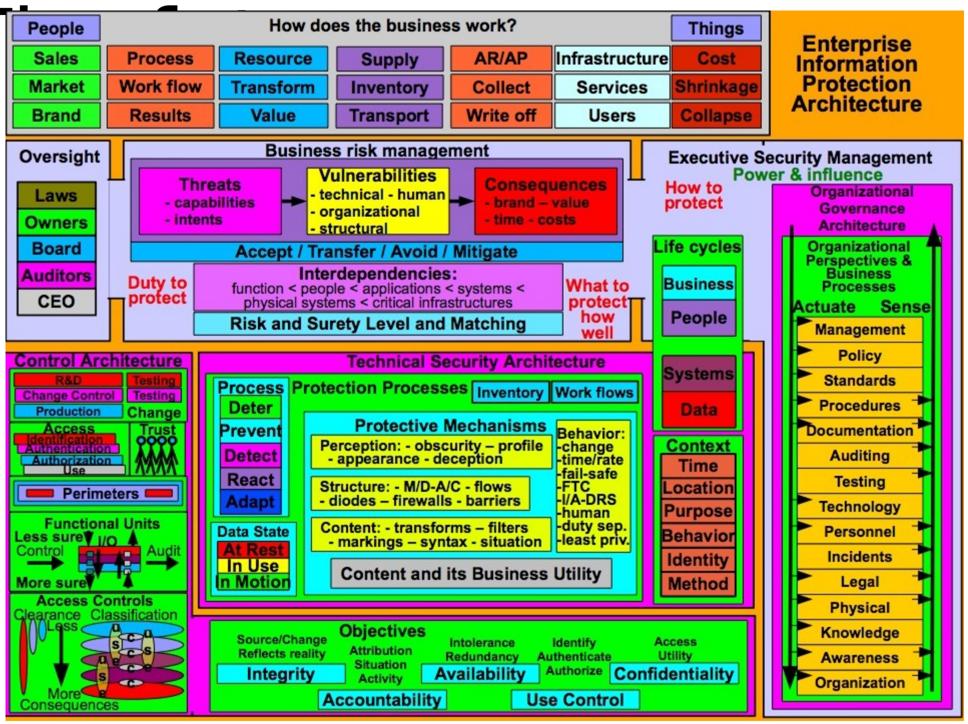
The need for and progress in science for information protection and digital forensics

