Issues in Building the Digital Forensics Bridge From Computer Science to Judicial Science

By

Michael Losavio, Deborah Wilson, Adel Elmaghraby, James Graham, S. Srinivasan, David Elder, Marcus Rogers

Presented At

The Digital Forensic Research Conference

DFRWS 2006 USA Lafayette, IN (Aug 14th - 16th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Working Between Disciplines

Issues in Building the Digital Forensics Bridge

From Computer Science to Judicial Science

Dr. Marcus Rogers & Mr. Michael Losavio, Esq., Panel Chairs

August 14, 2006, Purdue University

DFRWS 2006

University of Louisville Panel

- **Dr. Deborah Wilson,** (Department Chair), Justice Administration Department, College of Arts and Sciences
- **Mr. David Elder,** S.A.C. (retired), FBI, Kentucky, visiting professor, Justice Administration Department, project manager, Kentucky RCFL
- **Dr. Adel Elmaghraby** (Department Chair), Professor, Computer Engineering and Computer Science Department, Speed School of Engineering
- **Dr. S. Srinivasan**, Professor, Computer Information Systems Department, School of Business

Digital Forensics

& The Admissibility of Digital Evidence

"Digital forensics is the scientific study of the processes involved in extracting, analyzing and preserving all forms of electronic evidence."

IFIP Working Group 11.9 Digital Forensics

Concerns

- Scientific and engineering analysis re: digital objects, e.g. Lyle, "A Strategy for Testing Hardware Write Block Devices;" Khanna, et al, "A Survey of Forensic Characterization Methods for Physical Devices."
- Facts of digital evidence that impact use and rules of evidence *(reliability & persuasion)*
- *"We're still staffing this as if it's still 20% [of our caseload]* [Anonymous, DFRWS 2006]

