Forense em dispositivos de armazenamento baseado em conteúdo (CAS):

Análise da arquitetura e extração de dados

Kátia A R Fuchs

Computação Forense & Perícia Digital
Instituto de Pós-Graduação - IPOG

Como seria chegar até aqui?

Como seria chegar até a casa do Ari?

Organização de dados digitais

Raio-x

Músicas

Processos eletrônicos

CAD

SLA

Contratos

Laudos

Filmes

Tipo de dado que cresce 90% anualmente

Content Addressable Storage (CAS)

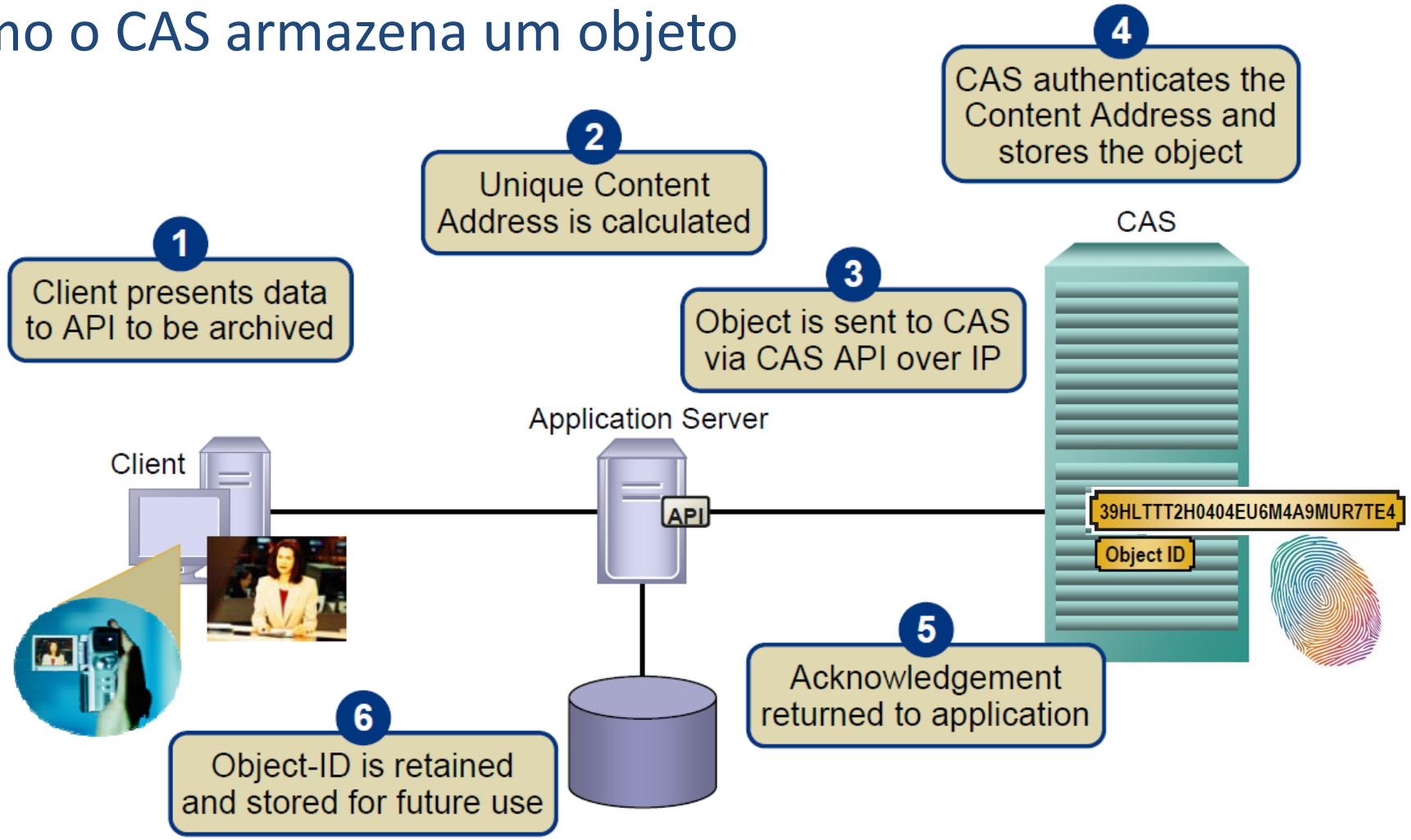
- Se propõem a facilitar o armazenamento e acesso a dados
- Os dados são endereçados e acessados com base em seu conteúdo e não na sua localização física
- *Hashes*

