this effort, the Computer Forensics Research & Development Center accomplished the following five tasks.

2.1   Tasks and Deliverables

2.1.1   Task 1 – Definition of a cyber-forensics experimentation methodology

The proposed concept was to develop a methodology for carrying out cyber forensics experiments. Such a model would provide a capacity to gauge the performance of cyber forensic tools designed for defensive and attack environments. An analysis of CFX 2000 results was a key component in this process.

The work in this area was limited to the analysis of the results of CFX 2000 to ascertain lessons learned to assist in the development of a test bed environment to gauge the performance of cyber forensic tools. While outside of the scope of the contract, CFX II was reviewed and recommendations are made for future events of this kind.

Deliverable:

➢ Report on CFX 2000 and CFX II with recommendations for similar events in the future.

2.1.2   Task 2 – Establish standards and criteria for cyber-forensic technologies

During this task, current state-of-the-art standards for key processes in cyber forensics were examined. Based on this review, the best of breed standards were compiled for the key processes in cyber forensics: evidence collection and preservation, evidence organization, evidence examination, and analysis.

Based on this assessment, it would be premature to present anything but the best of breed standards to date. Designing standards in a vacuum would be counterproductive. Efforts are underway to test some of these standards in very specific and narrow aspects of cyber forensics. Considerable consensus building will be required before a cyber forensics standard requirements document can be written. It is hoped that the International Journal of Digital Evidence (see Task 5) will be a key conduit in this process.

Deliverable:

➢ Report on the best of breed standards for key processes in cyber forensics.

2.1.3   Task 3 – Develop a certification process for cyber forensic technologies

This task examined certification process in other areas of forensics and applied the process to computer forensics and the current practices for certifying computer forensics tools and methodologies. Based on these reviews, an assessment was made for the efficacy of certification and validation of cyber forensic tools.

Deliverable:

  ➢ Certification Practices Requirement Document

2.1.4   Task 4 – Define the Cyber Forensic Information Analysis Center (CFIAC) charter

During this task, the structure and long term operational plan for a CFIAC was reviewed. Current Information Analysis Centers (IACs) in areas related to cyber forensics were examined. The research results of Tasks 1-3 were analyzed to determine if there was a need for a CFIAC. Based on this assessment, a design for a CFIAC was proposed.

Deliverable:

  ➢ CFIAC Requirements Document

2.1.5   Task 5 – Publish the quarterly cyber forensics journal TRACES

The CFRDC has taken the lead and established a quarterly journal in the area of cyber forensics, and renamed it the International Journal of Digital Evidence (IJDE). This included the establishment of an editorial board, developing and hosting the online journal on a web site, and the solicitation of articles for the first issue. Dr. Gary R. Gordon is the editor and Dr. John Leeson is the Associate Editor.

The IJDE is a forum for discussion of theory, research, policy, and practice in the rapidly changing field of digital evidence. In the first issue, there are three articles that address many of the issues raised in Tasks 2 & 3 of this report.

Deliverable:

  ➢ The inaugural issue of the International Journal of Digital Evidence (IJDE)

3 Task 1 – Definition of a Cyber Forensic Experimentation Methodology

3.1 Introduction

The Cyber Forensics Experiment (CFX 2000) was a project funded by Air Force Research Laboratories Information Directorate and hosted by the New York State Police in their Forensic Investigation Center (FIC), Albany, New York. The National Law Enforcement and Corrections Technology Center (NLECTC) was the prime contractor with Wetstone Technologies, Inc. the subcontractor.

The goal of CFX 2000 was to perform technical analysis and evaluation of computer forensic tools, and provide recommendations for the law enforcement and military defense communities in response to cyber threats. This was accomplished by enacting a realistic scenario depicting a cyber attack on an information and economic infrastructure.

The Computer Forensics Research and Development Center (CFRDC) at Utica College played a key role in the development of the cyber crime scenario, as well as the creation of the digital evidence associated with this scenario. The CFRDC developed evidentiary e-mails (as well as several megabytes of innocuous email), spreadsheets, documents, and other evidence that related to the scenario.

The Cyber Forensic Experiment was conducted over a three-day period, October 23-25, 2000, at the FIC in Albany. Law enforcement personnel skilled in cyber crime investigations, analysts, and administrators were invited to participate in the event. Teams of investigators and analysts used cyber forensic development tools, as well as GOTS and COTS, to analyze the data from the case study.. Members of the CFRDC and the NLECTC played the roles of suspect individuals in the scenario, and were available for interview by the investigators. Software developers were on hand to assist the participants with the state-of-the-art cyber forensics tools.

4 Statement of Work

The following is an excerpt from the original statement of work prepared by Chet Hosmer for Emergent Technologies.

4.1 Overview

The purpose of this effort is to formalize "Cyber-Forensic Experiment CFX-2000," a realistic multi-faceted scenario of an advanced cyber attack that could threaten U.S. interest. This effort is funded and supported by the U.S. Air Force Research Laboratory Information Directorate at Rome, for the sole purpose of evaluating the effectiveness of both offensive and defensive cyber-warfare technology.

This experiment will involve the DoD, Law Enforcement and private industry organizations and their personnel in order to carry out a realistic experiment. In order to accomplish this, the exercise must have elements that interest Law Enforcement, Business and Industry, and Defense as part of the experiment scenario. This is certainly difficult to do, since there has been limited cooperation in these matters in most documented cases to-date. Furthermore, jurisdictional, political, legal, proprietary, privacy, and publicity issues are typically difficult, if not impossible, to sort out. And, when the crime is multi-national, the situation is further complicated.

The purpose of the experiment is to produce an advanced, yet realistic cyber crime scenario that challenges the capabilities of public, private, and defense capabilities. Since the experiment is to be held over a 3-day period, evidence of the criminal activities will be manufactured, since the actual criminal and terrorist activities may have been planned and carried out over several months. In addition, all the organizations, computers, networks and equipment will be fabricated and generally represent fictitious entities and organizations.

Technical Approach and Objectives

Basic Premises

- Current forensic process is only partially automated.
- Forensic process is reactionary and postmortem – not systematic.
- We don't know what we don't know.
- We focus on inculpatory and discrete pieces of evidence, which is dangerous when investigating sophisticated multifaceted cyber-crimes.
- Tools are stove piped point solutions with no interoperability.
- Tracing back to the source of the attack is a lethargic manpower intensive process.
- Novel & sophisticated distributed attacks are difficult to identify, reconstruct, determine motive and intent, or identify the real or next targets.
- Sophisticated attackers are skilled at covering their tracks.

Hypothesis

Using a total systemic approach with an integrated forensic framework, it is possible to accurately understand the motive, intent, threat, sophistication, capabilities, identity and location, and the targets of cyber criminals and terrorists. By placing this information/intelligence in the right hands we can achieve true information superiority.

Metrics

- Knowledge (what do we know about: who, what, where, when, how and why?)
- Timeliness (when did we know it: in time or too late?)
- Accuracy (How much did we get right?)
- Depth (Did we find the obvious, the subtle, the obscure?)

Stage controlled experiment

- Develop multifaceted cyber-crime scenario (cyber-crime and cyber-terrorism)
- Get practitioners to develop (think like criminals not technologists)
- Carefully execute
- Integrate best of breed technologies and talent
- Build a top-down systematic process
- Structure the team and players
- Use an integrated Framework (SI-FI)
- Integrate GOTS, COTS, and R&D Tools
- Use real investigators / compliment with technology experts
- Evaluate
- Carefully collect all data, decisions actions during experiment
- Develop metrics for evaluation that match scenario
- Quantify results

What is different?

- Collaborative effort with DoD, NIJ, Law Enforcement, Commercial, and Academic organizations
- First known integration of automated tools for detecting and investigating an information attack
- Attempt to develop metrics to provide accurate evaluation of experiment results

4.1.1 Funding

4.1.2 Development Team

The following people were assigned to the development team and given primary responsibility for the development of the CFX scenario and generating the case data:

WetStone Technologies Inc.,

Chet Hosmer   President
Dr. Gary Gordon   Vice President
Chris Brennan   Technical/Network Specialist
Christine Siedsma   Cyber Forensics Researcher

The Computer Forensics Research & Development Center (CFRDC) at Utica College

Christopher Hyde   Project Coordinator
Steve Gimelli   Student Researcher
Jason Galarneau   Student Researcher
Shataqua Henry   Student Researcher
Jerry Stellatos   Student Researcher

Emergent Technologies

Fred Demma
Jim Ricardi
Barbara Plonish
Derrick Bronner
Robert McOrmond
Dan Kalil

4.1.3   Scenario Development

In order to create a real scenario, we first created a process for building the scenario in much the same way that a writer, novelist, or playwright would construct their art. The following are the steps that were taken in order to fabricate the crime scenario and crime scene for this experiment.

Determine High-level requirements for the scenario

Realistic and Complex Scenario: The scenario had to be complex enough to pose a challenge to the investigators but also be simple enough for them to make significant progress during the two-day investigative time limit.

Multiple Related Crimes: We wanted to create a scenario that included multiple crimes to add to the complexity of the scenario. This forced investigators to follow the crimes and use different tools on different types of evidence.

Multiple Jurisdictions: This was done to have the scenario appeal to the different types of investigators (Military, Federal and Local Law Enforcement, Private Sector) and to help make the scenario resemble real life situations where modern investigations tend to cross at least one of these boundaries.

Create a Storyboard

Based on these requirements, Chet Hosmer and Dr. Gary Gordon created an outline for a possible scenario that involved terrorist activity being funded by money laundering activities. They also specified certain organizations and the basic characters that would be involved. This information was given to the CFRDC team, which created a storyboard of the basic scenario using Analyst Notebook (See Appendix A).

Define in Detail all of the Fictitious Entities

The scenario for CFX 2000 required the creation of several fictitious entities. To add realism to the scenario, some of the entities we created are loosely based on real corporations and organizations. This scenario is a pure work of fiction and is not meant to imply anything about the actual entities or actual events. It was determined that the following entities would be needed to create the scenario.

Define in Detail all of the Key Players

To make the scenario realistic, key characters were named and details about them were recorded on a spreadsheet. Each key character was given a specific role designed for them in the scenario. In addition minor and characters who had little or nothing to do with the actual crimes where created to add depth and complexity to the scenario.

Create a Detailed Scenario

The CFRDC creative team next created and revised several drafts of a detailed scenario document. In these drafts details were added to the characters, organizations and the plot. Chris Hyde first reviewed these drafts and then Dr. Gary Gordon and Chet Hosmer added their feedback. During a half-day session Gordon, Hosmer, and Hyde finalized the draft of the scenario. This multi page detailed document was then written up over the next few days and was used to guide and plan the data generation (See Appendix B)

Define in Detail a list of Evidence Milestones

The final step of the scenario development was to develop a set of milestones. The milestone document contains a sequential list of predicted events that the investigators should follow to solve the case. We developed the list of goals or milestones for two reasons. The first reason was to create a guide to help us create evidence and organize that evidence for presentation during the event. The second reason was to provide a way to track investigators' progress during the event and to provide a "scorecard for post event analysis. (See Appendix C for complete milestone list.)

4.1.4 Data Generation

All data generation was performed at the Computer Forensics Research & Development Center at Utica College.

Define in Detail all Evidence Sources, Types, and Relationships

The first step of the data generation process was to define the sources and types of data that needed to be created. Once a general list of the types and sources of data was created we were able to define the relationships between the individual pieces of data. Once this was done we were able to create two categories of data. The two categories were time-sensitive data and non time-sensitive data.

Define Hardware/Software Requirements

We used the following hardware and software during CFX including the data generation and actual experiment.

Software Used

- Windows 98
- Windows NT Workstation
- Windows NT Server
- Microsoft SQL Server
- Linux
- NetMax (Linux based Internet Server/Firewall)
- Mail Again (Mail forwarding program developed inhouse)
- Microsoft Office
- SciFi
- Net4i
- Analyst Notebook
- Encase

Hardware Used

- 4 Acer
- 8 Microns
- 6 Dell
- 4 Gateway
- 2 Laptops
- (45) 15 GB Hard Drives
- White Board Projector Screen
- Image Master

Networking/Misc.

- 2 - 8 port switches
- 6 - 5 port hubs
- 6 – Extra NIC cards

Design Data Generation Network

In order to create the data in the most efficient and cost effective manner it was decided that each entity/organization would have an identical network setup. This decision allowed us to simulate a large number of computers using the limited number of computers to which we had access. We were able to accomplish this by switching out the hard drives on each of the computers when we needed to generate the data for a different

entity. To generate data and network traffic between two entities, we would set them both up at the same time on segregated network.

Create a Data Generation Plan

Based on the scenario, evidence list, time schedule, and network layout we were able to use Microsoft Project to generate a sequential list of tasks, which needed to be completed. The most important part of this process was to schedule in the time-sensitive events. The time-sensitive events were important because they relied on a time element i.e. Internet Mail which we could not manipulate. These time sensitive tasks were given highest priority and the non-sensitive tasks were scheduled around them.

Generate Cover Data

Cover data was generated using various methodologies including the following:

- Signing up scenario characters for email lists on Egroups. Using a real email address as a proxy and then randomly forwarding email to various users.
- Manually sending emails to different users.
- Using a spam program written in house to generate 2 million emails.
- Random web surfing.
- File downloading from the Internet and transfers between internal network computers.
- Placement on the computers of documents and programs.

Generate Actual Evidence

Actual data can be divided into three types: electronic document evidence, computer and network evidence, and physical evidence.

Electronic Document Evidence

- Banking records from ICU
- Banking records from the six US banks
- Banking records from the Belize Breeze Bank and Trust

Computer and Network Evidence

- Stephen Kellner's Hard Drive
  - Emails between Kellner and Lucky Lady Casino
  - Emails between Kellner and Taylor
- Christina Dennison's Hard Drive
  - Emails between Dennison and HJ
  - Emails between Dennison and Dex West
  - Hacking tools

- Dex West's Hard Drive
  - Emails between Dennison and Dex West
  - Hacking tools
  - Stego Tools

Physical Evidence

- Flight Data Strips

4.1.5 CFX Experiment

CFX 2000 was held on October 23rd, 24th, and 25th 2000 at the New York State Police Forensic Investigation Center (FIC) in Albany.

Day 1

      Day one was used primarily for set up and testing of equipment

Day 2

      Roles of Team
      Opening Briefing
      Separation into Teams
      Scenario Introduction
      Began Case Investigation

Day 3

      Completed Case Investigation
      Final Briefing for Observers
      Final Briefing for Investigators

5 Lessons Learned

5.1.1 CFX 2000

Upon completion of the experiment, the developers of the scenario, having acted as both active and passive participants, compiled their notes into the document that follows.

Resultant observations were grouped into four major headings:

- Development of the Scenario
- Use of Computer Forensic Tools
- Participants

- Recommendations for Future Experiments

Development of Scenario

The initial task of CFX 2000 was the development of a cybercrime scenario. This scenario created the involved entities, subjects, and the criminal activities under investigation. Evidence was produced that supported the scenario, and distributed to the investigative teams. Team members then performed the analysis, and the results of their investigation were based upon the team findings. Upon completion of the experiment, participants were queried as to their preconceived expectations of the experiment, if they had found the experiment challenging, and how they felt the experiment could be improved. This, coupled with the observations of the designers, provided us with insight as to future scenario development, and how the process may be improved.

A major issue with the CFX 2000 scenario was that it was extremely complex and multifaceted. The scenario incorporated many individuals, representing them as possible suspects, and several corporate and military entities, spread out over a large geographical area. The evidence consisted of many types of digital data files (databases, spreadsheets, emails, documents, etc.), existing on several pieces of physical media (hard drives, CDs, floppies). Individuals were designated as key characters in the scenario, and made available for interrogation as requested by the investigative team.

The mixing of law enforcement and military elements in the case proved to be problematic. It was found that the two entities have different interests and objectives when investigating a case, and while the scenario attempted to address the needs of both law enforcement and military analysts, the combination of both story lines confused many of the participants. These investigative approaches differ greatly. While law enforcement tends to investigate the more traditional crimes,[1] conducted postmortem (after the crimes have been committed), the military's main concern is tracking down "incidents" that have been identified on their systems as they occur.

The scenario proved to be very time consuming to develop, and not cost efficient in terms of man-hours. A large staff was assembled to create key elements and evidence for use within the scenario. Due to the complexity, data generation took a considerable amount of time to complete, and involved personnel from the Computer Forensic Research and Development Center (CFRDC) and Emergent, as well as several Utica College students.

In order to implement the complex scenario at the New York State Police's Forensic Investigation Center (FIC), a significant amount of equipment was dismantled at the CFRDC, and shipped to the FIC. This procedure took a significant amount of time. It was necessary to ensure proper documentation of the configuration of the systems, dismantle, tag, transport, and properly reassemble the equipment.

---

[1] Traditional crimes refer to crimes like child pornography, money laundering, etc

Due to the complexity of the scenario, it became apparent that there was not sufficient time available for the investigators to work the case, as well as solve it, during the course of CFX. Considerable help was provided to the investigative teams in order to steer them in the right direction, and approach completion.

The experiment was found to be difficult to manage, particularly while it was in progress. While some teams were proficient in certain areas, they needed a greater amount of assistance in other areas than did other teams. All of the teams did not make progress as quickly as anticipated. It would have helped to survey the participants prior to their attending CFX to ascertain their skill level and training. This would assist in selecting more balanced teams.

In order for the conclusions of an experiment to be valid, the results must be verifiable and repeatable. Again, because of the complex nature of this experiment, the conditions will not be easily replicated for future implementation in other testing environments.

Computer Forensic Tools: COTS, GOTS, and Development

The limited number of forensic tool developers participating in the experiment created some initial difficulties. This resulted in more reliance on COTS[2] /GOTS[3] tools. As a result, the participants were only able to become familiar with a limited number of new and cutting edge tools available in the cyber forensics field.

While several experiment participants were familiar with the available tools, others were not. Because the duration of the experiment was limited to three days, and much of this time was spent becoming familiar with the scenario and working the case, there was no time to train participants in the use of the different tools. This required the tool developers to provide significant assistance. Another problem was that some of the tools used during the analysis phase were not well suited for the developed scenario. Different forensic tools have particular strengths and weaknesses, and those that are most heavily relied upon were not the best choice for such a complex set of evidence.

It was also noted that law enforcement analysts tended to rely on those tools with which they were most familiar (e.g. Encase), rather than trying to familiarize themselves with new and unique tools. This tended to defeat the purpose of the experiment, which was to allow participants to use and evaluate other options.

Participants

The background of the participants varied greatly. Their positions/job descriptions included investigators, analysts, administrators and their guests, developers and program managers. The expertise of these participants ranged from the high level of sophistication and understanding of an analyst, to administrators with very little background in the field

---

[2] Commercial off the shelf
[3] Government off the shelf

of cyber forensics. Many had limited expertise in specific areas of investigation, such as money laundering, and bank practices, which were required for the scenario at hand.

Other than the Encase tool, the participants had limited knowledge of, or exposure to, different computer forensic tools.

Upon completion of the experiment, several participants, while being impressed with the scenario and the overall format of the experiment, did express a variety of unmet expectations. They had hoped to have more exposure to the computer forensic tools, more hands on experience with the tools, and they would have liked a sense of closure with the case.

Recommendations for Future Computer Forensics Experiments

This section gives recommendations, based on the lessons learned, for future computer forensics experiments.

Scenario

For the next computer forensics experiment, administrators should reduce the complexity of the scenario, and focus on more realistic scenarios. One suggestion is to have more than one scenario so that there can be closure and discussion. Administrators should devise scenarios not only to focus on realistic cases that law enforcement confronts, but also to showcase specific tools and the comparison of tools that purport to do similar functions.

Tools

The next experiment should provide a wider variety of greater number of development tools and more COTS/GOTS tools for comparison purposes. Training on all of the tools should be provided prior to the start of the experiment.

Participants

Teams involved in the experiment should be formed based on background, skill level, and current position of the participants. Roles of the various team members should also be defined prior to the start of the experiment. Team building should be included in the process. All of the attendees should be actively involved in the experiment.

Debriefing

Time should be provided for debriefing and discussion after each scenario. After the experiment is completed, participants should be interviewed to gather information about their feedback on the scenarios, tools, and the overall experience. Also, the contractors should provide a report that synthesizes the findings of the experiment, including post-experiment interviews. The attendees should receive copies of the report.

5.1.2 CFX II

While not part of the SOW, AFRL staff suggested that a review of CFX II would be useful in any planning of CFX III. CFX II differed greatly from CFX 2000 in format and goals. Instead of a case study that incorporated a wide range of tools, CFX II's approach combined informational/policy presentations with technology demonstrations by seven developers.

While CFX 2000 was held at the FIC in Albany, CFX II was split between two locations: SUNY Institute of Technology and the AFRL.

CFX-II Observations

A feedback session was held at CFX II. The following comments and suggestions are based on comments from the individuals at that session and from conversations with some of the software developers.

1. Demonstration time too short to truly understand what each technology or tool was able to do.
2. It would have been better if CFX II could have been held in one location.
3. More hands on experience like CFX 2000.
4. More exposure to the individual tools and some instruction on how to use them.
5. More realistic case studies. CFX 2000 was too complex and CFX II lacked case studies.
6. More tools showcased.

Recommendations

The general consensus is that CFX III should be a combination of CFX 2000 and CFX II. It would incorporate the best from both events including:

1. More detailed technology demonstrations followed by hands on instruction on how to use the tool.
   Scripted introductions (about one minute) would be useful to help the attendee decide whether they were interested in seeing more about the   tool, or if they should move on to the next. The scripted introduction should include: Nature of problem to be solved, Solution approach, Why the solution is novel, Expected payoff or improvement to current operations.

2. Mini cases that showcase individual tools or combinations of tools. These cases would be less complex than CFX 2000 and mirror real cases faced by law enforcement today.

3. Participants would like a take away CD with information on new technologies, case examples, and trial versions of tools if available.

6 Task 2 – Establish Standards and Criteria for Cyber Forensic Technologies

Webster's definition for the term "forensic" is "pertaining to, connected with or used in courts of law or public discussion and debate." Most traditional forensic disciplines (e.g., forensic pathology, forensic toxicology, forensic chemistry) have established standard processes and procedures that guide practitioners in the collection, preservation and transfer of forensic evidence to help guarantee that the integrity of such evidence is unimpeachable in the eyes of the court. Scholars like Noblett, Pollit and Presley (2000) point out that such standards are sadly missing from the field of computer forensics at a time when the demand for reliable computer forensic evidence is at its peak. The need for such standards is critical for the credibility of the field of computer forensics for it is inextricably tied to the ability of law enforcement and the victimized corporation to convincingly present logical conclusions based on this evidence. The success or failure of a computer crime case may ultimately rest with the level of trust the court has in the substantive merit of investigative procedures employed prior to the appearance of the evidence in the courtroom.

In situations in which traditional forensic evidence is presented in the courtroom, the court will use the accepted standards within the given discipline as a measuring stick by which the worth of the presented evidence can be judged. National or international associations typically establish these standards. These associations represent a virtual consensus, within the discipline, on the acceptable manner by which the evidence should be collected, preserved and transferred. Frequently, these standards are not exact, in that they offer some degree of latitude because of the broad concepts they present.

