



Summary Report from the
Digital Forensics Lab
Training #2: Cell Phone/PDA Forensics

April 2, 2009
8:00 AM-3:30 PM

University of Maryland, College Park, MD



DFL Training Session #2 Event Summary

Cell Phone/PDA Forensics Training took place from 8:00-3:00 PM in the Computer and Space Sciences Building Lab at the University of Maryland, College Park on 4-2-2009.

Description of workshop: *An overview of hand held cell technology. The class will cover cell signals and how they work, cell phones, and PDA's and how they store and transmit information. GPS units, GSM and CDMA cell phones and GPS technology in the cellular network will also be covered, as well as, recovery of information from cell providers and the physical devices. Participants will be given an opportunity to do hands-on work on cellular devices. Participants are asked to bring any and all cell phones, old and new working or not to class as demonstration units.*

Ken Haynes, a Computer Forensic Examiner with the Drug Enforcement Administration (DEA) from the Digital Evidence Laboratory led the training. Forty five enrolled. Thirty four people were in attendance, with the remaining enrollees viewing through the live broadcast or planning to watch the archived video of the event. Participants were asked to bring cell phones and members were walked through a variety of activities, in addition to having time to explore software and equipment used in the field. Resources will be added to the DFL website.

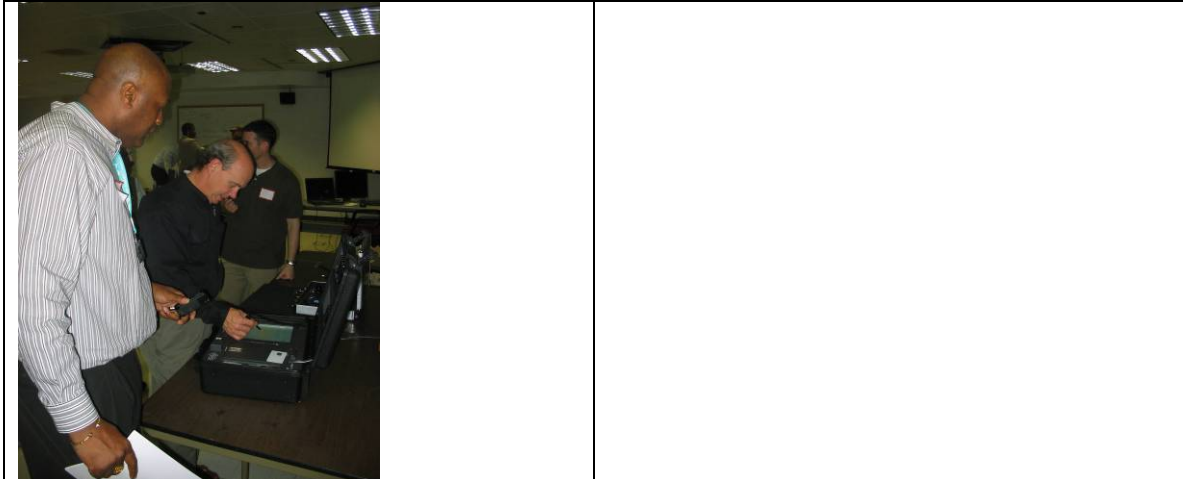
	Last Name	Representing/Organization
1	Hardy	Business/CW
2	Buie	Government/CW
3	Burt	PGCC
4	Hopkins	AACC
5	Caroland	UMUC
6	Waterman	AACC
7	McKalip	UMUC
8	McBorrough	NVCC
9	Keck	Harford Co Public Schools (IT)
10	O'Brien	CCBC
11	Burgin	CSMD
12	Jenkins	CSM
13	Hickey	Capitol College
14	Weil-Yates	Hagerstown CC
15	Knisley	Anne Arundel County Police Department
16	Medley	US Secret Service Electronic Crimes Task Force
17	White	AACC
18	Butler	Capitol College
19	McKelvie	Capitol College
20	Scott	UMD
21	Wright	Wilmington University
22	Cheng	Charles County Public Schools

23	Bennett	Charles County Public Schools
24	Stine	Charles County Public Schools
25	Reed	NVCC
26	Nguyen	PGCC
27	Dubrawsky	CW
28	Maimone	Harford Co Public Schools (IT)
29	Leary	NVCC
30	Harris	Maryland Office of the Attorney General
31	Chamlou	NVCC
32	Montalvo	Baltimore City Police Department
33	Maheshwari	AACC
34	McDowell	United States Secret Service
35	DuPree	PGCC
36	Redman	George Mason University
37	Webb	Montgomery College
38	Shank	Hagerstown Community College
39	Krist	NVCC
40	Lee	Howard
41	Hidalgo	CCBC
42	Lantz	Maryland State Police
43	Jenkins	CyberWatch Intern
44	Tender	UMD
45	Brown	VCCS
46	Sneeringer	UMD
47	Maxwell	UMD
48	Pruitt-Mentle	UMD/ETPRO/CW

