Summary Report from the

Digital Forensics Lab

Kickoff Event and Training #1

October 22, 2008 and November 13, 2008

University of Maryland, College Park, MD

DFL Kickoff
Event Summary

About the Virtual Digital Forensics Lab

CyberWATCH and the University of Maryland's Office of Information Technology (OIT) are proud to establish a Regional Digital Forensics Lab (DFL) through a grant from the National Science Foundation. The DFL will be a "virtual lab" that will serve as a resource in the teaching of digital forensics at CyberWATCH universities and community colleges, and will offer sample curricula and resources, including forensic case studies, for use by CyberWATCH member institutions and state and local agencies throughout the Washington, D.C. metropolitan area. The first full semester the DFL will be available for use in courses will be Spring 2009.

An important part of the project involves making available computing power and software appropriate for the forensic examination of both network activity and digital media. The virtual lab will consist of virtual machines running on hardware hosted at the University of Maryland, College Park that will function as forensic workstations.

The University of Maryland has been a part of the CyberWATCH consortium for many years, and we are excited to host this shared Digital Forensics Lab that will be used to provide hands-on experience and education to the next generation of information security professionals in the region.

> Dr. Jeffrey Huskamp
> Vice President and Chief Information Officer
> University of Maryland.

Funded by the National Science Foundation, the CyberWATCH consortium is composed of higher education institutions, businesses, and government agencies from across the region focused on improving cybersecurity and safety through education.

The Kickoff event took place at 10:30 AM in the Margaret Brent Room within the Stamp Union at the University of Maryland, College Park campus on October 22, 2008. Opening remarks came from Davina Pruitt-Mentle, Director of Education Technology Policy, Research and Outreach, Vera Zdravkovich, from Prince George's Community College and the CyberWATCH Regional Center Principal Investigator, and Robert Spear from Prince George's Community College and the future CyberWATCH Regional Center Principal Investigator. Welcoming remarks followed by Gerry Sneeringer, Director of Security, Office of Information Technology, UMCP for Jeffrey Huskamp, UMCP Vice president and Chief Information Officer, who was unable to attend. Steven Shirley, Executive Director of Department of Defense Cyber Crime Center (DC3) was the opening keynote speaker. He shared the need and potential impact of such a lab in our region. Sgt. J. Casey from the Maryland State Police, Computer Crimes Section/Computer Forensics Lab shared additional insight into the need from the law enforcement viewpoint. Ajay Gupta, president of GSecurity, Inc. and Director of Cyber Security Services at Prince George's Community College added insight from both small business and academic perspectives. Robert Maxwell, Lead Incident Handler, OIT Security at UMCP then unveiled the DFL website http://dfl.umd.edu/ and shared an explanation as to what and how faculty and others could access the resources. A luncheon reception followed which allowed for networking.

There were 52 in attendance at the kickoff event. The event was displayed on the University of Maryland homepage, the OIT homepage, and the university's calendar and FYI listserv. Media coverage included an article by the Campus newspaper.

Wecome to the Virtual Digital Forensics Lab Kickoff

10:30 AM **Opening Ceremony**

Steven Shirley - Department of Defense
Sgt. J. Casey - Maryland State Police
Ajay Gupta - GSecurity
Robert Maxwell - University of Maryland

Noon **Lunch Reception**

1 PM **Training Session**

October 22, 2008
Margaret Brent Room
Adele H. Stamp Student Union
University of Maryland

About the Virtual Digital Forensics Lab

CyberWATCH and the University of Maryland's Office of Information Technology (OIT) are proud to establish a Regional Digital Forensics Lab (DFL) through a grant from the National Science Foundation. The DFL will be a "virtual lab" that will serve as a resource in the teaching of digital forensics at CyberWATCH universities and community colleges, and will offer sample curricula and resources, including forensic case studies, for use by CyberWATCH member institutions and state and local agencies throughout the Washington, D.C. metropolitan area. The first full semester the DFL will be available for use in courses will be Spring 2009.

