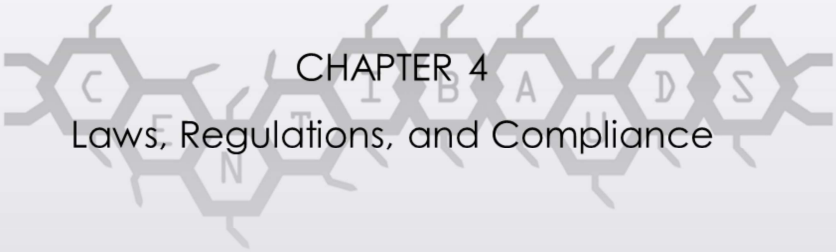
# CISSP

Aitizaz Uddin Syed (M.Engg, CISSP, CISSP-ISSAP, CCSP, CRISC, GICSP, TOGAF)


# Domain 1
# Security and Risk Management




# CHAPTER 4

## Laws, Regulations, and Compliance

# Laws in the world

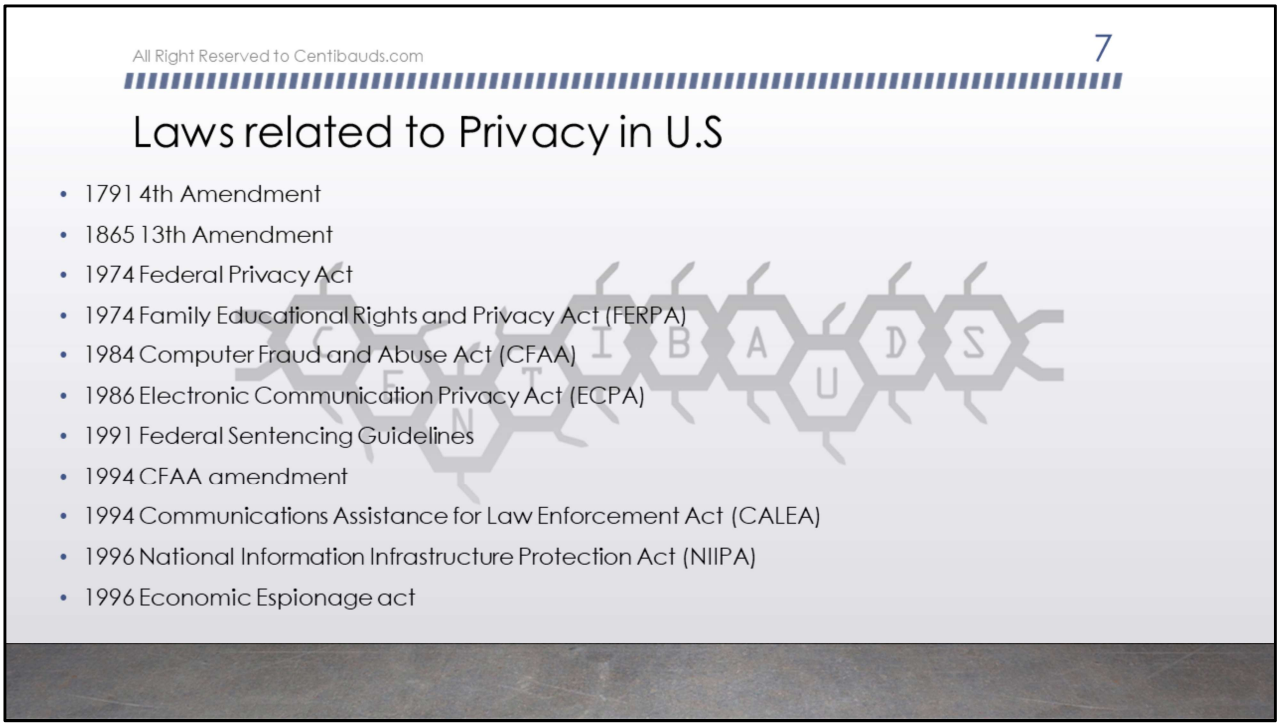
- Civil Code Law
  - Followed in most European countries
  - Since Justintin
  - Written and codified
  - Court independent strictly follow written code
- Common Law System
  - Initiated from England
  - Judges use to travel and make decision
  - Those decision used as a reference
  - Reflects people sentiments, situation, and what's best for Law and Order
  - Raises systems of Barristers, Magistrates, and a whole system that is mutable
- Religious and Custom Laws

