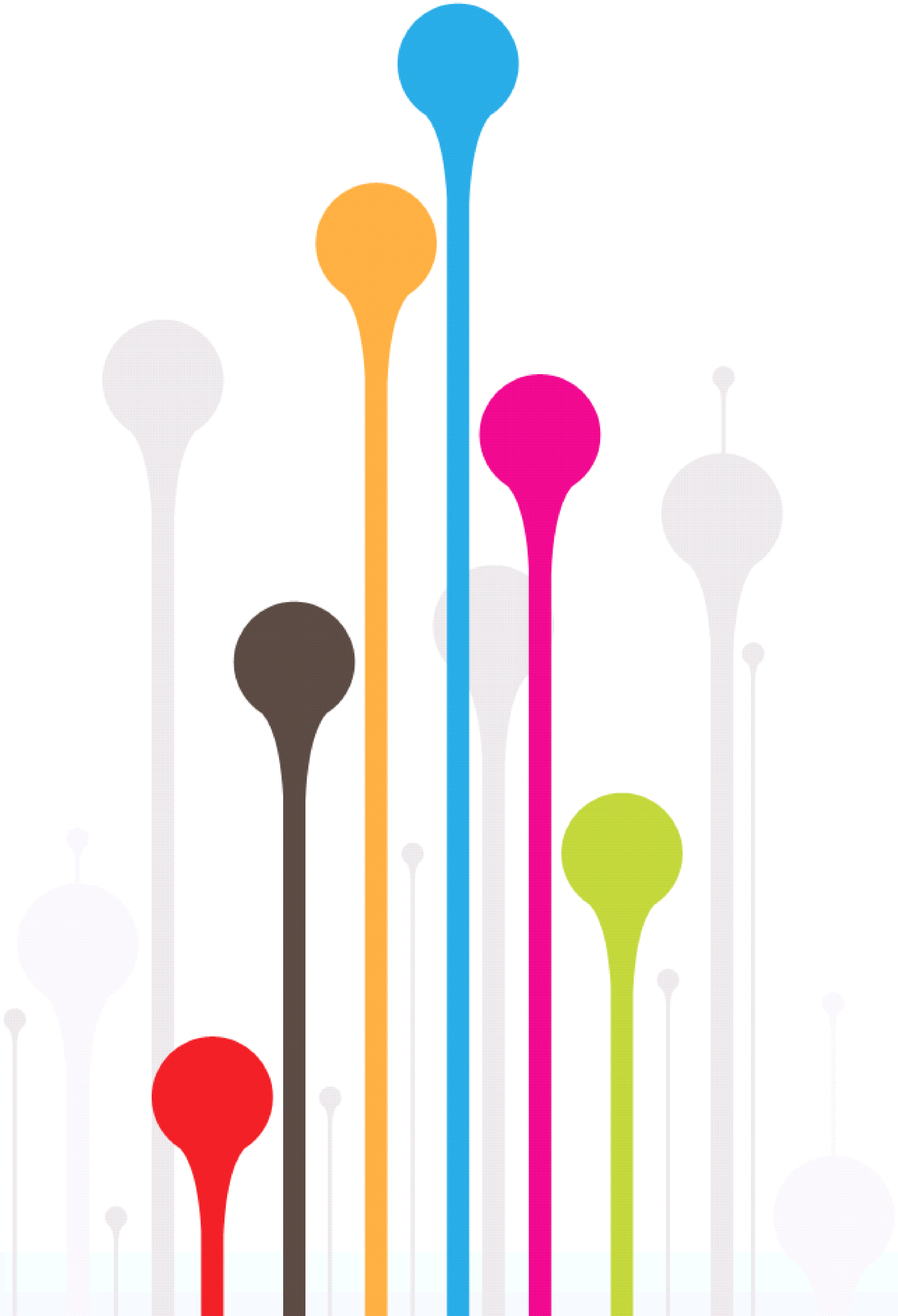
Cloud Forensics

Module 10



Cloud Forensics

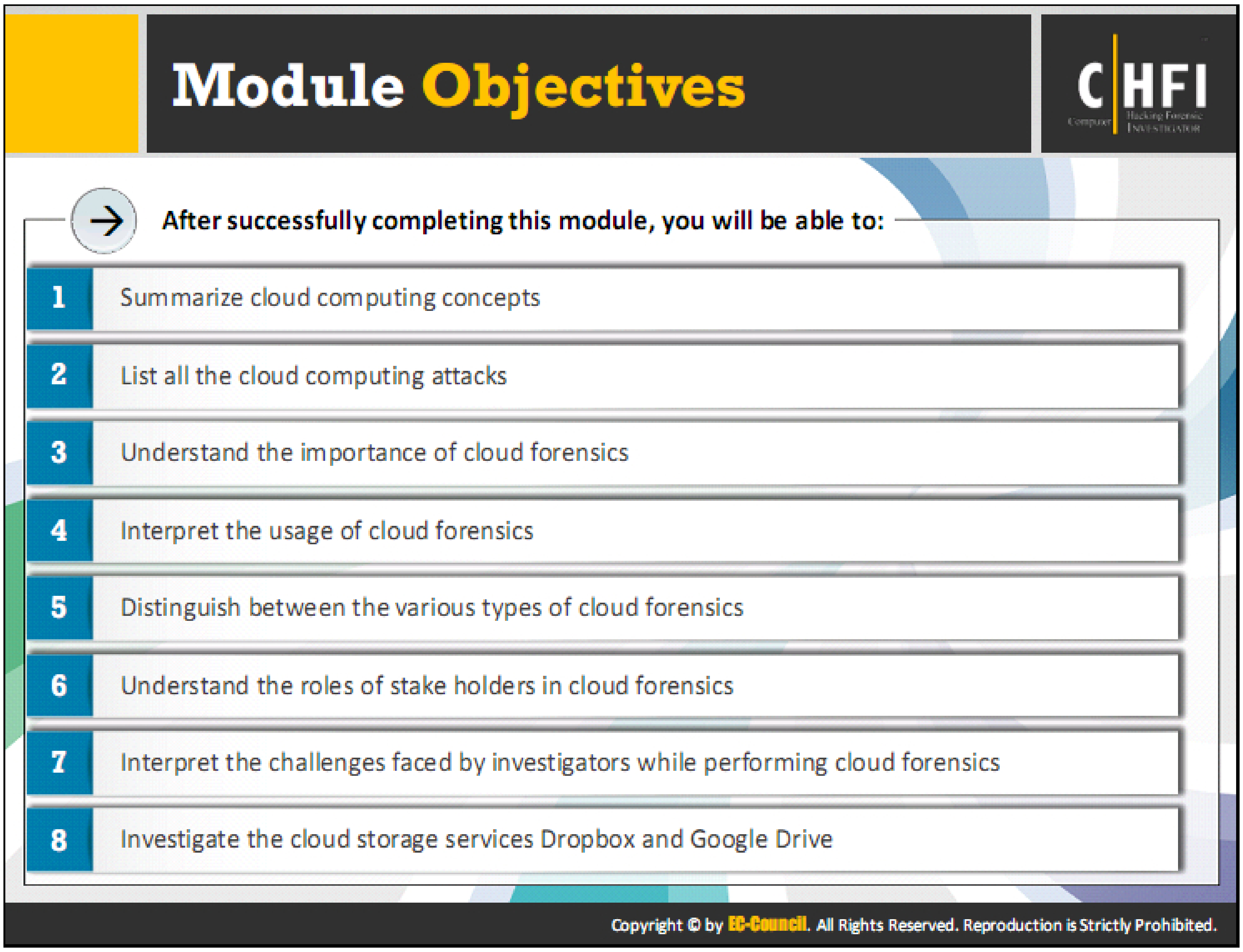
Module 10

Designed by Cyber Crime Investigators. Presented by Professionals.

Computer Hacking Forensic Investigator v9

Module 10: Cloud Forensics

Exam 312-49



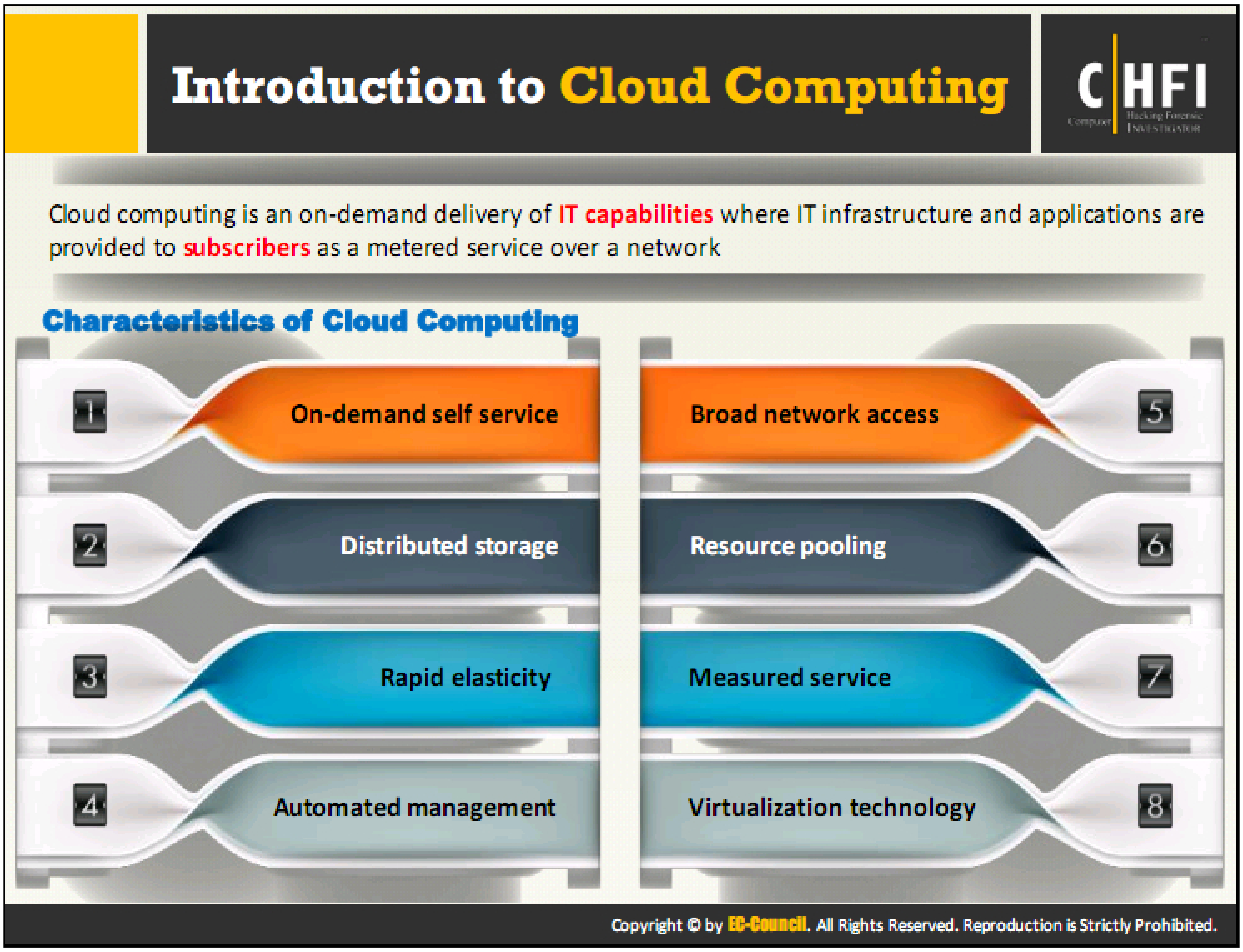
Module Objectives

After successfully completing this module, you will be able to:

1. Summarize cloud computing concepts
2. List all the cloud computing attacks
3. Understand the importance of cloud forensics
4. Interpret the usage of cloud forensics
5. Distinguish between the various types of cloud forensics
6. Understand the roles of stake holders in cloud forensics
7. Interpret the challenges faced by investigators while performing cloud forensics
8. Investigate the cloud storage services Dropbox and Google Drive

Cloud computing is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the Internet. Cloud implementation enables a distributed workforce, reduces organization expenses, provides data security, and, so on. As many enterprises are adopting the cloud, attackers make cloud as their target of exploit in order to gain unauthorized access to the valuable data stored in it. Therefore, one should perform cloud pen testing regularly to monitor its security posture.

This module starts with an overview of cloud computing concepts. It provides an insight into cloud computing threats and cloud computing attacks. Later, it discusses cloud computing security and the necessary tools. The module ends with an overview of pen-testing steps an ethical hacker should follow to perform a security assessment of the cloud environment.



Introduction to Cloud Computing

Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network

Characteristics of Cloud Computing

1. On-demand self service
2. Distributed storage
3. Rapid elasticity
4. Automated management
5. Broad network access
6. Resource pooling
7. Measured service
8. Virtualization technology

Cloud computing is an on-demand delivery of IT capabilities in which IT infrastructure and applications are provided to subscribers as metered services over networks. Examples of cloud solutions include Gmail, Facebook, Dropbox, and Salesforce.com.

Discussed below are the characteristics of cloud computing that attract many businesses today to adopt cloud technology.

- **On-demand self-service**

  A type of service rendered by cloud service providers that allow provisions for cloud resources such as computing power, storage, network, and so on, always on demand, without the need for human interaction with service providers.

- **Distributed storage**

  Distributed storage in the cloud offers better scalability, availability, and reliability of data. However, cloud distributed storage does have the potential for security and compliance concerns.

- **Rapid elasticity**

  The cloud offers instant provisioning of capabilities, to rapidly scale up or down, according to demand. To the consumers, the resources available for provisioning seem to be unlimited, and they can purchase in any quantity at any point of time.

- **Automated management**

  By minimizing the user involvement, cloud automation speeds up the process, reduces labor costs, and reduces the possibility of human error.

- **Broad network access**

  Cloud resources are available over the network and accessed through standard procedures, via a wide-variety of platforms, including laptops, mobile phones, and PDAs.

- **Resource pooling**

  The cloud service provider pools all the resources together to serve multiple customers in the multi-tenant environment, with physical and virtual resources dynamically assigned and reassigned on demand by the cloud consumer.

- **Measured service**

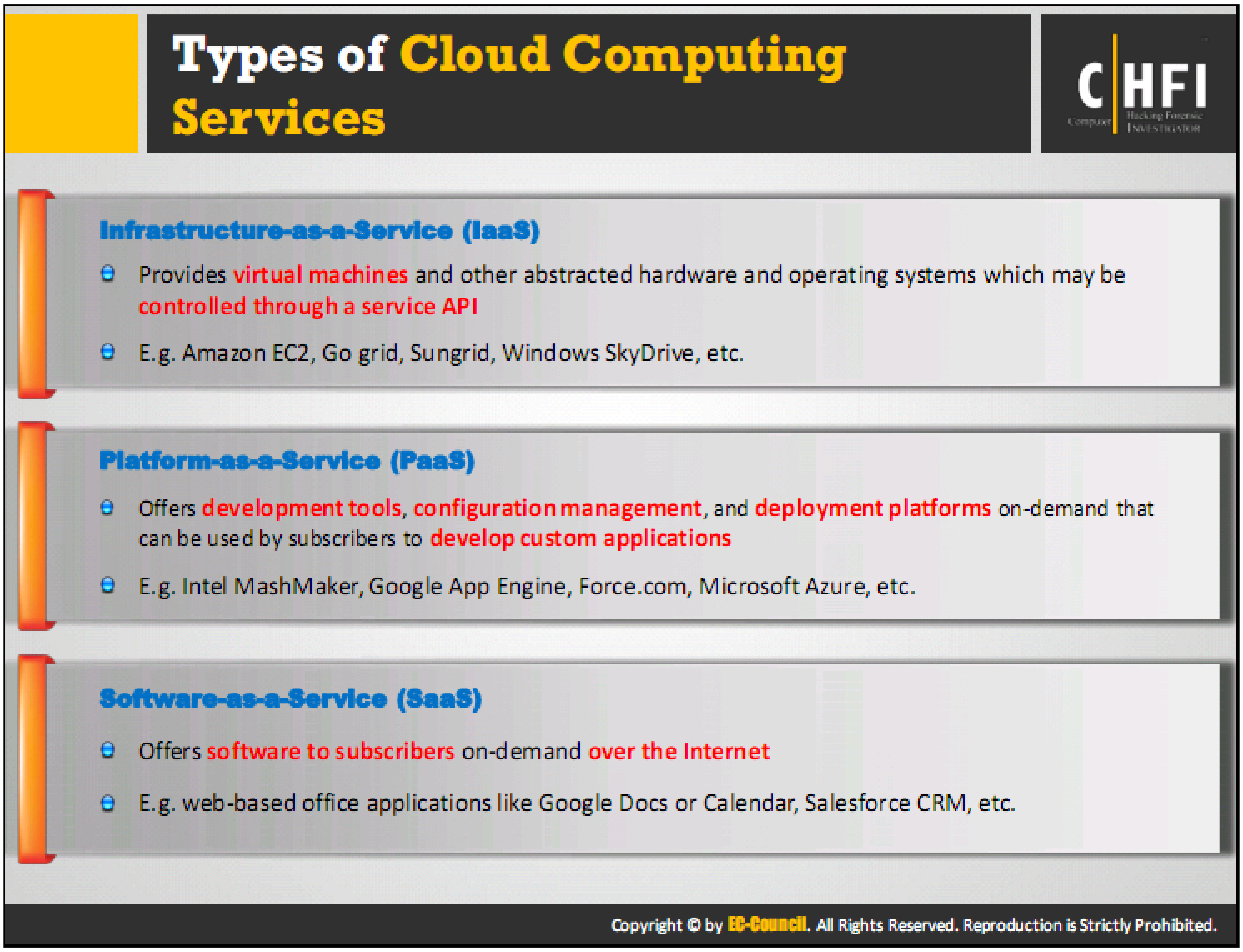
  Cloud systems employ "pay-per-use" metering method. Subscribers pay for cloud services by monthly subscription or according to the usage of resources such as storage levels, processing power, bandwidth, and so on. Cloud service providers monitor, control, report, and charge consumption of resources by customers with complete transparency.

- **Virtualization technology**

  Virtualization technology in the cloud enables rapid scaling of resources in a way that non-virtualized environments could not achieve.

Limitations of Cloud Computing:

- Organizations have limited control and flexibility
- Prone to outages and other technical issues
- Security, privacy, and compliance issues
- Contracts and lock-ins
- Depends on network connections



Types of Cloud Computing Services

Infrastructure-as-a-Service (IaaS)

- Provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API
- E.g. Amazon EC2, Go grid, Sungrid, Windows SkyDrive, etc.

Platform-as-a-Service (PaaS)

- Offers development tools, configuration management, and deployment platforms on-demand that can be used by subscribers to develop custom applications
- E.g. Intel MashMaker, Google App Engine, Force.com, Microsoft Azure, etc.

Software-as-a-Service (SaaS)

- Offers software to subscribers on-demand over the Internet
- E.g. web-based office applications like Google Docs or Calendar, Salesforce CRM, etc.

Cloud services are of three types based on the services provided:

Infrastructure-as-a-Service (IaaS)

This cloud computing service enables subscribers to use fundamental IT resources such as computing power, virtualization, data storage, network, and so on, on demand. As cloud service providers are responsible for managing the underlying cloud-computing infrastructure, subscribers can avoid costs of human capital, hardware, and others (e.g., Amazon EC2, Go grid, Sungrid, Windows SkyDrive).

Advantages:

- Dynamic infrastructure scaling
- Guaranteed uptime
- Automation of administrative tasks
- Elastic load balancing (ELB)
- Policy-based services
- Global accessibility

Disadvantages:

- Software security is at high risk (third-party providers are more prone to attacks)
- Performance issues and slow connection speeds

Platform-as-a-Service (PaaS)

This service offers the platform for the development of applications and services. Subscribers need not buy and manage the software and infrastructure underneath it but have authority over deployed applications and perhaps application hosting environment configurations. Advantages of writing applications in the PaaS environment includes dynamic scalability, automated backups, and other platform services, without the need to explicitly code for it.