Content Addressable Storage (CAS)

- Soluções
  - proprietárias x *open source*
  - *Hardware* x *software*
  - Cada uma com alguma diferença de implementação

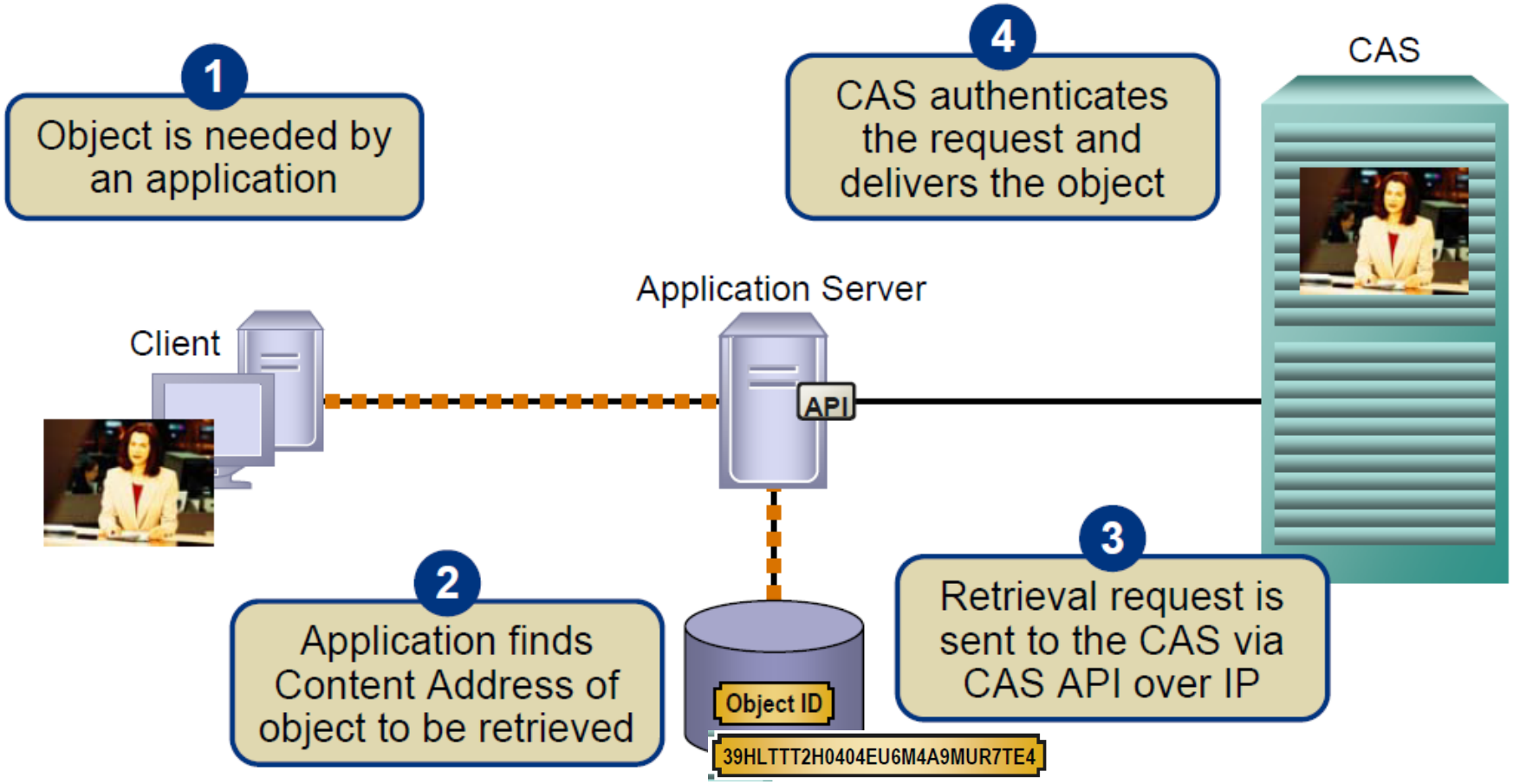
Arquitetura EMC CENTERA (CAS)