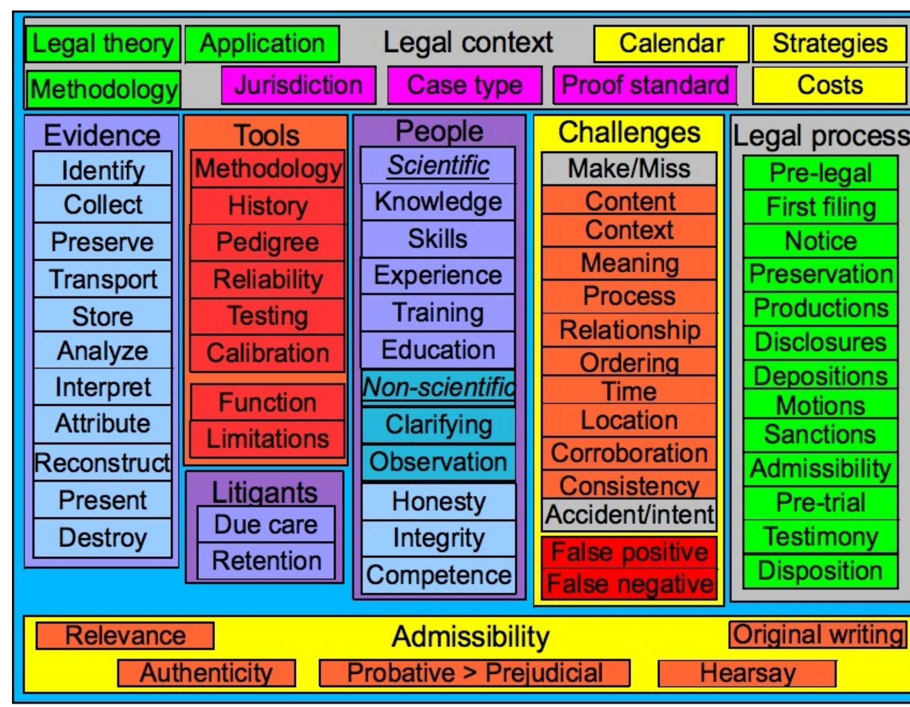
University of Pretoria – April 11, 2011

Dr. Fred Cohen
President - California Sciences Institute
CEO – Fred Cohen & Associates

Outline

- Introduction – the basics and the need
- Science as a social activity
- A different physics – an attempt at a theory
- T





Your speaker

- CEO - Fred Cohen & Associates / President CalSci
  - Enterprise information protection architecture
  - Digital forensics for (usually high-valued) legal cases
  - 501(c)3 research and educational institution
  - M.S. Advanced Investigation / Ph.D. Digital Forensics
- B.S. EE (C-MU '77), M.S. Info Sci (Pitt '81), Ph.D. EE (USC '86)
- >30 years of information protection R&D, design, engineering, testing, implementation, operation, etc.
- >20 years since first digital forensics case
- POST certified instructor in digital forensics, Guest lecturer FLETC, PMTS Sandia National Labs, etc.
- >>100 peer reviewed publications, many conference talks, ...

The basics

- Science is about causality
  - A scientific theory:
    - $C \rightarrow^{M} E$: Cause(C) produces Effect (E) via mechanism M
- The scientific method
  - Identifies the criteria for rejecting (or accepting, for now) a scientific theory
    - Hypothesize $C \rightarrow^{M} E$
    - Perform experiments to refute
    - Failure to refute → confirmation
    - Enough confirmations and hypothesis becomes theory
    - One refutation and theory becomes refuted (wrong)
      - But it may still be useful for limited cases

Example science

- Hypothesis: The World is flat
- Experiment: Keep sailing and see if you come back
  - Lots of them didn't come back... confirmed
  - So many didn't come back → theory
  - One made it around...
- Refutation – the theory was refuted (wrong)
  - But it may still be useful for limited cases
  - Do you account for the curvature of the Earth when you design a building? Or do you assume the Earth is flat?

A problem with science

- Scientists are people too
  - People make mistakes → Science makes mistakes
  - Science corrects big mistakes and does it slowly
    - When someone notices “something wrong”
    - When the wrong thing is important enough to someone
    - Scientists will check it out, refute the old, propose new
    - Old workable science is still useful (F=ma)
  - People lie → science examines refutation carefully
    - Confirmation not so much – because it's not surprising
    - A new result that's important will get checked out
    - Once you lie in science - nobody will likely believe you again – and your old work will be largely discounted

Science (protection & forensics)

