



# BUILDING A DIGITAL EVIDENCE CLASSIFICATION MODEL

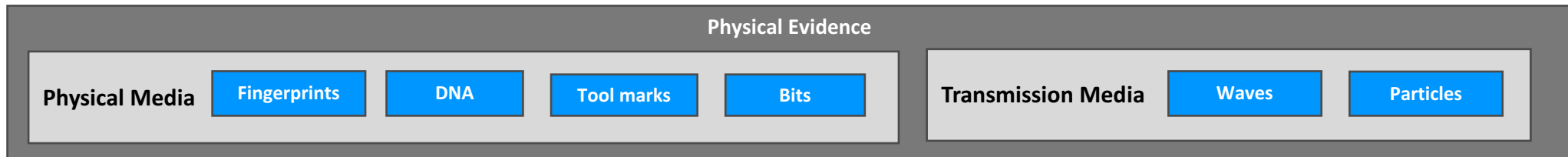
- While digital forensics plays a key role in cybersecurity, it is also a recognised and developing forensic science discipline
- As a forensic science discipline it needs to comply with established forensic science principles to continue to justify its place as a forensic science
- The development of 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*)

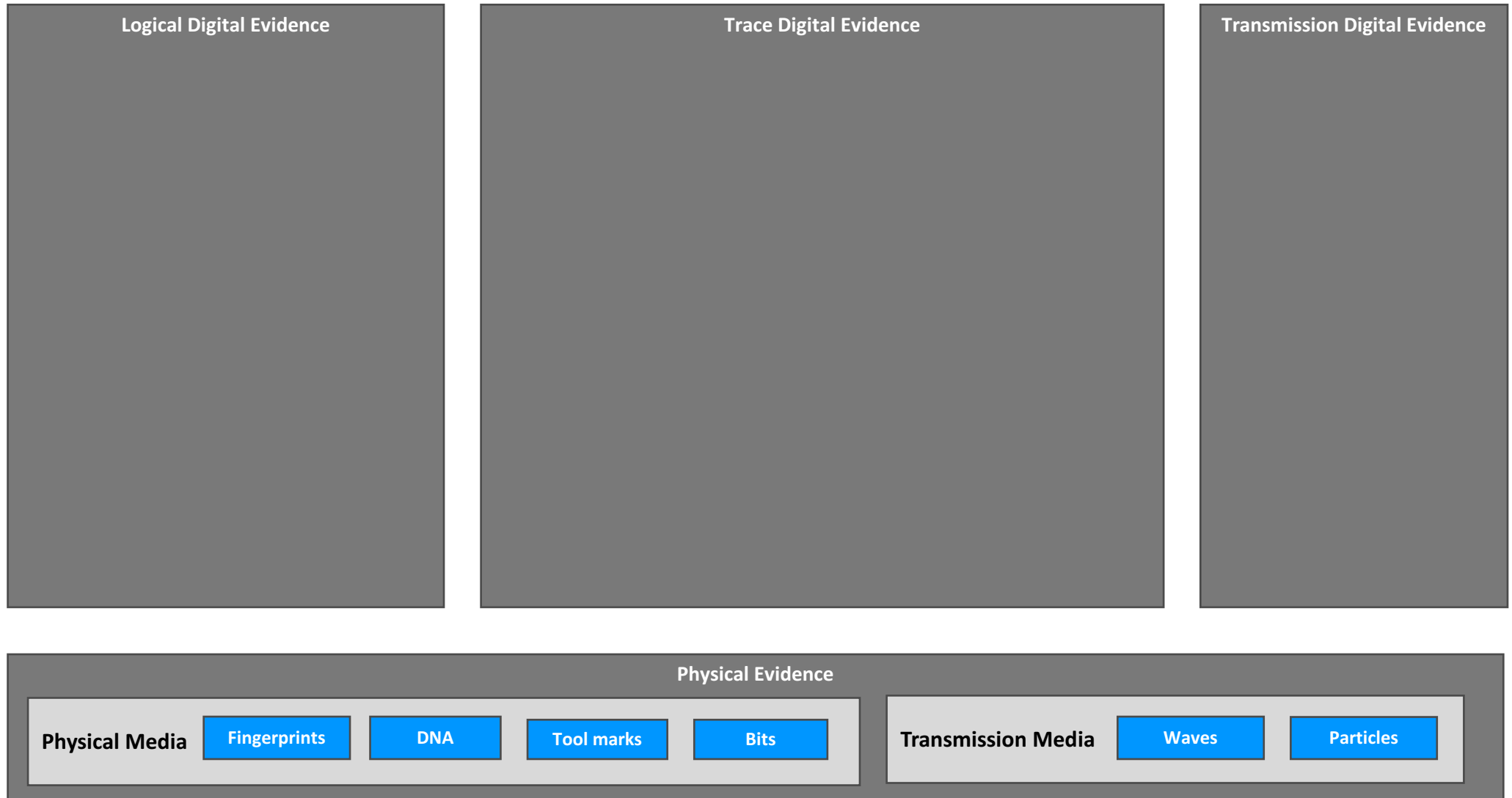
## THE NEED FOR A DIGITAL EVIDENCE CLASSIFICATION MODEL

