CLOUD FORENSICS

Dr. Digambar Pawar
Associate Professor
University of Hyderabad
dpr@uohyd.ac.in
+91 7601010528

Today's agenda

- Recent trends
- Cyber Crime
- Digital Forensics
- Cloud Computing
- Cloud Crime
- **Cloud Forensics**
- Discussion

CYBER CRIME


Ottawa Citizen
Syndicom.com
THE NAZIS ARE COMING, THE NAZIS ARE COMING!!
TERROR IN THE 20TH CENTURY...
THE E-MAIL SERVER IS DOWN!!
TERROR IN THE 21ST CENTURY...

Hacking

Student held for hacking into GTU website

Student changed data to get admission in MCA

PTI | June 5, 2010

A student has been arrested for allegedly hacking into the website of Gujarat Technological University (GTU) and changing its data to get admission in a post-graduation course, police said today.

Yogesh Patel, who hails from Jamnagar and has completed his Bachelor of Computer Application course (BCA), was arrested by Ahmedabad crime branch here last night, they said.

Patel had allegedly hacked into the GTU website for getting admission in Master of Computer Application (MCA).

Primary investigations revealed that Patel got an internet connection allegedly by submitting fake documents and was helped by four of his friends.

Patel has been taken to Ahmedabad for further questioning while efforts are on to nab his associates, police said.

The arrest was made following a complaint lodged by GTU in Ahmedabad.

Cyber Crime

"**Unlawful act wherein the computer is either a tool or a target or both**".

Two aspects:

- Computer as a tool to commit crime
  - Child porn, threatening email, assuming someone's identity, sexual harassment, defamation, spam, phishing
- Computer itself becomes target of crime
  - Viruses, worms, software piracy, hacking

Why Digital Evidence ?

We need a means for investigation & analysis of the crimes – to bring the culprits to conviction.

All solution lies in Digital Evidence

DIGITAL FORENSIC

Cyber Forensics

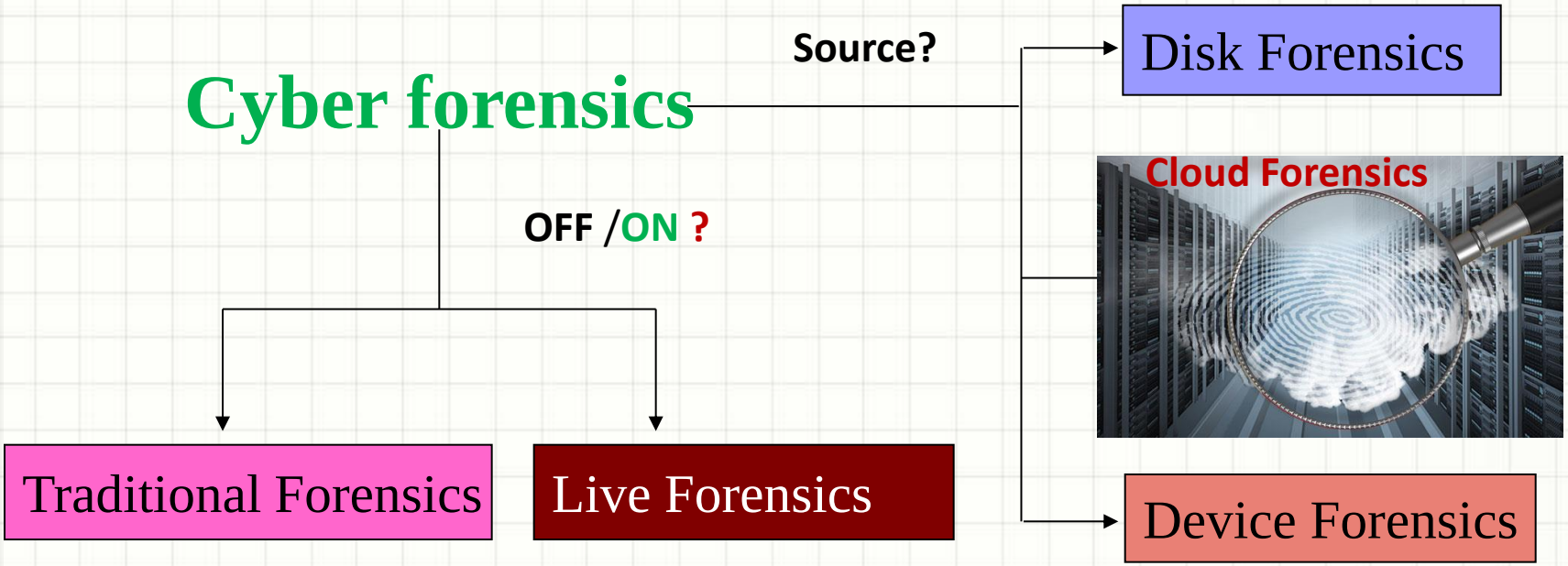
Cyber Forensics deals with forensic analysis of cyber crimes with the objectives of

- Identifying digital evidence
- Acquiring digital evidence
- Authenticating digital evidence
- Reporting digital evidence

Role of Cyber Forensics

A means of systematically gathering digital evidence, analyzing it to make credible evidence, authentically presenting it to the court of law.

Cyber Forensics :: Classification



CLOUD COMPUTING

What is Cloud Computing?

