



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

Paul CLAASSEN
GSEC Practical Paper
Assignment Version Number 1.4 Option 1

© SANS Institute 2000 - 2002, Author retains full rights.

First Responders: Training Scene of Computer Crime Investigators

Paul Claassen

June 5, 2002

Abstract

In order to meet the ever increasing need for trained personnel who can intervene quickly and effectively to an unauthorized use of computer incident, IT departments, law enforcement agencies, or those individuals responsible for computer security can maximize their chances of ensuring a timely and effective response by providing training sessions for selected candidates. Having a trained cadre of “first responders” who can perform the initial procedures designed to protect, seize and transport evidence to forensically trained personnel will enhance the chances of effectively pursuing any investigation relating to unauthorized computer use.

This paper presents two components of a training curriculum: the Course Training Standard through which the outline of the goals, objectives, delivery and testing are presented for upper management approval; and a sample Course Training Package which can be utilized as a template.

Note: this paper is law-enforcement oriented. However, wherever possible, generic wording and situations are utilized in order to make the material relevant to all IT practitioners. Also, this paper does not address the complicated world of networks. It focuses on providing practical training to personnel with limited computer knowledge or background but who nevertheless need to search and seize computer systems for evidentiary purposes.

Course Training Standard (CTS) Component

A Course Training Standard serves as a guideline for the construction of approved training programs involving specific subjects. The Standard is precisely that, a yardstick by which curriculums are evaluated. By adhering to a consistent standard, organizations can deliver a consistent quality of teaching. The Standard also helps ensure upper management “buy in” and will therefore receive recognition, support and (hopefully) course funding.

If your organization does not as yet possess a Course Training Standard, the following section will help focus on the key components necessary to meet the needs of a comprehensive policy. One of the clearest and easiest understood CTS outlines currently available on the Internet can be found online at <http://www.rcmp-learning.org/docs/ecdd0010.htm>. This Standard reflects the policies and procedures

followed by the Royal Canadian Mounted Police in designing their various training courses and programs. It provides a good starting point for designing a personalized version and as such serves as a guide for what good CTSs should contain.

[There are several other online resources available as well which provide useful information and guidelines on curriculum development. The following link is short and easy to read. If curriculum development is new or perhaps intimidating, check out: http://dce.unm.edu/familycommunity/training_support/guidelines_CD.htm]

From this document we find that in order to properly prepare a training course, the following aspects of the anticipated training should be addressed, including:

1. Title Page
2. Table of Contents
3. Guidelines for Using a CTS
4. Purpose of Course
5. Candidate Selection Criteria
6. Course Description
7. Delivery Method
8. Testing
9. References
10. Course Evaluation
11. Evaluation Plan
12. Course Syllabus and Timetable

By providing all this information in a formal proposal, management can assess the validity of the material and thought process behind the anticipated training. With approval from this point, the training will receive the backing and resources needed to adequately meet the objectives outlined in the original plan.

The following is an analysis of each of the outline points and suggests how to develop them further where needed. Note that there may not be a need to include every sub-topic in the CTS. Organizational needs will dictate what is required and what can be left out.

1. The Title Page is self-explanatory and will vary from organization to organization.
2. The Table of Contents depends on the length and detail of the CTS. It again is self-explanatory.
3. Guidelines for Using a CTS deals with what the various layers of managers and trainers are responsible for, including setup of the course, training the trainers, providing resources and equipment, and dealing with the issue of course evaluations and critiques in order to make the course better over time. Again, this portion of the CTS will be unique to each organization creating it. This guideline will not be included in the provided sample due to its uniqueness.