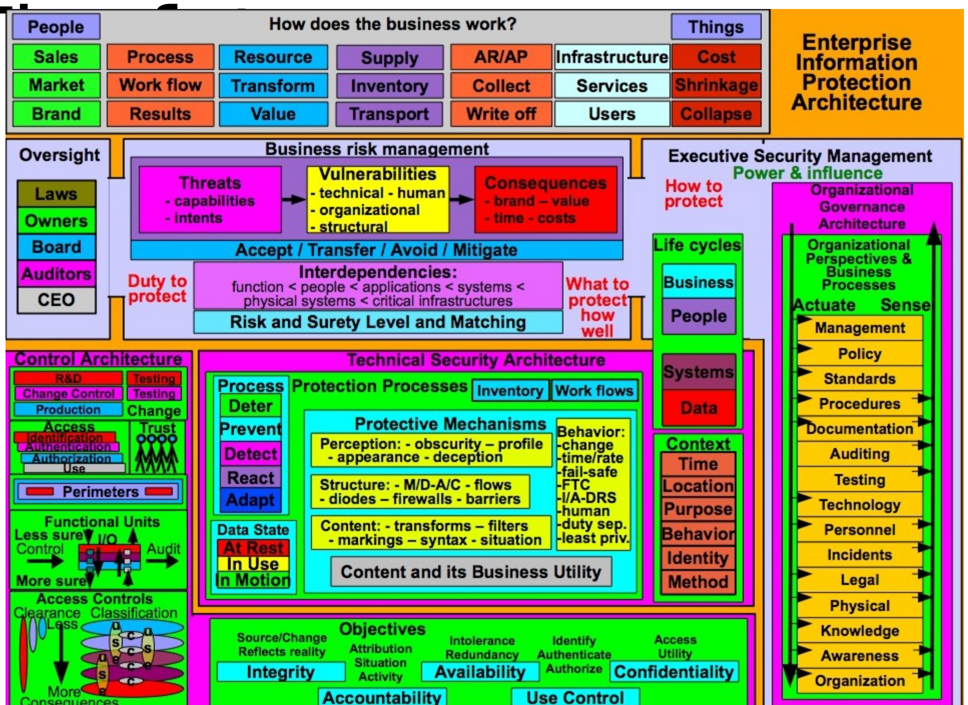
- Is digital forensics important enough to care?
  - It sends people to jail / kills / frees them
  - It forms a framework for the legitimacy of the courts – and civil society
  - The social contract fails if science does not aide justice
- Is information protection important enough?
  - We have created a highly dependent society
  - Advanced society may literally collapse without properly functioning information technology
- I think it's important enough, so I care... do you?

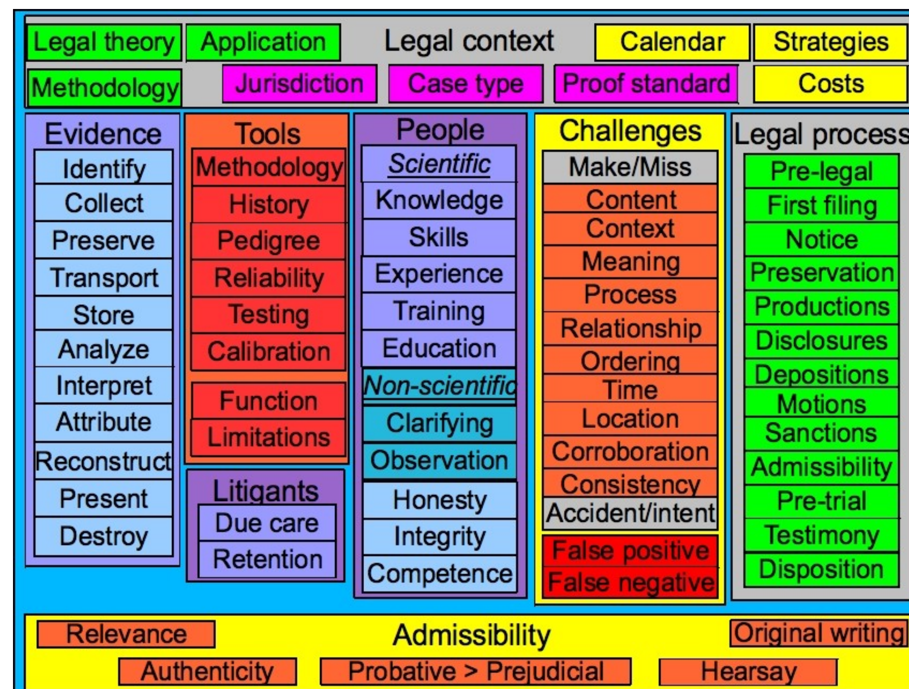
But suppose we don't care?