- *Cloud computing is a model for enabling **ubiquitous**, convenient, **on-demand** network access to a **shared pool** of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be **rapidly provisioned** and released with minimal management effort or service provider interaction.*

  (by NIST)

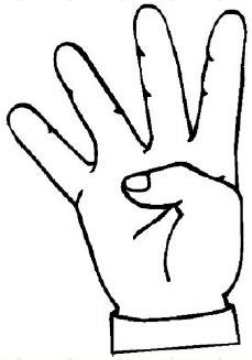
- "an Internet based computing paradigm that delivers on-demand software and hardware computing capability as a 'service' through virtualization where the end user is completely abstracted from the computing resources"

3-4-5 Rule ???

3 : Services

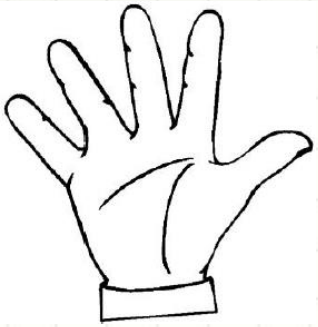
- IaaS (Infrastructure as a Service)
- PaaS (Platform as a Service)
- SaaS (Software as a Service)

4 : Deployment Models



- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud

5 : Characteristics



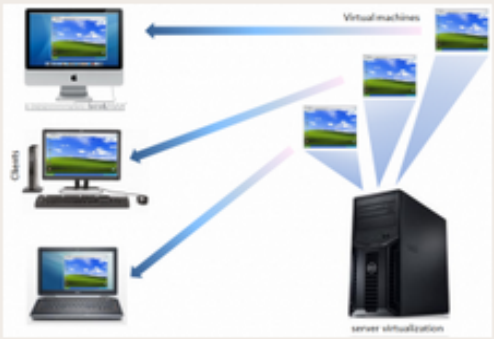
- On-demand self-service
- Broad network access
- Resource pooling
- Rapid Elasticity
- Metered or measured service

TAGS

Chrisis, Cybercrime, malware, Symantec, Virtual Environment, virtual machine., Virtualization

Malware is threatening virtual machines

by Pierluigi Paganini on August 18th, 2014



Malware is the primary threats for enterprise virtual machines according to report a recent report issued by Symantec

Symantec recently issued the "**Threats to virtual environments**" report to analyze principal menace for virtualized environments. The report is very actually and considers the rapid diffusion of the virtualization paradigm within enterprises.

According to Forrester Research more than 70 percent of organizations are planning to use server virtualization by the end of 2015, but we cannot ignore that malware author are targeting also these environments that anyway manage real users' data.

> *"However, virtual machines and their hosting servers are not immune to attack. Introducing virtualization technology to a business creates new attack vectors that need to be addressed, such as monitoring the virtual networks between virtual machines. We have seen malware specifically designed to compromise virtual machines and have observed attackers directly targeting hosting servers." states the report.*

CLOUD CRIME

Cyber Bulling

- **“Willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices” OR**
- **“The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature”**

❖ Children may be reluctant to admit to being the victims of cyber bullying

❖ Examples:

- ✓ Someone repeatedly makes fun of another person online
- ✓ Repeatedly picks on another person through e-mail or text message
- ✓ When someone posts something online about another person that they don’t like

Cyber Bulling (contd..)

Woman stands up to cyber blackmailer with a brave Facebook post

US-based Indian woman takes on cyber bully with a gutsy public post; receives support in her endeavour.

Subject: LONG TIME NO SEEN TARUNA ASWANI.Does that look familiar and more I got.
To: "taruna.aswani@gmail.com" <taruna.aswani@gmail.com>
Cc:

Hello there, it has been long since I saw you in Mumbai and I found out you went out of the country. I used my computer skills to trace you through your friends and social media and I found you. I have nude pictures and video that belongs to you that nobody else knows it exists beside the person you sent to and it looks good like I thought. All I am saying is if you want me to keep quiet on this and don't let the world(social media, Work place,family and friends) know then you have to excite me. Let me mustabate like you did in that video. I will give you 24 hrs to respond and 48hrs to send me and after that you might be famous if you act smart.
So you know I have plan B because I expect you to smart as per your past history and try go to police go ahead ...ooops I am 1000's of miles away but still I wanted to give you a chance. You can try your best and do that. This is not a treat but if I ask you nicely you won't do it, we might as well be both happy that this remains the way it is or be sad and live with it. You know what I have. You in the bathroom with your blue Sandles. I have access to your all your friends/social media.and family and co-workers(NMS healthcare and heritage inc)contacts that you have and I think some will be happy and some embarrassed to see it but if you have a thick skin then it shouldn't worry you.All I want is pics of your pussy opened with your fingers and a small clip, you don't have to include face I will know if it's you or not and I like it shaved I

22 October 2016

Dear Friends and Family,

I am posting this and emailing you individually as my online identity has been compromised.

I have in the last 24 hours received 2 emails from someone that claims to know me that has hacked into my google cloud back up.

He has been threatening to release some private pictures and videos of me to my friends family and colleagues.

As embarrassing as the videos may be (they were sent to my boyfriend at the time) I choose to stand up to this man. Instead of cowering down to his requests. I do this so that other women may take a lesson to stand up to bullies and low life's like this and may get the confidence to stand up as well in case he is known to us and is targeting all of us, but we're either too scared, ashamed or clueless in how to manage or handle such situations.

I implore you to share this post with as many people as you know to get the word out. Perhaps someone may be able to locate this person through his digital footprint.

Please help me in nabbing this sick pervert.

If you find any information on this, please inbox me so I can report it to the Detective working on the case or you may contact him directly on +1 301 699 2601 and mention my name for reference.

