Summary Report from the

Digital Forensics Lab

Training #3: Data Recovery Forensics

June 15, 2009
9:00 AM-3:00 PM

University of Maryland, College Park, MD

DFL Training Session #3
Event Summary

Data Recovery Training took place from 9:00-3:00 PM in the Computer and Space Sciences Building Lab at the University of Maryland, College Park on 6-15-2009.

Description of workshop: *Keith Thomas, Director, Forensic Services at immixGroup* will share current Data Recovery techniques and strategies. Participants will learn how to retrieve data from hard drives and other media such as thumb drives and flash media.

Participants will gain hands on experience utilizing imagery tools used for both lab and on-sight field acquisitions. Mr. Thomas will also cover special steps that need to be taken when data recovery is performed specifically for forensic or evidentiary purposes. Participants will actively perform steps at the training in order to be able to reproduce these techniques with their students. Plethora of resources provided.

	Last Name	Representing/Organization
1	Caroland	UMUC
2	Chen	UMUC
3	Chiang	Montgomery College
4	Dubrawsky	InfraGard/CyberWatch
5	DuPree	PGCC
6	Fung	GM University
7	Gross	Anne Arundel County Police
8	Haddock	HCC
9	Hammond	AACC
10	Jenkins	PGCC
11	Knisley	Anne Arundel County Police Department
12	Leitz	US Army, Ft Monmouth
13	Lynch	HCC
14	Matties	Bowie State
15	Moore	AACC
16	Nguyen	UMD
17	Nguyen	PGCC
18	Nguyen	SAIC
19	Nithianandam	HCC
20	Phillips	NVCC
21	Phillips	NVCC

22	Rentstrom	Homeland Security
23	Seda	St. Augustine's College
24	Taylor	AACC
25	Newman	SAIC
26	Misra	IRS
27	Pruitt-Mentle	ETPRO/CW/UMD
28	Maxwell	UMD

The event was very well received. 37 registered online. 4 dropped and gave notification that unexpected circumstances would cause them not to attend. 7 were no shows. 28 particpants attended the event with two members from UMD sponsoring the event also in attendance. Arrangements were made for all computers in the teaching lab to be available for particpants. Sign up was through an online registration mechanism. The live broadcast and materials will be available once posted to the Digital Forensics lab website.

Keith Thomas, *Director, Forensic Services at immixGroup* presented the full day workshop.

immixGroup's Keith Thomas to Present Data Recovery Training at the University of Maryland

Digital Forensics Practice Director Delivering Free Training Class Sponsored by CyberWATCH Consortium

McLEAN, VIRGINIA, June 3, 2009 - immixSolutions, a wholly-owned subsidiary of immixGroup, Inc. delivering information management services to government and commercial customers, today announced Keith Thomas, immixGroup's Director of Forensics Services, is the keynote presenter at the complimentary CyberWATCH Digital Forensics Training Workshop, *Data Recovery Techniques and Strategies*, to be held at the University of Maryland on June 15, 2009.

Mr. Thomas will share current Data Recovery techniques and strategies covering a variety of today's unique media. Participants will learn how to retrieve data from hard drives and other media such as thumb drives and flash devices, and gain hands on experience utilizing imagery tools used for both lab and on-sight field acquisitions. Mr. Thomas will also cover the special steps necessary when data recovery is performed specifically for forensic or evidentiary purposes in a court of law.

immixSolutions provides public and private sector clients with a comprehensive set of digital forensics services comprising data recovery, analysis, and technical assistance pertaining to all types of digital media. From cellular phones to hard drives, immixSolutions' certified experts are highly experienced in acquiring data from various platforms, including Linux, Unix, NT, Novell servers, PCs, and other non-conventional platforms such as fax machines, telephone systems, and video monitoring systems.

This training class is to be held on the University of Maryland's College Park campus,

Monday, June 15 from 9:30am - 3:00pm. A light networking breakfast precedes the class at 9:00am and lunch will also be served. Registration is available online through June 5. Please contact the event coordinator, Davina Pruitt-Mentle, PhD., for further information.

About CyberWATCH

CyberWATCH: Washington Area Technician and Consortium Headquarters is a consortium of higher education institutions, businesses, and government agencies in the Washington D.C./Maryland/Virginia region that is focused on building and maintaining a stronger information security/assurance workforce. In addition, CyberWATCH is committed to improving the quality and increasing the awareness of information security/assurance in the education and business communities. Consortium members collaborate to share best practices, methodologies, curricula, course modules and materials, and provide faculty training and support to schools who want to develop an information security/assurance curriculum. CyberWATCH is funded by a grant from the National Science Foundation (NSF).