- Without a reliable C → E model
  - We make a lot of mistakes (which happens anyway)
  - Those mistakes don't get corrected
  - They may be replaced by other mistakes
- How's that working out for you?
  - We pay too much and get too little
  - Snake oil sales prosper in the marketplace
  - We still do ridiculous things we did 25 years ago
    - Change your password how often?
- A scientific approach will help us get to “right”

Outline

- Introduction – the basics and the need
- Science as a social activity
- A different physics – an attempt at a theory
- T





Consensus: Digital Forensics

- The “scientific community” in digital forensics lacks consensus even around the very basic notions
- Compared to the consensus on human activity producing global climate change (86% or more) the basic notions of digital forensics are not at consensus levels:
  - Digital evidence is made of bit sequences.
  - You can observe bits without altering them.
  - You can duplicate bits without removing them.
  - Digital evidence is trace evidence

Challenge!!!

- There are only about 500 peer reviewed articles on digital forensics in the literature
  - Terminology is not widely agreed or uniformly applied – lots “made up”
  - Testability, validation, and scientific principles have not been widely addressed
  - The small corpus of published results limits the scientific basis for statements
  - Claims w/out supporting experiments common.
- “The State of the Science of Digital Evidence Examination” - 2011 IFIP DF conference

Consensus: Info. Protection

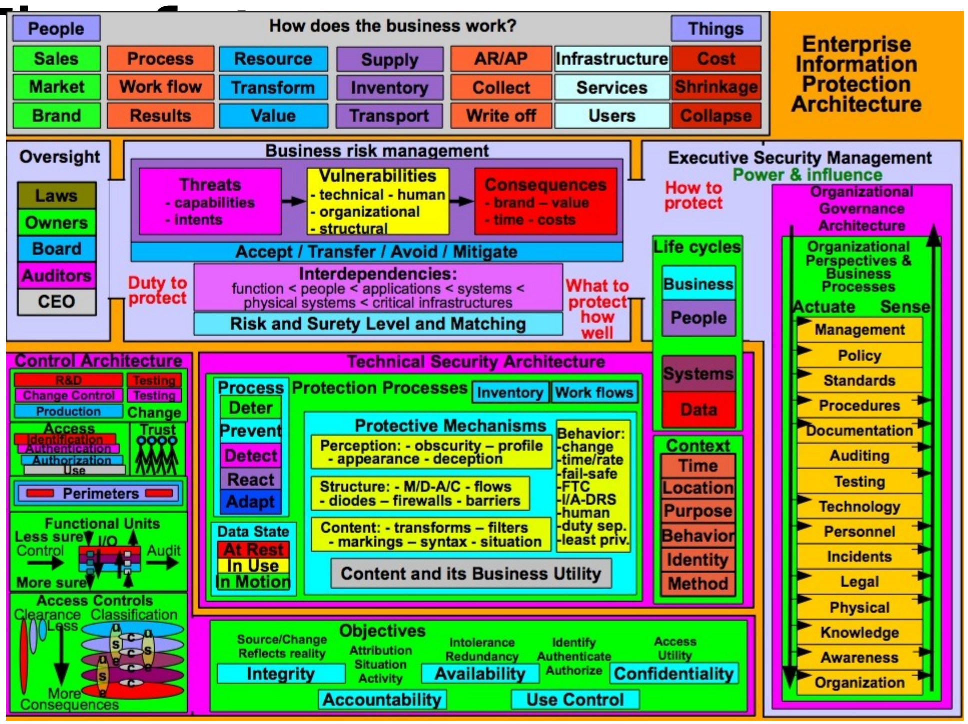
- We have a reasonably consistent set of words
  - Most CISSPs understand most of the words I use
  - There are 10,000+ peer reviewed articles
    - ~5 real journals (outside of cryptography)
    - Many peer reviewed conferences
    - Lots of funding all over the world
  - Testability, validation, and scientific principles have not been widely addressed
  - Claims w/out supporting experiments common
  - Lots of long-term mistakes and rote approaches
- Example: most of my submissions get accepted
  - Many w/out comment (good for me, not for science)

