Mobile Devices, IOT, & Cloud

Objectives

- Explain the basic concepts of mobile device forensics
- Describe procedures for acquiring data from mobile devices
- Summarize the challenges of forensic acquisitions of data stored on Internet of Anything devices
- 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

Mobile Device Basics

Why Cell Phones?

- People store a wealth of information on cell phones
  - Calls
  - Messages (SMS, MMS, Email, etc.)
  - Web pages
  - Pictures, video, music
  - Calendars
  - Application specific information of the above types

The Cell Phone Problem is Hard

- There is not a single standard for how to store phone messages between disparate devices

- Phones change rapidly and they’re often not directly compatible or comparable to previous models

Cell Phone Network Types

- Code Division Multiple Access (CDMA)
- Global System for Mobile Communications (GSM)
- Time Division Multiple Access (TDMA)
- Integrated Digital Enhanced Network (iDEN)
- Digital Advanced Mobile Phone Service (D-AMPS)
- Enhanced Data GSM Environment (EDGE)
- Orthogonal Frequency Division Multiplexing (OFDM)

Cell Phone Internals

- Many similar components to a personal computer
  - Likely additional components for cellular phone and data
  - Perhaps a touch screen as well
- Electronically Erasable Programmable Read-Only Memory (EEPROM) can store system data and allow changes to devices without physical access
- Subscriber Identity Module (SIM) cards
  - Contains small amount of internal memory for storing basic connection & backup info

Additional Phone Storage

- SD or Micro SD cards
  - Can contain certain artifacts from applications but often will contain multimedia files as they're generally the largest

Mobile Device Acquisition

Considerations of Mobile Acquisition

- The same concerns we have for collecting evidence from network connected systems apply to phones
  - Connected / networked phones can be remotely wiped or modified
  - There is volatile data in RAM on phones that can be valuable if we’re able to collect it
- Warrant / subpoena / search authorization may only allow collection in a specific window so it’s important to isolate the phones outbound connection (and to prevent modification)
- Isolation can be done with airplane mode, a faraday bag, or turning the device off
  - This will increase battery use while device searches for signal

SANS Phone Collection Notes

- If device is on and unlocked - isolate it from the network, disable the screen lock, remove passcode

- If device is on and locked - what you can do varies depending on the type of device

- If device is off - attempt a physical static acquisition and turn the device on

Storage of Interest on Mobile Devices

- Internal
- SIM Card
  - Service-related data, such as identifiers for the SIM card and the subscriber
  - Call data, such as numbers dialed
  - Message information
  - Location information
- Removable media (SD / Micro SD)
- Network provider / cloud storage
  - This likely requires a separate warrant or subpoena depending on how initial warrant or subpoena was written

Mobile Forensics Equipment

- Required hardware and software can vary by device manufacturer and the type of acquisition you'd like to do
- NIST guidelines list six types of mobile forensics methods
  - Manual extraction
  - Logical extraction
  - Physical extraction
  - JTAG extraction
  - Chip off
  - Micro read

Manual Extraction

- Examiner accesses device as regular user
- Document what you see and find with photographs as you go
- Worst case for forensics as you'll be modifying log data and other system access info as you continue to use the device

Logical or Physical Extraction

- Mobile device is connected to a forensic workstation
- Logical collects file system layout in the same way we do on a computer
  - No deleted files will be recovered
  - Typically used on encrypted devices or devices where physical collection isn’t supported by your tool suite
- Physical collects the state of the disk itself and the file system is parsed later
  - Deleted items can be retrieved from this type of extraction

JTAG, Chip Off, & Micro Read

- JTAG is a standard for verifying designs of printed circuit boards after manufacturing – this debug interface can be used to read data from certain chips on a mobile device

- Chip off is the method of removing storage media that’s soldered to mobile devices and reading it with a chip programmer or forensic interface

- Micro read uses a high-powered microscope to review the contents of devices

IOT

Internet of Things / Internet of Anything

Forensics in the Connected World

- In 2010, VMware and BlackBerry were developing type 2 hypervisors for mobile devices
    - Useful for security and protecting personal information but will add another level of complexity to forensics investigations
- Internet of Things (IoT)
    - The number of devices that connect to the Internet is higher than the amount of people
        - That number is expected to reach 50 billion in the next few decades

Evolution

- Evolution from Internet of Thing (IoT) to Internet of Everything (IoE) to Internet of Anything (IoA)
- IoE adds features that aren’t tangible but are widespread on the Internet
  - Google search engine and YouTube
- IoA includes cars, homes, pets, livestock, and applications for making all these things work together
  - Eventually will include 5G smart devices
- 5G devices categories:
  - enhanced Mobile Broadband (eMBB)
  - Ultra-reliable and Low-latency Communications (uRLLC)
  - massive Machine Type Communications (mMTC)

Challenges

- 5G devices introduce new challenges for digital forensics:
  - People-to-device communications (P2D)
  - Device-to-device (D2D) communications
  - Device-to-cloud (D2C) communications
- Wearable computers will pose many new challenges for investigators
- Vehicle system forensics
  - Addresses the many parts that have sensors in cars

Cloud Overview

What is Cloud Computing?