4. The Purpose of the Course begins to look at the meat of what will be taught. It should outline the key knowledge and skills the course candidate will come away with at the conclusion of the training session.
5. Candidate Selection Criteria is an important consideration. Every organization has a different resource base upon which to draw and build upon. Perhaps the most important aspect of determining this criterion is the minimum level which can be effectively accommodated. It may be the case that there really are no individuals currently employed which can meet the minimum standard required in order to receive this training. If that is the case, preliminary groundwork must be undertaken to bring selected individuals up to this level prior to initiating this training, otherwise the integrity of this training can, and will, be brought into question.
6. Course Description is a brief, general description and summation of what the parameters of the training will be including the length, location, number of candidates, and any pre-reading or studying that may be required.
7. Delivery Method outlines the main teaching strategy to be used by the trainer to accomplish the objectives of the course. It should indicate that a variety of methods will be used including lecture-based content, hands-on practical applications, and on-going questions and answer techniques. This variety of teaching methods will help ensure subject material mastery by the candidates. Remember that doing something is far more effective than merely hearing about it or seeing it done for you.
8. Testing addresses the need for an objective measuring device whereby the candidate's mastery of the subject material will be determined. The type and form of the testing method(s) should be explained and the passing criteria should be established from the outset of the course. The wider the variety of testing methods, the greater the validation of the candidates' knowledge of the course material and also the less dependency on handicapping those individuals who learn in different ways (some are more visually orientated and others more practical/hands-on orientated).
9. References help provide both the theoretical and practical frameworks upon which the course is built. Although there may be some benefit to re-inventing the wheel, the best use of time and resources lies in building on foundations established by others who have already explored the area being addressed. Fortunately, there does not appear to be any shortage of research and effort in the areas of either training or in the fundamentals of Computer Crime Scene Investigation.
10. Course Evaluation deals with three different aspects of evaluating this particular course's effectiveness. At the classroom level, ongoing feedback from course candidates is received by the trainer through the means of in-class questions and answer, other verbal interaction, and also through non-verbal observations. It is at this level that the skill of the instructor truly reveals itself. Adaptability, a sense of humor, knowledge of a variety of communications approaches, and mastery of the course content itself are crucial to the successful teaching of any course. It is at

this level that the candidates are liable to succeed or fail in their attempts to master the course material. The second level of course evaluation rests with the candidates themselves. Soliciting course feedback and having the candidates complete course evaluation forms helps provide the instructor with, preferably, anonymous suggestions for future course improvements and training needs from the perspective of the candidates. The final evaluation occurs when the training received by the candidates is tested out in the field, in a real-life situation. At this time the developer of the course can undertake to evaluate where any shortcomings may exist or what should be added in order to more fully round-out the training in this area. It is here also, where future course proposals can be initiated and prepared in order to build on what is now (hopefully) a successful program.

11. The Evaluation Plan component builds on the Course Evaluation and elevates the course assessment to the management level. At this point, the procedure for evaluating the program from the organization's perspective should be proposed. Questions such as: is the course both resource and time effective?, is it practical?, what is the success rate of both the candidates in the classroom and their results out in the "real world"?, and finally, can we do without this program?, all need to be addressed. To ensure an objective answer to these important questions, the Evaluation Plan proposes what the "Indicators of Effectiveness" are and supports those indicators by listing who will undertake the program assessment and what should be covered in the assessment. This should be realistic and relatively simple to accomplish, otherwise it will not be done and the program may suffer in the long term. Management buy-in is crucial for the ongoing success of training initiatives.
12. Course Syllabus and Timetable is the breakdown of the program into its time-managed pieces. Here is the heart of the course. With a proper outline of what will be covered and within what teaching framework, any knowledgeable and qualified instructor should be able to step in at any point in the course and pick up where another left off. This is where the Lesson Plan originates from and where micro-management is a good thing!

With a carefully researched and crafted course submission based on the preceding guidelines, the foundation for an effective course should be sufficiently solid to enable rapid management approval.

Sample Course Training Standard

The following is offered as a sample Course Training Standard as it is applied to the topic: Training Scene of Computer Crime Investigators. As stated earlier, the Title Page is largely subjective and should be designed with the needs and format requirements of each organization in mind. As such, it is not included in this sample.

Reminder: As stated in the Abstract above, the sample CTS presented below reflects a training program from a police officer/law enforcement perspective. As such it encompasses training related to Search Warrants in addition to the other practical aspects of seizing and searching computer systems. Furthermore, the search and seizure of networked computer systems is not addressed due to the vast range of possible scenarios an investigator may encounter when dealing with this sort of situation. Again, the target group for this training is relatively unsophisticated users who have a need for this program.