Unfortunately, associations that represent the interests of computer forensic practitioners have been hesitant to unveil recommended practices and procedures that would represent standards of some kind. The American Society of Crime Laboratory Directors (ASCLD) has no accreditation standards for computer forensics practitioners and the International Association of Computer Investigative Specialists (IACIS) only lists some guidelines that are made available to criminal investigators but not to corporate practitioners. The International Organization on Computer Evidence (IOCE), established in 1995, does offer some general principles for the handling of computer evidence. Likewise, the CERT Coordination Center has developed some similar guidelines.

The following information targeted for the computer forensics examiner represents an effort to glean the most consistent elements of the various existing guidelines and merge them with additional, updated material to form standard operating procedures for evidence collection, preservation and transportation. We have drawn upon other recent works from scholars in the field[4] to enhance the applicability of these standards.

---

[4] Stephenson, 2000; Holley, 1999; Noblett, Politt & Presley, 2001

Any developed standards for computer forensics should be led by certain agreed upon objectives. Such objectives must include the preservation of the unspoiled nature of the evidence and the ability to duplicate this evidence exactly for examination purposes. Holley's (1999) Cardinal Rules for computer forensic examination is a good starting point for this direction:

> *Never Work on the Original Evidence* – The primary reasons for this are quite simple. First, if the examiners modify hard drive data in an attempt to recover evidence, changes to the original may disallow it as evidence in court. Second, any changes that examiners must make to extract substantive details from the background (e.g., manipulation of digital pictures) may be permanent, requiring the use of a copy. Third, the use of copy(s) permits other entities to independently reproduce analysis results.

> *Never Trust the Subject's Operating System* – The key reason for this is because the computer criminal may have modified routine operating commands to perform destructive commands.

> *Document Everything* – To ensure evidence integrity, such documentation includes a description of: 1) everyone with physical access to the evidence; 2) who actually accessed the evidence and when it was accessed; 3) what software tools were used on the evidence and how they were used; and 4) the results of any searches conducted on the evidence.

These guides closely parallel the three general principles set forth by the IACIS to ensure that computer forensics evidence is not mishandled. These three principles are that:

1. *Forensically sterile examination media must be used*

2. *The examination must maintain the integrity of the original media*

3. *Printouts, copies of data and exhibits resulting from the examination must be properly marked, controlled and transmitted.*[5]

The following is a new standard operating procedure (SOP) that follows the lead offered by the above principles and rules of thumb. It is critical that the computer forensics examiner follow these standards, at a bare minimum, to ensure that evidence collected remains free from mere hint of taint.

Development of a Corporate SOP on Computer Forensic Evidence Collection, Examination and Analysis - Whatever the SOPs are for a given organization, the elements of the SOP must be clearly articulated and set down by management in a document form. Such SOPs must be preserved in this form as being representative of management's official position on maintaining the integrity of all computer forensic evidence. Due to the pace of technological advances in the computer technology field,

---

[5] IACIS, 2001

these SOPs should undergo internal review and revision to ensure they do not become outdated

Permanency of Case Notes/ Records – All handwritten notes must be in ink and changes/revisions must be initialed by the individual making the change/revision with date and reason for the alteration. Notes/records should be authenticated with digital signatures.

Documentation of Steps in Recovering Information – This should be done to avoid making impulsive decisions in recovery and to construct a record of steps taken to recover to be used for future reference.

Disconnecting of Compromised Systems From Network – As part of a stepwise process: 1) All compromised computers must be disconnected from the network, and; 2) Operate in single user mode in UNIX or as a local administrator in NT (this will protect the computer while engaged in the recovery process).

Regardless of the connection type (e.g., 10BaseT, thin net) the physical point of disconnection should be at the wall to permit proper documentation of the computer end.

Modem connections should be disconnected at the wall to avoid problems recalling the connections when documenting them.

Each connection should be tagged in a manner to permit accurate reassembly.

Imaging of the Compromised System - Prior to analyzing the intrusion, a duplicate image (e.g., a bitstream copy) of the system must be created which will be used for analysis purposes. The duplicate image should be transferred to a test computer upon which all analyses will be performed.

A second duplicate should be created to serve as an official documentation of the system in its original state.

The original system should never be used for analysis. Such an action could likely bring the integrity of the data into question.

A detailed description of the bitstream copying or imaging process used should be documented and preserved. Identification of the software and hardware used in the imaging should be included in the description.

The computer should only be booted from a known-good floppy disk (i.e., a disk that boots DOS, not Windows).

Examination of the Hard Disk – The following steps should be taken in conducting an effective examination of a computer hard disk drive (all steps should be documented in the event that there is a legal investigation):

Search for Any Alterations to Data, Software and Configuration Files.

Boot record data and user defined system configuration and operation command files should be examined and findings documented. Anomalies should be noted.

Check all system binaries against distribution media. Check binaries commonly replaced by Trojan Horses (e.g., telnet, login, su, netstat, fund, sync) and binaries referenced in critical network and system programs.

Check password files for unauthorized accounts.

Check the hard drive mirror for keywords related to the incident.

Check for new SUID and SGID files.

Check for unauthorized hidden shares with the "net share" command.

Check the "slack" area of each file for lost or hidden data.

Check the contents of all user data files in the root directory and each sub-directory.

<u>Collection of Evidence</u> – Depending on your original hypothesis on how the original intrusion occurred, evidence should be collected on any information that could help support or contradict that hypothesis. The following are procedures that should be performed as part of this evidence collection.

Search for tools and data that may have been left by the intruder. The primary intruder tools that should be checked include Trojan Horse programs, network sniffers, backdoors, vulnerability exploits, and tools that could be used to launch denial of service attacks. Regardless of what type of tool is used to search for intruder tools, it will be necessary to use a known clean copy of the tool employed.

<u>Review log files</u>. Reviewing of files should be conducted to help answer the question of "how" the computer was compromised. Possible log files to be reviewed could include:

•Messages log – Check anomalies and events occurring at the time of the intrusion;
•Xferlog – Check this log file to identify intruder tools uploaded and data downloaded;
•Utmp – By using the "who" command, one can check who is logged in;
•Wtmp – The "last" tool can be used to determine, in this log file, any suspicious connections from unauthorized hosts;
•Secure – Check for services that were accessed that are not commonly used.

Search for Network Sniffers. Check if any process has network interfaces in "promiscuous" mode. This could be evidence of a network sniffer. (Possible tools used for this purpose are cpm and ifstatus). Also check for log files that grow quickly in size.

If a sniffer is discovered, examine the output file from the sniffer to identify other computers at risk.

<u>Documentation and Preservation of Evidence</u> – Impound any physical evidence, such as handwritten notes, printouts, backup tapes, CR-ROMS that may be related to the intrusion.

All relevant equipment, cables, and connections must be labeled in a way to ensure ease in reconnection in the proper order.

Physical evidence must be collected and preserved using a proper chain of custody. Each piece of evidence must be preserved in a sealed envelope/evidence bag with a label containing, at a minimum, date, description of contents and identification number. Identification of those in the chain of custody who access the evidence must be clear (with signature) along with a recording of the date of access.

To ensure the integrity of computer files saved as evidence, they should be hashed using MD5 or SHA1 algorithms, these yielding a hexadecimal signature when run against a file. Any subsequent change to that file alters this hexadecimal signature. These hash values may also be used in the "known file filtering" process, which compares these newly created hash values to a database of hashes[6] created for known file types.[7] This comparison streamlines the investigative process, allowing the analyst to eliminate many types of files from further examination, as the hash value has identified it as a known file.

7   Concluding Remarks

The state-of-the-art of standards for key processes in cyber forensics has been articulated in this section. It is less mature than anticipated and will require much more debate and consensus building to approximate the other forensics areas. The process of developing standards for cyber forensics presented through this paper is, at once, utilitarian, evolutionary and iterative. The process is utilitarian in that it offers necessary standards that are within a realistic range of achievement for most cyber forensic investigative units. The process is evolutionary in that presently developed standards are the product of an understanding, appreciation and incorporation of the recent history of cyber forensics: lessons learned from both the successes and failures of past investigative methods. Finally, it is, by necessity, iterative in that it fuses insights from a host of diverse sources dedicated to producing the most logical guides to effective cyber forensic procedures. Adhering to these three principles of cyber forensic process development helps ensure that any standards developed are not static, but adaptable to changes in technology that affect cyber forensic procedures.

---

[6] One such database is NIST's National Software Reference Library.
[7] Application file types that are commonly found on hosts.

Based on this assessment, it would be premature to present anything but the best of breed standards to date. Designing standards in a vacuum would be counterproductive. Efforts are underway to test some of these standards in very specific and narrow aspects of cyber forensics. Considerable consensus building will be required before a cyber forensics standard requirements document can be written. It is hoped that the International Journal of Digital Evidence will be a key conduit in this process. An article in the first issue written by Carrie Whitcomb, National Center for Forensic Science, entitled, *An Historical Perspective of Digital Evidence: A Forensic Scientist's View,* begins this discussion.

8 References

Cert Coordination Center (2002). *Steps for Recovering From a UNIX or NT System Compromise*. Retrieved January 2002, from
http://www.cert.org/tech_tips/root_compromise.html

Haase, Norman (2001). *Computer Forensics: Introduction to Incident Response and Investigation of Windows NT/2000*. Retrieved January 2002, from
http://rr.sans.org/incident/comp_fornsics3.php

International Association of Computer Investigative Specialists (IACIS). (2001). *Forensic Examination Procedures*. Retrieved January 2002, from
http://www.cops.org/forensic_examination_procedures.htm

Kruse, Warren G. and Jay G. Heiser (2002). Computer Forensics: Incident Response Essentials. Indianapolis: Addison-Wesley.

National White Collar Crime Center (1999). *CyberCop 101 Training*. Morgantown, WV: National White Collar Crime Training and Research Institute.

Noblett, M. G., Pollitt, M. & Presley, L. (2000). Recovering and Examining Computer Forensic Evidence. *Forensic Science Communication*, Vol. 1, Num. 4. Retrieved June 2001, from http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm

Holley, J. O. (1999). Computer Forensics in the New Millennium. *SC Security Magazine*. Retrieved June 2001, from
http://www.scmagazine.com/scmagazine/1999_09/survey/survey.html

Pettinari, Dave (2000). *Procedures for Seizing Computers*. Retrieved December 2001, from http://www.crime-research.org/eng/library/procedures

Stephenson, Peter (2000). Investigating Computer-Related Crime. Boca Raton: CRC Press.

Stephenson, P. (2000). *Using Formal Methods for Forensic Analysis of Intrusion Events - A Preliminary Examination*. Retrieved January 2002, from
http://www.imfgroup.com/docs/wpapers/Using%20Formal%20Methods%20for%20Forensic%20Analysis%20of%20Intrusion%20Events.pdf

Upchurch, Jason (2001). *Combating Computer Crime*. Retrieved December 2001, from
http://rr.sans.org/incident/combat.php

9 Task 3 - Develop a Certification Process for Cyber Forensic Technologies

This task defines processes by which developers may acquire certification of their forensic technologies. A framework for the certification of forensic software tools and technologies will be developed.

10 Objective

The focus of this task is to create a formal process by which developers of digital forensic tools can acquire certification and/or validation of their digital forensic technologies.

The approach to *certification* is twofold:

- Tools can be certified to be safe to run in specific computer environments.

- Tools can be certified to provide admissible evidence if key processes are performed in a particular way.

In Task 2, a proposal for the standardization of the *key processes* within the cyber forensic discipline was outlined. While a "standard operating procedure" is an essential part of the puzzle, it only addresses one requirement within that puzzle. This task expands on the need for standardization by bringing specific requirements for tools into the equation, and further articulates the need for added layers of trust within the forensic process.

By defining a process by which digital forensic tools may be certified, an additional layer of credibility is added to the current practices of digital forensic examiners. If the operations the tools perform can be verified, the approaches taken by examiners can be further validated. Analysts and experts can present their findings in a court of law, bolstered by the fact that there is a set of legally sufficient standards in place upon which the courts can rely when determining the admissibility of the evidence.

11 Introduction

Throughout the 20th century, the role of criminal forensics grew to be an important factor in the criminal justice process. Evidence collected and preserved by forensic chemists, forensic pathologists, and forensic biologists emerged as indispensable to the successful outcome of criminal prosecutions. In many instances, such evidence formed the centerpiece of the criminal prosecutor's case, without which criminal charges may never

have been brought. While the types of forensic evidence (e.g., entomology evidence, toxicology evidence) can differ greatly, all disciplines of criminal forensics maintained, and still maintain, sets of rules and regulations that serve the function of validating relevant forensic processes toward establishing a certification for practitioners within the respective disciplines. The validation of forensic methodologies, tools and processes, always by a recognized expert organization or association, is important because it represents a "stamp of approval" that guarantees that applied procedures are conducted within acceptable parameters for accuracy, objectivity and reliability. It is the only way that criminal court judges can be confident of conclusions drawn from the evidence collected.

An example of how accepted validation processes has led to a formalized certification program in criminal forensics is the work of the American Society of Crime Lab Directors (ASCLD). The ASCLD has established a voluntary program to certify crime labs that engage in traditional criminal forensics. Certification includes proficiency testing and the development and maintenance of criteria that laboratory directors can use for self-evaluation and quality control. Labs must submit to periodic on-site reviews and inspections to ensure the continuation of ASCLD certification. In addition, the ASCLD offers the general public a means of identifying which labs have met the ASCLD standards (ASCLD, 2000). Such a thorough certification program instills a lasting sense of confidence in the evidentiary results generated from ASCLD-approved crime labs. Unfortunately, the ASCLD offers no certification program for computer forensics examiners or computer forensics labs, nor is there any other national entity that offers such a certification. Consequently, computer forensics lacks the last essential ingredient, beyond standards of operation and validation processes, which would elevate the discipline to the quality recognition enjoyed by the more traditional criminal forensics disciplines.

Some contend that the reason that the computer forensics discipline does not presently have a formal certification program is that computer forensics is hamstrung by certain characteristics inherent in the field.[8] Unlike other traditional forensic disciplines, computer forensics requires that examinations occur in locations other than a controlled laboratory environment, complicating efforts to establish protocol applicable to account for all possible settings (e.g., the crime scene itself, data processing departments). In addition, the individual conducting the computer forensics examination is not always at arms length from the actual investigation, as a forensic chemist would be, raising concerns of potential bias. Furthermore, computer forensics does not develop interpretive statements regarding the reliability of the data collected from an evidence sample, as is the case with the analysis of DNA evidence, but instead is centered on the flawless recovery of crime-related information from a much greater pool of diverse pieces of information. Finally, because computer forensic science is market driven, it must be able to adapt to technological innovations much more rapidly than in other forensics disciplines, affecting the recommendation of which forensic tools to use for which procedure and how those tools should be used.[9]

---

[8] Noblett, Pollitt and Presley, 2000
[9] Noblett, Pollitt and Presley, 2000; Holley, 1999

Despite the differences between computer forensics and other forensics disciplines, the expectations of results by criminal justice professionals remain the same for all forensics disciplines. Regardless of the forensics discipline, the evidentiary results must be derived from state-of the-art procedures that are peer-reviewed, regarded by the scientific community as sound and, thus, defensible in court. But an added burden is placed on the computer forensics examiner. While, forensics examiners in other disciplines must be concerned with the appropriate handling of physical items in their control, the computer forensics examiner must employ the use of tools and procedures that preserve the latent information contained in the physical items. Unfortunately, there are little or no standards on which to classify, and subsequently assess, the functionality of the different tools. Thus, tools that may be useful in one area of cyber forensics may not be relevant to or useful as an investigative tool within another area.

In the previous task (Task 2), a set of procedural standards that may be applied to the cyber forensic process has been documented. While these standards are not tool-centric, that is, they do not make recommendations of specific tools that should be implemented for a given procedure, the task does take some significant steps in providing the practitioner with a process upon which subsequent standards may be built.

Cyber forensics, like other forensic disciplines, has sub-disciplines. The sub-disciplines in the cyber forensics field include computer forensics, incident forensics, and network forensics. These are considered sub-disciplines because the techniques, skills and most notably, the tools required for operation within these various disciplines in a forensically sound manner are quite different.

Practitioners within each given sub-discipline currently conduct their investigations and analyses in a manner consistent with their personal knowledge of the platform or operating system. The tools and techniques available for the different platforms and systems vary greatly. Practitioners are often faced with using tools outside of the "mainstream" of current cyber forensic technologies. They may employ tools and utilities that have been designed for other purposes, but have features and capabilities useful in the forensic process. Some may author their own utilities, in the programming language with which they are most familiar. These practices threaten the integrity of the investigative process, as there is currently no infrastructure in place that allows the practitioner to validate or test the reliability of the tool.

While most legal challenges to digital evidence currently stem from the reliability of the audit trail (chain of custody) related to the evidence, it is only a matter of time before the tools themselves are attacked on various levels. Critical evidence may be excluded if it cannot be shown that the tools and techniques used to obtain the evidence operated as the analyst would have the court believe, that they could not alter the evidence in any way, and that they were used in a manner generally accepted by the community at large.

In the sections that follow, we will discuss several aspects that directly impact the cyber forensic process, as it applies to the use of the technological tools. Among these:

- Issues surrounding the admissibility of evidence;
- Current software certification programs;
- Efforts to validate cyber forensic technologies;

12 Examination of Certification Process in Other Areas of Forensics

To obtain a basic understanding of how certification of tools and technologies within each discipline is conducted, the following areas of practice were examined.

- Fingerprint Analysis;
- DNA Analysis;
- Ballistics.

These were selected as a focus because of the amount of attention they receive within the forensic community, and the amount of general interest by the media and by the population at large. However, the research shows that these areas of practice do not refer to a certification process for the tools or technologies applied during the forensic process. Instead, the focus appears to be on validation. Members of the forensic community refer to the practice of *validation* of tools, techniques and methodologies. The term *certification* is reserved for testing the proficiency of the individual practitioners, or for the certification of the laboratories in which analyses are conducted.

An appropriate authority, such a Scientific Working Group, provides the guidelines for conducting proficiency testing of individuals. "Their goals are to assist in the advancement of forensic science, and promote a commitment to excellence among the members of the forensic community. Proficiency testing is one of the key measures of performance."[10] By the same token, the American Society of Crime Lab Directors certifies forensic laboratories.[11]

Beyond that, acceptance of forensic practices, and the tools and methods they use when conducting forensic analysis has been shaped by community consensus, as well as within the legal arena. The forensic community relies upon organizations such as the American Academy of Forensic Sciences (AAFS), which provides members with information about conferences, seminars, meetings, workshops, training courses, symposiums, and professional journals.

The AAFS provides members with information pertaining to such topics as:

- Current practices

---

[10] SWGMAT, 2001
[11] See page 31 of this document for a discussion of Laboratory Accreditation.

- SOPs
- Guidelines
- Documentation
- Validation
- Qualification
- Issues
- Compliance
- Reporting

Practitioners are required to follow generally accepted practices within their field, and apply accepted tools and methods appropriately. These accepted practices are reached by consensus within the community through the resources mentioned above. The concepts of participation and continuing education are stressed within the membership, and active affiliation with such an organization further bolsters the credibility of the forensic practitioners.

Because the acceptance of current scientifically obtained forensic evidence is based upon its survivability in the courts, a brief discussion of the case law is provided.

12.1.1 Forensic Legal Issues

There are a variety of recognized forensic disciplines, aside from those mentioned earlier. These disciplines have recognized methodologies, techniques, and protocols developed through consensus within their field. These are provided to practitioners in the form of guidelines and procedural manuals, which are supported by a recognized body. Forensic practitioners adherence to the accepted approaches allows them to render a thorough, scientific, unbiased statement of fact to the court that is supported within the discipline.

Standards for Admissibility

Once evidence has been presented to the court, the process by which it was obtained must withstand the scrutiny of the presiding judge. Courts and judges rely upon case law to provide them with the guidance needed to accept evidence obtained by technological processes not previously accepted in courts.

Problems have arisen in courtrooms when information was presented that was seemingly difficult for a layperson to evaluate for its accuracy. Rules needed to be devised to decide whether scientific evidence ought to have legal weight.

United States v. Frye, 293 F. 1013 (D.C. Cir. 1921)[12]

The District of Columbia's Frye v. United States Court of Appeals ruling of 1923 was the original decision used as a guideline for the admissibility of scientific evidence in courts. In this case, the defense counsel tried to present as evidence the results obtained from a

---

[12] http://www.law.harvard.edu/publications/evidenceiii/cases/frye.htm

27

device that measured blood pressure levels during interrogation of a suspect (the forerunner to the polygraph).

The court decided that the 'technology' on which the expert's testimony is based must be "sufficiently established to have gained general acceptance in the particular field in which it belongs." It was also necessary that the testimony be beyond the general knowledge of the jury. This Frye standard became general practice in most courts and continued to influence decisions for many years. It precluded the need for courts to hold evidentiary hearings about the scientific evidence itself.

However, critics claimed that the Frye standard excluded theories that were unique, but still supported by evidence. In 1975, the Federal Rules of Evidence went into effect. Rule 702 of the Federal Rules of Evidence states: "If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training or education, may testify thereto in the form of an opinion or otherwise." But the application of these standards varied greatly within the courts system.

In 1993, the Frye standard was superceded, in many jurisdictions, by the Daubert decision.

Daubert v. Merrell Dow Pharmaceuticals, 113 S. Ct. 2786 (1993)

This decision gave the judge much more discretion in determining the admissibility of scientific evidence. The focus was placed more on the process used to obtain the findings than on the results. "The focus must be solely on principles and methodology, not on the conclusions they generate" [13]

The Daubert decision stated that the Federal Rules of Evidence superseded the "general acceptance" guidelines for admissibility of novel scientific evidence. The "general acceptance" test, which arose from Frye, is at odds with the liberal ideas put forth in the Federal Rules of Evidence concerning opinions of expert witnesses, the basis and the content of their testimony. Rule 702 states:[14]

> "If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case."

---

[13] http://www.law.harvard.edu/publications/evidenceiii/cases/daubert.htm
[14] Article VII. See http://www.law.cornell.edu/rules/fre/overview.html

While the trial judge must still screen scientific evidence to ensure it is relevant and reliable, his focus must be solely on the principles and methodology incorporated in the forensic process, not on the conclusions that are generated.

Factors the courts must now consider include:

- General acceptance within the scientific community;
- Peer review;
- Relevancy to the issue at hand;
- Testing and validation of the theory;
- Potential error rate (if known).

It is the last two points that incorporate scientific acceptance of forensic evidence into the evaluation process. Not only must the procedures be documented, and widely accepted by the forensic community, but the results must be verifiable, and repeatable. Along with this is the notion that, as a scientific procedure, the procedure has been implemented enough times as to supply statistics related to errors in the process (e.g. false negatives).

These cases point to a notable change in the climate surrounding the issue of admissible scientific forensic evidence. Expert testimony, and the accompanying evidence, have been rejected when it was found lacking in standards, if the quality of the equipment was found to be suspect, or the conditions under which the evidence was collected vary so much as to have a significant impact on the procedure. The same standard goes for the knowledge and skill of the analyst/expert.

This means that where there appears to be no sufficient scientific basis for bringing the results into court, or where forensic experts within the same field apply different result criteria in their analysis, evidence will be not be accepted that lacks a level of reliability.

