Digital Forensics

Dr K Rama Subramaniam
Vice Chairman
Information Security & Digital Forensics Research Foundation

Session – 1: Digital Forensics Foundations

- Basics of Forensics as a discipline
- Evolution of Digital Forensics
- Digital Forensics Taxonomy
- Forensics in the context of open source technologies

Session – 1: Digital Forensics Foundations

Basics of Forensics as a discipline

- **Forensic science** is the scientific method of gathering and examining information about the past which is then used in a court of law.
- The word forensic comes from the Latin term *forēnsis*, meaning "of or before the forum."

Computer Society of India - Thiruvananthapuram
Program on Digital Forensics

Session – 1: Digital Forensics Foundations

Basics of Forensics as a discipline

- **Forensic science** is the scientific method of gathering and examining
- ~~information about the past~~ which is then used in a court of law.
  E V I D E N C E
- The word forensic comes from the Latin term *forēnsis*, meaning "of or before the forum."

Session – 1: Digital Forensics Foundations

Basics of Forensics as a discipline

- **Forensics is all about evidence**
- **FORENSICS requires**
  - **Identification of Evidence**
  - **Preservation of Evidence**
  - **Analysis of Evidence and *Interpretation***
  - **Presentation of Evidence**

Session – 1: Digital Forensics Foundations

Evolution of Digital Forensics

- The increasing menace of Cyber Crimes
  - Motivation
  - Financial compensation
  - Risk of committing crimes
  - Routine Activity theory of Felson & Cohen
  - Geo-spatial spread
  - Trans-border attack vectors

Session – 1: Digital Forensics Foundations

Evolution of Digital Forensics

- Application of Key Principles of Forensics to Digital Forensics
  - **Frye Principle** – for the results of a scientific technique to be admissible, the technique must be sufficiently established to have gained general acceptance in the particular field
  - **Coppolino Principle** – a novel or new form of evidence or interpretation can be accepted if a strong conceptual foundation can be laid even if such a piece of evidence or interpretation is new to the profession as a whole
  - **Marx Principle** – the assessor / interpreter of the evidence is satisfied that common sense in understanding and evaluating the evidence is not sacrificed
  - **Daubert Principle** – The validity, reliability, benchmarking, algorithms and error rates of any evidence investigation process must be tested rigorously before accepting the evidence interpretation

Session – 1: Digital Forensics Foundations

Digital Forensics Taxonomy

- Taxonomy in evolutionary phase
- Classical definition of Digital Evidence (by Krause and Heiser):
  - Preservation
  - Identification
  - Extraction
  - Documentation
  - Interpretation of computer media for evidentiary and / or root cause analysis

Session – 1: Digital Forensics Foundations

Digital Forensics Taxonomy

Tending to prove a particular proposition

- Information of probative value stored or transmitted in digital form
  - *Scientific Working Group on Digital Evidence*
- Information stored or transmitted in binary form that may be relied upon in court
  - *International Organization for Computer Evidence*

Computer Society of India - Thiruvananthapuram
Program on Digital Forensics

Session – 1: Digital Forensics Foundations

Digital Forensics Taxonomy

- "Electronic Form Evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.

  - Sec 79A of Information Technology Act, 2000.
    [As amended by Information Technology (Amendment) Act 2008]

Session – 1: Digital Forensics Foundations

Digital Forensics Taxonomy

- "Computer Evidence" is not defined in IT Act but has to be read in conjunction with Indian Evidence Act
- Electronic records are defined in Sec. 2(1)(t) of the IT Act and their admissibility as evidence is dealt with in Sec 65B of the Indian Evidence Act
- Supreme Court Judgment in *Anvar vs Basheer* (delivered on 18 Sept 2014) fortifies concept of admissibility of Electronic records as evidence

Computer Society of India - Thiruvananthapuram
Program on Digital Forensics

Session – 1: Digital Forensics Foundations

Digital Forensics Taxonomy

- "***electronic record***" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche - Sec 2 (1)(t) of Indian IT Act
- …any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein or which direct evidence would be admissible.
  - Sec 65B of Indian Evidence Act

Session – 1: Digital Forensics Foundations

Digital Forensics Taxonomy

- Conditions for accepting ***electronic record*** as evidence:
  (i) at the time of the creation of the electronic record, the computer that produced it must have been in regular use;
  (ii) the kind of information contained in the electronic record must have been regularly and ordinarily fed in to the computer;
  (iii) the computer was operating properly; and,
  (iv) the duplicate copy must be a reproduction of the original electronic record.