There are of course many other approaches to training first responders. For another perspective, the following online site provides an excellent outline of a course developed for the purpose of recognizing “The Personal Computer as Evidence”. It is particularly strong in identifying measurable performance objectives and as a result everyone can plainly see what the final result of the training should be:

<http://www.computerforensics.net/copgoals.htm>

After the completion of the sample CTS, a sample Lesson Plan with PowerPoint™ slides will be presented as a suggested starting point for a training course.

© SANS Institute 2000 - 2002, Author retains full rights.

Scene of Computer Crime Investigator's Training Course**Table of Contents**

Title Page	i
Table of Contents	ii
Purpose of Course	1
Candidate Selection Criteria	1
Course Description	2
Delivery Method	2
Testing	2
References	3
Course Evaluation	3
Evaluation Plan	4
Course Syllabus and Timetable	4

© SANS Institute 2000 - 2002, Author retains full rights.

Scene of Computer Crime Investigator's Training Course

Purpose of the Course

This course is designed to provide members with both the theoretical and practical knowledge of how they can effectively find and seize evidence related to the unlawful use of computers. This course will also provide the basic understanding and knowledge of Search Warrant requirements.

Successful candidates on this course will be able to:

- A. Make an accurate assessment of the urgency of a given situation as it relates to the destruction of evidentiary data.
- B. Identify the key requirements for a successful Search Warrant and utilize generally acceptable and provided wording in a Warrant drafted by the member.
- C. Conduct a thorough search of a given location and identify the key and necessary components of a computer system.
- D. Seize all relevant devices and data storage media related to the investigation in question.
- E. Safely package, store and transport seized evidence to a designated location for further analysis when required.
- F. Articulate the key evidence required to pursue the successful prosecution of a suspect.
- G. Clearly understand the court and evidentiary issues surrounding the successful prosecution of a suspect as it relates to the illegal use of computer systems.
- H. Identify special situations where the investigator may be able to undertake a more active role in the examination of evidence or where the investigator recognizes the need to call in experts to deal with the scene.

Candidate Selection Criteria

Candidates for this course should be members who have either already investigated occurrences of illegal activity involving the use of computers or who have expressed an interest in such investigations either through the taking of courses, assistance to others involved in ongoing investigations, or through contact with training and/or technological crime section members.

Course Description

This half-day (four hour) course is designed to meet the needs of organizations and jurisdictions where the incidences of computer crime investigations are increasing beyond the ability of dedicated investigational resources to respond to the demands for service. The objective of this training is to produce members who are capable and eager to assist in the investigation of illegal computer use.

Delivery Method

The participation of candidates is essential to every aspect of this course. The format of the course utilizes a combination of lecture style delivery of information along with practical demonstrations coupled together with candidates' hands-on participation in simulated search environments and scenarios. Considerable emphasis is placed on problem solving and dealing with unique situations in a rapidly-changing environment.

Testing

Two primary means of testing the candidates' knowledge will be used:

1. Skill display, and
2. Written Examination

Both of these components are vital to ensuring that candidates passing the course possess the theoretical knowledge and understanding of what they are searching for and subsequently seizing, and also the ability to properly document, prepare and transport exhibits for further specialist processing.

Specific examination marks will remain confidential and candidates will be advised only as to whether they have passed or failed the course requirements. The instructor will review the examination questions with the candidates at the conclusion of the marking so that weaknesses or errors may be addressed and to provide the candidates the opportunity to raise concerns or issues with any of the techniques and/or theory taught.

[A note with regard to testing: the time has long since passed when testing a candidate in fact tested his/her ability to remember trivia and/or to "regurgitate" what the teacher/instructor said. In the Information Society in which we now live, the amount of knowledge and raw data far outstrips the ability of almost everyone to memorize, let alone understand, the full depth of almost any given subject. It is incumbent upon course designers to be totally up front with course candidates and tell them right from the beginning of class what they need to know and what they will be tested on. There are no

secrets. The objective is to teach what must be learned, and to test that knowledge. If everyone passes with 100%, great! If everyone fails, then there is a systemic problem which needs to be addressed. In this case either the instructor failed, the material was too difficult, or the candidates lacked the foundation upon which to base the new course material. In any event, the objectives and testing of those objectives must be revisited and rethought.]