# Laws related to privacy and Cyber Security

- Common Law
  - Criminal Law
  - Civil Law
  - Administrative Law
- Criminal Law
  - Deals with crimes
  - Maintain Law and Order
  - Penalties in the form of Monetary fines, Mandatory service, and/or Deprivation of liberties in prison
  - LEAs involved

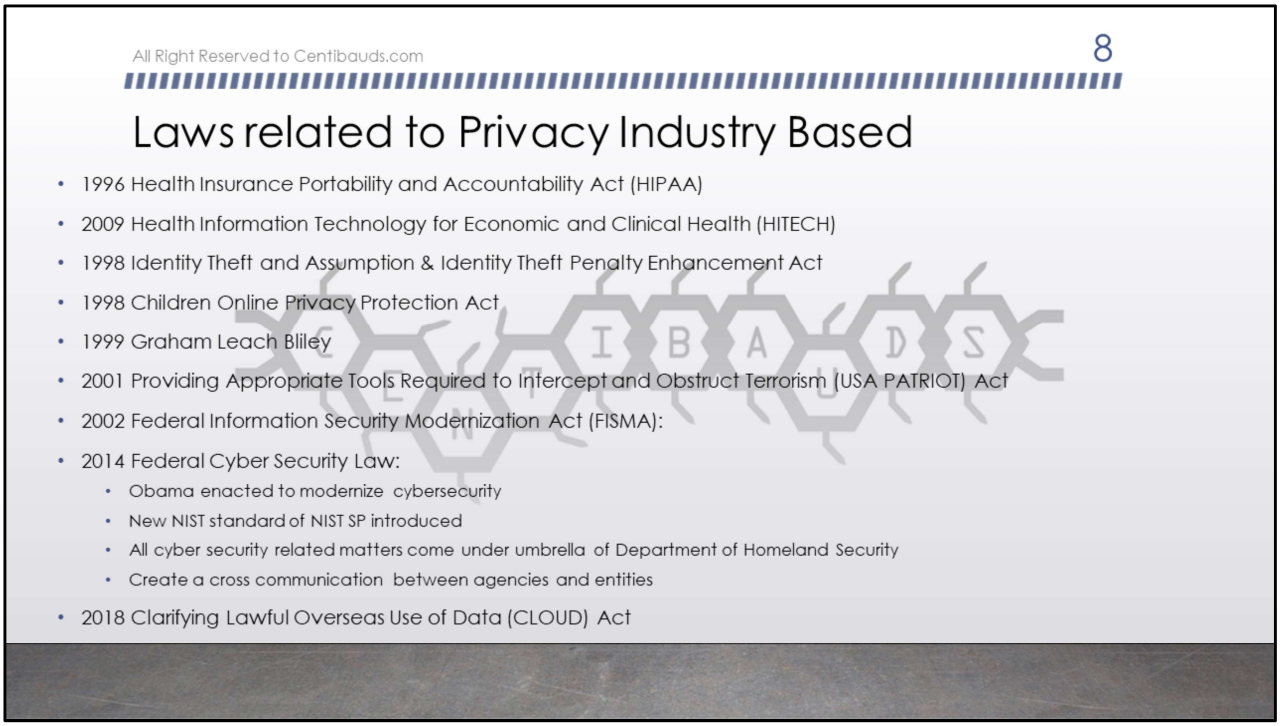
# Laws related to Privacy and Cyber Security (contd..)

