



Cloud Forensics and IR

Natan Eliezer
Chief Research Officer
Digital Forensics Association
Champlain College

First

<https://takeout.google.com/>

Sign up and get a google
takeout of yourself!

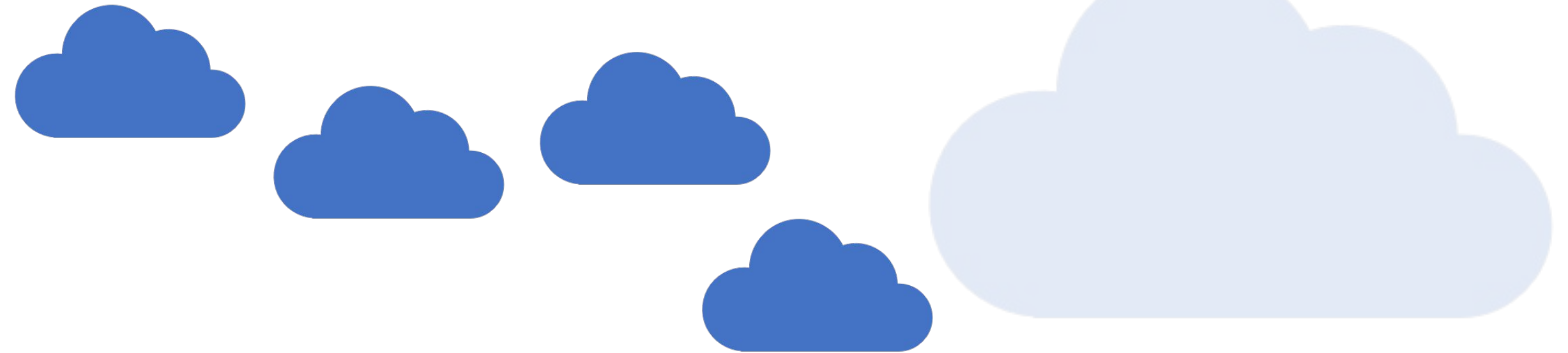
(this will be used later)

Table of Contents

- Introduction
- What is the Cloud
- Challenges in Cloud Forensics
- Cloud Forensics Process
- Cloud Tools and techniques
- Legal considerations
- Investigate yourself



“Cloud, Cloud, Cloud”



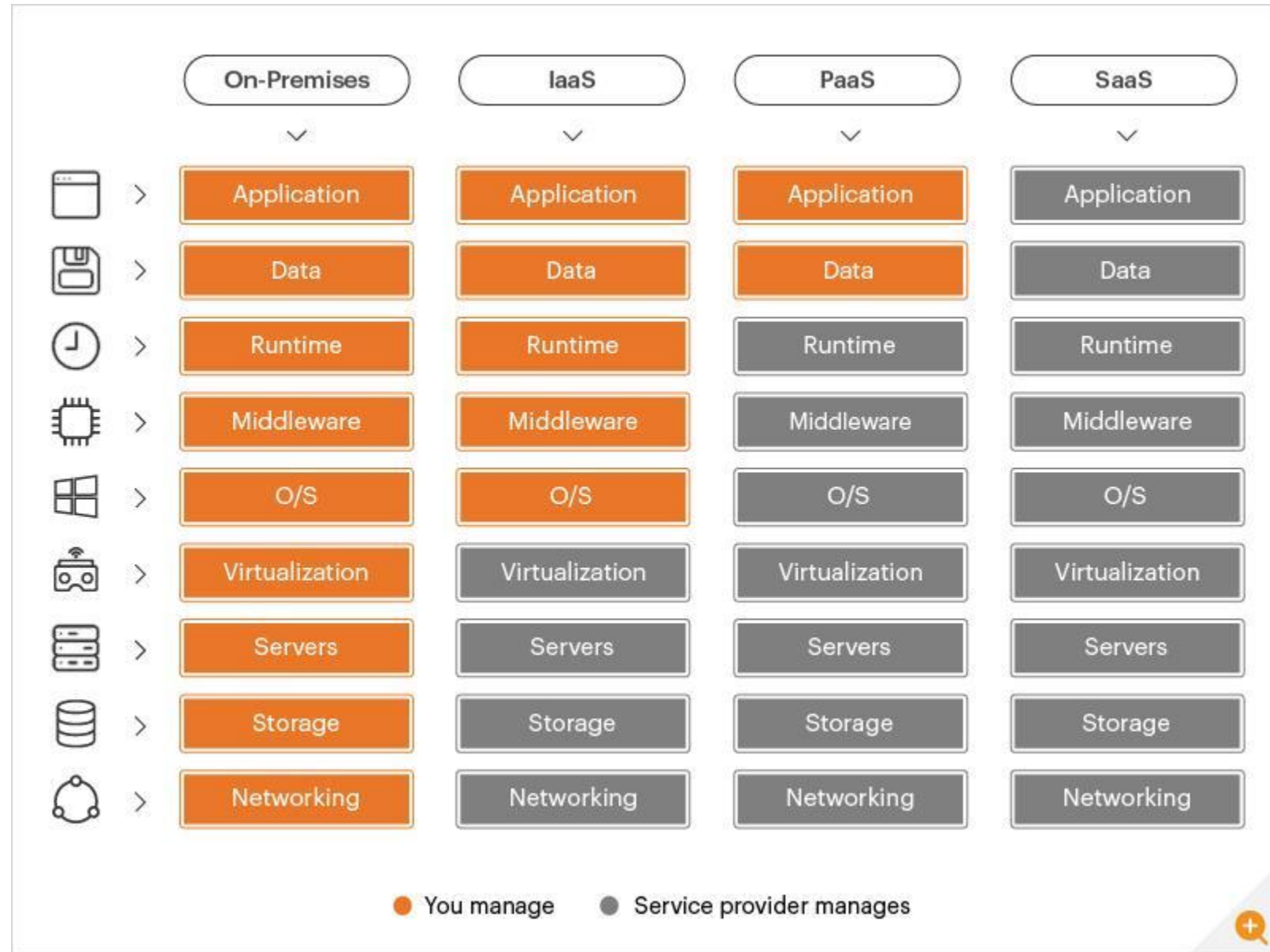
What is the cloud?

- Data that is stored in a third-party data center/service provider
- More accessible
- Cost less
- Cloud Storage
- Cloud Computing
 - Processes
 - Infrastructure



Models

- On Premises
- IaaS
 - Azure
 - AWS
- PaaS
 - Google App Engine
- SaaS
 - Gmail
 - Slack



Challenges

- Lack of control
- Data fragmentation
- Jurisdiction
- Lack of standardization
- Scope



Cloud Forensics Processes



IDENTIFICATION



PRESERVATION



ACQUISITION



ANALYSIS

Identification

- Identify what evidence is relevant to the case
- Digital Investigation
 - What cloud storage providers were used?
 - Are you able to request the data?
- Incident Response?
 - What is the scope?
 - What cloud servers were attacked?
 - Where are they hosted?



Preservation

- Make acquisitions ASAP
- Less control
- Secure storage
- Large amount of data

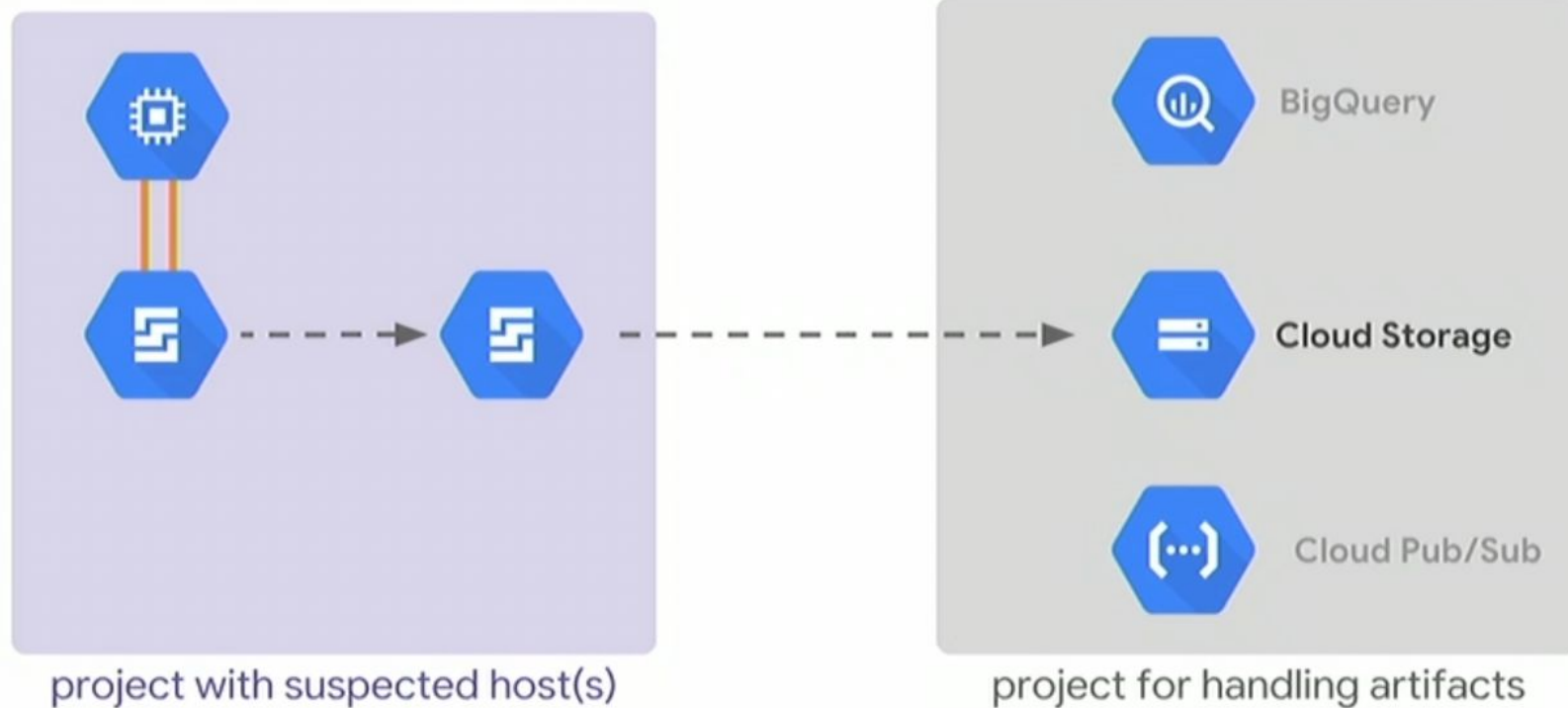


“Grab the disk drive”

Identify affected host(s)
and all attached disks

Create an duplicate of
the disk(s) while online

Send the duplicated
disk image for analysis



“Grab the disk drive”

Create a **snapshot**
from GCE attached disk

```
gcloud compute disks snapshot badhost \  
--snapshot-names=badhost-snapshot
```

Create an **image** from
the named snapshot

```
gcloud compute images create badhost-image \  
--source-snapshot badhost-snapshot
```

Export the disk image
to **GCS** artifacts bucket

```
gcloud compute images export \  
--destination-uri=gs://bad-disks/badhost.qcow2 \  
--image=badhost-image --export-format=qcow2
```



Analysis

- Make acquisitions ASAP
- Greatly depends on the amount of logging
- Cloud data can be very volatile

EVIDENCE SOURCES

SELECT EVIDENCE SOURCE



COMPUTER



MOBILE



CLOUD



VEHICLE



REMOTE COMPUTER

Tooling

- Sleuth Kit - [Link](#)
- Cloud-forensics-utilities - [Link](#)
- Axiom
- Network Forensics
- Google Rapid Response - [Link](#)

A pair of ornate brass scales of justice, symbolizing law and equity. The scales are made of dark, polished metal with intricate carvings on the base. Two pans are suspended by chains from a central vertical post. The left pan is lower, indicating it is heavier, while the right pan is higher. The background is a plain, light-colored surface, and the lighting creates soft shadows on the surface below the scales.

Legal Considerations

Certifications/Training

















- GIAC Cloud Forensics Responder found [here](#)
- [SANS FOR509: Enterprise Cloud Forensics and Incident Response](#)
- [DFIR Diva - Cloud Trainings](#)



Do some investigations on yourself!

- Now back to that google takeout

Logs!

 Access Log Activity	2/14/2024 3:57 PM	File folder
 Assignments	2/14/2024 3:46 PM	File folder
 Calendar	2/14/2024 3:46 PM	File folder
 Chrome	2/14/2024 3:46 PM	File folder
 Contacts	2/14/2024 3:46 PM	File folder
 Drive	2/14/2024 3:54 PM	File folder
 Google Account	2/14/2024 3:46 PM	File folder
 Google Business Profile	2/14/2024 3:46 PM	File folder
 Google Chat	2/14/2024 3:46 PM	File folder
 Google Finance	2/14/2024 3:46 PM	File folder
 Google Pay	2/14/2024 3:46 PM	File folder
 Google Photos	2/14/2024 3:46 PM	File folder
 Google Play Movies & TV	2/14/2024 3:46 PM	File folder
 Google Shopping	2/14/2024 3:46 PM	File folder
 Google Workspace Marketplace	2/14/2024 3:46 PM	File folder
 Groups	2/14/2024 3:46 PM	File folder

Request your data!



Takeout.google.com



Facebook takeout
support



Copy of discord data



Snapchat self archive

And many more!

Questions?