Grateful for your help in this, I have enclosed along with this screen shots of his emails- I have deleted the photos/videos he had attached.

Thanks for all your help and support in this.

Yours truly,

Taruna

Well known Cloud Crimes

- Running of “Zeus botnet controller” on an EC2 instance on Amazon’s cloud infrastructure was reported in 2009
- iCloud hack (2014)
- Sony Pictures (2014)
- Home Depot (2015)
- Anthem (2015)

Cloud crime:

“a crime that involves cloud computing in a sense that the cloud can be the object, subject or tool of crimes”

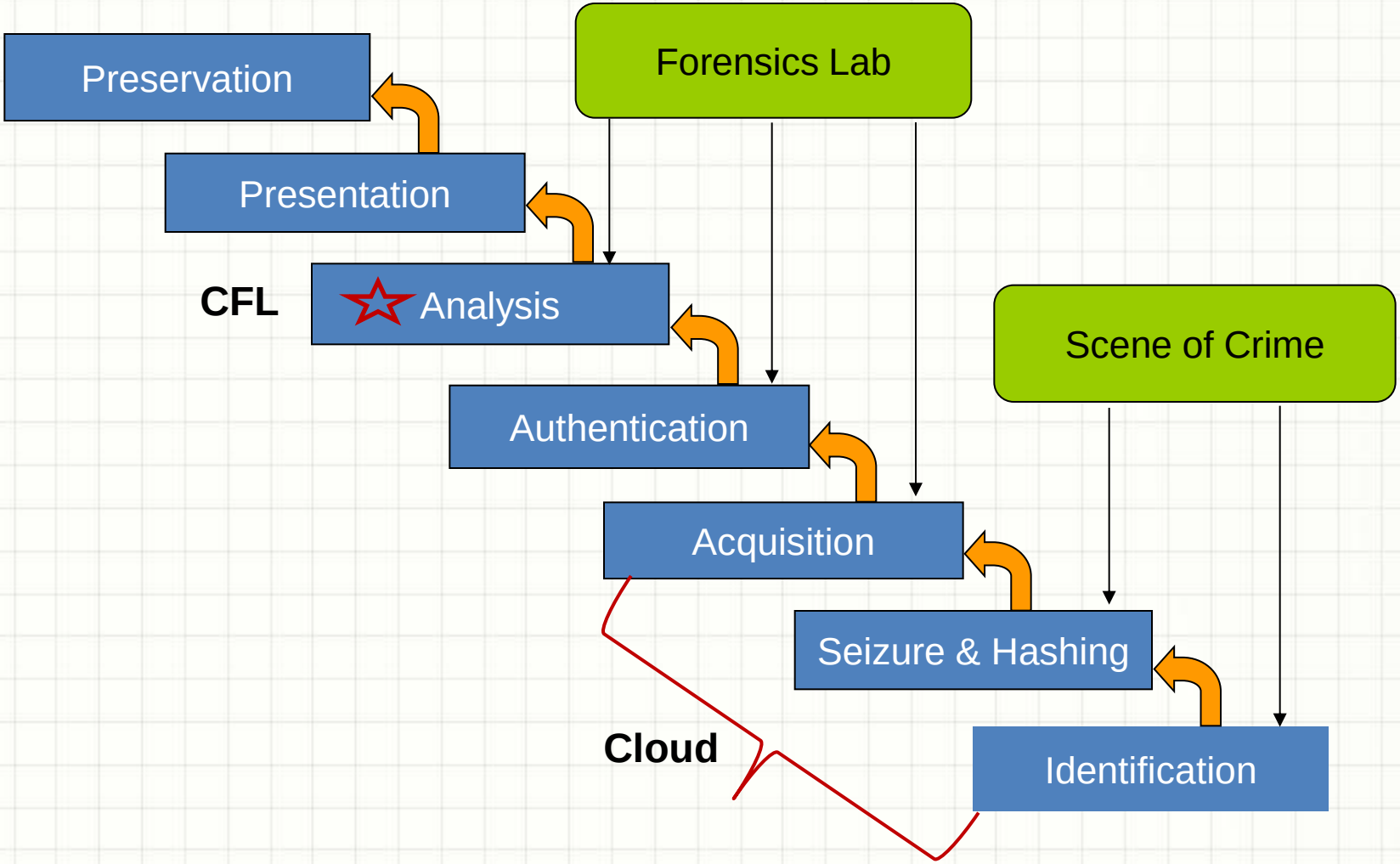
- Object - CSP(cloud service provider) is the target of the crime;
- Subject - cloud is the environment where the crime is committed;
- Tool - cloud can also be the tool used to conduct or plan a crime

Cloud forensics:

- Cloud forensics is a subset of network forensics
- “The application of computer forensic principles and procedures in a cloud computing environment”

- “The process of applying various digital forensic phases in cloud platform depending on the service model and deployment models of cloud”