- Civil Law
  - No crime involved but fulfilment of obligations and agreed terms
  - Contractual disputes resolution
- Administrative Law
  - Applies to government employees, agencies, LEAs and departments
  - Act in a proper order, policies, rules, regulations and Code of federal regulations




-1791 4th Amendment: No one is allowed to trespass property and privacy unless there is a warrant.
-1865 13th Amendment: Every one is free and abolishment of slavery.
-1974 Federal Privacy Act: Only collect information if required for investigation, Discard if the concerned individual innocent and no information needed.
-1974 Family Educational Rights and Privacy Act (FERPA): Institutes are entitled to secure records correctly (maintain integrity) and not disclose unless approved.
-1984 Computer Fraud and Abuse Act (CFAA): Inflicting damage to federal government or financial institute computers is crime & monetary punishment applies.
-1986 Electronic Communication Privacy Act (ECPA) : Prevent unauthorized disclosure of any electronic communication.
-1991 Federal Sentencing Guidelines: Prudent man rule; Chain of custody; Contracts and terms assertion.
-1994 CFAA amendment: Creation of malicious code (even unintentional) is a crime; broaden scope of concerned compute systems includes the interstate communication systems.
-1994 Communications Assistance for Law Enforcement Act (CALEA): Get an approval from judge and perform monitoring of electronic link and surveillance.
-1996 National Information Infrastructure Protection Act (NIIPA): CFAA extended to all

assets of the states let it be commerce, railway, power grids, sewerage,  etc. Any damage to these entities is a felony and there are strict penalties.
-1996 Economic Espionage act: Stealing Intellectual Property and secrets of any U.S based organization is a felony.




-1996 Health Insurance Portability and Accountability Act (HIPAA): Allow PHI to be transferred between registered entities. Ensure protection of PHI by applying strict measures.
-2009 Health Information Technology for Economic and Clinical Health (HITECH): enhances HIPAA by introducing a written contract called Business Associate Agreement (BAA) and establishes that any PHI breach should be notified in due time.
-1998 Identity Theft and Assumption & Identity Theft Penalty Enhancement Act: Identity theft a crime with stinging penalties.
-1998 Children Online Privacy Protection Act: Protection of child information and take parents consent if younger then 13 to take record.
-1999 Graham Leach Bliley: Allow banks, insurance organizations, credit providers and financial institutions to share

details of individuals but retain privacy.
-2001 Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act: Allows LEA to sniff /collect information of suspicious individuals without consent.
-2002 Federal Information Security Modernization Act (FISMA): Obligatory to implement Information security program according to NIST for all the government entities and agencies along with the contractors who intend to participate and work with government.
-2014 Federal Cyber Security Law:

- Obama enacted to modernize cybersecurity
- New NIST standard of NIST SP introduced
- All cyber security related matters come under umbrella of Department of Homeland Security
- Create a cross communication between agencies and entities

-2018 Clarifying Lawful Overseas Use of Data (CLOUD) Act: All digital organizations under jurisdiction OR under agreement with U.S government are entitled to provide data footprint for criminal investigation processing. Even if data us outside the U.S.

# EU General Data Privacy Right (GDPR)

- Introduced in 2016 is the most comprehensive law on PII
- Notify victims and authorities in specified time or face the penalty
- It covers aspects of :
  - Lawfulness, Fairness, Transparency
  - Purpose Limitation
  - Data Minimization
  - Accuracy
  - Storage Limitation
  - Integrity and Confidentiality
  - Accountability

# EU Data Privacy Right (GDPR) (contd..)

- Cross border data transfers
- Data of PII cant go outside EU unless their is
  - Standard Contractual Clauses
  - Binding Corporate Rules approved by every EU member nation
- Safe Harbour and Privacy Shield allow movement of EU data into US by digital companies
  - Safe Harbour is pre-GDPR
  - Privacy Shield is post-GDPR

# Other nations privacy laws

- Personal Information Protection and Electronic Documents Act (PIPEDA): Privacy Law in Canada briefly identifies the information that applies as PII
- Personal Information Protection Law (PIPL): Privacy Law in China replicate GDPR
- Protection of Personal Information Act (POPIA): Privacy Law in South Africa replicates GDPR
- State Privacy Laws: In U.S different states have their own privacy laws and organizations if intend to operate there should comply to those beside federal laws
- E.g California Consumer Privacy Act (CCPA) replicates GDPR