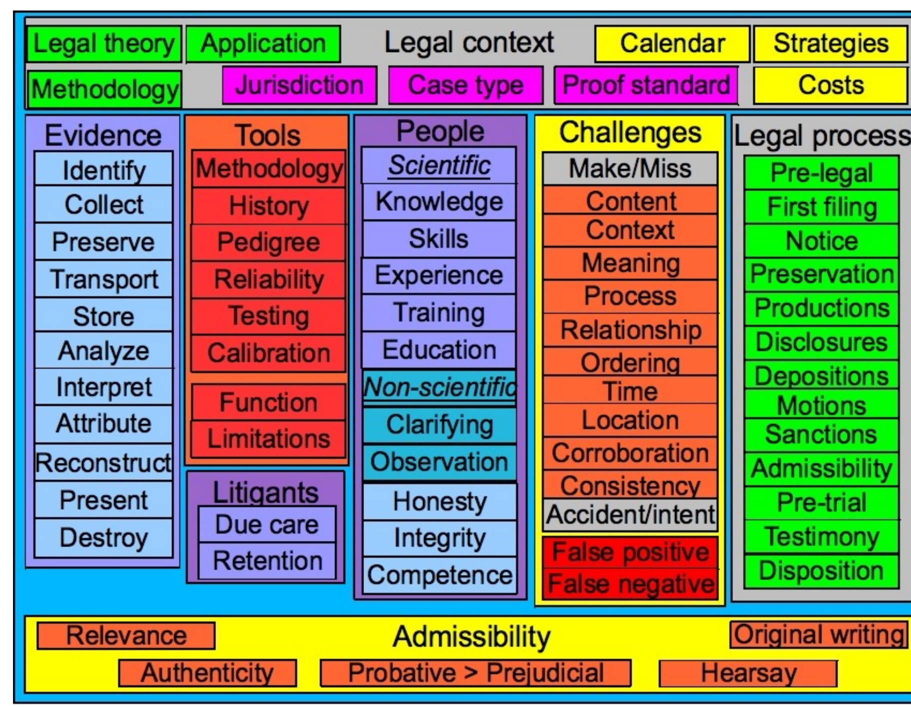
Info Pro Big Problems

- There are almost no scientific experiments
  - No widely used theory of measurement
  - Almost no useful metrics
  - Almost no scientifically valid experiments
  - We don't even have a physics
- A big part of the problem:
  - We have a purely mathematical basis
  - And it ignores the people and processes
- A big part of the solution:
  - Social sciences integrated with artificial sciences

Outline

- Introduction – the basics and the need
- Science as a social activity
- A different physics – an attempt at a theory
- T





Differences in physics

- Some basic physics of the digital world:
  - **Digital data** is entirely **sequences of bits**
  - The atomic unit is the “bit”
  - Nothing smaller (finite granularity)
    - No longer dealing with the digital evidence
    - Smaller than a bit it's physical evidence
  - Finite bit granularity → finite time granularity
    - Bits can only store traces (of time) at finite granularity (a finite bit sequence)
- **Normal space: infinite** granularity space/time
- **Digital space: finite** granularity space/time

Challenge!!!

- Finite granularity → time is a partial ordering
  - A before B (A<B), A after B (A>B), Can't tell (A≈B)
  - Traces as recorded are subject to Δt
    - What is the Δt for your traces / time stamps?
  - Is the claim a sequence of events?
    - Don't know Δt → don't know the sequence!
- Precision vs. accuracy
  - Trace time stamps are subject to delays, etc.
    - They look precise (2010-11-02 03:34:54.455)
    - But often aren't as accurate (off by 9 hours)
  - Mixed granularity misleading as to sequences
    - Some Windows time stamps at 1-day granularity

Differences in physics 2

- Observation without alteration:
  - **Normal space: Not possible** to observe a physical particle without altering it
  - **Digital space: Possible** to observe a bit without altering it - because the media storing bits is highly stable and engineered for this purpose.
- Duplication without removal:
  - **Normal space: No "exact" duplicates.** When we steal something, the original is gone.
  - **Digital space: Exact duplicates:** We can "steal" bits leaving the original intact and unaltered.

