CTSC

CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Building a Digital Forensics Program

Warren Raquel

2017 NSF Cybersecurity Summit
2017-08-15

trustedci.org

Center for Trustworthy Cyberinfrastructure

CTSC's mission is to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

Who we are

Warren Raquel - Senior Security Engineer at the National Center for Supercomputing Applications

CTSC - Provides the NSF community with a coherent understanding of how cybersecurity is important to them and the resources to achieve and maintain a cybersecurity program appropriate for them.

Class Outline

- Introduction
- Section 1 — What is the role of digital forensics?
- Section 2 — The general Digital Forensics Process
- Section 3 — What you need to get your program off the ground

Forensics

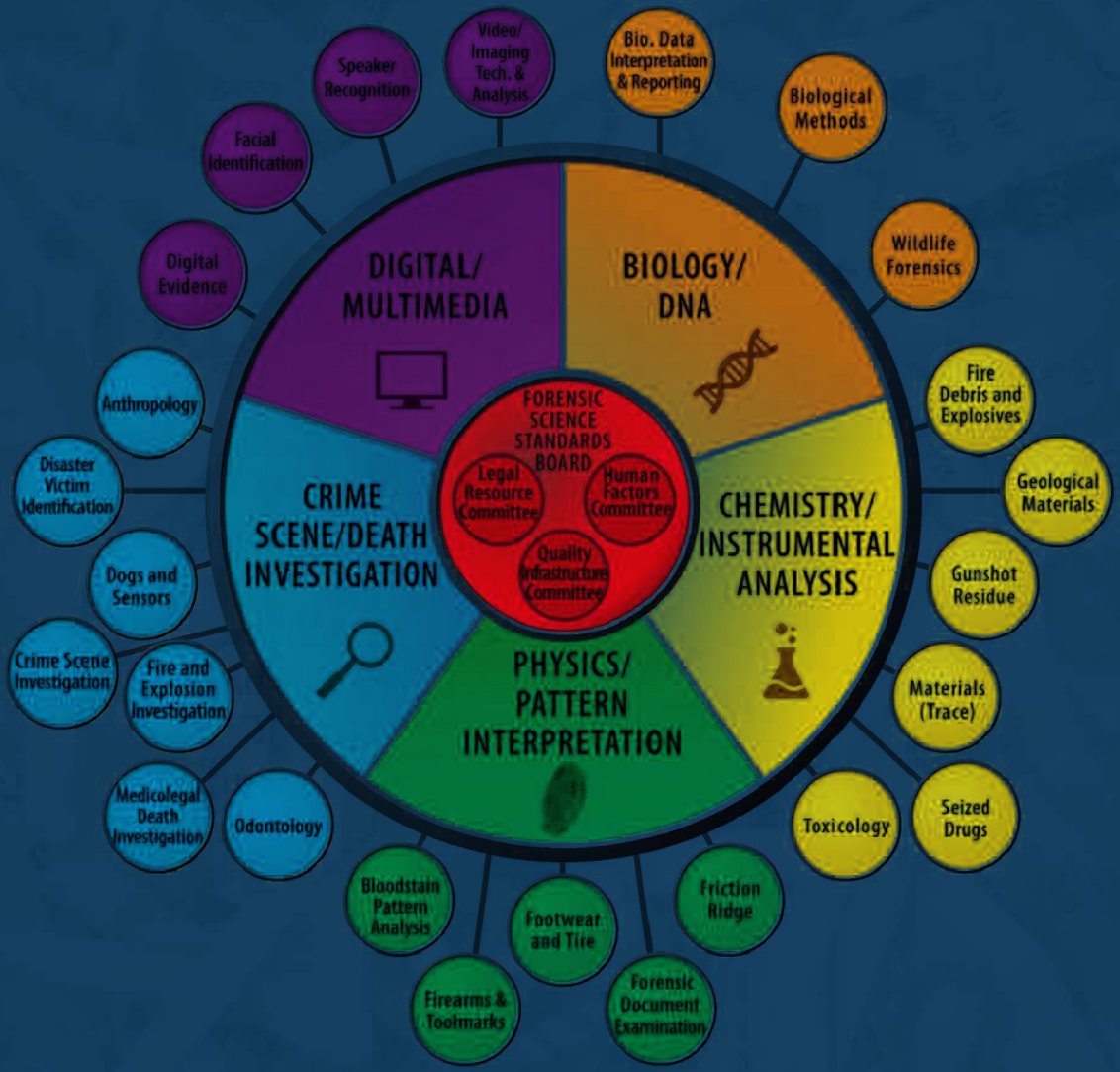
Adjective

"relating to or denoting the application of scientific methods and techniques to the investigation of crime."

Noun

"scientific tests or techniques used in connection with the detection of crime"

Organization of Scientific Area Committees for Forensic Science (OSAC)



CTSC

Digital Forensics

The application of scientific methods and techniques in the investigation of a computer crime.

NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response

The Digital Forensic Process

- Collection
- Examination
- Analysis
- Reporting

Process - Collection

- Collection of data
- Chain of custody

Process - Examination

- Data Extraction

Process - Analysis

- Timestamp synchronization
- Log interpretations
- Observations that validate or refute your hypothesis

Process - Reporting

- Conclusion
- Keep audience in mind
- Provide action items

Logistics

- Equipment
- Staffing
- Support

Equipment

- Write blockers
- Adapters
- Software
- Storage
- Chain of Custody forms
- Anti-static bags
- Examination Workstation
- Forensic Software
- Office space

Equipment - Office Space

- Secured Office
- Safe
- Encryption

Equipment - Forensic Workstation

- Ability to keep cases separate
- Lots of storage access (local or network)
- Additional speed for indexing
- Forensic Recovery of Evidence Device
  - Digital Intelligence
  - Built for forensics

Equipment - Storage

- Where do we store acquired images?
  - SAN
  - External storage
  - Network shares?
  - Optical?
  - Tape?

Equipment - Write Blockers

- Could be done via software writeblocks
- USB
- SATA
- PATA

Equipment - Software

- Forensic Suites
  - EnCase
  - FTK
- Volatile Acquisition
- Open Source Tools
  - Autopsy - Free
  - Kali Linux
  - SIFT

Equipment - Miscellaneous

- USB drives
- Chain of Custody forms
- Anti-static bags
- Evidence Bags
- Mouse jiggler
- Hot-plug kit
- Camera
- Voice Recorder
- Notebooks

Staffing

- Pattern recognition is a key skill
- Experience with the platform they are investigating
- Ability to work with others

Starting our your forensics program

- What do you need at a very minimum?
  - Policies
  - Staff
  - Workstation
  - Storage
    - Office/Data/evidence
  - Write Blockers

Growing your forensics program

- In-house procedures
- Expand storage to attached storage.
- Hardware based acquisition devices
- Upgrade forensics workstation
- Additional Training
- Look at enterprise level options like remote acquisition or suites for team analysis.

Other considerations

- How long to retain data?
- Do we need mobile forensics?

Core considerations

- Must be a repeatable process
- Tools and techniques must be easily repeated and/or accepted by the general forensic scientific community.
- Integrity of evidence must be maintained.
- Bias can often misdirect investigations.

Questions?

CTSC

CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Thank You

trustedci.org
@TrustedCI

We thank the National Science Foundation (grant 1547272) for supporting our work.