An important part of the project involves making available computing power and software appropriate for the forensic examination of both network activity and digital media. The virtual lab will consist of virtual machines running on hardware hosted at the University of Maryland, College Park that will function as forensic workstations.

The University of Maryland has been a part of the CyberWATCH consortium for many years, and we are excited to host this shared Digital Forensics Lab that will be used to provide hands-on experience and education to the next generation of information security professionals in the region.

Dr. Jeffrey Huskamp
Vice President and Chief Information Officer
University of Maryland.

Funded by the National Science Foundation, the CyberWATCH consortium is composed of higher education institutions, businesses, and government agencies from across the region focused on improving cybersecurity and safety through education.

Key Personnel:

Dr. Vera Zdravkovich
Prince George's Community College
CyberWATCH Regional Center Principal Investigator

Dr. Jeffrey Huskamp
Vice President and Chief Information Officer
University of Maryland.

Gerry Sneeringer
Director of Security, Office of Information Technology
Campus IT Security Officer
University of Maryland, College Park

Robert Maxwell
Lead Incident Handler
OIT Security
University of Maryland

Dr. Davina Pruitt-Mentle
Education Technology Policy, Research and Outreach,
CyberWATCH K-12 PI

CyberWATCH – University of Maryland
Digital Forensics Lab Kickoff Agenda
Wednesday, October 22, 2008
Adele H. Stamp Student Union
Margaret Brent Room

10:30 AM

OPENING REMARKS
Dr. DAVINA PRUITT-MENTLE
Director, Educational Technology Policy, Research and Outreach

DR. VERA ZDRAVKOVICH,
Prince George's Community College
CyberWATCH Principal Investigator

GERRY SNEERINGER
Director of Security, Office of Information Technology
Campus IT Security Officer
University of Maryland, College Park

STEVEN D. SHIRLEY
Executive Director
Department of Defense Cyber Crime Center (DC3)

SGT. J. CASEY
Maryland State Police
Computer Crimes Section/Computer Forensics Lab

AJAY GUPTA, PRESIDENT
GSecurity
Director of Cyber Security Services
Prince George's Community College

ROBERT MAXWELL
Lead Incident Handler
OIT Security
University of Maryland

12:00 NOON
LUNCHEON RECEPTION

1:00 - 3:00 PM
TRAINING OPPORTUNITY

An examination of browser forensics, focusing on atypical browsers and alternative Operating Systems (OS). We will look at Internet Explorer on Windows briefly, then on to Firefox, Opera, Chrome, and others. We will look at the effects of “private browsing” and running from removable media. From there we will tackle those pesky "alternative" OSes: Linux and OSX. Altogether an interesting afternoon for cybersleuths.

About the University of Maryland

The University of Maryland is the state's flagship university and one of the nation's preeminent public research universities. Ranked No. 18 among public universities by U.S. News & World Report, it has 29 academic programs in the U.S News Top 10 and 90 in the Top 25. The Institute of Higher Education (Jiao Tong University, Shanghai), which ranks the world's top universities based on research, puts Maryland at No. 37 in the world and No. 8 among U.S. Flagship universities. The faculty includes three Nobel Laureates, seven Pulitzer Prize winners, 40 members of the National Academies of Science, and scores of Fulbright scholars. The university is also recognized for its diversity, with one-third of the student population being students of color. For more information about the University of Maryland visit www.umd.edu.

About CyberWATCH

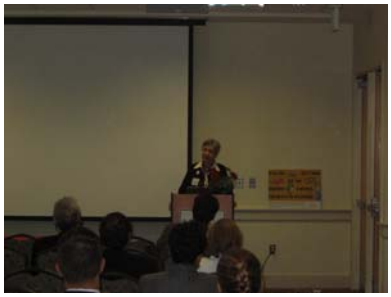
CyberWATCH: Washington Area Technician and Consortium Headquarters is a consortium of higher education institutions, businesses, and government agencies in the Washington D.C./Maryland/Virginia region that is focused on building and maintaining a stronger information security/assurance workforce. In addition, CyberWATCH is committed to improving the quality and increasing gthe awareness of information security/assurance in the education and business communities. For more information about CyberWATCH, visit www.cyberwatchcenter.org.

