CAE New & Early Career Faculty Development and Mentoring Workshop- Digital Forensics

2024 CAE Community Symposium

Dr. Michael Tu

Purdue University Northwest

Hands-on Preparations

- PNW NDG Access
- Run the Tools
  - Launch the FTK Case
  - Launch Cellebrite Reader case

- **Welcome**
- In an effort to reduce lag and slowdowns, please compete the following now:
  1. Log into the workstation – check your materials folder for your sign-in info
  2. Navigate to **ndg.pnw.edu** using a web browser, and sign-in
     - Adjust the reservation time to last until **at least 4:30pm (16:30)**
       - This is to avoid having to start a new reservation at the half-way point
  3. Open FTK 7.4 on the Desktop of the training VM (please wait for it to appear after clicking "Yes" on the "Do you want to allow this app to make changes to your device?" pop-up)
     - Sign-in (user: pnw | password: password)
     - Double-click on the iPhone X Full File System – Small Reader case to open it
  4. Navigate to Documents\Cellebrite Reader Reports\ iPhone X Full File System – Small Reader\
     - Double-click CellebriteReader.exe

2024 CAE Community Symposium

Digital Forensics Experiences

-- A Little Bit About Myself

- **Certifications**
  - COO (Cellebrite Certified Operator), CCPA (Cellebrite Certified Physical Analyst)
  - CHFI (expired), ACE (Expired in 2023)
- **Industry Training**
  - 2020: AccessData (Adv. FTK, Win Registry, Win 10 OS, Adv SQLite, FTK Mobile, IOS Forensic)
  - 2016: AccessData (MAC Forensics, Linux Forensics, Cloud Forensics, Win 10, Win 8 OS, Win Registry, Adv. Forensics, Packet Analysis)
  - 2007-2008: AccessData (Win OS, FTK, Internet Forensics, Applied Decryption), InfoSec, CHFI
- **Teaching**
  - 15+ years of Forensics teaching in Computer Forensics to both under & graduate
  - Offered training to law enforcement officers, veteran, and transitioning military
- **Research**
  - Applied IoT forensics research, Forensics modeling, cybersecurity hacking forensics, forensic education

2024 CAE Community Symposium

Digital Forensics Course Offering Levels

- Undergraduate
- Technical
- CAE KUs
- NCWF Work Roles

- **Entry Level**
  - Digital Forensics Fundamentals or CHFI or Digital Forensics Investigation
  - CAE Knowledge Units covered
    - Cyber Crime (CCR), Digital Forensics (DFS)
  - NCWF Work Roles
    - Cyber Crime Investigator (IN-INV-001)
    - LE/Counter Intelligence Forensics Analyst (IN-FOR-001
    - Cyber Defense Forensics Analyst (IN-FOR-002)
- **Advanced Level I**
  - IoT & Mobile Forensic or Cell Phone Forensics
  - CAE Knowledge Units covered
    - Device Forensics (DVF), Media Forensics (MEF)
  - NCWF Work Roles:
    - LE/Counter Intelligence Forensics Analyst (IN-FOR-001)
    - Cyber Defense Forensics Analyst (IN-FOR-002)
- **Advanced Level II**
  - Windows Forensics or Computer Forensics
  - CAE Knowledge Units covered
    - Host Forensics (HOF), Media Forensics (MEF), Network Forensics (NWF)
  - NCWF Work Roles:
    - LE/Counter Intelligence Forensics Analyst (IN-FOR-001)
    - Cyber Defense Forensics Analyst (IN-FOR-002)

2024 CAE Community Symposium

Entry Level – CHFI Prep or Digital Forensic Investigation

- Curriculum Topics
- Tools
- Labs
- Resources

- **Curriculum Topics**
  - Cyber crimes, cyber crime law and regulations, digital forensics investigation procedures, Rules of Evidence.
  - Fundamentals of digital investigation techniques
    - FAT and NTFS File system forensics, Win Registry forensics, network traffic log analysis, data carving, delete file recovery, steganography
- **Tools**
  - No commercial license needed: Wireshark, Autopsy, Process Explorer, FTK Imager,
- **Hands-on Labs**
  - Create disk image, create a case, analyze file systems/registry, password cracking, network traffic log analysis
  - File recovery and data carving, search, metadata analysis
- **Resources**
  - CLARK Site: Curriculum
  - NDG NetLab+: NDG Forensics V2
  - CWCT Training: Curriculum and PNW NDG (https://ndg.pnw.edu/)

2024 CAE Community Symposium

Entry Level – CHFI Prep or Digital Forensic Investigation

- Training
- Certification
- Hands-on Practice
- Competency Statements

- **Training**
  - Exterro/AccessData Forensics Training
  - InfoSec, SANS
  - CWCT255: Digital Forensics Investigator (Free until 2025)
- **Certification**: EC Council CHFI, CCF
- **Hands-on Practice (15 minutes)**
  - Log into PNW NDG (3 minutes)
  - Create a case using Autopsy (5 minutes)
  - Navigate the case (7 minutes)
- **Competency Statement**
  - Cybersecurity students taking an ITS3xx00 (CWCT255) Digital Forensic Investigation course who have completed ITS25000 (Fundamentals of Information Assurance) will act as a Cyber Crime Investigator and Cyber Defense Forensics Analyst with access to the cybersecurity incidents evidence copy and forensics workstation installed with Autopsy to conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion (T0027) and decrypt the seized data using various techniques (T0049). They are expected to recover the cyber incidents with the cause (who, when, and what, and how the cyber incident take place) within defined time depends on the size of the incident and prepare a forensic report which clearly communicates the law enforcement officers and judges.

