ASU
Arizona State University

CSE 469: Computer and Network Forensics

Topic 8: Cloud and Web Forensics

Dr. Mike Mabey | Spring 2019

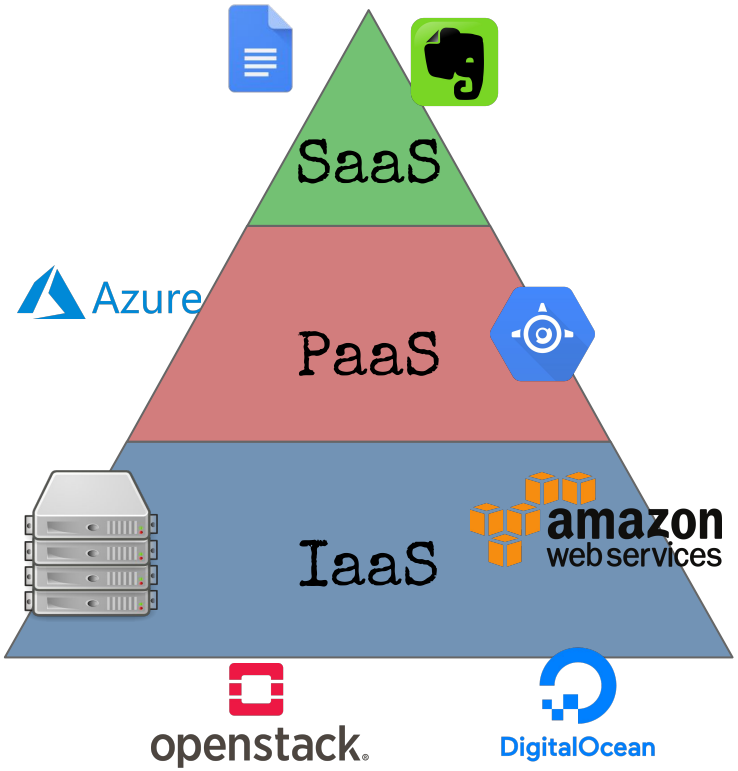
What is "The Cloud"?

- "A computing storage system that provides on-demand network access for multiple users and can allocate storage to users to keep up with changes in their needs."
  - Paraphrasing of NIST SP 800-145 (from the textbook).
- Layer of abstraction for computer **hardware**, **operating systems**, and **software**.
  - Abstracting these away means you don't have to worry about the details as much.

History of the Cloud

- **1961**: Professor John McCarthy of MIT proposed selling computing resources and software as a service like public utilities.
- **1963**: Dr. J. C. R. Licklider proposed interconnecting programs and data to share resources.
- **1968**: ARPA Program Plan No. 723, Resource Sharing Computer Networks, initiated. Developed into ARPANET, the predecessor to the Internet.
- **1999**: Salesforce.com developed CRM Web service, which led the way to the cloud.
- **2002**: Amazon created Amazon Mechanical Turk, providing storage, computations, and human intelligence.
- **2006**: Amazon launches its Elastic Compute Cloud (EC2) service.
- **2009**: Web 2.0 ushers in many other cloud service providers.

Cloud Service Levels



- Software as a Service (Saas)
  - Applications are delivered via the Internet, such as Google Docs.
  - Target is the end user of an application.
- Platform as a Service (Paas)
  - OS installed on a cloud server, users can install their software and tools.
  - Target is the application developer.
- Infrastructure as a Service (IaaS)
  - Customer rents hardware, installs OS of choice. Highly configurable network options. Tremendous scaling ability.
  - Target is the system administrator.