13 Software Certification Authorities

In order to identify, and possibly adopt for our purposes, a general approach for *Cyber Forensic Software Certification Guidelines*, a review of several entities promoting the concept of software certification was conducted. Included in this section is a sampling of entities currently involved in specific aspects of software certification. The major function of these entities is to provide assurance to potential consumers of the software the product may be relied upon to a designated "degree of trustworthiness."

This sampling is not all-inclusive. There are many more entities that conduct software certification, both publicly, as a commercial service, and privately, as internal assurance.

International Common Criteria
"The Common Criteria represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the international community."[15] They provide a common set of requirements for security software as an assurance scale, known as Evaluation Assurance Levels. This is used to indicate different levels of confidence in *security* products. The purpose of their evaluation and certification scheme is to aid consumers in selecting a software security product that will best fit their requirements, needs and available resources.

The Center for National Software Studies
This consortium is studying the concept of certification of software's "trustworthiness," and the dependent parameters. "The mission of the CNSS is to elevate software to the National agenda, and to provide objective expertise, studies, and recommendations on National software issues."[16] They are currently assessing the added value of software implemented in national infrastructures, and the trustworthiness of such implementations for interoperability and fault tolerance.

TruSecure (formerly International Computer Security Association)
TruSecure's ICSA certification approach involves testing, and attempting to subsequently break implemented security approaches, such as firewalls, intrusion detection, and anti-virus software. It is a for-profit software certification authority that uses industry consensus building as a basis testing. They certify that specific known problems are not present in the applicant's system. As an example, their firewall certification program is based on the input of industry representatives who meet periodically to decide what known problems should be checked for.[17]

13.1.1 Approaches to Software Certification

Certifications of software focus upon specific elements of the software's operation.

- Usability;
- Interoperability with other components;
- Conformity with similarly operating applications;
- Source code analysis.

1) Usability (a.k.a. COTS-worthiness[18])
This is a core component of most software certifications. The certifying authority assesses the tool from the perspective of how easily the product may be installed and implemented by the consumer of this product. Items such as the graphical interface, automated functions, the user's manual, and technical support, are evaluated, and the product is graded on this basis.

---

[15] http://www.commoncriteria.org/
[16] http://www.cnsoftware.org/
[17] http://www.trusecure.com/html/secsol/certification.shtml
[18] Yacoub , Mili, Kaveri, & Dehlin, 2000

2) Interoperability with other components

This approach to certification assumes the software product will be used in conjunction with or as a component of a large, complex application environment. Potential consumers of such component products are concerned that the software component may not operate reliably when used in a certain way. The consumer wants assurances that the new component will not create an unstable environment for the other components it is intended to support.

3) Conformity with similarly operating applications

This criterion is what the security-based software authorities are currently operating under. These authorities install the software within a 'test bed' that is applicable to the particular classifications of the security software product. It is then judged by how it performs and reacts to circumstances within this testing environment. Products achieve certification when they pass, by a certain percentage, the rigorous tests set up by the authority.

4) Source code analysis

This approach to certification relates to the open source movement, where application developers freely release the source code of their applications for independent evaluation and scrutiny. One example of this would be the 100% Pure Java Certification Program, intended to evaluate applications to be conformant with the Java APIs.

13.1.2 Assessment

Unfortunately, these approaches to software certification do not fit well with the notion of certification of cyber forensic technologies.

1) Cyber forensic analysts are not, and should not, be concerned with the usability of a forensic tool. Cyber forensic science is not intended to be a user-friendly discipline. Dependence on easy to use graphical interfaces and point and click functionality only serves to undermine the credibility of the analyst, who must be aware of the underlying functionality of the tools he uses in order to support his reason for using them when called upon to do so.

2) Forensic applications are not currently intended for incorporation as a component of a larger system of interoperable software components.[19]

3) Software certification of security-based applications focuses upon assessing the *reactive* nature of security applications (e.g. given this tool, does it react/respond to the given scenario as would be expected?). Security tools are judged within specific taxonomies of tools, the results based upon their capabilities of handling taxonomy-specific scenarios.

---

[19] While tools are and continue to be developed independently, it is hoped that, in the future, tools may be developed in such a way as to be interchangeable components within a forensic infrastructure.

Conversely, software forensic tools are *active* tools, operated by and assisting the analyst to automate several small tasks for him. Unlike reactive tools, there is no finite set of tests that may be performed on or by the tools to prove they are effective. Each function of a forensic toolkit works independently of the others, and produces different output. The analyst then manually assimilates the data for analysis.[20]

Analysts currently employ a wide variety of software tools for forensic purposes, whether they were intended as forensic tools or not. They perform a variety of single and/or multitude functions, sometimes as part of an integrated forensic application, but most often, as an independently operating utility that is utilized by the analyst to address a specific need or set of circumstances. Given this, the concept of conformity testing is not a practical approach.

4) Source code analysis is not possible for many cyber forensic applications. Developers of forensic applications, commercial, government and otherwise, are not likely to be releasing the source code for their applications, as they wish to protect both the current and future commerciality of their tools. Additionally, governmentally developed tools have traditionally been black box applications, useful, but not available for public scrutiny.

These models assume the evaluation of similar operating, high-end applications/products in a manner that will provide potential consumers of such products with information that is independent of the vendor, paid endorsers, current customers, etc. (the Consumer Reports of security products). Because of the cost of these software solutions,[21] vendors are willing to submit their products, for a fee, to these authorities to give consumers added confidence in the capabilities of their products.

Software certification authorities evaluate products from a wholly different perspective than that required for forensic technologies. Their methodologies do not fit the needs of the cyber forensic community.

14 Certification Practices for Forensic Software Tools & Methodologies

Currently, formal efforts in the cyber forensic discipline are focused upon the development of testing methodologies for selected categories of forensic software, with an eye on the subsequent validation of forensic software tools. Informal efforts involve loosely organized forums where digital forensic practitioners share independently developed methodologies and test results, seeking the validation of their practices by other participants in the forum. Certification of existing technologies is not conducted within the digital forensic discipline.

---

[20] Certifying that the tool is operated as expected; identifying, analyzing, and/or eliminating all possible evidence, would be heavily dependent on the proficiency of the analyst, and dependent upon his expertise.
[21] Cost of a single ID system can run into the tens of thousands of dollars, and more.

Validation of digital forensic software tools is a necessary function, providing practitioners with a legally sufficient basis to justify continued use of a particular technology. But, it is only the first of many steps toward the ultimate goal of certification of cyber forensic technologies.

14.1.1 Formal Efforts

National Institute of Standards and Technology (NIST)

NIST provides a forum for conducting projects through the collaboration of practitioners and other interested parties and agencies. NIST has attempted to apply their expertise in the field of testing of tool conformance to a field that has, to date, no recognized standards. Current NIST projects related to cyber forensic technologies are:

- Computer Forensic Tool Testing.
- National Software Reference Library.

Computer Forensics Tools Testing (CFTT)[22]

This project involves the development of a testing program that encompasses the development of the methodologies, processes, and precise tests, for software tools used in the investigations of computer-related crimes, the aim being the production of valid results. The overall objective of the CFTT effort is to enhance the admissibility of electronic forensic evidence, by verifying the performance of commercially available computer forensic software through rigorously applied testing, and establishing minimum performance standards for the software.

NIST generally follows these steps in its computer forensic tool testing process:[23]

- Start with All Possible Tools
- Classify Tools (according to major functions)
- Select the Most Useful Feature(s) of Tool
- Acquire and Install the Tool
- Note difficulties
- Become familiar with the Tool
- Test the Tool and Verify the Results
- Report Findings

These steps are the logical progression that would apply to the testing of any software application. NIST has acknowledged that forensic software tools do present a unique set of problems. "The development of a test methodology was complicated by the lack of standards or specifications that describe what forensic tools should do, and the need for

---

[22] http://www.cftt.nist.gov/
[23] Higgins, 2001

these tools to survive the scrutiny of a judicial process."[24] Conformity testing models are difficult to develop and implement in a field in which standards are still evolving.

Because there are no current standards, they have decided to abide by the International Organization for Standards (ISO) 17025,[25] which has a provision for cases where there is no standard test method. It is suggested that the results of each step will be made available for public review, so that this process is an open, public process, which incorporates and reflects the needs of a wide variety of entities.

Currently, **Disk Imaging** and **Write-Blocking** tools are the only classes of tools that have had testing requirements developed and published.

In their document entitled "Disk Imaging Tool Specification"[26] (October 12, 2001), NIST has laid out the criteria for testing disk imaging tools, those tools that are used by the forensic analyst for copying evidentiary digital media (analysts are required to maintain the integrity of the original evidentiary media, so a copy is produced upon which further analysis is conducted). The document lists assertions and requirements that must be observed in the application of the disk imaging tool testing. The draft "Hard Disk Write Block Tool Specification"[27] (May 1, 2001) does the same for forensic write-blocking tools.

While these documents are an invaluable resource for outlining the approach that must be taken in validating disk imaging and write-blocking tools, it would be difficult to apply the same approach to other types of forensic tools. The distinction is that the sole function of disk imaging and write-blocking tools is to assist in the *collection* of the data from the evidentiary media, operating independently of the contents of the media they are enlisted to copy.

The differences in disk-imaging testing criteria are based solely upon the hardware and BIOS differences between the forensic platform and the evidentiary system. While this may be a very long list, encompassing all possible configuration combinations, the list is finite. Subsequent forensic analysis, and the applicable tools, is dependent upon the operating system, file system, and resident applications present on the evidentiary system.

As an addendum to NIST's CFTT, they have recently released the Forensic Software Testing Support Tools (FS-TST), which is "a package of programs that can be used to support testing of disk imaging tools used in computer forensic examinations."[28] At this

---

[24] NIST's CFTT, 2001
[25] An international standard that contains all of the requirements that testing and calibration laboratories have to meet if they wish to demonstrate that they operate a quality system, are technically competent, and are able to generate technically valid results.
[26] http://www.cftt.nist.gov/DI-spec-3-1-6.doc
[27] http://www.cftt.nist.gov/WB-spec-assert-1-may-02.doc
[28] From the Readme.txt document included in the current release located at http://www.cftt.nist.gov/Fs-tst10.zip

time, the software package is provided with little support or documentation, but design notes and a user manual are forthcoming.[29]

National Software Reference Library (NSRL)[30]

This NIST project, while not directly related to forensic tool testing, is a project relevant to the field of cyber forensics. Its purpose is to provide a repository of 'signatures'[31] of known software applications. By processing commercially available software applications and operating systems, using one or more hashing algorithms, unique identification signatures are produced for each application. The analyst then uses these signatures to perform "known file filtering" functions. The current collection of signatures is stored in the NSRL as Reference Data Sets, for use by investigators and in legal proceedings.

14.1.2 Informal Efforts

Currently, validation of independently developed forensic utilities[32] is sporadically conducted, and typically performed by an interested individual in the field. The resulting documentation provides guidelines for other interested parties to build upon. But, this validation is not necessarily reliable.

Some developers release limited numbers of their tools for Beta testing to other forensic practitioners (SMART,[33] as an example). These practitioners perform their own testing and evaluation independently, using their own methodologies, under less than rigorous standards. They share their findings with the community of other interested practitioners, and allow others to verify and confirm their findings.

The Computer Forensic Tool Testing Group is an informal forum where forensic practitioners can share information and findings related to a variety of tools currently used for forensic applications. "The group is for discussing and coordinating computer forensics tool testing. Testing methodologies will be discussed, as well as the results of testing various tools. The ultimate goal of these tests is to ensure that tools used by computer forensics examiners are providing accurate and complete results." [34]

While participants in the group are among the foremost researchers and practitioners in the field of cyber forensics, the approaches to testing the tools and the methodologies employed are not formally established for or by the group. The existence of this forum would tend to support the ISO 17025 provision mentioned earlier. It would also support

---

[29] http://ois.nist.gov/nistpubs/technipubs/forthcoming/search.cfm?dbibid=11420
[30] http://www.nsrl.nist.gov/
[31] Hash values created by several algorithms
[32] Many forensic practitioners write their own utilities for specific purposes, usually because they have encountered something within the course of their analysis for which no applicable software exists. This approach leaves the performance of these small, independent utilities open to question and a potential challenge by defense attorneys as to the integrity of the output of these applications.
[33] Storage Media Archival and Recovery Toolkit. http://www.asrdata.com/smart.html
[34] http://groups.yahoo.com/group/cftt/

the legal requirements set out by the Daubert rule, that the scientific techniques employed by the forensic analyst be generally accepted within the community of practitioners.

15 Issues with 'Certification' of Forensic Software

One:
The term "certification", as it applies to software, implies placing a stamp of approval on a product that has been rigorously tested with an exhaustive set of all known variables that may be applied to that particular classification of tool, testing for flaws in the implementation of the tool that would make that tool less than effective in its performance. While this is a useful function for software implemented for purposes of security within a given environment, this approach may not be possible for tools that are used as analysis tools.

An analysis tool is used within environments where there may be no pre-existing knowledge of what will be encountered. How is it possible to *certify* that the tool will identify, to a degree of certainty, all idiosyncrasies within a system? (As an example, a pathologist conducting an autopsy may screen for a standard, limited set of common toxins, but in conducting this limited screen, miss the actual cause of death, as the toxin may be of a more exotic type not normally encountered)

Two:
Certifying that a tool will run safely within a certain computer environment may be of interest to certain parties, and useful for verifying the claims made by the tool's author. But, owing to the continually evolving nature of contemporary computing environments, and the infinite number of possible configurations of a system, this type of certification may only serve to create a challenge by defense attorneys if this tool was run in an environment other than those that it has been certified for operation.

Current environmental testing of software applications are provided for certain software application to ensure that the implementation of the tool itself within the existing configuration of the system will not create more problems than it is intended to prevent (e.g. a firewall product that creates a buffer overflow vulnerability).

Three:
Certification of a software product is typically performed on commercial products for the purpose of perspective purchasers' assurance. Vendors submit their products, for a fee, to the certification authority in order to obtain the certification. Because of the nature and cost of these software products, a fee-based approach is viable. It is a substantial investment on the part of the consumer for such products and associated technical support.

Four:

Many forensic practitioners use tools that, while not specifically designed for use in the forensic process, have been adopted for use in the forensic process, because they have a function that analysts have found useful during certain phases of the analysis. An example of this may be a password cracking application. While not forensic tools per say, they are a class of tool often employed by the examiner within a forensic analysis. The strict use of only certified forensic tools would prohibit analysts from using these types of applications.

A related topic involves the commercial forensic tool Encase, which provides users with a proprietary scripting language known as Escript. Practitioners using the Encase tool are encouraged to author small scripts that provide additional functionality to the Encase tool suite. They then may share these scripts with other users on the Encase website.[35]

Additionally, utilities that are native to a particular operating system are commonly used during a typical forensic analysis (such as Linux dd). The question here is whether the certification authority is required to certify the functionality of system utilities that have already been proven for use by the community of forensic analysts.

Five:
A handful of commercially available forensic tools are in actuality "tool suites," meaning that they provide many functionalities/capabilities to the forensic analyst. While some of these suites are actually separately functioning utilities that are executed independently of each other (and thus may be tested and certified individually, on their own merit), several tools are now available that are integrated suites of tools, functioning parallel to and dependent on each other in order to perform their operations in an efficient and timely fashion.

A problem arises when the certification authority is tasked with evaluating and certifying these integrated suites of tools. How does one evaluate the functions of the tools separately from one another, especially when some of those functions are dependent upon the output of other functions? And, what happens when certain functions of the tool are found acceptable, but others are found lacking? Is the tool then 'partially' certified?

Six:
Certification of a software tool leaves the certifying agency open to the possibility of legal action if that tool does not perform as would be expected after a certification has been awarded.

Seven:
Getting developers to submit their existing or newly developed tools for such certification may pose a significant problem. There are already several tools that are widely used and trusted within the forensic community. The developers of these tools would have no significant reason to submit their products for certification, as they have general acceptance in courts of law. And, because development of new forensic tools is not likely

---

[35] http://www.guidancesoftware.com/html/escript_library.htm

to be of any financial benefit to developers, they have no compelling reason to go through a costly certification process.

The current criterion is "general acceptance" in the community of forensic analysis. (The Fry or Daubert rules) While a certification may bolster the Fry or Daubert rules, it is not a necessity.

Eight:
Generally, a certification, or lack of one, would only serve to create more grounds with which to legally challenge the use of a tool than it would serve to justify the use of it.

Nine:
Most certification schemes assess and evaluate whether the software is operating as it is *designed* to run, independent of overt human interaction (other than installation/configuration). Upon installation, the software operates within an acceptable range of performance. Forensic software cannot be certified in such a way. It is interactive, responding to the commands of the user. The user then further interprets the results, and the user again, performs subsequent actions.

16 Approaches to Digital Forensic Software Certification

Digital forensics is that discipline where law enforcement and computer science intersect. Practitioners of digital forensics may be either law enforcement officers that have been specially trained in the analysis of digital evidence, or computer scientists that have taken an interest in the collection and analysis of computer and network based evidence, and are now familiar with and adhere to the laws of evidence.

While they bring different perspectives to the table, the goal is the same: to produce digital evidence that will withstand the skepticism and scrutiny of today's court system.

In order to satisfy both disciplines involved in the digital forensic process, and advance it as both a legally recognized forensic practice and a science, a two-pronged approach relating to the use of technology should be taken; the *validation* of digital forensic technologies within the community, for legal sufficiency; and the *certification* of digital forensic technologies, in order to ensure the veracity of tools employed during the scientific process.

While some of the requirements of the separate prongs, or "tracks," are unique to that track, some intersect and/or compliment the other track. As this is the case, they should be developed in parallel, so as not to waste time and resources that would benefit both avenues.

The discussion that follows will focus upon the certification prong, but will introduce elements of validation where appropriate, as it would be beneficial to keep the two perspectives from loosing site of each other.

In order to establish a formal certification procedure for digital forensic applications, an infrastructure must be in place that can reliably support the needs of the digital forensic discipline.

Current needs include:

- Development of the principles for the classification of digital forensic tools;
- Development of the standard processes that may be applied to digital forensic tools for purposes of testing;
- Development and construction of the testing environment (test bed);
- Digital Forensic Testing Laboratory Accreditation;

In February 2002, at the meeting of the American Academy of Forensic Sciences (AAFS)[36], the area of Forensic Computer Science was recognized, and included as a subcategory within their listing of generally accepted forensic sciences. While this is a significant step in the acceptance of digital forensics as a forensic science, the draft standards requirements for acceptance in this organization do not address the needs outlined above.

The first requirement, the development of the principles for the classification of digital forensic tools, may be approached in several ways.

- Tools may be classified according to the general category of cyber forensics in which they would be most useful, these general categories being computer, incident, or network forensics. The tools may then be further subdivided into collection, preservation, extraction, analysis, organization and reporting. Other subcategories may be added where necessary.
- Tools may be classified according to operating system, and further subdivided into more specific categories. One example of this classification would be "TUCOFS – The Ultimate Collection of Forensic Software."[37]
- The tools may be classified according to the specific operation they perform, and then further subdivided as to the specific operating system(s). Integrated forensic tool suites would be included within multiple classifications.

Currently, there is no consensus as to the proper classification of digital forensic tools.

The second requirement, the development of the standard processes that may be applied to digital forensic tools for purposes of testing, would ultimately be dependent on the classification scheme. General areas for evaluation may include, but not be limited to:

---

[36] The AAFS is a professional society dedicated to the application of science to the law.
[37] http://www.tucofs.com/tucofs/tucofs.asp?mode=mainmenu

- Accuracy
- Performance
- Speed
- Documentation
- Support
- Platform requirements/limitations

Basic testing requirements would include:

- A controlled environment
- Thorough documentation
- Verifiable results
- Repeatability

Again, refinements in the process would be based upon forensic tool taxonomies.

Third, the development and construction of the testing environment(s) (test beds), is quite problematic, and widely debated within the digital forensic community at this time. There is much disagreement as to what would be a "representative test environment." The virtually unlimited number of system configurations (hardware, operating system, and software) makes this a huge challenge. There will need to be several such testing environments, but what they should be comprised of will be open to debate for some time to come.

The last major requirement is for the establishment of *accredited* laboratories that have the resources (personnel[38], hardware, software, etc.) to perform the independent evaluation of tools and technologies, providing testing, validation, and subsequent certification, of digital forensic technologies.

16.1.1 Laboratory Accreditation

---

[38] Laboratory accreditation also requires the certification of key personnel within the discipline.

There are two approaches to laboratory accreditation that meet the needs of the digital forensic community. The first, the NVLAP's approach to accreditation, would most closely adhere to the needs of a laboratory established exclusively for the testing, and subsequent *certification*, of specific technologies. These types of accredited laboratories adhere to detailed testing techniques and methodologies, applying them to the individual classification of technologies.

The second, the ASCLD/LAB's accreditation program most closely satisfies the requirements of *validation* of digital forensic practices and technologies. Once accredited laboratories are established, and utilize specific digital forensic technologies, the legal requirement of general acceptance within the discipline becomes more solidified.

NVLAP Accreditation

"The National Institute of Standards and Technology (NIST) administers the National Voluntary Laboratory Accreditation Program (NVLAP)[39]. NVLAP is comprised of a series of laboratory accreditation programs (LAPs), which are established on the basis of requests and demonstrated need. Each LAP includes specific calibration and/or test standards, and related methods and protocols, assembled to satisfy the unique needs for accreditation in a field of testing or calibration. NVLAP accredits public and private laboratories based on evaluation of their technical qualifications and competence to carry out specific calibrations or tests."[40]

Accredited laboratories demonstrate compliance with the National Voluntary Laboratory Accreditation Program (NVLAP) for satisfactory compliance with criteria established in Title 15, Part 285 Code of Federal Regulations. These criteria encompass the requirements of ISO/IEC Guide 25, and the relevant requirements of ISO 9002 (ANSI/ASQC Q92-1987) as suppliers of calibration or test results.

Currently, the NVLAP accredits laboratories in only two areas of information technology; Common Criteria Testing (IT security) and Cryptographic Modules Testing. Both areas relate to 'conformity,' a term that cannot currently be applied to most digital forensic technologies.

While the general model (general laboratory requirements, practices, and procedures) provided by NVLAP may assist in the establishment of laboratories for forensic tool testing and subsequent certification, at this time the NVLAP only accredits labs within a limited range of practices, all narrowly defined, and none having to do with forensic expertise or testing of tools that are in a field as divergent as cyber forensics.

ASCLD/LAB Accreditation

The American Society of Crime Lab Directors (ASCLD) currently accredits labs and examiners in eight forensic disciplines.

---

[39] http://ts.nist.gov/ts/htdocs/210/214/214.htm
[40] NVLAP Program Summary

- Controlled substances
- Toxicology
- Trace evidence
- Serology
- Biology (DNA)
- Firearms/tool marks
- Questioned documents
- Latent prints

"The Crime Laboratory Accreditation Program, established by the American Society of Crime Laboratory Directors (ASCLD), is a voluntary program in which any crime laboratory may participate to demonstrate that its management, operations, personnel, procedures, equipment, physical plant, security, and health and safety procedures meet established standards. The program is managed by the American Society of Crime Laboratory Directors, Laboratory Accreditation Board (ASCLD/LAB) which is responsible to the Delegate Assembly composed of the directors of all accredited laboratories."[41]

According to the ASCLD's website, the Laboratory Accreditation Board has adopted four accreditation objectives that define the purposes and nature of the program. They are:[42]

- To improve the quality of laboratory services provided to the criminal justice system;
- To develop and maintain criteria which can be used by a laboratory to assess its level of performance and to strengthen its operation;
- To provide an independent, impartial and objective system by which laboratories can benefit from a total operational review;
- To offer to the general public and to users of laboratory services a means of identifying those laboratories which have demonstrated that they meet established standards.

