REQUIRED Cover Page

APPLICATION FOR PROFESSIONAL DEVELOPMENT GRANT

**All applicants please complete this cover page.

Choose one: [ ] Creative activity [ ] Research activity [X] Professional Enhancement activity	**Date of Last PDG Award** (Semester and Year awarded): _____ **Date of ATU Faculty Appointment** (Semester and Year): Fall 1997

1. Project Title: Computer Forensics Training

2. Name of Principal Investigator/Project Director: Johnette Moody

3. School (abbrev): System Science **4. Department: Computer and Information Science**

5. Campus Mail Address: Corley 258 **6. PI/PD Campus Phone: 968-0670**

7. Amount Requested: $4,430.60 **8. Total Cost of Project: $4,430.60**

9. Does this project involve: **10. Duration of Project: 1 week**

Yes	No	
[ ]	[X]	human subjects?
[ ]	[X]	animals/animal care facility?
[ ]	[X]	radioactive materials?
[ ]	[X]	hazardous materials?
[ ]	[X]	biological agents or toxins restricted by the USA Patriot Act?
[ ]	[X]	copyright or patent potential?
[ ]	[X]	utilization of space **not** currently available to the PI/PD?
[ ]	[X]	the purchase of equipment/instrumentation/software currently **available** to the PI/PD?

NOTE: If the answer is "yes" to any of the above questions, the investigator must attach appropriate documentation of approval or justification for use/purchase.

SIGNATURES

Larry Morell 1-19-07
Department Head **Date**

1-19-07
Dean **Date**

This Section to be completed by the Office of Academic Affairs

PDC Committee Award Recommendation: Yes____ No____
PDC Committee Proposal Rank: _____ of _____ Total Proposals.
Recommendation of VPAA: Yes____ No _____
Recommendation of President: Yes____ No _____
Award Date: _____

ABSTRACT

Technological advances have supported the proliferation of the personal computer supporting its infiltration in to every aspect of modern society. However, this growth has resulted in increased electronic crimes. In turn, this increase has stimulated the growth of computer forensics. Computer forensics can be defined as, "the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law. In addition, the goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it (Search CIO, 2007).

The Department of Computer and Information Science recognized the need and met the challenge to provide educated students capable of entering the workforce trained in computer forensics. Beginning fall of 2006, the department began offering a four-year degree in Information Technology with an initial course offering of one course in computer forensics. This course has been met with overwhelming success. Far more students sought to enroll in the course than allowable. As a result, the department desires to add additional courses. While students in this department enroll in programming courses, the blend of programming skills with computer forensics training will place our graduates in high demand. However, the department lacks faculty trained in computer forensics.

Search CIO (2007). Retrieved January 18, 2007, from http://searchcio.techtarget.com/gDefinition/0,294236,sid19_gci1007675,00.html.

PROFESSIONAL DEVELOPMENT GRANT

Purpose/Objectives

- To support the department's mission
- To support the 4-year Information Technology degree in the area of computer forensics
- To prepare graduates for the high-tech positions
- To prepare graduates in the rapidly growing field of computer forensics

Significance/Need

- The department lacks trained faculty
- To expand the courses offered by the department
- To produce qualified graduates in the area of computer forensics
- To prepare graduates that will be in high demand

Process for Attainment of Objectives/Goals

Certified Computer Examiner Boot Camp
Kennesaw, Georgia

~~February 26-March 2, 2007 (7AM – 6PM)~~

- Intensive one week classroom and laboratory training course
- Morning classroom lecture
- Afternoon labs

PROPOSED BUDGET
PROFESSIONAL DEVELOPMENT GRANT

1.	Graduate assistant stipend		$ 0
	Fringe benefits @ .4% (4/10 percent) of graduate assistant stipend		0
2.	Non-work study stipend		0
	Fringe benefits @ .4% (4/10 percent) of non-work study stipend		0
3.	*Supplies (please list items to be purchased and estimated price		
	Training/Registration	Estimated Price	$ 2,650.00
	Item No. 1 Forensics Exam	Estimated Price	345.00
	Total estimated supplies		$ 2,995.00
4.	Travel (please list travel expenditures by date and estimated costs):		
	Travel No. 1 Airfare (2/25-3/2/07)	Estimated Price	$ 515.10
	Travel No. 2 Hotel (2/25-3/1/07)	Estimated Price	575.00
	Travel No. 3 Car (2/25/3/2/07)	Estimated Price	185.00
	Travel No. 4 Meals (2/25-3/3/07)	Estimated Price	160.50
	Total estimated travel		$ 1,435.60
5.	*Capital Outlay (please list items to be purchased and estimated price per item including taxes and shipping, if appropriate):		
	TOTAL PROPOSED BUDGET		$ 4,430.60

*Items purchased under $2,500 (including taxes and shipping) are considered supply items. Capital Outlay items are those which cost $2,500 or more (including taxes and shipping). Please contact the Purchasing Office for questionable items.