Cloud Forensics-Steps

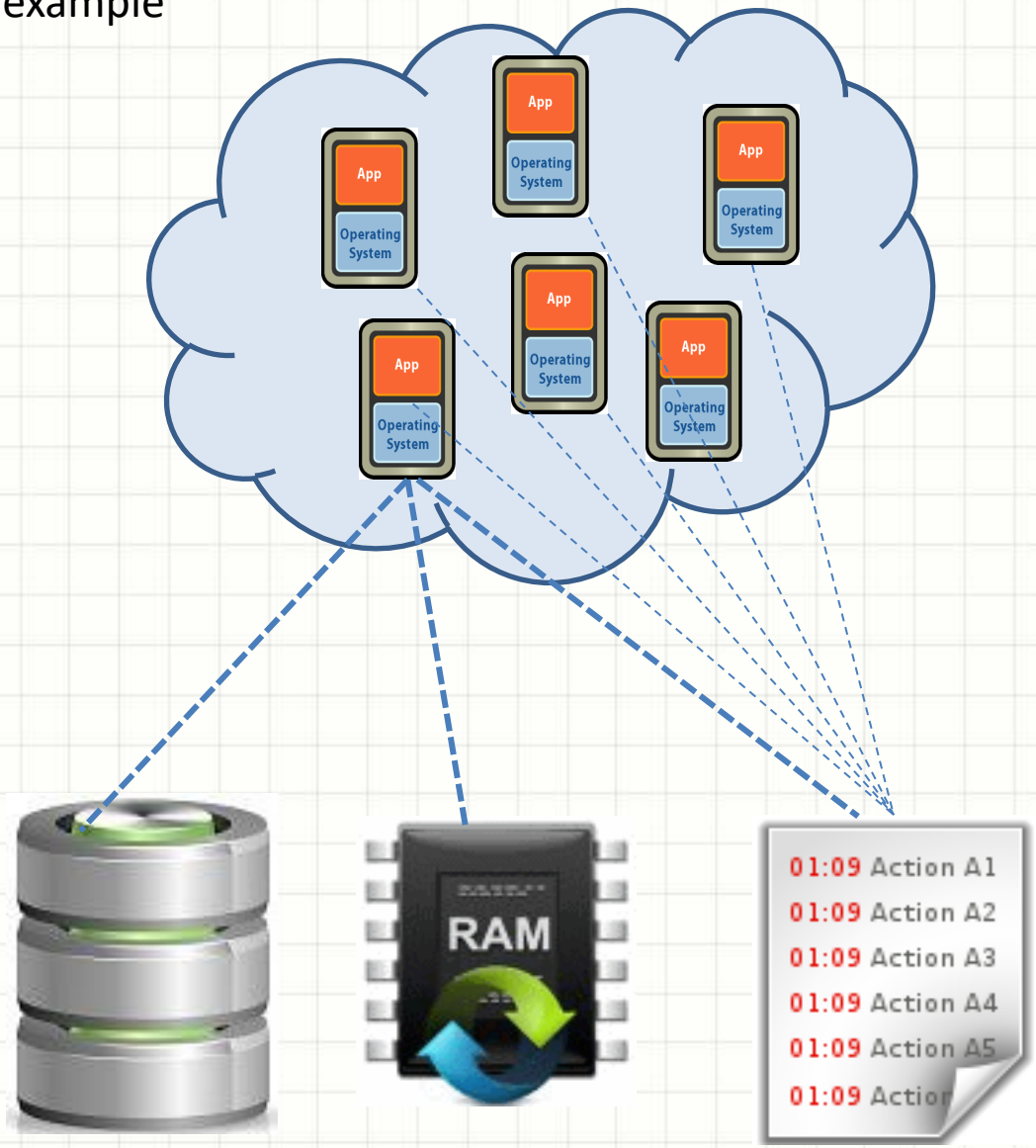


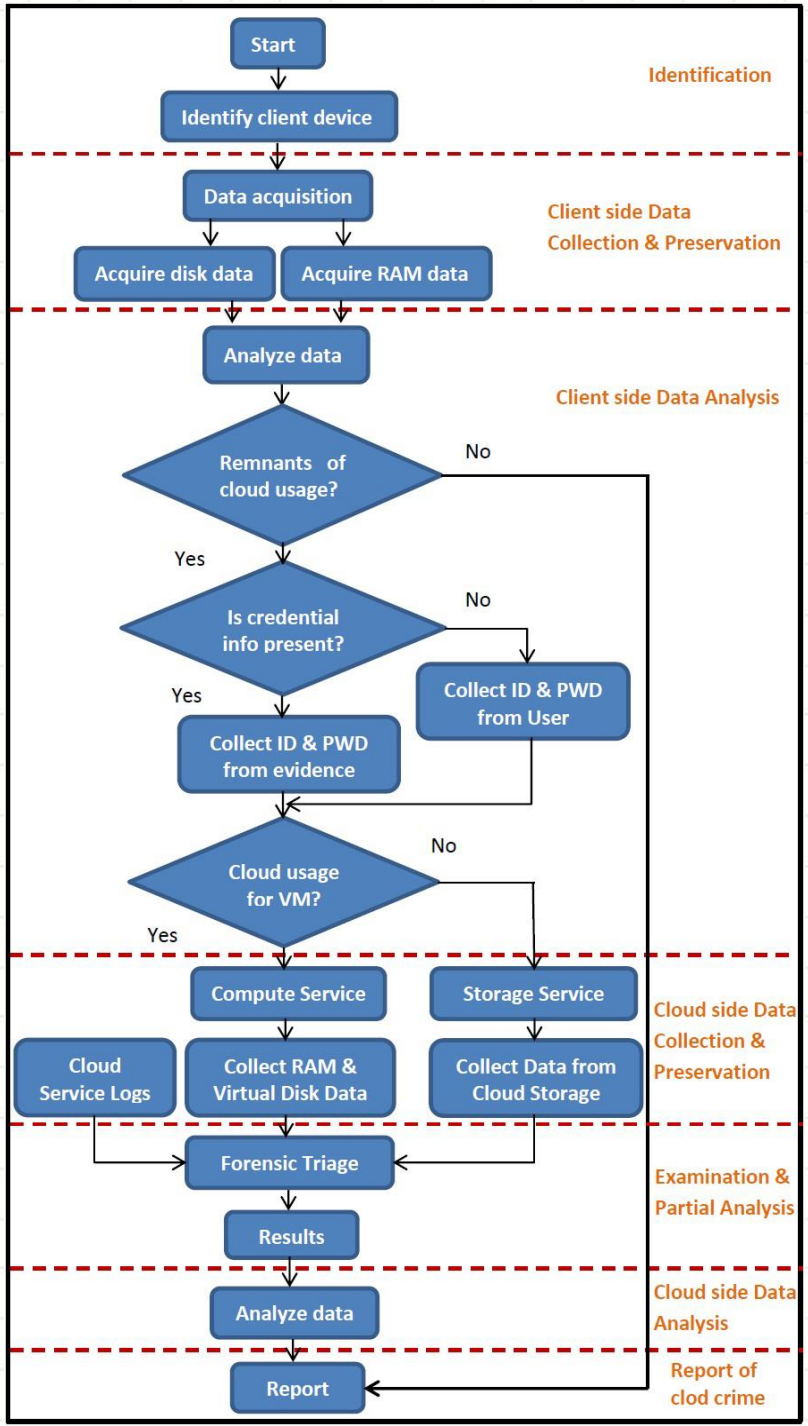