Course References

[The following are examples – add to them as required and as utilized by yourself or organization.]

U.S. Department of Justice., Electronic Crime Scene Investigation – A Guide for First Responders., July 2001 <http://www.ncjrs.org/txtfiles1/nij/187736.txt>

Canadian Police College., Notes and course material from Electronic Search and Seizure Course., October 1999

Course Evaluation

Upon completion of course training and candidate evaluation, a formal standardized course evaluation form should be completed by each course candidate. The questions asked by the evaluation are unique to each organization administering the course, but should solicit feedback from the following general areas:

- A. Effectiveness of the Instructor
- B. Applicability of Course Content to Real World Situations
- C. Identification of Most Relevant Material
- D. Identification of Least Relevant Material
- E. Any Area That Needs Improvement
- F. Any General Overall Comments or Suggestions

The value of this feedback mechanism lies in the ability to tune the course for future candidates in such a way as to enhance the value and effectiveness of the material. This is an important and necessary aspect of the learning cycle and should not be omitted or overlooked.

Further evaluation of the course occurs when candidates utilize the material and concepts learned in their day-to-day duties. As the techniques are used in the field, a method of monitoring the success and (hopefully) few inevitable failures should enable the “tweaking” of course material to meet the needs and issues which arise in the real world. This monitoring can take place through the implementation of the Evaluation Plan included in the next section.

Evaluation Plan

In order to determine whether training/learning is achieving its objectives of improving or maintaining a standard of job performance, indicators of effectiveness are identified when a course is designed. These indicators are used to assess both course quality and the impact of training/learning on the job performance.

Indicators of effectiveness for the Scene of Computer Crime Investigator's Training Course are:

1. Positive assessments of graduate's performance with drafting of appropriate Search Warrants and the subsequent search and seizure of computer systems from noted locations.
2. The assessment of the confidence level of the graduate when dealing with a computer search and seizure.
3. The graduate's successful resolution of computer crime related investigations in court.

These indicators will be monitored either by the graduate's immediate supervisor, a qualified instructor of the course, or by a member of a dedicated technological crime investigational unit. This evaluation should take place fairly regularly initially after the implementation of the training course (its pilot phase) and then as required in order to obtain an accurate picture of future course and development needs.

Course Syllabus and Timetable

The following timetable should meet the general needs for training in this area:

<u>Time</u>	<u>Objective</u>
0800	Course Orientation <ul style="list-style-type: none"> - opening address, introductions, objectives & purpose - testing procedures, teaching method, administration
0815	Computers as Tools to Commit Crimes <ul style="list-style-type: none"> - types of crimes, types of tools (programs) Computers as Data Storage Devices <ul style="list-style-type: none"> - principles of data storage, concept of RAM - removable media as storage, what to look for
0900	Computer Crime Investigation <ul style="list-style-type: none"> - importance of time, determination of urgency - Search Warrant requirements, expectation of privacy - drafting ISP Warrants, residence Warrants
1000	Break

1015	Hands On Examination and Seizure of Hardware Components <ul style="list-style-type: none">- do's and don'ts, what to look for- importance of documentation and proper storage Transportation of Evidence <ul style="list-style-type: none">- how to get exhibits intact to forensic lab
1100	Forensic Analysis <ul style="list-style-type: none">- general overview of procedure- importance of providing descriptors Court/Evidentiary Issues <ul style="list-style-type: none">- notes, chain of evidence, integrity of original exhibits- forensic analysis report – what it says
1115	Special Situations <ul style="list-style-type: none">- networks, encryption, e-mail
1130	Exam <ul style="list-style-type: none">- administer, mark and review exam
1150	Course Evaluation <ul style="list-style-type: none">- candidate feedback
1200	Lunch – Finish

Lesson Plan - PowerPoint™ Slides

The following screenshots are provided as a template upon which to build a personalized course lesson plan. By adhering to the timetable above and by utilizing the following slides, this sample course for **Training Scene of Computer Crime Investigators** is yours to add to, modify, or delete as needed. Each slide contains notes or annotations accompanying it, as deemed appropriate.