Cloud Deployment Methods

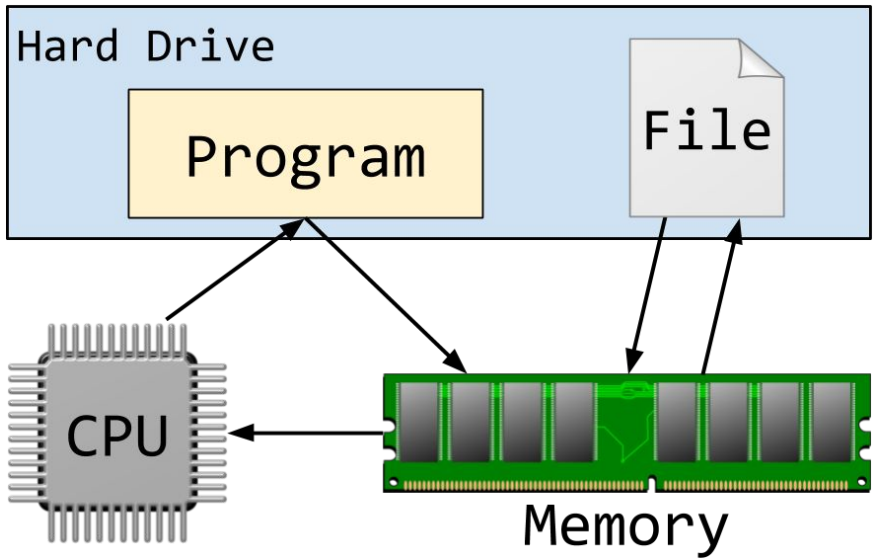
- Public Cloud:
  - Cloud services are available to anyone.
- Private Cloud:
  - Limited-access, typically on-premises.
  - Uses a cloud architecture such as OpenStack.
- Community Cloud:
  - A way to bring people together for a specific purpose.
- Hybrid Cloud:
  - A public and private cloud that talk to each other.
  - Gives companies more control over data and services.

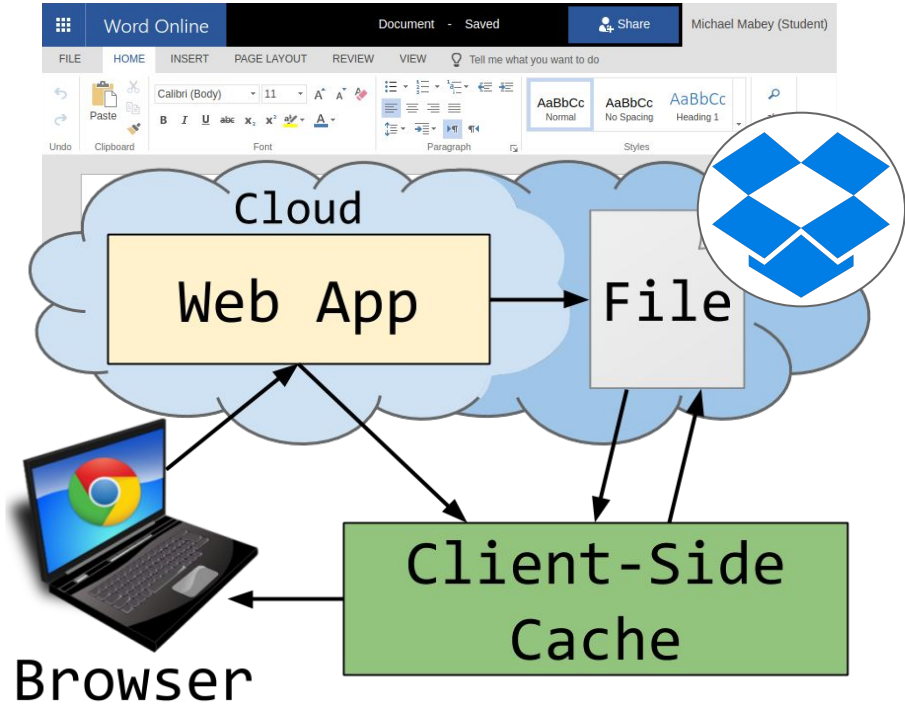
Cyber Crimes Using the Cloud

- Cloud assisted:
  - Using cloud VMs as bots or Command and control servers
  - Data breach (tool)
- Cloud targeted:
  - Cyber attack against a cloud
  - Policy violations in accessing a cloud
  - Data breach (victim)
- Cloud incidental:
  - Fraud
  - Data breach (storage)