Como o CAS armazena um objeto



Arquitetura EMC CENTERA (CAS)

Como o CAS recupera um objeto



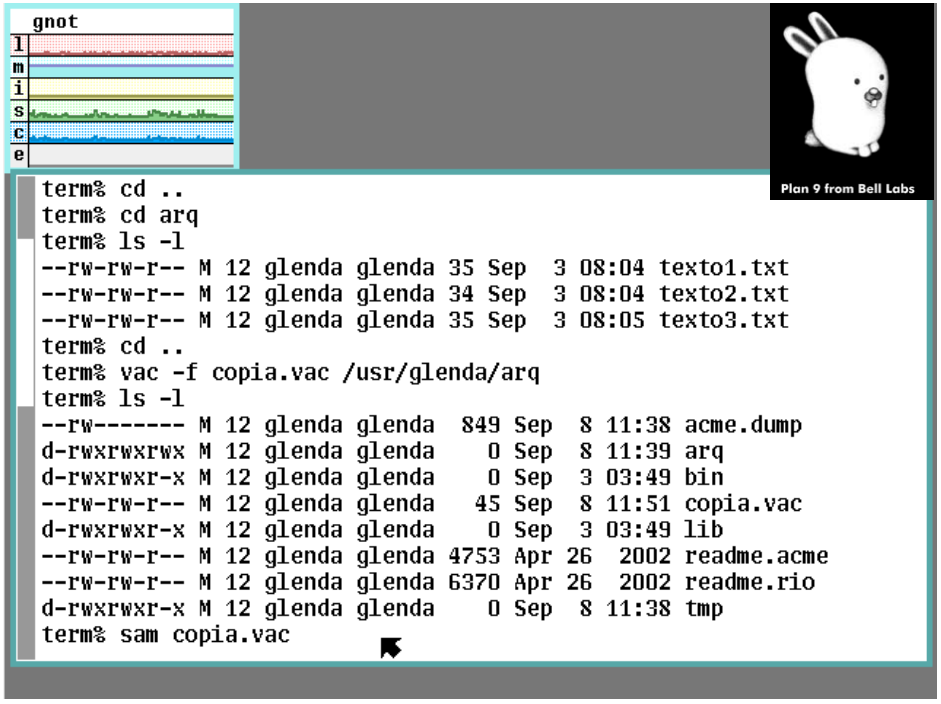
Desafios forenses?

- Soluções proprietárias
  - De difícil acesso em ambiente de produção
  - Diferentes implementações
- Localizar artefatos em várias camadas da arquitetura ou em *hosts* geograficamente distribuídos
- Ferramentas forenses

Extração de dados de um dispositivo CAS

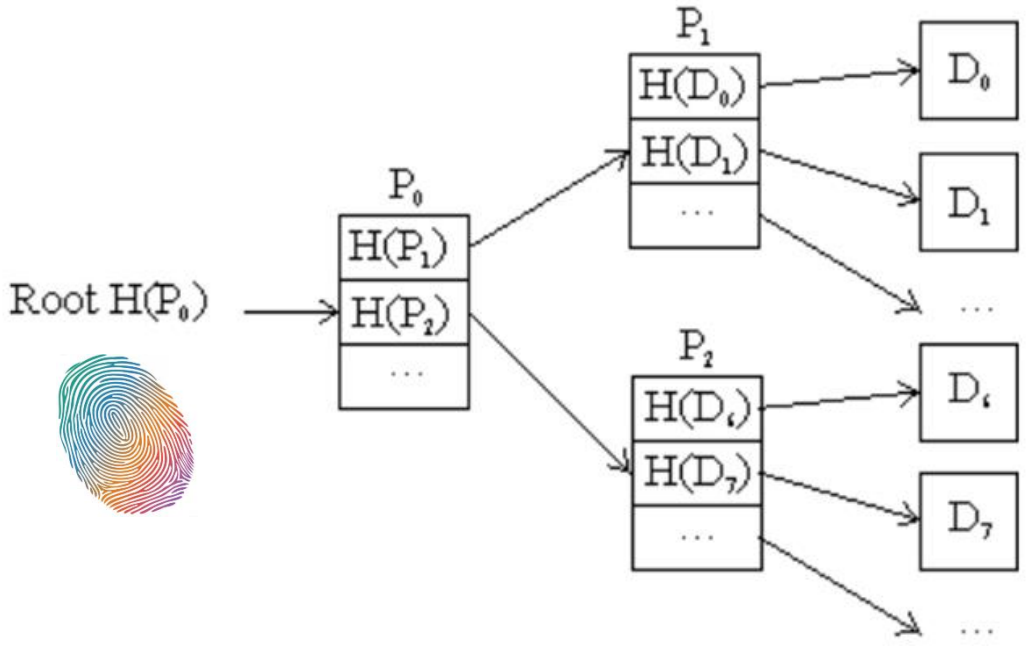
- Implementação: Ambiente em Vm
- Sistema operacional Plan9
    - Fossil+venti