About immixGroup, Inc.

immixGroup is one of the largest and fastest growing providers of enterprise technology products and services in the government market, representing more than 150 leading manufacturers, including Oracle, IBM, AccessData, and Guidance Software. In its 11th year of bringing technology solutions to government customers, managing complex government contract processes, and developing high performance government channel sales operations, immixGroup is a recognized leader in the government technology marketplace. For more information, contact immixGroup, Inc. at (703) 752-0610, via email at info@immixgroup.com or on the web at www.immixgroup.com.

Media Contact:

Rob Marks
Director, Corporate Marketing
immixGroup, Inc.
703-752-0651
rob_marks@immixgroup.com

After a short introduction, Keith shared terminology, strategies and techniques needed to recover data from a variety of digital devices including USB drives and laptops. Particpants then had a chance to experience first hand and observe a variety of tools used to recover digital date. Tools included HELIX and FTK imager. Attendees received a variety of tools and resources to include:

- CD of HELIX 1.7 User manual
- Full version of HELIX 1.7 on CD
- CD of FTK User manual
- FTK imager full version loaded on lab computers
- FTK imager lite loaded on thumb drives
- CD of hard drive with images

Ample time was given to a variety of question and inquiries from the audience. Particpants received certificates of completion at the end of the training session.

Summary Evaluations from the Attendees

Evaluation and Feedback (1-4) 4 being the highest	
General Questions	**Average**
How satisfied were you with the registration process	3.8
The content of the Data Recovery Forensics workshop met my expectations/needs	3.7
The program objectives were clearly stated	3.7
The length of this workshop was appropriate	3.7
Enough time for discussion and queries was provided	3.8
The time frame of the workshop was kept	3.8
The content of the workshop session was appropriate and informative	3.8
The workshop was well organized	3.8
Speaker/Facility	
Rating scale (poor = 1, fair=2, good=3 and excellent =4)	**Average**
Keith Thomas	4.0
Facilities	3.5
Would you recommend such a workshop for future meetings?	100% yes
Approximately how many workshops/trainings of this type do you attend annually? • 0= Don't usually attend workshop/training sessions • 1= 1-2 per year • 2= 3-4 per year • 3= 4-6 per year • 4= more than 6 per year	1.3

What did you like most about the workshop?

- good info, well-presented tools
- "It is a science that I was not clear before"
- the instructor was great!
- information well explained
- it moved at an appropriate pace
- the speaker was very well organized. Provided excellent information
- presenters knowledge of the topic
- good information & examples
- relevant information, very well organized
- information learned and tools acquired

- price and food
- Keith's presentation style

What did you like least about the workshop?

- temp in room
- nothing
- everything was great!
- more hands on
- parking (2)
- computers in lab did not have admin rights --it affected the ability to use the forensic software
- lab was not set up to run the CD/DVD

Comments?

- efficiently organized and run. Nice facilities
- overall well done. Be certain lab experiences can be done with available equipment
- speaker was well informed and had comments/of issues discussed

Future topics for workshops/training sessions?

- Linux autopsy
- additional information on computer forensics--a part II of this class with same instructor
- browser/internet trace evidence email forensic spam/spoofing/phishing

Lessons Learned

Particpants enjoy and appreciate the hands on activities. Although there are field service particpants and industry representatives (law enforcement/homeland security), the majority of particpants are faculty who come to learn more about the topic for their own knowledge base and to share with their students. Therefore, handouts, exercises and materials/resources were a huge hit. A critical piece will be to figure out if the archived live broadcast is able to be posted and accessible to others unable to attend.

The biggest hurdles still lie in the preparation of the lab and the campus parking issues. Particpants were given several notices about visitor parking. Reminder notices included links to the interactive campus website and a pdf of the campus map. Several parking locations were given, however, it was suggested that they park in the Stadium garage. Unfortunately, the Stadium Garage was under renovation and therefore the morning of we realized particpants would need to park in either the

Paint Branch parking lot or the Stamp Union parking garage. While several did follow the email directions and found the next available parking location, several particpants parked in the open student garage across from the Computer and Space Science Building. When they checked in we asked where they had parked, and re directed them to park in one of the visitor parking garages. When they went to move their vehicle, they had already received a ticket. Additionally, some went to the Stamp Union Garage only to find it temporarily closed (while a truck unloaded). The parking experience was frustrating to many. Even more detailed directions and a larger map were suggestions offered by particpants for future events.

Keith Thomas made a trip to the UMD lab to test out all software. Unfortunately, we failed to access the CD files at the individual stations. This was frustrating for particpants who were looking forward to a more hands on experience with some of the software applications. A detailed run through to assure the lab is ready for the training will be part of the planning stage for future events.