Categories of Cloud Forensic Challenges

• **Architecture (e.g., diversity, complexity, provenance, multi-tenancy, deleted data recovery, data segregation, etc.)**
  
  Architecture challenges in cloud forensics include issues such as variability in cloud architectures between providers; accessing the data of one tenant without breaching the confidentiality of other tenants; multiplicity of systems and locations that can store data; accurate and secure provenance for securing chain of custody; seizure of cloud resources without disrupting other tenants; collecting data which are volatile and constantly changing; abstraction of cloud resources available to consumers; data integrity in a multi-tenant environment where data are shared among multiple computers in multiple locations and under control of multiple parties; inability to image all the evidence in the cloud; etc.

• **Data collection (e.g., data integrity, data recovery, data location, imaging, etc.)**
  
  Data collection challenges in cloud forensics include issues such as locating evidence in a large, distributed and quickly changing system; collecting data which are volatile and constantly changing; data collection from virtual machines; data integrity in a multi-tenant environment where data are shared among multiple computers in multiple locations and under control of multiple parties; inability to image all the evidence in the cloud; accessing the data of one tenant without breaching the confidentiality of other tenants; recovery of deleted data in a shared and distributed virtual environment; etc.

• **Legal (e.g., jurisdictions, laws, service level agreements, contracts, subpoenas, international cooperation, privacy, ethics, etc.)**
  
  Legal challenges in cloud forensics include issues such as identifying and addressing issues of jurisdictions for legal access to data; limited investigative powers; channels for international communication and cooperation during an investigation; data acquisition that relies on the cooperation of cloud providers, as well as their competence and trustworthiness; missing terms in contracts and service level agreements; issuing subpoenas without knowledge of the physical location of data; seizure and confiscation of cloud resources may interrupt business continuity of other tenants; etc.

• **Standards (e.g., terminology, testing, validation, SOPs, no single process, etc.)**
  
  Standards challenges in cloud forensics include issues such as lack of common terminology; lack of standard operating procedures, practices, and tools; no one accepted standard for digital or cloud forensics processes; lack of interoperability among cloud providers; lack of test and validation procedures; etc.

• **Analysis (e.g., correlation, reconstruction, time synchronization, logs, metadata, timelines, etc.)**
  
  Analysis challenges in cloud forensics include issues such as correlation of evidence across and within cloud providers; separating real from false evidence; reconstruction of virtual images or
storage; synchronization of timestamps; lack of unification in log formats; authenticity and accuracy of metadata; timeline analysis of log data; etc.

- **Anti-forensics (e.g., obfuscation, data hiding, malware, etc.)**
  Anti-forensics are a set of techniques used as countermeasures to forensic analysis. Challenges in cloud forensics include issues such as the use of obfuscation, malware, data hiding, or other techniques to compromise the integrity of evidence; malware may circumvent virtual machine isolation methods; etc.

- **Incident first responders (e.g., trustworthiness of cloud providers, response time, reconstruction, etc.)**
  Incident first responder challenges in cloud forensics include issues such as confidence, competence, and trustworthiness of the cloud providers to act as first-responders; challenges in response time due to location uncertainty; difficulty of determining how to reduce the overall data set for selective data acquisition; reconstruction of virtual images or storage; etc.

- **Role management (e.g., data owners, identity management, users, access control, etc.)**
  Role management challenges in cloud forensics include issues such as uniquely identifying the owner of an account; decoupling between cloud user credentials and physical users; ease of creating fictitious identities online; determining which users own certain data; authentication and access control; ability of criminals to operate as multiple cells without knowing their identities; etc.

- **Training (e.g., legal, forensic investigators, instructors, cloud providers, qualification, certification, etc.)**
  Training challenges in cloud forensics include issues such as use of digital forensic training materials that are not applicable to cloud forensics; lack of cloud forensic training and expertise for both investigators and instructors; lack of familiarity with virtualization by investigators and evidence collectors; limited knowledge by record-keeping personnel in cloud providers about evidence; etc.