Data center

Where is my data stored?

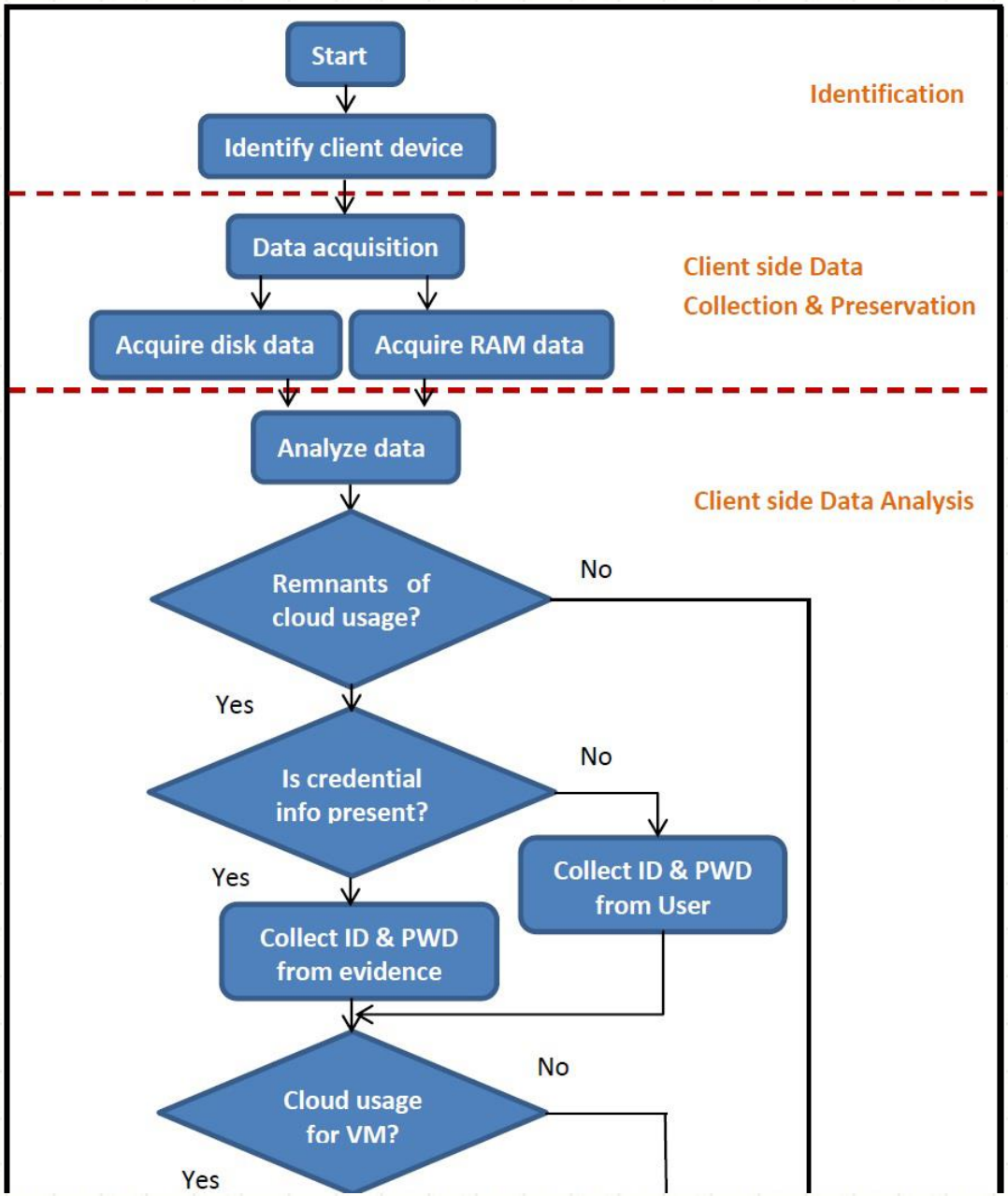
Cloud Data?