Challenge!!!

- Courts have held bit-for-bit copies acceptable as original writing for digital evidence - BUT:
  - A scientific basis is required to demonstrate that the duplication was properly done
- FRE 702: sound methodology properly applied
  - An underlying digital physics
  - Proper use of properly functioning tools
- We don't have a widely accepted and uniformly applied way to do this today
  - Each instance is a possible challenge
  - Each expert better understand it all

Differences in physics 3

- **DFE** is "**trace**" evidence
  - Finite State Machines (FSMs) execute
  - They produce outputs that may get stored
  - Stored outputs are "**traces**" of the event sequences in the FSMs
- **DFE** is **NOT "transfer"** evidence
  - **Normal evidence:** Two objects touch → each leaves part of itself with the other
  - **Digital evidence:** systems in "contact" with each other, do NOT leave parts
  - Systems **may** independently produce (different) traces as a result of "contact"

Challenge!!!

- Most digital forensics folks are unaware of the history of **natural world** forensics
  - **Natural world:** 1900 or so, **"transfer"**
  - **Transfer** is the scientific basis for trace evidence
- There is **no transfer in digital evidence**:
  - The **scientific basis** for evidence acceptance in the natural world **does not apply**
- But there are still **traces**
  - Products of the execution of FSMs
  - The basis for admission and use is different
  - Does your expert understand these principles?

Differences in physics 4

- FSMs have “perfect” forward predictability.
  - Given an FSM, initial state, and input sequence, all state and output sequences are precisely defined
- Thus **digital space “converges” with time**
  - **Normal space** admits to only one past but many possible futures.
  - **Normal space “diverges” with time!**
- **Many FSMs and input** sequences produce **identical output** sequences
  - Traces do not uniquely identify how they came to be!

Challenge!!!

- Suppose an asserted expert says:
  - Based on digital traces alone, a specific event sequence definitely happened
- But digital space converges with time:
  - Traces do not uniquely identify how they came to be!
- This is not a valid expert opinion
  - And it puts the expertise in question
- Be careful... precise wording is important
  - If you don't understand the physics, its easy to screw up

Information physics details

- Digital space converges with time
  - FSM: (I,O,S,m:{IxS}→{O,S'}) IF |I|>(|O|+|S|) THEN ∃(i,i')∈I:∃(o)∈O,∃(s)∈S, i→(o,s) and i'→(o,s)
  - Also note that *h*(O) ≤ *h*(I+S) (Shannon's *h*)
  - **Normal space diverges with time** *(2nd law of thermodynamics)*
  - **Digital space converges with time**
- You can't normally identify I^n from traces T
  - T: |T|<|I^n|, ∃(i,i')∈I^n:∃(t)∈T, i→(t) and i'→(t)
  - In digital space, history is not uniquely determined by the present

Differences in physics 5

- FSMs are syntactic in nature
  - Semantics is driven entirely by context
  - The same sequence of bits can “mean” a lot of different things
  - Different sequences of bits can “mean” the same thing
- This means that “interpretation” is required for any meaningful use of digital evidence
  - There are a very large number of possible interpretations
  - But few of them are consistent, which is key

DFE scientific methodology

- The fundamental theorem of DFE examination:
  - **What is inconsistent is not true**
- DFE examination consists of testing hypotheses to try to refute them.
  - No matter how many tests are performed, except for special cases, ***you can't prove that any real world event is true***.
  - The ***best*** you can do, is show that your ***tests failed to refute*** the ***hypotheses*** at issue.
  - The ***most*** you can say (in proof) is that the ***results*** of the tests you did were ***consistent with*** some set of ***hypotheses***.