Advantages:

- Simplified deployment
- Prebuilt business functionality
- Lower risk
- Instant community
- Pay-per-use model
- Scalability

Disadvantages:

- Vendor lock-in
- Data privacy
- Integration with the rest of the system applications

Software-as-a-Service (SaaS)

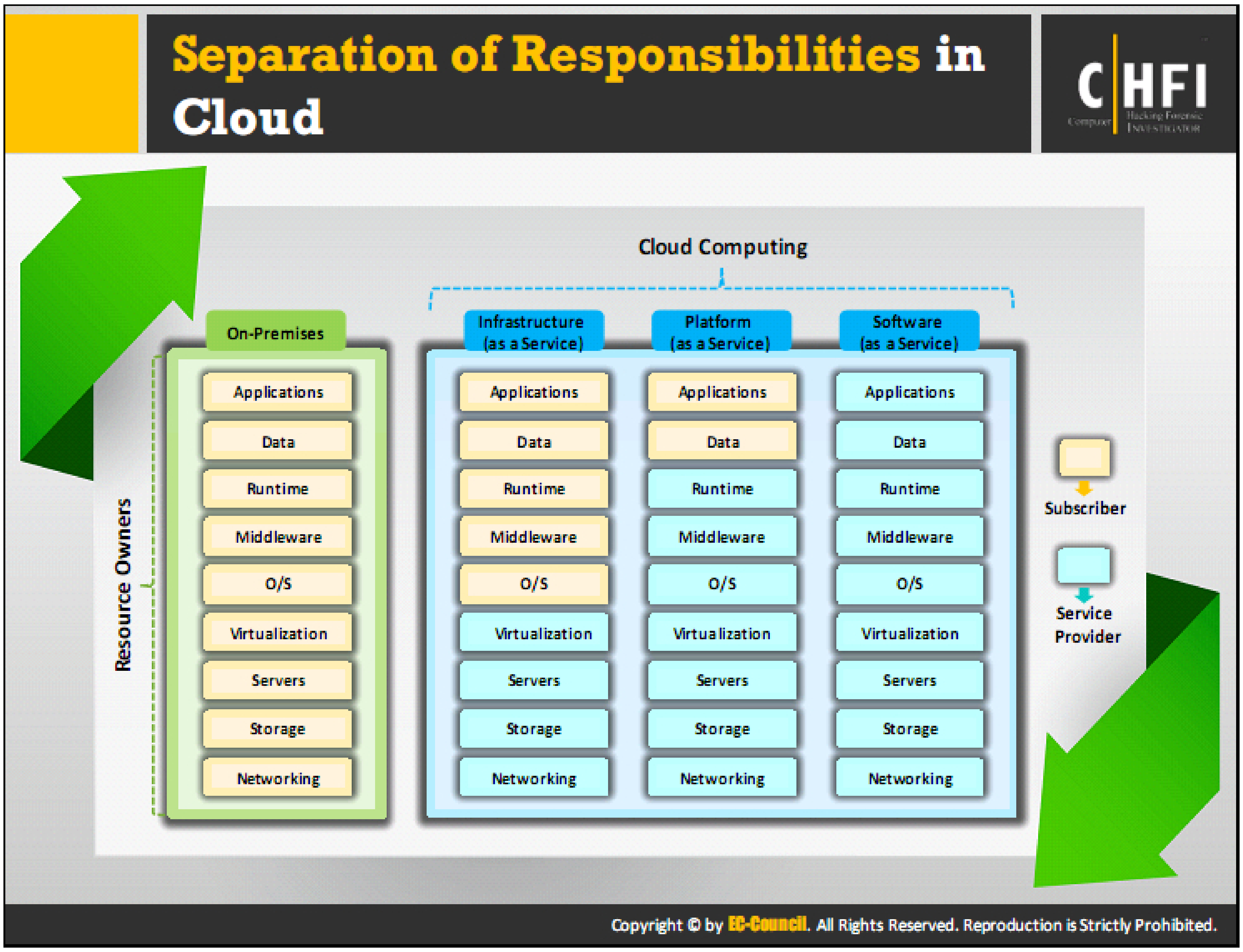
This cloud computing service offers application software to subscribers' on-demand, over the Internet. The provider charges for it on a pay-per-use basis, by subscription, by advertising, or by sharing among multiple users.

Advantages:

- Low cost
- Easier administration
- Global accessibility
- Compatible (Requires no special hardware or software)

Disadvantages:

- Security and latency issue
- Total dependency on the Internet
- Switching between SaaS vendors is difficult



Separation of Responsibilities in Cloud

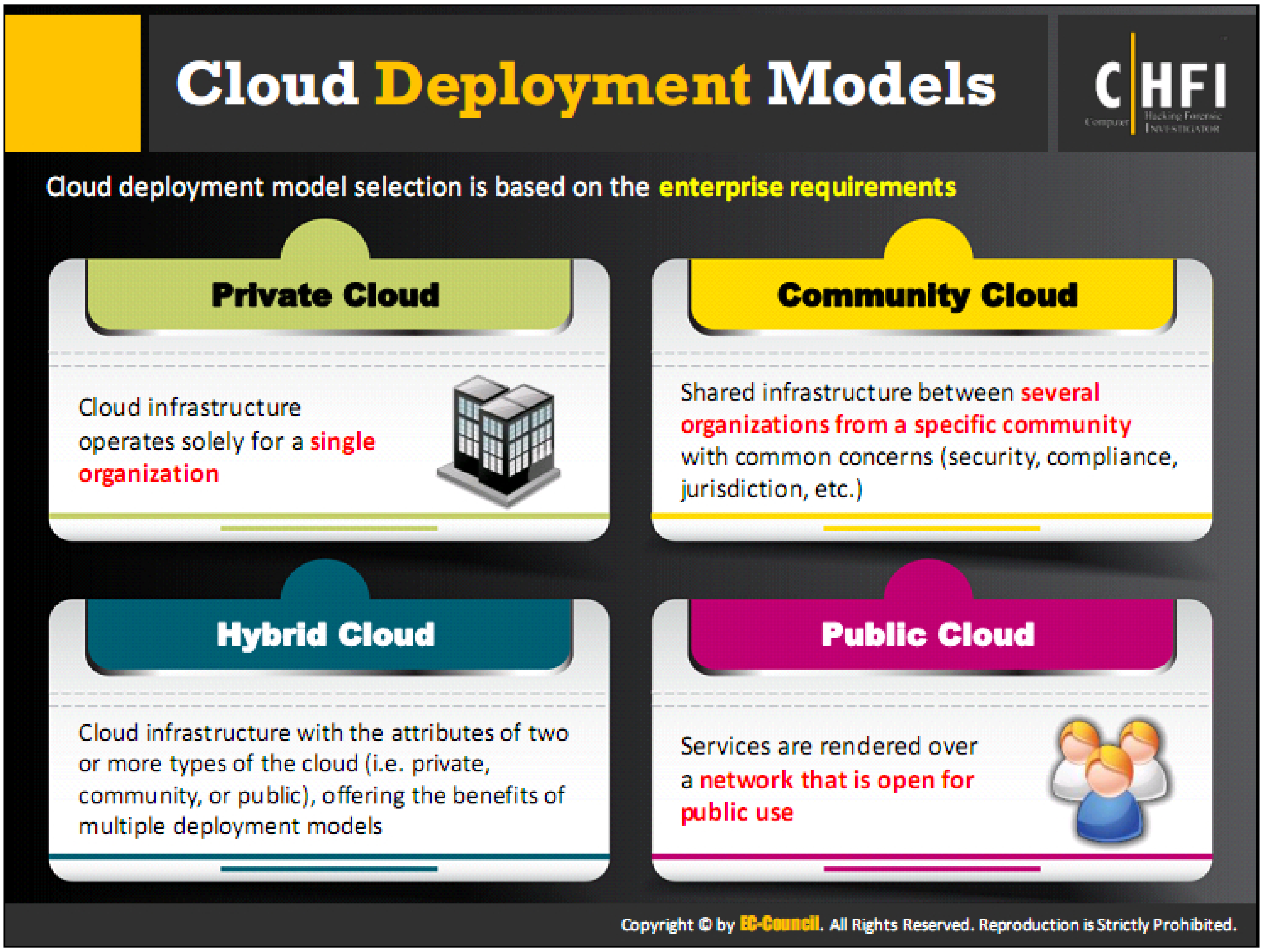
On-Premises	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
🟨 Applications	🟨 Applications	🟨 Applications	🟦 Applications
🟨 Data	🟨 Data	🟨 Data	🟦 Data
🟨 Runtime	🟨 Runtime	🟦 Runtime	🟦 Runtime
🟨 Middleware	🟨 Middleware	🟦 Middleware	🟦 Middleware
🟨 O/S	🟨 O/S	🟦 O/S	🟦 O/S
🟨 Virtualization	🟦 Virtualization	🟦 Virtualization	🟦 Virtualization
🟨 Servers	🟦 Servers	🟦 Servers	🟦 Servers
🟨 Storage	🟦 Storage	🟦 Storage	🟦 Storage
🟨 Networking	🟦 Networking	🟦 Networking	🟦 Networking

🟨 Subscriber

🟦 Service Provider

In cloud computing, separation of subscriber and service provider responsibilities is essential. Separation of duties prevents conflict of interest, illegal acts, fraud, abuse, and error, and helps in identifying security control failures, including information theft, security breaches, and evasion of security controls. It also helps in restricting the amount of influence held by any individual and ensures that there are no conflicting responsibilities.

Three types of cloud services exist, IaaS, PaaS, and SaaS. It is important to know the limitations of each cloud service delivery model when accessing particular clouds and their models. The diagram on the slide illustrates the separation of cloud responsibilities specific to service delivery models.



Cloud Deployment Models

Cloud deployment model selection is based on the **enterprise requirements**

Private Cloud

Cloud infrastructure operates solely for a **single organization**

Community Cloud

Shared infrastructure between **several organizations from a specific community** with common concerns (security, compliance, jurisdiction, etc.)

Hybrid Cloud

Cloud infrastructure with the attributes of two or more types of the cloud (i.e. private, community, or public), offering the benefits of multiple deployment models

Public Cloud

Services are rendered over a **network that is open for public use**

One can deploy cloud services in different ways, according to the factors given below:

- Where cloud computing services are hosted
- Security requirements
- Sharing cloud services
- Ability to manage some or all of the cloud services
- Customization capabilities

The four common cloud deployment models are:

Private Cloud

A private cloud, also known as internal or corporate cloud, is a cloud infrastructure that a single organization operates solely. The organization can implement the private cloud within a corporate firewall. Organizations deploy private cloud infrastructures to retain full control over corporate data.

Advantages:

- Enhance security (services are dedicated to a single organization)
- More control over resources (organization is in charge)
- Greater performance (deployed within the firewall; therefore data transfer rates are high)

- Customizable hardware, network, and storage performances (as private cloud is owned by the organization)
- Sarbanes-Oxley, PCI DSS, and HIPAA compliance data are much easier to attain

Disadvantages:

- Expensive
- On-site maintenance

Hybrid Cloud

It is a cloud environment comprised of two or more clouds (private, public, or community) that remain unique entities but bound together for offering the benefits of multiple deployment models. In this model, the organization makes available, manages some resources in-house, and provides other resources externally.

Example: An organization performs its critical activities on the private cloud (such as operational customer data) and non-critical activities on the public cloud.

Advantages:

- More scalable (contains both public and private clouds)
- Offers both secure resources and scalable public resources
- High level of security (comprises private cloud)
- Allows to reduce and manage the cost as per the requirement

Disadvantages:

- Communication at the network level may differ as it uses both public and private clouds
- Difficult to achieve data compliance
- Organization has to rely on the internal IT infrastructure for support to handle any outages (maintain redundancy across data centers to overcome)
- Complex Service Level Agreements (SLAs)

Community Cloud

It is a multi-tenant infrastructure shared among organizations from a specific community with common computing concerns such as security, regulatory compliance, performance requirements, and jurisdiction. The community cloud can be either on-premises or off-premises and governed by the organizations that took part or by a third-party managed service provider.

Advantages:

- Less expensive compared to the private cloud
- Flexibility to meet the community's needs
- Compliance with legal regulations
- High scalability

- Organizations can share a pool of resources and from anywhere via the Internet

Disadvantages:

- Competition between consumers in usage of resources
- No accurate prediction on required resources
- Who is the legal entity in case of liability
- Moderate security (other tenants may be able to access data)
- Trust and security concern between the tenants

Public Cloud

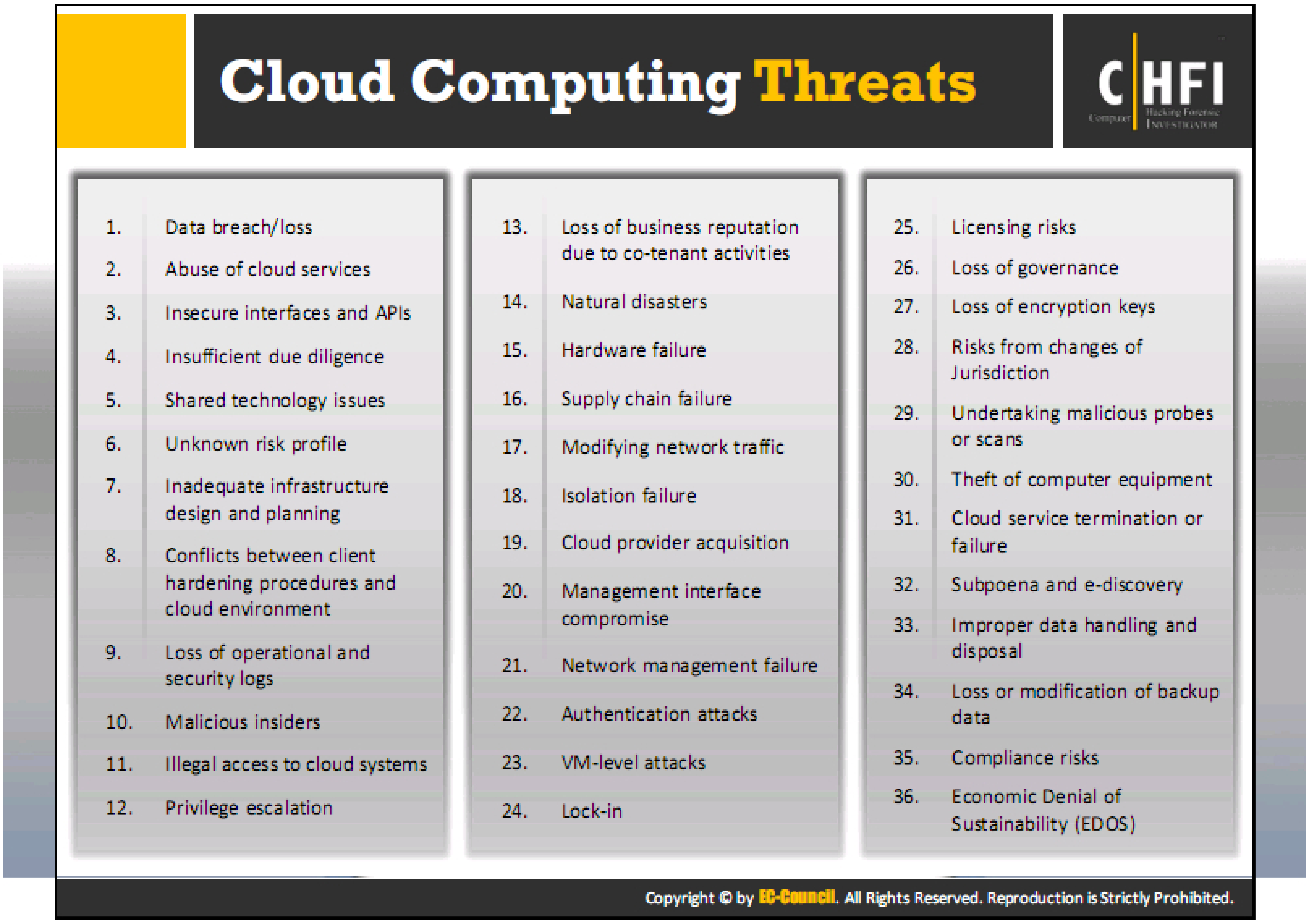
In this model, the provider makes services such as applications, servers, and data storage available to the public over the Internet. In this model, the cloud provider is liable for the creation and constant maintenance of the public cloud and its IT resources. Public cloud services may be free or based on a pay-per-usage model (e.g., Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Google App Engine, and Windows Azure Services Platform).

Advantages:

- Simplicity and efficiency
- Low cost
- Reduced time (when server crashes, needs restart or reconfigure cloud)
- No maintenance (public cloud service is hosted off-site)
- No Contracts (no long-term commitments)

Disadvantages:

- Security is not guaranteed
- Lack of control (third-party providers are in charge)
- Slow speed (relies on Internet connections, data transfer rate is limited)



Cloud Computing Threats

1. Data breach/loss
2. Abuse of cloud services
3. Insecure interfaces and APIs
4. Insufficient due diligence
5. Shared technology issues
6. Unknown risk profile
7. Inadequate infrastructure design and planning
8. Conflicts between client hardening procedures and cloud environment
9. Loss of operational and security logs
10. Malicious insiders
11. Illegal access to cloud systems
12. Privilege escalation
13. Loss of business reputation due to co-tenant activities
14. Natural disasters
15. Hardware failure
16. Supply chain failure
17. Modifying network traffic
18. Isolation failure
19. Cloud provider acquisition
20. Management interface compromise
21. Network management failure
22. Authentication attacks
23. VM-level attacks
24. Lock-in
25. Licensing risks
26. Loss of governance
27. Loss of encryption keys
28. Risks from changes of Jurisdiction
29. Undertaking malicious probes or scans
30. Theft of computer equipment
31. Cloud service termination or failure
32. Subpoena and e-discovery
33. Improper data handling and disposal
34. Loss or modification of backup data
35. Compliance risks
36. Economic Denial of Sustainability (EDOS)

Data Breach/Loss

Data loss issues include:

- Data is erased, modified or decoupled (lost)
- Encryption keys are lost, misplaced or stolen
- Illegal access to the data in cloud due to Improper authentication, authorization, and access controls
- Misuse of data by Cloud Service Provider (CSP)

Improperly designed cloud computing environment with multiple clients is at greater risk of the data breach as a flaw in one client's application cloud allow attackers to access other client's data. Data loss or leakage depends heavily on cloud architecture and its operation.

Abuse of Cloud Services

Attackers create anonymous access to cloud services and perpetrate various attacks such as password and key cracking, building rainbow tables, CAPTCHA-solving farms, launching dynamic attack points, hosting exploits on cloud platforms and malicious data, botnet command or control and distributed denial-of-service (DDoS).

The presence of weak registration systems in the cloud-computing environment gives rise to this threat. Attackers create anonymous access to cloud services and perpetrate various attacks.

Insecure Interfaces and APIs

Insecure interfaces and APIs related risks include circumvention of user defined policies, a breach in logging and monitoring facilities, unknown API dependencies, reusable passwords/tokens, and insufficient input data validation.

Interfaces or APIs enable customers to manage and interact with cloud services. Cloud service models must be security integrated, and users must be aware of security risks in the use, implementation, and monitoring of such services.

Insufficient Due Diligence

Ignorance of CSP's cloud environment pose risks in operational responsibilities such as security, encryption, incident response, and more issues such as contractual issues, design and architectural issues, etc.

Shared Technology Issues

Most underlying components that make up the cloud infrastructure (ex: GPU, CPU caches, etc.) does not offer strong isolation properties in a multi-tenant environment which enable attackers to attack other machines if they can exploit vulnerabilities in one client's applications.

IaaS vendors use the same infrastructure to cater multiple clients, and most of the shared components do not offer strong isolation properties. To address this issue, vendors install virtualization hypervisors between guest OSs and the physical resources to contain loopholes. Issues include Rutkowska's Red and Blue Pill exploits and Kortchinsky's CloudBurst presentations.

Unknown Risk Profile

Client organizations are unable to get a clear picture of internal security procedures, security compliance, configuration hardening, patching, auditing, and logging, etc. as they are less involved with hardware and software ownership and maintenance in the cloud.

Software updates, threat analysis, intrusion detection, security practices, and others determine security posture of an organization. Organizations are unable to provide a clear picture on the level of security, as they are less involved with hardware and software ownership and maintenance in the cloud. However, organizations must be aware of issues such as internal security procedures, security compliance, configuration hardening, patching, and auditing and logging.

Inadequate Infrastructure Design and Planning

An agreement between the CSP and customer states the quality of service that the CSP offers such as downtime, physical and network-based redundancies, regular data backup, and restoring processes, and availability periods.

At times, cloud service providers may not satisfy the rapid rise in demand due to the shortage of computing resources and/or poor network design (e.g., traffic flows through a single point, even though the necessary hardware is available) giving rise to unacceptable network latency or inability to meet agreed service levels.

Conflicts between Client Hardening Procedures and Cloud Environment

Certain client hardening procedures may conflict with a cloud provider's environment, making their implementation by the client impossible. The reason for this is because a cloud is a multi-tenant environment, the colocation of many customers indeed causes conflict for the cloud providers, as customers' communication security requirements are likely to diverge from one another.

Loss of Operational and Security Logs

The loss of operational logs makes it difficult to evaluate operational variables. The options for solving issues are limited when no data is available for analysis. Loss of security logs may occur in case of under-provisioning of storage.

Malicious Insiders

Malicious insiders are disgruntled current/former employees, contractors, or other business partners who have/had authorized access to cloud resources and could intentionally exceed or misuse that access to compromise the confidentiality, integrity, or availability of the organization's information. Threats include loss of reputation, productivity, and financial theft.

Illegal Access to the Cloud

Weak authentication and authorization controls could lead to illegal access thereby compromising confidential and critical data stored in the cloud.