- Wikipedia
  - Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user.
- NIST
  - 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

https://en.wikipedia.org/wiki/Cloud_computing

Brief History

- 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)
- 1999 – salesforce.com
- 2006 – Amazon Web Services (AWS) Elastic Compute Cloud (EC2)
- 2009 & beyond – countless cloud provider options

Service Levels *

- **Software as a service (SaaS)** - applications delivered via the Internet and access provided via subscription

- **Platform as a service (PaaS)** – a platform is provided to run an application (such as a database or webapp) without the user having to consider hardware and operating system

- **Infrastructure as a service (IaaS)** - customers can rent hardware or VMs and install whatever OSs and applications they need

* There are other service levels defined elsewhere – these are core ones from NIST 800-145

Evidence Location by Service Level

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.

Cloud Deployment Methods

- **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

Cloud Service Providers

- Salesforce
- IBM Cloud
- Cisco Cloud Computing
- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- Rackspace
- Oracle Cloud
- Digital Ocean

Basics of Cloud Forensics

- 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

Required Tool Capabilities for 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

Legal Challenges of Cloud

Computers At Large

- When investigating a cloud system, consider factors involving a CSP’s relationship with cloud users

- **Cloud service agreements (CSAs)** - a contract between a CSP and the customer that describes
  - Services provided at what level
  - Support options
  - Penalties for services not provided
  - System performance
  - Fees
  - Provided software or hardware

Scope of CSAs

- 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
- 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

Jurisdiction Issues

- 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

Jurisdiction Issues (Cont.)

- 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

5 Mechanisms of Access

- 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

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
- 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

Subpoenas & 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

Technical Challenges of Cloud Forensics

Technical Challenges

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

CSP 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

Anti-Forensics

- Anti-forensics - destroying electronically stored information (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

Anti-Forensics (Cont.)

- 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

CSP Incident Response

- 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; 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?

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

Acquisition

- Methods used to collect evidence in cloud investigations depend on the nature of the case
- Recovering deleted data from cloud storage might be hindered by the type of access you have to the cloud instance
  - If it’s IaaS, you probably can gather a disk image
  - If it’s PaaS/SaaS you’ll be limited by what the CSP can provide
- 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 assess individually

Encryption in Cloud Environments

- 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

Encryption in Cloud Environments (Cont.)

- 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 systems 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

Cloud Investigations

The Basics Still Apply

- 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
- Ch 5 & 6 can help with traditional investigations
- Ch 9 & 10 can help with cyberattacks and network investigations

CSP Incident Support

- CSPs often have staff that directly support e-discovery and incident response
- 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?
  - 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?

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

- 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

Side Note: Prefetch

- The Prefetcher is a component of Microsoft Windows … that can speed up the Windows boot process and shorten the amount of time it takes to start up programs.
  - Track what programs access when system boots; use that info to perform more efficient opening of files and similar when booting
  - Application prefetch is similar but used for applications
  - Could show application use even if application has been removed from system
  - More in the next module…

https://en.wikipedia.org/wiki/Prefetcher

Cloud Data on a PC by Provider

- Dropbox
- Google Drive
- OneDrive

Dropbox

- Default user data path: C:\Users\<user>\Dropbox
- App syncing info: C:\Users\<user>\AppData\Roaming\Dropbox

- Magnet Axiom is a powerful tool for review Dropbox information

Google Drive

- Popular for personal accounts and business accounts using G Suite/Google Workspace
- Default user data path: C:\Users\<user>\Google Drive
- Default sync info path: C:\Users\<user>\App Data\Local\Google\Drive\user_default (or other profile names)
  - Sync info: sync_config.db
  - Local cloud entries: snapshot.db
  - Log: sync_log.log

OneDrive

- Logs: C:\Users\<user>\AppData\Local\Microsoft\OneDrive\logs
  - Win8 replaces OneDrive with SkyDrive
- Registry stores much of the configuration information
  - Text note: many registry entries use SkyDrive as the name still
- OneDrive additionally collects telemetry data which could contain location info

Tooling for Cloud Forensics

- Guidance Software EnCase eDiscovery
- AccessData AD eDiscovery
- F-Response
  - Can connect remote cloud resources as local USB devices for analysis by traditional tools
- Magnet Axiom

FROST

- 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
  - Moves collection from host to the IaaS directly
  - https://www.sciencedirect.com/science/article/pii/S174228761300056X

References

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*