The Bridge

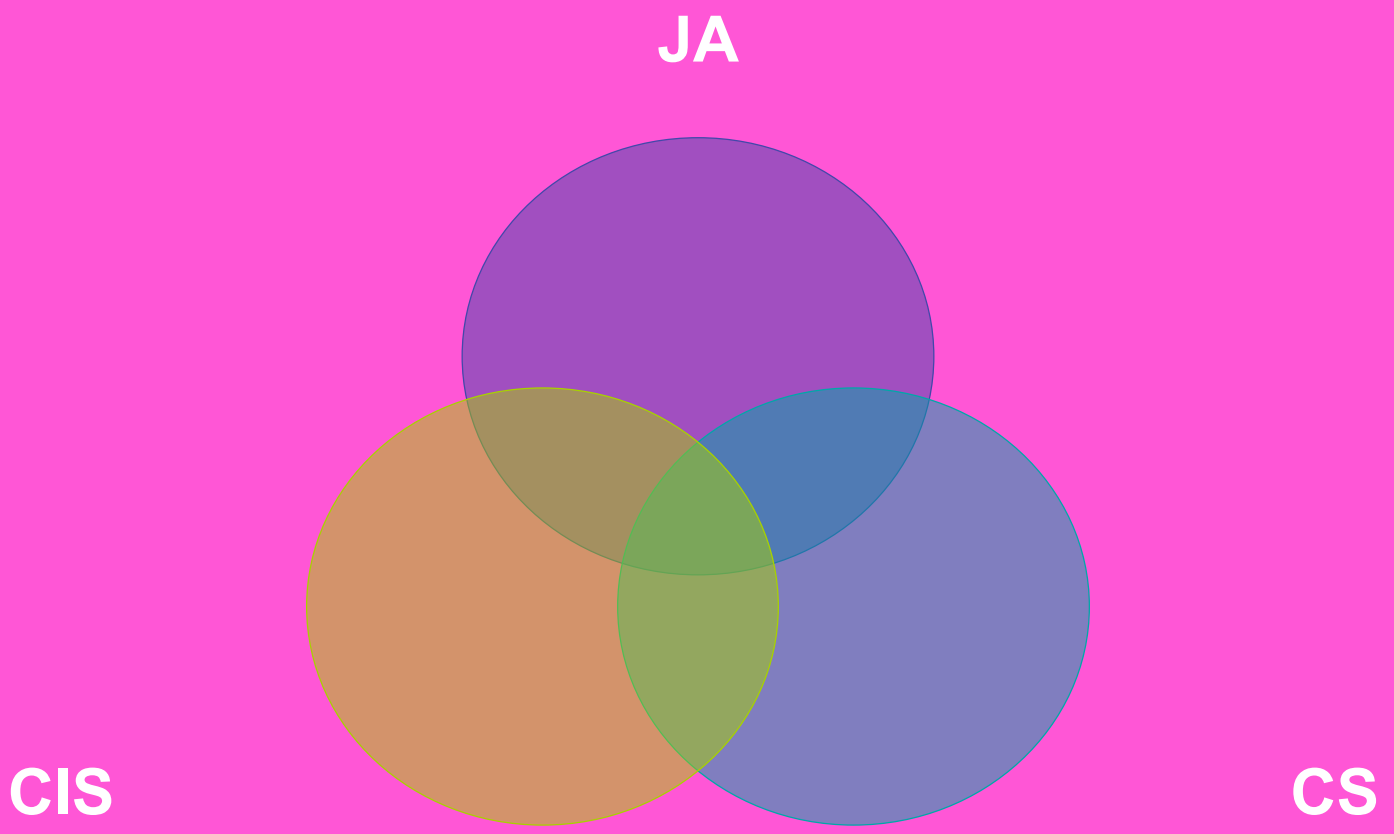
From

Justice Administration <=> Computer Information Systems <=> Computer Science

Or perhaps just trying not to fall…

The Intersection of Disciplines

justice administration (**JA**)
computer information systems (**CIS**)
computer science and engineering (**CS**)



It's Not Just Us,

- Others have issues with the study, investigation and legal use of digital evidence
  - Kerr, Orin "Digital Evidence and the New Criminal Procedure" 105 Colum. L. Rev. 279 (January 2005) & Treglia, Stephen "Criminal Law's Slow Evolution on Electronic Discovery", 95 New York Law Journal 5 (May, 2004).
  - Brinson & Robinson "A Cyber Forensics Ontology:Creating a New Approach to Studying Cyber Forensics (DFRWS 2006) ; Ieong, " FORZA- Digital Forensics Investigation Framework that Incorporates Legal Issues" (DFRWS 2006)
  - Lindsey, *Comment on Issues with Usability & Visualization*, DFRWS 2006

The view from the end of the bridge

- We will review as to digital forensics futures
  - Managerial/administrative,
  - educational/training and
  - judicial/legal issues

Regional Computer Forensics Laboratories

- Issues in implementing a reliable computer forensics laboratory for justice purposes, including
  - administrative,
  - financial
  - and liaison with law enforcement, courts and the academy.

Teaching and Training

- Challenges for introducing digital forensics into academic education,
  - pedagogy,
  - training and
  - adult education.