Privilege Escalation

A mistake in the access allocation system such as coding errors, design flaws, and others can result in a customer, third party, or employee obtaining more access rights than required. This threat arises because of AAA (Authentication, authorization, and accountability) vulnerabilities, user provisioning and de-provisioning vulnerabilities, hypervisor vulnerabilities, unclear roles and responsibilities, misconfiguration, and others.

Loss of Business Reputation due to Co-tenant Activities

Resources are shared in the cloud; thus the malicious activity of one co-tenant might affect the reputation of the other, resulting in poor service delivery, data loss, etc. that bring down organization's reputation.

This threat arises because of lack of resource isolation, lack of reputational confinement, vulnerabilities in the hypervisors, and others.

Natural Disasters

Based on geographic location and climate, data centers are prone to natural disasters such as floods, lightning, earthquakes, etc. that can affect the cloud services.

Hardware Failure

Hardware failure such as switches, servers, routers, access points, hard disks, network cards, and processors in data centers can make cloud data inaccessible. The majority of hardware failures happen because of hard drive problems. Hard disk failures take a lot of time to track and fix because of their low-level complexities. Hardware failure can lead to poor performance delivery to end users and can damage the business.

Supply Chain Failure

This threat arises because of incomplete and non-transparent terms of use, hidden dependency created by cross-cloud applications, inappropriate CSP selection, lack of supplier redundancy, and others. Cloud providers outsource certain tasks to third parties. Thus the security of the cloud is directly proportional to security of each link and the extent of dependency on third parties

A disruption in the chain may lead to loss of data privacy and integrity, services unavailability, violation of SLA, economic and reputational losses resulting in failure to meet customer demand, and cascading failure.

Modifying Network Traffic

This threat arises because of user provisioning and de-provisioning vulnerabilities, communication encryption vulnerabilities, and so on. In cloud, the network traffic may alter due to flaws while provisioning or de-provisioning network, or vulnerabilities in communication encryption. Modification of network traffic may cause loss, alteration, or theft of confidential data and communications.

Isolation Failure

Multi-tenancy and shared resources are the characteristics of cloud computing. Strong isolation or compartmentalization of storage, memory, routing, and reputation between different tenants is lacking. Because of isolation failure, attackers try to control operations of other cloud customers to gain illegal access to the data.

Cloud Provider Acquisition Countermeasure:

Acquisition of the cloud provider may increase the probability of tactical shift and may effect non- binding agreements at risk. This could make it difficult to cope up with the security requirements

Management Interface Compromise Countermeasures:

This threat arises due to the improper configuration, system and application vulnerabilities, remote access to the management interface, and so on. Customer management interfaces of cloud provider are accessible via the Internet and facilitate access to a large number of resources. This enhances the risk, particularly when combined with remote access and web browser vulnerabilities.

Network Management Failure Countermeasures:

Poor network management leads to network congestion, misconnection, misconfiguration, lack of resource isolation, etc., which affects services and security.

Authentication Attacks Countermeasures:

Weak authentication mechanisms (weak passwords, re-use passwords, etc.) and inherent limitations of one-factor authentication mechanisms allow the attacker to gain unauthorized access to cloud computing systems.

VM-Level Attacks

Cloud computing extensively uses virtualization technologies offered by several vendors including VMware, Xen, Virtual box, and vSphere. Threats to these technologies arise because of vulnerabilities in the hypervisors.

Lock-in

This threat leaves the clients unable to shift from one cloud service provider to another or in-house systems due to the lack of necessary tools, procedures or standards data formats for data, application, and service portability. This threat is due to the inappropriate selection of CSP, incomplete and non-transparent terms of use, lack of standard mechanisms, etc.

Licensing Risks

The organization may incur a huge licensing fee if the CSP charges the software deployed in the cloud on a per-instance basis. Therefore, the organization should always retain ownership over its software assets located in the cloud provider environment. Risks to licensing occur because of incomplete and non-transparent terms of use.

Loss of Governance

In using cloud computing services, cloud service providers have more control over the security related issues compared to the customers. Sometimes, such issues may not be part of the agreement, which leaves the stored data defenseless. Reasons for this threat include uncertain roles and responsibilities, shortage of vulnerability detection process, lack of jurisdiction, unavailability of the audit, and others.

Loss of governance results in not complying with security requirements, lack of confidentiality, integrity, and availability of data, poor performance and quality of service, and so on.

Loss of Encryption Keys

This threat arises due to the poor management of keys and poor key generation techniques. The loss of encryption keys required for secure communication or systems access provides a potential attacker with the possibility to access unauthorized assets.

Risks from Changes of Jurisdiction

Cloud service provider may have cloud databases in multiple locations, which can include places with higher risk possibility, countries with weak digital laws and legal framework, which might result in enforced disclosure or seizure of the data or information system. Customers should consider jurisdictional ambiguities before adopting a cloud, as local laws of a particular country for data storage could provide government access to private data.

Undertaking Malicious Probes or Scans

Malicious probes or scanning allows an attacker to collect sensitive information that may lead to loss of confidentiality, integrity, and availability of services and data.

Theft of Computer Equipment

Theft of equipment may occur due to poor controls on physical parameters such as smart card access at the entry etc. which may lead to loss of physical equipment and sensitive data.

Cloud Service Termination or Failure

Termination of cloud service because of non-profitability or disputes might result in data loss unless end-users protect themselves legally. Many factors, such as competitive pressure, lack of financial support, and inadequate business strategy, could lead to termination or failure of the cloud service.

This threat results in poor service delivery, loss of investment, quality of service, and so on. Furthermore, failures in the services outsourced to the CSP may affect cloud customers' ability to meet its duties and commitments to its customers.

Subpoena and E-Discovery

This threat occurs due to the improper resource isolation, data storage in multiple jurisdictions, and lack of insight on jurisdictions. Customer data and services are subpoenaed or subjected to a cease request from authorities or third parties.

Improper Data Handling and Disposal

When clients request data deletion, the service provider may not wipe the data completely which will result in presence of data traces over the cloud that attackers can use to recover the data after hacking the infrastructure. It's hard to determine data handling and disposal procedures followed by CSPs due to limited access to cloud infrastructure.

Loss/Modification of Backup Data

Attackers might exploit vulnerabilities such as Structured Query Language (SQL) injection and insecure user behavior (e.g., storing or reusing passwords) to gain illegal access to the data backups in the cloud. After gaining access, attackers might delete or modify the data stored in the databases. Lack of data restoration procedures in case of backup data loss keeps the service levels at risk.

Compliance Risks

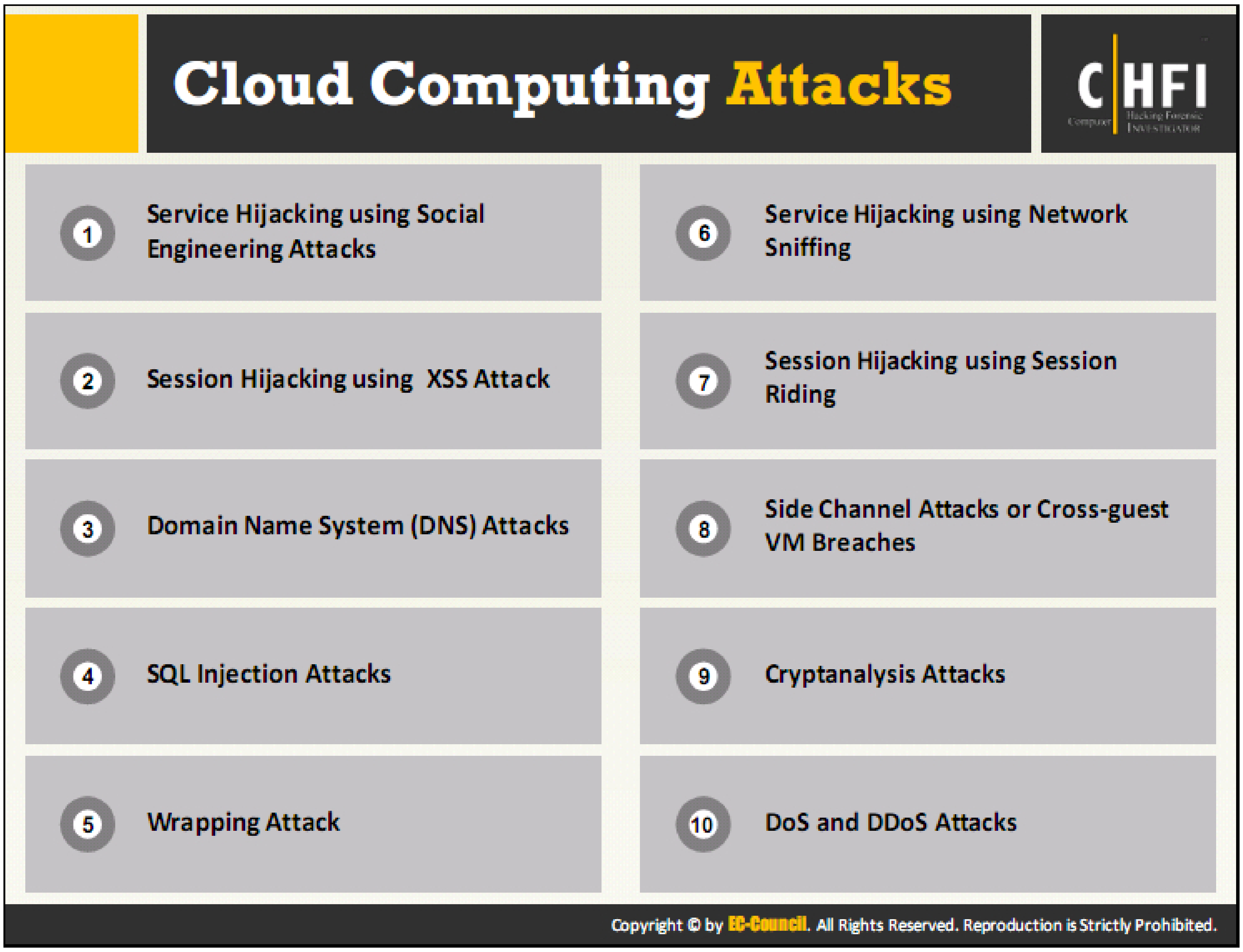
This threat is due to the lack of governance over audits and industry standard assessments. Thus, clients are not aware of the processes, and practices of providers in the areas of access, identity management, and segregation of duties.

Organizations need to comply with the standards, and laws may be at risk if the service does not fulfill the necessary requirements or if the service provider outsources the cloud management to third parties.

Economic Denial of Service (EDoS)

The payment method in a cloud system is "No use, no bill": the CSP charges the customer according to the recorded data involved when customers make requests, the duration of requests, the amount of data transfer in the network, and the number of CPU cycles consumed.

Economic denial of service destroys financial resources; in the worst case, this could lead to customer bankruptcy or other severe economic impact. If an attacker engages the cloud with a malicious service or executes malicious code that consumes a lot of computational power and storage from the cloud server, then the legitimate account holder has to pay for this kind of computation, until the service provider finds the primary cause of CPU usage.



Cloud Computing Attacks

1. Service Hijacking using Social Engineering Attacks
2. Session Hijacking using XSS Attack
3. Domain Name System (DNS) Attacks
4. SQL Injection Attacks
5. Wrapping Attack
6. Service Hijacking using Network Sniffing
7. Session Hijacking using Session Riding
8. Side Channel Attacks or Cross-guest VM Breaches
9. Cryptanalysis Attacks
10. DoS and DDoS Attacks

Service Hijacking using Social Engineering Attacks

In account or service hijacking, an attacker steals CSP's or client's credentials by methods such as phishing, pharming, social engineering, and exploitation of software vulnerabilities. Using the stolen credentials, the attacker gains access to the cloud computing services and compromises data confidentiality, integrity, and availability.

Attackers might target cloud service providers to reset passwords, or IT staff to access their cloud services to reveal passwords. Other ways to obtain passwords include password guessing, keylogging malware, implementing password-cracking techniques, sending phishing emails, and others. Social engineering attacks result in exposed customer data, credit card data, personal information, business plans, staff data, identity theft, and so on.

Session Hijacking using XSS Attack

An attacker implements cross-site scripting (XSS) to steal cookies used in user authentication process; this involves injecting malicious code into the website. Using the stolen cookies attacker exploits active computer sessions, thereby gaining unauthorized access to the data.

Note: Attacker can also predict or sniff session IDs.

The attacker hosts a web page with the malicious script onto the cloud server. When the user views the page hosted by the attacker, the HTML containing malicious script runs on the user's browser. The malicious script will collect browser cookies and redirects the user to the attacker's server; it also sends the request with the collected cookies.

Domain Name System (DNS) Attacks

The attacker performs DNS cache poisoning, directing users to a fake website to gather the authentication credentials. Here, the user queries the internal DNS server for DNS information. The internal DNS server then queries the respective cloud server for DNS information. At this point, attacker blocks the DNS response from the cloud server and sends DNS response with IP of a fake website to the internal DNS server. Thus, the internal DNS server cache updates itself with the IP of fake website and automatically directs the user to the fake website.

Types of DNS Attacks

- **DNS Poisoning:** Involves diverting users to a spoofed website by poisoning the DNS server or the DNS cache on the user's system
- **Cybersquatting:** Involves conducting phishing scams by registering a domain name that is similar to a cloud service provider
- **Domain Hijacking:** Involves stealing a cloud service provider's domain name
- **Domain Snipping:** Involves registering an elapsed domain name

SQL Injection Attacks

SQL is a programming language meant for database management systems. In SQL injection attack, attackers insert malicious code (generated using special characters) into a standard SQL code to gain unauthorized access to a database and ultimately to other confidential information.

- Attackers target SQL servers running vulnerable database applications
- It occurs generally when application uses input to construct dynamic SQL statements
- In this attack, attackers insert a malicious code (generated using special characters) into a standard SQL code to gain unauthorized access to a database
- Further attackers can manipulate the database contents, retrieve sensitive data, remotely execute system commands, or even take control of the web server for further criminal activities

Wrapping Attack

When users send a request from their VM through a browser, the request first reaches a web server, which generates a SOAP message containing structural information, which it will exchange with the browser during message passing. Before message passing occurs, the browser needs to sign the XML document and authorize it. In addition, it should append the signature values to the document. Finally, the Simple Object Access Protocol (SOAP) header should contain all the necessary information for the destination after computation.

For a wrapping attack, the adversary does its deception during the translation of the SOAP message in the TLS (transport layer service) layer. The attacker duplicates the body of the message and sends it to the server as a legitimate user. The server checks the authentication by the Signature Value (which is also duplicated) and checks its integrity. As a result, the adversary can intrude in the cloud and can run malicious code to interrupt the normal functioning of the cloud servers.

Service Hijacking using Network Sniffing

Network sniffing involves interception and monitoring of network traffic sent between two cloud nodes. Unencrypted sensitive data (such as login credentials) during transmission across a network is at greater risk. Attacker uses packet sniffers (e.g., Wireshark, Cain and Abel) to capture sensitive data such as passwords, session cookies, and other web-based services security configuration such as the UDDI (Universal Description Discovery and Integrity), SOAP, and WSDL (Web Service Description Language) files.

Session Hijacking using Session Riding

Attackers exploit websites by engaging in cross-site request forgeries to transmit unauthorized commands. In session riding, attackers "ride" an active computer session by sending an email or tricking users to visit a malicious web page, during login, to an actual target site. When the user clicks the malicious link, the website executes the request as if the user had already authenticated it. Commands used include modifying or deleting user data, performing online transactions, resetting passwords, and others.

Side Channel Attacks or Cross-guest VM Breaches

Attackers compromise the cloud by placing virtual machines (VMs) in proximity to a target cloud server. They run these VMs on the same physical host of the victims' VM and take advantage of shared physical resources (processor cache) to launch side-channel attacks (timing attack to extract cryptographic keys/plain text secrets to steal the victim's credentials. The attackers then use the stolen credentials to impersonate the victim.

Cryptanalysis Attacks

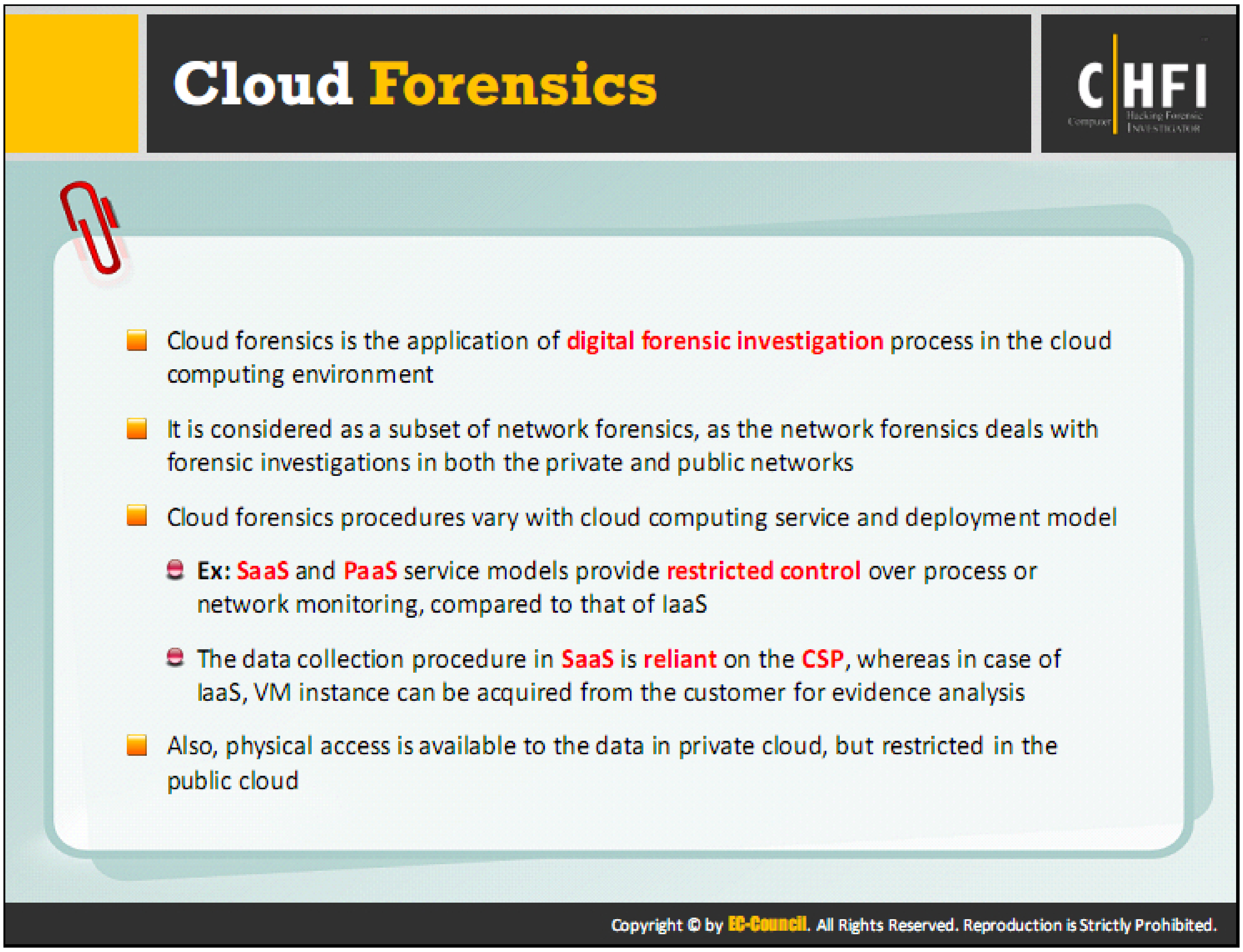
Insecure or obsolete encryption makes cloud services susceptible to cryptanalysis. The cloud may store encrypted data to prevent it from disclosure to malicious users. However critical flaws in cryptographic algorithm implementations (ex: weak random number generation) might turn strong encryption too weak or broken; also there exist novel methods to break the cryptography. Attackers can obtain partial information from encrypted data by monitoring clients' query access patterns and analyzing accessed positions.

DoS and DDoS Attacks

Performing denial-of-service (DoS) attacks on cloud service providers could leave tenants without access to their accounts. In the cloud infrastructure, multi-tenants share CPU, memory, disk space, bandwidth, and so on. Thus, if attackers gain access to the cloud, they generate fake data requests or a type of code that can run applications of legitimate users.

Such malware requests consume server's CPU, memory, and all other devices and once the server reaches its threshold limit, it starts offloading its jobs to another nearest server. The same happens to other inline servers, and finally, the attackers will succeed in engaging the whole cloud system just by interfering the usual processing of one server. This makes legitimate users of the cloud unable to access its services.

If the attacker performs a DoS attack by using a botnet (a network of compromised machines), then it is a DDoS attack. A DDoS attack involves a multitude of compromised systems attacking a single target, thereby causing the denial of service for users of the targeted system.