# Contracting, procurement and Compliance

- Compliance
  - Organizations are suppose to comply to all laws, rules and regulations
  - Compliance is documented and audited evidence that you fulfill the aforementioned requirements
- Compliance VS Conformance
- Contractors and procured products should also fulfil rules, laws, and regulations
- Contractor should also exercise the same level of protection to PII
- Cross border data transfer after anonymization, pseudonymization, and tokenization

# Intellectual Property (IP)

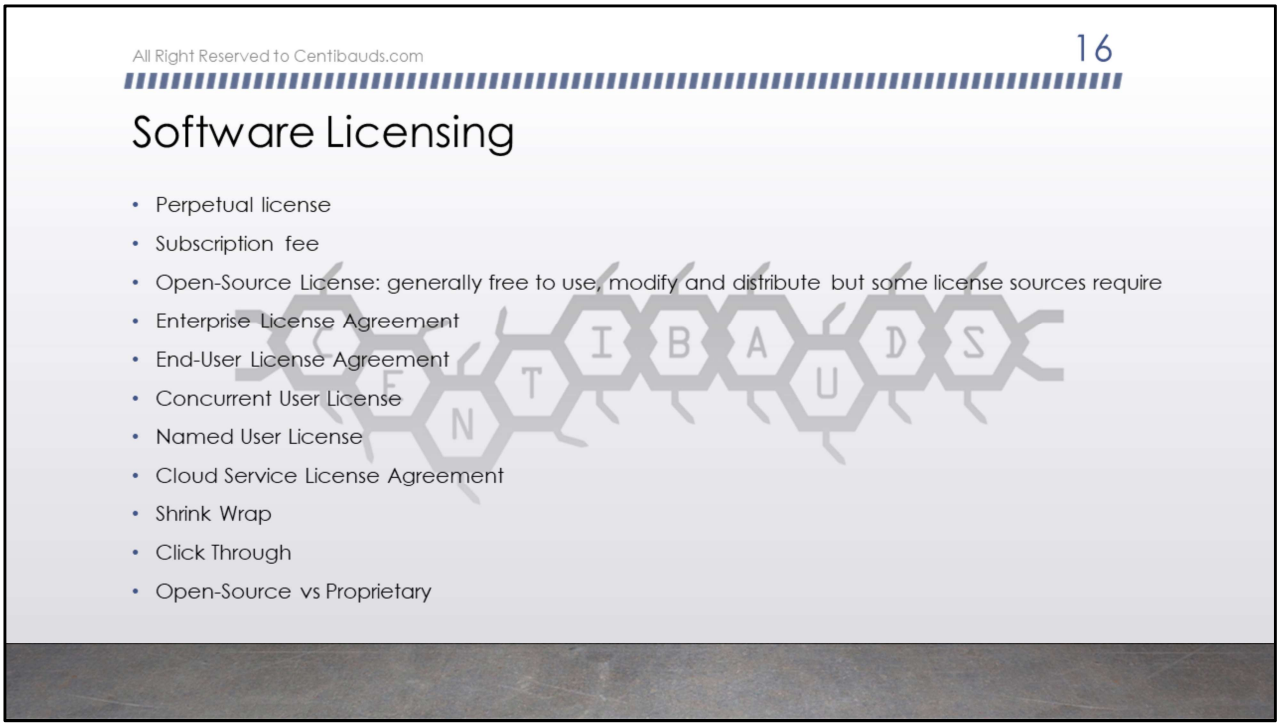
- Intangible assets as a result of creation by individuals giving them ownership and right.
- Various laws are in place and types of IP are Patent, Copyright, Trademark, Trade Secret
- Copyright
  - Literary and artistic work
  - Only source code can be regarded in this actual logic is not copyright
  - Indicated by this sign ©
  - Provide exclusive right of 70 years after the last author dies OR 95 years from the first published date OR 120 years from creation date