The established standards for personnel in each of the forensic disciplines includes a requirement that examiners have a good understanding of the principles, uses and limitations of the instruments, and the methods and procedures used in their discipline. Examiners must have special knowledge in their functional area.

Quality standards are in place for other forensic disciplines. These standards must be met in order for laboratories to obtain accreditation in those areas. Currently, the ASCLD does not have an accreditation process for computer forensics labs. But, according to the ASCLD/LAB's March newsletter, the Scientific Working Group on Digital Evidence (SWGDE) has developed a draft set of accreditation standards and criteria, and submitted

---

[41] http://www.ascld.org
[42] http://www.ascld.org

it for approval as part of the process in becoming a recognized discipline of the ASCLD/LAB.[43]

16.1.2 Affiliation with a Related Facility

One possible approach to the placement of such a facility may be to associate the practice of validation with an accredited laboratory, such as the Department of Defense Computer Forensic Laboratory (DCFL), or a Regional Computer Forensic Laboratory (RCFL). Not only will this give a validation service more credibility, it will provide a pool of expertise from which to draw on for any given circumstance.

The accredited laboratory approach to validation, and subsequent certification, would assure that the proper resources are available to conduct credible analysis of methodologies, and provide validation. The laboratory technicians would already have the proper credentials/certifications, leading to the assumption that the laboratory can provide authoritative analysis. And, as an independently operating facility, product bias could be minimized or eliminated, as affiliation with the laboratory would eliminate the supposition of affiliation with a specific developer.

16.1.3 Forensic Experts Peer Review

While the accreditation of forensic computer science laboratories is the ultimate goal, it would be beneficial to set up an intermediary authority until such time as this goal can be realized. One such intermediary authority would be a review panel of cyber forensic experts that oversees the validation and certification processes. By establishing a forensic panel of qualified, independent cyber forensic practitioners to conduct validation of forensic software, it is possible to meet the Daubert standard for peer review and acceptability in forensic sciences.

One such group in existence, The Forensic Panel, is a "peer reviewed forensic expert consultation practice."[44] Their method of examining scientific questions ensures the integrity of an objective examination. They maintain that their "conclusions reflect the state of the art of the pertinent science."[45] Their objective is "to conform to new standards of admissibility and to enhance the integrity of forensic testimony in the court."[46] While the areas of expertise of this particular Forensic Panel are limited to Psychiatry, Psychology, Neuropsychology and Toxicology, the basic model is one that could be followed in establishing a similarly functioning Forensic Panel for cyber forensic practitioners.

For the purposes of cyber forensic application, peer review, as well as expert testimony review, can be provided by a respected collection of cyber forensic scientists and practitioners, providing the level of scientific certainty that the courts require.

---

[43] http://www.ascld-lab.org/pdf/2002MarchNewsletter.pdf
[44] http://www.forensicpanel.com
[45] ibid.
[46] ibid.

Participation may be solicited from the cyber forensic community, with applicants holding a position of respect within the community, and as a prerequisite, a certification from an approved agency/entity. Further admission requirements may include rigorous testing, and validation of background, references, and credentials.[47]

Results of the review process would be released to the cyber forensic community in the form of a newsletter or professional journal, such as the International Journal of Digital Evidence, as an additional way to promote cyber forensic standards and awareness of current progress in the field.

17 Forensic Software Validation

NIST was found to be the only authoritative entity that provides an approach to cyber forensic software evaluation. Restating their steps:[48]

1. Start with the 'Universe' of Tools
2. Classification of Tools (functionality of methods/procedures)
3. Select the Most Useful Tools within each Classification
4. Acquire and Install the Tools
5. Note difficulties
6. Familiarization with the Tools
7. Test the Tool, and Verify the Results
8. Report Findings

The researchers felt that the above steps needed further elaboration, and offer the following.

1. All tools that are currently used for, or may have functionality useful to, the cyber forensic analysis are compiled and documented.
2. The tools are then separated according to the functionality that is most useful within the forensic analysis. While this step would at first glance appear rudimentary, it is actually quite complex, as, to date, no entity has created a set of classifications in which to logically group individual tools. Tools that are used for the investigation of "traditional" crimes will not be in the same general classification as those used to investigate "non-traditional" crimes,[49] and must be separated accordingly.
3. The initial selection of the most useful tools is an arbitrary process, and not well defined at this point. Usefulness of an individual tool or set of tools will vary from user to user, especially when analysts use different operating

---

[47] See "Admission to the Panel." http://www.forensicpanel.com/aboutus/admissions/index.htm
[48] Higgins, et. al.
[49] Traditional crimes, and the associated evidence, are those crimes that, while now having the computer as an additional source of evidence, have been addressed by statutory law for quite some time. Conversely, non-traditional crimes are those that the advent of computing technologies has served to create.

systems from which to conduct their investigations. This step also appears to exclude tools that, while initially deemed "not useful", may have features beneficial to certain aspects of the process.

4. Acquisition and installation of the tool is operating system dependent, and the tools will have to be subdivided accordingly.
5. Difficulty during installation will be noted, as this data may play a role in the later selection of the tool by analysts.
6. The designated authority will, after installation, become familiar with the proper usage of the tool, noting the command and switch options (if command line), or options that can be implemented while navigating within the GUI environment.
7. The approach taken for tool testing will vary greatly from tool to tool. Utilities that have only a single function will have to be tested on a variety of media, to ensure that they operate as purported. Multiple functioning utilities/tool suites will be problematic, as all functions of the tool must be tested separately.
8. Findings will be documented and presented to the validation/certification authority, and subsequently released to the cyber forensic community.

While the following model incorporates the basic premises of the NIST model, we have expanded it to incorporate additional elements that would support a certification process for those technologies identified within the testing phase of being worthy.

```
                    ┌─────────────────────────────┐
                    │ Certification of Computer   │
                    │ Forensics                   │
                    │ Software Tools & Methods     │
                    └─────────────────────────────┘

┌─────────────────────────┐              ┌─────────────────────────┐
│ Universe –              │              │ Testing to              │
│ Identify Tools & Methods │─────────────▶│ Verify Results          │
└─────────────────────────┘              └─────────────────────────┘
           │                                         │
           ▼                                         ▼
┌─────────────────────────┐              ┌─────────────────────────┐
│ Classification –         │              │ Report Findings to       │
│ Functionality           │              │ Certifying Organization  │
│ of Method/Procedures    │              │ (CO)                    │
└─────────────────────────┘              └─────────────────────────┘
           │                                         │
           ▼                                         ▼
┌─────────────────────────┐              ┌─────────────────────────┐
│ Determine Right Tools    │              │ Designated CO –          │
│ For Each Classification  │              │ DCFL – DoD, NIST – LE/PS │
└─────────────────────────┘              └─────────────────────────┘
           │                                         │
           ▼                                         ▼
┌─────────────────────────┐              ┌─────────────────────────┐
│ Identify Certification   │              │ Certifying Tools &       │
│ Labs & Examiners         │              │ Methods                  │
└─────────────────────────┘              └─────────────────────────┘
           │                                         │
           ▼                                         ▼
┌─────────────────────────┐              ┌─────────────────────────┐
│ Acquisition             │              │ Certifying Analysts      │
│ & Installation          │              │                         │
└─────────────────────────┘              └─────────────────────────┘
           │
           ▼
┌─────────────────────────┐
│ Familiarization         │──────────────┘
└─────────────────────────┘
```

Notable changes to the original model include a provision for the identification of accredited laboratories and examiners to conduct the initial testing of the forensic software tools. NIST is currently focused on the creation of a methodology and framework for tool testing, but they have not yet identified the facilities within which these tests will be conducted, or by whom. This step will require a community consensus as to an acceptable facility.

18 Certification Summary

Cyber forensic science is in its infancy. It continues to grow and change, evolving to address the challenges created as computing technologies are developed. And, the discipline will continue to seek better alternative methods that will expedite the process.

The courts demand that forensic science and technologies, as well as statistical findings, be proved accurate, with the results being reproducible.

Not only is there a need for a formal, standardized process for the application of cyber forensic science, but there is a need for a formal accreditation of computer forensic laboratories in which such tool testing and validation would be performed. Without an

infrastructure in place that can perform this task, a certification/validation process cannot be properly implemented.

The American Academy of Forensic Sciences has only recently accepted Forensic Computer Science as a valid area of forensics. There is now the need for the creation of a board or academy to oversee/coordinate/steer the direction of cyber forensics as a science.

Increased research and training facilities are needed for cyber forensic science if it is to grow and keep up with demand.

Recognized facilities must be established that provide the resources needed by practitioners in order to coordinate their activities, and provide the forum for the general consensus within the field that courts currently demand.

Through this infrastructure, the standards can then evolve that support a framework for a validation, and subsequent certification, of cyber forensic methods and technologies.

19 References

American Society of Crime Laboratory Directors. http://www.ascld.org

Fisher, G. E. (2001). Computer Forensics Guidance. *ITL Bulletin*. Retrieved December 2001, from the Computer Forensics Tool Testing (CFTT) Project Web Site: http://www.cftt.nist.gov/itlbulletin.html

Hayes, J. (1999). Buyer Beware: Who Certified Your Software Certifier? *International Software Assurance Certification Conference*. Retrieved November 2001, from http://www.isacc.com/isacc99/presentations/hayes.html

Hervey, G. (2002). Assessing Liability for Software Failure. *Software Risk Management,* Vol. 2, No. 1. Retrieved January 2002 from http://www.srmmagazine.com/issues/2002-01/liability.html

Higgins, K. (2001, July). *Bringing Cybercrime into the Forensic Arena*. Retrieved from the National Law Enforcement Training Center website: http://www.nlectc.org/nlectcse/download/higgins_cybercrime.ppt

High Confidence Software and Systems Coordinating Group, Interagency Working Group on Information Technology Research and Development. (2001). *High Confidence Software and Systems Research Needs*. Retrieved January 2002, from http://www.ccic.gov/pubs/index.html

Holley, J. O. (1999). Computer Forensics in the New Millennium. *SC Security Magazine*. Retrieved June 2001, from http://www.scmagazine.com/scmagazine/1999_09/survey/survey.html

National Institute of Standards and Technology (NIST), Computer Forensics Tool Testing (CFTT) project. (2001). *Disk Imaging Tool Specification*, version 3.1.6. Retrieved from http://www.cftt.nist.gov/DI-spec-3-1-6.doc

National Institute of Standards and Technology (NIST), Computer Forensics Tool Testing (CFTT) project. (2001). *General Test Methodology for Computer Forensic Tools*. Retrieved November 2001, from http://www.cftt.nist.gov/Test%20Methodology%207.doc

Noblett, M. G., Pollitt, M. & Presley, L. (2000). Recovering and Examining Computer Forensic Evidence. *Forensic Science Communication*, Vol. 1, Num. 4. Retrieved June 2001, from http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm

Scientific Working Group for Materials Analysis (SWGMAT). (2001). Trace Evidence Proficiency Testing Guidelines. *Forensic Science Communications*. Retrieved December 2001, from http://www.fbi.gov/hq/lab/fsc/backissu/july2001/swgmat.htm

Voas, J. (1997). *A Defensive Approach to Certifying COTS Software*. Retrieved November 2001, from the Cigital website: http://www.cigital.com/papers/download/specialcots.pdf

Voas, J. (1997). *A Recipe for Certifying High Assurance Software.* Retrieved November 2001, from the Cigital website: http://www.cigital.com/papers/download/higha.pdf

Voas, J. (1998). *Software Certification Laboratories?* Retrieved November 2001, from the Cigital website: http://www.cigital.com/papers/download/crosstalk98.pdf

Voas, J. (2000). *User Participation-Based Software Certification*. Retrieved November 2001, from the Cigital website: http://www.cigital.com/presentations/eurovav99/

Wallace, D. (1999). Software Verification &Validation's Role Toward Software Certification. *International Software Assurance Certification Conference*. Retrieved November 2001, from http://www.isacc.com/isacc99/presentations/wallace/

Walls, T.J., Shah, V., & Ghosh, A. (2000). Towards Certifying Software for Security. *International Software Assurance Certification Conference*. Retrieved November 2001, from http://www.isacc.com/isacc2000/presentations/3c-vs/

Yacoub , S., Mili, A., Kaveri, C., & Dehlin, M. (2000). A Hierarchical Model for Developing COTS Certification Criteria. *COTS Workshop*. Retrieved December 2001, from http://wwwsel.iit.nrc.ca/projects/cots/icse2000wkshp/Papers/20.pdf

Yacoub , S., Mili, A., Kaveri, C., & Dehlin, M. (2000). A Hierarchy of COTS Certification Criteria. *The COTS Certification Project*. Retrieved December 2001, from http://www.csee.wvu.edu/COTS-Criteria/

20 Task 4: Define the Cyber Forensic Information Analysis Center (CFIAC) Charter

21 Objectives

The purpose of this task is to establish the structure and long term operational plan for a CFIAC.

Research issues to be investigated include:

- Study current Information Analysis Centers in areas related to cyber forensics.

- Based on the research results of Tasks 1-3, determine if there is a need for a CFIAC.

- Based on the results of the first two points, propose a design for a CFIAC.

22 Introduction

Currently, there is no central repository of information or clearinghouse dedicated to cyber forensics and digital evidence.[50] With the proliferation of cyber crime, there has been a rapid increase of information in the areas of cyber crime, cyber forensics, and digital evidence. Coupled with the information explosion is a growing need for a variety of research services. This is the reason an Information Analysis Center (IAC) dedicated to the cyber forensics field is worth considering at this time.

The following section describes the background of IACs, what the concept of an IAC is, and what services they provide. Also, this section lists IACs that are chartered by the DoD, and the military, and describes what services these organizations offer and who might use them.

23 Background

IAC stands for Information Analysis Center. An IAC is an organization that consists of individuals who assist subscribers in finding, analyzing, and using information that they desire. "IACs are formal organizations chartered by the DoD to facilitate utilization of

---

[50] A few web sites, such as Zeno's Forensics Site (http://forensic.to/forensic.html), provide links to information in these fields.

existing scientific and technical information."[51] The subscriber uses the services of an IAC to provide him with the information he is seeking. For example, if a subscriber is looking for information on the greenhouse effect and global climate change, he might visit the CDIAC, or Carbon Dioxide Information Analysis Center. IACs exist for various types of information.

The DTIC, Defense Technical Information Center is an organization developed by the DoD to oversee other DoD organizations and make sure they are up-to-date with current challenges faced. This organization, which has been an element of the Defense Information Systems Agency (DISA) since January 1998, "Continues to provide access to and facilitate the exchange of scientific and technical information (STI), thereby contributing to the management and conduct of Defense research, development, and acquisition efforts."[52]

The DoD decides which IACs they want to sponsor/form. Therefore, the only organization that can start a DoD IAC is the DoD. These IACs arise after it is shown that there is a need for an IAC in a specific area of interest. Once it is found that there is a need for a particular IAC, and the DoD announces their desire to start this particular IAC, various organizations propose their interest in running the IAC.[53]

IACs tend to focus on very wide areas of information. When information relative to an IAC is requested, the IAC will narrow its focus to that particular request, and obtain the information necessary to complete the request.

An example of a working IAC is the Weapon Systems Technology Information Analysis Center (WSTIAC). The WSTIAC has approximately six thousand users of their services and products. The WSTIAC is currently working on twenty-four tasks that range from one thousand dollars to billions of dollars. Most of the tasks are year long to multi-year long contracts. This IAC has about one hundred personnel involved, with twelve part-time personnel working on core programs, and the rest of the personnel working on funded tasks. Subscribers fund the work that they request, while the DoD funds the rest of the activities performed by the WSTIAC.[54]

The DTIC is responsible for the DoD's IACs. The DoD and the military sponsor various IACs. The ***DOD*** sponsored IACs include the following.

- AMPTIAC – Advanced Materials & Processes Technology IAC
- CBIAC – Chemical Warfare/Chemical & Biological Defense IAC
- CPIA – Chemical Propulsion Information Agency
- DACS – Data & Analysis Center for Software
- HSIAC – Human Systems IAC
- IATAC – Information Assurance Technology Analysis Center

---

[51] Dean, 2001
[52] DoD IAC, 2002
[53] Kitchens, 2002
[54] Kitchens, 2002

- IRIA – Infrared IAC
- MSIAC – Modeling & Simulation IAC
- MTIAC – Manufacturing Technology IAC
- NTIAC – Nondestructive Testing IAC
- RAC – Reliability Analysis Center
- SURVIAC – Survivability/Vulnerability IAC
- WSTIAC – Weapons Systems Technology Information Analysis Center

The *military* sponsored IACs are listed here.

- APMIAC – Airfields, Pavements, & Mobility IAC
- CEIAC – Coastal Engineering Defense IAC
- CRSTIAC – Cold Regions Science & Technology IAC
- CTIAC – Concrete Technology IAC
- DTRIAC – Defense Threat Reduction IAC
- EIAC – Environmental IAC
- HEIAC – Hydraulic Engineering IAC
- SAVIAC – Shock & Vibration IAC
- SMIAC – Soil Mechanics IAC

Most of the DTIC's information collection relates to defense research. As shown by the IACs above, the DoD's interests are widespread and information is collected in other various areas that include:[55]

- Biology;
- Chemistry;
- Energy;
- Environmental Sciences;
- Oceanography;
- Computer Sciences;
- Sociology;
- Logistics, and;
- Human Factors Engineering.

24 Services Provided

The mission of an IAC is, "To improve the productivity of researchers, engineers, and program managers in the research, development, and acquisition communities by collecting, analyzing, synthesizing, and disseminating worldwide scientific and technical

---

[55] DoD IAC, 2002

information in clearly defined, specialized fields or subject areas. The secondary mission is to promote standardization within their respective fields."[56]

While both missions are equally important, it is the secondary mission that is critical to the emerging cyber forensic community. The establishment of an IAC for the cyber forensic sciences will promote the standardizations needed within the field. The necessity for clear standards is supported by the research findings in Tasks 2 and 3.

These missions are accomplished by, "Providing in-depth analysis services and creating products. IACs respond to technical inquiries; prepare state-of-the-art reports, handbooks, and data books; perform technology assessments; and support exchanges of information among scientists, engineers, and practitioners of various disciplines within the scope of the IAC."[57] As a catchall phrase, "IACs provide easy access to essential, timely information."[58] An IAC is ready to perform the tasks, and/or research that they are presented with in their respected areas of interest.

The DTIC also lists four strategic goals that their IACs hope to obtain. These goals are:[59]

- Goal 1: Provide excellent customer service.
- Goal 2: Make access to information easy.
- Goal 3: Promote the use of information to enhance decision-making and leverage of the technology base.
- Goal 4: Promote excellence in Human Resources.

25 Possible Subscribers

Subscribers might want to use the services of an IAC if they fall into one of the following categories:[60]

- Are short-staffed;
- Need analysis of large quantities of available information in a particular subject area;
- Want to ensure that any previous research is considered in their design;
- Are beginning to work on a new system and looking for applicable information from analogous systems;
- Need to establish contact with leading researchers and scientists in a particular field.

---

[56] DoD IAC, 2002

[57] DoD IAC, et. al.

[58] Dean, et. al.

[59] DoD IAC, et.al.

[60] DoD IAC, et. Al.

26 Cyber Forensics Related IACs

One of the objectives in this task was to study current Information Analysis Centers in areas related to cyber forensics. The only two that appeared to have related missions were the DACS - Data & Analysis Center for Software, and the IATAC - Information Assurance Technology Analysis Center. Of the two, only the IATAC provides information in the area of cyber forensics.

When the two IACs were contacted via e-mail, both were unable to provide any information about their cyber forensic work. The DACS stated that they are performing work in the areas of defensive information warfare and information hiding. They are not currently involved with work in the area of digital forensics, but do anticipate it in the future.[61]

The IATAC stated that they have several staff members who work full time on cyber forensics issues for the Department of Defense. However, their work is classified so they are not able to release information to non-registered individuals.[62]

26.1.1 DACS - Data & Analysis Center for Software

"The DACS is a central distribution hub for software technology information sources." This IAC provides state-of-the-art information on current computer software technology for the software community. This organization is mainly concerned with software technology and software engineering. "The DACS offers a wide-variety of technical services designed to support the development, testing, validation, and transitioning of software engineering technology."[63]

The DACS provides information in some of the following areas.

- Software Process Improvement
- Formal Methods
- Non-Ada to Ada Conversion
- Study of Software Management
- Analysis of Two Formal Methods: VDM and Z
- Analyzing Quantitative Data Through the Web
- Artificial Neural Networks Technology
- COTS Based Software Development and Integration
- Mining Software Engineering Data
- Modern Empirical Cost and Schedule Estimation Tools
- Object-Oriented Database Management Systems

---

[61] Snell, Dan ("personnel communication," January, 2002)
[62] Abraham, Usher ("personnel communication," January, 2002)
[63] http://iac.dtic.mil/dacs/

- Present Value of Software Maintenance
- Software Design Methods
- Software Engineering Baselines
- Software Interoperability
- Software Prototyping and Requirements Engineering
- Technology Transfer Across the Internet
- Understanding and Improving Technology Transfer in Software Engineering
- Using Defect Tracking to Improve Software Quality

The DACS offers services such these.

- Bibliographic Services
- Databases & Datasets
- Technical Reports
- DACS Document CD
- Software Tech News
- DACS Software Tools
- Product and Service Brochures

26.1.2 IATAC - Information Assurance Technology Analysis Center

The IATAC's mission is to "Provide the DoD a central point of access for information on Information Assurance emerging technologies in system vulnerabilities, research and development, models, and analysis to support the development and implementation of effective defense against Information Warfare attacks."[64] This organization is a source of valuable information relating to Information Assurance and most importantly information on present and emerging vulnerabilities that could plague companies.

The IATAC provides information in the following areas.

- Biometrics
- Certification & Accreditation
- Computer Forensics
- Computer Network Defense
- Data Embedding
- Defense Information Operations
- Firewalls
- Information & Infrastructure Assurance
- Intrusion Detection
- Information Operations (IO)
- IO War game/Exercise Development
- Malicious Code Detection
- Operations Security

---

[64] http://iac.dtic.mil/iatac/help_desk/contact_us.htm

- Penetration Testing
- Public Key Infrastructure
- Steganography
- Virtual Private Networks
- Vulnerability Assessment

The IATAC offers the following services.

- Basic Inquiry
- Extended Inquiry
- Search and Summary
- Review and Analysis
- Technical Area Tasks (TATs)
- Training Courses/Workshops
- Conference/Event Planning
- Subscription Accounts

After studying these IACs, it is clear that cyber forensics is not a top priority, and that only one tangentially addresses cyber forensics.