There is a very good online guide which can help the lesson designer with the task of setting up an effective plan for teaching any given subject. This site can be found at: <http://www.su.edu/faculty/jcombs/effect/sld001.htm> and additional details from the same author, Dr. Jurgen Combs, can be found at: <http://www.su.edu/faculty/jcombs/lesson%20plans/comless.htm>. Effective lesson plan design is actually part art and part science, and therefore requires the careful blend of matching material to delivery methods.



Touch on each of the points noted above and explain how they relate to the course. (This material is based on the information contained in the CTS.)

Computers as Tools

- Traditional Crime Using New Technology
 - Fraud
 - Counterfeiting
 - Threats
 - Pornography
- New Computer-specific Crimes
 - Denial of service attacks
 - Web services
 - Trojans, Viruses

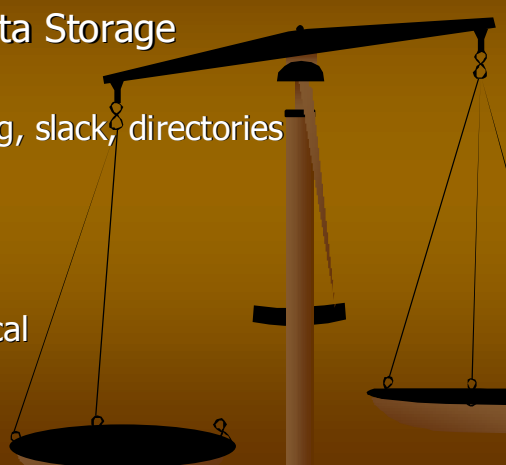


5/24/2002 Computer Crime Investigations Unit 3

All of this information (and all of the following as well) should be second nature to the instructor.

Computers as Storage Devices

- Principles of Data Storage
 - RAM
 - Reading, writing, slack, directories
- Media Types
 - Fixed
 - Removable
 - Magnetic, Optical



5/24/2002 Computer Crime Investigations Unit 4

The importance of providing this basic background material lies in making the candidate aware of the sensitive physical nature of the storage media, and to recognize that valuable information may be contained on any type of removable or fixed material.

Crime Scene Investigation

- Determine Urgency
 - Establish what must be found or preserved
 - Verify who owns the evidence and who has had access to it
- Determine any Civil Liability Issues
 - Consider disruption level of search
 - Be conscious of potential lost income to business/office environments due to removal of evidence

5/26/2002 Computer Crime Investigations Unit 5

Refer to the provided Investigator's Checksheet following the slide presentation. This will cover the basic information needed by a first responder and provide a handy means of ensuring complete and accurate notes are taken at the scene of an incident.

Crime Scene Investigation continued...

- Search Warrants
 - Voluntary Consent to Search/Seize
 - General/Special Warrants
- Warrant Crafting
 - Wording
 - Items to be searched for, ISPs, residences, businesses

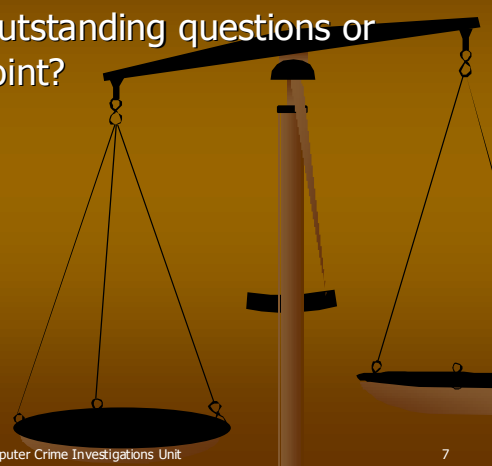
5/24/2002 Computer Crime Investigations Unit 6

For this training segment, a DA or crown prosecutor would be an ideal resource person to have on hand. Barring that, a seasoned investigator capable of producing examples and a "war story" or two would be very effective. Some general information on warrants and their legality can be found at:

<http://www.usdoj.gov/criminal/cybercrime/searchmanual.htm>

Break

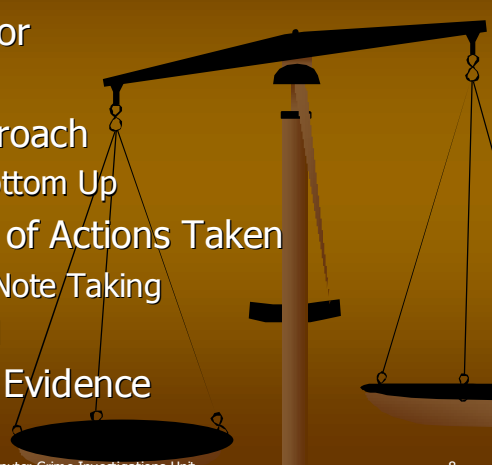
- Are there any outstanding questions or issues to this point?



5/24/2002 Computer Crime Investigations Unit 7

Seizing Computer Systems

- What to Look For
 - Scene analysis
- Methodical Approach
 - Perimeter or Bottom Up
- Documentation of Actions Taken
 - Importance of Note Taking
 - What to Record
- Preservation of Evidence



5/24/2002 Computer Crime Investigations Unit 8


What to Look For:

(Note: this, and the following slides make extensive use of the Electronic Crime Scene Investigation – A Guide for First Responders publication which can be found at:

<http://www.ncjrs.org/txtfiles1/nij/187736.txt>).

Transportation of Evidence

- Storage of Media and Components
- What Should be Transported
- Chain of Custody Issues
- PRACTICE – HANDS ON




5/24/2002 Computer Crime Investigations Unit 9

At this point in the course, every candidate should be exposed to a variety of computer hardware devices including everything from the box/CPU to various storage media. Examination of this hardware is essential for grasping the concepts of data sensitivity, volatility and variety. Proper packaging and storage and transportation issues should also be addressed.

Forensic Analysis

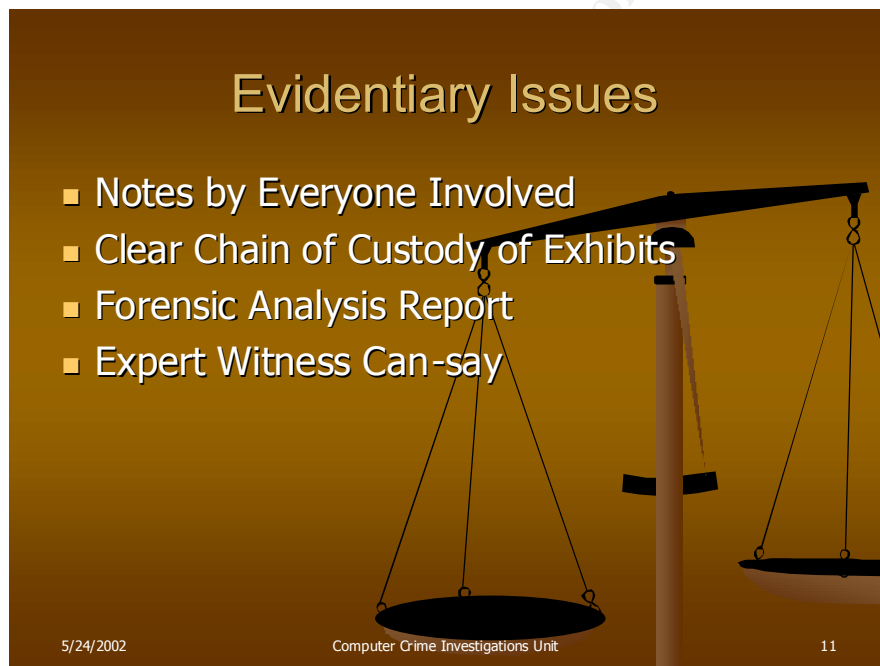
- General Procedure Overview
 - Methodology
 - Objectives
- Role of the Analyst
 - Expert Witness
 - Resource Person
- Role of the Investigator
 - Provides Overview of Investigation
 - Requests Specific Service From Analyst



5/24/2002 Computer Crime Investigations Unit 10

This course does not focus on forensics, but an introduction to what the methodology and examination entails should provide a useful insight into what can and cannot be obtained via a forensic examination. For details and additional information, the following online sites provide a good starting point for the basics of computer forensic analysis:

www.cops.org/forensic_examination_procedures.htm#Forensic%20Examination%20Procedures (IACIS site), <http://computerforensics.net/forensics.htm> (A basic “Explanation of Computer Forensics” by Judd Robbins. He touches on what role the analysis plays in the judicial system.)



