Guide to Computer Forensics and Investigations Sixth Edition

Chapter 13

Cloud Forensics

Objectives

- Describe the main concepts of cloud computing
- Summarize the legal challenges in conducting cloud forensics
- Give an overview of the technical challenges with cloud forensics
- Describe how to acquire cloud data
- Explain how to conduct a cloud investigation
- Explain what remote access tools can be used for cloud investigations

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Cloud Computing

- The cloud has introduced ways of managing data that didn't exist a decade ago
- Cloud investigations have unique challenges
- New standards are being developed to improve security practices and incident responses in cloud environments

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

History of the Cloud (1 of 2)

- Idea of cloud computing came from several people:
  - Professor John McCarthy of MIT
  - Dr. J.C.R. Licklider, director at the U.S. Department of Defense Advanced Research Projects Agency (ARPA)
- In 1999, Salesforce.com developed a Web service that applied digital marketing research to business subscribers
  - This service led the way to the cloud

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

History of the Cloud (2 of 2)

- Amazon created Amazon Mechanical Turk in 2002
  - Provided storage, computations, and human intelligence
  - Started Elastic Compute Cloud (EC2) in 2006, aimed at supporting small businesses
- After Web 2.0 in 2009, other providers started their own cloud services
  - Google Apps, Apple iCloud, Microsoft OneDrive, and more

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Cloud Service Levels and Deployment Methods (1 of 4)

- The National Institute of Standards and Technology (NIST) defines cloud computing as:
  - 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

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Cloud Service Levels and Deployment Methods (2 of 4)

- The cloud has three service levels:
  - **Software as a service (SaaS)** - applications are delivered via the Internet
  - **Platform as a service (PaaS)** - an OS has been installed on a cloud server
  - **Infrastructure as a service (IaaS)** - customers can rent hardware and install whatever OSs and applications they need

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Cloud Service Levels and Deployment Methods (3 of 4)

Table 13-1	Locations of evidence in different service levels
Service level	**Locations of evidence**
SaaS	Most likely stored on a desktop, laptop, tablet, or smartphone.
PaaS	Most likely found on a desktop or server, although it could also be stored on a company network or the remote service provider's infrastructure.
IaaS	Usually found on a desktop or server; infrastructure equipment can be owned by the company or the remote service provider.

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Cloud Service Levels and Deployment Methods (4 of 4)

- Deployment methods for a cloud:
  - **Public** - accessible to anyone
  - **Private** - can be accessed only by people who have the necessary credentials
  - **Community** - a way to bring people together for a specific purpose
  - **Hybrid** - enables a company to keep some information private and designate other files as public or community information

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Cloud Vendors

- Some **cloud service providers (CSPs)** and cloud applications:
  - Salesforce
  - IBM Cloud
  - Cisco Cloud Computing
  - Amazon EC2
  - AT&T Synaptic
  - Google Cloud Storage
  - HP Helion
  - Microsoft Azure
  - XenServer and XenCenter Windows Management Console
  - Rackspace
  - Oracle Cloud

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Basic Concepts of Cloud Forensics (1 of 2)

- Cloud forensics is considered a subset of network forensics
- Cloud forensics can have three dimensions:
  - Organizational - addresses the structure of the cloud
  - Legal - covers service agreements and other jurisdictional matters
  - Technical - deals with procedures and specialized applications designed to perform forensics recovery and analysis in the cloud

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Basic Concepts of Cloud Forensics (2 of 2)

- Forensic tool capabilities needed to handle acquiring data from a cloud:
  - *Forensic data collection* - must be able to identify, label, record, and acquire data from the cloud
  - *Elastic, static, and live forensics* - must be able to expand and contract their storage capabilities
  - *Evidence segregation* - different businesses and users share the same applications and storage space
  - *Investigations in virtualized environments* - should have the capability to examine virtual systems

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Legal Challenges in Cloud Forensics

- When investigating a cloud system, consider factors involving a CSP's relationship with cloud users
- This section explains:
  - A CSP's contract obligations with cloud users
  - How warrants and subpoenas are applied to CSPs and users

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Service Level Agreements (1 of 5)

- **Cloud service agreements (CSAs)** - a contract between a CSP and the customer that describes what services are being provided and at what level
  - Includes service legal agreements (SLAs)
- CSAs should also specify:
  - Support options
  - Penalties for services not provided
  - System performance
  - Fees
  - Provided software or hardware

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Service Level Agreements (2 of 5)