      (sistema de arquivos e servidor de dados)
- Vac e Vacfs

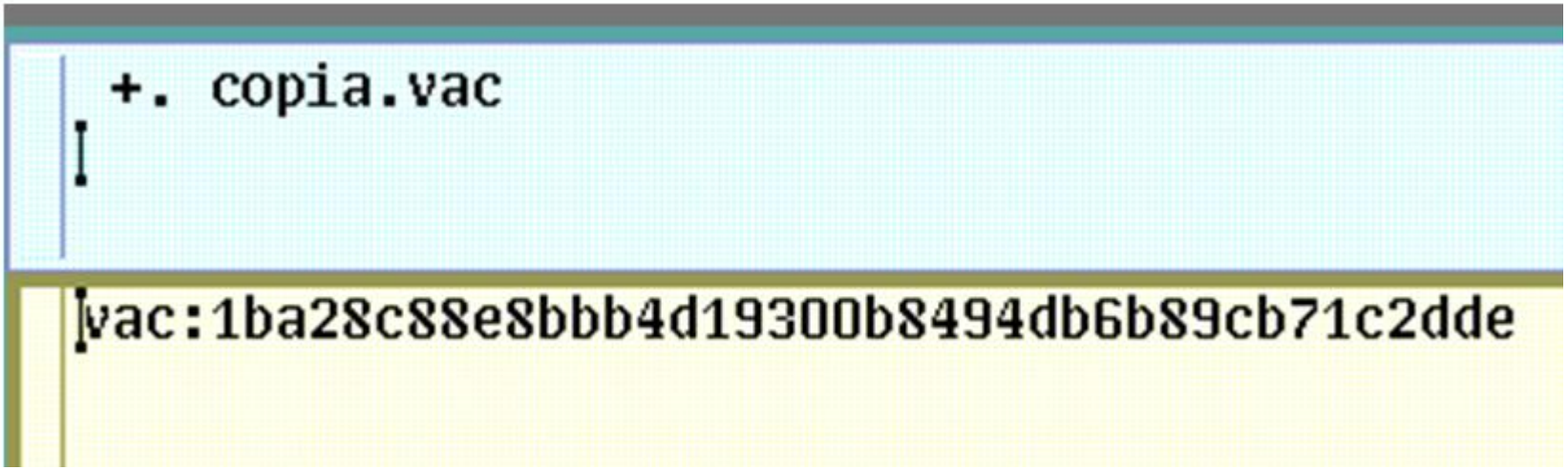


Arquitetura Venti

- Endereçamento de blocos com base seu em contéudo
- A função SHA1 gera um código de 160 bits (20 bytes)



Vac



Conteúdo do arquivo copia.vac

Fonte: Dados produzidos pelo autor (2019)

Vacfs

```
term% vacfs copia.vac
term% cd /n/vac
term% ls -l
d-rwxrwxrwx M 49 glenda glenda 0 Sep  8 11:39 arq
term% cd arq
term% ls -l
--rw-rw-r-- M 49 glenda glenda 35 Sep  3 08:04 texto1.txt
--rw-rw-r-- M 49 glenda glenda 34 Sep  3 08:04 texto2.txt
--rw-rw-r-- M 49 glenda glenda 35 Sep  3 08:05 texto3.txt
term%
```

Extração do *snapshot* e acesso ao diretório /n/vac

Fonte: Dados produzidos pelo autor (2019)

Obrigada!

KATIA A R FUCHS

Especialista em perícia digital
rkatia79@gmail.com