The Legal & Judicial Systems

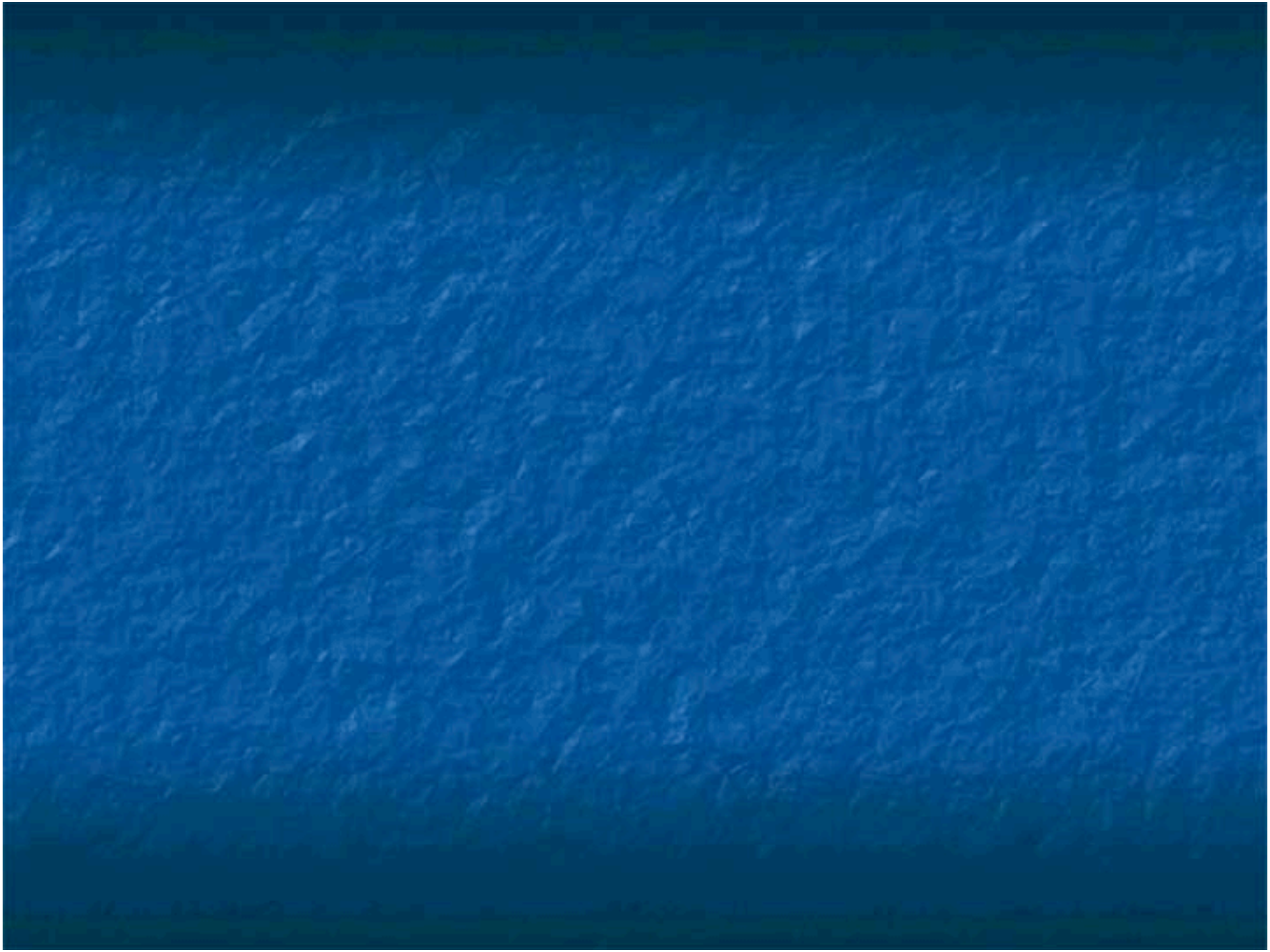
- Action and response issues within the justice system itself, including
  - the "presumption of reliability,"
  - authentication challenges v. expert evidence challenges and
  - "weight" along the evidentiary spectrum *(the bridge from suspicion to conviction)*.