DEPARTMENT OF COMPUTER AND INFORMATION SCIENCE
ARKANSAS TECH UNIVERSITY, RUSSELLVILLE, ARKANSAS 72801

To: Faculty Development Committee

From: Larry Morell

Date: January 19, 2007

Re: Application for funding by Dr. Moody

I wholeheartely support the application that Dr. Moody has submitted to support the department's efforts to enhance our offerings in the area of computer forensics. Computer forensics is the study of the how to detect, deter, defend against, and analyze attacks on computer systems. It is essential that students in our new IT degree be given a strong background in this area. Dr. Moody has agreed to head up our efforts to develop a series of course in this area, the first of which she is teaching this semester.

The development of this collection of courses requires extensive training and up-to-date equipment and software. The department has committed $1000 to support the purchase of necessary software and hardware for this course this semester. The department will continue to support these efforts in the coming years. Your support in providing additional education in forensics for Dr. Moody will greatly help to enhance the curriculum and our ability to provide students with the best possible education in this area.

Thank you for your consideration of this request.

Dates and LocationsCourse DetailsStaffFeeGI Bill and DODSoftware ProvidedDistance Learning VersionContactHome

Affiliated Colleges and Institutions

Student Discounts

Access Data

DataLifter

Maresware

InfinaDyne

Course Information

This is not a "watered down" training course. Not like other courses, we tell you in detail what we cover during the course and what our experience and expertise is. We have a great training course, great material, experienced instructors and we truly want you to learn the material and to become good forensic examiners. We want you to compare and decide what is best for you.

You will be provided well developed, detailed handouts of the course material. The course contains a number of practical exercise problems in the form of specially prepared diskettes or a hard disk drive that must be examined. The practical exercises will reinforce the material and teach "hands-on" skills. A case scenario will be used where a fictional private investigator brings you, the examiner, each diskette or a hard disk drive for examination. Each diskette will build to the next exercise, until finally a hard disk drive is examined and the case is concluded. Real life computer forensic issues will be covered by the practical exercises.

Clear, concise, accurate reports that draw appropriate conclusions are a very important factor in presenting the results of a forensic examination. We require reports detailing each "practical exercise" examination. Because of the time constraints of the bootcamp, the reports will be written after the course and submitted to your instructor. We critically review your reports as if we were the "other side" and will help you develop excellent report writing skills. Your final reports can be used as your "template" for real examinations.

Our instructors are all Certified Forensic Computer Examiners or Certified Computer Examiners (CCE)® who are currently involved in computer forensic examinations. They will coach and tutor you through the practical exercises, your reports and through the test questions for each module. Our instructors are highly qualified, experienced and understand forensic examinations far beyond the material in this course. Your interaction with your instructor will normally be via email, but direct assistance is available. We truly want you to learn the material and to become a good forensic examiner.

The course is broken up into five modules. The material is constantly being revised and is subject to change. The current modules consist of:

Module 1

- **An overview of what types of crimes computer evidence might be used in.**
- **How to deal with clients and employers.**

- How to initially determine the scope of the examination.
- How to determine what must be done and how you should proceed in an examination.
- An overview of why trained forensic examiners should be used and what they may expect to encounter.
- Software ethics.
- Forensic ethical standards.
- Forensic examination procedures.
- Preparing and verifying forensically sterile examination media.
- Note taking and report writing.
- Personal computer construction, hardware and software with focus on the BIOS, BIOS limitations, hard disk translation schemes and how they can effect forensic examinations.
- A very broad overview of several operating systems including:
  - Windows NT/2000
  - Novell
  - Unix/Linux
  - DOS
  - Windows 95/98
- A broad overview of networks.
- Instruction on the acquisition, collection and seizure of magnetic media.
- How to best acquire, collect or seize the various operating systems.
- Legal and privacy issues.
- Establishing a sound "chain of custody".
- The beginning logical structures of the Microsoft operating system FAT file system.
- How to recover simple deleted files.
- There are four practical exercises in preparing and verifying forensically sterile media, using a "carving" utility to recover data from unallocated space and the manual recovery of simple deleted files.
- A written examination regarding the material covered in this module.