Private cloud example

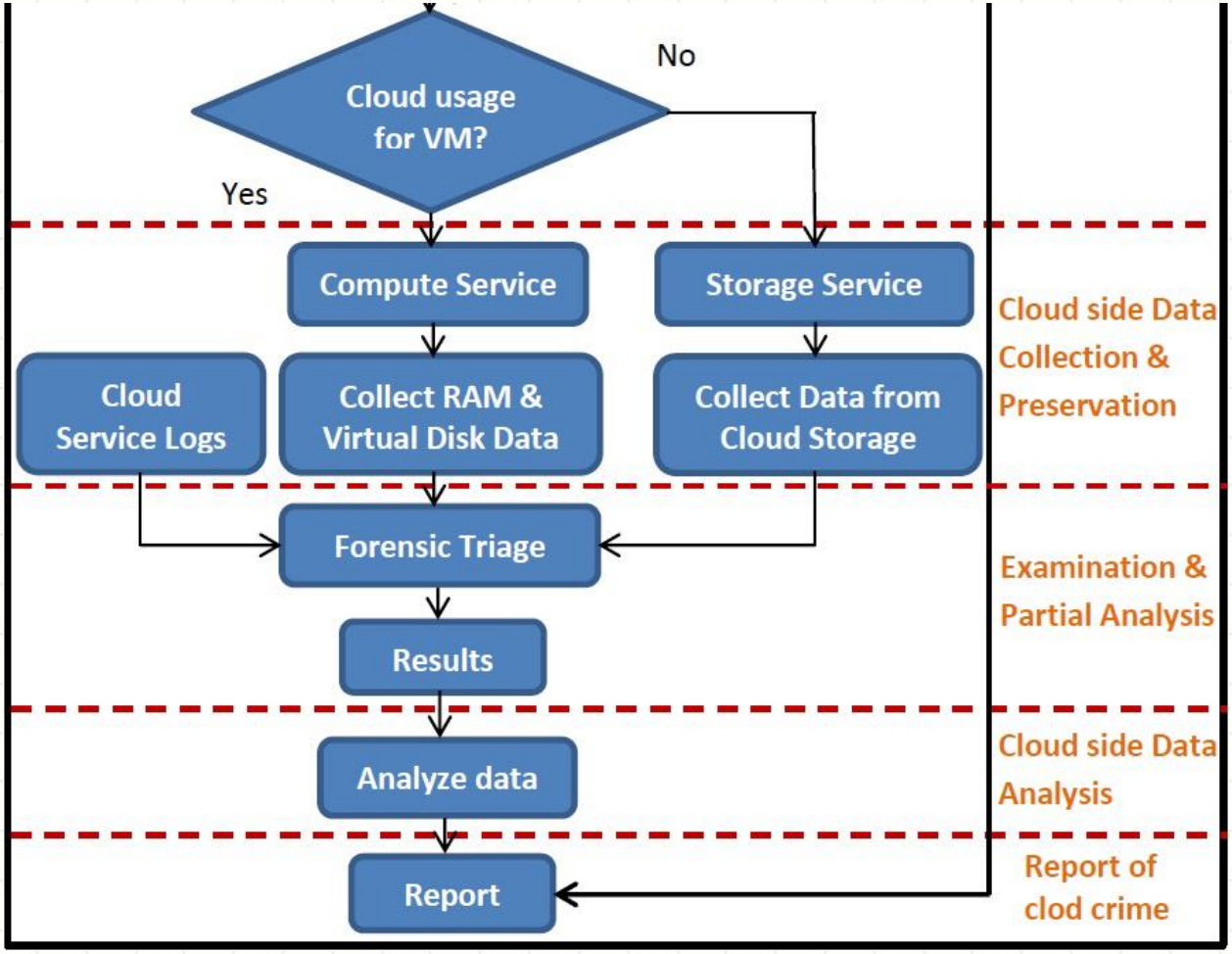




Digital forensic model for the cloud computing systems

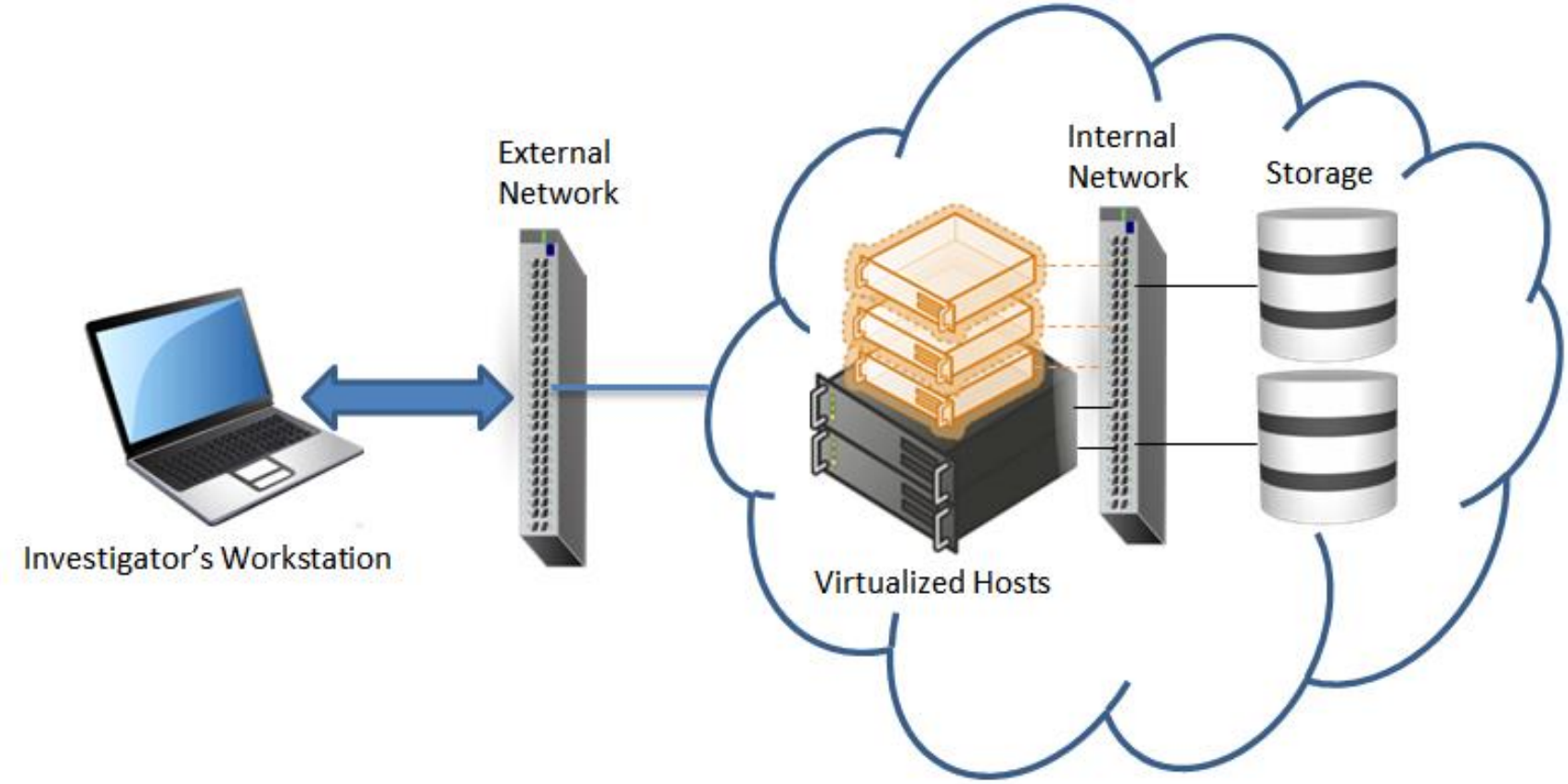