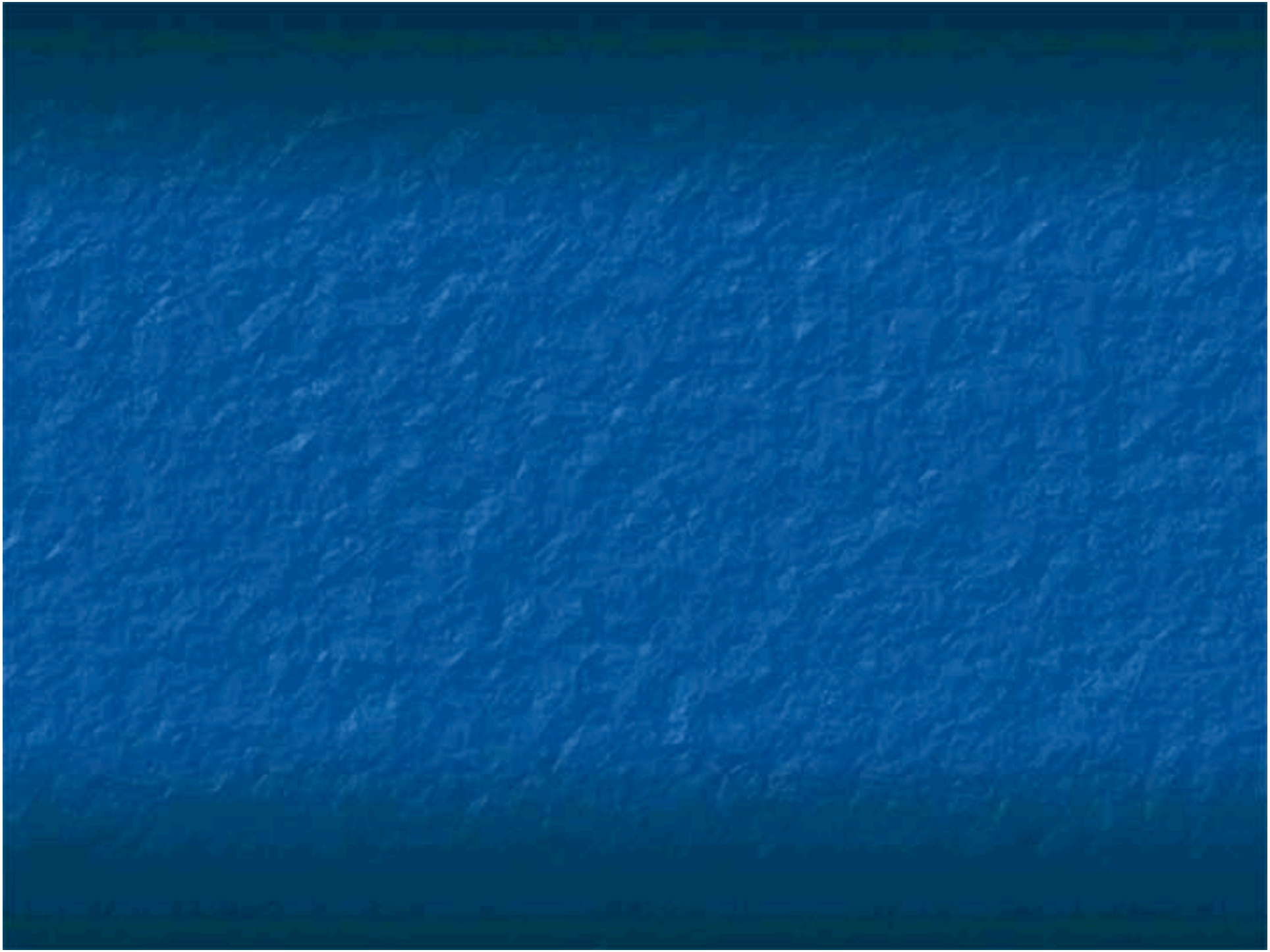
Judicial/Legal Considerations
for electronic evidence