Refutation is king

- On the other hand...
  - One refutation disproves a hypothesis.
  - The ***least*** you can say based on refutation is that the ***hypothesis is not true***.
- Thus the methodology consists of:
  - Devise testable hypotheses (A ***consistent*** with B)
  - Test those hypotheses against the evidence
    - A scientific test should seek to refute a hypothesis and not to confirm it (seek ***inconsistency***)
  - Inductive and deductive logic are valuable tools for testing hypotheses
  - As is experimental technique

Differences in physics 6

- DFE is (normally) latent in nature
  - It can't be directly observed with human senses
  - The bits must be observed through tools
- How do we understand and trust the tools?
  - Most tools are computer programs (sequences of bits interpreted by FSMs)
  - How do we assess and present tool reliability?
- Most examiners today don't discuss this
  - But the Supreme court seems to think this is not up to snuff for other sorts of evidence

Challenge!!!

- DFE is latent → depends on tools
  - FRE702:“product of reliable principles & methods”
  - What are the principals and methods of the tools?
  - How reliable are the tools?
  - What are the limits of the tools?
- A scientific methodology to evaluate tools?
  - No methodology → regardless of what the tools tell us, we don't know how to interpret it
- What is the basis for trusting your tools?
  - In most cases, no basis is provided
  - Do you know the principals and methods?

Does your expert do this?

- How reliable?
  - What sort of errors are made by the tools?
  - To do this, we need an error model
    - See “Challenges to Digital Forensic Evidence”
- How do we calibrate and test tools?
  - Calibration → validation with known samples
    - What known samples are right for the matter?
    - What is the “right” answer and how do we tell?
  - Testing involves software verification
    - Mathematical proofs
    - Tests against error models

Even if the tool was “perfect”

- FRE 702: “the witness has applied the principles and methods reliably to the facts of the case”
  - Tools must be properly used w/in their limits
  - Results must be meaningfully interpreted
  - This implies relevant examiner knowledge, skills, experience, training, education
- A theory of measurement is needed:
  - What does the tool measure? How does it do it?
  - Do I need / can I use the same tool to test it?
  - Can I use a tool that doesn't reveal mechanisms producing its outputs?

Differences in physics 7

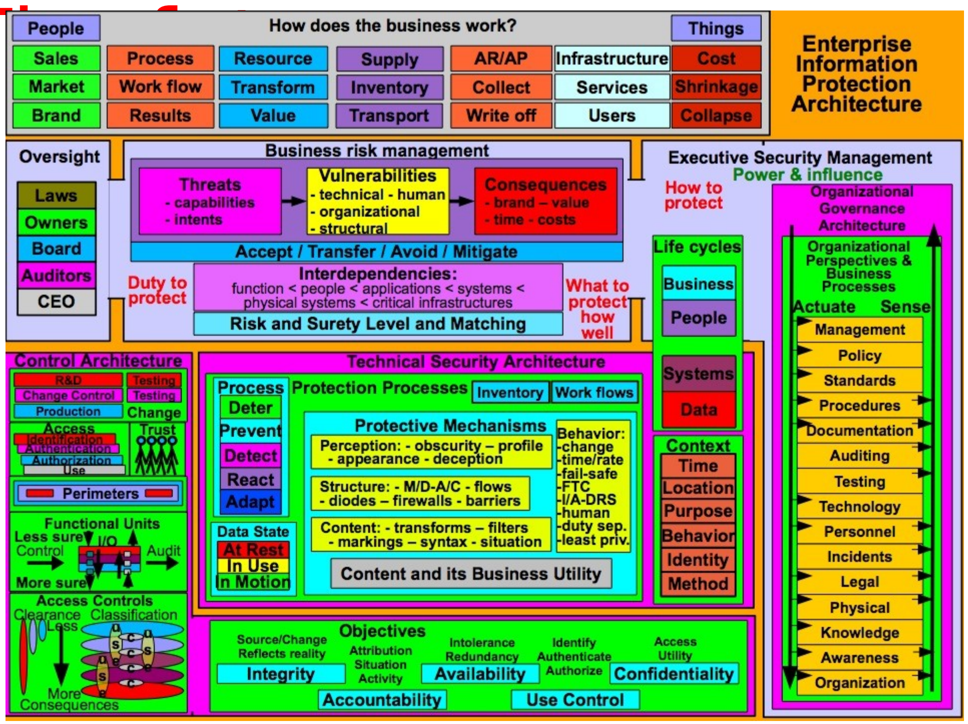
- **Normal space is limited by the speed of light**
  - Speed of light (c) ~186,000 mi/s ($3*10^8$m/s)
  - Matter can't be accelerated past c
  - Light and signals travel no faster than c
- **Digital space is also limited by c!!!**
  - Digital systems exist in the physical world
  - So these physical constraints apply to them
- **Digital space** and computational complexity
  - Computational complexity limits what operations can be performed with what computing capacity in what time frame: another "c" for digital space