Module 2

- The DOS and Windows boot process.
- A continuation of how files are created and stored.
- How to recover more complex deleted files.
- The significance and determination of the creation date and time.
- The significance and determination of the last accessed date and the modification date and time.
- How Windows long file names are stored.
- What happens when Windows long file names are deleted.
- How to recover Windows long file names.
- How sub-directories are stored.
- What happens when sub-directories are deleted.
- How to recover a deleted sub-directory and it's files.
- What happens when a diskette or hard disk drive is formatted.
- How to recover files, sub-directories and data from formatted disks.
- How to determine which files had been deleted prior to formatting.
- What file slack is and how to recover data from file slack.
- There are five practical exercises on the logical structure of FAT file systems, file storage and the recovery of fragmented deleted files, the recovery of long file names, the recovery of deleted sub directories and the recovery of formatted disks.
- A written examination regarding the material covered in this module.

Module 3

- An in-depth exploration of NTFS logical structures (nothing similar is available *anywhere*) , including:
  - The partition table
  - The boot record
  - Bitmaps

        - The root directory
        - The MFT
        - Headers
        - Attributes
        - Resident files
        - Non-resident files
        - Run lists, etc.
        - Alternate data streams
        - File storage
        - The various dates and times stored in attributes
        - File deletion
        - File recovery
        - Directory storage
        - Tracing files/directories
        - The NTFS registry "hive".
        - Examining NTFS drives
    - A practical exercise involving the detailed exploration of the NTFS logical structures on a specially prepared NTFS dive.
    - A written examination regarding the material covered in this module.

Module 4

- How to make a Windows 98 forensic boot disk
- How to make "exact" images of media - the various imaging methods
- The use of Firewire write blockers
- The significance, location and recovering data from:
    - Swap Files
    - Temporary Files
    - Internet Cache Files
    - The various types of Email files
    - Internet Cookies
    - Internet Sites Visited
- Basic Internet issues. Doing a basic "whois" and similar Internet checks.
- How to preserve the original media.
- How to prevent inadvertent writes to the original media, virus introduction to the original media, and activation of "booby" traps on the original media.
- How to make bitstream (exact copies) of the original media.
- The safe handling of the media by the forensic examiner.
- The most common situations that an examiner may encounter during an examination.
- Finding and documenting normal data or graphical files.
- How people commonly try to hide data.
- Finding and documenting data and files in unallocated space.
- Finding hidden data.
- An overview of password protection and unlocking passwords.
- Accessing and interpreting "metadata" in MS Office documents.
- There are three practical e xercises on recovering data from swap files, temporary files, etc., determining registration of a URL, finding and documenting normal data on magnetic media, finding hidden data and unlocking passwords, unlocking passwords and accessing metadata.
- A written examination regarding the material covered in this module.

Module 5

- Data formats and types.
- Basic data format conversion.
- Examining CDR media and accessing multiple unclosed sessions.
- Managing data.
- Presenting the data to the client in a useful format.
- Presenting data in court or other proceedings in a clear and understandable manner.
- The marking, storage and transmittal of evidence.

- **The basic use of automated forensic suites (Access Data's Forensic Tool Kit (FTK))**
- **A practical exercise where you examine a specially prepared hard disk drive. This hard disk drive will contain many current "real life" issues covered in this course and will require you to conduct a complete examination of the media. You must examine this hard drive, draw the appropriate conclusions, write a good report and present the evidence found in a manner that is clear and understandable.**

A written final examination will be given.

On the final day of the CCE BootCamp® training course, the online portion of the CCE certification examination will be provided. The balance of the CCE process will be available at a discount price for our students.

We will provide a detailed handout for each module covered. The handouts are provided in advance of the training for self study before the actual bootcamp training course. The handouts can be used as a reference manual. Sample reports, additional practical exercises, a DOS primer, Diskedit primer and other useful information and applications will be provided. You will be subscribed to our listservers that provide both administrative and technical information. Even after you complete the course, as material is updated, you will be able to download the new material from our web site.

We will provide all of the forensic software necessary for the course, including:

- **A fast and thorough wiping program**
- **A fast checksum program**
- **A fast program that documents files (including deleted files) on a drive**
- **A program that will allow examination of unallocated space**
- **A program that will make exact forensic copies of floppy diskettes**
- **An excellent forensic "carving" utility**
- **The Passware Kit from Lost Password.com**
- **Norton Utilities**
- **Norton Ghost**
- **QuickView Plus (a viewing application) QuickView**
- **A good virus scanning utility**
- **The demo version of Access Data's Forentic Tool Kit (FTK)**
- **See hardware and software requirements for details on the software provided.**

Click here to be added to our mailing list for information on boot camp training .