Cloud Forensics

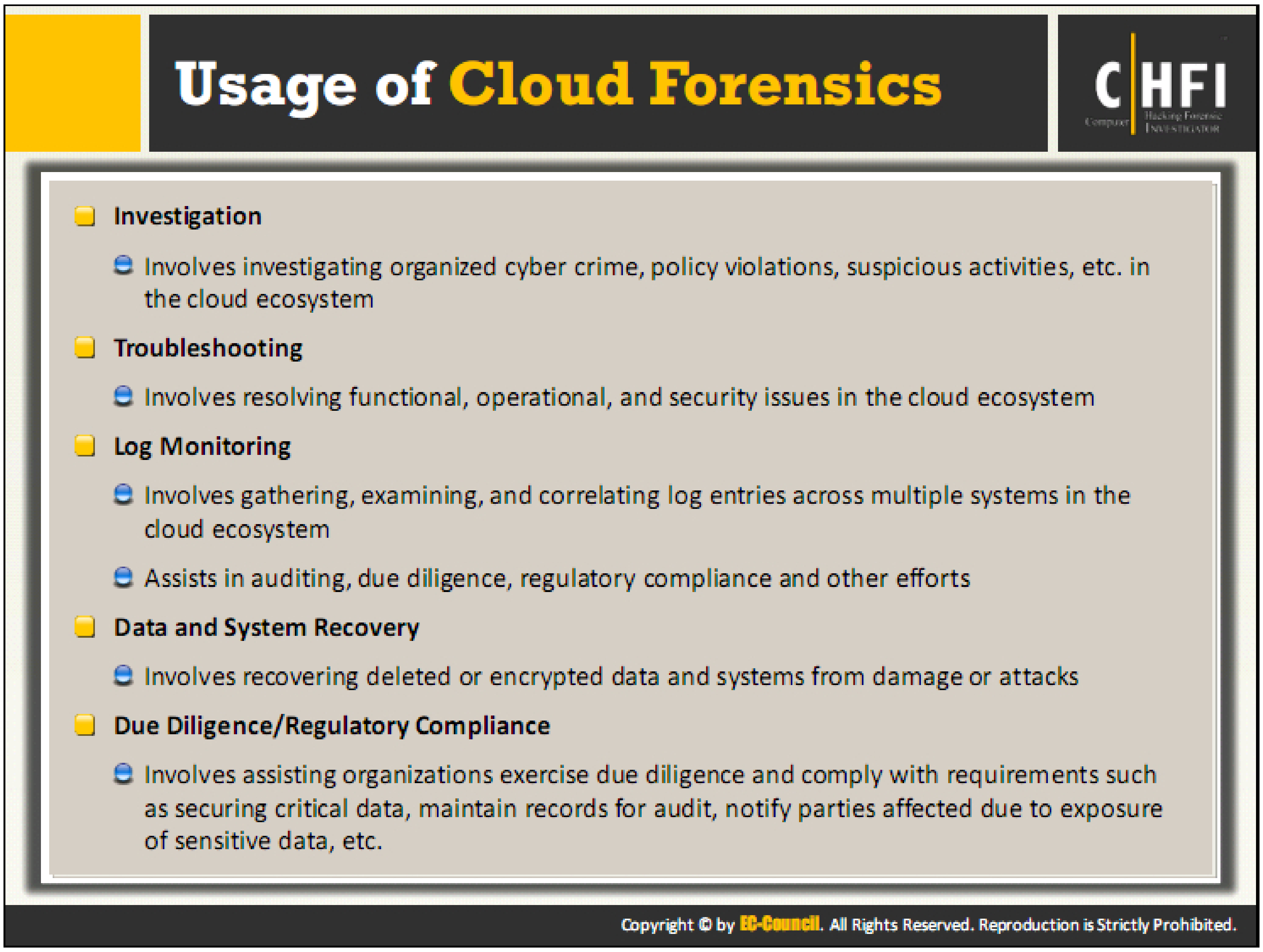
- Cloud forensics is the application of **digital forensic investigation** process in the cloud computing environment
- It is considered as a subset of network forensics, as the network forensics deals with forensic investigations in both the private and public networks
- Cloud forensics procedures vary with cloud computing service and deployment model
  - **Ex:** **SaaS** and **PaaS** service models provide **restricted control** over process or network monitoring, compared to that of IaaS
  - The data collection procedure in **SaaS** is **reliant** on the **CSP**, whereas in case of IaaS, VM instance can be acquired from the customer for evidence analysis
- Also, physical access is available to the data in private cloud, but restricted in the public cloud

Cloud forensics is the application of digital forensic investigation in a cloud environment and a division of network forensics and involves dealing with the public and private networks.

“Digital Forensics is the application of science to the identification, examination, collection, and analysis of data while preserving the information and maintaining a strict chain of custody for the data” according to the NIST.

Cloud computing is spread across the large network and has custom tailored principles. Therefore, the forensic procedures in cloud computing differ according to the service provided and the deployment model.

The initial phases of evidence collection vary from model to model. In SaaS model, the investigators have to completely depend on the CSP for collecting application log. Whereas in IaaS, the investigator can acquire the instance of a virtual machine from the client and initiate the forensics examination and analysis process. Similarly, the cloud forensic examiners can have physical access to the digital evidence in private cloud service, but it is hard to gain physical access to public deployment models.



Usage of Cloud Forensics

- **Investigation**
  - Involves investigating organized cyber crime, policy violations, suspicious activities, etc. in the cloud ecosystem
- **Troubleshooting**
  - Involves resolving functional, operational, and security issues in the cloud ecosystem
- **Log Monitoring**
  - Involves gathering, examining, and correlating log entries across multiple systems in the cloud ecosystem
  - Assists in auditing, due diligence, regulatory compliance and other efforts
- **Data and System Recovery**
  - Involves recovering deleted or encrypted data and systems from damage or attacks
- **Due Diligence/Regulatory Compliance**
  - Involves assisting organizations exercise due diligence and comply with requirements such as securing critical data, maintain records for audit, notify parties affected due to exposure of sensitive data, etc.

Usage of Cloud Forensics

Cloud technology enables users to conveniently access the configurable computing resources (such as servers, applications, services, etc.) on demand for which the cloud service providers need to outsource their private and sensitive data in the cloud. Attackers have been thereby targeting the cloud to gain unauthorized access to this private information. Cloud forensic techniques help forensic practitioners and also everyday users to handle and protect themselves from such security incidents.

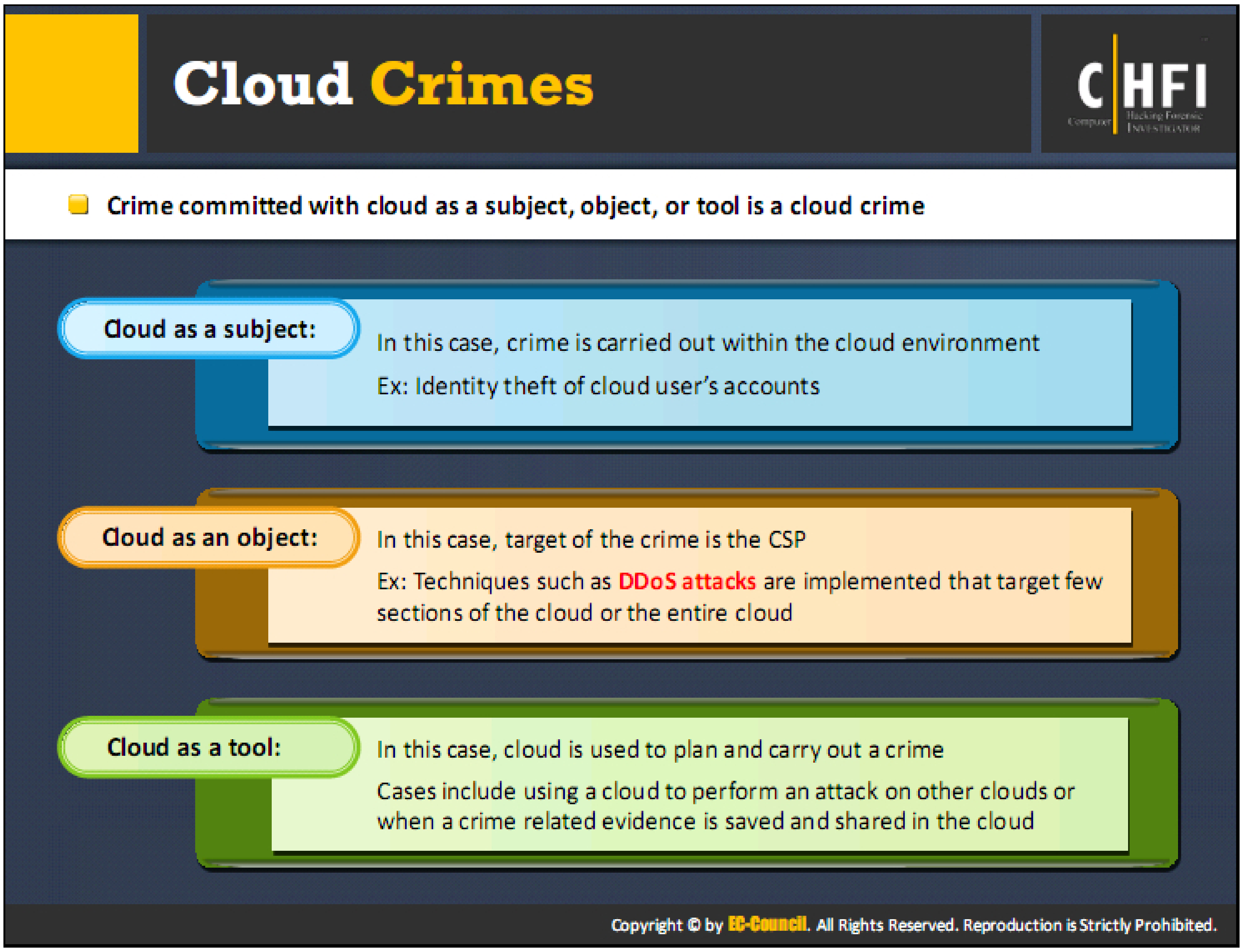
Cloud forensics has many uses like:

- **Investigation:** Cloud forensics will help in finding the source of different cloud-based crimes and solving organized cloud crimes, policy violations in a public environment, and suspicious activities that happen in the cloud environment. The process will investigate all the sources including mechanical or manual and reveal the results, which would help clients and service providers to secure their cloud services.
- **Troubleshooting:** Cloud forensic techniques assist users in troubleshooting process when an incident has taken place, through determining the data and hosts physically and virtually present in a cloud environment. They allow users to find and resolve any errors, and security issues in the cloud. They help in understanding the trends of the past security attacks so as to tackle any incident in the future.
- **Log Monitoring:** Cloud forensic techniques include the processes to generate, store, analyze, and correlate the massive volumes of log data created within a cloud

environment. This data helps the users and service providers to audit, analyze and calculate various aspects of cloud environment as well as helps the security officials to keep in check if the cloud complies with the regulatory standards.

- **Data and System Recovery:** Cloud forensics involves recovery procedures that help the forensic practitioners in recovering lost, accidentally deleted, corrupted and inaccessible data. It also allows data acquisition of cloud systems and creation of a forensic copy of the data that the service providers can use as back up and forensics experts can produce as evidence in the court of law.

- **Due Diligence/Regulatory Compliance:** Cloud forensics also deals with the security aspects of an organization in securing critical data, maintaining necessary records for auditing purposes, and notifying the concerned team when any suspicious activity has been reported, for instance, any private data has been misused or exposed, etc. It also helps to find the sections that miss the regulatory compliance and tune them to be in accordance with the standards.



Cloud Crimes

- Crime committed with cloud as a subject, object, or tool is a cloud crime

Cloud as a subject: In this case, crime is carried out within the cloud environment

Ex: Identity theft of cloud user's accounts

Cloud as an object: In this case, target of the crime is the CSP

Ex: Techniques such as DDoS attacks are implemented that target few sections of the cloud or the entire cloud

Cloud as a tool: In this case, cloud is used to plan and carry out a crime

Cases include using a cloud to perform an attack on other clouds or when a crime related evidence is saved and shared in the cloud

Any criminal activity that involves a cloud environment may it be a subject, object or a tool, is a cloud crime.

Cloud as a subject

It refers to a crime in which the attackers try to compromise the security of a cloud environment to steal data or inject a malware.

Ex: Identity theft of cloud user's accounts, unauthorized modification or deletion of data stored in the Cloud, installation of malware on the cloud, etc.

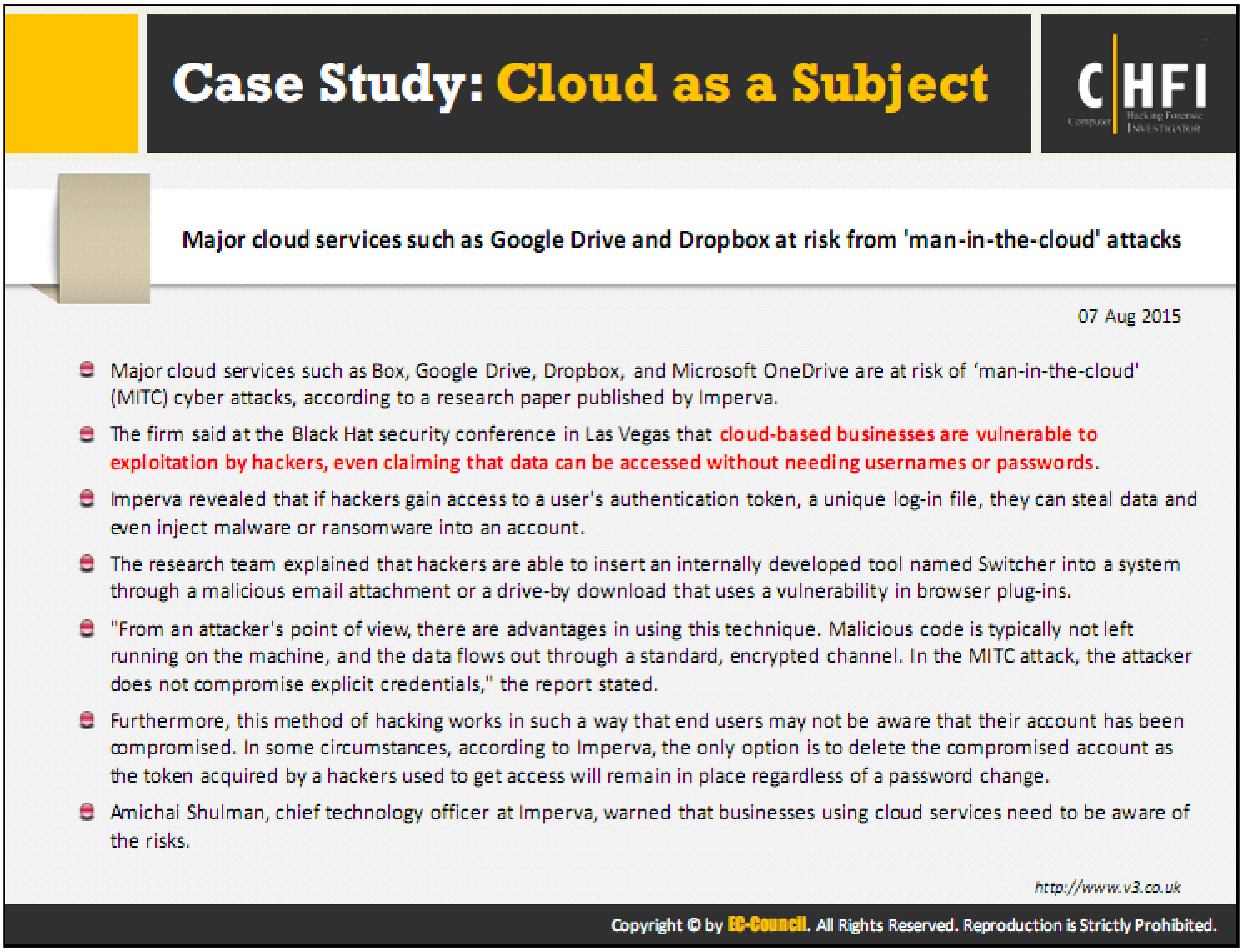
Cloud as an object

In a cloud crime, the cloud behaves like an object, when the attacker uses the cloud to commit a crime targeted towards the CSP. In this case, the main aim of the attacker is to impact cloud service provider than cloud environment.

Ex: DDoS attacks over the cloud that can bring the whole cloud down.

Cloud as a tool

In a cloud crime, the cloud becomes a tool when the attacker uses one compromised cloud account to attack other accounts. In such cases, both the source and target cloud can store the evidence data.



Case Study: Cloud as a Subject

Major cloud services such as Google Drive and Dropbox at risk from 'man-in-the-cloud' attacks

07 Aug 2015

- Major cloud services such as Box, Google Drive, Dropbox, and Microsoft OneDrive are at risk of 'man-in-the-cloud' (MITC) cyber attacks, according to a research paper published by Imperva.
- The firm said at the Black Hat security conference in Las Vegas that cloud-based businesses are vulnerable to exploitation by hackers, even claiming that data can be accessed without needing usernames or passwords.
- Imperva revealed that if hackers gain access to a user's authentication token, a unique log-in file, they can steal data and even inject malware or ransomware into an account.
- The research team explained that hackers are able to insert an internally developed tool named Switcher into a system through a malicious email attachment or a drive-by download that uses a vulnerability in browser plug-ins.
- "From an attacker's point of view, there are advantages in using this technique. Malicious code is typically not left running on the machine, and the data flows out through a standard, encrypted channel. In the MITC attack, the attacker does not compromise explicit credentials," the report stated.
- Furthermore, this method of hacking works in such a way that end users may not be aware that their account has been compromised. In some circumstances, according to Imperva, the only option is to delete the compromised account as the token acquired by a hackers used to get access will remain in place regardless of a password change.
- Amichai Shulman, chief technology officer at Imperva, warned that businesses using cloud services need to be aware of the risks.

http://www.v3.co.uk

Major cloud services such as Google Drive and Dropbox at risk from 'man-in-the-cloud' attacks

Source: *http://www.v3.co.uk*

Major cloud services such as Box, Google Drive, Dropbox and Microsoft OneDrive are at risk of 'man-in-the-cloud' (MITC) cyber attacks, according to a research paper published by Imperva.

The firm said at the Black Hat security conference in Las Vegas that cloud-based businesses are vulnerable to exploitation by hackers, even claiming that data can be accessed without needing usernames or passwords.

Imperva revealed that if hackers gain access to a user's authentication token, a unique log-in file, they can steal data and even inject malware or ransomware into an account.

The research team explained that hackers can insert an internally developed tool named Switcher into a system through a malicious email attachment or a drive-by download that uses vulnerability in browser plug-ins.

"From an attacker's point of view, there are advantages in using this technique. Malicious code is typically not left running on the machine, and the data flows out through a standard, encrypted channel. In the MITC attack, the attacker does not compromise explicit credentials," the report stated.

Furthermore, this method of hacking works in such a way that end users may not be aware that their account has been compromised.

In some circumstances, according to Imperva, the only option is to delete the compromised account as the token acquired by hackers used to get access will remain in place regardless of a password change.

The report said that it is unlikely that an unsuspecting victim who is not carefully monitoring "device-sync activity" will detect an intrusion.

"It is extremely difficult to recover from an attack once it is detected, and may require the victim to cancel the existing account and open a new one," Imperva said.

Amichai Shulman, chief technology officer at Imperva, warned that businesses using cloud services need to be aware of the risks.

"Since we have found evidence of MITC in the wild, organizations that rely on protecting against infection through malicious code detection or command and control communication detection are at a serious risk," he told V3.

"Taking over an endpoint is only putting the foot in the door. Attackers are usually after corporate data stored in databases and file servers and processed through business applications."

Meanwhile, Itsik Mantin, director of security research at Imperva, told V3 that the new attack is "almost invisible" from the user's perspective.

However, he noted that "for some of the cloud services examined, the user may receive notification mail from the cloud service, notifying that the account was accessed from a new device or new geo-location".

Mantin added: "Personal cloud services like Dropbox give the attackers new ways to get into the organization, and in the new attack to smooth their way to the victim's data and ease the exfiltration of the data to the attacker's premises."

Tim Erlin, director of security and product management at Tripwire, explained that the "end game" of this sort of attack could vary.

"MITC provides the attacker with a functional capability to exfiltrate data from and deliver data to a system. That capability can have many uses for an attacker, from stealing sensitive information to delivering malware," he told V3.