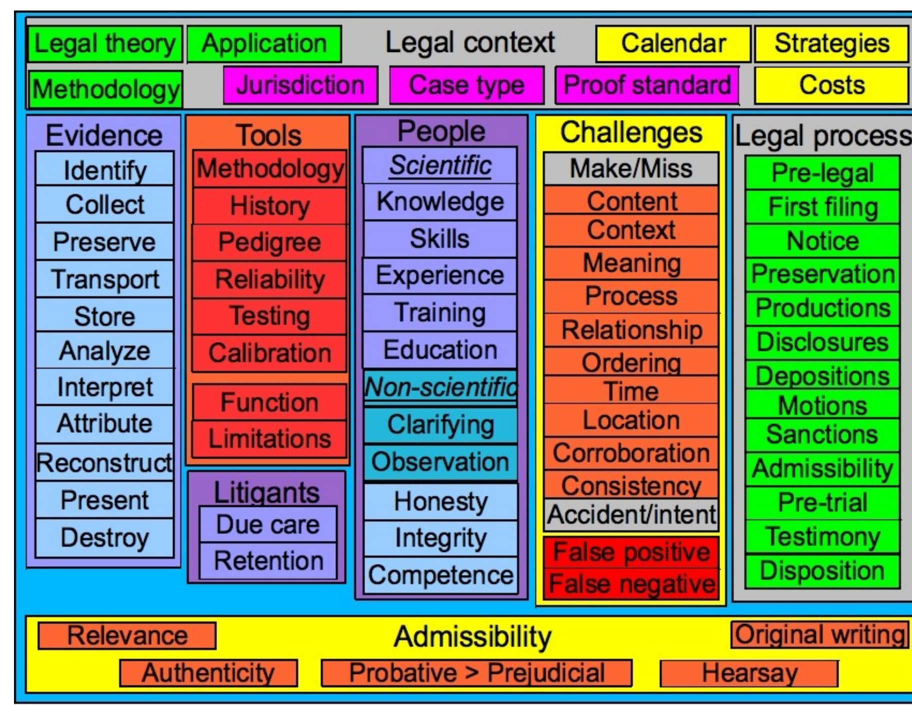
Differences in physics ...

- There are many more examples of differences between the physics of digital information and the physics of the natural world.
- For details see:
  - F. Cohen, "Digital Forensic Evidence Examination - 3rd ed.", ASP Press, 2011

Outline

- Introduction – the basics and the need
- Science as a social activity
- A different physics – an attempt at a theory
- T





Where from here?

- The social part of science...
  - Here I am – trying to convince you
    - If I do, you will try to convince others
  - In the marketplace of ideas, mindshare wins
    - For a while... until failures force abandonment
    - Refutation is king
  - The “meme”s that survive are more “fit”
    - In the environmental niches they live in
  - Evolution is not optimization
    - But refutation pushes us out of our gravity wells
- I would love to discuss your research...

Thank You

http://calsci.org/ - calsci at calsci.org

http://all.net/ - fc at all.net