# Digital Millennium copyright and Trademark

- Digital Millennium Copyright
  - Grant exclusive rights to digital content with penalties introduced to violators
  - Addressed ISP and communication carrier dilemma
  - Software license based record of the end machine
  - Digital Rights Management now integrate to DLP solutions to give specific time based rights
- Trademarks
  - Words, Logo, Slogan
  - Initial assigned logo ™ upgrades to ®
  - Register with USPTO with renewable in 10 years

# Patent and Trade Secret

- Patent
  - New idea or concept
  - 20 years exclusive rights from the filing of application
- Trade Secret
  - Not disclosed by organization unlike patent or copyright. They keep liberty to maintain its security itself
  - Trade secret lifetime unlike patent and copyright
  - Put controls yourself and use NDA




-Perpetual license: 1 time fee
-Subscription fee: recurring fee in fix duration
-Open-Source License: These softwares are generally free to use, modify and distribute but some license sources require General Public License (GPL) or the MIT license
-Enterprise License Agreement: Agreement between software entity and enterprise organization to use organization-wide in agreed terms
-End-User License Agreement: Agreement between software entity and end-user to use
-Concurrent User License: License quantity dictated by consecutive users
-Named User License: under user account and/or name
-Cloud Service License Agreement: Agreement between cloud service provider and end-user to use its service in agreed terms

Shrink Wrap: Written on package. By opening, you comply to terms
Click Through: At installation you agree to terms
Cloud/Online Services: You are redirected to different page to acknowledge terms and conditions

# Software Licensing (contd..)

- Import/Export Laws
  - During Cold war era, exporting encryption technology was not permitted in U.S. Now such rules are relaxed even for high performance compute except few countries
- Two major entities control export/import
  - International Traffic in Arms Regulations (ITAR): Majorly cover defence and military products
  - Export Administration Regulations (EAR): By Department of Commerce and it maintains Commerce Control List (CCL) not allowed to export. Information Security products normally resides here

