• While digital forensics plays a key role in cybersecurity, it is also a recognised and developing forensic science discipline
• As a forensic science discipline it needs to comply with established forensic science principles to continue to justify its place as a forensic science
• The development of scientifically validated models can assist in this
• Considered the core of forensic science:
  • Transfer (Locard Exchange Principle)
  • Identification (Placing Objects in a Class)
  • Individualisation (Narrowing the Class to One)
  • Association (Linking a Person with the Event)
  • Reconstruction (Understanding the Sequence of Past Events)
• Classification is a core part of the Identification principle in the Inman-Rudmin Paradigm
• Having a clear classification model can help investigators and legal practitioners better understand the digital evidence at a conceptual level
• V1 of the model published in 2014
• Scientific validation identified shortcomings in the V1 model
• V2 model developed based on validation findings
DIGITAL EVIDENCE CLASSIFICATION MODEL

Physical Evidence

- Physical Media
  - Fingerprint
  - DNA
  - Tool marks
  - Bits

- Transmission Media
  - Waves
  - Particles
DIGITAL EVIDENCE CLASSIFICATION MODEL

Logical Digital Evidence

Trace Digital Evidence

Transmission Digital Evidence

Physical Evidence

Physical Media: Fingerprint, DNA, Tool marks, Bits

Transmission Media: Waves, Particles
DIGITAL EVIDENCE CLASSIFICATION MODEL

Logical Digital Evidence

Trace Digital Evidence

Transmission Digital Evidence

User Created Artefacts

Application Artefacts

Operating System Artefacts

File System Artefacts

Physical Evidence

Physical Media
- Fingerprints
- DNA
- Tool marks
- Bits

Transmission Media
- Waves
- Particles

User Created Artefacts

Application Artefacts

Operating System Artefacts

File System Artefacts
DIGITAL EVIDENCE CLASSIFICATION MODEL

Logical Digital Evidence

User Created Artefacts

Application Artefacts

Operating System Artefacts

File System Artefacts

Trace Digital Evidence

Logical User Created Artefacts

Logical Application Artefacts

Logical Operating Artefacts

Logical File System Artefacts

Transmission Digital Evidence

Physical Evidence

Physical Media

Fingerprints

DNA

Tool marks

Bits

Transmission Media

Waves

Particles

BUILDING A DIGITAL EVIDENCE CLASSIFICATION MODEL

8
DIGITAL EVIDENCE CLASSIFICATION MODEL
DIGITAL EVIDENCE CLASSIFICATION MODEL

User Created Artefacts
- Logical User Created Artefacts
- Reconstructed User Created Artefacts
- Trace User Created Artefacts

Application Artefacts
- Logical Application Artefacts
- Reconstructed Application Artefacts
- Trace Application Artefacts

Operating System Artefacts
- Logical Operating Artefacts
- Reconstructed Operating System Artefacts
- Trace Operating System Artefacts

File System Artefacts
- Logical File System Artefacts
- Reconstructed File System Artefacts
- Trace File System and Protocol Artefacts

Physical Evidence
- Physical Media: Fingerprints, DNA, Tool marks, Bits
- Transmission Media: Waves, Particles

BUILDING A DIGITAL EVIDENCE CLASSIFICATION MODEL
• Validation testing of V2 model
• Publication of peer reviewed paper in reputable and widely read academic journal
• Acceptance of the model by the broader forensic science community