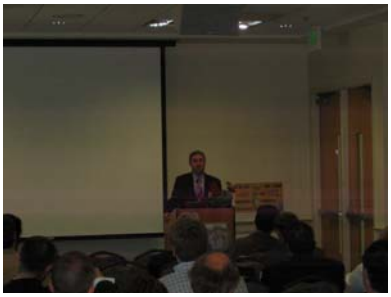
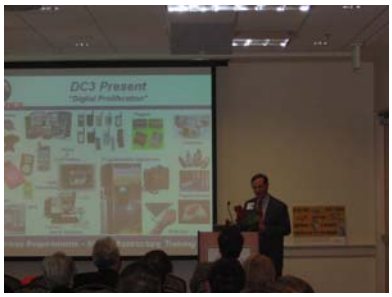
CyberWATCH is funded by a grant from the National Science Foundation (NSF).

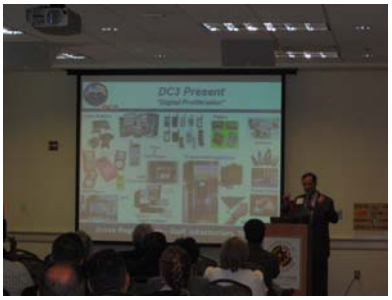
About NSF

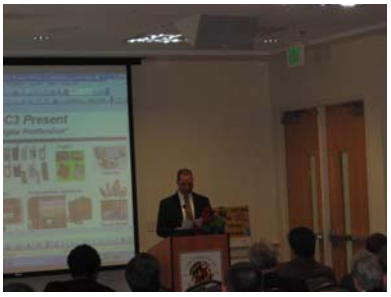
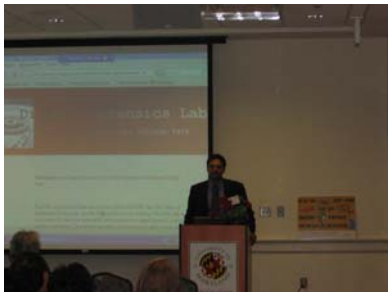
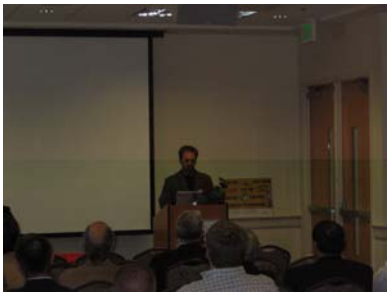
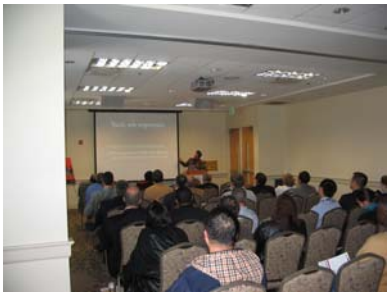
The National Science Foundation (NSF) is an independent federal agency that supports fundamental research and education across all fields of science and engineering, with an annual budget of $5.92 billion. NSF funds reach all 50 states through grants to over 1,700 universities and institutions. Each year, NSF receives about 42,000 competitive requests for funding, and makes over 10,000 new funding awards. The NSF also awards over $400 million in professional and service contracts yearly. For more information about NSF, visit http://www.nsf.gov/.