- CSAs define the scope of services the CSP provides:
  - Service hours
  - Restrictions applied to the customer by the CSP
  - Availability of the cloud to the customer
  - Levels of support for the customer
  - Response time for data transfers
  - Throughput, limitations
  - Contingency plan for incident response
  - Business continuity and disaster recovery plan

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Service Level Agreements (3 of 5)

- CSAs define the scope of services the CSP provides (cont'd):
  - Fees for the subscription to the cloud and fees for additional services as they occur
  - Security measures
  - Terminology of the cloud's systems and applications
- CSP components must state who is authorized to access data and what the limitations are in conducting acquisitions for an investigation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Service Level Agreements (4 of 5)

- Policies, Standards, and Guidelines for CSPs
  - Digital forensics should review CSPs policies, standards, and guidelines for daily operations
  - Policies - detailed rules for a CSP's internal operation
  - Standards - give guidance to staff for unique operations, hardware, and software and describe the staff's obligations regarding security of the CSP environment
  - Guidelines - describe best practices for cloud processes and give staff an example of what they should strive to achieve in their work

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Service Level Agreements (5 of 5)

- CSP Processes and Procedures - are detailed documents that define workflow and step-by-step instructions for CSP staff
  - Often include hardware configuration diagrams, network maps, and application processing flowcharts
  - Digital forensics examiners can use them to understand how data is stored, manipulated, secured, backed up, restored, and accessed by CSP staff and customers
- Additional documents of interest:
  - CSP business continuity and disaster recovery plans

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Jurisdiction Issues (1 of 2)

- Although there are plans to revise current laws
  - Many cross-jurisdiction legal issues haven't been resolved
- No law ensures uniform access or required handling procedures for the cloud
- Investigators should be concerned about cases involving data commingled with other customers' data
- Often, figuring out what law controls data stored in the cloud is a challenge

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Jurisdiction Issues (2 of 2)

- How privacy rights are defined in different jurisdictions is a major factor in problems with the right to access data
- EU Directive 95/46/EC is more restrictive than rules in other countries, including the U.S.
  - Protects private information for all EU citizens
- Digital forensics examiners could be held liable when conducting an investigation involving cloud data
  - Consult with legal experts to be aware of possible restrictions

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Accessing Evidence in the Cloud (1 of 4)

- The Electronic Communications Privacy Act (ECPA) describes five mechanisms the government can use to get electronic information from a provider:
  - Search warrants
  - Subpoenas
  - Subpoenas with prior notice to the subscriber or customer
  - Court orders
  - Court orders with prior notice to the subscriber or customer

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Accessing Evidence in the Cloud (2 of 4)

- Search Warrants
  - Can be used only in criminal cases and must be requested by a law enforcement officer who has evidence of probable cause that a crime was committed
  - Law requires search warrants to contain specific descriptions of what's to be seized
  - For cloud environments, the property to be seized usually describes data rather than physical hardware, unless the CSP is the suspect

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Accessing Evidence in the Cloud (3 of 4)

- Search Warrants (cont'd)
  - Must also describe the location of items to be seized
    - Difficult when dealing with cloud data because servers are often dispersed across state or national borders
  - Must establish how it will be carried out
    - Specifying the date and time of day to minimize disruptions to people and business operations

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Accessing Evidence in the Cloud (4 of 4)

- Subpoenas and Court Orders
  - *Government agency subpoenas* - customer communications and records can't be knowingly divulged to any person or entity
    - Used to get information when it's believed there's a danger of death or serious physical injury
  - *Non-government and civil litigation subpoenas* - used to produce information from private parties for litigation
  - *Court orders* - written by judges to compel someone to do or not do something

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Technical Challenges in Cloud Forensics

- Challenges in conducting cloud forensics
  - Architecture
  - Data collection
  - Analysis of cloud forensic data
  - Anti-forensics
  - Incident first responders
  - Role management
  - Legal issues
  - Standards and training

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Architecture

- No two CSPs are configured exactly the same way
- Depending on the type of cloud architecture
  - Customer's data could be commingled
- Most CSPs keep data storage locations secret for security reasons
- Differences in recording procedures or log keeping can make it difficult to determine data's origin
  - And complicate an investigation's chain of evidence

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Analysis of Cloud Forensic Data

- Analyzing digital evidence from a cloud requires verifying the data with other data and log records
- Data may need to be reconstructed to determine what actually occurred during an incident
- Examining logs can be useful to compare the modified, last access, and create (MAC) dates and times for files

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Anti-Forensics (1 of 2)

- Anti-forensics - destroying ESI that may be potential evidence
- Hackers may use specialized malware for defeating evidence collection
- Additional methods for anti-forensics:
  - Inserting malware programs in other files
  - Using encryption to obfuscate malware programs activated through other malware programs
  - Using data-hiding utilities that append malware to existing files