27 Cyber Forensic Information Analysis Center (CFIAC)

This section describes a potential CFIAC model that would incorporate the best characteristics of the IACs studied. The need for an IAC or similar organization solely focused on cyber forensics is articulated. The organizational structure including the services provided, who might benefit from these services, and the design of the CFIAC are discussed in detail.

27.1.1 Need

An important objective in this task was to determine if there is a need for a CFIAC. The following section expresses this need, as well as gives examples of instances where this organization would be of value to subscribers.

Cyber crime is an area that is growing very rapidly. With the proliferation of computer use in the 20th and 21st centuries, cyber crimes have risen substantially. However, the resources of the organizations charged with investigating these crimes and the skill level of the investigators have not evolved as quickly.

Growing caseloads, increasingly complex cases, and the lack of sufficient numbers of trained personnel have plagued law enforcement and office of special investigations. Additionally, the need for new tools and methods, combined with the growing legal demands for scientific standards, validation, and certification, require a much more

sophisticated approach. It is difficult now for experts in this field to keep up with the rapidly growing information in this area, and it will be almost impossible as the field expands. A CFIAC can fill this gap and provide the most current information available to key decision makers and investigators.

A law enforcement official might use the services of a CFIAC to gain information to aid in an ongoing case. For example if the analysis indicated the use of steganography and the officer was not familiar with investigating it, he could contact the CFIAC for support. Depending on the officer's need, the information could include what steganography is, data hiding tools and methods, how to conduct an investigation where steganography has been utilized, and tools used to detect it.

Another example of the need for a CFIAC would come from the legal community. A lawyer who is prosecuting a cyber crime case might want to retrieve information related to his particular case. In most complex economic crime and computer crime cases, prosecutors must rely on subject matter experts to provide information on how the crime was perpetrated, how to uncover evidence, and how to present that to a judge and jury. They would be able to request some of this information from a CFIAC.

27.1.2 Services Provided

A CFIAC would provide information on cyber forensics tools, methods, processes, research, and development. The information would not only include computer forensics, but incident forensics, and network forensics.

The CFIAC would provide information on various tools used, standards, and steps taken in the four major categories of cyber forensics, which include:

- Collection and Preservation;
- Extraction;
- Examination, and;
- Organization.

In order to catch the offenders, an investigator must be aware of the tools and methods used by these criminals. Therefore, not only would the CFIAC provide information about forensic/investigative tools, it would provide subscribers with information about hacking/offender tools. If an investigator wanted to know first hand information about descriptions, uses, detection, or even evidentiary value of these tools, the CFIAC would provide him with it.

Services offered by a CFIAC would include:

- Inquiries (Research Services);
- Reviews and Analysis, and;
- Conference Information/News and Events.

Products offered would include:

- Technical Reports;
- White Papers;
- Cyber Forensic Tool Reviews and Assessments;
- Cyber Forensic Tool Database;
- Certification and Validation Status Reports;
- Case Studies for Training, Testing, and Education Purposes;
- Education Opportunities;
- Bibliography of Cyber Forensics Information, and;
- International Journal of Digital Evidence.

Resources offered would include:

- Links to related sites;
- For DoD inquiries, links to other IAC sites;
- Links to tool vendor sites;
- Links to commercial sites, and;
- Links to academic sites.

The cost of the services completed by the CFIAC would be based on the amount of time it would take to complete the task(s). The prices would range from free services to large grants. Free services would include questions answered over the phone or e-mail and simple research tasks that take minimal time. Large grants would range from in-depth technical reports, to tool testing and assessments that would be month to year-long contracts.

27.1.3 Possible Subscribers

A CFIAC would be available to any legitimate organizations seeking information related to the cyber forensics field. In order for this to be possible, the CFIAC would need to be a non-DoD organization that had close links to the DoD, possibly through a Cooperative Research & Development Agreement (CRADA). The potential subscriber base would include:

- Government Organizations;
- Law Enforcement;
- Military;
- DoD;
- Legal Community;
- Corporate Community, and;
- Academic Institutions.

However, subscribers of the CFIAC would have to go through a registration and vetting process before they were eligible to request and receive information.

27.1.4 Design

An objective in this task was to propose a design for a CFIAC. The following section suggests a way to utilize the CFIAC in order to fulfill the best interests of all entities involved.

Initially, the CFIAC could function as a clearinghouse of cyber forensics information. This would provide a significant service to those working and doing research in the area of cyber forensics. Through the clearinghouse, the CFIAC reputation as a center for information, research, and evaluation would begin to evolve.

A small staff would be required in the early stages of this IAC, increasing as the business of the CFIAC grows. In addition to full-time staff members, part-time employees/interns/ students would be used for various tasks. Using interns and students for tasks would not only provide them with great opportunities for hands-on experience with cyber forensics tool and methods, but it would make the staffing costs significantly less.

27.1.5 Funding

A local non-DoD organization should host the CFIAC. The funding could come from an annual grant from the AFRL and NIJ. This grant would cover the setting up a CFIAC and provide seed money for many of the research projects. Fee based services and products would generate funds to cover cost of expansion, equipment, and staff. Routine services would be funded by grants and provided free of charge to government organizations, law enforcement agencies, and faculty and students.

28 Recommendations

Based on the research in Task 4, it is our recommendation that a CFIAC, or an organization similar to an IAC, must be developed in the area of cyber forensics. The Air Force Research Lab is in a unique position to provide leadership and help make a CFIAC a reality in Central New York. Such a venture would increase jobs in the Mohawk Valley in the cyber forensics area and keep other jurisdictions from developing this concept and expertise.

An entity like the Computer Forensics Research and Development Center (CFRDC) at Utica College could function as the Cyber Forensics Information Analysis Center (CFIAC). This would allow information to be distributed to many entities rather than just the DoD. The CFRDC is in a unique position as it can work directly with law enforcement, has a strong relationship with the AFRL through a CRDA, has significant corporate connectivity through its relationship with the Economic Crime Investigation Institute (ECII), and is a recognized educational leader in this area.

29 References

Dean, Lon, R. (2001). Information Analysis Center (IAC) Program Overview. *Software Tech News*. Vol. 4, No. 2. Retrieved December 2001, from http://www.dacs.dtic.mil/awareness/newsletters/stn4-2/stn4-2.pdf

Department of Defense Information Analysis Center (DoD IAC). (2002). *IAC Mission*. Retrieved January 2002, from http://iac.dtic.m il/framesets/resources_2.htm

Department of Defense Information Analysis Center (DoD IAC). (2002). *What are IACs?* Retrieved January 2002, from http://iac.dtic.mil/1_about/about_iacs.htm

Department of Defense Information Analysis Center (DoD IAC). (2002). *What is DTIC?* Retrieved January 2002, from http://iac.dtic.mil/1_about/about_dtic.htm

Kitchens, W. (2002) Director of the Weapon Systems Technology Information Analysis Center. Telephone interview.

30 Task 5 - Publish a quarterly cyber forensics journal

The CFRDC will produce a quarterly journal in the area of cyber forensics. This will provide a venue to publish results of current and future research in the area of cyber forensics. This will include establishing an editorial staff, hosting the journal on a web site, and the solicitation of articles for the first year.

31 History

The need for an online peer reviewed scholarly journal in the area of cyber forensics has been discussed in several forums and mentioned in grant reports over the last three years. Chet Hosmer and Gary Gordon first addressed this in the Forensic Information Warfare Study in 1998. John Leeson and Gary Palmer led discussions regarding such a journal at the DFRWS held in Utica in August 2000. Numerous other individuals have also stated that if the cyber forensics is to develop into a scientific and legally recognized area of forensics that a scholarly journal is critical.

In order to meet the objectives of Task 5, Gary Gordon entered into conversations with all the advocates for such a journal. TRACES was renamed the International Journal of Digital Evidence (IJDE) to better characterize the mission of the journal. An editorial board has been formed to represent the individuals and organizations that have been advocates of a journal in this area. The editorial board represents individuals from academe, military, government, law enforcement, and industry. In addition, a list of peer reviewers is in the process of being established. These individuals are subject matter experts who can augment the experts on the editorial board or in some case can provide expertise not current found on the board.

Key information on IJDE:

1. Published online quarterly. The first Issue 1 Volume 1 was made available at the end of March 2002. Issue 1 Volume 2 will be published in June 2002. The remaining issues will appear in September and December 2002.
2. Hosted at www.ijde.org. The web site was developed by Trainor Interactive/Arachnomedia in New Hartford, NY. A number of web sites will point to the Journal. Some of these include www.ecii.edu, www.ncfs.org, www.utica.edu, www.wetstonetech.com, www.dfrws.org,
3. Solicitation of articles for the June, September, and December issues is currently in progress. Solicitation has occurred through personal contacts, listservs, and organization mailing lists, such as DFRWS. Individuals who present at the DFRWS will have the option of submitting their presentation for inclusion in the IJDE.

4. Information on the www.ijde.org web site includes About IJDE, Editorial Board, Current Issue, Archives, Author Instructions, Contact Information, and Related Links.

Screen shot of home page of www.ijde.org.
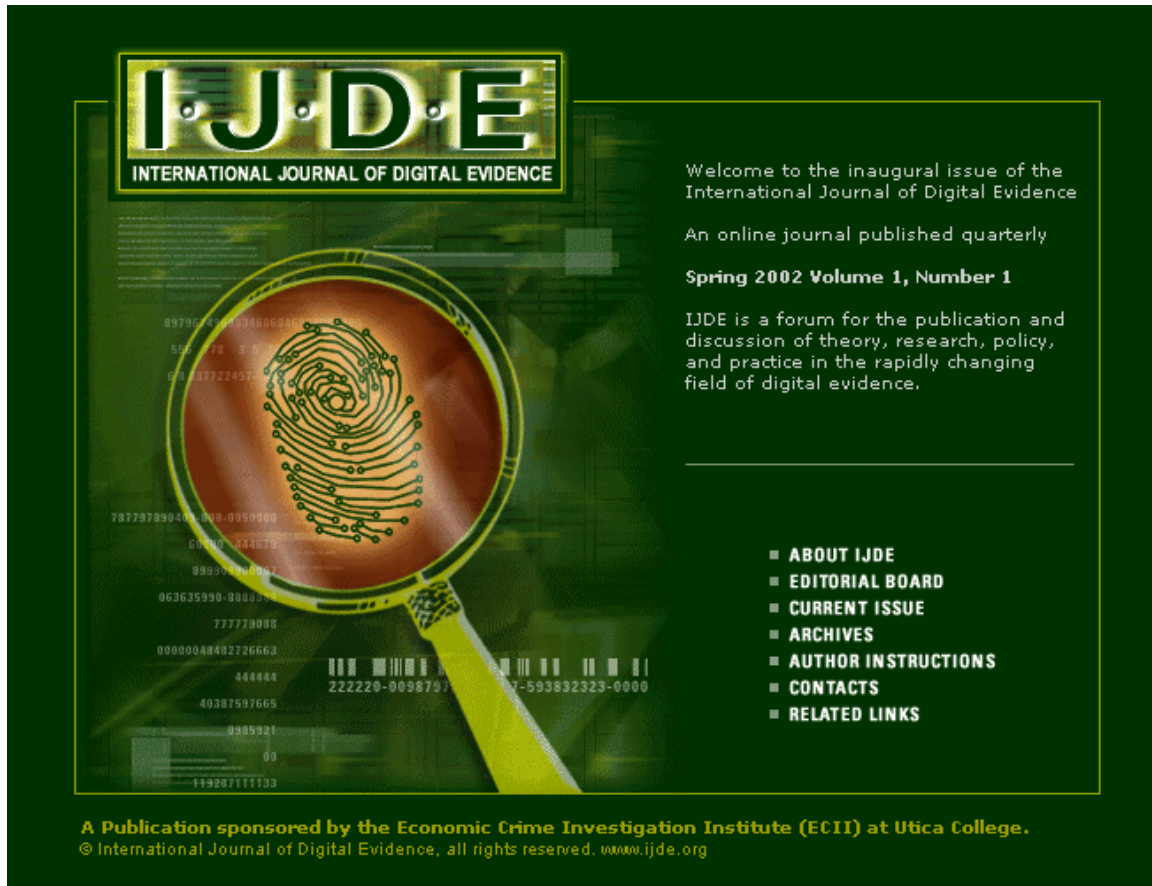
The following pages provide the information behind the links on the navigation bar including: About IJDE, Editorial Board, Current Issue, Archives, Author Instructions, Contacts, and Related Links.

31.1.1 About IJDE

International Journal of Digital Evidence (IJDE) is a forum for discussion of theory, research, policy, and practice in the rapidly changing field of digital evidence.

IJDE is supported by two organizations at Utica College in Utica, New York: the Economic Crime Investigation Institute (ECII) and Computer Forensics Research and Development Center (CFRDC). The editor is Gary R. Gordon, Ed.D., who is the Executive Director of the ECII, the Director of the CFRDC, and Professor of Economic Crime Management. The associate editor is John Leeson, Ph.D. Associate Professor of Computer Science, University of Central Florida and Assistant Director, National Center for Forensic Science. Dr. Leeson is also certified as a computer forensic examiner by the International Association of Computer Investigative Specialists.

The need for a journal such as this has been discussed in several forums and mentioned in grant reports over the last three years. The Editorial Board represents many of the organizations and individuals who have argued for a journal in the field of digital evidence. In order for the Journal to be successful, it must be embraced by the key contributors in this field. In that spirit, we welcome offers of support, including article submission, peer reviewers, and constructive comments.

Initial funding for IJDE has been provided by two sources: a grant (F30602-01-1-0506) from the Air Force Research Lab Information Directorate at Rome, NY to the Computer Forensics Research and Development Center (CFRDC) at Utica College and the support from the Directors of the Economic Crime Investigation Institute (ECII). Utica College will support and house the IJDE.

Editorial Policy

IJDE welcomes contributions from individuals actively engaged in digital evidence theory, research, policy, and practice. Submissions will be peer reviewed by the Editorial Board and, in cases where outside expertise is required, by invited peer reviewers. Because we are committed to full and vigorous discussion of issues, IJDE will provide space for anyone who is criticized herein to respond.

31.1.2 Editorial Board

Editor:

Gary R. Gordon, Ed.D. Executive Director, Economic Crime Investigation Institute (ECII) and Professor of Economic Crime Management at Utica College

Associate Editor:

John Leeson, Ph.D. Associate Professor of Computer Science, University of Central Florida,
Assistant Director, National Center for Forensic Science,
CFCE, International Association of Computer Investigative Specialists

Editorial Board:

Zeno Geradts Forensic Scientist, Netherlands Forensic Science Laboratory

Joseph Giordano Technical Director, Information Directorate Air Force Research Laboratory

Chet Hosmer President, WetStone Technologies, Inc.

Larry Leibrock, Ph.D. CTO – McCombs Business School and IAT - University of Texas at Austin

James Lyle, Ph.D. Computer Scientist, National Institute of Standards and Technology

Gary Palmer INFOSEC Scientist, Mitre Corporation

Ronald Stevens Senior Investigator, New York State Police

Tom Talleur Managing Director Forensics Technology Team, KPMG

Carrie Whitcomb Director, National Center for Forensic Science

31.1.3 Current Issue

IJDE Spring 2002 Volume 1, Issue 1

From the Editors

Gary R. Gordon & John Leeson
The Inaugural Issue: A Message from the Editors [HTML] [PDF]

Articles

Tom Talleur
Digital Evidence: The Moral Challenge
IJDE 2002 1:1 [HTML] [PDF]

Carrie Morgan Whitcomb
An Historical Perspective of Digital Evidence: A Forensic Scientist's View
IJDE 2002 1:1 [HTML] [PDF]

Gary L. Palmer
Forensic Analysis in a Digital World
IJDE 2002 1:1 [HTML] [PDF]

Chet Hosmer
Proving the Integrity of Digital Evidence with Time
IJDE 2002 1:1 [HTML] [PDF]

N.B. The articles can be found in Appendix D.

31.1.4 Archives

Past issues will be available here.

31.1.5 Author Instructions

The IJDE will only consider original manuscripts, written in English, for publication. Each submission must be accompanied by a cover letter, in which the author states the work in this manuscript has not been published previously and that the article is not being submitted to other publications simultaneously. The cover letter should also include an MD5 hash for each file being submitted electronically. All files can be combined into a single zip file for electronic submission. In that case, a single MD5 hash for the zip file will suffice. Articles may be submitted electronically as email attachments to the editor. The cover letter and copyright releases, however, must be received in hard copy prior to publication.

The manuscripts must be prepared according to the Publication Manual of the American Psychological Association (5th ed.). Information on this citation method can be found at http://www.apastyle.org/elecref.html. The manuscript should be double-spaced and authors must provide an abstract of up to 150 words.

Statements made in the work submitted and images included in or submitted separately with the work are the authors' sole responsibility. Authors are responsible for requesting permission from copyright owners where necessary.

Contributions should be in Microsoft Word format (*.doc), or ascii format (*.txt), in that order of preference. Images embedded in articles should be in GIF (*.gif) or JPEG [preferred](*.jpg, *.jpeg) formats. Images submitted separately may also be in TIFF (*.tif, *.tiff) format.

Times Roman font is the preferred font for submissions. Use 20-point bold for the title, 12 point bold for section headers, 12-point regular for the body of the article and for the references.

Articles should be prepared in single column format with 1-inch top, bottom, left, and right margins. Text should be left justified.

Each figure should have a label such as Fig. 1. Use 12 point bold for labels and center them under the figures. It is appropriate for small figures embedded in Word documents to have text flow around them.

Append a brief "about the author" bio to the end of the article, after the references. This should include contact information and could include a hyperlink to the author's site for a more extensive bio.

31.1.6 Contacts

Submissions

Submissions may be e-mailed to the Editor, Dr. Gary R. Gordon ggordon@utica.ucsu.edu or the Associate Editor, Dr. John Leeson jjleeson@hotmail.com.

Correspondence

Dr. Gary R. Gordon
IJDE Editor
Utica College
1600 Burrstone Road
Utica, NY 13502

Feedback

Comments about the appearance of the web site, broken links, and other technical matters should be sent directly to webmaster.

Comments for the editors should be directed to ggordon@utica.ucsu.edu or jjleeson@hotmail.com.

31.1.7 Related Links

Organizations that have provided resources to support IJDE are included here.

Academic

http://www.ecii.edu/   Economic Crime Investigation Institute, Utica College
http://ncfs.ucf.edu/   National Center for Forensic Science University of Central Florida
http://praetor.bus.utexas.edu   University of Texas at Austin (Dr. Liebrock)

Law Enforcement

http://www.troopers.state.ny.us/   New York State Police

Government

http://www.cftt.nist.gov/   National Institute of Standards and Technology

DoD

http://www.rl.af.mil/   Information Directorate, Air Force Research Lab

Commercial

http://www.us.kpmg.com/services/content.asp?l1id=10&l2id=550
KPMG Forensic Technology Services

http://www.wetstonetech.com/   Wetstone Technologies, Inc.

Organizations/Other

www.dfrws.org   Digital Forensics Research Workshop (DFRWS)
http://forensic.to/forensic.html   Zeno's Forensic Site

Appendix A - CFX 2000 Scenario Storyboard Diagram

Lady Luck Casino (LLC)
- Robert VanHouten (Owner - Chairman of BOD)
- Daren Hicks (VP)
- Joshua Freddo (Guest Services Supervisor)
- Victor Delgato (Pitboss)
- Employees
- Cheryl Provo (Assistant CFO) — Main Contact between ICG and Kellner

Big Shell Industries (BSI) — Owns / Own

International Crime Group (ICG)
- Harold Jernigan (HJ) (Preisident)
- Po Box — Mails Flight Slips to
- Hires

Foriegn Industrial Spies Hunting Information (FISHI)
- Brian "Hawkeye" Karp — Dumpster Diving

National Aeronautical Authority (NAA)
- Flight Slips — Dumpsters contain flight strips with flight information

Payments 1

Hires

Discovers money laundering and triggers investigation

High Action CracKERS (HACKERS)
- Christina Dennison

United States Millitary Movers (USMM)
- Databases store information on flight manifests and policies and procedures in case of fire
- Database Server — Hacks Into

Payments 2

Becomes acting manager while Kellner is on forced vacation

Hires

Blackmail and Bribe — Trusted Network Connection

United Terrorists in Criminal Activity (UTICA)
- Charlie Fisher
- Cody Judy

Trusted Research & Development, Inc. (TRDI)
- Dex West Computer Scientist (Insider)

Email with Stego (Manifest and Flight Slips) — Sends

Bring Multiple Cash Deposits Under 10k on a Daily Basis

Illinois Credit Union (ICU)
- ICU
- Stephen Kellner (Credit Union Manager) — Gives money for deposits
- Jennifer Devlin (Asst. Mgr)
- Lady Luck Casino Cover Account — One Deposit
- Amy Taylor (Teller)
- Majority of Deposits
- Fake Jerry Vigue Account

Banco Popular

Glacier Bank

Barnes Bank and Trust

McAllen National Bank

Belize Breeze Bank, Ltd
- Brian Vigue Account
- BBB
- Belize

The First National Bank of Calumet

First Progressive Bank

Steal Crypto Box from refueling plane

Dubai Airport

Fire Policy manual — Sends

70

Appendix B - CFX 2000 Scenario

B.1.   Premise

Harold Jernigan the leader of The International Crime Group (**ICG**) has a plan to steal a Top Secret Crypto Box the KG-84 from a military plane when it stops to refuel at the Dubai Airport. To carry out this plan the ICG hires three different criminal groups:

- Foreign Industrial Spies Hunting Information (**FISHI**) who specialize in dumpster diving and industrial espionage. This group is lead by Brian Karp and they primarily use – (BK_Hawkeye@exite.com) as their contact email address

- High Action CracKERS (**HACKERS**) expert hackers who specialize in social engineering and economic espionage. The primary contact for Jernigan is Christina Dennison (elite@bignet.net) and (denni@antionline.org)

- United Terrorists in Criminal Activity (**UTICA**) a small but organized anti-American terrorist group for hire located in Dubai. They are lead by two men known only by their aliases – Charlie Fischer (utica100@hotmail.com) and Cody Judy (fuerzapeligrosa@yahoo.com).

The three groups know nothing about each other's involvement and generally deal directly with the ICG.

B.2.   Economic Crime Element

To fund their operations, the ICG must find a way to launder the money produced by their illegal activities. Jernigan decides to launder the money through the Lady Luck Casino (**LLC**), which the ICG owns through a shell company called - Big Shell Industries (**BSI**).

B.2.1 Monday, June 5, 2000

The ICG sends an email to Robert VanHoughton (Rvan@llc.com) telling him "…To be on the lookout for potential special customers who could help increase BSI's profits…" Mr. VanHoughton (Rvan@llc.com) sends back an email that says he knows a "…special customer who fits the bill – Stephen Kellner…" Stephen Kellner is the manager of the local branch of the Illinois Credit Union (**ICU**) and a frequent visitor to the casino. The crime group decides to target him as a possible way to launder money.

B.2.2 Friday, June 9, 2000

Mr. VanHoughton (Rvan@llc.com) sends an email to Joshua Freddo (jfreddo@llc.com) the guest services supervisor instructing him to send a special VIP invitation to Kellner (skellner@icu.com) for the extended Fourth of July weekend.