Digital forensic model for the cloud computing systems (1)



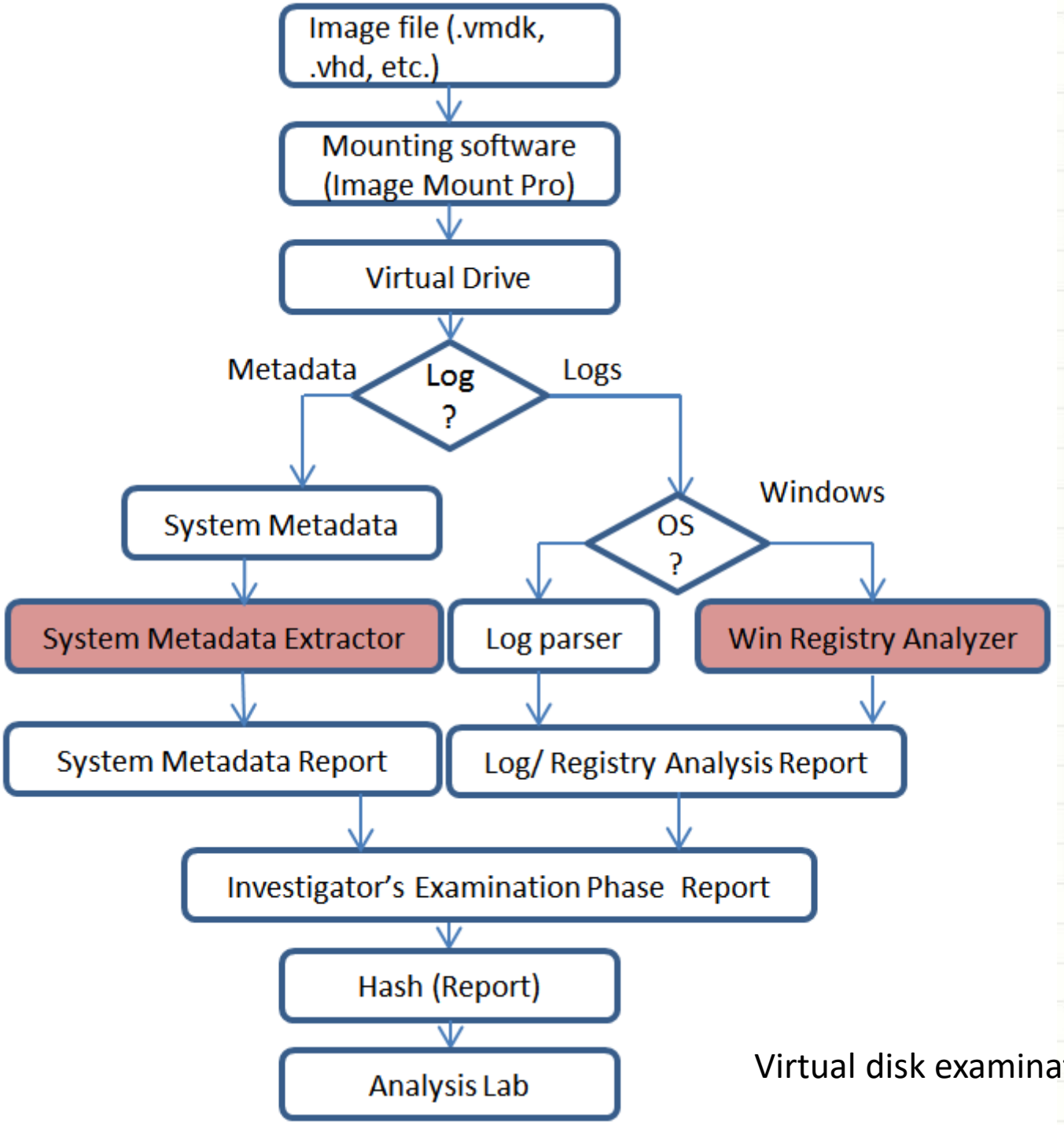
Digital forensic model for the cloud computing systems (2)