The event was very well received. 45 enrolled in the class, with three members from UMD sponsoring the event also in attendance. Arrangements were made for all computers in the teaching lab to be available for participants. Additional, chairs were placed around the walls of the rooms for extra attendees. Sign up was through an online registration mechanism. When we reached capacity a notice was sent to participants explaining that we had reached capacity, but they could attend if they did not mind bringing their own laptop. Internet connection would be provided. On the date of the event, thirty four were in attendance (face to face). Others had decided to view the event through the live broadcast and/or review the material once posted to the Digital Forensics lab website.

Ken Haynes, a Computer Forensic Examiner with the Drug Enforcement Administration (DEA) from the Digital Evidence Laboratory led the training. After introduction Ken shared strategies and techniques needed to recover data from cell phones. Participants removed the SIM card from a variety of cell phones (old and new) and then using equipment brought in by Ken walked through several exercises of creating and deleting files and then recovering. Ample time was given to a variety of question and inquiries from the audience. Participants 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	3.89
The content of the Cell phone/PDA Forensics workshop met my expectations/needs	3.47
The program objectives were clearly stated	3.53
The length of this workshop was appropriate	3.63
Enough time for discussion and queries was provided	3.79
The time frame of the workshop was kept	3.79
The content of the workshop session was appropriate and informative	3.68
The workshop was well organized	3.74
Speaker/Facility	
Rating scale (poor = 1, fair=2, good=3 and excellent =4)	Average
Ken Haynes	3.68
Facilities	3.68
Would you recommend such a workshop for future meetings?	3.79
Approximately how many workshops/trainings of this type do you attend annually? <ul style="list-style-type: none"> • 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 	2.39

What did you like most about the workshop?

- forensics applied to cell phone
- hearing other people's experiences
- hands-on
- variety of equipment to view
- forensics is needed in education it was an excellent choice to offer
- hands on examples
- good information-good hands on
- hands on tools
- the hands on activities were very helpful
- the hands on equipment and software and possible job opportunity
- Hands on training
- hands on activities
- Hands on
- instructor was able to address wide range of experiences of attendees
- hands on opportunity with hardware
- hands on use of phone tools
- exposure to cell phone forensics

What did you like least about the workshop?

- speaker skipped technical subjects
- speaker went through PPT's too quickly to be able to take notes
- distance
- I liked it!
- no handouts on information
- not enough content
- inability to get copy of briefs
- space was small—OK
- no substantial content, no handouts
- have a couple of workable cell phones

Comments?

- thank you for inviting me
- thanks to Ken for taking the time and UMD and Davina for making it possible!
- the group had enough expertise & knowledge to get technical part of workshop that was not included
- workshops for college students should also be included
- worthwhile seminar--thank you
- very enjoyable workshop
- the workshop was good overall--good information and hands on and

- great resources
- would like to have more resources to show students ppts, handouts etc...
- worthwhile day overall
- network intrusion forensics
- look forward to the next one
- good presentation and set up
- Linux forensics
- good class--good covering of topic--knowledgeable instructor
- support from Davina was excellent. Speaker did seem prepared with clear objectives and content. His main focus was getting to the lab portion, but no real background info was provided. Based on course description I was expecting SOME explanation on signals and cell technology. We saw a list of providers and were told there are 2 kinds of networks. That's it. Presumed audience knowledge of forensics procedures, no real explanations offered. This was disappointing.
- show how to interpret reports

Future topics for workshops/training sessions?

- capturing and recovering data in a way that is safe
- show how to interpret reports
- wireless networking security
- computer forensics, i.e. discovery
- setting up infrastructure for online labs
- any DF topic

Lessons Learned

Participants enjoy and appreciate the hands on activities. Although there are field service participants (law enforcement/secret service), the majority of participants 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 need to be a staple in future sessions. Although faculty have a background in this area, they come to learn more about the technical processes—this needs to be included more in future sessions. A critical piece will be to figure out a way to archive the live broadcast –which can then be added to the website. Many participants sign up on the assumption that materials and/or the video will be available online.