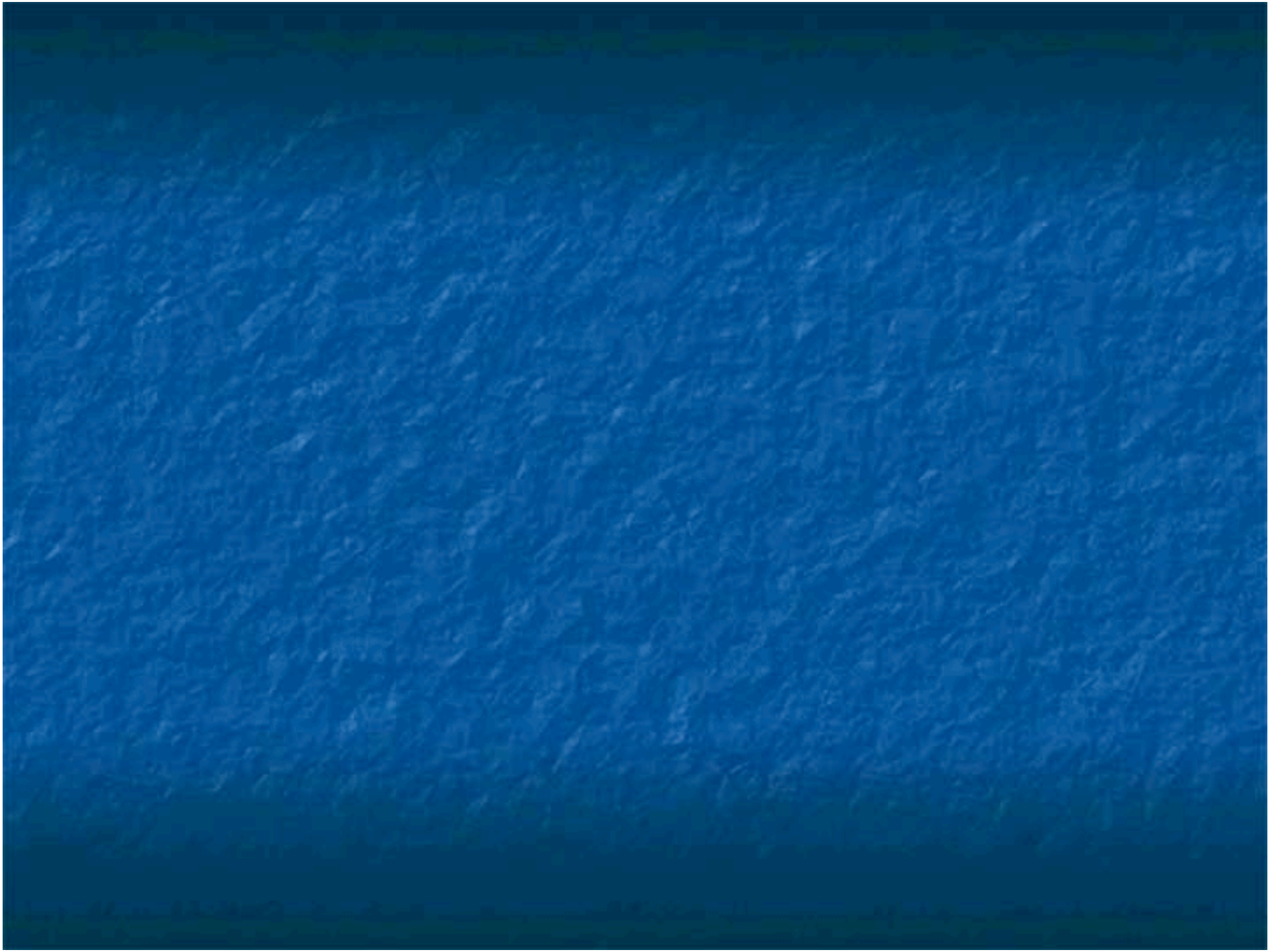
- Discovery battles
- Sufficiency determinations
- Privilege determinations
- Relevance determinations
- Authenticity determinations
- Weight determinations
  - Trial
  - Pretrial
    - Search warrants, EPO, ECO