Data Acquisition



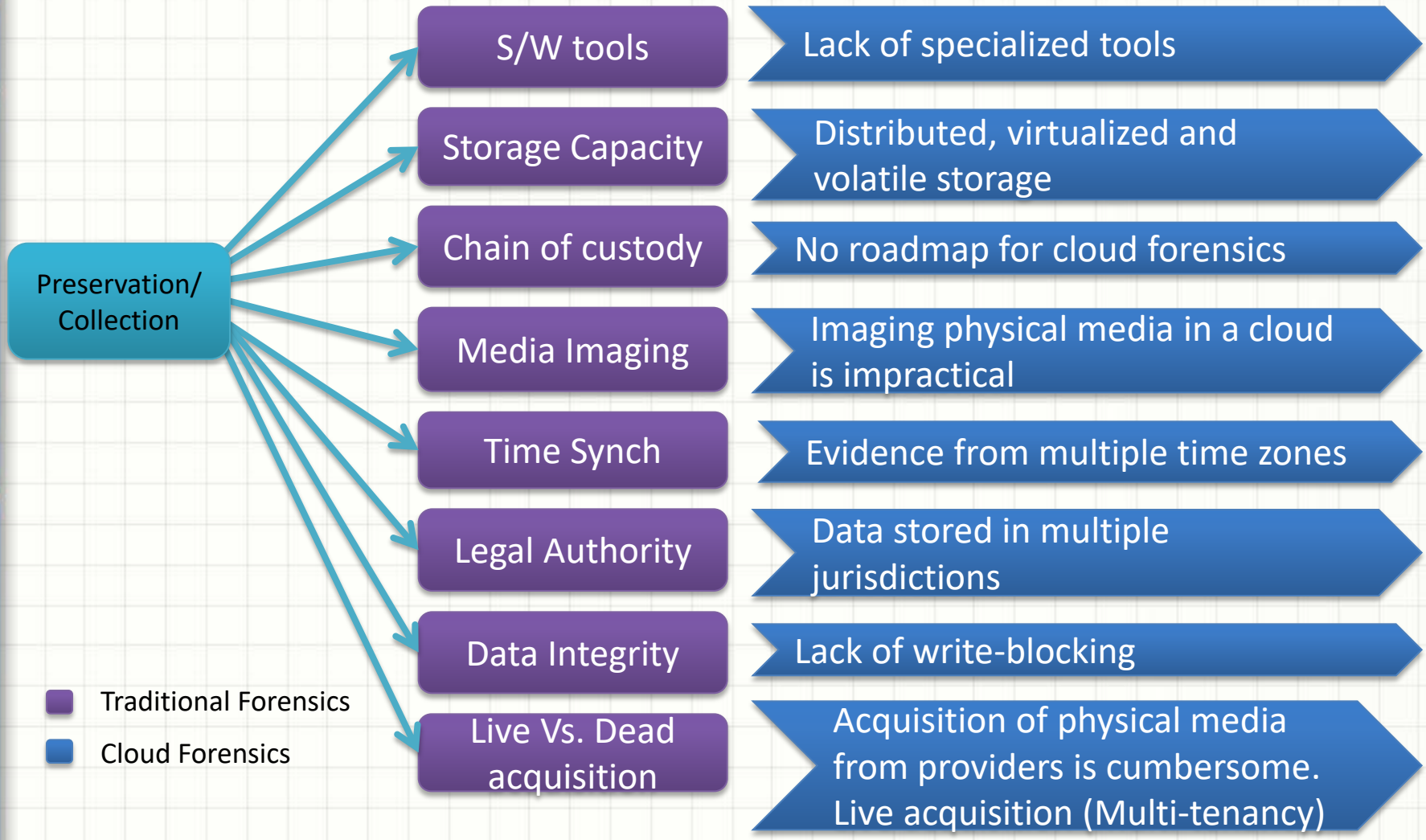
Data Analysis

- **Within the Virtual Machine**
  - ✓ Analysis of virtual hard disk data
  - ✓ Analysis of VM's RAM
- **Outside the Virtual Machine**
  - ❖ Segregation of logs
  - ❖ Acquisition of logs



Virtual disk examination process

A roadmap ahead



Conclusion

- Cloud computing is still an evolving computational platform which lacks the support for crime investigation in terms of the required frameworks/tools
- Need to be Self Reliant. Make In India and Digital India are opportunities for us to emerge with indigenous solutions and products for Digital Forensics (specially for cloud, IoT, Fog, etc.)
- Take major initiatives for educating and making people aware of the dangers and the ways to mitigate them
- Launch programmes and schemes to increase the **number of cyber security experts** in the country
- Establish strong Public-Private links
- "**Monitoring of Critical Infrastructure Systems**"

Discussion

Thank You