Evidentiary Issues

- Notes by Everyone Involved
- Clear Chain of Custody of Exhibits
- Forensic Analysis Report
- Expert Witness Can-say

5/24/2002 Computer Crime Investigations Unit 11

The two page checksheet provided on the next pages highlights the important information which should be recorded at the start of a search. It can be changed to reflect the needs of individuals or organizations as required.

Computer Search & Seizure Investigator's Checksheet

File Information

Primary Investigator: _____ Telephone: _____
File Number: _____ Exhibit Report Number: _____
File Caption: _____

Search Location Information

Date: _____ Time: _____

Name(s) of Searcher(s): _____

Location Address: _____

Location Type: ☐ Residence ☐ Business ☐ Professional Office

Owner(s) of Premises: _____

Owner of Item(s) to be Searched For: _____

Primary User: _____ Passwords: _____

Other: _____ Passwords: _____

Other: _____ Passwords: _____

Search Authorized by: ☐ Warrant ☐ Voluntary Consent ☐ Other

Seizure of Exhibits

Note – Officer and Scene Safety First! Secure exhibits ASAP!

Brief Description of Exhibit Environment:

State of Computer System: ☐ On – Active Program(s): _____ ☐ Off

Photos Taken: ☐ Yes - Name of Photographer: _____ ☐ No

Key Items: ☐ Computer box/laptop
☐ Data Storage Media (includes: floppies, zip, burned CDs)
☐ Written or printed documents (includes: e-mails, contacts, passwords)

Secondary: ☐ PDA ☐ Pager/Cell phone ☐ Other _____

Exhibit Report Items Seized at the Scene

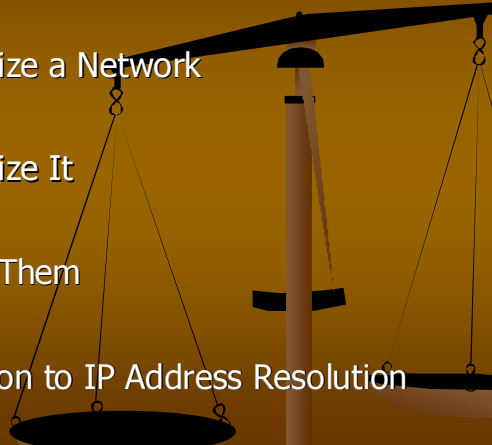
Item #	Item Description			
	Seized by			
<u>Unique ID</u>	<u>Make</u>	<u>Model</u>	<u>Serial #</u>	<u>Seized by:</u>
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

Record movement of exhibit details if subsequently transported to another location (i.e. for Forensic Analysis).

Special Situations

- Networks
 - How to Recognize a Network
- Encryption
 - How to Recognize It
- Passwords
 - How to Obtain Them
- E-mail Tracing
 - Brief Introduction to IP Address Resolution

5/24/2002 Computer Crime Investigations Unit 12




The amount of coverage given to these topics depends on several factors: remaining time, candidate interest, and/or candidate “need to know”. These topics deal with more advanced themes and really serve to introduce complexity into an otherwise basic level of needed knowledge and instruction. Pick and choose as required by the organization’s training needs.

Exam

- Format
- Time Limit
- Pass/Fail Result

5/24/2002 Computer Crime Investigations Unit 13

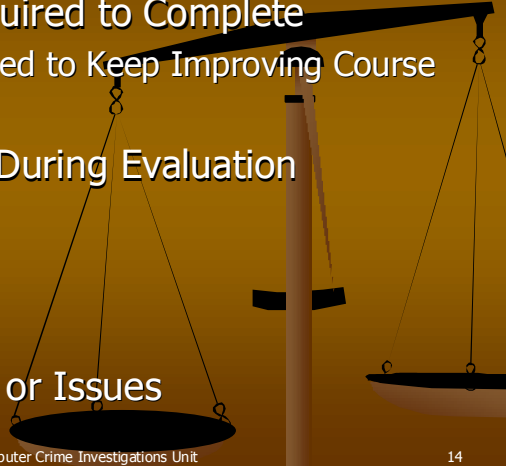


The exam should cover only the material taught and should ensure that the objectives laid out at the start of the course have been met. The format of the exam can consist of: multiple choice, short answer, fill-in the blanks, or any combination thereof. Every exam is unique to the organization or individual putting on the course.