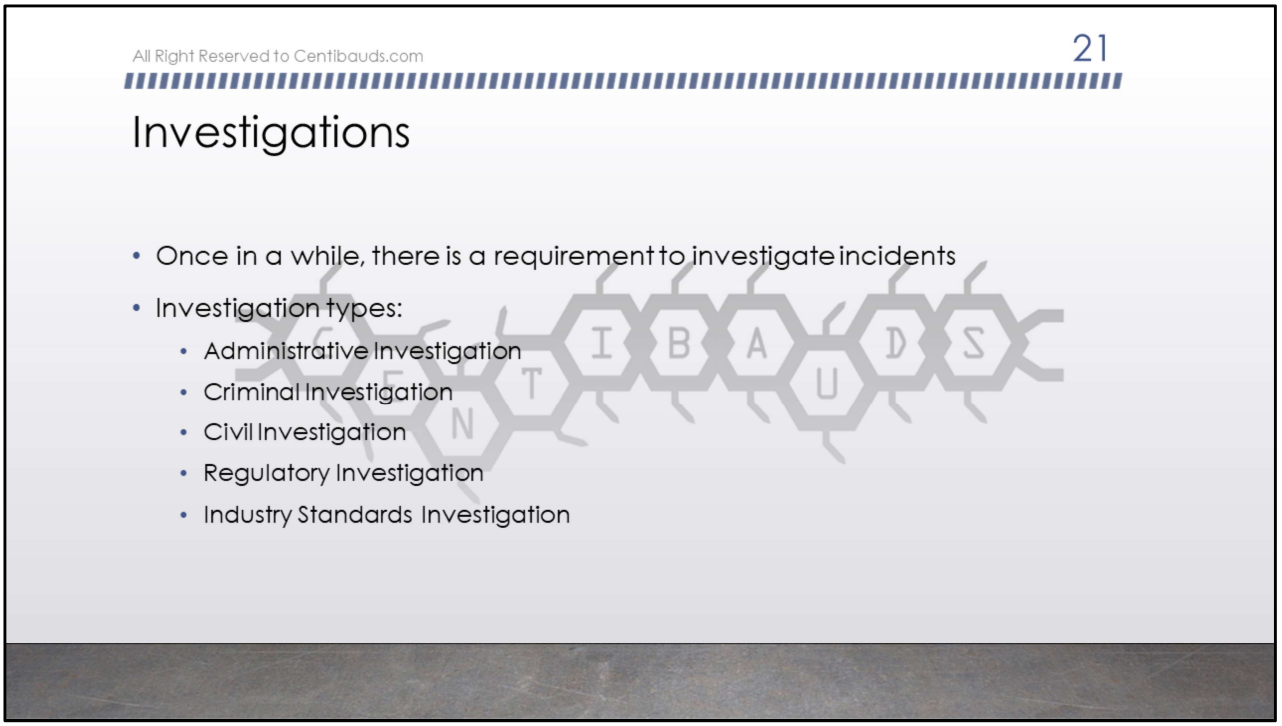
# Some governance terms

- Threat Analysis/Assessment
- Security Control Assessment
- Gap assessment: Evaluate the organization's maturity in security controls
- BIA: Calculate RTO, RPO, MTD
- Risk Analysis/Assessment: Identify various risks, calculate ALE, SLE,
- Audit: Conformance to a standard or framework to achieve certification status