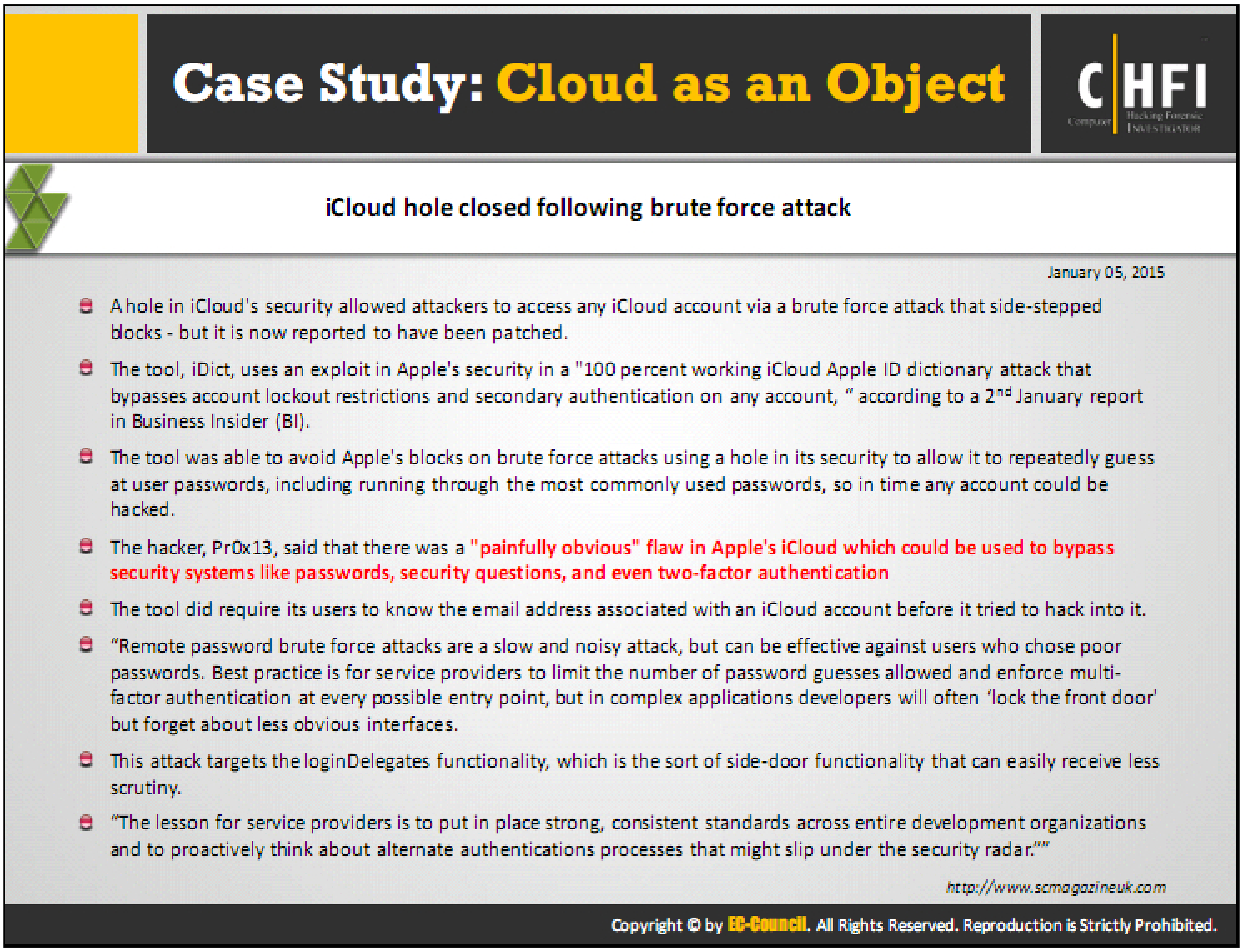
Erlin stressed that the MITC attack "has to start with some other attack to execute the initial Switcher code", and that "individual users should avoid clicking on files they're not sure of".

"The capabilities afforded by the cloud provide advantaged and additional risk. If we find a tool useful for business, we should expect attackers will too because cybercrime is, after all, big business," he warned.

V3 contacted a number of the companies involved in the study for comment but received no replies by the time of publication.

A strain of malware originating in Russia called Hammertoss was recently discovered that also uses cloud-based attacks.

The malware uses Twitter, GitHub and cloud storage systems to relay commands and extract data from compromised networks.



Case Study: Cloud as an Object

iCloud hole closed following brute force attack

January 05, 2015

- A hole in iCloud's security allowed attackers to access any iCloud account via a brute force attack that side-stepped blocks - but it is now reported to have been patched.
- The tool, iDict, uses an exploit in Apple's security in a "100 percent working iCloud Apple ID dictionary attack that bypasses account lockout restrictions and secondary authentication on any account, " according to a 2nd January report in Business Insider (BI).
- The tool was able to avoid Apple's blocks on brute force attacks using a hole in its security to allow it to repeatedly guess at user passwords, including running through the most commonly used passwords, so in time any account could be hacked.
- The hacker, Pr0x13, said that there was a "painfully obvious" flaw in Apple's iCloud which could be used to bypass security systems like passwords, security questions, and even two-factor authentication
- The tool did require its users to know the email address associated with an iCloud account before it tried to hack into it.
- "Remote password brute force attacks are a slow and noisy attack, but can be effective against users who chose poor passwords. Best practice is for service providers to limit the number of password guesses allowed and enforce multi-factor authentication at every possible entry point, but in complex applications developers will often 'lock the front door' but forget about less obvious interfaces.
- This attack targets the loginDelegates functionality, which is the sort of side-door functionality that can easily receive less scrutiny.
- "The lesson for service providers is to put in place strong, consistent standards across entire development organizations and to proactively think about alternate authentications processes that might slip under the security radar.""

http://www.scmagazineuk.com

iCloud hole closed following brute force attack

Source: http://www.scmagazineuk.com

A hole in iCloud's security allowed attackers to access any iCloud account via a brute force attack that side-stepped blocks - but it is now reported to have been patched.

2015 began, predictably, with a major hack of a global service provider, when on New Year's Day a tool to hack all accounts on Apple's iCloud was announced – via a vulnerability reported today to have been fixed.

The tool, iDict, (see iDict's GitHub page) uses an exploit in Apple's security in a "100 percent working iCloud Apple ID dictionary attack that bypasses account lockout restrictions and secondary authentication on any account, " according to a 2nd January report in Business Insider (BI).

The tool was able to avoid Apple's blocks on brute force attacks using a hole in its security to allow it to repeatedly guess at user passwords, including running through the most commonly used passwords, so in time any account could be hacked.

The hacker, Pr0x13, said that there was a "painfully obvious" flaw in Apple's iCloud which could be used to bypass security systems like passwords, security questions, and even two-factor authentication

Apple did respond quickly, and it was reported on 2nd January that people trying to use the service were causing iCloud accounts to be locked for security, preventing hackers from gaining access.

The tool did require its users to know the email address associated with an iCloud account before it tried to hack into it.

Michele Borovac, VP at HyTrust (www.hytrust.com), the cloud control company commented to the press: "Dictionary attacks have been around for a long time. The reality is that passwords can be broken given enough time and compute power. This makes the practice of using two-factor authentication even more critical for any account that holds sensitive data. Two-factor authentication combines something you know - like a password- with something you have - a token, or similar."

"As these types if attacks proliferate, we will see companies introduce two-factor authentication methods as a baseline part of their security offerings."

Patrick Thomas, security consultant at Neohapsis (www.neohapsis.com), a security and risk management consulting company specializing in mobile and cloud security services, adds: "If valid, this is an attack technique and vulnerability almost identical to the weakness in the 'Find my iPhone' used in the iCloud breach which compromised celebrity photos in August.

"Remote password brute force attacks are a slow and noisy attack, but can be effective against users who chose poor passwords. Best practice is for service providers to limit the number of password guesses allowed and enforce multi-factor authentication at every possible entry point, but in complex applications developers will often 'lock the front door' but forget about less obvious interfaces.

"This attack targets the login Delegates functionality, which is the sort of side-door functionality that can easily receive less scrutiny.

"The lesson for service providers is to put in place strong, consistent standards across entire development organizations and to proactively think about alternate authentications processes that might slip under the security radar."

Nathaniel Couper-Noles, the senior security consultant at Neohapsis (www.neohapsis.com), suggests the problem is the inherent weakness of passwords and concludes there is no ideal solution: "In economics, this problem is addressed in classical principal-agent theory. Passwords are hard to work with, and by design there is an inherent information asymmetry. Users will be prone to exercise 'economy of effort' (e.g., selecting weak passwords or reusing passwords).

"Principal-agent theory suggests alternatives, none of which is a perfect fit:

1. Reducing the information asymmetry. For example:

   Forcing users to disclose their passwords to external sites and auditing compliance. In addition to the obvious ethical problems, this is illegal in some jurisdictions.

Merely asking users whether they reuse their passwords and engaging collaboratively with them to understand and address the problem. This relies on users to self-report, but a collaborative approach may yield better results than empty threats.

2. Forcing users to select complex passwords and rotate them periodically. This turns the users' economy of effort against them because now they will have to update external sites if they are hell-bent on reusing passwords. But in so doing, it increases the total effort of maintaining complex passwords. This happens to be a standard recommendation in information security circles.

3. Automating processes and creating separate machine or process accounts for internal systems wherever feasible (essentially cutting users out of the loop and minimizing access). Process automation necessitates capital investment, which is potentially cost prohibitive, but may proceed at its own rate as technology advances.

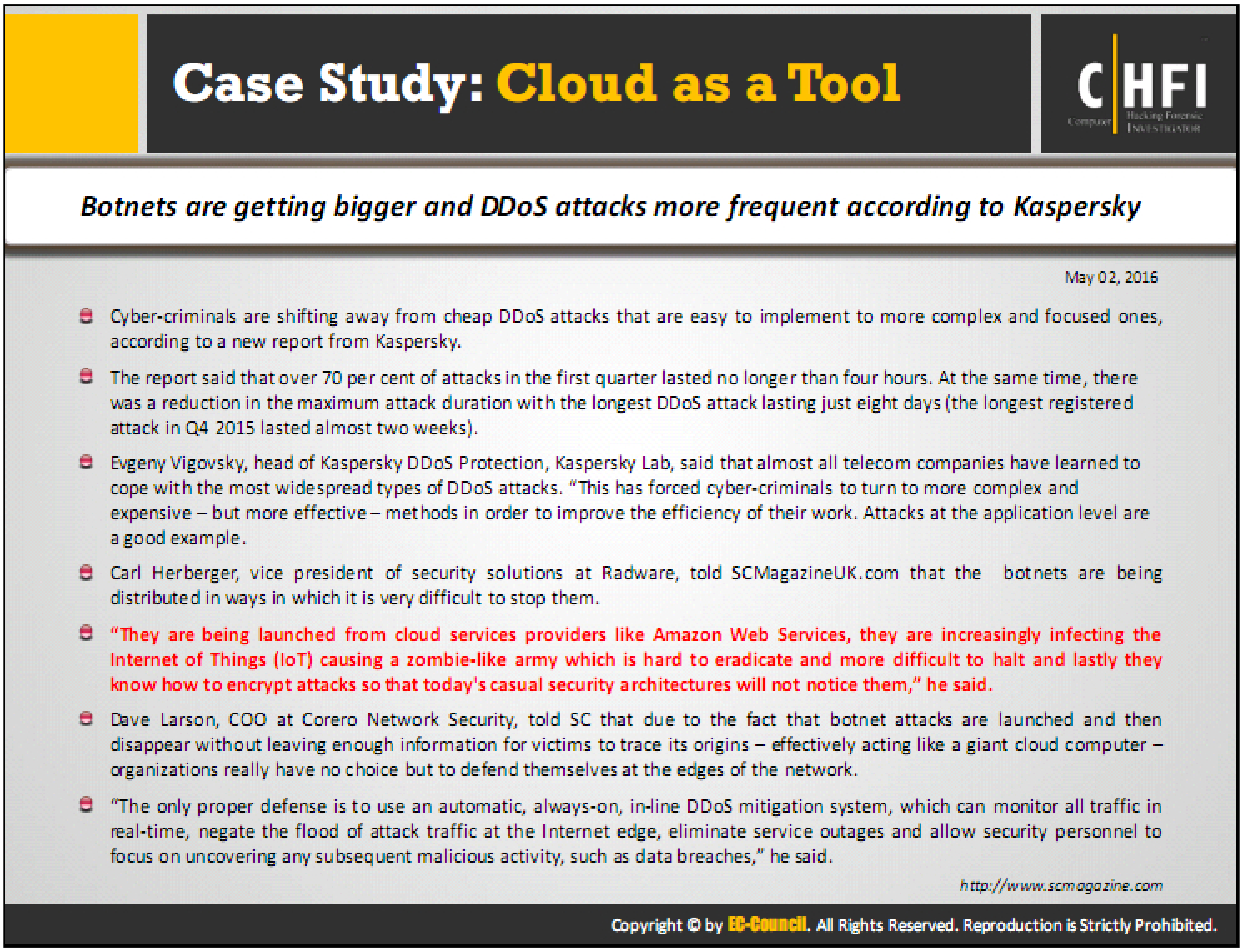
4. Restricting user access to outside (e.g., social media) sites, such as by blocking access while at work. This doesn't prevent users from re-using passwords on prohibited sites while they are not at work or while they are using personal devices. Plus it's not entirely practical - many legitimate business processes across industries will involve external sites (e.g., vendor, supplier, and regulatory systems).

5. Eschewing passwords for enterprise use. It is not practical for most enterprises to eliminate passwords entirely, but single-sign-on, key management, alternative authentication and centralized password systems can at least reduce the difficulty of remembering many passwords.

   Alternative authentication schemes, such as certificates, two-factor authentication systems, biometrics and identity card (smart card) systems all have their own drawbacks, but many have seen limited adoption.

6. Deferred compensation - incentivizing users somehow, perhaps by linking part of compensation or other awards, benefits or incentives to whether the users' password was breached in a third party website. This might mean checking lists of breached sites and accounts, which itself may involve accessing shady parts of the internet.

As you can see, none of these is a perfect solution.”



Case Study: Cloud as a Tool

Botnets are getting bigger and DDoS attacks more frequent according to Kaspersky

May 02, 2016

- Cyber-criminals are shifting away from cheap DDoS attacks that are easy to implement to more complex and focused ones, according to a new report from Kaspersky.
- The report said that over 70 per cent of attacks in the first quarter lasted no longer than four hours. At the same time, there was a reduction in the maximum attack duration with the longest DDoS attack lasting just eight days (the longest registered attack in Q4 2015 lasted almost two weeks).
- Evgeny Vigovsky, head of Kaspersky DDoS Protection, Kaspersky Lab, said that almost all telecom companies have learned to cope with the most widespread types of DDoS attacks. "This has forced cyber-criminals to turn to more complex and expensive – but more effective – methods in order to improve the efficiency of their work. Attacks at the application level are a good example.
- Carl Herberger, vice president of security solutions at Radware, told SCMagazineUK.com that the botnets are being distributed in ways in which it is very difficult to stop them.
- **"They are being launched from cloud services providers like Amazon Web Services, they are increasingly infecting the Internet of Things (IoT) causing a zombie-like army which is hard to eradicate and more difficult to halt and lastly they know how to encrypt attacks so that today's casual security architectures will not notice them," he said.**
- Dave Larson, COO at Corero Network Security, told SC that due to the fact that botnet attacks are launched and then disappear without leaving enough information for victims to trace its origins – effectively acting like a giant cloud computer – organizations really have no choice but to defend themselves at the edges of the network.
- "The only proper defense is to use an automatic, always-on, in-line DDoS mitigation system, which can monitor all traffic in real-time, negate the flood of attack traffic at the Internet edge, eliminate service outages and allow security personnel to focus on uncovering any subsequent malicious activity, such as data breaches," he said.

http://www.scmagazine.com

Botnets are getting bigger and DDoS attacks more frequent according to Kaspersky

Source: *http://www.scmagazine.com*

Cyber-criminals are shifting away from cheap DDoS attacks that are easy to implement to more complex and focused ones, according to a new report from Kaspersky.

In its quarterly DDoS Intelligence report, the firm said that there was also a nearly fourfold increase in the number of DDoS attacks. Around 74 countries were targeted by DDoS attacks in Q1 and as in the previous quarter, the vast majority of those resources were located in just ten countries, with Ukraine, Germany and France all making a new appearance.

The report said that over 70 per cent of attacks in the first quarter lasted no longer than four hours. At the same time, there was a reduction in the maximum attack duration with the longest DDoS attack lasting just eight days (the longest registered attack in Q4 2015 lasted almost two weeks). During the reporting period, the maximum number of attacks against a single target increased: 33 attacks compared to 24 in the previous quarter.

However, a fall was reported in the number of attacks targeting communication channels, accompanied by an increase in the number of application-layer attacks. The firm suggested amplification attacks, which regained popularity last year, have begun to lose their appeal.

The confirmed a trend towards reduced duration and increased frequency combined with greater complexity. During the first three months of the year, Kaspersky Lab resources countered almost as many attacks as the whole of 2015. The majority of those attacks were also short-lived application-layer attacks.

Evgeny Vigovsky, head of Kaspersky DDoS Protection, Kaspersky Lab, said that almost all telecom companies have learned to cope with the most widespread (and, as a rule, technologically ‘simple') types of DDoS attacks.

“This has forced cyber-criminals to turn to more complex and expensive – but more effective – methods in order to improve the efficiency of their work. Attacks at the application level are a good example.

“Only a highly professional anti-DDoS solution with an intelligent junk-filtering algorithm is capable of detecting genuine user requests from the general flow. That's why companies, especially those whose business depends on the availability of online services, can no longer rely solely on the capabilities of an Internet provider,” he added.

Carl Herberger, vice president of security solutions at Radware, told SCMagazineUK.com that the botnets are being distributed in ways in which it is very difficult to stop them.

“They are being launched from cloud services providers like Amazon Web Services, they are increasingly infecting the Internet of Things (IoT) causing a zombie-like army which is hard to eradicate and more difficult to halt and lastly they know how to encrypt attacks so that today's casual security architectures will not notice them,” he said.

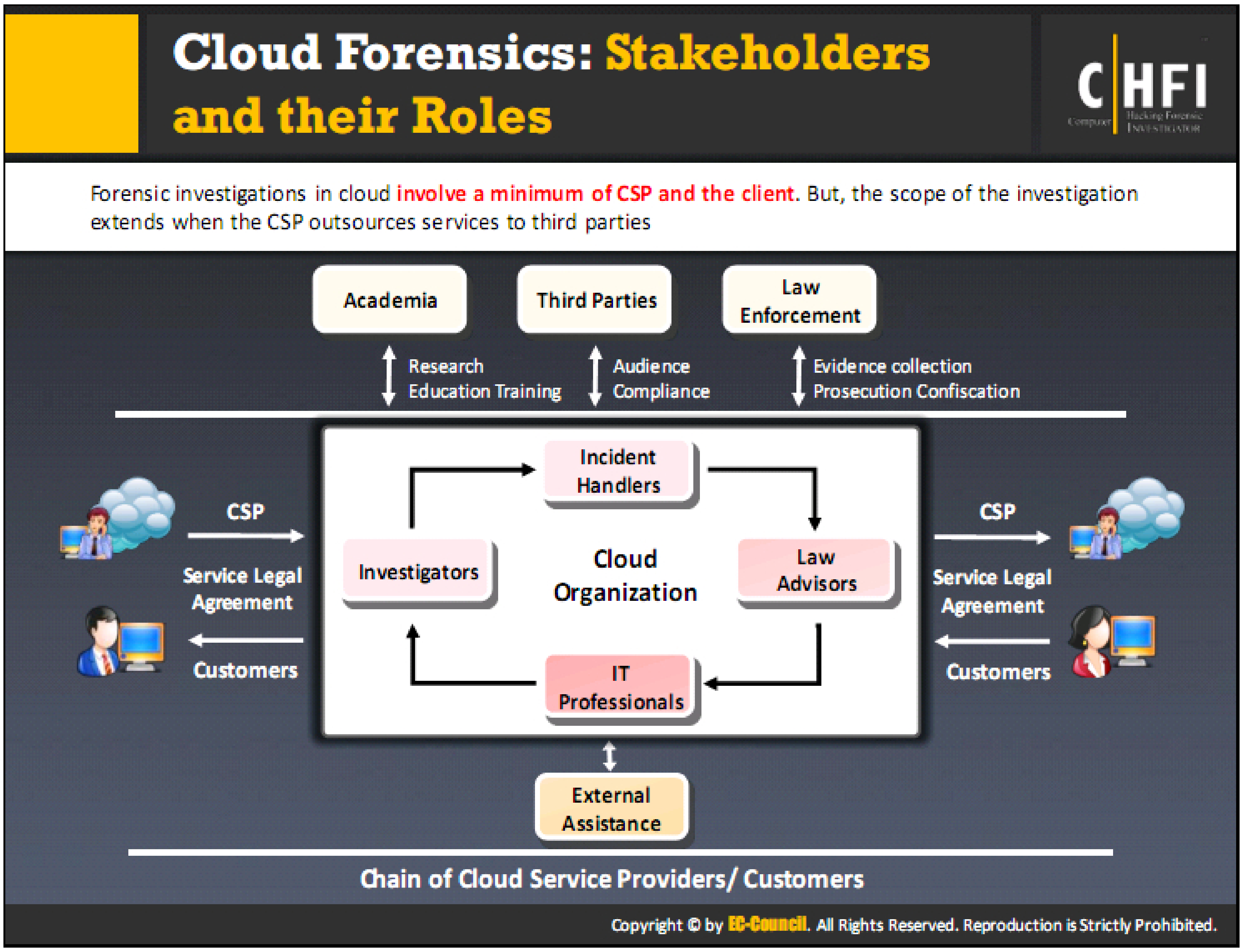
Dave Larson, COO at Corero Network Security, told SC that due to the fact that botnet attacks are launched and then disappear without leaving enough information for victims to trace its origins – effectively acting like a giant cloud computer – organisations really have no choice but to defend themselves at the edges of the network.