- from Sec 65B (2) of Indian Evidence Act

Computer Society of India - Thiruvananthapuram
Program on Digital Forensics

Session – 1: Digital Forensics Foundations

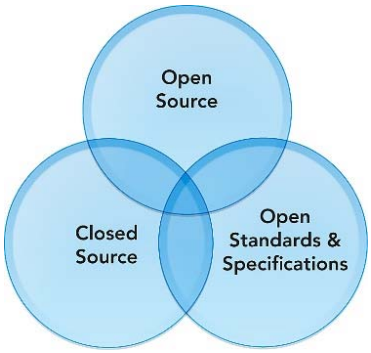
Digital Forensics Taxonomy

- If data are stored by computer or similar device, any print out or other output readable by sight, shown to reflect the data accurately, is an original

- US Federal Rules of Evidence 1001-3

Session – 1: Digital Forensics Foundations

Forensics in the context of open source technologies



Open source software is software in which the **source** code used to create the program is freely available for the public to view, edit, and redistribute.

What does it mean for the Forensic Investigator?

Computer Society of India - Thiruvananthapuram
Program on Digital Forensics

Session – 1: Digital Forensics Foundations
Forensics in the context of open source technologies

- Growth of Open Source Forensic Tools
- Research findings on problems in using Open Source Forensic Tools
- Challenges in proving ‘reliability’ of Open Source Forensic Tools

Session – 2: Technological Dimensions of Digital Forensic Investigation

- The digital forensics Life Cycle
- Creating forensically relevant evidence from Information systems and information processing facilities
- Standards and 'best practice' guidelines for digital forensics practitioners

Session – 2: Technological Dimensions of Digital Forensic Investigation

The Digital Forensics Life Cycle

- Digital Forensic investigation is NOT an ad-hoc process
- It is NOT just about tools
- It is ALL about EVIDENCE
- It is all about INTERPRETATION of EVIDENCE

Computer Society of India - Thiruvananthapuram

Program on Digital Forensics

Session – 2: Technological Dimensions of Digital Forensic Investigation

The Digital Forensics Life Cycle

The problem of DISCOVERY is applicable to Digital Investigation as much as it does to traditional crime investigation

www.isdfr.org

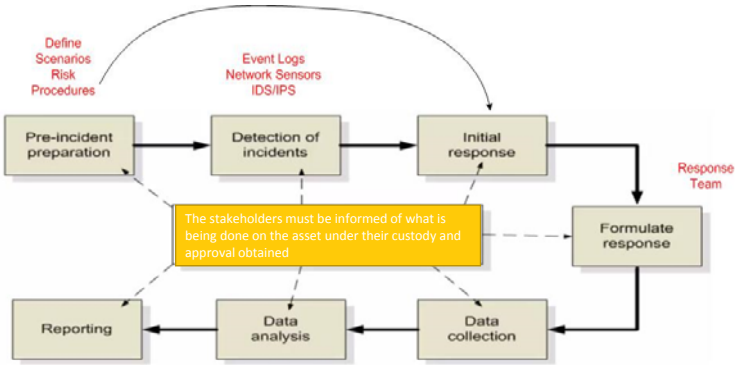
ISDFRF

Computer Society of India - Thiruvananthapuram

Program on Digital Forensics

Session – 2: Technological Dimensions of Digital Forensic Investigation

The Digital Forensics Life Cycle



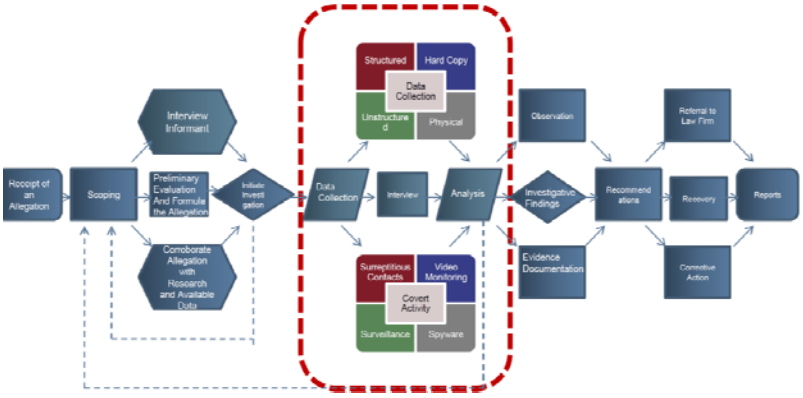
Is there anything we can do to be ready for Digital Forensic Processes to succeed?