A Framework for Web Environment Forensics

Traditional Program vs. Web App

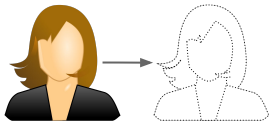




Unique Web Forensic Challenges

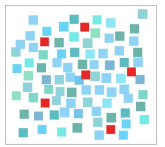
C0. Complying with the Rule of Completeness

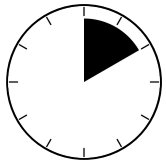
C1. Associating a suspect with online personas



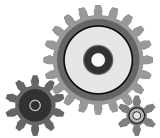
C2. Gaining access to the evidence stored online

C3. Contextualizing evidence in terms of content (*thematic context*) and time (*temporal context*)





C4. Integrating tools to perform advanced analyses



Framework

F1. Evidence Discovery and Acquisition

- Connect suspect and persona (**C1**)
- Gain access to evidence from web services (**C2**)*

F2. Analysis Space Reduction

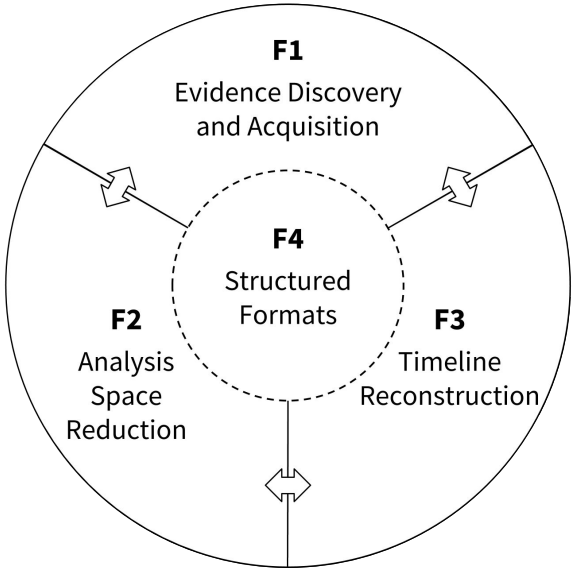
- Filter irrelevant artifacts (**C3** *Thematic* Context)*

F3. Timeline Reconstruction

- Reconstruct timeline (**C3** *Temporal* Context)*

F4. Structured Formats

- Bridges the other three components
- Facilitate tool interoperability (**C4**)

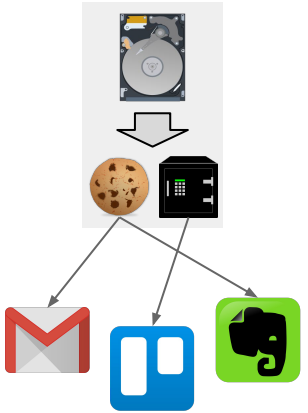


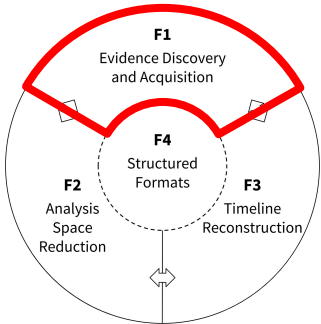
	F1	F2	F3	F4
C0: Rule of Completeness	●	●	●	○
C1: Associating Personas	●	○	○	○
C2: Evidence Access	●	○	○	○
C3: Relevant Context	○	●	●	○
C4: Tool Integration	○	○	○	●

* Also addresses **C0**: Rule of Completeness

F1: Evidence Discovery and Acquisition

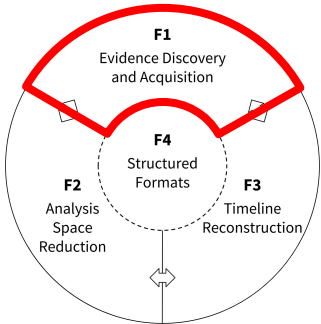
- Examiner's Process:
  - Discovery
    - Search storage of devices in custody for service credentials
    - Derive the corresponding service
  - Acquisition
    - Devise means to acquire data from service, e.g. use available APIs