# Domain 7
# Security Operations


# CHAPTER 19

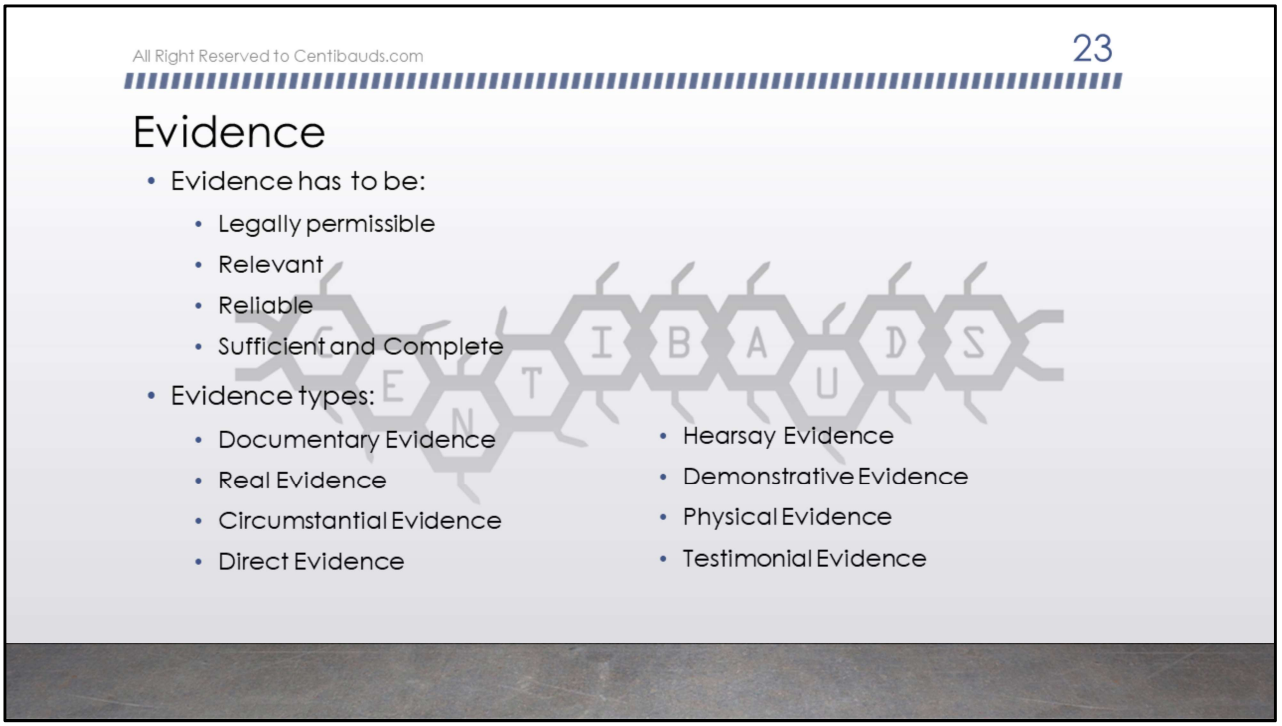
## Investigations and Ethics




-Administrative Investigations: Normal investigation in organizations, Operational investigations looking for RCA is an example
-Criminal Investigations: Performed by LEAs to make someone accountable against criminal law. Requires evidence beyond reasonable doubt standard, Strict rule of forensics and evidence management
-Civil Investigations: Performed between various parties to address disputes, Evidence requirements not that stringent even share the documents with each other. It has preponderance of the Evidence that burden the other party in suspicion and liable in percentages
Regulatory investigation: Performed by government entities and agencies based on administrative law
-Industry Standards investigations: Performed  against the standard of the organization policies

# Electronic Discovery

- In legal proceedings, evidences has to be treated, protected and presented using Electronic Discovery Reference Method (EDRM)
- EDRM has nine aspects:
  - Information Governance
  - Identification
  - Preservation
  - Collection
  - Processing
  - Review
  - Analysis
  - Production
  - Presentation




-Documentary Evidence is written unavoidable proof
-Real Evidence is something physical revealed
-Circumstantial Evidence refers to proofing situation and circumstances that establishes unavoidable proof
-Direct Evidence is clearly identifiable undeniable evidence
-Hearsay Evidence is based on what you have been told of
-Demonstrative Evidence involves showing a physical process or experiment as a proof
-Physical Evidence is a physical item available as a proof
-Testimonial Evidences are bringing people who testify the incident to the court

# Chain of Custody

- From the beginning to the end, create a precise and complete record of actions and tasks conducted with the data
- Make sure integrity, confidentiality is intact else it becomes inadmissible
- Label every component, document every occurrence, sign-off every copy

# Forensics

- The art/science of authenticating and analysing content for digital criminal investigation
- Follow procedures of Scientific Work Group on Digital Evidence (SWGDE)
  - When dealing with evidence follow procedures and processes always
  - Never change evidence maintain its integrity
  - Skilled and trained resource should deal with evidence
  - All activities related to evidence should be recorded and documented
  - Evidence possession person/organization is ultimately responsible

## Attacker and Investigation

- Similar to other crimes, computer crimes also have MOM (Motive-> Opportunity-> Means)
- Hacker has MO (ModusOperandi) i.e pattern of attack that specifies approach to inflict damage
- This eventually leads investigator to incident details
- Types of Analysis and Assessment by investigator
  - Network Analysis: Check logs, path tracing, correlation of logs
  - Media Analysis: Disk Space, Registry, Timeline analysis, Shadow volume
  - Software Analysis: Reverse Engineering, Malicious code, Exploits
  - Hardware/Embedded Analysis: Appliance attack points, Firmware, Memory, OS, Hypervisor, etc.

-Take a traffic dump as a part of investigation via SPAN port
-Media Analysis involves recovering all data even the formatted one; Take disk out and install in write-blocker, take its hash for the record, and take a bit wise copy for forensics
-Get a memory dump file take its hash and then observe its content

# Forensics Investigation

- Forensics process:
  - Identify->Preserve> Collect- > Examine -> Analysis-> Present -> Decision
- Tools used in Forensics are:
  Tool Kit (FTK)  EnCase Forensic  Dd Utility xx

