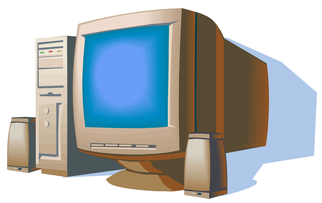
DICo

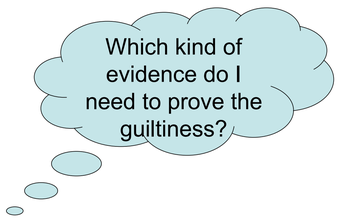
Computer Aided Forensics

University of Milan

Problem : 1

Law enforcement people have to deal with a huge amount of criminal conduits and apparently unrelated evidence data



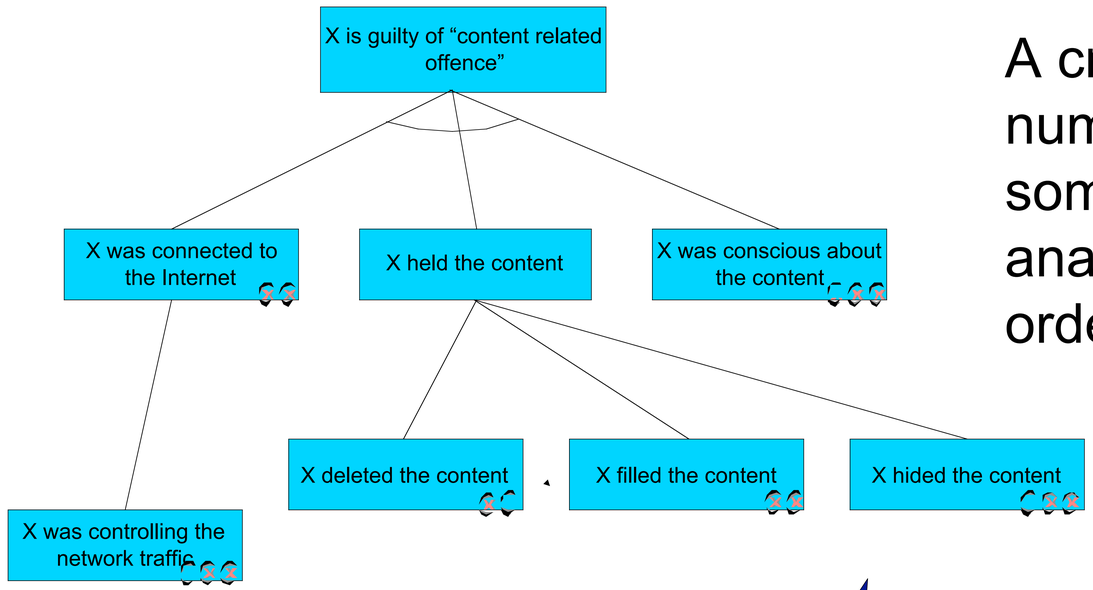


Goals: 2

- Produce reusable knowledge about investigations
- Organize evidence support
- Support less skilled detectives during evidence collection

Approach: 3

The prosecution aims at proving the accusatory "theorem" on the basis of evidence collected



A criminal offence implies a number of conditions (that sometimes can be furtherly analyzed) to be verified in order to establish guiltiness

Evidence support provided by performed tests can evaluated to asses global soundness and completeness of the inquiry

Investigation methodology gets recorded 4

For each condition the experience suggests typical tests

X was controlling network traffic:
- Check if IP spoofing was possible
- Check if spoofing was possible at application level (proxy)
- Check if trojans were present on the device

References

Wigmore, J. H. *Wigmore on Evidence*, 1983 Tillers rev. Little, Brown, Boston.
Schum, D. A. *Evidential Foundations of Probabilistic Reasoning*, 1992, Northwestern University Press
Leveson, N. *Safeware: System Safety and Computers* Addison Wesley

Contacts

Danilo Bruschi bruschi@dico.unimi.it
Mattia Monga monga@dico.unimi.it
Igor Nai Fovino nai@dico.unimi.it
http://cert-it.dico.unimi.it