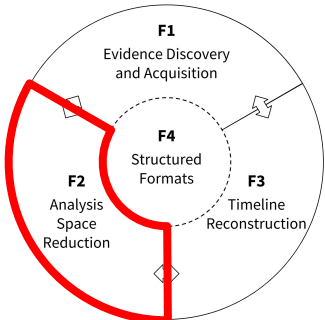
F1: Evidence Discovery and Acquisition

- Challenges:
  - Volume of data
  - Boundaries of data are ambiguous
    - Geographically
    - Ownership
  - User may have many accounts
    - Difficult to discover and acquire all data
    - Harder to determine relevance (**F2**)



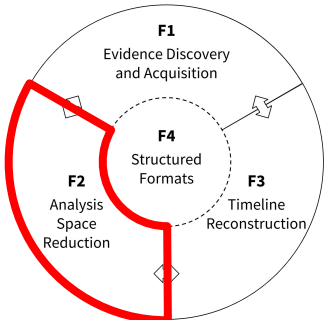
F2: Analysis Space Reduction

- Examiner's Process:
  - Classification
    - Place labels on artifacts indicating subject or theme
    - Filter for relevant labels
  - Identification
    - Determine *what* the evidence is
    - Helpful when evidence is encrypted



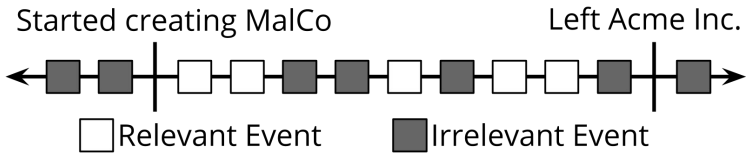
F2: Analysis Space Reduction

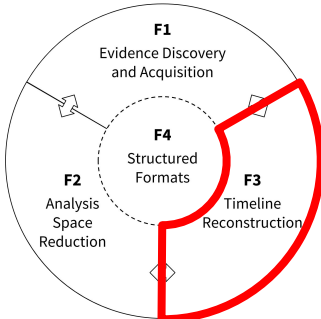
- Challenges:
  - False positives (labeling artifact as relevant when not)
    - Sub-optimal reduction
  - False negatives
    - Obscures relevant data from examiner, altering outcome of investigation
  - Exculpatory evidence (suggesting innocence)
    - Prone to false negatives
    - Difficult to identify



F3: Timeline Reconstruction

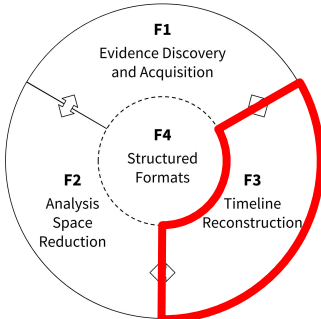
- Examiner's Process:
  - Collect and combine available time data
    - Requires **F1** tools and methods
  - Remove irrelevant data
    - Extra metadata
    - Data outside timeframe of interest
  - Establish relationship between entries
    - Chronological ordering
    - Correlations





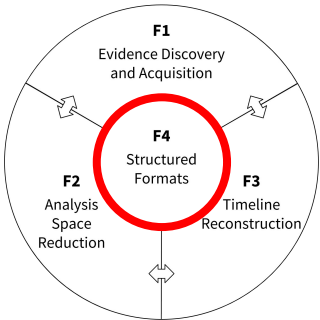
F3: Timeline Reconstruction

- Challenges:
  - Incorporation into existing tools
    - Extra metadata from web services
  - Large variety of types and formats of logs
    - IoT devices
  - Reconcile time data from different sources, time zones
    - Cannot assume UTC



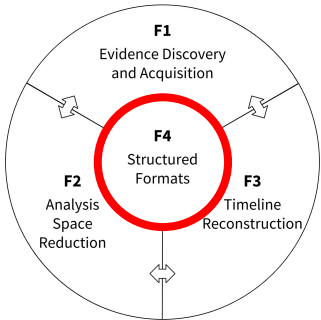
F4: Structured Formats

- Examiner's Process:
  - Examiners should not have to work directly with structured storage formats