B.2.3 Monday, June 26, 2000

Joshua Freddo (jfreddo@llc.com) sends an email to Kellner (skellner@icu.com) thanking him for accepting their invitation and saying that everything is set for his arrival on Friday June 30th.

B.2.4 Friday, June 30 – Tuesday, July 4, 2000

During his visit to the Lady Luck Casino Kellner receives special treatment including a VIP suite, unlimited credit etc… On his last day the casino Mr. VanHoughton (Rvan@llc.com) contacts Victor Delgato (vdelgato@llc.com) who is a pit boss at the casino and has him fix a poker game with Kellner. By the end of the game Kellner is in so much debt that he has no choice but to agree to help the International Crime Group. After a long meeting with Mr. VanHoughton and his associates, Kellner is told that Cheryl Provo (cprovo@llc.com) will contact him soon and that he is to follow any directions she gives him.

B.2.5 Wednesday, July 5, 2000

Kellner (skellner@icu.com) is instructed by Cheryl Provo (cprovo@llc.com) the assistant CFO at LLC during a phone call to open two accounts at the ICU one in the name of Lady Luck Casino and another under a false name and then to wait for further instructions. She follows up the phone call with an email that says, "…As you know from our previous conversations the Lady Luck Casino is thinking about changing banks and are considering ICU as a strong candidate. We would like to open an account on a trial basis to see if your customer service is as good as you say it is…" Kellner opens the two accounts with the help of his girlfriend Amy Taylor (ataylor@icu.com) who is a teller at the ICU branch he manages. The name they use on the dummy account is Jerry Vigue. Kellner sends email to Provo telling her that, "…her account is now open. We look forward to doing business with you…"

Illinois Credit Union	Account Name: Jerry Vigue
	Account Number: 075-56897-8273-00373
Illinois Credit Union	Account Name: Lady Luck Casino
	Account Number: 075-56897-8273-00371

B.2.6 Thursday, July 6, 2000

Cheryl Provo (cprovo@llc.com) sends email to Kellner "…thanking him for his excellent customer service and saying that LLC employees will soon be bringing in deposits…" Kellner sends a broadcast email to all ICU employees saying that, "…LLC is considering switching all of their business to ICU and how important that would be since they are the biggest employer in the area. To ensure proper customer service he is assigning one employee (Amy Taylor) to work exclusively on the account.

B.2.7 Monday, July 10 – Thursday, October 19, 2000

LLC employees bring in between three and ten deposits per business day and give them directly to Kellner. Kellner then takes the deposits to Amy Taylor (ataylor@icu.com) his girlfriend who is assisting him in the money laundering to help him get out of debt. One to five of these deposits are placed in the real LLC account as a cover and the rest are placed into the dummy account. The deposits into the Jerry Vigue account are generally under $10,000 and are primarily cash with some checks. On a weekly basis each Monday thereafter Kellner wires all but $1,000 from the dummy account to six different US banks.

1. Barnes Bank and Trust
Account Name: Rachel Vigue
Account Number: 003-27765-1500-32670

2. Banco Popular de Puerto Rico
Account Name: Tyler Vigue
Account Number: 187-20493-5400-43970

3. First Progressive Bank
Account Name: Andrew Vigue
Account Number: 363-47643-1499-71345

4. McAllen National Bank
Account Name: Melanie Vigue
Account Number: 548-69422-1600-10901

5. The First National Bank of Calumet
Account Name: Kay Vigue
Account Number: 845-32864-3200-45009

6. Glacier Bank
Account Name: Rebecca Vigue
Account Number: 988-34669-6533-25732

The funds from these six accounts are wired on a bi-weekly basis to a single account at the Belize Breeze Bank and Trust. This account is in the name of Brian Vigue. These funds are then used to fund the ICG's ongoing operations including the current plan to steal the Top Secret Crypto Box. Funds are distributed primarily by checks that are signed by Brian Vigue.

B.2.8 Friday, October 20, 2000

Kellner comes into work as normal and is met by Jennifer Devlin (jdevlin@icu.com) his assistant manager. He is told that the head office, after reviewing the branches human resource records, has ordered him to take his mandatory two-week vacation starting today. Devlin is to assume all of Kellner's responsibilities immediately. Before leaving, Kellner goes to his desk and sends an email to Cheryl Provo (cprovo@llc.com) saying that, "…he had to go on vacation and that he would be unable to provide personal

customer service for the next two weeks and telling her to deal only with Amy Taylor during his absence if she needs anything…"

After sending the email Kellner deletes all of his email. Kellner then leaves on vacation. Unfortunately for Kellner and the ICG, Cheryl Provo is also on vacation and has left Darin Hicks (dhicks@llc.com) in charge of the money drops. An automated email reply saying she is on vacation will be sent and arrive after Kellner leaves and will be the only email in Kellner's inbox.

When the LLC employees come in to make the regular deposit they proceed to Kellner's desk and give the deposits to Devlin who is working there. Devlin is suspicious and looks up both accounts and recognizes the obvious pattern of money laundering and calls in the banks internal auditors who in turn call in Federal Law Enforcement to investigate the situation.

B.2.9 Tuesday, October 24, 2000

This is where the LIVE EVENT begins. Investigators will be given a briefing on the case. They will be told that there have been some suspicious transactions discovered after an employee was forced to take a mandatory vacation. The investigators have been brought in to figure out what is going on. The investigative teams will then be given access to the following items:

- A floppy disk containing the following 5 files
    - Teller List
    - Account information for the LLC Account
    - Account information for the Jerry Vigue Account
    - Deposit records for the above accounts
    - Money transfer transaction records for the above accounts

Once the investigators have figured out the money laundering pattern from these records, they will be able to subpoena the following items to help them follow the money trail and to corroborate the evidence from the disk.

- Stephen Kellner and Amy Taylor's workstation hard drive
- Information from the six US banks which will contain the following
    - Account information
    - Deposit transaction records
    - Money transfer transaction records

From these files the investigators will be able to determine that the source of the money is the Lady Luck Casino and that from these accounts the money is being funneled back into a single account that is located at the Belize Breeze Bank and Trust.

B.3   The Real Crime

The UTICA terrorist group (Charlie Fischer utica100@hotmail.com and Cody Judy fuerzapeligrosa@yahoo.com) has agents in place at the airport that work on the ground crew at Dubai airport. The ICG plan is to have the terrorist group set a small fire on or near the plane when it is being refueled. The ICG needs three pieces of information to carry out their plan.

- Identify a specific plane type that carries the Top Secret Crypto Box
- Discover what the polices and procedures are in case of a fire on that type of plane
- Discover when one of the planes that meets the above two requirements will land to refuel in Dubai

The two steps in this process are to identify a specific plane carrying the crypto boxes and to find out what the fire policies and procedures are on that plane. This information can be obtained from the databases located on an internal network at a military organization called the United States Military Movers **(USMM)**. The USMM controls the deployment of troops, equipment, etc…for all US armed forces. The only problem is that these databases are stored on a secure internal network with no publicly accessible external connections. The task of solving this problem is given to the hacker group HACKERS.

The HACKERS do some exploratory research on the Internet and discover that if they can infiltrate the network of the Trusted Research and Development Incorporated **(TRDI)** they can get into the USMM network through a trusted network connection. They decide to look for an accomplice that they can turn and use as an insider to get into USMM. The hackers decide to target a new employee who may be more vulnerable to their plans. The hacker Christina Dennison (elite@bignet.net) is assigned to gather new employee information through social engineering. Once she obtains a list of new employees and their applications from HR she begins calling previous employers to obtain more information. When she checks on Dex West, (dwest@trdi.com and dexwest@my-deja.com) through her social engineering skills, she finds out that he quit his previous job just before the company fired him for alleged drug use. Christina Dennison contacts Dex by phone and through a combination of seduction and blackmail gets him to agree to help out the HACKERS.

Dex is already computer expert and so the hackers send him some basic hacking tutorials, exploits, and links to hacker sites and tools. Dennison (elite@bignet.net) then sends email to Dex (dexwest@my-deja.com) telling him "…about her trip to Florida and telling him that he should go there soon and that she could help him make planes because she has connections…". Dex then uses the tools and exploits to escalate his privileges and access the USMM database server. Once he has administrative privileges he plants a copy of the Back Orifice Trojan. Dex then sends an email saying that "he was planning to go to Florida and was thinking about talking to a travel agent to get tickets and would love her help in planning the trip…". ICG (JdoeMrX@netscape.net) now sends a message to Dennison (elite@bignet.net) that says "The confirmation number for your friends room is…" Dennison (elite@bignet.net) then sends a message to Dex

(dexwest@my-deja.com) with the same number the says, "…My friend is a travel agent I had him make reservations at my favorite hotel. Your hotel confirmation number is... Dex then accesses the USMM manifest database and locates a list of flights that carry the Crypto Box. He copies the file to his computer and sends it as an attachment to Dennison (elite@bignet.net) with a message that reads, "…Which flight do you recommend I take…" Dennison (elite@bignet.net) then forwards the information to ICG (JdoeMrX@netscape.net) with the message "…Which flight do you think my friend should take?"

The ICG also knows that all flight records are kept within the National Aeronautical Authority **(NAA)**. So the ICG (JdoeMrX@netscape.net) instructs Brian Karp (BK_Hawkeye@excite.com) to obtain flight records of the flights ordered by the USMM that stop over to refuel in Dubai. In the email they say, "My friend is planning a trip to Florida and he needs some flight information. Any help you can provide would be greatly appreciated… After several nights of work Karp gets enough slips of flights he makes copies of them and sends them to a PO Box. The PO box is owned by Big Shell industries and the contact name is Harold Jernigan. Once they receive the flight slips ICG instructs The Belize Breeze Bank **(BBB)** to transfer $10,000 into Brian Karp's bank account.

IGC (JdoeMrX@netscape.net) emails the flight numbers to the HACKERS (so they can obtain information on the flights. Christina then forwards the list of flight numbers to Dex in an email message that says, "Here are your lucky lottery numbers. I hope to see you at the party next week…" Dex then uses the Back Orifice Trojan to access the USMM Manifest database and locate a flight that will be carrying the crypto box. Dex sends a message to the hackers saying, "I am ready for the party do you need me to bring anything?" Christina sends back a message saying, "We need you to bring the boom box to the party? By the way can you send a picture of your sister to my cousin Charlie? He is thinking about asking her on a date and bringing her to the party. His email address is utica100@hotmail.com" Dex then uses Steganography to hide the manifest and flight information in a message and sends it to the hotmail account.

B.4   Planned Sequence of Live Events

- Investigators receive a briefing on the suspected money-laundering incident at Illinois Credit Union.

- Investigators are given a disk containing the reports listed above.

- Kellner and Taylor are on "vacation" but investigators can seize their computer hard drive.

- Investigators trace deposits from the "Jerry Vigue" account at ICU to the six US bank accounts.

- Investigators "subpoena" transaction and account records on the specific accounts from the six banks.

- Investigators trace money flow from the six US banks to the Belize Breeze Bank (BBB).

- Investigators send "subpoena" request for bank records to the Belize Breeze Bank.

- BBB sends records containing checks including several to Brian Karp.

- Investigators will use criminal database and find that Brian Karp is a known criminal with a history dumpster diving and industrial espionage.

- Investigators detain and interview Brian Karp. He gives them the following items:
    - Copies of flight slips from the NAA
    - A partial PO Box address that can be traced back to Harold Jernigan (HJ)

- BBB sends second set of records containing checks including several to Christina Dennison.

- Investigators will use criminal database and find Christina Dennison is a known criminal with a history of hacking and industrial espionage. They will also learn that she is currently in custody in New York State on an unrelated charge and her computer has been seized and is already at the FIC.

- Investigators now have access to Christina's computer for investigation purposes.

- Investigators use evidence from Christina's computer to seize Dex West's computer and detain Dex West.

- Investigators detect a stegoed image on Dex West's computer using SDART.

- Investigators interview Dex West and get the name of the stego program and the password for the image.

- Investigators decode the image and find a message containing a manifest and flight information for the targeted flight.

- Investigators warn the USMM who in turn warns the planes crew to reroute and not to land in Dubai.

Appendix C - CFX Experiment 2000 Milestones

1. Money laundering is suspected from Lady Luck Casino to the Illinois Credit Union
2. Kellner and Taylor are accomplices at the credit union involving the laundering of money
3. The money is laundered from the credit union to six U.S. Banks is discovered
4. The money is funneled back to a single account at the bank of Belize
5. Brian Karp received money that was paid via the suspect account from the Belize bank
6. Brian Karp is identified as a known dumpster diver.
7. Brian Karp dumpster diving target was flight data strips
8. The flight data strips represented military fights that were heading to Dubai
9. Christina Dennison is identified as someone was paid from Belize bank account
10. Christina Dennison is identified as a known computer hacker
11. Christina Dennison is interested in TRDI
12. Christina Dennison has an interest in military cryptography devices specifically the KG-84
13. Christina Dennison has a plethora of hacking tools on her computer
14. Dex West is identified as an accomplice of Christina Dennison
15. Dex West is an employee of TRDI
16. Dex West's computer is a dual-boot Linux / NT system
17. Hacking tools were discovered on Dex West's computer in the Linux environment
18. A Trojan application "NetBus" was found on Dex West's computer on the NT system
19. E-mail message containing the NetBus Trojan was e-mailed to B. Shatner's at USMM
20. NetBus software client was found on Dex West's NT system
21. Fire Emergency Policies and Procedures manual for the C-5 Galaxy Aircraft found on Dex West's computer
22. Aircraft manifest lists found on Dex West's Computer
23. E-Mails found on Dex West's computer containing coded communications with known hacker Christina Dennison
24. The manifest list found on Dex West's computer contains entries for the KG-84 the same device that Christina Dennison had specs on
25. E-mail found on Dex West's computer sent to Charlie Fischer containing the Fire Emergency Policies and Procedures Manual of the C-5 Galaxy aircraft
26. E-mail found on Dex West's computer sent to Cody Judy containing a suspicious message with an attached image is found
27. Deleted Stego software and deleted images found on the Linux drive of Dex West's computer
28. Attachment found on the suspicious e-mail is suspected to have Steganography "secret messages" embedded in side.
29. The password for the stego program is provided to investigators by Dex West
30. The secret message is extracted that contains, time, date, flight number and manifest of the target aircraft
31. The manifest is found to contain the KG-84 crypto device
32. The recipient of the message containing the flight data and the manifest is found to be part of a terrorist organization in Dubai

Appendix D - Inaugural Issue of the International Journal of Digital Evidence

The Inaugural Issue: A Message from the Editors

Welcome to the inaugural issue of the International Journal of Digital Evidence (IJDE), Spring 2002 Volume 1, Number 1. IJDE will be an online journal published quarterly: March, June, September, and December.

IJDE is a forum for the publication and discussion of theory, research, policy, and practice in the rapidly changing field of digital evidence. The focus will be on research findings; advancement of new theories; discussions of evolving standards, validation methods, and certification processes based on scientific methods; presentations of key legal and legislative issues; reports on significant advances is technology; and analyses of innovative policies and practices in the digital evidence field.

The articles in this issue were solicited to lay the foundation for discussion in many of the areas listed above. We appreciate the willingness of the four individuals to provide their thoughts on a very tight time schedule. In order to launch this journal in a timely fashion, some of the peer review processes that will be applied to future submissions were truncated.

Tom Talleur's OP-ED piece, Digital Evidence: The Moral Dilemma, lays the foundation for future discussion regarding the moral, legal, ethical, and other overarching issues within the digital evidence field.

An Historical Perspective of Digital Evidence: A Forensic Scientist's View by Carrie Morgan Whitcomb, provides insight into the evolution of the various groups working on definitions, standards, and certification, first in computer forensics and then in the more inclusive field of digital evidence.

In Proving the Integrity of Digital Evidence with Time, Chet Hosmer discusses the need for a secure, non-forgeable, auditable time stamping process to prove the when of an event. Innovative technologies are discussed that provide the capability to accomplish this task.

Gary L. Palmer's Forensic Analysis in a Digital World, reviews the scientific approach used by other forensic sciences and makes the argument that the same exacting standards should be applied to digital evidence. Palmer argues that, "Incorporation of the scientific method is the key to providing forensic evidence or suitable information meant to persuade, whether it is for courts of law, military operations, banking or homeland defense."

Initial funding for IJDE has been provided by two sources: a grant from the Air Force Research Lab Information Directorate at Rome, NY to the Computer Forensics Research and Development Center (CFRDC) at Utica College and from the Directors of the

Economic Crime Investigation Institute (ECII). Utica College will support and house the IJDE. Additional funding will be sought; suggestions or volunteers are welcomed.

In order for the Journal to be successful, it must be embraced by the key contributors in this field. In that spirit, we welcome offers of support, including article submission, peer reviewers, and constructive comments. I can be reached at ggordon@utica.ucsu.edu or at 508.247.9504. John Leeson's e-mail address is jjleeson@hotmail.com.

The summer issue will be available in late June. Submissions must be received by the editors by May 20, 2002. The fall issue will be published in late September. Submission must be received prior to July 22, 2002.

Please share the IJDE with your colleagues, students, organizations whose focus is related to digital evidence and forensics, and others who may find the information in the journal valuable. We thank you in advance for your support as we help launch this important endeavor.

Gary R. Gordon, Ed.D.
Utica College

John J. Leeson, Ph.D., CFCE
University of Central Florida

An Historical Perspective of Digital Evidence: A Forensic Scientist's View

Carrie Morgan Whitcomb, Director, National Center for Forensic Science

Author's Comments

During my tenure as director of the Postal Inspection Headquarters Laboratory (1988-1992), a Postal Inspector submitted a computer to examine for the presence of specific evidence he had enumerated in the letter of request. The evidence technician logged in the computer, assigned it a case number, and brought the request to me, inquiring "What should we do with this?" That was the beginning of an odyssey that I still pursue.

The Inspection Service Laboratory had a Questioned Document Section. Since a computer seemed to be an obvious evolution of paper documents, I called the manager of that section, Drew Somerford, and asked him to take the case. He was reluctant to sign for the evidence. Even though there might have been "documents" on the hard drive, it was outside his expertise. How do you secure and preserve the evidence? How do you collect it without changing it? What are the accepted practices related to computer evidence that would stand the scrutiny of court? What are the examination protocols? It was technology that we did not know how to handle in the crime laboratory.

We submitted the computer evidence to the Federal Bureau of Investigation (FBI). The FBI Laboratory had a unit for computer evidence, and they worked the case. The Postal Inspection Service had a team of inspectors who were trained to work computer crime cases, but the laboratory was not equipped to assist them in processing evidence at that time.

Background

Computer forensic science is largely a response to a demand for service from the law enforcement community. As early as 1984, the FBI Laboratory and other law enforcement agencies began developing programs to examine computer evidence. To properly address the growing demands of investigators and prosecutors in a structured and programmatic manner, the FBI established the Computer Analysis and Response Team (CART). Although CART is unique in the FBI, its functions and general organization are duplicated in many other law enforcement agencies in the United States and other countries (Noblett, Pollitt, & Presley, 2000).

An early problem addressed by law enforcement was identifying resources within the organization that could be used to examine computer evidence. These resources were often scattered throughout the agency. Today, there appears to be a trend toward moving these examinations to a laboratory environment. In 1995, a survey conducted by the U.S. Secret Service indicated that 48 percent of the agencies had computer forensic laboratories and that 68 percent of the computer evidence seized was forwarded to the experts in those laboratories. As encouraging as these statistics are for a controlled programmatic response to computer forensic needs, the same survey reported that 70

percent of these same law enforcement agencies were doing the work without a written procedures manual (Noblett, et al., 2000).

From Computer Forensics to the more inclusive "Digital Evidence"

In 1990, the Postal Inspection Service Laboratory moved to a new facility at Dulles, Virginia, and by 1996-97, had established a Computer Forensic Unit. The Inspection Service had worked closely with the FBI for several years in the development of computer forensic capabilities. About the same time, audio and video enhancement was moving from analog to digital format. Should the same guiding principles be applied to all forms of digital evidence regardless of the output? Would an inclusive "Digital Evidence Unit" be more appropriate than a "Computer Forensic Unit"?

The federal crime laboratory directors in the Washington, DC, area met twice a year to discuss issues of mutual interest. They were instrumental in forming what is now known as the Scientific Working Group Digital Evidence (SWGDE). The concept of finding "latent evidence on a computer" was known as computer forensics at that time. The concept of digital evidence, which included digital audio and digital video evidence was brought before the federal laboratory directors on March 2, 1998, at a meeting hosted by the U. S. Postal Inspection Service, Forensic and Technical Services Division, Dulles, Virginia. This first discussion concentrated primarily on digital photography. The discussion about digital evidence, including digital computer evidence, digital audio and video evidence, needed technical people to lead the discussion. A second meeting was held on May 12, 1998, and the directors brought their technical experts to the meeting to further discuss the technical merits of digital evidence. Dr. Don Kerr, then Assistant Director, FBI Laboratory, invited Mark Pollitt, Unit Chief of the FBI's Computer Analysis and Response Team, to speak to the directors about the concept of digital evidence. Scott Charney, head of the Department of Justice, Computer Crimes and Intellectual Property Section (CCIPS), was invited to discuss legal aspects of computer evidence and to talk about search warrant requirements for seizing digital evidence. The outcome of the May meeting was the formation of another Technical Working Group to address the forensic issues related to digital evidence.

There are ongoing efforts to develop examination standards and to provide structure to computer forensic examinations.   As early as 1991, a group of six international law enforcement agencies met with several U. S. federal law enforcement agencies in Charleston, South Carolina, to discuss computer forensic science and the need for standardized approach to examinations. In 1993, the FBI hosted an International Law Enforcement Conference on Computer Evidence that was attended by 70 representatives of various U.S. federal, state and local law enforcement agencies. All agreed that standards for computer forensic science were lacking and needed. This conference again convened in Baltimore, Maryland, in 1995, Australia in 1996 and the Netherlands in 1997, and ultimately resulted in the formation of the International Organization on Computer Evidence (IOCE). In addition, a Scientific Working Group on Digital Evidence (SWGDE) was formed to address these same issues among federal law enforcement agencies (Noblett, et al., 2000).

On June 17,1998, the Technical Working Group Digital Evidence (TWGDE) held their first meeting. Mark Pollitt, Special Agent, FBI, was elected Chair and Carrie Morgan Whitcomb, Manager, Forensic Services, U. S. Postal Inspection Service was elected Co-Chair. Federal forensic laboratories that were represented included the Bureau of Alcohol, Tobacco and Firearms (ATF), U. S. Customs, the Drug Enforcement Administration (DEA), FBI, Immigration and Naturalization Service (INS), Internal Revenue Service (IRS), National Aeronautics and Space Administration (NASA), U. S. Secret Service (USSS), and the U. S. Postal Inspection Service. TWGDE met monthly to prepare organizational procedures and develop relevant documents. Mark Pollitt gave many international presentations to groups such as the International Organization on Computer Evidence (IOCE) and INTERPOL concerning the work of TWGDE.