Course Evaluation

- Candidates Required to Complete
 - Feedback Needed to Keep Improving Course
- Exams Marked During Evaluation
- Exam Review
- Final Questions or Issues

5/24/2002 Computer Crime Investigations Unit 14



Course feedback questionnaires are unique to each organization or individual teaching the material. The primary objective of soliciting candidate feedback is to help improve the content and flow of presentation for the next group of candidates.

Thanks For Attending!

- Contacts:
 - Course Instructor:
 - Training Section:
 - Emergency:

5/24/2002 Computer Crime Investigations Unit 15



Conclusion

Training “First Responders” to effectively and efficiently attend various scenes of computer crimes is a daunting yet necessary task. Individuals and organizations responsible for these duties require trained, or at least “informed”, technically savvy individuals to assist in the ever-increasing demands for their time. In order to facilitate the offloading of some of the simpler investigative steps, a short but comprehensive training session can enhance the abilities of eager or designated candidates to complete the initial stages of an investigation in a legally sound manner.

By preparing a comprehensive Course Training Standard and producing an accompanying Lesson Plan, individuals or departments responsible for conducting training sessions will be in a better position to obtain management approval for whatever training needs they may have. With a plan in place and support for the program, the task of meeting the training and educational needs of both employees and the organization will be made much simpler.

List of References

Anonymous. Maximum Security, Third Edition. Indianapolis: SAMS, 2001.

Combs, H. Jurgen. “Lesson Plan Design”. Complete Lesson Plan. Updated June 23, 1999.

URL: <http://www.su.edu/faculty/jcombs/lesson%20plans/comless.htm> (June 2002)

Combs, Jurgen. “Effective Lesson Plan Design”. PowerPoint™ Presentation format. February 20, 1997.

URL: <http://www.su.edu/faculty/jcombs/effect/sld001.htm> (June 2002)

Galil, Yair. “New Federal Guidelines for Searching and Seizing Computers – from servers to PDAs. The Internet Law Journal. Updated February 5, 2001.

URL; www.internetlawjournal.com/content/litigationheadline02050102.htm (June 2002)

GRC-RCMP. “Guidelines for Developing a Course Training Standard”. Ecdp0010.doc Revised June 4, 1998.

URL: <http://www.rcmp-learning.org/docs/ecdd0010.htm> (June 2002)

International Association of Computer Investigative Specialists. “Forensic Examination Procedures”. Forensic Procedures. Modified April 7, 2002.

URL: www.cops.org/forensic_examination_procedures.htm#Forensic%20Examination%20Procedures (June 2002)

Mandia, Kevin. & Proise, Chris. Incidence Response – Investigating Computer Crime. Berkeley: Osborne/McGraw-Hill, 2001. 92-94

National Institute of Justice. “Electronic Crime Scene Investigation: A Guide for First Responders”. NIJ Guide. July 2001.

URL: <http://www.ncjrs.org/txtfiles1/nij/187736.txt> (June 2002)

Robbins, Judd. “An Explanation of Computer Forensics”.

URL: <http://computerforensics.net/forensics.htm> (June 2002)

Robbins, Judd. “Goals and Objectives for The Personal Computer as Evidence Course”.

URL: <http://www.computerforensics.net/copgoals.htm> (June 2002)

StevensDominguez, Meave. “Some General Guidelines for Curriculum Development”. Last changed September 8, 1998.

URL: http://dce.unm.edu/familycommunity/training_support/guidelines_CD.htm (June 2002)

USDOJ. “Search and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations”. Computer Crime and Intellectual Property Section. January 2001.

URL: <http://www.usdoj.gov/criminal/cybercrime/searchmanual.htm> (June 2002)

© SANS Institute 2000 - 2002
Author retains full rights.