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Anti-Forensics (2 of 2)

- Other techniques affect file metadata by changing the modify and last access times
- Changing timestamps can make it difficult to develop a timeline of a hacker's activities
- Calculating hash values of files and comparing the results with known good files' hash values can help identify files that might have been altered

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Incident First Responders (1 of 2)

- CSPs have personnel trained to respond to network incidents
  - They become first responders when a network intrusion occurs
- When CSPs do not have an internal first responder team, the forensics examiner should organize CSP staff to handle these tasks

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Incident First Responders (2 of 2)

- Some factors to address include:
  - Will the CSP's operations staff be cooperative and follow directions, and will management issue orders stating that you're the leader of the investigation?
  - Do you need to brief staff about operations security? For example, you might need to explain that they should talk only to others who have a need to know about the incident and the investigation's activities
  - Do you need to train staff in evidence collection procedures, including the chain of custody?

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Role Management

- Role management in the cloud covers:
  - Data owners
  - Identity protection
  - Users
  - Access controls
- As an investigator, you need to collect this information so you can identify additional victims or suspects

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Standards and Training (1 of 2)

- There is an effort to standardize cloud architectures for:
  - Operating procedures
  - Interoperability
  - Testing
  - Validation
- The Cloud Security Alliance (CSA) has develop resource documentation for CSPs and their staff

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Standards and Training (2 of 2)

- Cloud investigators should have an understanding of cloud architecture
  - In addition to basic digital and network forensic skills
- Sources for cloud forensics training:
  - (ISC)²'s Certified Cyber Forensics Professional
  - INFOSEC Institute
  - SANS Cloud Forensics with F-Response
  - National Institute of Justice Digital Forensics Training
  - University College Dublin Centre for Cybersecurity and Cybercrime Investigation

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquisitions in the Cloud

- Methods used to collect evidence in cloud investigations depend on the nature of the case
- Recovering deleted data from cloud storage might be limited to the type of file system the CSP uses
- With cloud systems running in a virtual environment, snapshots can give you valuable information before, during, and after an incident
  - Forensic examiners should re-create separate cloud servers from each snapshot, acquire an image of each server, and calculate a hash for all files

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Encryption in the Cloud (1 of 3)

- Many CSPs and third parties offer encryption services for cloud users as a security measure
  - Expect to find encrypted files in cloud investigations
- You need assistance from the data owner or the CSP to decrypt data with the right encryption key
  - If data owner is uncooperative, you may need to turn to the attorneys handling the case or data owner's management

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Encryption in the Cloud (2 of 3)

- Encrypted data in the cloud is in two states:
  - Data at rest - data that has been written to disk
  - Data in motion - data being transmitted over a network
- Some system also have encryption for data in use (data that's in RAM)
- If encrypted data is encountered
  - Find out from the CSP what type of encryption was used and who knows how to recover it

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Encryption in the Cloud (3 of 3)

- Vendors that offer encryption services for cloud data:
  - Atalla Cloud Encryption from Micro Focus
  - SecureCloud from Trend Micro
  - SafeGuard Encryption and Sophos Mobile Control from Sophos
- Homomorphic encryption
  - Uses an “ideal lattice” mathematical formula to encrypt data
- Block chain technology
  - Used by companies such as Bitcoin, is a way to trace your information while keeping it secure

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Conducting a Cloud Investigation

- When investigating cloud incidents:
  - Use a systematic approach just like the one covered in Chapter 1
- The type of incident determines how to proceed with planning the investigation
- If the investigation involves searching for and recovering data from cloud storage or cloud customers
  - Follow methods described in Chapters 5 and 6

CENGAGE
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Investigating CSPs (1 of 2)

- If a CSP has no team or limited staff, investigators should ask the following questions to understand how the CSP is set up:
  - Does the investigator have the authority to use cloud staff and resources to conduct an investigation?
  - Is detailed knowledge of the cloud's topology, policies, data storage methods, and devices available?
  - Are there any restrictions on collecting digital evidence from remote cloud storage?

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Investigating CSPs (2 of 2)

- Investigators should ask the following questions to understand how the CSP is set up (cont'd):
  - For e-discovery demands on multitenant cloud systems, is the data to collect commingled with other cloud customers' unrelated data? Is there a way to separate the data to prevent violating privacy rights or confidentiality agreements?
  - Is the data of interest to the investigation local or remote? If it's in a remote location, can the CSP provide a forensically sound connection to it?