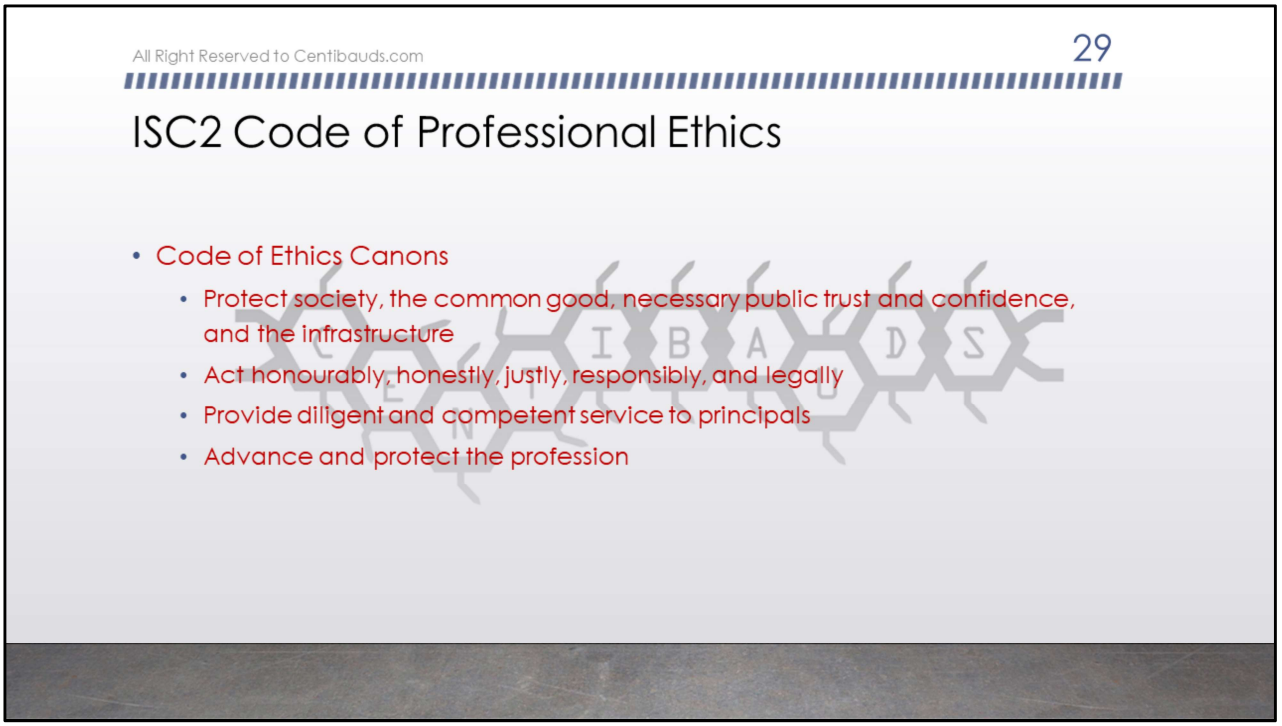
Some tips for digital forensics:

- Precision expertise should be adhered in extracting bit by bit data
- Take backup of a ON system
- Keep original data intact only work on copy
- Every copy should be tamper proof
- Exercise chain of custody

## Forensics Investigation Process and Stages

- Gathering Evidence:
  - Voluntarily Surrender
  - Subpoena enforces person to surrender evidence (documented order from court)
  - Seized by LEA on the basis of Plain View Doctrine
  - Search Warrant
  - Exigent circumstances action
  - Calling LEA is a concern as:
    - Organization looses authority in its execution and has no visibility
    - The news might become public causing its defamation

-Plain View Doctrine means the evidence that probably leads to criminality confirmation is visible
-In all cases make sure privacy is not affected
-Exigent circumstances action means Seize and search without warrant if destroying evidence is possibility




-Loyal to society
-Loyal to your conscience
-Loyal to your employer
-Loyal to your profession (Cyber security career path)

# Ethics and the Internet

- In 1989, the Internet Architecture Board (IAB) defined following ethics for the internet users:
  - Seeks to gain unauthorized access to the resources of the Internet
  - Disrupts the intended use of the Internet
  - Wastes resources (people, capacity, computer) through such actions
  - Destroys the integrity of computer-based information
  - Compromises the privacy of users