“The only proper defence is to use an automatic, always-on, in-line DDoS mitigation system, which can monitor all traffic in real-time, negate the flood of attack traffic at the Internet edge, eliminate service outages and allow security personnel to focus on uncovering any subsequent malicious activity, such as data breaches,” he said.

James Henry, UK Southern Manager at Auriga Consulting, told SC that most organisations simply seek to batten down the hatches when it comes to a DDoS attack and hope for the best.

“Their security stance is defensive, not proactive, and few have access to the kind of intelligence that would provide them with the forewarning needed to weather and rapidly recover from these attacks,” he said.

“That's because the monitoring of botnet activity and accompanying chatter on legitimate and deep web social media networks and forums that typically precedes these types of attack simply isn't being monitored. Like an incoming storm, there are always signs to indicate and forecast DDoS attacks if you know how to read them but you need access to that data,” added Henry.



Cloud Forensics: Stakeholders and their Roles

Forensic investigations in cloud involve a minimum of CSP and the client. But, the scope of the investigation extends when the CSP outsources services to third parties

Academia
Research
Education Training

Third Parties
Audience
Compliance

Law Enforcement
Evidence collection
Prosecution Confiscation

CSP
Service Legal Agreement
Customers

Cloud Organization
Incident Handlers
Law Advisors
IT Professionals
Investigators

CSP
Service Legal Agreement
Customers

External Assistance

Chain of Cloud Service Providers/ Customers

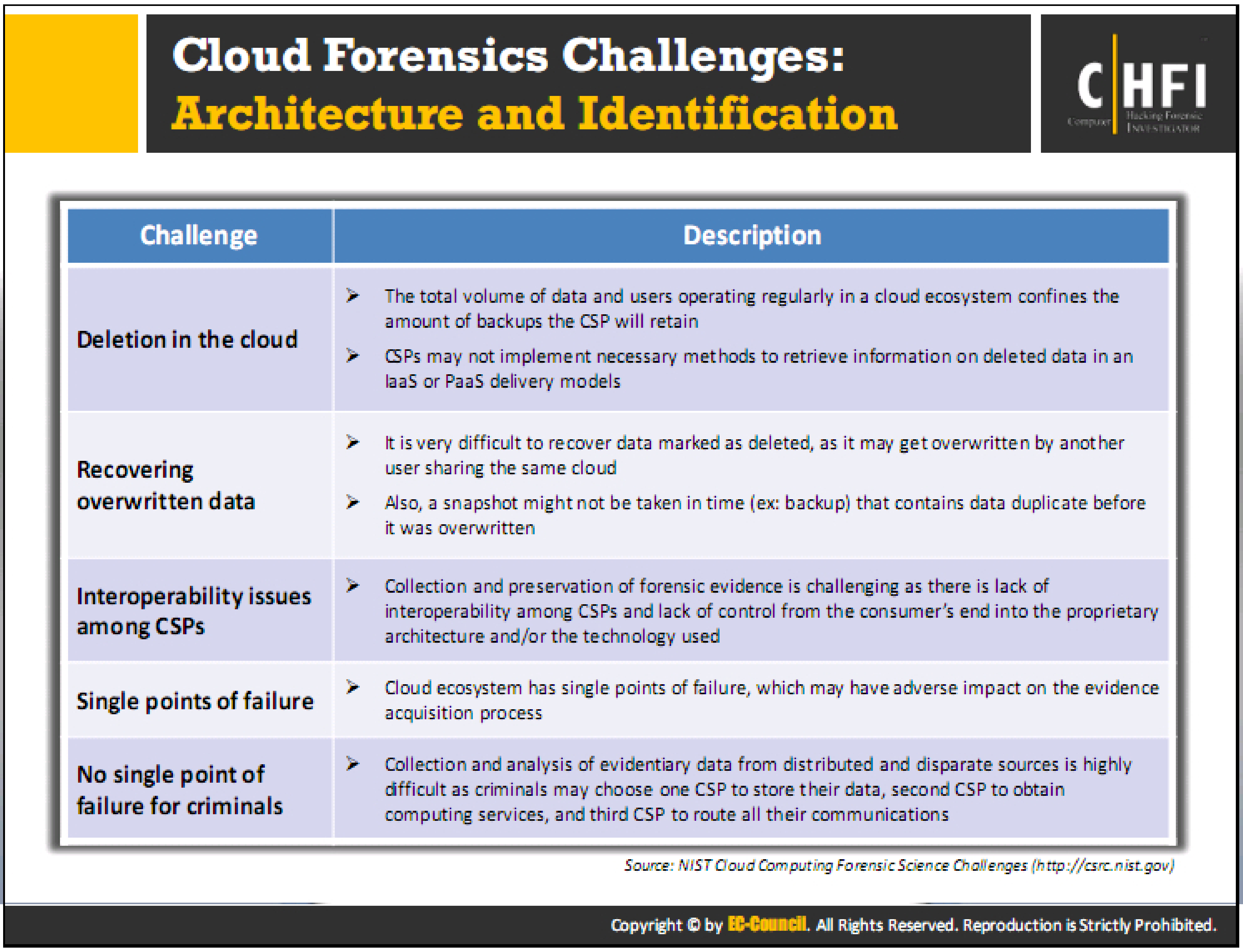
A cloud forensic activity consists of many stakeholders including government members, industry partners, third parties, law enforcement, etc. Investigators should be able to understand the roles and responsibilities of each stakeholder for effective investigation. This will also help the investigators find the technical, legal, and organizational stakeholders as well as allocate and document their interests and generate reports accordingly. It will also help in the management of the different tasks of the cloud and the responsibilities when signing the contract.

To enable forensic capability of the cloud, a proper internal structure should be present involving the CSPs and the customers, a define collaboration between the CSP and customer, and also an external assistance which accomplishes the following roles:

- **IT Professionals:** This team includes professionals responsible for managing and maintaining all the aspects of the cloud, such as cloud security architects, network administrators, security administrators, ethical hackers, etc. They are capable of providing knowledge about the functioning of the cloud, assist the investigators and can help in data collection. They may also be questionable in case of internal attacks.

- **Investigators:** The investigators in a cloud organization are responsible for conducting forensic examinations against allegations made regarding wrongdoings, found vulnerabilities and during attacks over the cloud. They should also work in collaboration with the external investigators, law enforcement agencies for forensic investigations on the internal assets.

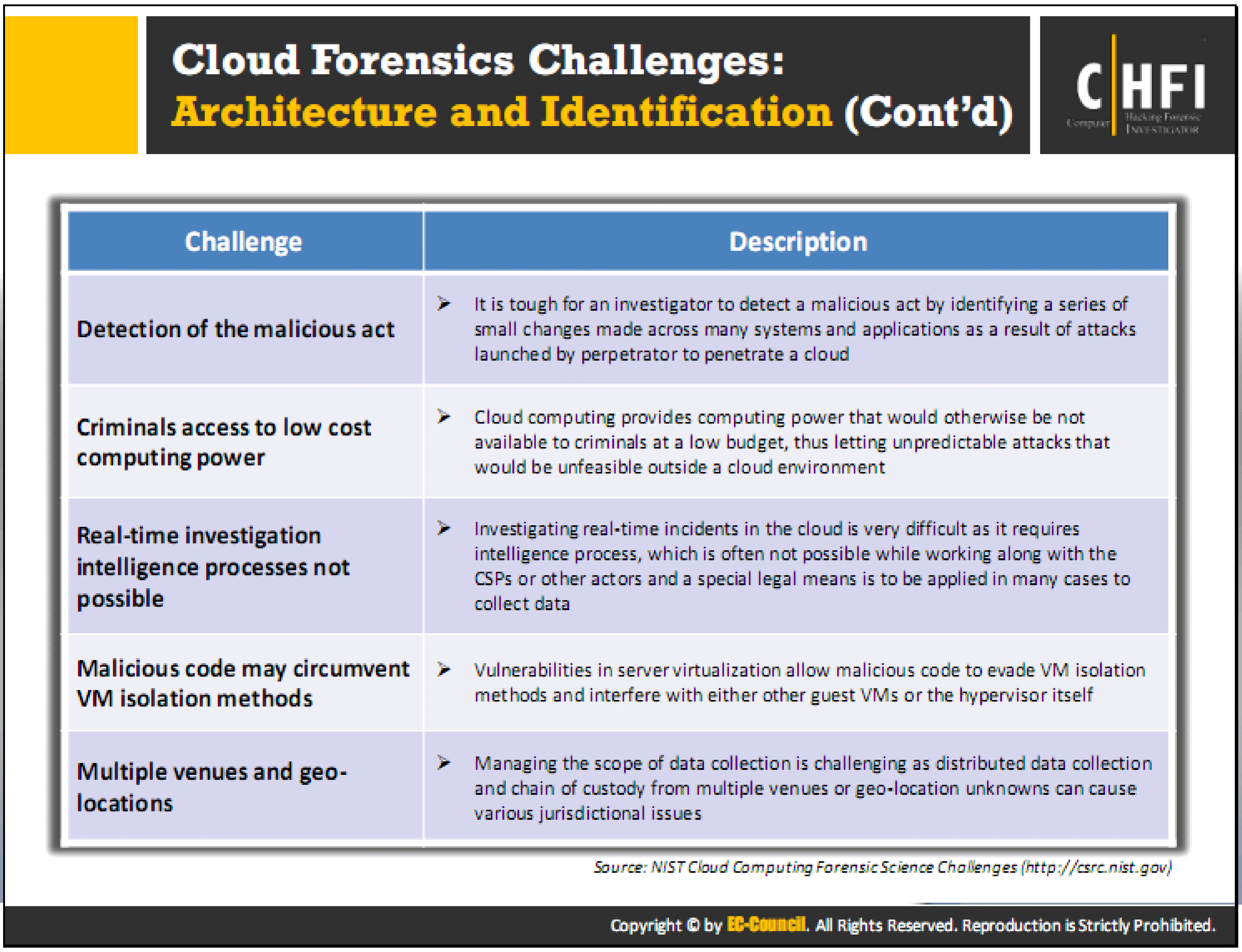
- **Incident Handlers:** The incident handlers are the first responders for all the security incidents taking place on a cloud. They are the first line of defense against cloud security attacks and their primary role is to respond against any type of security incident immediately.
- **Law Advisors:** The key responsibility of the law advisors is to make sure that all the forensic activities are within the jurisdiction and not violating any regulations or agreements.
- **External Assistance:** The role of external assistance comes when the internal team requires an external support in performing any task apart from the once which they have already performed, such as investigation of civil cases, e-discovery, etc. Before taking external assistance, the internal team should be clear enough about forensic activities the external assistance needs to perform.



Cloud Forensics Challenges: Architecture and Identification

Challenge	Description
Deletion in the cloud	➢ The total volume of data and users operating regularly in a cloud ecosystem confines the amount of backups the CSP will retain ➢ CSPs may not implement necessary methods to retrieve information on deleted data in an IaaS or PaaS delivery models
Recovering overwritten data	➢ It is very difficult to recover data marked as deleted, as it may get overwritten by another user sharing the same cloud ➢ Also, a snapshot might not be taken in time (ex: backup) that contains data duplicate before it was overwritten
Interoperability issues among CSPs	➢ Collection and preservation of forensic evidence is challenging as there is lack of interoperability among CSPs and lack of control from the consumer's end into the proprietary architecture and/or the technology used
Single points of failure	➢ Cloud ecosystem has single points of failure, which may have adverse impact on the evidence acquisition process
No single point of failure for criminals	➢ Collection and analysis of evidentiary data from distributed and disparate sources is highly difficult as criminals may choose one CSP to store their data, second CSP to obtain computing services, and third CSP to route all their communications

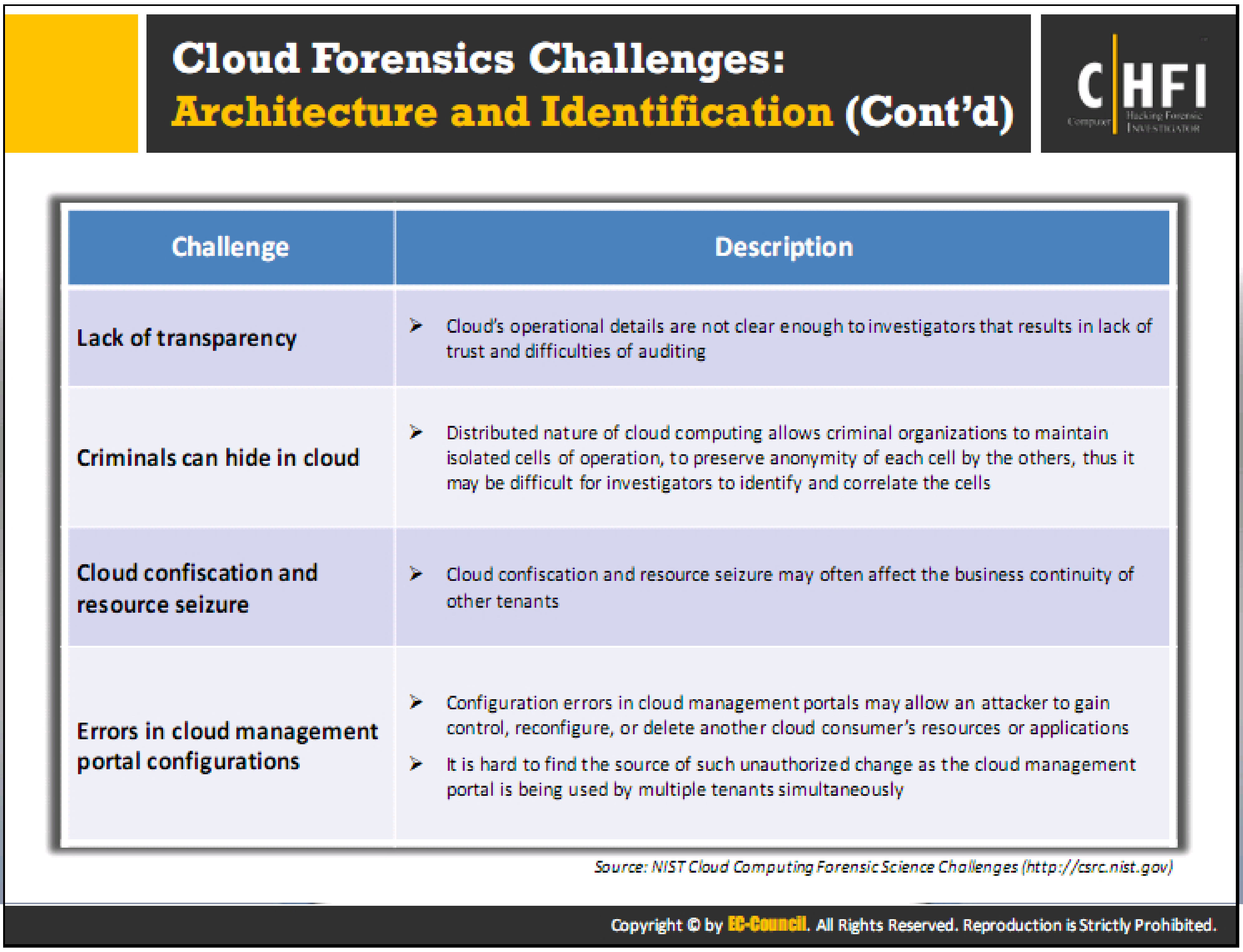
Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)



Cloud Forensics Challenges: Architecture and Identification (Cont'd)

Challenge	Description
Detection of the malicious act	➢ It is tough for an investigator to detect a malicious act by identifying a series of small changes made across many systems and applications as a result of attacks launched by perpetrator to penetrate a cloud
Criminals access to low cost computing power	➢ Cloud computing provides computing power that would otherwise be not available to criminals at a low budget, thus letting unpredictable attacks that would be unfeasible outside a cloud environment
Real-time investigation intelligence processes not possible	➢ Investigating real-time incidents in the cloud is very difficult as it requires intelligence process, which is often not possible while working along with the CSPs or other actors and a special legal means is to be applied in many cases to collect data
Malicious code may circumvent VM isolation methods	➢ Vulnerabilities in server virtualization allow malicious code to evade VM isolation methods and interfere with either other guest VMs or the hypervisor itself
Multiple venues and geo-locations	➢ Managing the scope of data collection is challenging as distributed data collection and chain of custody from multiple venues or geo-location unknowns can cause various jurisdictional issues

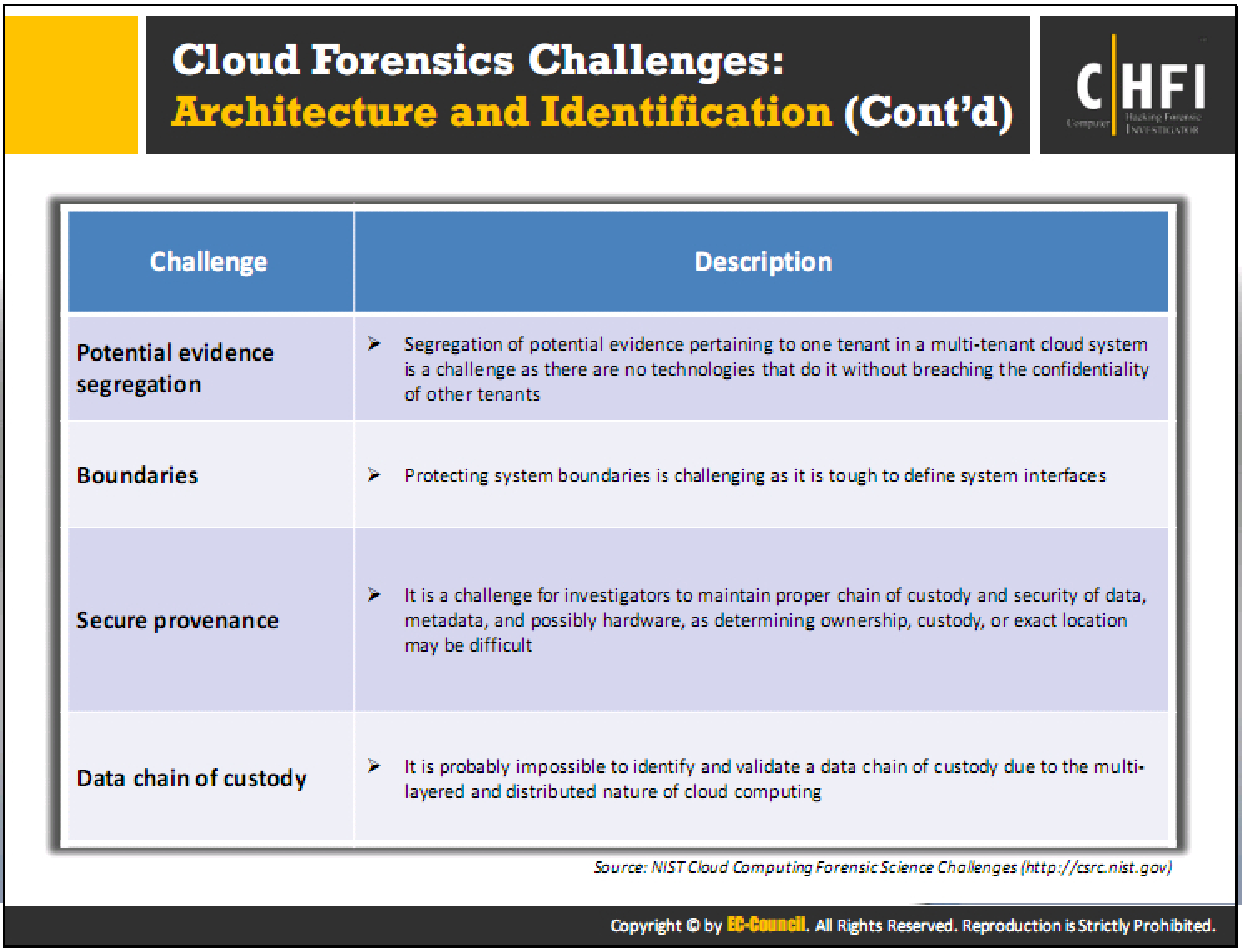
Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)



Cloud Forensics Challenges: Architecture and Identification (Cont'd)

Challenge	Description
Lack of transparency	➤ Cloud's operational details are not clear enough to investigators that results in lack of trust and difficulties of auditing
Criminals can hide in cloud	➤ Distributed nature of cloud computing allows criminal organizations to maintain isolated cells of operation, to preserve anonymity of each cell by the others, thus it may be difficult for investigators to identify and correlate the cells
Cloud confiscation and resource seizure	➤ Cloud confiscation and resource seizure may often affect the business continuity of other tenants
Errors in cloud management portal configurations	➤ Configuration errors in cloud management portals may allow an attacker to gain control, reconfigure, or delete another cloud consumer's resources or applications ➤ It is hard to find the source of such unauthorized change as the cloud management portal is being used by multiple tenants simultaneously