www.isdfr.org

ISDFRF

Session – 2: Technological Dimensions of Digital Forensic Investigation

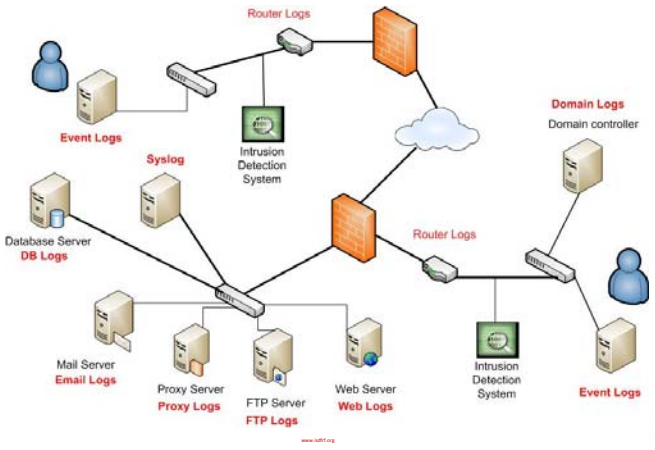
The Digital Forensics Life Cycle



Computer Society of India - Thiruvananthapuram
Program on Digital Forensics

Session – 2: Technological Dimensions of Digital Forensic Investigation

The Digital Forensics Life Cycle



Session – 2: Technological Dimensions of Digital Forensic Investigation

The Digital Forensics Life Cycle

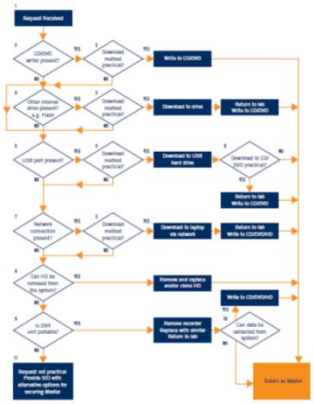
Computer Society of India - Thiruvananthapuram
Program on Digital Forensics

Session – 2: Technological Dimensions of Digital Forensic Investigation

The Digital Forensics Life Cycle

- Admissibility of evidence
  - Relevant
  - Foundation of admissibility
  - Legally permissible
- Related areas of importance
  - Establish MOM
  - *<mens rea>* and *<actus rea>*

Creating Forensically Relevant Evidence is not through flashes of brilliance; it is through very clearly designed processes that are followed meticulously



Source: The ACPO Good Practice Guide for Computer-Based Electronic Evidence

Session – 2: Technological Dimensions of Digital Forensic Investigation

Creating Forensically Relevant Evidence

- Admissibility of evidence
  - Relevant
  - Foundation of admissibility
  - Legally permissible
  - Evidence identification
  - Preservation of evidence

Session – 2: Technological Dimensions of Digital Forensic Investigation

Creating Forensically Relevant Evidence

- Relevant
  - Proof that crime occurred
  - Documentation of events/time frame
  - Identification of acts/methods
  - Proof linking suspects - acts/methods
  - Proof of suspect's motives

Computer Society of India - Thiruvananthapuram
Program on Digital Forensics

Session – 2: Technological Dimensions of Digital Forensic Investigation

Creating Forensically Relevant Evidence

- Foundation Requirements - Demonstrate trustworthiness
  - Custodian identity
  - Custodian familiarity with IT record procedures
  - Description of procedures
  - Precautions against errors
  - Error correction
  - Established normal business methods

Session – 2: Technological Dimensions of Digital Forensic Investigation

Creating Forensically Relevant Evidence

- Legally Permissible
  - Unconstitutional obtaining of evidence
  - Unlawful search & seizure
  - Secret recording (except authorized by court)
  - Questionable privacy violations (access to personal data)
  - Forced confessions/statements

Computer Society of India - Thiruvananthapuram
Program on Digital Forensics

Session – 2: Technological Dimensions of Digital Forensic Investigation

Creating Forensically Relevant Evidence

- Identifying and Preserving Evidence
  - Concept of Chain of Custody
  - Demonstrating to Court – evidence is reliable

Session – 2: Technological Dimensions of Digital Forensic Investigation

Creating Forensically Relevant Evidence

- Who is involved
  - Scientific Working Group on Digital Evidence (SWGDE)
  - Scientific Working Group for Imaging Technologies (SWGIT)
  - International Organization on Computer Evidence (IOCE)
  - Forensic Computing Group, United Kingdom
  - European Network of Forensic Science Institutes
  - National Institute of Justice, United States Department of Justice (NIJ)
  - High Tech Crime Sub-Group of the G-8
  - Interpol – Technology Crimes Group
  - Council of Europe

Session – 3: Digital Forensics Process – Legal Perspectives

- The mismatch between law and technology in cybercrime investigation.
  - How can the technologists help?
- Specific issues arising from common law dispensation –
  - commingling of data;
  - evidence in normal course of business;
  - jurisdictional arbitrage.

Session – 4: Criminological and Victimological aspects of Digital Forensic Investigation

- Failure of shaming theory and its impact on digital forensics investigation
- Tenets of societal response to crime - challenges in digital forensics investigation
- Application of Lockard's Exchange Principle to technology crimes – how does a digital forensic investigator benefit?
- Victim's role in enhancing or thwarting digital forensics investigation
- Applying Sutherland's findings on white collar crimes to cybercrimes – shifting focus of digital forensics

ISDFRF

Thank you for coming

rama@valiant-technologies.com