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Investigating Cloud Customers

- If a cloud customer doesn't have the CSP's application installed
  - You might find cloud-related evidence in a Web browser's cache file
- If the CSP's application is installed
  - You can find evidence of file transfers in the application's folder
  - Usually found under the user's account folder

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Prefetch Files (1 of 2)

- Prefetch files - contain the DLL pathnames and metadata used by an application
- The OS reads the associated prefetch file and loads its information into the computer's memory
  - Speeds an application's start time
- The OS can handle other tasks instead of waiting for an application to load needed libraries
- Example:
  - Metadata in a prefetch files contains an application's MAC times in UTC format and a counter of how many times the app has run

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Prefetch Files (2 of 2)

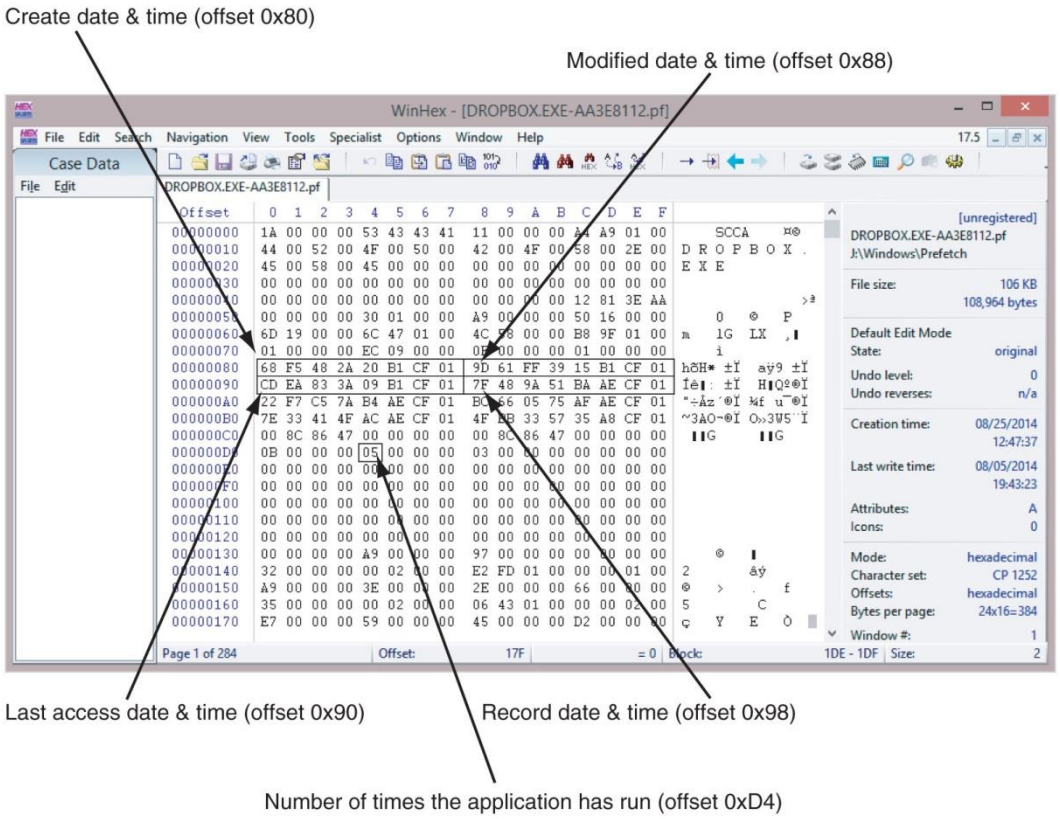

Figure 13-1 Showing the offset positions for the counter and the dates and times for `Dropbox.exe`

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Stored Cloud Data on a PC (1 of 6)

- Three widely used cloud services:
  - Dropbox
  - Google Drive
  - OneDrive
- Services are free for storage up to 2 GB for Dropbox and up to 15 GB for Google Drive and OneDrive
- These applications have Registry entries
- Users must maintain control over access to their cloud accounts

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Stored Cloud Data on a PC (2 of 6)

- Dropbox offers third-party applications, such as e-mail, chat, Cisco WebEx, and other collaboration tools
- Since 2012, Dropbox has used base-64 format to store content
  - Reading them requires specialized software
  - Magnet Forensics has a tool called Internet Evidence Finder (IEF) designed for this purpose

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Stored Cloud Data on a PC (3 of 6)

- Gmail users have access to Google Drive for cloud data storage and applications
- Google Drive is installed in:
  - C:\Program Files (x86)\Google\Drive
- Each user has a configuration file stored in C:\Users*username*\AppData\Local\Google\Drive
  - Called a “user profile”
- If Google Drive has been installed, it creates a folder in the path C:\Users*username*\Google Drive