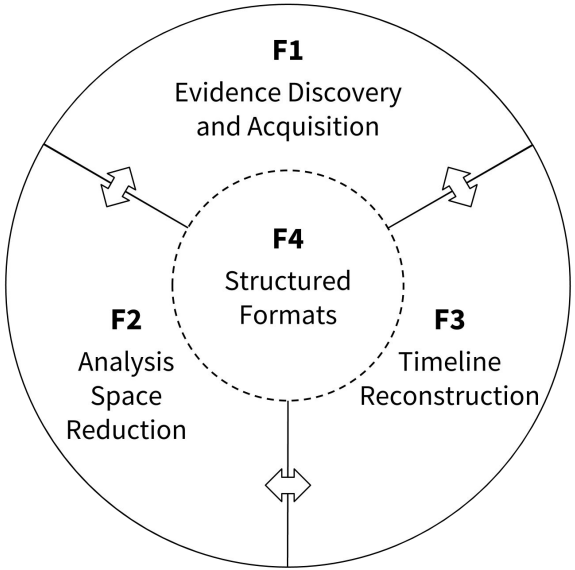
F4: Structured Formats

- Challenges:
  - Three requirements for structured formats:
    - Precise representation of original data
    - Method of verifying data conforms to specification
    - Specification must be published
  - Trade-offs
    - Supporting different platforms
    - Keeping specification concise



Framework: Summary

- Directly addresses the unique forensic challenges (**C0**-**C4**)
- Gives examiners a way to approach web-based evidence
- Provides examiners with:
  1. Previously unknown data
  2. Relevant context
- Non-sequential structure
- Fits within existing forensic processes



	F1	F2	F3	F4
C0: Rule of Completeness	●	●	●	○
C1: Associating Personas	●	○	○	○
C2: Evidence Access	●	○	○	○
C3: Relevant Context	○	●	●	○
C4: Tool Integration	○	○	○	●

Considerations for Forensic Investigations in the Cloud

Legal Challenges

- Service Level Agreements (SLAs):
  - Among other things, these state **who** is authorized to access data and **what the limitations are** in conducting acquisitions for an investigation.
- Jurisdiction issues:
  - Perpetrator, victim, and instrument of the crime can all be in **different locations** with **different laws** applying to each in **different ways**.
- Accessibility:
  - **Search Warrant**: Used only in **criminal** cases, requested by **law enforcement** with probable cause of a crime. Used to **seize hardware**.
  - **Subpoenas and Court Orders**: Used when **information** (or **data**) is needed, not the original equipment.

Technical Challenges (1)

- Cloud architectures vary:
  - No two providers are alike.
- Data collection and authentication:
  - Remote acquisitions are hard.
  - Virtual network switches == duplicate IPs, IP spaces.
  - Encrypted data (now common) requires cooperation of cloud provider to access the data.
- Analysis of cloud forensic data:
  - Verifying integrity, reconstructing timeline is even harder.

Technical Challenges (2)

- Anti-forensics:
  - Myriad ways for criminals to undermine evidence collection and analysis.
- Incident first responders:
  - Will they be cooperative, well-trained, and capable?
- Role management:
  - Who has what roles (owner, user, etc.)?
- Standards and training:
  - Never-ending struggle to keep up with current technologies and approaches.

Levels of Investigation

- Cloud Service Provider (CSP):
  - Requires detailed knowledge of the cloud's topology, policies, data storage methods, and devices available.
- Cloud customers:
  - Data may be stored on computers, mobile devices, in web browser cache, etc.
- Locally-stored cloud data:
  - Popular cloud storage services have sync clients that leave artifacts even when uninstalled.
  - May include info about files that were never synced.

Conclusion

Each of the layers of abstraction that make cloud computing so *awesome* for the rest of the world make a forensic examiner's job **WAY** more difficult.