- 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

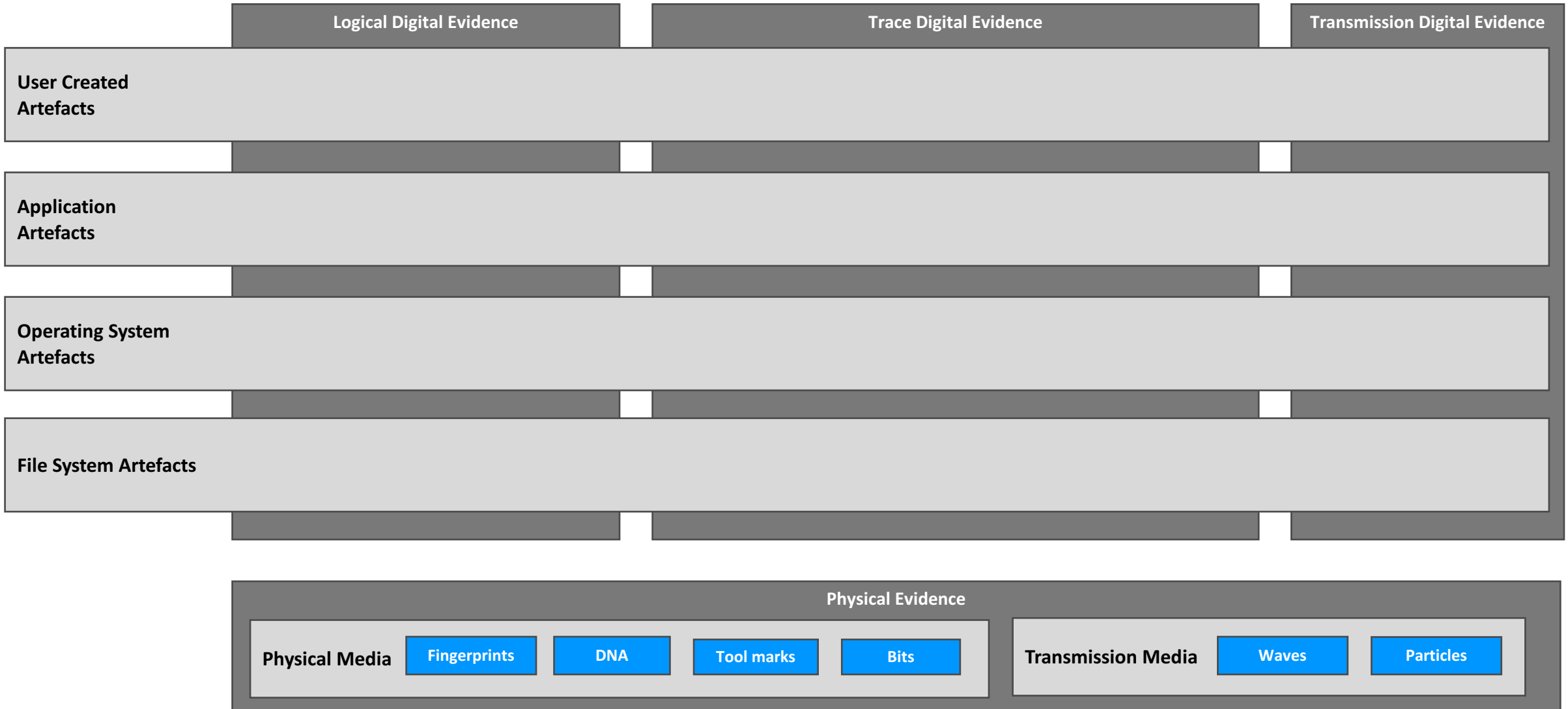
# DIGITAL EVIDENCE CLASSIFICATION MODEL



# DIGITAL EVIDENCE CLASSIFICATION MODEL



# DIGITAL EVIDENCE CLASSIFICATION MODEL

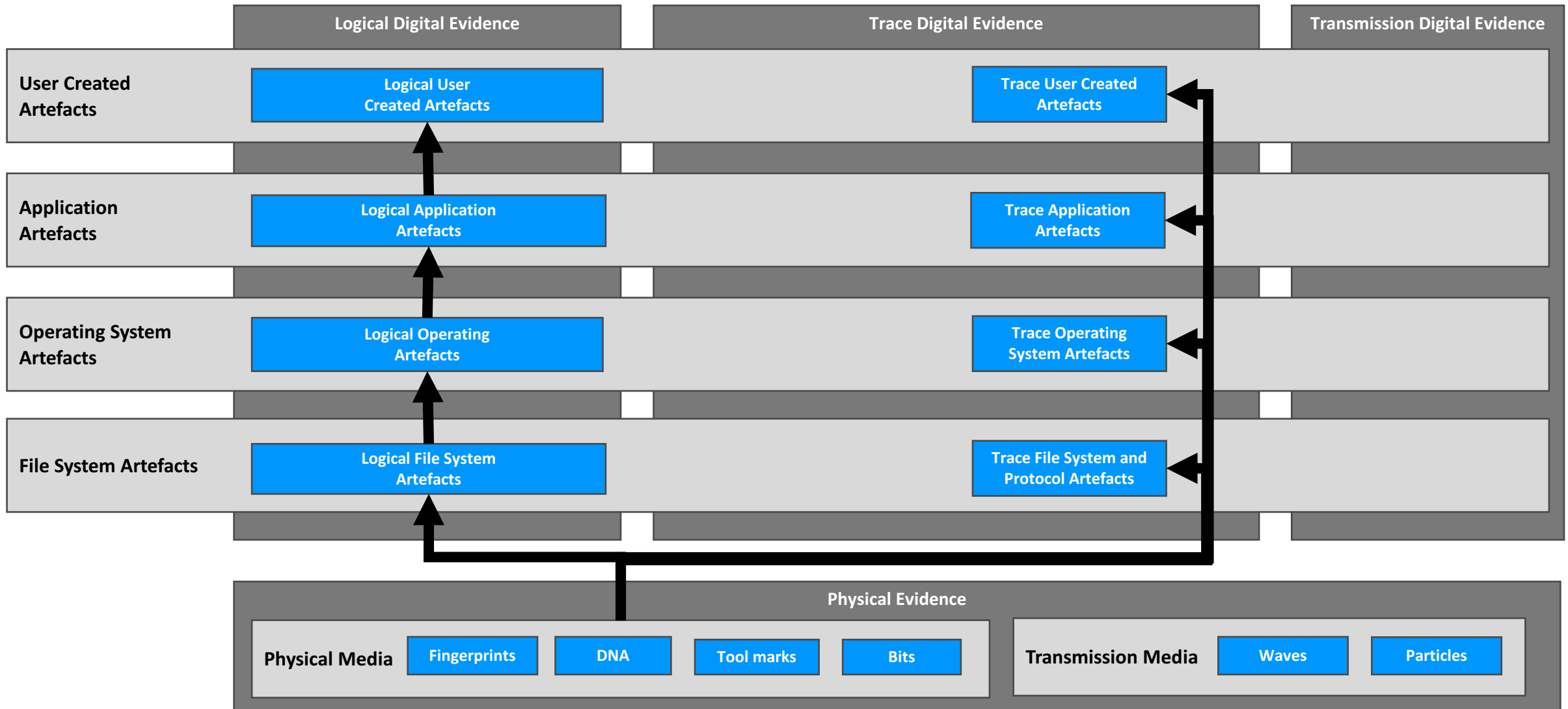