Pictures from the Event






Press

21 October 2008

Official Kickoff of Virtual Digital Forensics Lab

15 May 2008

UMD's Office of Information Technology to Create a Virtual Digital Forensics Lab

http://www.networkworld.com/community/node/27848

http://www.oit.umd.edu/ITforUM/2008/spring/DFL.html

http://net.educause.edu/content.asp?page_id=1020687&PRODUCT_CODE=SEC09/SESS23&bhcp=1

http://www.bizmonthly.com/8_2008_focus/f_13.shtml

https://wiki.maxgigapop.net/twiki/pub/MAX/Newsletters/NewsLetMay08.pdf

https://listserv.umd.edu/cgi-bin/wa?A2=ind0810&L=fyi&D=1&P=27269

http://nodemagazine.wordpress.com/

DFL Training Session #1
Event Summary

Browser Forensics Training took place from 12:00-3:00 PM in the Computer and Space Sciences Building Lab at UMD on 11-13-2008.

Description of workshop: *An examination of browser forensics, focusing on atypical browsers and alternative OSES. We'll look at IE on Windows briefly, then Firefox, Opera, Chrome, and others. We'll look at the effects of "private browsing" (i.e., porn mode) and running from removable media. From there we'll tackle those pesky "alternative" OSES: Linux and OSX*

Robert Maxwell lead the training. Twenty two enrolled. Twenty members were in attendance. Two DVD's were given out and Robert walked participants through activities and investigations. Resources were added to the DFL website.

	Last Name	Representatives/Organization
1	Chiang	IHE
2	Bosse	IHE
3	Carrington	
4	Gupta	IHE
5	Harris	State
6	McKelvie	IHE
7	Singh	IHE
8	Dubrawsky	IHE
9	Burgin	IHE
10	Ashman	
11	Diedrichs	
12	Shank	IHE
13	Knisley	
14	Littleton	IHE

15	Hall	IHE
16	Chen	IHE
17	Jenkins	IHE
18	Sullivan	IHE
19	Hardy	state
20	Howard	state
21	Nithianandam	IHE
22	O'Guinn	

Lessons Learned

The event was originally scheduled to occur after the kickoff event. However, due to the large numbers signing up and the limited lab space, arrangements were made to make a short presentation in the same room after the kickoff event. The training took place several weeks later in the Computer and Space Sciences building lab. While the facilities were exceptional, the parking at the UMCP campus was limited. The day was raining, pouring at times. The main parking space participants were advised to park in was filled due to bad weather. Participants were able to find another parking garage but had to walk across campus in the rain. Two participants later emailed and stated that they were unable to find parking and just gave up and drove back home.

The event was to start at 12:00 PM. Participants were comfortable starting a little late as they understood the weather and parking situations. However, the presenter did not adequately prepare ahead of time; coming to the lab at 12:15. It was soon noted that the projector bulb was out. A second projector also malfunctioned. A third projector was brought in and the training actually started at 12:45. Later in the presentation the DVD to be used by participants would not run on the computers in the lab. The error message stated the file was too large. Fortunately, a participant was able to figure out how all members in the training could access the files. A second DVD was to be used but was not ready for distribution for the participants. Instead both files were added to the website. While there were glitches in the first training offered, members still seemed pleased with the training.

Summary Evaluations from the Attendees

Evaluation and Feedback (1-3) 3 being the highest	
General Questions	**Average**
The content of the Browser Forensics workshop met my expectations	2.3
The program objectives were clearly stated	2.4
The length of this workshop was appropriate	2.3
Enough time for discussion and queries was provided	2.5
The time frame of the workshop was kept	2.2
Speaker's Presentations	
Rating scale (poor = 0, fair=1, good=2 and excellent =3)	**Average**
Robert Maxwell	2.9
Facilities	2.6
Would you recommend such a workshop for future meetings?	13 yes/2 no

How could this course be improved?

- Full day w/ a better case study
- Instructor seemed knowledgeable but was unprepared. Facilities were unprepared-projector did not work, files did not run on workstations. Fortunately a student figured out how to make it run
- very good workshop--good focus on topic
- found it very effective
- please provide more hands on lab sessions --location good
- please provide more hands on lab sessions in the future the location is great
- Better parking or parking directions/alternative parking

Future topics for workshops/training sessions?

- cell phones forensics, search and seizure topics
- other topics in forensics
- specific exam techniques--ipod forensics--blackberry forensics
- any forensics class will do hands on information etc…