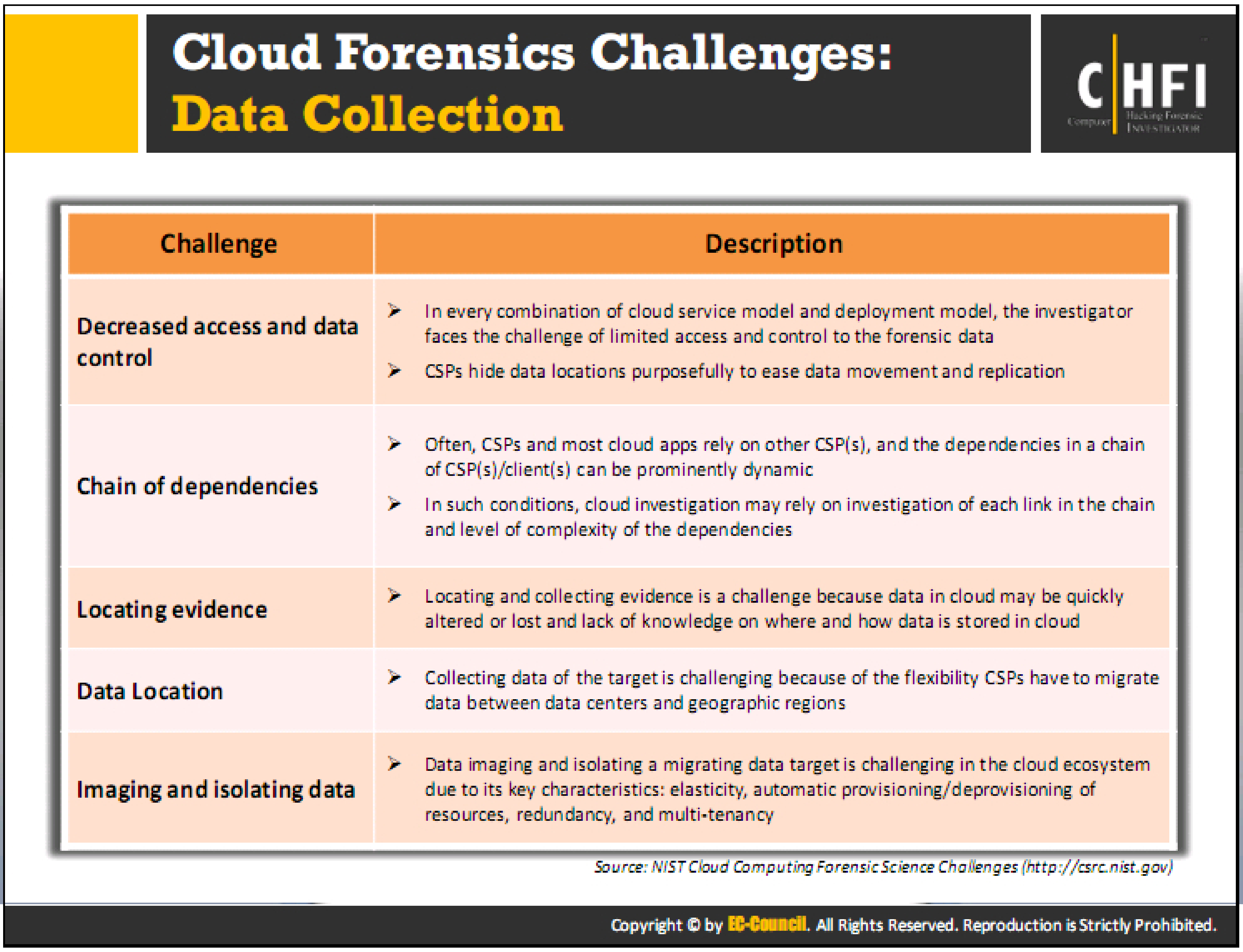
Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)



Cloud Forensics Challenges: Architecture and Identification (Cont'd)

Challenge	Description
Potential evidence segregation	➤ Segregation of potential evidence pertaining to one tenant in a multi-tenant cloud system is a challenge as there are no technologies that do it without breaching the confidentiality of other tenants
Boundaries	➤ Protecting system boundaries is challenging as it is tough to define system interfaces
Secure provenance	➤ It is a challenge for investigators to maintain proper chain of custody and security of data, metadata, and possibly hardware, as determining ownership, custody, or exact location may be difficult
Data chain of custody	➤ It is probably impossible to identify and validate a data chain of custody due to the multi-layered and distributed nature of cloud computing

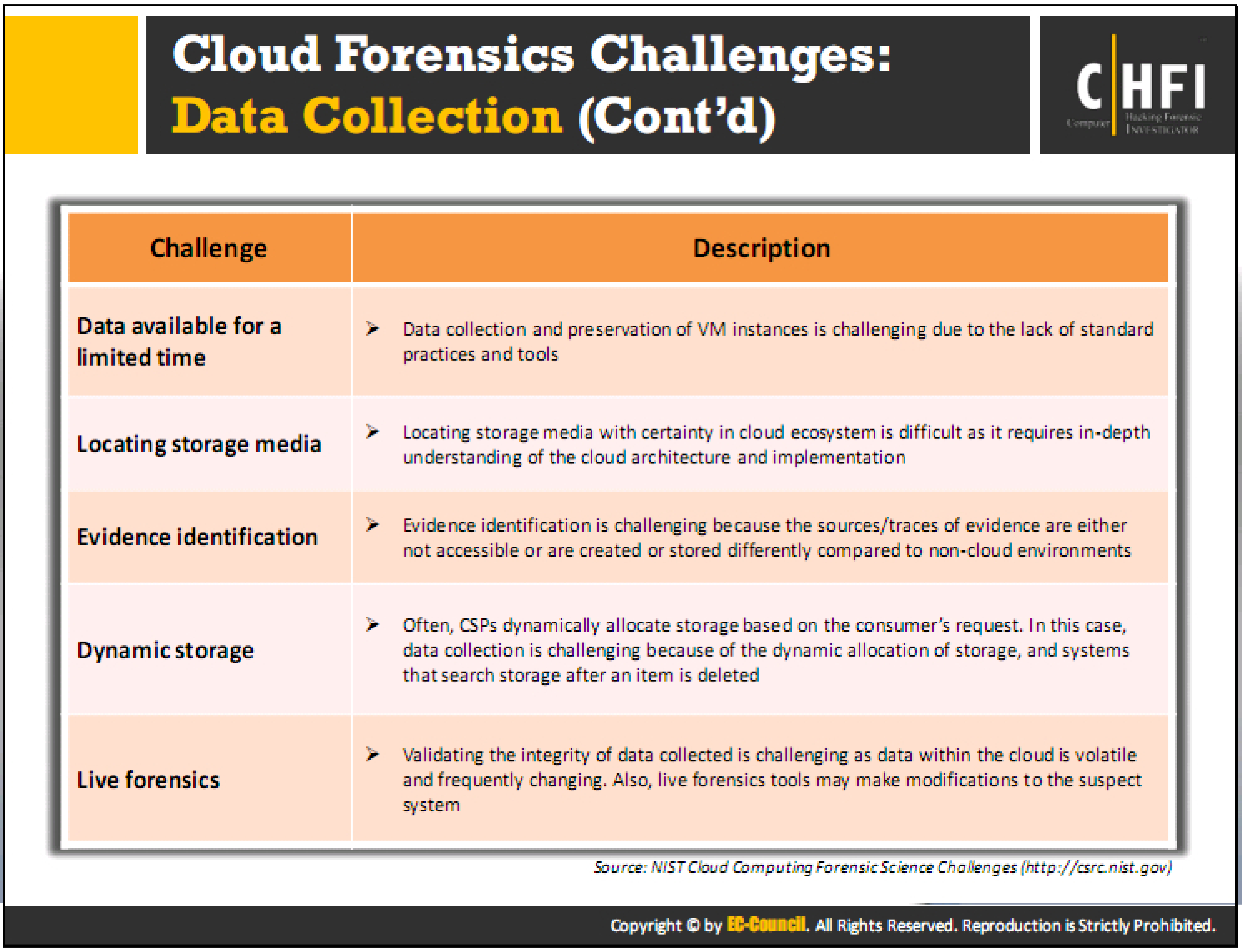
Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)



Cloud Forensics Challenges: Data Collection

Challenge	Description
Decreased access and data control	➢ In every combination of cloud service model and deployment model, the investigator faces the challenge of limited access and control to the forensic data ➢ CSPs hide data locations purposefully to ease data movement and replication
Chain of dependencies	➢ Often, CSPs and most cloud apps rely on other CSP(s), and the dependencies in a chain of CSP(s)/client(s) can be prominently dynamic ➢ In such conditions, cloud investigation may rely on investigation of each link in the chain and level of complexity of the dependencies
Locating evidence	➢ Locating and collecting evidence is a challenge because data in cloud may be quickly altered or lost and lack of knowledge on where and how data is stored in cloud
Data Location	➢ Collecting data of the target is challenging because of the flexibility CSPs have to migrate data between data centers and geographic regions
Imaging and isolating data	➢ Data imaging and isolating a migrating data target is challenging in the cloud ecosystem due to its key characteristics: elasticity, automatic provisioning/deprovisioning of resources, redundancy, and multi-tenancy

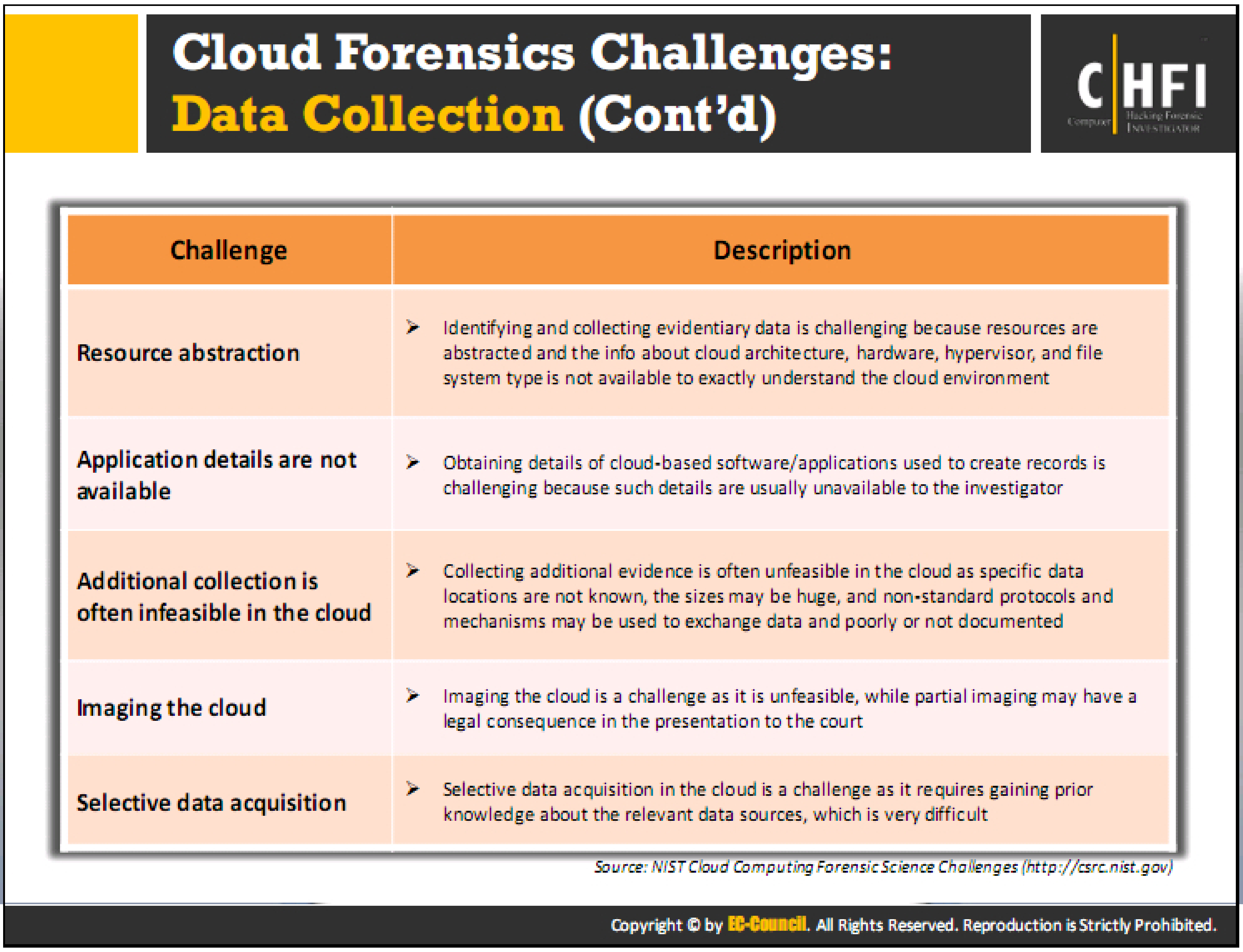
Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)



Cloud Forensics Challenges: Data Collection (Cont'd)

Challenge	Description
Data available for a limited time	➢ Data collection and preservation of VM instances is challenging due to the lack of standard practices and tools
Locating storage media	➢ Locating storage media with certainty in cloud ecosystem is difficult as it requires in-depth understanding of the cloud architecture and implementation
Evidence identification	➢ Evidence identification is challenging because the sources/traces of evidence are either not accessible or are created or stored differently compared to non-cloud environments
Dynamic storage	➢ Often, CSPs dynamically allocate storage based on the consumer's request. In this case, data collection is challenging because of the dynamic allocation of storage, and systems that search storage after an item is deleted
Live forensics	➢ Validating the integrity of data collected is challenging as data within the cloud is volatile and frequently changing. Also, live forensics tools may make modifications to the suspect system

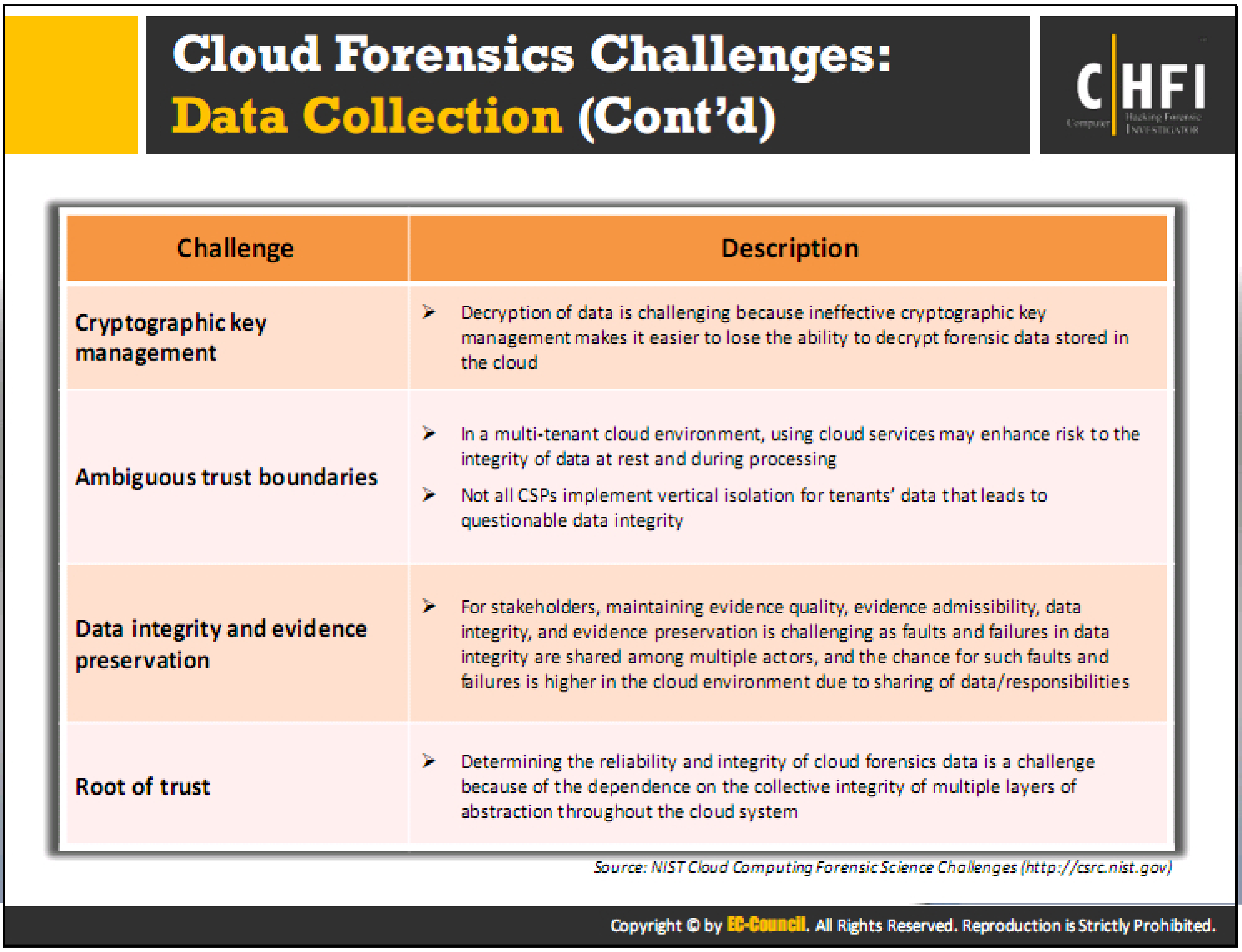
Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)



Cloud Forensics Challenges: Data Collection (Cont'd)

Challenge	Description
Resource abstraction	➢ Identifying and collecting evidentiary data is challenging because resources are abstracted and the info about cloud architecture, hardware, hypervisor, and file system type is not available to exactly understand the cloud environment
Application details are not available	➢ Obtaining details of cloud-based software/applications used to create records is challenging because such details are usually unavailable to the investigator
Additional collection is often infeasible in the cloud	➢ Collecting additional evidence is often unfeasible in the cloud as specific data locations are not known, the sizes may be huge, and non-standard protocols and mechanisms may be used to exchange data and poorly or not documented
Imaging the cloud	➢ Imaging the cloud is a challenge as it is unfeasible, while partial imaging may have a legal consequence in the presentation to the court
Selective data acquisition	➢ Selective data acquisition in the cloud is a challenge as it requires gaining prior knowledge about the relevant data sources, which is very difficult

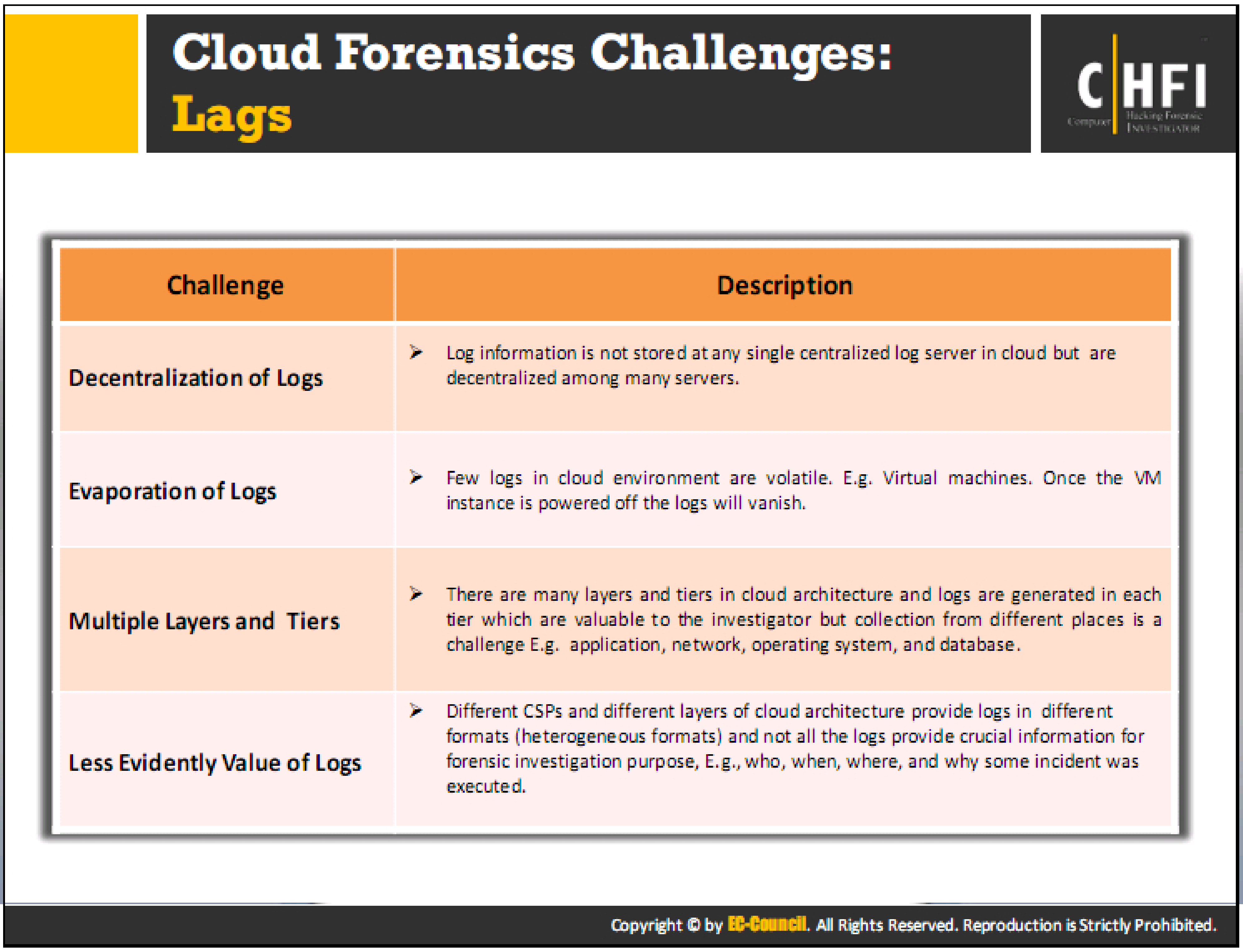
Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)