Contact us

Dates and LocationsCourse DetailsStaffFeeGI Bill and DODSoftware ProvidedDistance Learning VersionContactHome

Key Computer Service, Inc.(keycomputer.net) is doing business as cce-bootcamp.com and cftco.com

Johnette Delp Moody, DBA
503 South Boulder
Russellville, AR 72801
(479) 968-4758
email: jmoody@atu.edu

Employment History

Arkansas Tech University, Computer and Information Science Department, Russellville, AR 72801; August 1997 to present

- Introduction to Computer Based Systems – COMS 1003
- Microcomputer Applications - COMS 2003
- PC Hardware and Operating Systems – COMS 2723
- Foundations of Programming I – COMS 2103
- Computer Orientation – COMS 1403
- Introduction to Databases – COMS 2233
- Web development – INFT 5303
- E-mail and Internet – EDMD 6163
- Networking - INFT5703
- Emerging Trends (Research) INFT 6903
- Introduction to Computer Forensics, COMS 2733

Russellville Adult Education, Russellville, AR 72801; 1997
Computer Instructor/Coordinator

- Developed Windows95 curriculum
- Direct instruction of Windows95 classes
- Direct instruction of Windows3.1 classes
- Direct instruction of satellite classes using notebook computers to Ladish, Bibler Brothers Lumbers, and various community organizations
- Computer maintenance
- Oversaw purchase and implementation of upgraded computer
  lab and notebook computers

Russellville School District, Russellville, AR 72801; UE5G
Maternity leave for Sarah Coker; 1996

- Lesson plans
- Direct instruction of Science, Math, and Reading

Employment History

Arkansas Tech University, Russellville, AR 72801; Graduate Assistant; 1995 – 1996

- Assist students in Curriculum Library
- Proctor tests
- Teaching assistant
- Assist students in computer lab

Employment History, continued

Russellville School District, Russellville, AR 72801; Substitute Teacher; 1994 – 1996
Dwight Elementary School, Russellville, AR 72801; Library Aide; 1993 – 1994

- Maintenance of computer program and database
- Class check out/check in of books
- Processed new inventory

Dwight Elementary, Russellville School District, Russellville, AR 72801; Migrant Aide, 1989 – 1992

- Tutored students on a one-to-one basis
- Maintained student records
- Home visits
- Assisted nurse during yearly checkup of Migrant students
- Attended scheduled workshops
- Chairperson of COE, Monitoring and Assessment Committee
- Computerized student enrollment files
- Assisted in all phases of standardized testing

Service to University

*Bridge to Excellence; Fall 2002 to present
*Casino Night; Fall/Spring 2002 to present
*Rising Junior Exam proctor; 2003
*Chairperson, Student Affairs Committee; Fall 2004 to present
*Departmental meetings secretary
*Information Technology degree (departmental)
* Information Systems degree (departmental)
* Recruitment and Retention Committee (departmental)
*Faculty Welfare; 2006 to present
*Chairperson of INFT Associate degree committee
*Computer Club Advisor, 2006 and 2007
*Course coordinator for COMS 1003
*Faculty Search Committee, 2006
*COMS 1003/2003 Curriculum Committee; 2002 to present
* Advisor for Information Technology

Publication

Distance Education: Why are the attrition rates so High? *The Quarterly Review of Distance Education*, 5(3), Fall 2004.

Educational Experience, continued

Student Advising

NCATE team, Arkansas Tech University, Russellville, AR; 1995

Textbook selection/recommendation team; Arkansas Tech University; 1994

Teacher Education Council, Graduate Representative; Arkansas Tech University, Russellville, AR 72801; 1995 – 1996

Teacher Appeal Committee; Arkansas Tech University; Russellville,
AR 72801; 1996

Seminars/ Conferences

IBM Academic Initiative Summer School, 2006
Prentice Hall Information Technology Symposium, March 2006
The Columbine Tragedy Seminar, 2006
SE Cybercrime Summit, 2005
IBM iScholars School, 2005
International Conference on Information Systems, 2005
EAST Conference, 2005
E-Books and Technology, 2005
Microsoft Office Launch, 2004
Web Survey, 2004
Prentice Hall Information Technology Seminar, 2003
Microsoft Office 2003 Launch, 2003
Prentice Hall Information Technology Seminar, 2002
Course Technology Seminary 2001
Arkansas Technology Institute, 1997

Education

Argosy University of Sarasota, Sarasota, FL 34235
2006; Doctorate of Business Administration with emphasis in Information Systems; Advanced Certificate in Management
Technological Issues Impacting Distance Education

Arkansas Tech University, Russellville, AR 72801; December 1996; M.Ed. with emphasis in Instructional Technology/Media; Outstanding Graduate Student

Arkansas Tech University, Russellville, AR 72801; December 1994; BS in Elementary Education; High Honors graduate