From Technical Working Groups (TWGs) to Scientific Working Groups (SWGs)

In forensic science, groups of experts in a particular forensic discipline have evolved into bodies that develop standards, best practices, and protocols. They began as Technical Working Groups (TWGs) in the early1990s. In 1999, the name was changed to Scientific Working Groups (SWGs) in an attempt to distinguish the FBI supported long term working groups from National Institute of Justice (NIJ) TWGs that were of short duration and usually had a single deliverable, such as a guidebook on a specific topic. SWGs are ongoing groups that meet at least once per year, comprised of no more than 50 federal, state and local members. The members may be either sworn (law enforcement) or non-sworn.

The first SWG was organized to deal with the issues related to new forensic technology, DNA. It was called the Scientific Working Group for DNA Analysis Methods (SWGDAM).

Since the early 1990s, the FBI Laboratory has led the way in sponsoring Scientific Working Groups (SWG) to improve discipline practices and build consensus with our federal, state, and local forensic community partners. In early 1998, the FBI Laboratory performed a strategic review of all SWGs" (Adams & Lothridge, 2000).

The result was the development of a framework for operational bylaws for the SWGs.

The establishment, constitution, and goals of a Scientific Working Group (SWG) are a matter of the needs of the particular scientific discipline and professional expertise. Bylaws are required to effectively implement and execute the deliberations of SWGs, and it is important that each SWG develop written bylaws for operation. Although not every SWG can or should be covered by preset standardized rules, certain standards of performance that are common to all SWGs are necessary" (Adams and Lothridge, 2000).

Processes have been developed by SWGs to gain input from non-members on proposed guidelines and procedures before finalizing such documents. In February 1999, TWGDE was changed to SWGDE. The Scientific Working Group Image Technology (SWG-IT)

is closely associated with SWGDE and was originally part of SWGDE. For example, the taking of digital pictures of evidence at a crime scene is digital imagery. When the digital picture itself is the evidence (as in the case of child pornography), it would be digital evidence and part of SWGDE. As SWGIT develops enhancement protocols, there is much commonality between the two SWGs. "The mission of the Scientific Working Group on Imaging Technology (SWGIT) is to facilitate the integration of imaging technologies and systems in the criminal justice system by providing definitions and recommendations for the capture, storage, processing, analysis, transmission and output of images" (SWGIT, 1999).

Defining Digital Evidence

"Digital Evidence is any information of probative value that is either stored or transmitted in a binary form," (SWGDE, July 1998). Later "binary " was changed to "digital".   Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines, etc. The discussion following the formulation of this definition suggested that it was important to put a date on definitions. In the future, time stamps might also be needed to keep up with the changing technologies.

At the August 1998 meeting, SWGDE began to draft definitions. These definitions, as well as standards, were presented at the International Hi-Tech Crime and Forensics Conference held in London in October 1999 (SWGDE/IOCE, 2000).

Draft SWGDE Definitions, Standards and Principles

Acquisition of Digital Evidence: Begins when information and/or physical items are collected or stored for examination purposes. The term "evidence" implies that the collection of evidence 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**: Objects or information of potential probative value that are associated with physical items. Data objects may occur in different formats without altering the original information.

> **Digital Evidence**: Information of probative value stored or transmitted in digital form.

> **Physical Items**: Items on which data objects or information may be stored and/or through which data objects are transferred.

> **Original Digital Evidence**: Physical items and the data objects associated with such items at the time of acquisition or seizure.

Duplicate Digital Evidence: An accurate digital reproduction of all data objects contained on an original physical item.

Copy: An accurate reproduction of information contained on an original physical item, independent of the original physical item.

Standards

Principle 1

In order to ensure that digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system. Standard Operating Procedures (SOPs) are documented quality-control guidelines that must be supported by proper case records and use broadly accepted procedures, equipment, and materials.

Standards and Criteria 1.1

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

Discussion. The use of SOPs is fundamental to both law enforcement and forensic science. Guidelines that are consistent with scientific and legal principles are 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 SOPs on an annual basis to ensure their continued suitability and effectiveness.

Discussion. Rapid technological changes are the hallmark of digital evidence, with the types, formats, and methods for seizing and examining digital evidence changing quickly. In order to ensure that personnel, training, equipment, and procedures continue to be appropriate and effective, management must review and update SOP documents annually.

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. Because 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 and the proper steps for successful use should be listed or discussed. Any limitations in the use of the procedure or the use or interpretation of the results should be established. Personnel who use these procedures must be familiar with them and have them available for reference.

Standards and Criteria 1.5

The agency must use hardware and software that is appropriate and effective for the seizure or examination procedure.

Discussion. Although many acceptable procedures may be used to perform a task, considerable variation among cases requires that personnel have the flexibility to exercise judgment in selecting a method appropriate to the problem. 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 must be tested to ensure that it produces reliable results for use in seizure and/or examination purposes.

Standards and Criteria 1.6

All activity relating to the seizure, storage, examination, or transfer of digital evidence must be recorded in writing 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 arrive at the same conclusions as the originator.
The requirement for evidence reliability necessitates a chain of custody for all items of evidence. Chain-of-custody documentation 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, although pencil (including color) may be appropriate for diagrams or making tracings. Any corrections to notes must be made by an initialed, single strikeout; nothing in the handwritten information should be obliterated or erased. Notes and records should be authenticated by handwritten signatures, initials, digital signatures, or other marking systems.

Standards and Criteria 1.7

Any action that 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 has value only if it can be shown to be accurate, reliable, and controlled. A quality forensic program consists of properly trained personnel and appropriate equipment, software, and procedures to collectively ensure these attributes (SWGDE/IOCE, 2000, pp. 3-7).

Accreditation of Digital Evidence by ASCLD/LAB

While SWGDE was working on best practices, it was determined that we must also have a deliberate plan for gaining acceptance by the forensic science community. We were on the "frontier" of a new forensic science. Others have blazed the trail and all we need to do is follow it. DNA created the SWG process. The American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) has an accreditation process that spells out criteria that must be met by specific disciplines in forensic laboratory operations. SWGDE voted to follow the format of the ASCLD/LAB Accreditation Manual for writing their standards. The major categories are: Principle, Standards and Criteria, Discussion. The manual addresses Laboratory Management and Operation, Personnel Qualifications, and Physical Plant.

Membership in The American Academy of Forensic Sciences (AAFS) for Digital Evidence Examiners

The AAFS is the most prestigious national organization for forensic scientists. Thus far, digital evidence papers have been presented in various sections. If the digital evidence community is to consider forming their own section, there must be a minimum of fifty academy members that petition the board to form such a section. As the Executive Secretary of SWGDE, I gave a presentation to the AAFS Board of Directors at the 2002 meeting concerning the activities of SWGDE and the status of forensic digital evidence. AAFS suggested that all potential members in the digital evidence discipline, who wanted to take part in a digital evidence program, could join the General Section of the Academy. From there, a separate section might be formed.

Chaos and Certification of Digital Evidence Examiners

I believe that the ultimate organization of this diverse community lies with professional certification, covering all aspects of digital evidence. The issues of good science and lawful procedures span the collection of digital evidence at the crime scene, the forensic examinations in laboratories, and the analysis of data by law enforcement. There must be consistent principles that apply to all areas of digital evidence for justice to be served. By the very nature of digital evidence, professional certification is also an international issue. Until we have a universal measure of individual competency and expertise, it will be difficult to move forward in an organized and effective manner. Technology will push

the standards and protocols, which in turn will push training and education, which will feed into certification processes. The legal system will be the end user and will dictate process and procedures. The community must be organized with processes that will meet these many challenges.

The issue is how to successfully bring the multitude of experts along an organized and effective path to address the many issues related to digital evidence with rapidly changing technology. We must create a structure in which the response to change can produce a technically competent workforce of massive proportions. Is an international certification body operated by a consortium of national and international organizations the answer? The National Center for Forensic Science will facilitate a discussion on international professional certification issues utilizing representatives from a broad spectrum of existing organizations and groups to participate.

If chaos precedes a higher level of organization, then we may be ready for professional certification.

References

Adams, D. E., & Lothridge, K. L. (2000). Scientific Working Groups [on-line]. Forensic Science Communications, 2(3). Available: http://www.fbi.gov/hq/lab/fsc/backissu.htm.

Noblett, M.G. (1995). Report of the Federal Bureau of Investigation on development of forensic tools and examinations for data recovery from computer evidence. Proceedings of the 11th INTERPOL Forensic Science Symposium, Lyon, France. Boulder, CO: The Forensic Sciences Foundation Press.

Noblett, M.G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and Examining Computer Forensic Evidence [on-line]. Forensic Science Communications, 2(4). Available: http://www.fbi.gov.hq/lab/fsc/backissu/oct2000/computer.htm.

Scientific Working Group on Digital Evidence and International Organization on Digital Evidence. (2000). Digital Evidence: Standards and Principles [on-line]. Forensic Science Communications, 2(2). Available: http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

Scientific Working Group on Imaging Technologies. (1999). Definitions and Guidelines for the Use of Imaging Technologies in the Criminal Justice System [on-line]. Forensic Science Communications, 1(3). Available: http://www.fbi.gov/hq/lab/fsc/backissu/oct1999/swigit2.htm.

About the Author

Carrie Morgan Whitcomb (whitcomb@mail.ucf.edu) is the Director of the National Center for Forensic Science (NCFS), a program of the National Institute of Justice (NIJ) hosted by the University of Central Florida (UCF) in Orlando, Florida. The NCFS provides research, education, training, tools and technologies to serve the current and future needs of the forensic science, investigative, and criminal justice communities

Ms. Whitcomb serves on many committees working on definitions, best practices, and standards in the digital evidence field including: Co-Chair of Scientific Working Group for Digital Evidence (SWGDE), and Chair of the Industry and Academia Portfolio of the National Cybercrime Training Partnership (NCTP).

She earned a Masters of Science in Forensic Science, 1976 from George Washington University in Washington, DC and a Bachelors of Science in Zoology and a minor in Chemistry from the University of Kentucky in 1967.

Digital Evidence: The Moral Challenge

Tom Talleur, Managing Director, KPMG LLP's Forensic Practice

My colleagues, co-founders, and I, are fortunate to have this opportunity to characterize a framework for discourse on the topic of digital evidence in this initial edition of the International Journal of Digital Evidence (IJDE). In this respect, we have an opportunity to identify, prioritize, and focus upon some of the most important aspects of this issue, free of irrelevant influences.

Our deliberations begin at a most critical time indeed. The content of this journal may quickly and understandably focus on examinations of the best tools, techniques and related themes of interest to a wide range of readers. Because of this, I thought it might be helpful for all of us to reflect upon the humble origins of our craft and the conditions of the present, and thus embrace the moral challenge before us with a renewed sense of vision and conviction.

The impact of digital information technologies (DIT) upon our world certainly poses endless benefits for the citizens of our growing global village. Many global citizens have seen how technology may be used to advance the condition of man and to correct miscarriages of justice, as with the use of DNA analysis to reverse criminal convictions. But many have also observed, with increasing alarm, how DIT can provide a low cost, high performance, seemingly anonymous conduit empowering man to destroy property or injure the rights others at will, very quickly, and with devastating impact — a fact raising serious social, moral, and legal issues for debate. One need only read a United States newspaper article about the latest event of cyber related misbehavior, to infer the need for clarity in addressing the issues relating to digital evidence from the social, moral, and legal points of view, as well as technical perspectives.

Not surprisingly, the digital evidence recovery (DER) movement paralleled the rise in cyber related crimes. Save the earlier telephone hacker (Phreaker) threat, this movement started loosely in the United States in the early to mid-1980's featuring a handful of federal investigators, with a few state and local police officers and a smattering of prosecutors, striving to make sense out of and to bring order and insight to what then appeared to be a cascading problem: the use of computers by criminals and the need to recover digital evidence in connection with investigations. The level of individual technical skill on the part of these early DER examiners notwithstanding, they were a small, close-knit, clever and resourceful group that began to congregate as the Federal Computer Investigations Committee. Their small size and self-critical nature, buttressed through the oversight of devoted prosecutors, ensured an effort to balance the rights of suspects with the need to make "good case law," while enforcing the law and addressing inadequacies in the law through legislative and other initiatives. To be sure, individual members of this group made mistakes as they attempted to address the pandemic dearth of knowledge, skills, abilities, and the lack of training in the field through advocacy and a "master craftsman to layman" approach in training. Often, the use of their findings in courts or other forums went unchallenged for a variety of reasons. All parties to the

process knew that it would only be a matter of time before the judgment of all DER examiners would be questioned in every respect. The best efforts of these early DER pioneers notwithstanding, we now find ourselves as a global information society with moral challenges before us.

Most investigations and litigation in the United States today involve digital evidence. Law enforcement digital evidence examiners and some private sector service providers try to adhere to a general practice of functioning as evidence specialists to avoid the certain pitfalls associated with declaring themselves to be "technology experts." We do not yet have a generation of forensic investigators, examiners, and members of the legal profession who are equally adept at conducting sound, objective thorough investigations and positioning findings in the form of sound litigation in matters involving digital evidence.

In the private sector, DER has now become a "big business" of interest to litigators and professional service providers. Litigation in the form of "electronic discovery" is epidemic, as technologically challenged DER examiners and members of the legal profession struggle with technology issues, while setting case law precedent in the process. Victims and litigators regularly employ information technology or security specialists to deal with digital evidence matters not knowing or caring, in some instances, of the implications of their actions. Software development firms, sensing a profitable market, deploy "one-size-fits-all" digital forensic products for use by anyone able to afford the cost of the software along with one and two week commercial software certification courses – an approach that has had some appeal with members of the legal, audit, network security and other disciplinary communities seeking to "cross over" into the digital evidence field. These conditions raise a host a standards, independence, and related issues implying the potential for mistakes in judgment, error, and even willful misbehavior on the part of examiners or others in the process, and raises frightening possibilities. DER examiners increasingly, and thankfully I might add, find their activities and judgments subject to searing scrutiny, with their practices and procedures coming into question on an increasing basis. Fortunately, both law enforcement and private sector practitioners have the beginning framework of standards posed by the International Organization of Computer Evidence (IOCE), the National Institute of Standards (NIST), and the United States Department of Justice. So what might we do in this context? Obviously, it is neither likely nor desirable to suspend technology advancements or DER initiatives, but the stakes are high, given the potential and increasing impact digital evidence will have on the liberty and rights of individuals in the future.

With this in mind, I raise a theme that all might agree may form the basis of an underlying premise in the digital evidence field: that the use of digital evidence findings as a basis of making moral judgments about the actions and intentions of others is worthy of continuous reflection and debate as a conceptual underpinning to this discipline and the standards associated with it. This theme begs, of course, many of the central issues tugging at the conceptual framework of the digital evidence issue. These issues revolve around the need for a common understanding of the concept of evidence generally,

standards in a variety of conceptual senses, and, a framework for making ethical judgments about the interpretations and uses of digital evidence in a broad sense. Of course, some may reject this lattermost idea altogether. After all, are not DER examiners simply "fact finders" who report their interpretations to others who then render judgments based upon their reports? Perhaps. But somehow this contention seems to conflict with the premise and long established practice that examiners must know "all of the relevant facts" in a given case prior to conducting an examination, so that their analysis is relevant. Are we now performing an ethical analysis in the process, since we a) have the facts b) render judgments about we will and will not report as relevant and c) interpret what we report to others? Can we now assert we are just "independent fact finders" and that we do not make ethical judgments about others in the process of our examinations? Do we need to consider an overarching standard for ethical conduct on the part of all DER examiners?

Perhaps we might turn our attention for the moment to the concept of evidence, generally. In this respect, the issue of digital evidence relates more to the concept of evidence and knowing, in general, than it does to the digital technologies we often place at the focal point of discussions through our discussions of tools and techniques. This in turn begs the issue of the conditions to know.

The first generally accepted condition to the concept of knowing is, if one claims to know something, then that which he or she knows must be true. Stated differently, it is contradictory to assert that one knows something and that the object of his knowing is not true, unless, the person making the claim is willfully untruthful, has been mislead, is mistaken, is making a playful utterance, or the like. Second, if one claims to know something, he or she must believe it. Again, stated differently, it is contradictory to assert that one knows something, but that he or she does not believe in knowing the object of his knowledge, unless, the person making the claim is willfully untruthful, has been misled, is mistaken, is making a playful utterance, or the like. And finally, if one knows something, he or she should be able to give good evidence for it.

Those DER examiners who consider themselves to be "fact finders" only may be relieved to know that, with respect to the conditions to know as I have cited them above, we are concerned only with derivative knowledge (since we perform examinations based upon extant material following premises, fact patterns, through standards, policies, procedures, etc.) and not epistemic knowledge (for matters that are claimed to be "self-evident"). Also, it might be presumed that these conditions of derivative knowledge are implicit in the daily representations of DER examiners, litigators and expert witnesses as they represent their findings. It is possible, for example, that well intentioned but untrained, poorly trained, technology-challenged, lazy, or careless persons, or those of malign intent, acting as witnesses, victims, or examiners, could alter or misrepresent digital evidence leading, for example, to the wrongful conviction of an individual in a court of law. These individuals, save those of malign intent, could literally believe their actions as meeting the conditions of knowing even with the "good evidence standard" as described above. As disconcerting as this possibility is, we at least know that the actions of those involved in many instances are subject to independent oversight or judgment.

It is clear that we no longer live in a world where a handful of federal investigators subject to strict oversight conduct digital evidence examinations. Second, it is clear that we do operate in a world where DER examiners make moral judgments about the actions and intent of others based upon their examinations. The question remains, what basis exists for these practitioners to claim they make these judgments in accordance with an overarching framework for an ethical analysis standard? Is there a need to set this standard now? My hope is that we will remain mindful of this issue and address it in our future deliberations along with the overarching issue areas of ethics, morality, and relevant law, following the precepts of critical thinking. My belief is that this issue will become increasingly important, especially when we find ourselves gravitating to granular dialogues about technologies, methodologies, and related tactical issues.

About the Author

Tom Talleur ((ttalleur@cox.rr.com) is a Managing Director in KPMG LLP's Forensic Practice and the firm's U.S. practice leader for Forensic Technology Services. He has extensive executive, law enforcement, intelligence community, and public policy making experience regarding cyber crimes, advanced technology exploitations, and national infrastructure defense matters. He completed a 31-year career as a US federal criminal investigator in December 1999 and served as the Advanced Technology Programs Executive in charge of the Network & Advanced Technology Crimes Division at NASA just prior to joining KPMG. He is the recipient of awards from the White House and the Attorney General for his work in the computer crime field. A graduate of the US Naval War College and the Federal Executive Institute,

Mr. Talleur is a keynote speaker to a number of associations and training seminars around the world and serves as an analyst and consultant for television, radio and print media on topics related to computer crimes and the exploitation of technologies. He is a Seized Computer Evidence Recovery Specialist, Certified Fraud Examiner, and a UNIX and Network Security Specialist. He is an advisor to the President of the Information Systems Security Association (ISSA) (http://www.issa.org/board.html), President of the National Capitol Region ISSA Chapter (www.issa-dc.org) and a cyber crime commentator for E-Business Advisor magazine. He also serves on the editorial oversight board of the International Journal of Digital Evidence.

Forensic Analysis in a Digital World

Gary L. Palmer, INFOSEC Scientist, The MITRE Corporation

Perception

World cultures have formed ever-increasing dependencies on digital systems and networks. As such, digital technology is becoming commonplace and in some cases necessary in many people's normal day-to-day activities. It stands to reason that, much like other cultural changes that have moved in to modify our lives, digital technology will increasingly be used by anti-social and nefarious types as well as normal citizens in our expanding digital world.

The basic stages involved in adapting society to the wrongful use of many technologies are as follows. First, is a realization by consumers of the technology that it can and is being used for unauthorized and possibly unlawful purposes. Growing concern as incidents rise and become more serious then follows realization. The volume of misuse and percentage of unlawful activity will eventually cause authorities to recognize that they need some level of expertise to help identify, understand and possibly thwart any future wrongdoing. This stage is preceded by cultivating certified expertise supported by an ever-deeper understanding of the problem, its symptoms and the motivations of those involved in wrongful use. How thoroughly these stages are implemented is a function of several related factors. Two of those factors are, perhaps, most important. First, is the complexity involved in the technology. True subject matter experts are required to understand the associated technology completely as a prerequisite to stating opinions or conclusions about evidence. Second, sufficient conclusive research must stand behind techniques and methods (including tools) employed to analyze and examine exhibits that could become evidence or proof. Up to the present, actions to address both of these related issues have been closely aligned with the formation and evolution of most "forensic" disciplines.

Due, in large part, to our focus on entertainment in western society such as "Quincy ME" or Discovery Channel's "The New Detectives" or "CSI: Crime Scene Investigators," the word "forensic" conjures up specific images. Most everyone, even those in the scientific community, have a pre-conceived notion of the discipline called forensic analysis, and it usually involves visions of autopsies, DNA analysis, and men and women in white coats in a cold, sterile lab. The domain of analysis performed at a "brick and mortar" crime lab, by highly trained (and sworn in most cases) practitioners on tangible, physical items found on, in or around a body at the scene of a crime involving death or terrible injury and solely in support of Law Enforcement and the courts.

With that in mind, where does the emerging discipline called Computer Forensics or the even less understood area named Network Forensics fit?   Aside from the fact that in many cases a physical computer or hard drive has been seized and shipped to a "brick and mortar" lab, one has to wonder where the connection is between forensic analysis and the digital systems and digital networks so prevalent today. The latter seems to call for near

real-time techniques applied to active systems and networks that strive to be predictive or anticipatory. The former appears to reside in an ex post facto world where exhibits are seized, sent to a cloistered facility, and slowly, meticulously analyzed, a totally reactive process. In either case very little of the potential evidence is tangible, or physical. Rather, it is highly interpreted and subject to complex transformations that act on the raw data to place it in a form that can be scrutinized or analyzed.

Computers and other digital components are very complex systems. The product of decades of engineering and manufacturing improvements supported by centuries of scientific study and academic research, computers are truly marvelous devices with great positive potential. This potential makes it certain that digital systems will be used in positive and negative ways. So, as our culture's authorities step through the stages to form the expertise they need to recognize and stop wrongdoing, two important issues must be addressed. Experts must understand the complexity involved in digital technology and that must be aided by serious academic research as a prelude to effective tools and techniques applied in the analysis of digital systems. This paper contends that, up to the present, the evolution of digital forensics has taken a different path. Primarily due to urgent need recognized by analysts and examiners, the field has grown somewhat in reverse of convention. Tools and techniques came before research and expert cultivation. My contention is that for our field to become a true forensic discipline this trend must be reversed. Defense attorneys are beginning to question long established precedent, and courts are increasingly calling for scientific and technical evidence to be judged by rigorous standards (Pollack, 2002). Part of the solution lies in the realization that although forensic analysis is commonplace in support of criminal cases, it is not necessarily under the sole purview of Law Enforcement. Rather, it should be viewed as a rigorous scientific specialty whose purpose is to provide information "suitable" for the courts or public forum. This definition allows for a broader application that will be explored in some detail over the next few pages.

Historical View

Given their long history and current success in providing factual, testimonial evidence for the courts, it is prudent to begin by referencing more traditional methods in forensic science. Review of other forensic analysis methods will help in understanding how we can apply similar techniques when dealing with information systems. Traditional methods include

- chromatography, spectroscopy, hair and fiber analysis, serology (DNA..);
- pathology, anthropology, odontology, toxicology; structural engineering, and questioned documents;
- behavioral patterns revealed by tests such as polygraphs and psychological battery exams.

