H

Agenda Item Request Form

Hays County Commissioners' Court

9:00 a.m. Every Tuesday

Request forms are due in the County Judge's Office

no later than 2:00 p.m. on WEDNESDAY.
Phone (512) 393-2205 Fax (512) 393-2282

AGENDA ITEM: Approve Out of State Training Travel Request for Angelo Floiran in the Sheriff's Office.

CHECK ONE: ☒ **CONSENT** ☐ **ACTION** ☐ **EXECUTIVE SESSION** ☐ **WORKSHOP** ☐ **PROCLAMATION** ☐ **PRESENTATION**

PREFERRED MEETING DATE REQUESTED: July 26, 2011

AMOUNT REQUIRED: $0.00

LINE ITEM NUMBER OF FUNDS REQUIRED: N/A

REQUESTED BY: Captain Mike Davenport/Hays County Sheriff's Office

SPONSORED BY: Debbie Ingalsbe

SUMMARY: The grant is funding the Out of State Training so there are no county funds required.

FILED: JUL 26 2011
HAYS COUNTY COMMISSIONERS' COURT
Resolution # 28244 VOL U PG 634

United States Secret Service

WWW.NCFI.USSS.GOV

Courses

BICEP

Basic Investigation of Computer and Electronic Crimes Program

BICEP is a five-day course designed to provide investigators with the ability to act as a first responder to a variety of cyber related cases. Investigators will gain hands-on experience with computer hardware, operating systems, cell phones, PDAs, GPSs, networking fundamentals, email investigations, legal issues, and search and seizure. The course combines instructor-led discussions and practical exercises to teach methodologies and techniques used during investigations involving digital evidence.

After completing this course, students will:

- Be able to identify system components
- Install and troubleshoot basic computer hardware
- Understand the significance of different file systems
- Install and configure different operating systems
- Know standard protocols for seizing and storing digital evidence
- Be able to use forensic tools to conduct analysis of digital data
- Be able to create a comprehensive digital evidence case report
- Know legal issues applicable to digital evidence investigations

Prerequisites:

- None

top

BCERT

Basic Computer Evidence Recovery Training

This is a five-week course designed to provide hands-on experience with computer hardware, device imaging solutions, forensic analysis tools, legal issues and report generation for law enforcement officers performing as cyber incident responders and digital evidence examiners. The course combines instructor-led discussions and practical exercises to teach methodologies and techniques used during investigations involving digital evidence.

After completing this course, students will:

- Be able to identify system components
- Install and troubleshoot basic computer hardware
- Understand the significance of different file systems
- Install and configure different operating systems
- Know standard protocols for seizing and storing digital evidence
- Be able to use forensic tools to conduct analysis of digital data
- Be able to generate a comprehensive digital evidence case report
- Know legal issues applicable to digital evidence investigations

Prerequisites:

- BICEP or equivalent

top

ACERT

Advanced Computer Evidence Recovery Training

This is a five-day course designed to provide experienced forensic examiners with the knowledge and abilities to apply network/server based forensics processing skills. The course combines instructor-led discussions and practical exercises to teach methodologies and techniques used during investigations involving digital evidence on networks and/or servers.

After completing this course, students will:

- Identify and explain the use of networking hardware
- Identify and explain the types of networking topology and connectivity
- Understand the various roles that servers have on the Internet
- Understand how to collect files normally found on servers running Microsoft Windows, Linux, and Solaris UNIX.

Prerequisites:

- BICEP or equivalent
- Minimum of 6-12 months of experience in conducting digital forensic examinations

top

NITRO

Network Intrusion Response Program

This is a 14 day course designed to provide training on how to effectively respond to a network incident including mitigation of the problem, collection of volatile data, and intrusion investigation of a network based crime. The course combines instructor led discussions and practical exercises to teach methodologies and techniques used during

About NCFI

- Home
- Overview & History
- Facility
- Contact Us
- Field Offices
- Brochure

Get Started

- Login

- Identify and explain the types of networking topology and connectivity
- Be aware of the common network crimes and their methods of operation
- Be able to properly report accounts of a network crime
- Be able to collect and analyze network logs using the scientific method
- Be able to use forensic tools to gather and analyze network data

Prerequisites:

- BICEP or equivalent

top

AFT

Advanced Forensics Training

This is a 14 day course designed to focus on advanced digital forensic data recovery topics, tools, and practices through a combination of lecture, instructor-led demonstrations, and practical exercises.

After completing this course, students will:

- Discuss advanced data recovery situations and solutions that may occur in a digital forensic environment
- Practice using various data recovery tools and techniques to identify and recover information of investigative relevance from digital media
- Explain the ramifications of techniques such as steganography and encryption in a forensic environment

Prerequisites:

- BICEP or equivalent
- Minimum of 6-12 months of experience in conducting digital forensic examinations

top

CFC-J

Computer Forensics in Court - Judges

This four-day course provides hands-on experience with computer and networking technology to allow judges to obtain knowledge and insight into presiding over criminal cases involving digital evidence. The course combines instructor led discussions and practical exercises to demonstrate methodologies and techniques used by investigators, as well as instruction of digital evidence legal issues.

After completing this course, students will:

- Identify system components
- Understand the significance of how data is stored on computers
- Understand the basic differences between popular operating systems
- Understand the role that the Internet and networks play in computer crimes
- Understand the entire forensic process performed by investigators
- Better understand legal obstacles present in computer crimes
- Understand how to better evaluate computer crime cases in court

Prerequisites:

- None

top

CFC-P

Computer Forensics in Court - Prosecutors

This five-day course provides hands-on experience with computer and networking technology to allow prosecutors to obtain knowledge and insight into handling criminal cases involving digital evidence. The course combines instructor led discussions and practical exercises to teach methodologies and techniques used by investigators, as well as instruction of digital evidence legal issues.

After completing this course, students will:

- Identify system components
- Understand the significance of how data is stored on computers
- Understand the basic differences between popular operating systems
- Understand the role that the Internet and networks play in computer crimes
- Understand the entire forensic process performed by investigators
- Better understand legal obstacles present in prosecuting computer crimes
- Understand how to better evaluate and present computer crime cases in court

Prerequisites:

- None

top

MDDR

Mobile Device Data Recovery

MDDR is a 10 day course designed to provide hands-on experience with mobile devices. Investigators will gain experience with a wide array of mobile devices such as cell phones, GPS units, and tablets, forensics analysis tools, legal issues, and report generation for law enforcement. The course combines instructor-led discussions and practical exercises to teach methodologies and techniques used during investigations involving digital evidence of mobile devices with traditional investigative techniques.

After completing this course, students will: