LUCID TRUTH TECHNOLOGIES

Differential File System Analysis for the Quick Win

Kenneth G. Hartman

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
SUMMIT & TRAINING 2023

About Me

LUCID TRUTH TECHNOLOGIES

LucidTruthTechnologies.com

forensicate.cloud

TorrentialDownpour.net

Kenneth G. Hartman

- Owner – Lucid Truth Technologies, a Digital Forensics Firm
- BS Electrical Engineering, Michigan Technological University
- MS Information Security Engineering, SANS Technology Institute
- Multiple Security Certifications: CISSP, GIAC Security Expert, etc.
- SANS Certified Instructor – SEC488: Cloud Security Essentials & SEC510: Public Cloud Security: AWS, Azure, and GCP

www.kennethghartman.com
@kennethghartman

The content and opinions in this presentation are my own and do not necessarily reflect the positions, strategies, or opinions of any current client or previous employer.

SANS

CLOUD SECURITY

CURRICULUM ROADMAP

Baseline

SEC 388 — **Introduction to Cloud Computing and Security**
Ground school for cloud security

Foundational Security Techniques

SEC 488 — **Cloud Security Essentials | GCLD**
License to learn cloud security.

Security Management

MGT 520 — **Leading Cloud Security Design and Implementation**
Chart your course to cloud security.

Core

SEC 510 — **Public Cloud Security: AWS, Azure, and GCP | GPCS**
Multiple clouds require multiple solutions.

SEC 540 — **Cloud Security and DevSecOps Automation | GCSA**
The cloud moves fast. Automate to keep up.

SEC 541 — **Cloud Security Attacker Techniques, Monitoring & Threat Detection | GCTD**
Attackers can run but not hide. Our radar sees all threats.

SEC 549 — **Enterprise Cloud Security Architecture**
Design it right from the start.

Specialization

SEC 522 — **Application Security: Securing Web Apps, APIs, and Microservices | GWEB**
Not a matter of "if" but "when." Be prepared for a web attack. We'll teach you how.

SEC 588 — **Cloud Penetration Testing | GCPN**
Aim your arrows to the sky and penetrate the cloud.

FOR 509 — **Enterprise Cloud Forensics and Incident Response | GCFR**
Find the storm in the cloud.

sans.org/cloud-security @SANSCloudSec linkedin.com/showcase/sanscloudsec

Agenda

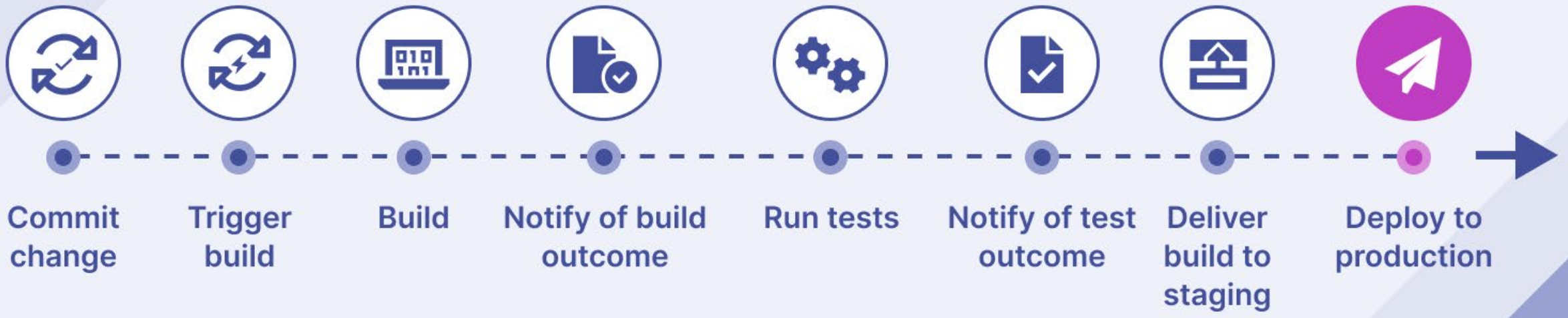
- AWS EC2 Concepts: Volumes, Snapshots & Images
- CI/CD, Secure DevOps, and the Cloud
- Hardened Images
- The SIFT workstation (in the Cloud?)
- Early EC2 Forensic Automation Proof of Concept
- Differential Filesystem Analysis
- XFS File System
- DEMO
- Automated Forensics Orchestration

AWS EC2 Concepts

- **EC2 –** "Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud." ***(Virtual Machine)***
- **EBS –** "Amazon Elastic Block Store (Amazon EBS) is an easy-to-use, scalable, high-performance block-storage service" ***(Virtual Hard Drive)***
- **AMI –** "An Amazon Machine Image (AMI) is a supported and maintained image provided by AWS that provides the information required to launch an instance. You must specify an AMI when you launch an instance. You can launch multiple instances from a single AMI when you require multiple instances with the same configuration." ***(Virtual Machine Template)***
- **Snapshot** – "Amazon Elastic Block Store (EBS) Snapshots provide a simple and secure data protection solution that is designed to protect your block storage…EBS Snapshots are a point-in-time copy of your data…" Snapshots are incremental backups.

- https://aws.amazon.com/ec2/getting-started/
- https://aws.amazon.com/ebs/
- Are Snapshots of Cloud Virtual Hard Drives Forensically Valid?
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

CI/CD, Secure DevOps & Cloud

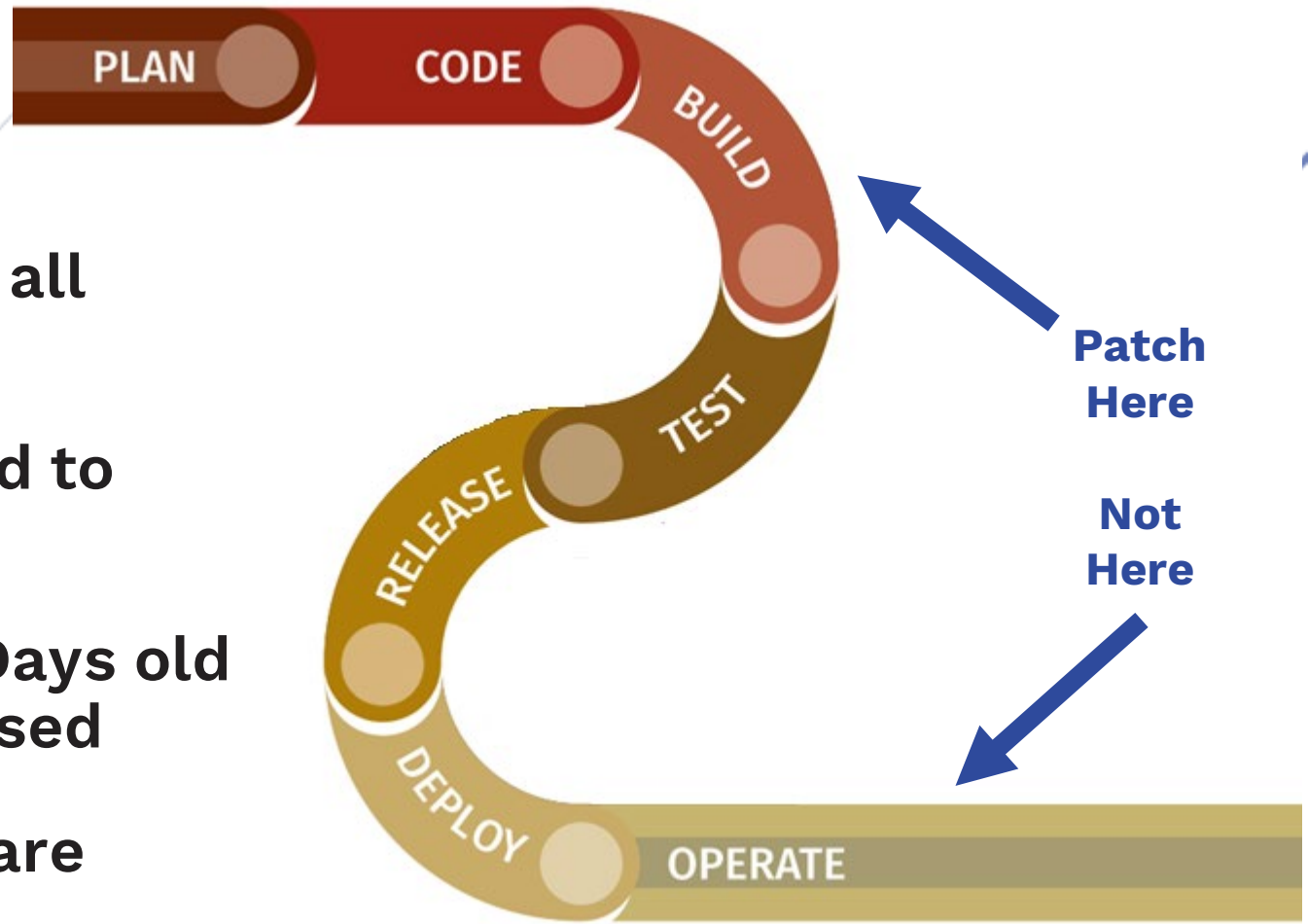


https://katalon.com/resources-center/blog/ci-cd-pipeline

- Lessons Learned from Illumina's SecDevOps Transition - https://youtu.be/El0HZt44wbc
- Can You Really Be More Secure in the Cloud? - https://youtu.be/ahTn5UhEkpQ
- SANS SEC540 - https://www.sans.org/cyber-security-courses/cloud-security-devsecops-automation/

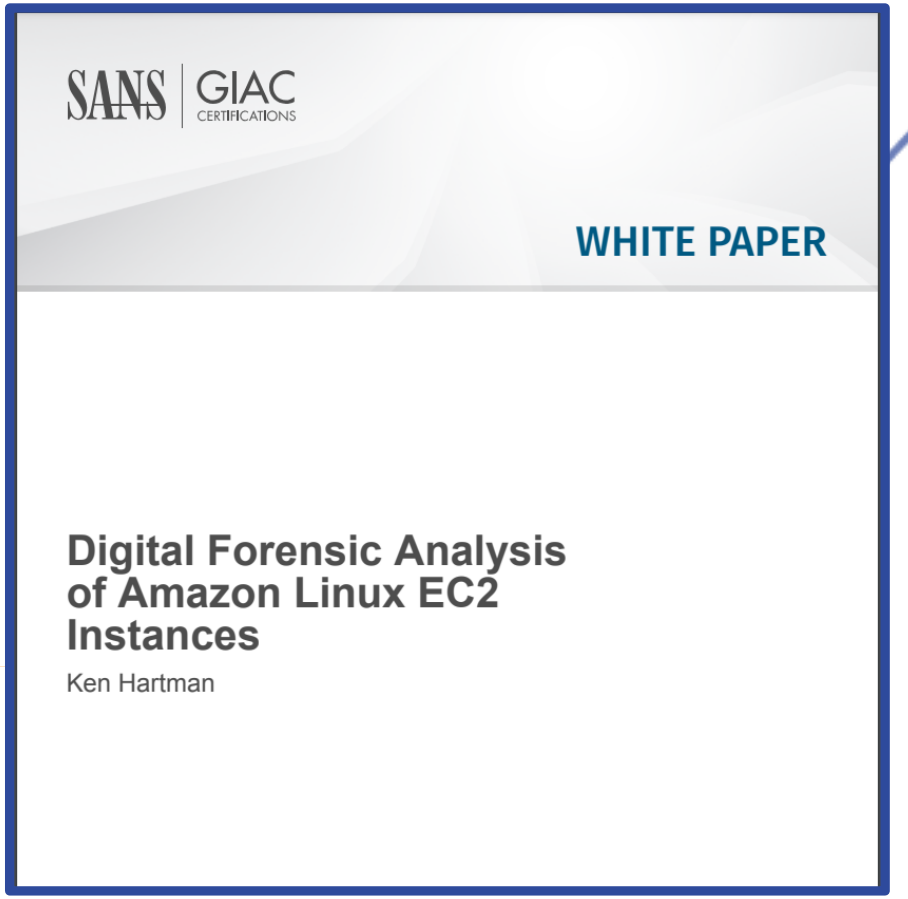
Hardened Images

- Use automation to “bake” a hardened image (AMI) that is fully-patched
- Share these “blessed” AMIs to all accounts in scope
- Limit the AMIs that can be used to launch EC2 Instances
- Un-share the AMIs that are X Days old so that the newest is always used
- Terminate EC2 Instances that are older than the Patching SLO



The SIFT Workstation (in the cloud?)

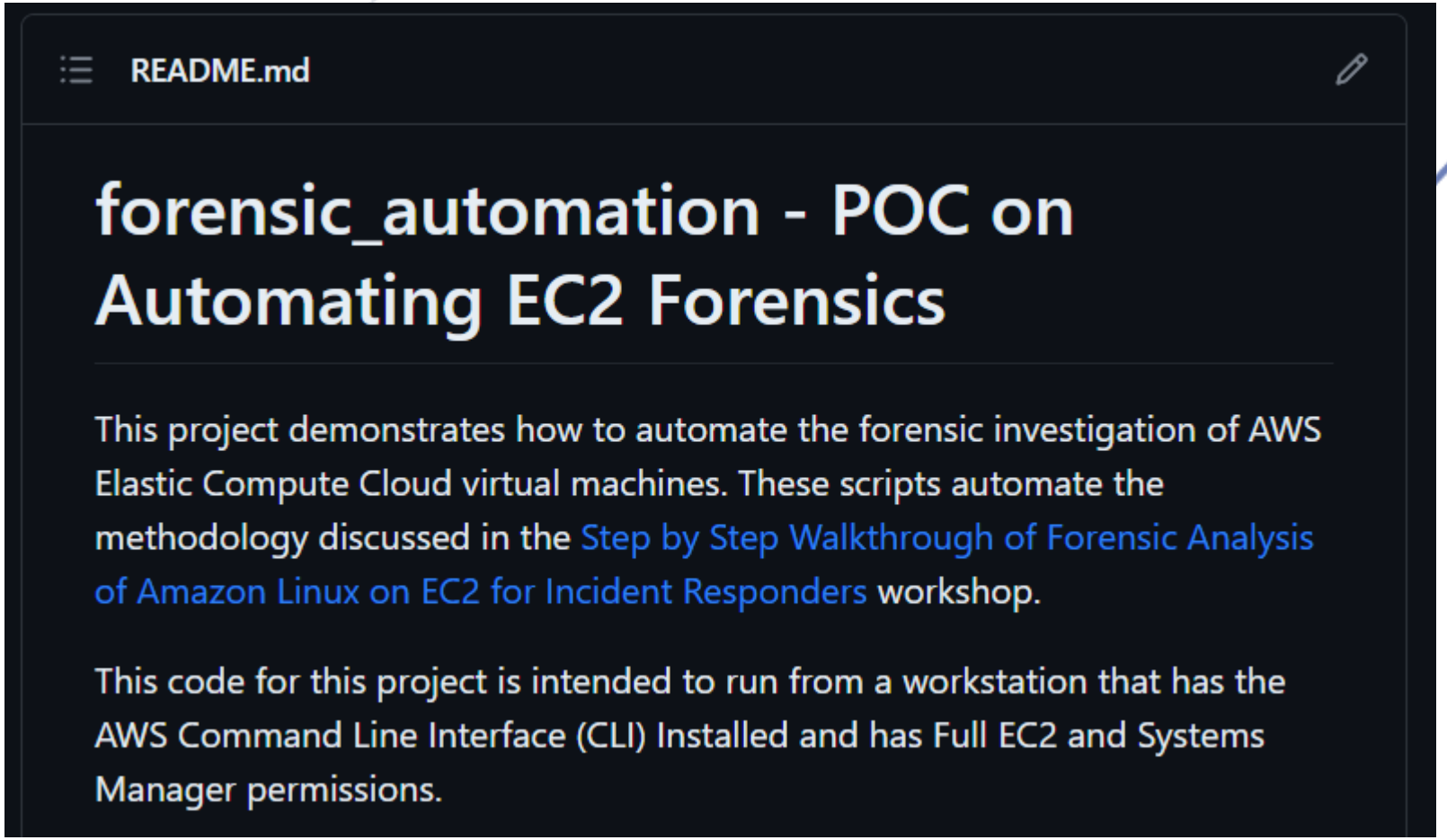
- **Took FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics**
- **Gold Paper: *Digital Forensic Analysis of Amazon Linux EC2 Instances* (Jan 2018)**
- **Bsides Vancouver: *Step by Step Walkthrough of Forensic Analysis of Amazon Linux on EC2 for Incident Responders* (2019)**
  https://forensicate.cloud/ws1/
- **Make a SIFT Workstation AMI**
  https://forensicate.cloud/aws/sift-ami



https://www.sans.org/white-papers/38235/

Early EC2 Forensic Automation PoC

- Used a SIFT EC2 VM
- SIFT VM had SSM agent installed
- Processed EBS Volumes according to a SQS Queue
- Sent Artifacts to a S3 bucket


README.md

forensic_automation - POC on Automating EC2 Forensics

This project demonstrates how to automate the forensic investigation of AWS Elastic Compute Cloud virtual machines. These scripts automate the methodology discussed in the Step by Step Walkthrough of Forensic Analysis of Amazon Linux on EC2 for Incident Responders workshop.

This code for this project is intended to run from a workstation that has the AWS Command Line Interface (CLI) Installed and has Full EC2 and Systems Manager permissions.

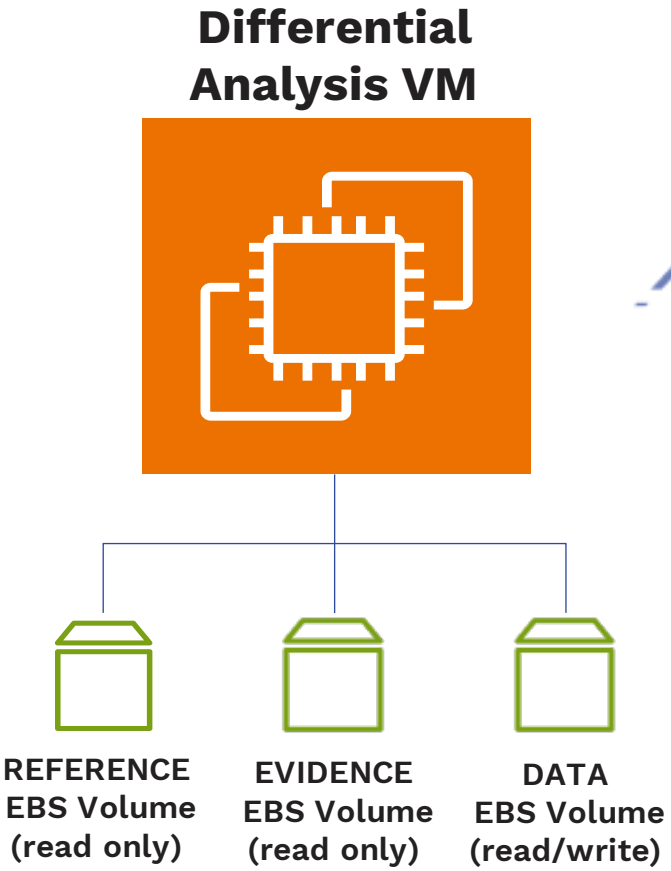
Initial Commit: Aug 19, 2019

https://github.com/Resistor52/forensic_automation

Differential Filesystem Analysis

1. Use a Snapshot prior to compromise to create the “REFERENCE” EBS volume.

   >> OR: Make a snapshot of another VM just launched from the same AMI.
2. Use snapshot after compromise to make “EVIDENCE” volume.
3. Make a new “DATA” volume.
4. Launch a “DFIR_host” and attach the RFERENCE & EVIDENCE volumes as read only. Attach the DATA volume as read-write.
5. Mount all three volumes
6. Generate Hash Databases and Determine the Files that have been added, deleted, and changed.



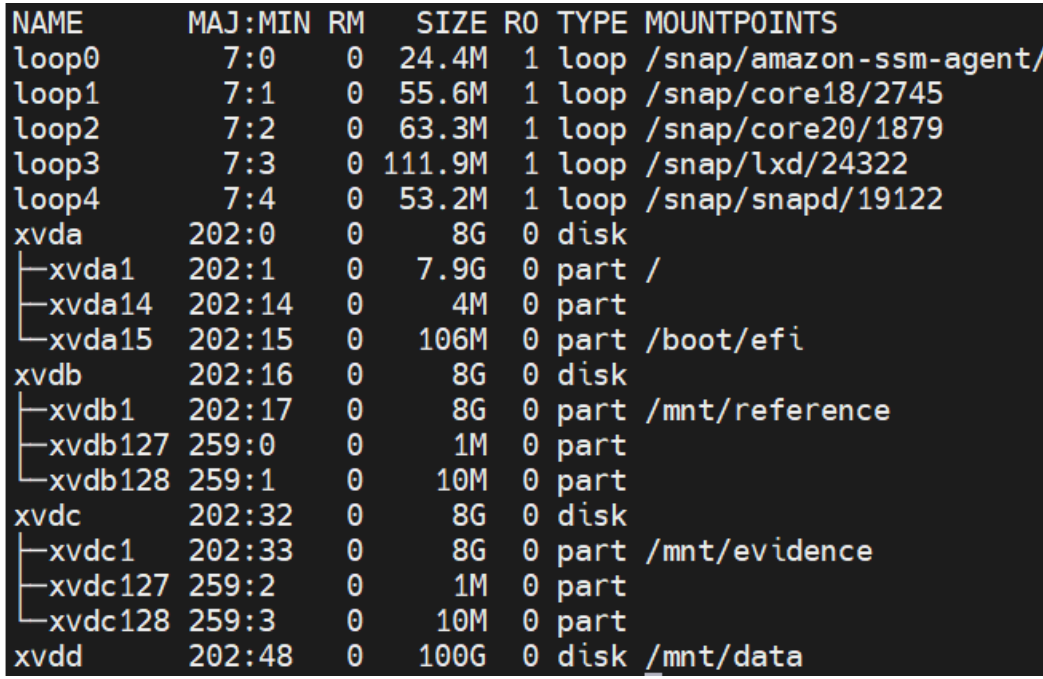
XFS File System

- XFS is a high-performance, journaling Linux file system that supports large files and file systems.
- XFS supports a maximum file system size of 500 TB and a maximum file size of 16 TB.
- It's the default file system for RedHat Linux 7 and is supported by most Linux distributions.
- Amazon Linux 2 uses XFS whereas Amazon Linux used ext4. Amazon Linux 2023 continues to use XFS
- Sleuthkit does not support XFS ☹ (yet?)

➢ **https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-using-volumes.html**

Mounting the Volumes

```
# Format the new `DATA` volume
mkfs -t xfs /dev/xvdd
# Make mount points for the three partitions
mkdir /mnt/reference
mkdir /mnt/evidence
mkdir /mnt/data
# Change the UUID of the `REFERENCE` partition
xfs_admin -U $(uuidgen) /dev/xvdb1
# Mount the `REFERENCE` and `EVIDENCE` as read-only and mount the `DATA` as read-write.
mount -o ro -t xfs /dev/xvdb1 /mnt/reference
mount -o ro -t xfs /dev/xvdc1 /mnt/evidence
mount /dev/xvdd /mnt/data
```



```
NAME      MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
loop0       7:0    0  24.4M  1 loop /snap/amazon-ssm-agent/
loop1       7:1    0  55.6M  1 loop /snap/core18/2745
loop2       7:2    0  63.3M  1 loop /snap/core20/1879
loop3       7:3    0 111.9M  1 loop /snap/lxd/24322
loop4       7:4    0  53.2M  1 loop /snap/snapd/19122
xvda      202:0    0     8G  0 disk
├─xvda1   202:1    0   7.9G  0 part /
├─xvda14  202:14   0     4M  0 part
└─xvda15  202:15   0   106M  0 part /boot/efi
xvdb      202:16   0     8G  0 disk
├─xvdb1   202:17   0     8G  0 part /mnt/reference
├─xvdb127 259:0    0     1M  0 part
└─xvdb128 259:1    0    10M  0 part
xvdc      202:32   0     8G  0 disk
├─xvdc1   202:33   0     8G  0 part /mnt/evidence
├─xvdc127 259:2    0     1M  0 part
└─xvdc128 259:3    0    10M  0 part
xvdd      202:48   0   100G  0 disk /mnt/data
```

Hash Databases

```
# Create REFERENCE Hash Set
find /mnt/reference -type f -print0 | xargs -0 md5sum | tee reference_files.md5

# Create EVIDENCE Hash Set
find /mnt/evidence -type f -print0 | xargs -0 md5sum | tee evidence_files.md5

# Create the Hash Database
hfind -i md5sum reference_files.md5
hfind -i md5sum evidence_files.md5
```

hfind looks up hash values in a database using a binary search algorithm. This allows one to easily create a hash database and identify if a file is known or not. It works with the NIST National Software Reference Library (NSRL) and the output of 'md5sum'.

- https://www.sleuthkit.org/informer/sleuthkit-informer-6.html#hashes
- https://www.sleuthkit.org/informer/sleuthkit-informer-7.html

Quick Win Analysis

MD5 Exists in		Conclusion	New Hash Set Filename
REFERENCE Hash Set	EVIDENCE Hash Set		
YES	NO	File was Deleted or Changed	missing+changed_files+hashes_from_evidence.md5
NO	YES	File is New or Changed	new+changed_files+hashes_in_evidence.md5

Filename Exists in		Conclusion
missing+changed_files+hashes_from_evidence.md5	new+changed_files+hashes_in_evidence.md5	
YES	YES	File Has Changed
YES	NO	File was Deleted
NO	YES	File is New

```
wc -l evidence_files.md5 \
reference_files.md5
  42157 evidence_files.md5
  39619 reference_files.md5
  81776 total
```

```
wc -l CHANGED_FILES.txt NEW_FILES.txt DELETED_FILES.txt
   32 CHANGED_FILES.txt
 2529 NEW_FILES.txt
    1 DELETED_FILES.txt
 2562 total
```

2561 / 42157 = .06 ← Reduced to 6% of Files!

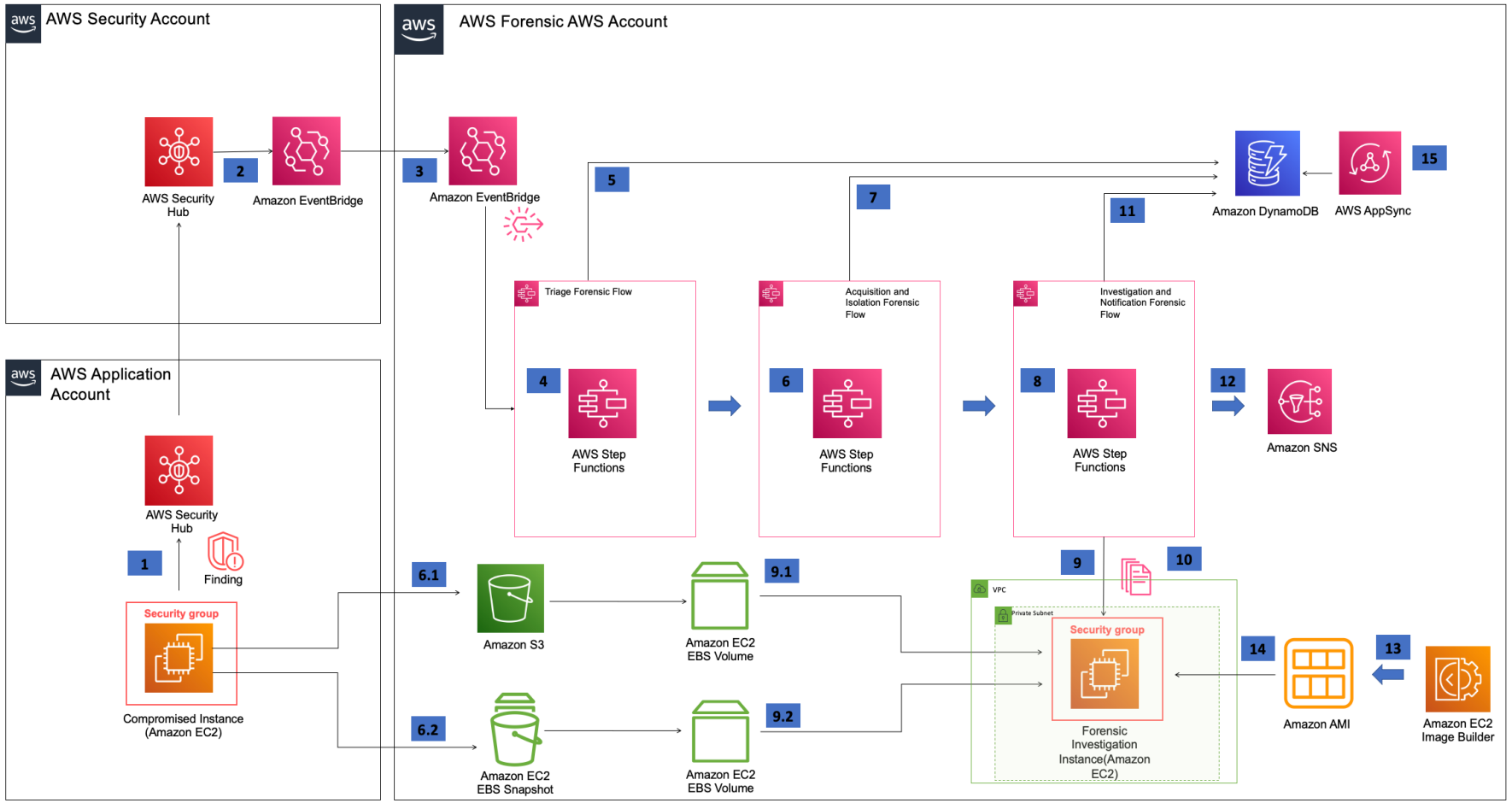
DEMO

https://github.com/Resistor52/DifferentialAnalysis

https://youtu.be/onC7x-BftSk

Automated Forensics Orchestrator for EC2

1) GuardDuty Alert sent to Security Hub
2&3) EventBridge invokes workflows using instance ID
4) Step Functions triage the request and initiates acquisition
5) Triaging details are stored in DynamoDB
6) Memory & Disk forensics flows are started in parallel
7) Acquisition details are stored in DynamoDB
8) After acquisition, notice triggers investigation Step Function
9) Forensic instance started from forensic AMI, loads memory capture and creates an EBS volume from snapshot
10) AWS Systems manager documents run the forensic investigation
11) Output is stored in DynamoDB
12) Results are shared via SNS
13&14) EC2 Image Builder builds the Forensic AMI used by Step Functions
15) Forensic timeline can be queried by AWS AppSync



- https://www.sans.org/white-papers/sans-2022-devsecops-survey-creating-culture-improve-organization-security/
- https://aws.amazon.com/blogs/security/how-to-automate-forensic-disk-collection-in-aws/ (2021)
- https://aws.amazon.com/solutions/implementations/automated-forensics-orchestrator-for-amazon-ec2/

Thank You

LUCID TRUTH
TECHNOLOGIES