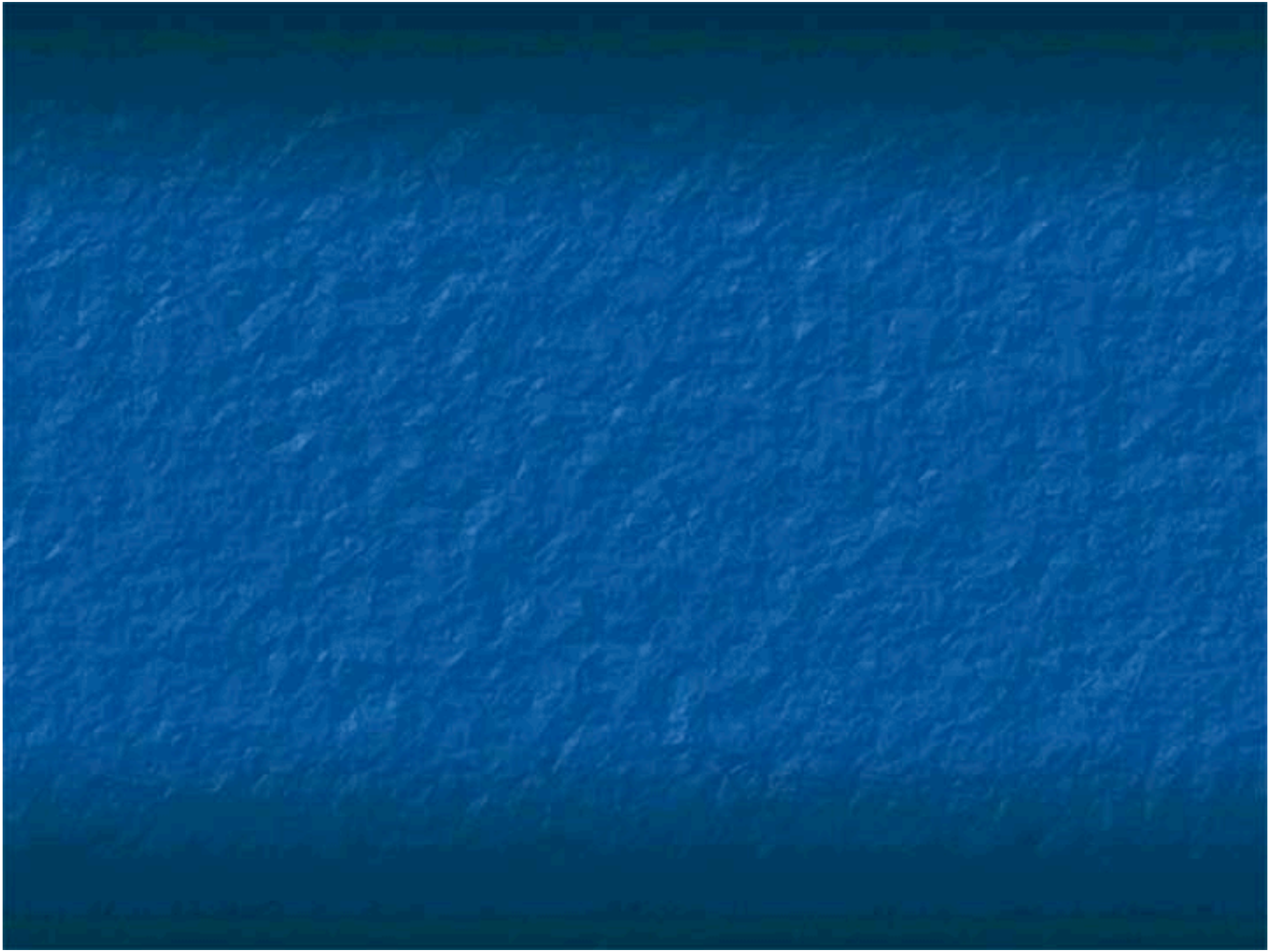
Conclusion

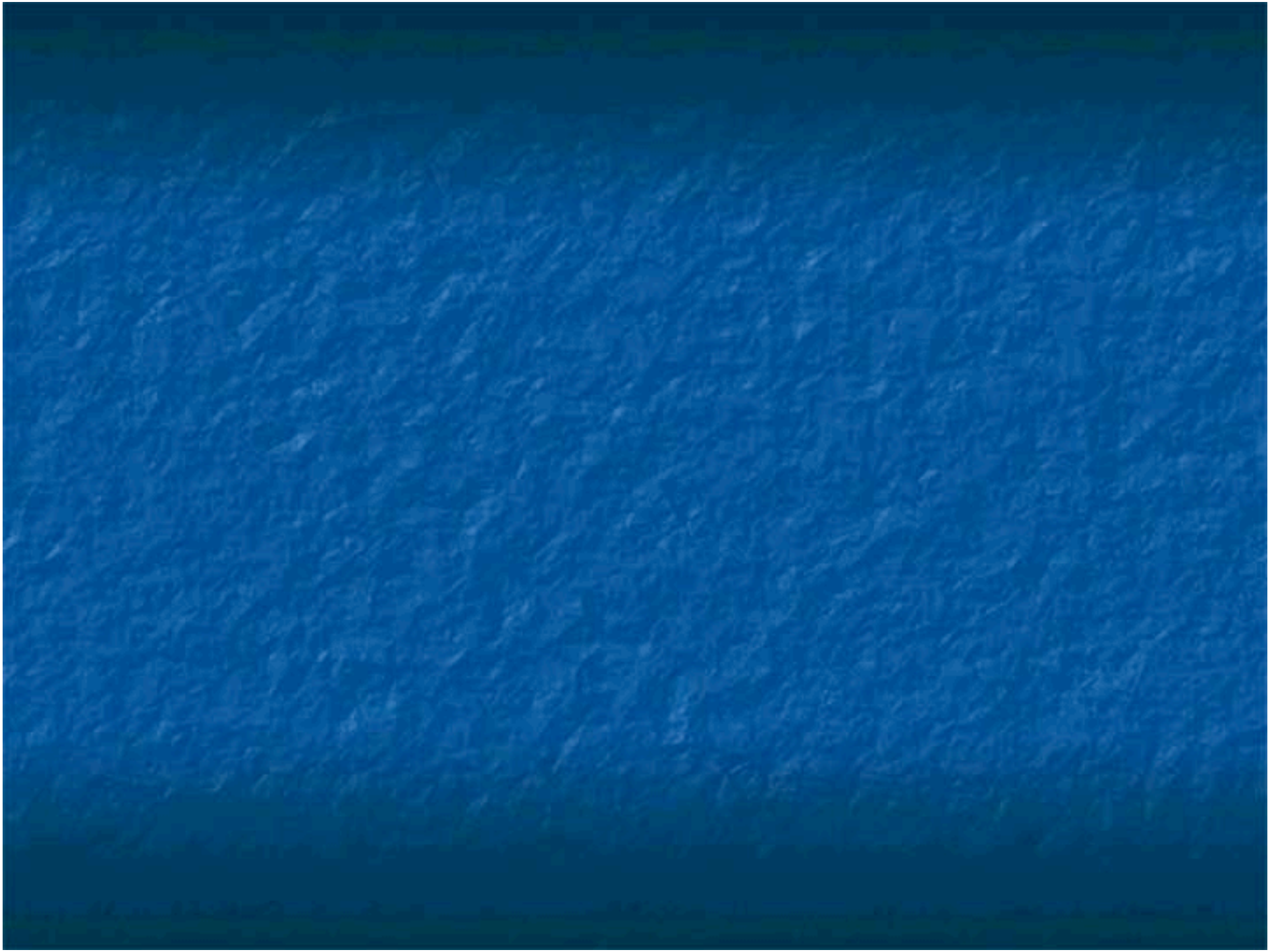
- We’ve still got a long way to go,
- But we’ve got a good start.











Resources

- www.krollontrack.com
- www.dfrws.org