What is "evidence"?

- Information stored or transmitted in binary form that may be relied on in court
- data and info about the data (files, meta-data, non-filesystem data, anything at all!)
- Will be used by investigator to:
  - Gather info about individuals (WHO)
  - Determine events that transpired (WHAT)
  - Construct a timeline (WHEN)
  - Discover tools / exploits used (HOW)