Most of these forensic disciplines began to flourish alongside the evolving science of criminalistics, which, in the United States, emerged during the 1920's. Advances in medicine, chemistry and microscopy prepared the way for the adoption of scientific

analysis, rather than pure observation and intuition as the cornerstone of criminal investigation. The result of this advancement was, of course, to replace supposition with reality (or fact) and present testimonial evidence to the trier-of-fact (judge or jury) in criminal or civil proceedings.

The vast majority of analytical methods employed by traditional forensic sciences grew out of university laboratories. In fact, before 1929 no official crime laboratory even existed in the United States. Instead, police departments interested in using scientific analysis in the solving of crimes would solicit the assistance of prominent university professors to help them collect and examine potential evidence (Eckert, 1997). Over time, as more and more federal, state and local jurisdictions realized the importance and necessity of scientific investigation, professionals with particular interest in the forensic aspects of analysis transitioned their practices to newly established laboratories that focused on forensic analysis in support of the courts. This trend remains true to this day, although, as stated previously, forensic analysis of computer systems has taken a different evolutionary path

The gradual paradigm shift, from intuition or supposition to fact derived from analysis, took hold in the early twentieth century for a number of reasons. The sciences, both hard (physics) and soft (biology), were advancing rapidly and many of their discoveries were being exposed to a larger percentage of the common population. Perhaps more important was the fact that surface observation alone had been proven time and time again to lead to suspect conclusions. Over time, conclusions presented as scientific evidence in the courts became subject to more rigorous scrutiny. The court system realized that testimony proffered as scientific and conclusive was, for the most part, beyond their complete understanding. In addition, the courts also understood that these analytical methods were not irrefutable. They were derived by experimentation that contained (or should contain) measures of error and other indices that help describe the veracity of statistics and narrative results. This leads to standards and rules of admissibility as well as the expert testimony that must accompany scientifically derived testimonial evidence (Eckert, 1997).

Mostly in criminal proceedings, the courts, and public opinion, have come to rely heavily on certain evidence derived by the scientific method. Perhaps the most commonly stated, but least understood, is DNA profiling. This relatively new method is performed for the courts as a technique used by forensic serologists. It is relied upon because of its purported ability to discriminate down to the individual thus replacing other, older, methods like blood typing as a primary evidentiary mechanism. Looking a little deeper DNA analysis, though certainly more reliable than typing alone, is not a panacea. The general assumption is that presenting DNA evidence in court is irrefutable and can therefore not be contested. This supposition is founded upon studies based on population genetics where false positive rates are exceptionally small (i.e. one in billions) or stated another way, a reliance on the probability that the DNA analysis will correctly determine that a defendant was the source of evidence found at the crime scene. However, when statistics that take laboratory practice and data collection factors into consideration are gathered, false positive detection rates range from one per hundred to one per thousand

(Koehler, 1995). This begins to approach the false positive rates for blood typing. This view of DNA evidence seems much more applicable to courts since they are serviced by laboratories like those studied (Koehler). It renders the studies based on population genetics potentially irrelevant since so much error can be interjected by incorrect collection and handling of the DNA source material.

One lesson to be learned is that there is error in every analysis method. There is no doubt that the scientific community has agreed that DNA profiling is very accurate. The question that remains relates to the reliability of any particular test. This same question is a pivotal issue for current and future practitioners in computer forensic analysis. Are bits dropped on the floor during an imaging operation? If so, is there a measurable frequency of that occurrence and is it statistically significant? Are collection tools missing or not reporting exculpatory data? If yes, when, under what circumstances or conditions? Is the algorithm for verifying graphic format missing all ART files? Is it checking file types rather that using a "magic" file to read and verify file headers and trailers? These are but a tiny sample of questions that should be asked and addressed to help understand these complex digital systems and verify the tools and techniques we will use. The point to be made is that error rates in analysis are a fact. They should not be feared, but they must be measured. That is one of the reasons experiments are performed. Until very recently, the scientific community has been conspicuously absent in the development of standards, processes and protocols related to forensic analysis of digital components (CFTT, 2002). This has lead to the court's reliance on precedent rather than statistical significance and repeatability when ruling on admissibility of evidence derived from digital sources. As judges, juries, defense attorneys and asset managers become better schooled in digital technology and understand its complexity more completely, it is likely that we will see the call for a more rigorous approach to analysis. Once this begins decision makers will ask more compelling questions and expect more detailed, scientifically proven explanations from those providing testimony or persuasive argument. This new view of evidence coupled with increasingly dynamic, networked environments will force a paradigm shift. This shift will slowly change law enforcement's use of technology and allow for a wider use of forensic techniques in business, industry, government, and the military. In fact, we have already seen the start of this trend in recent judicial opinions that site the need for more rigorous science as criteria for admissibility (Pollack).

Although viewed, initially, as troublesome, the benefit of adding rigor to the collection analysis and presentation of scientific evidence will result in much higher confidence levels associated with the information presented to all decision-makers including judges and juries. For the digital forensic analyst working in near-real-time environments, it will allow for quicker responses based upon more reliable evidence derived from proven technology grounded in accepted standards. The goal is to produce reliable information that serves to maintain continuity of operations, while at the same time possessing characteristics that make it suitable for presentation in the courts.

Solution Path

The forensic analysis of computer systems, whether it be for the trier-of-fact in the courts or decision makers in business or military operation, has the same goal; persuasion based on factual evidence. The information must be sufficient to help commit a judge and jury to a verdict, or it must help allow a decision maker to change resource allocations or operational goals (and accept residual risk). In the courts, for information to have the opportunity to persuade it must first be admitted. In business and the military decision makers must have confidence in the messenger and the mechanism. At the core they are essentially identical, just called by different names. In general, the information must be:

- Relevant and/or Material: will this information assist the decision maker in his task?
- Credible and/or Competent: is the information believable, trustworthy, true and, if so, by what measure?

Some subset of these characteristics are applied to all information offered to persuade. In the fledgling science of forensic analysis of information systems this is becoming more evident. Whereas the traditional forensic sciences have long established histories and defined laboratory protocols for tests, professional advocacy groups, and university support, computer forensic analysis has only recently come on the scene in response to undefined, illegal use of readily available technology. In a sense, we are where the other disciplines were in the early part of the twentieth century: an evolving scientific discipline, becoming more familiar to the general populace, and searching for measures of accuracy and reliability so as to increase confidence and credibility.

Measures of reliability and accuracy for the techniques and methods used in analysis goes to the level of confidence expected in the evidence and accompanying testimony. Information derived from computer forensic analysis has yet to be contested to any great extent by defense lawyers in judicial proceedings or analysts in investigations of computer misuse. Most techniques used today are assumed plausible if not incontestable because they are developed by reputable companies, used by experts or practitioners in the field, and have been used in courts, or to otherwise persuade authority, before. The techniques themselves and the conclusions they lead to have yet to be tested for reliability in controlled environments under experimental protocols. Strict interpretations of the rules of evidence and court precedence imply that this will soon be necessary if digital evidence is taken to task (Foster 1997, FRE 2000). The complexity evident in digital systems will make this a very difficult road, one that our community of researchers and practitioners should at least be getting ready to travel on soon.

Parting Thoughts

Some of the methods employed by the traditional forensic sciences have much to teach those interested in the new field of computer forensic analysis. Using DNA as an example once again, one can see the cumulative effect of discovery through the years. Johann Meischer's analysis of old bandages in the Crimean War lead to his discovery of

what he called "nuclein" in 1869. Watson and Crick defined the structure of DNA in 1953, which gave researchers a blueprint. Gilbert and Sanger described how to sequence DNA in 1977, which allowed researchers to analyze small parts of the structure. Alex Jeffery found the uniquely human part of the strand in 1985, which made unique comparisons possible. These four distinct events along with hundreds occurring over 116 years represent how scientific discovery works. If we expect computer forensics to join serology in the ranks of proven forensic disciplines, then we should expect similar processes to be at work with strong interaction among academic research, field practitioners, and legal experts.

In the courts, admission and presentation of scientific evidence is guided by established judicial rule and legal precedence. It stands to reason that evidence analyzed from computer systems will, in the near future, be called upon to meet the same exacting standard. So even though we can do binary analysis with hashing algorithms to analyze the very fibers of the computer system itself, it will be the accuracy and reliability of the hash employed that may be called into question. We can claim to use proven correct tools to do an 'autopsy' on a computer system after it has been compromised. The questions will be "Define proven correct?" and "Using what standard?"

These issues only get more complicated as we move from a single host at a physical crime scene to the "virtual crime scene," which consists of networked systems, and devices located anywhere in our infosphere. No matter what the environment, the need for admissible, conclusive evidence will be required and must be collected from all sources available. This includes the subject or compromised host itself, as well as distant firewalls, routers, smart hubs, application gateways, wireless devices, cellular components, deployed agents, and intrusion detection systems. In the near future, the collection, fusion and correlation of data from all these sources and more will be vital to investigations, both civil and criminal. It will be increasingly important that evidence and the methods and techniques used to uncover it are accurate, reliable, and accepted as standard in our field. Coupled with certified expertise, the incorporation of the scientific method is the key to providing forensic evidence or suitable information meant to persuade, whether it is for courts of law, military operations, e-commerce or homeland defense.

References

Eckert, W.G., (1996). Introduction to Forensic Sciences. Boca Raton, FL: CRC Press. LLC.

CFTT, Computer Forensic Tool Testing Program, (2002). Computer Imaging Specification, Version 3.1.6, National Institute of Standards and Technology [on-line]. Available: www.cftt.nist.gov

Foster, K. & Huber, R. (1997). Judging Science: Scientific Knowledge and the Federal Courts, Boston: MIT Press.

FRE, Federal Rules of Evidence (2000). Article VII. Opinion and Expert Testimony, Rule 702 & Rule 703 [on-line]. Available: www.house.gov/judiciary/evid00.pdf

Koehler, J. J., Chia, A. & Lindsey, S. (1995). The Random Match Probability in DNA evidence: Irrelevant or Prejudicial, Jurimetrics Journal, winter: 201-219.

Pollack J. (2002). US District Court, PA: U.S. v Plaza, Acosta (Cr. No. 98-362-10, 11,12) Strengthening the Criteria for Admissibility of Fingerprint Evidence, Judicial Opinion [on-line]. Available: www.paed.uscourts.gov/documents/opinions/02D0046P.htm

About the Author

Gary Palmer (palmerg@mitre.org) works as a Senior INFOSEC Scientist for the MITRE corporation out of Orlando, Florida where he supports the Air Force Research Laboratory (ARFL) programs related to Digital Forensic Analysis, Intrusion Detection and Defensive Information Warfare. Over the last 22 years Gary has worked in the areas of large systems development, integration, database design, software development and information assurance. He is currently lead coordinator for AFRL's Digital Forensic Research Workshop and R&D lead for the CyberForensic Science and Technology Center.

Proving the Integrity of Digital Evidence with Time

Chet Hosmer, President & CEO WetStone Technologies, Inc.

Background

During the latter half of the 20th century, a dramatic move from paper to bits occurred. Our use of digital communication methods such as the world-wide-web and e-mail have dramatically increased the amount of information that is routinely stored in only a digital form. On October 1, 2000 the Electronic Signatures in National and Global Commerce Act was enacted, allowing transactions signed electronically to be enforceable in a court of law. (Longley) The dramatic move from paper to bits combined with the ability and necessity to bring digital data to court, however, creates a critical question. How do we prove the integrity of this new form of information known as "digital evidence"?

Digital evidence originates from a multitude of sources including seized computer hard-drives and backup media, real-time e-mail messages, chat-room logs, ISP records, web-pages, digital network traffic, local and virtual databases, digital directories, wireless devices, memory cards, and digital cameras. The trust worthiness of this digital data is a critical question that digital forensic examiners must consider. Many vendors provide technology solutions to extract this digital data from these devices and networks. Once the extraction of the digital evidence has been accomplished, protecting the digital integrity becomes of paramount concern for investigators, prosecutors and those accused.

The ease with which digital evidence can be altered, destroyed, or manufactured in a convincing way – by even novice computer users – is alarming. To make matters worse, the need to preserve, archive and protect the integrity of digital evidence for long periods of time has arrived, and the methods used today rely on the integrity of individuals, process, procedures, and physical access security. These methods are costly to implement, fraught with potential errors, vulnerable to accidental or malicious modification, and constrain the widespread utilization of digital evidence in crucial litigious procedures.

Fortunately the computer science and information security field has defined what digital integrity is and has contributed a multitude of methods for protecting the integrity of digital data – at least in the general case. Digital integrity can be defined as, "the property whereby digital data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source" (Vanstone et.al. 1997). Applying and adapting methods from computer science and information security to the domain of digital evidence is complex and involves technology, and the expertise and understanding of what it means to prove the integrity of digital evidence. The question then actually is what are we actually trying to prove?

In the simplest case let's assume that we have seized a piece of digital evidence in the form of a floppy disk. At a minimum we would like to prove that the contents of the floppy disk (the digital data) have not been altered in any manner from the moment that

we seized the disk. We need to be able to prove this fact many years after the evidence was originally seized, independent of those involved in the original seizure.

Proving the Integrity of Digital Evidence Today

To date, several methods have been adapted from the computer science and information security to the domain of digital evidence. The table below illustrates the method, advantages and disadvantages of each.

Method	Description	Common Types	Advantages	Disadvantages
Checksum	A method of checking for errors in digital data. Typically a 16- or 32-bit polynomial is applied to each byte of digital data that you are trying to protect. The result is a small integer value that is 16 or 32 bits in length and represents the concatenation of the data. This integer value must be saved and secured. At any point in the future the same polynomial can be applied to the data and then compared with the original result. If the results match some level of integrity exists.	CRC 16 CRC 32	⇒ Easy to compute ⇒ Fast ⇒ Small data storage ⇒ Useful for detecting random errors	⇒ Low assurance against malicious attack ⇒ Simple to create new data with matching checksum ⇒ Must maintain secure storage of checksum values ⇒ Does not bind identity with the data ⇒ Does not bind time with the data
One-way hash algorithm (MD2, MD4, MD5, SHA	A method for protecting digital data against unauthorized change. The method produces a fixed length large integer value (ranging from 80 – 240 bits) representing the digital data. The method is said to have one-way ness because it has two unique characteristics. First given the hash value it is difficult to construct new data resulting in the same hash. Second given the original data it is difficult to find other data matching the same hash value. (Schneier)	SHA-1 MD5 MD4 MD2	⇒ Easy to compute ⇒ Can detect both random errors and malicious alterations	⇒ Must maintain secure storage of hash values ⇒ Does not bind identity with the data ⇒ Does not bind time with the data
Digital Signature	A secure method of binding the identity of the signer with digital data integrity methods such as one-way hash values. These methods use a public key crypto-system where the signer uses a secret key to generate a digital signature. Anyone can then validate the signature generated by using the published public key certificate of the signer. The signature produces a large integer number (512 – 4096 bits)	RSA DSA PGP	⇒ Binds identity to the integrity operation ⇒ Prevents unauthorized regeneration of signature unless private key is compromised	⇒ Slow ⇒ Must protect the private key ⇒ Does not bind time with the data ⇒ If keys are compromised or certificate expires digital signature can be invalidated

Adding Time to the Equation

Using the best practices afforded us today – digital signatures – we are able to successfully bind "who" (the signer) with the "what" (the digital data). However, digital signatures have shortcomings that leave two critical questions unanswered:

1. When did the signing of the digital evidence occur? How long after the evidence was seized, was its integrity protected?
2. How long can we prove the integrity of the digital evidence that we signed?

For both of these questions, time becomes a critical factor in proving the integrity of digital evidence. We need to determine how we can bind time, and more importantly, a trusted source of time to digital evidence. To understand this we first must understand a little about time itself and what is necessary if we are to trust that it is accurate.

From ancient societies to the present day, time has been a function interpreted in many ways. Time essentially is an agreement that allows society to function in an orderly fashion – where all parties are able to easily understand the representation. Examples of time measurement include:

- Earliest calendars were based on the moon because everyone could easily agree on this as a universal measure of time. The Egyptians were the first to understand the solar year and develop a calendar based on the rotation of the earth around the sun. The calendar we use today uses this solar basis to arrive at the number of days in the year.

- In 1582, Pope Gregory XIII introduced his calendar, which is the calendar used today and referred as the Gregorian Calendar.

- In 1967, an international agreement defined the unit of time as the second, measured by the decay of Cesium using precision instruments known as atomic clocks.

- In 1972, the Treaty of the Meter (established in 1875) was expanded to include the current time reference known as Coordinated Universal Time (UTC), which replaced Greenwich Mean Time (GMT). More than forty countries running a collection of over two hundred atomic clocks administer UTC. This is where the time reference originates, enabling government entities to establish their respective "national time."

Establishing the "when" of an event in the emerging digital world necessitates new agreements on how time is used. Time as a quantified value is used in nearly all aspects of commerce and security in order to bind validity, grant access, and reconstruct the order of events. In manual systems, an authorized individual, such as a notary, can attest to the date-time of a transaction based upon some standard practice. Notarization, in particular, can provide three valuable time services: an accurate date from an authoritative source, a

certification that the date supplied applies to the transaction in question, and a format that can be verified by disinterested or trusted third parties under a broad range of circumstances.

Secure and Auditable Time

This problem has created an opportunity to establish a new standard of secure and auditable time stamps that are represented electronically. In the course of the past two years many providers and users of digital signature technologies have begun to understand the importance of using the same rigor in authenticating the source of the time as they have with authenticating an individual.   This process utilizes the same types of public key infrastructure processes used by Certificate Authorities and combines this with the official world sources of time.

This approach is able to secure the time stamp and simultaneously provide the evidentiary trail of the time source within the time stamp. Once you have created a time stamp that is resistant to manipulation and provides an authenticated audit trail you can electronically "bind" these secured date/time stamps to digital evidence so that they can be verified by a third party.

Ideally then, "secure, auditable digital date/time stamps" will have the following attributes:

- **Accuracy**. The time presented is from an authoritative source and is accurate to the precision required by the transaction, whether day, hour, or millisecond.

- **Authentication**. The source of time is authenticated to a National Measurement Institute (NMI) timing lab so that a third party can verify the precision and accuracy of the time.

- **Integrity**. The time should be secure and not be subject to corruption during normal "handling."   If it is corrupted, either inadvertently or deliberately, the corruption should be apparent to a third party.

- **Non-repudiation**. An event or document should be bound to its time so that the association between event or document and the time cannot be later denied.

- **Accountability**. The process of acquiring time, adding authentication and integrity, and binding it to the subject event should be accountable, so that a third party can determine that due process was applied, and that no corruption transpired.

Adding secure and auditable time to digital evidence eliminates the potential for fraud and unintended errors. The use of secure date/time stamps can not only improve the integrity of digital evidence, but also can provide higher assurance required for digital chain of custody. Quite simply, using secure and auditable time ensures that any

important electronic event has a time stamp that cannot be corrupted and has an evidentiary trail of authenticity.

Proving the Integrity of Digital Evidence with Time

In order to effectively use digital evidence to prove the motive, opportunity and means of cyber-criminals we must:

- Significantly advance the accuracy and trust of digital time.
- Digitally bind this trusted electronic time with digital data and computer events on a routine basis.
- Make the process routine, ubiquitous and standardized throughout the digital world.
- Make this trusted electronic time traceable to a legal time source(s).

The steps are:

Step 1: Traceability to Legal Time Sources

Since 1972 over 40 countries throughout the world have adopted Coordinated Universal Time or UTC as their official time source. This agreement between nations has resulted in a stable source of time that we can all agree upon. In order for the time of digital evidence to be considered trusted we must be able to trace any digital timestamp back to at least one of the UTC time sources in the world.

Step 2: Time Distribution

The secure distribution and traceability of time from these UTC sources is certainly a significant undertaking but a necessary one if we are to effectively bind meaningful time with digital events. The solution we arrive at must provide continuous audit and provable traceability to UTC sources. This solution must be resistant to attack, malicious or accidental altering of critical time sources and denial of service.

Step 3: Secure Digital Timestamping

The secure issuance of timestamps for digital evidence has at least these critical components.

1. First the binding of time with digital data must occur itself within a trusted computing environment in order to assure the efficacy of the time stamping process.
2. The accuracy of the clock used as the source for time stamping should be appropriate for the application. For example, the accuracy of a timestamp denoting access to a secure facility through the use of a card access or biometric device of 30 seconds may be reasonable. However, the time stamping of an electronic stock transaction or money transfer may require a finer resolution.

3. The calibration and audit of the local trusted clock used as the source for time stamping must be routine, continuous and traceable. Furthermore, a trusted, disinterested 3rd party must be relied on to accomplish this calibration and audit of such clocks.
4. The validation of the resulting timestamps must be verifiable by issuer and by any party that has the need to evaluate the accuracy, validity, trust-worthiness or traceability of a timestamp.

Summary

Proving the integrity of digital evidence with time offers significant advantages over existing best practice methods. We can now bind for the first time the "who" (the identity of the signer), the "when" (the time the signing took place) and the "what" (the digital data we are trying to protect). This new digital integrity mark will allow us to prove the integrity of digital evidence today and in the future. We hope that this new level of protection for digital evidence will advance the collection, preservation, and use of digital evidence.

References

Hosmer, C., (2001). The Importance of Binding Time to Digital Evidence. Paper presented at the 12th Annual Economic Crime Investigation Institute Conference, McLean, VA.

Hosmer, C., (1998). Time-Lining Computer Evidence. Paper presented at the IEEE Information Technology Conference.

Hosmer, C., Feldman, J., & Giordano, J., (1998). Advancing Crime Scene Computer Forensics Techniques. Paper presented at the SPIE's International Symposium on Enabling Technologies for Law Enforcement and Security Conference.

Hosmer, C., (1998). Using SmartCards and Digital Signatures to Preserve Electronic Evidence. Paper presented at the SPIE's International Symposium on Enabling Technologies for Law Enforcement and Security Conference.

Longley, R. (2001). E-Sign – Be Careful What You Ask For.   U.S. Gov Information Resource [On-Line]. Available: http://usgovinfo.about.com/library/weekly/ aa072300a.htm.

Schneier, B. (1996.) Applied Cryptography (2nd ed.), John Wiley & Sons.

Vanstone, S., van Oorschot, P., & Menezes,A. (1997) Handbook of Applied Cryptography. CRC Press.

WetStone Technologies, Inc. (2001) Sovereign Time© Providing the "When" for the Electronic World. Unpublished manuscript.

About the Author

Chet Hosmer (chet@wetstonetech.com) is a co-founder, President and CEO of WetStone Technologies, Inc. He has over 25 years of experience in developing high technology software and hardware products, and during the last 11 years, Chet has focused exclusively on information security technologies. This focus has resulted in technology innovations in secure time stamping, steganography, network and host based intrusion detection systems, digital watermarking and digital forensics.

Chet is a co-chair of the Technology Working Group, one of the seven working groups of National Cybercrime and Terrorism Partnership Initiative sponsored by the National Institute of Justice. He is also the Research Advisor of the Computer Forensics Research and Development Center (CFRDC) of Utica College and serves on the Board of Directors for the Economic Crime Investigation Institute. Chet is a member of IEEE and the ACM, and holds a B.S. degree in Computer Science from Syracuse University.