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Stored Cloud Data on a PC (4 of 6)

- Important Google Drive files:
  - `sync_config.db` - an SQL database file with Google Drive upgrade number, highest application version number, and local synchronization root path
  - `snapshot.db` - contains information about each file accessed, the URL pathname, the modified and created dates and times in UNIX timestamp format, and the file's MD5 value and size
  - `sync_log.log` - has a detailed list of a user's cloud transactions

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Stored Cloud Data on a PC (5 of 6)

- OneDrive - created by Microsoft and was originally called SkyDrive
  - Available with Windows 8 and later
  - Similar to DropBox and Google Drive and offers subscription services for Microsoft software
- OneDrive stores user profiles in the user's account path
- Log files and synchronized files are kept in various places under the user's account (depending on the Windows version)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Stored Cloud Data on a PC (6 of 6)

- You can find more information in the following Windows 8.1 log files, which are in the C:\Users\username\AppData\Local\Microsoft\Windows\SkyDrive\logs folder
  - `SyncEngine-yyyy-mm-ddnn.nnn-n.et1` manages synchronization between OneDrive and a user's computer
  - `SyncDiagnostics.log` contains client ID, clientType, clientVersion, device, deviceID, and timeUtc values

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Windows Prefetch Artifacts

- You can collect prefetch file artifacts with a disk editor or forensics tool
- Follow the steps in the activity starting on page 546 to use WinHex's Data Interpreter to find an application's MAC dates and times
  - And the number of times DropBox has run

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tools for Cloud Forensics

- Few tools designed for cloud forensics were available
- Many digital, network, and e-discovery tools can be combined to collect and analyze cloud data
- Some vendor with integrated tools:
  - Guidance Software EnCase eDiscovery
  - AccessData Digital Forensics Incident Response
  - F-Response

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensic Open-Stack Tools (1 of 2)

- Forensic Open-Stack Tools (FROST) integrates with OpenStack running in IaaS cloud environments
  - Adds forensics response capabilities for a CSP
- OpenStack - an open-source computing platform intended for public and private cloud services
- FROST is the first known effort to provide a forensics response process for a cloud service

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensic Open-Stack Tools (2 of 2)

- A feature of FROST
  - It bypasses a VMs hypervisor
  - Collected data is placed in the cloud's **management plane**, which is a tool with application programming interfaces that allow reconfiguring the cloud on the fly
  - Special malware can take control of the virtual session and deny or alter access
  - Can also prevent or interfere with forensic analysis and data collection

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

F-Response for the Cloud

- F-Response is a remote access tool that can be applied to cloud forensics
  - Uses USB forwarding techniques to allow non-remote-capable forensics tools to access remote servers and their data storage
- Two tools are needed:
  - F-Response Enterprise or Consultant
  - KernelPro USB-Over-Ethernet

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Magnet AXIOM Cloud

- Magnet AXIOM created a Cloud module to go with its Process and Examine modules
- Magnet AXIOM Cloud
  - Retrieves information from Facebook Messenger, Skype, Instagram, Twitter, iCloud, and others
  - You still need usernames and passwords

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 4)

- Three service levels are available for the cloud: software as a service, platform as a service, and infrastructure as a service
- CSPs use servers on distributive networks or mainframes that allow elasticity of resources for customers
- With multinational clouds, you should seek legal counsel before proceeding with an investigation
- Cloud investigations are necessary in cases involving cyberattacks, policy violations, data recovery, and fraud complaints

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 4)

- Before initiating a cloud investigations, review the CSA to identify any restrictions that might limit collecting and analyzing data
- Technical challenges in cloud forensics involve cloud architecture, data collection, analysis of cloud forensic data, anti-forensics, incident first responders, role management, legal issues, and standards and training
- Anti-forensics is an effort to alter log records as well as date and time values of important system files and install malware to hide hacker's activities

CENGAGE
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 4)

- CSPs should have an incident response team ready to respond to network intrusions
- Role management defines the duties of CSP staff and customers
- The Cloud Security Alliance has developed resources that guide CSPs in privacy agreements and security measures
- Procedures for acquiring cloud evidence include examining network and firewall logs, performing disk acquisitions of a cloud system's OS, and examining data storage devices

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (4 of 4)

- When investigating a cloud incident, apply a systematic approach to planning and processing the case
- The three cloud services Dropbox, Google Drive, and Microsoft OneDrive contain data on a user's computer or mobile device that can reveal what files were copied or accessed
- Vendors offer tools that can be combined for cloud forensics

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.