Digital Forensics Research: A Roadmap

Women in Forensic Computing
March 28, 2022

Presented by: Mariya Shafat Kirmani
Ph.D. Scholar (Digital Forensics)
Department of Electronics and Instrumentation Technology,
University of Kashmir, India.
mariyakirmani@gmail.com

Agenda

- **Digital Forensics**
  - **Introduction**
  - **Why?**
  - **How?**

- **Digital Forensics Research**
  - **Goal- Digital Evidence**
  - **Challenges**
  - **Research Directions**

Presented and designed by Mariya Shafat Kirmani

March 28, 2022

Why Digital Forensics?

Cyber Security

Cyber Security Incident

Digital Forensics

Presented and designed by Mariya Shafat Kirmani

Women in Forensic Computing

March 28, 2022

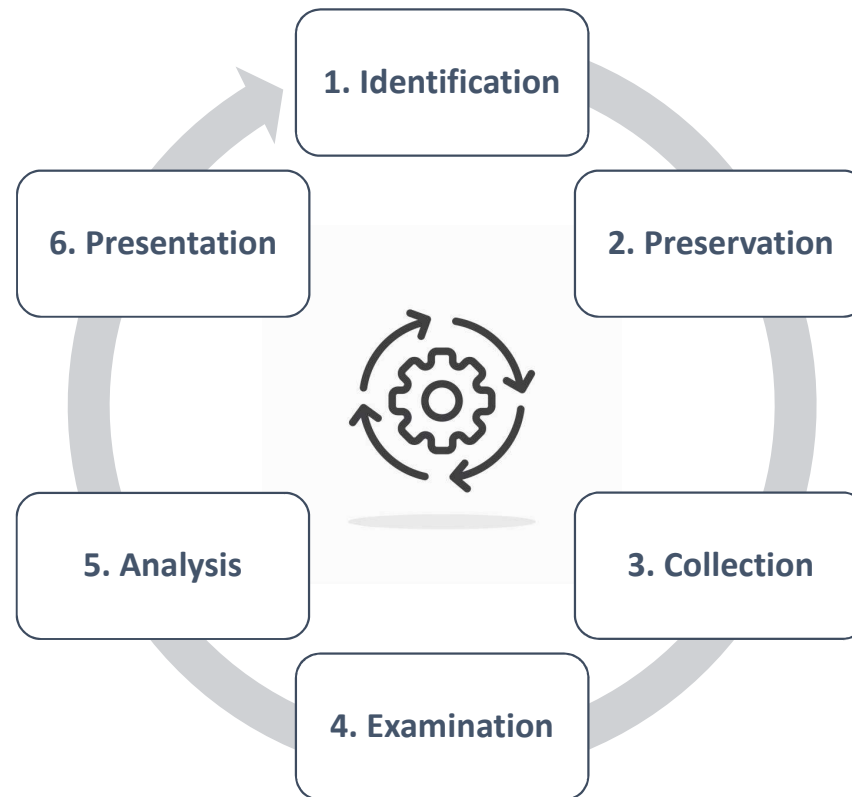# Digital Forensics History

1978 — The first cybercrimes recognized (1978, Florida Computer Crimes Act)

1980 — Federal laws begin to incorporate computer offenses

1984 — FBI launches Computer Analysis and Response Team

1992 — Computer forensics first used in academic literature

1993 — FBI hosted the first International conference on computer evidence at the FBI Academy in Quantico, Virginia

1995 — Same conference was held in Baltimore (World Organization on Computer Evidence (IOCE) was formed)

2001 — First Digital Forensics Research Workshop was held

2002 — The Scientific Working Group on Digital Evidence (SWGDE) produce Best Practices for Computer Forensics

2004 — The Convention of Cybercrime comes into force (treaty signed by 43 nations)

2005 — ISO standard for digital forensics released (ISO 17025)

2010 — Simson Garfinkel recognized issues facing digital investigation.

05-04-2022

Presented and designed by Mariya Shafat Kirmani

WinFC
Women in Forensic Computing
March 28, 2022

Digital Forensics Process

The process cycle: 1. Identification → 2. Preservation → 3. Collection → 4. Examination → 5. Analysis → 6. Presentation

Presented and designed by Mariya Shafat Kirmani

Women in Forensic Computing

March 28, 2022

Digital Forensic Research- What should you know?

- **What are the requirements of digital forensic consumers?**

- **What are the challenges faced by digital forensic experts?**

- **What are the specific research directions in the digital forensics field?**

Presented and designed by Mariya Shafat Kirmani

Women in Forensic Computing
March 28, 2022

What is at the heart of Digital Forensics?

Digital Evidence

Chain of Custody

Event Reconstruction

Forensic Soundness

Presented and designed by Mariya Shafat Kirmani

Women in Forensic Computing

March 28, 2022

Digital Evidence

Digital Evidence- Attributes

- **Latent**
- **Borderless**
- **Fragile**
- **Time Sensitive**

Digital Evidence- Management

- **Acquisition**
- **Storage**
- **Organization**
- **Chain of Custody**
- **Archival**

Presented and designed by Mariya Shafat Kirmani

WinFC
Women in Forensic Computing
March 28, 2022

Digital Forensic Challenges

Technical
- Volume of Data
- Heterogeneity
- Cloud Computing
- Internet of Things
- Big Data
- Anti-forensics
- Resilient Tools & Automation

Personnel-related
- Lack of Qualified Personnel (Training, Education, Certification)
- Semantic Disparities
- Licensing Requirements

Operational
- Lack of Standardization
- Training, Experience, & Skills
- Adversarial Tactics

Legal
- Jurisdiction
- Political Issues
- Admissibility of Tools & Techniques
- Privacy
- Ethical Issues

WinFC
Women in Forensic Computing
March 28, 2022

Digital Forensics Research Directions

- **Malware Forensics**
- **Network Forensics**
- **Memory Forensics**
- **Mobile Device Forensics**

- **IoT Forensics**
- **Cloud Forensics**
- **Big Data Forensics**
- **Distributed Processing**
- **Machine Learning & Data Mining**

Presented and designed by Mariya Shafat Kirmani

Digital Forensics Research- Mobile Phones

Mobile Phone Forensics

IoT Forensics

Your network is only as secure as your weakest point!

Presented and designed by Mariya Shafat Kirmani

WinFC

Women in Forensic Computing

March 28, 2022

Digital Forensics- Skills you should have

- **Technical Aptitude**
  - **Digital Comprehension**
  - **Networking**
  - **Operating System**
  - **Programming**
- **Attention to detail**
- **An understanding to Law and Criminal Investigation**
- **Communication Skills**
- **Cyber Security Fundamentals**
- **Analytical Skills**
- **Desire to Learn**

Presented and designed by Mariya Shafat Kirmani

WinFC
Women in Forensic Computing
March 28, 2022

Digital Forensics- Certifications

Vendor-neutral Certifications:

- **GIAC Certified Forensic Examiner (GCFE)**
- **GIAC Advanced Smartphone Forensics (GASF)**
- **GIAC Certified Forensic Analyst (GCFA)**
- **GIAC Network Forensic Analyst (GNFA)**
- **GIAC Cyber Threat Intelligence (GCTI)**
- **GIAC Reverse Engineering Malware (GREM)**
- **CDFE (Certified Digital Forensics Examiner): NICCS**
- **CHFI (Computer Hacking Forensic Investigator): EC-Council**
- **CFCE (Certified Forensic Computer Examiner): IACIS**

- …

Vendor-specific Certifications:

- **EnCE (EnCase Certified Examiner): OpenText**
- **EnCEP (EnCase Certified eDiscovery Practitioner): OpenText**
- **Exterro ACE (AccessData Certified Examiner)**

- …

Presented and designed by Mariya Shafat Kirmani

WinFC
Women in Forensic Computing
March 28, 2022

Digital Forensics Research- The Path Forward

- **What is the vision for digital forensic investigation?**
- **What should be prioritized to achieve the goals?**

Presented and designed by Mariya Shafat Kirmani

Women in Forensic Computing

March 28, 2022

Presented and designed by Mariya Shafat Kirmani

March 28, 2022

Much Love from Kashmir...