2024 CAE Community Symposium

Adv. Level I – IoT & Mobile Forensics

- Curriculum Topics
- Tools
- Labs
- Resources

- **Curriculum Topics**
  - IoT & mobile forensics tools and acquisition, SQLite database basics and programming, IOS system, communication, web forensics, Android system, communication, web forensics, IoT device, mobile app, and network Forensics
- **Tools**
  - Commercial license required: Cellebrite UFED, Physical Analyzer, FTK
  - No commercial license needed: Wireshark, Cellebrite Reader
- **Hands-on Labs**
  - Cell phone evidence extraction and process using UFED and Physical Analyzer, SQLite Database programming labs, IoS evidence examination, Android evidence examination, IoT Device evidence examination, IoT SQLite database evidence process, IoT network traffic analysis
  - Adv. Labs: IOS phone jailbreak, Android phone rooting, MITM attack for IoT Network traffic interception
- **Resources**
  - CLARK Site: Curriculum (to be uploaded)
  - CWCT Training: Curriculum and PNW NDG (https://ndg.pnw.edu/)
  - Maybe published to NDG NetLab+

2024 CAE Community Symposium

Adv. Level I – IoT & Mobile Forensics

- Training
- Certification
- Hands-on Practice
- Competency Statements

- **Training**
  - Cellebrite Forensics Training
  - InfoSec, SANS, Exterro/AccessData Forensics Training
  - CWCT240: IoT & Mobile Forensics (Free until 2025)
  - PNW training camp to Law Enforcement (depend on funding availability)
- **Certification**: Cellebrite COO, CCFP, CMFE (entry), GIAC ASF (Adv.)
- **Hands-on Practice (15 minutes)**
  - Log into PNW NDG (3 minutes)
  - Open Cellebrite Reader for iPhoneX File System SmallReader (3 minutes)
  - Navigate the case (9 minutes)
- **Competency Statement**
  - Cybersecurity students taking an ITS45800 (CWCT240) IoT & Mobile Forensic course who have completed ITS35200 (Cybersecurity & Risk Management) will act as a Cyber Defense Forensics Analyst with access to the acquired cell phone and license Cellebrite UFED to create a forensically sound copy of the evidence (i.e., forensic extraction) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes (T0048, T241). They are expected to complete the full file system extraction for a 64GB iPhone X within 3 hours and prepare a forensic report which clearly communicates the law enforcement officers and judges.

2024 CAE Community Symposium

Adv. Level II – Computer Forensics

- Curriculum Topics
- Tools
- Labs
- Resources

- **Curriculum Topics**
  - FTK tools basics, FAT, NTFS, GPT file system analysis, Windows registry analysis, applied decryption, Windows OS forensics, MS Office forensics, Web-browser and cloud forensics, and network Forensics, advanced FTK
- **Tools**
  - Commercial license required: FTK Tool Suite
  - No commercial license needed: Wireshark, FTK Imager
- **Hands-on Labs**
  - Cell phone evidence extraction and process using UFED and Physical Analyzer, SQLite Database programming labs, IoS evidence examination, Android evidence examination, IoT Device evidence examination, IoT SQLite database evidence process, IoT network traffic analysis
  - Adv. Labs: IOS phone jailbreak, Android phone rooting, MITM attack for IoT Network traffic interception
- **Resources**
  - CLARK Site: Curriculum (to be uploaded)
  - CWCT Training: Curriculum and PNW NDG (https://ndg.pnw.edu/)

2024 CAE Community Symposium

Adv. Level II– Computer Forensics

- Training
- Certification
- Hands-on Practice
- Competency Statements

- **Training**
  - Exterro/AccessData Forensics Training
  - CWCT235: IoT & Mobile Forensics (Free until 2025)
- **Certification**: AccessData ACE
- **Hands-on Practice (15 minutes)**
  - Log into PNW NDG (3 minutes)
  - Open FTK with iPhoneX File System SmallReader Case (3 minutes)
  - Navigate the case (9 minutes) – plist files
- **Competency Statement**
  - Cybersecurity students taking an ITS45200 (CWCT235) Computer Forensic course who have completed who have completed ITS35200 (Cybersecurity & Risk Management) will act as a Cyber Defense Forensics Analyst with access to the network devices and forensics workstation installed with Wireshark to collect and analyze network traffic associated with malicious activities (T0240). They are expected to perform the network traffic collection and be able to recover the crime scene of the malicious activities over the network and prepare a forensic report which clearly communicates the law enforcement officers and judges.

2024 CAE Community Symposium

Resources & Tools

- **Work Roles:**
  - NICE: https://niccs.cisa.gov/workforce-development/nice-framework
  - DCWF: https://dodcio.defense.gov/Cyber-Workforce/DCWF/
- **CLARK Link:**
  - https://clark.center
- **Lab Setups**
  - Netlab Setup for CHFI
  - Labs for Windows Forensics
  - Labs for IoT & Mobile Forensics

2024 CAE Community Symposium