# DIGITAL EVIDENCE CLASSIFICATION MODEL

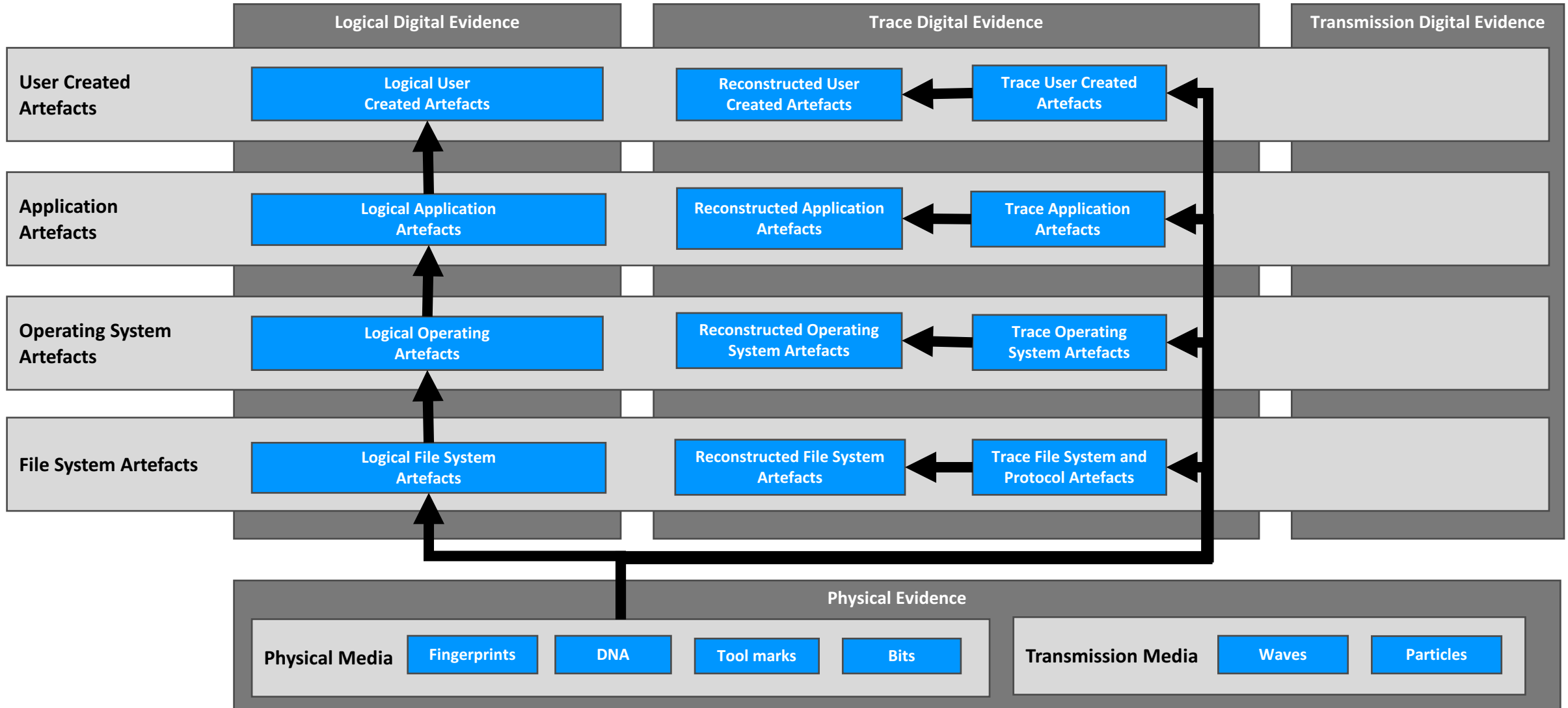




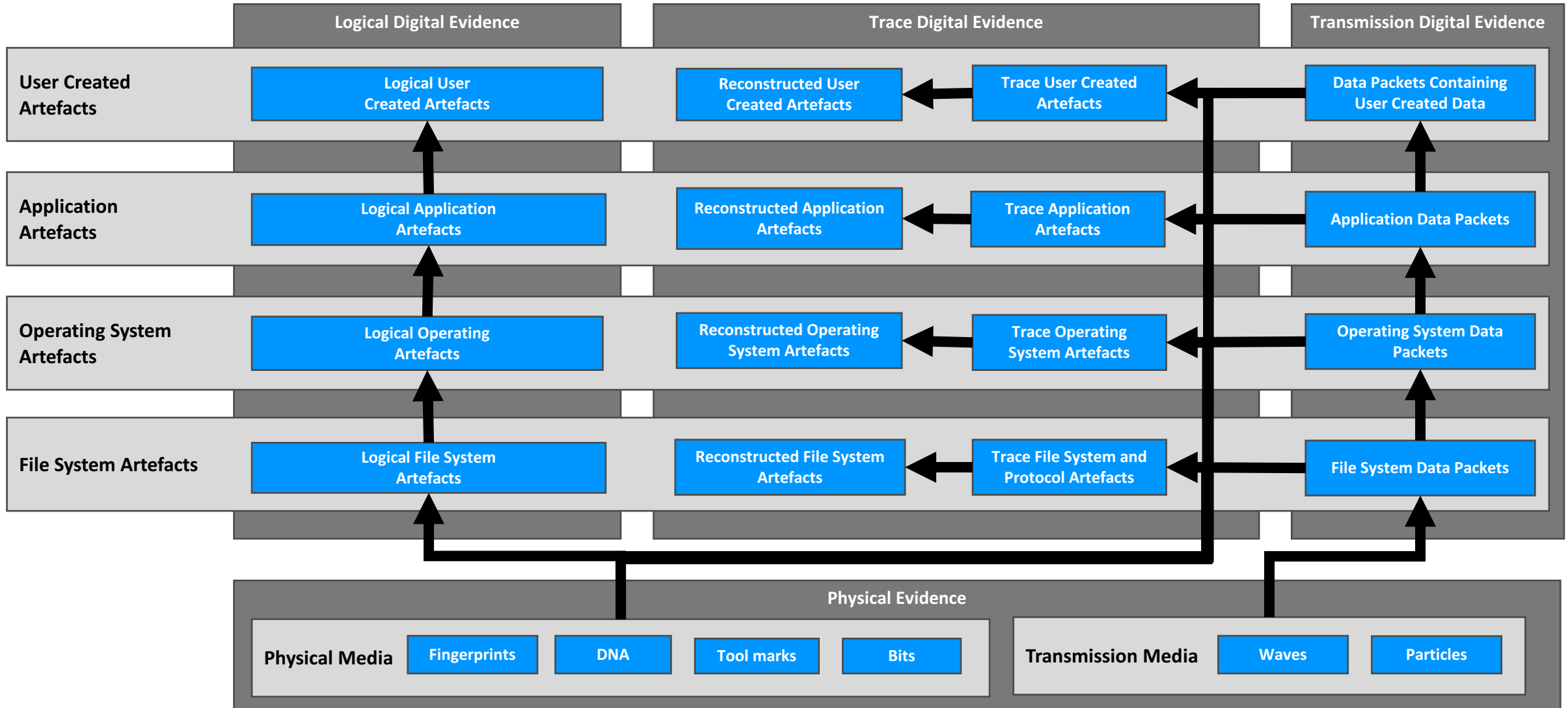
# DIGITAL EVIDENCE CLASSIFICATION MODEL



# DIGITAL EVIDENCE CLASSIFICATION MODEL



# 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

# SANS DFIR RESOURCES AND CONTACT INFORMATION



## PRESENTER CONTACT

Jason Jordaan  
Email: [jason@dfirlabs.com](mailto:jason@dfirlabs.com)  
Twitter: [@DFS\\_Jasonj](https://twitter.com/DFS_Jasonj)



## SANS INSTITUTE

8120 Woodmont Ave., Suite 310  
Bethesda, MD 20814  
301.654.SANS(7267)



## DFIR RESOURCES

[digital-forensics.sans.org](http://digital-forensics.sans.org)  
Twitter: [@sansforensics](https://twitter.com/sansforensics)



## SANS EMAIL

GENERAL INQUIRIES: [info@sans.org](mailto:info@sans.org)  
REGISTRATION: [registration@sans.org](mailto:registration@sans.org)  
TUITION: [tuition@sans.org](mailto:tuition@sans.org)  
PRESS/PR: [press@sans.org](mailto:press@sans.org)