

CF-102 Forensic Tools and Techniques
Course Syllabus - 2006

Course Instructors:

Dr. David Dampier
Phone: 662-325-8923
Email: dampier@cse.msstate.edu

Gary Cantrell
Phone: 662-325-2756
Email: cantrell@cse.msstate.edu

Kendall Blaylock
Phone: 662-325-2422
Email: kblaylock@gmail.com

Course Description:

This course is an introduction to the tools and techniques used by a digital forensics examiner. It complements CF101 in that it provides laboratory exercises and hands on tasks that give a deeper understanding of CF101 topics.

Course Objectives:

On the completion of this course the student will be familiar with some of the free and commercial tools used by a digital forensic examiner during an investigation. They will also be familiar with some of the issues involved with more advanced topics such as email tracing and cell phone forensics.

Course Requirements:

All students must complete CF101 or have permission from our director Dr. David Dampier before taking this course.

Fees:

This course is free to any law enforcement official in the Southeast region of the US. Any other applicant may inquire about attendance through our director Dr. David Dampier.

Food and Lodging:

Food and lodging will be supplied by Mississippi State University for the duration of the course. Lodging is supplied in the form of a local hotel. Food is either provided as catering or reimbursement.

Registration:

All students must register prior to attending this course. Registration can be made:

Online: <http://security.cse.msstate.edu/ftc>

By Phone: 662-325-2756

By Mail: Through letter or with the use of the registration form found in our brochures.

Completion Conditions:

A student is considered to have completed this course if he/she attends all three days, and satisfactorily completes the assigned exercises/tasks/tests. On completion each student is presented with a certificate of completion for CF-102.

Schedule:

This is a three day course and usually runs next to our CF101. Unless otherwise stated, it runs from 1300 to 1700 on day one and 0800 to 1700 on days 2 and 3. Instruction time totals 18 hours.

Topics:

Topics in this course include the following:

- Windows file system basics
- Command line usage
- How to find and use freeware
- File identification based on file signatures
- The use of metadata in investigations
- How to reconstruct web browser history
- Password cracking methods
- How to trace emails
- Introduction to cell phone forensics
- Introduction to data hiding

Lab exercises from previous topics will include:

- Manual data recovery
- File hashing
- Image creation