Cloud Forensics Challenges: Data Collection (Cont'd)

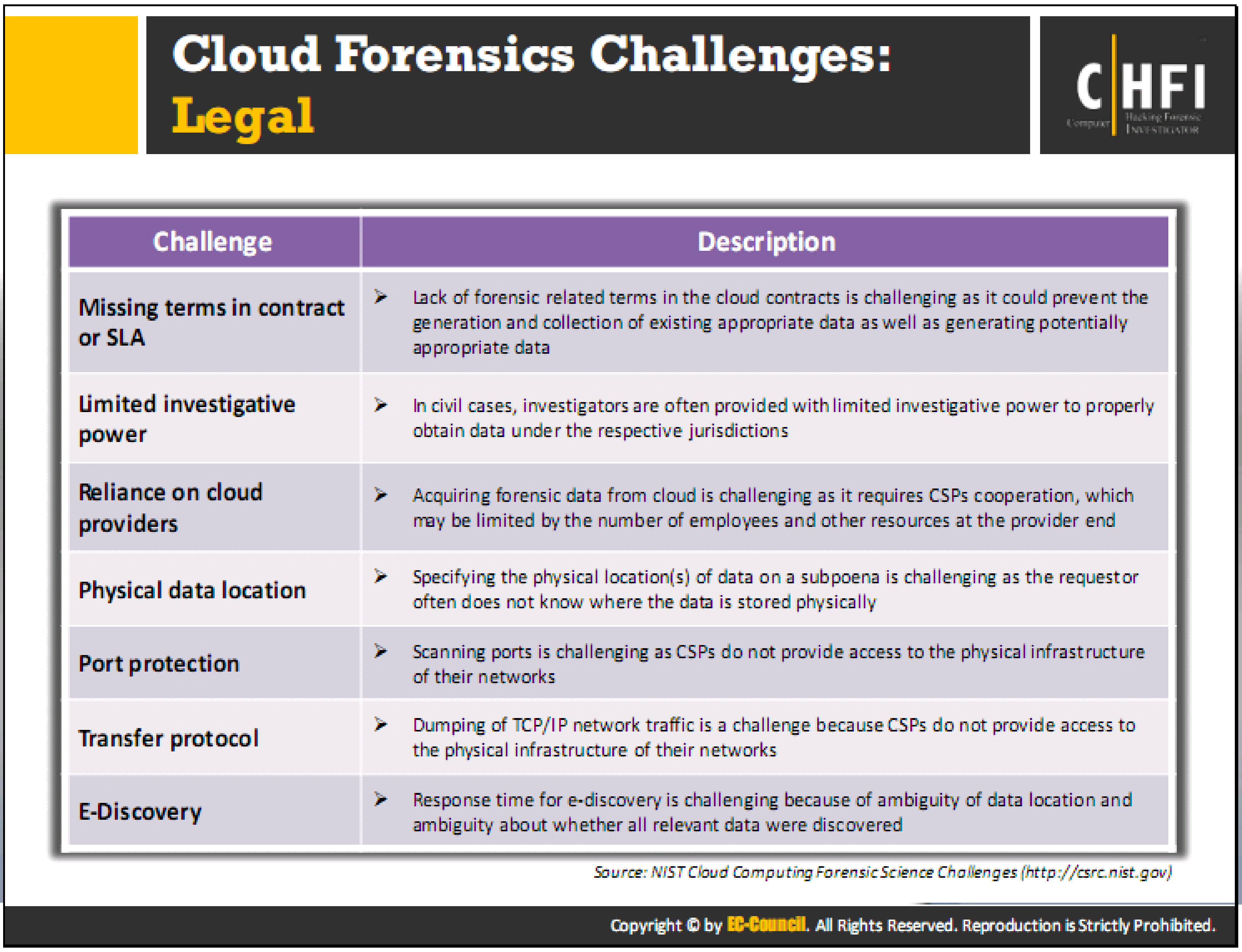
Challenge	Description
Cryptographic key management	➢ Decryption of data is challenging because ineffective cryptographic key management makes it easier to lose the ability to decrypt forensic data stored in the cloud
Ambiguous trust boundaries	➢ In a multi-tenant cloud environment, using cloud services may enhance risk to the integrity of data at rest and during processing ➢ Not all CSPs implement vertical isolation for tenants' data that leads to questionable data integrity
Data integrity and evidence preservation	➢ For stakeholders, maintaining evidence quality, evidence admissibility, data integrity, and evidence preservation is challenging as faults and failures in data integrity are shared among multiple actors, and the chance for such faults and failures is higher in the cloud environment due to sharing of data/responsibilities
Root of trust	➢ Determining the reliability and integrity of cloud forensics data is a challenge because of the dependence on the collective integrity of multiple layers of abstraction throughout the cloud system

Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)



Cloud Forensics Challenges: Lags

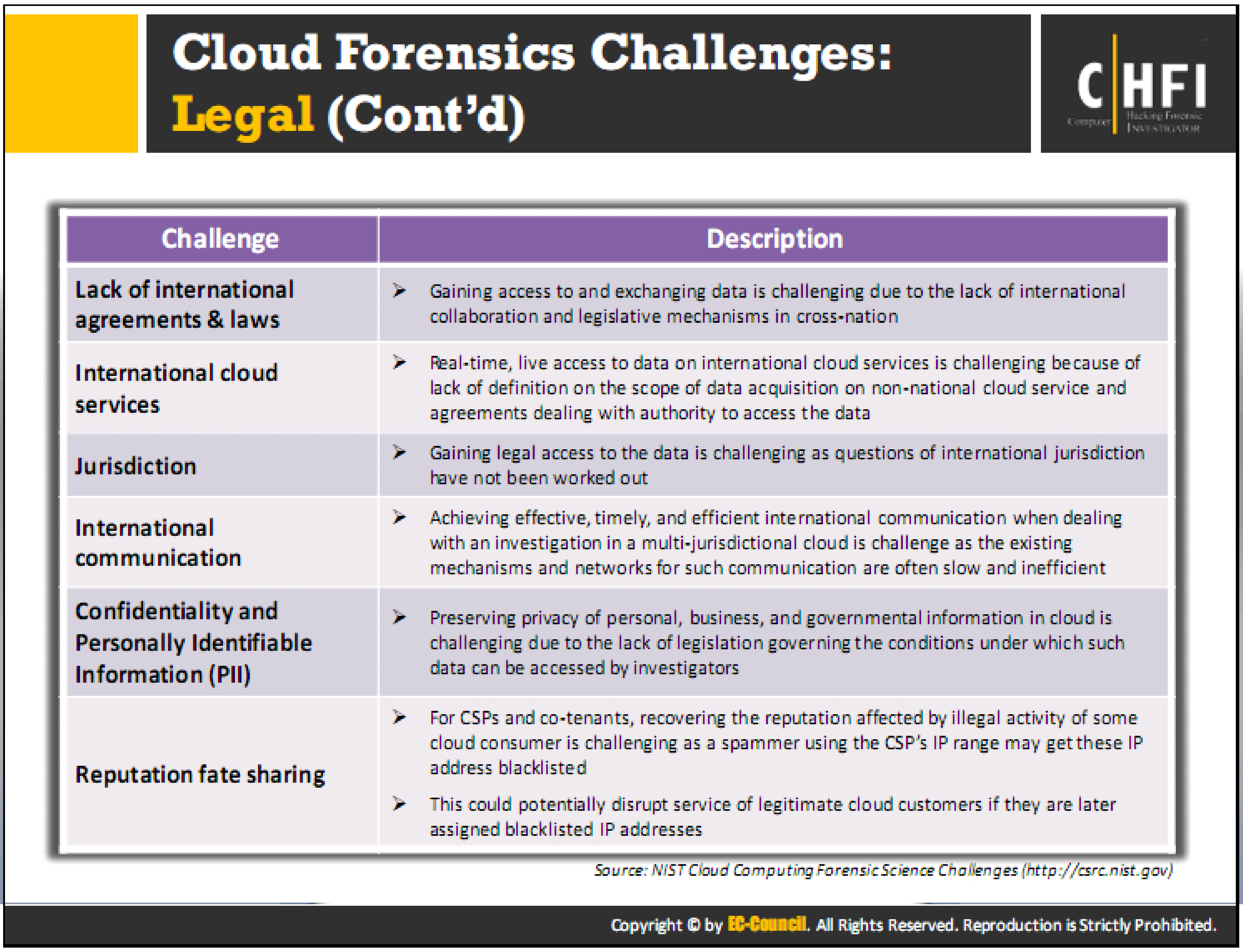
Challenge	Description
Decentralization of Logs	➢ Log information is not stored at any single centralized log server in cloud but are decentralized among many servers.
Evaporation of Logs	➢ Few logs in cloud environment are volatile. E.g. Virtual machines. Once the VM instance is powered off the logs will vanish.
Multiple Layers and Tiers	➢ There are many layers and tiers in cloud architecture and logs are generated in each tier which are valuable to the investigator but collection from different places is a challenge E.g. application, network, operating system, and database.
Less Evidently Value of Logs	➢ Different CSPs and different layers of cloud architecture provide logs in different formats (heterogeneous formats) and not all the logs provide crucial information for forensic investigation purpose, E.g., who, when, where, and why some incident was executed.



Cloud Forensics Challenges: Legal

Challenge	Description
Missing terms in contract or SLA	➢ Lack of forensic related terms in the cloud contracts is challenging as it could prevent the generation and collection of existing appropriate data as well as generating potentially appropriate data
Limited investigative power	➢ In civil cases, investigators are often provided with limited investigative power to properly obtain data under the respective jurisdictions
Reliance on cloud providers	➢ Acquiring forensic data from cloud is challenging as it requires CSPs cooperation, which may be limited by the number of employees and other resources at the provider end
Physical data location	➢ Specifying the physical location(s) of data on a subpoena is challenging as the requestor often does not know where the data is stored physically
Port protection	➢ Scanning ports is challenging as CSPs do not provide access to the physical infrastructure of their networks
Transfer protocol	➢ Dumping of TCP/IP network traffic is a challenge because CSPs do not provide access to the physical infrastructure of their networks
E-Discovery	➢ Response time for e-discovery is challenging because of ambiguity of data location and ambiguity about whether all relevant data were discovered

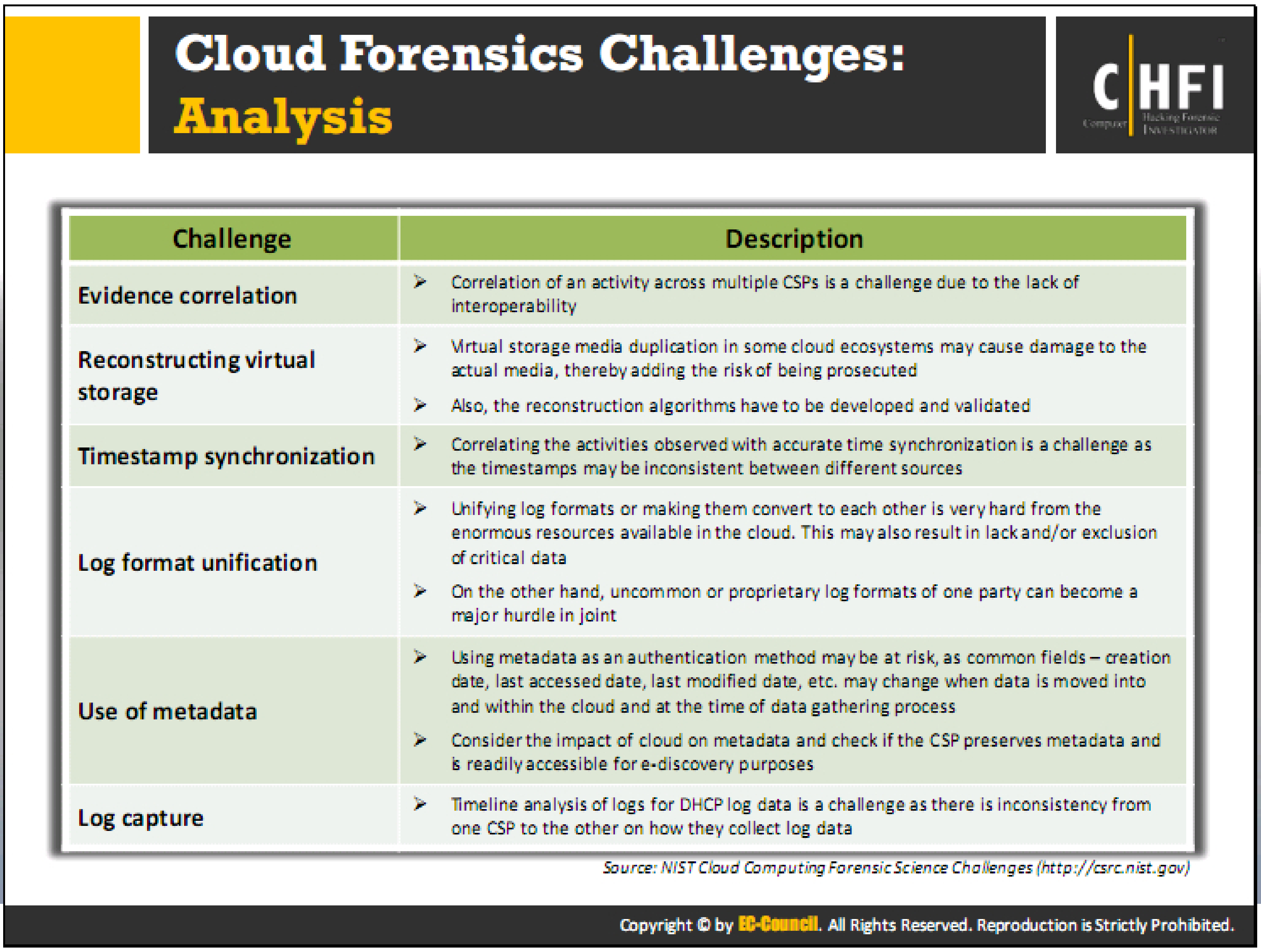
Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)



Cloud Forensics Challenges: Legal (Cont'd)

Challenge	Description
Lack of international agreements & laws	➤ Gaining access to and exchanging data is challenging due to the lack of international collaboration and legislative mechanisms in cross-nation
International cloud services	➤ Real-time, live access to data on international cloud services is challenging because of lack of definition on the scope of data acquisition on non-national cloud service and agreements dealing with authority to access the data
Jurisdiction	➤ Gaining legal access to the data is challenging as questions of international jurisdiction have not been worked out
International communication	➤ Achieving effective, timely, and efficient international communication when dealing with an investigation in a multi-jurisdictional cloud is challenge as the existing mechanisms and networks for such communication are often slow and inefficient
Confidentiality and Personally Identifiable Information (PII)	➤ Preserving privacy of personal, business, and governmental information in cloud is challenging due to the lack of legislation governing the conditions under which such data can be accessed by investigators
Reputation fate sharing	➤ For CSPs and co-tenants, recovering the reputation affected by illegal activity of some cloud consumer is challenging as a spammer using the CSP's IP range may get these IP address blacklisted ➤ This could potentially disrupt service of legitimate cloud customers if they are later assigned blacklisted IP addresses

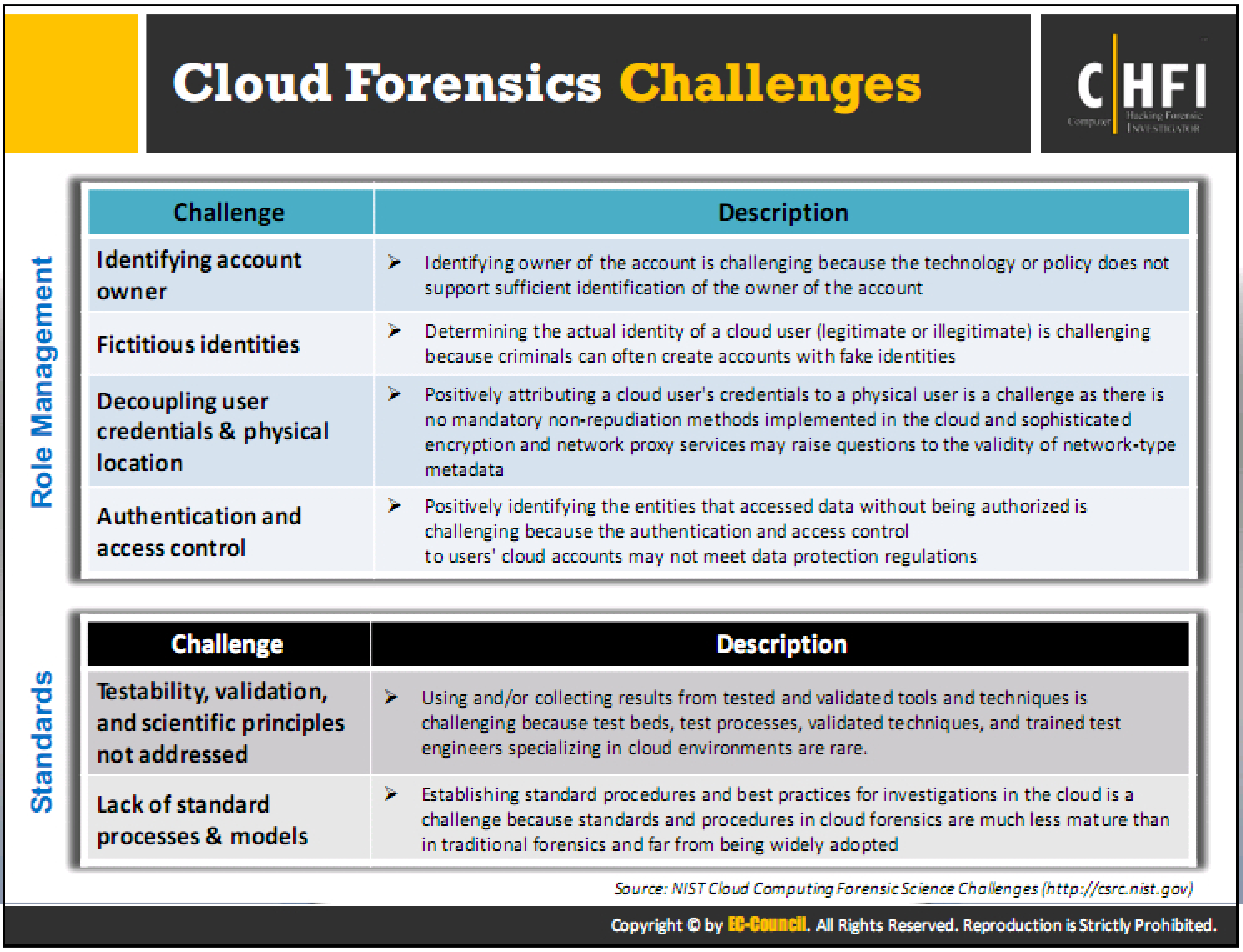
Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)



Cloud Forensics Challenges: Analysis

Challenge	Description
Evidence correlation	➤ Correlation of an activity across multiple CSPs is a challenge due to the lack of interoperability
Reconstructing virtual storage	➤ Virtual storage media duplication in some cloud ecosystems may cause damage to the actual media, thereby adding the risk of being prosecuted ➤ Also, the reconstruction algorithms have to be developed and validated
Timestamp synchronization	➤ Correlating the activities observed with accurate time synchronization is a challenge as the timestamps may be inconsistent between different sources
Log format unification	➤ Unifying log formats or making them convert to each other is very hard from the enormous resources available in the cloud. This may also result in lack and/or exclusion of critical data ➤ On the other hand, uncommon or proprietary log formats of one party can become a major hurdle in joint
Use of metadata	➤ Using metadata as an authentication method may be at risk, as common fields – creation date, last accessed date, last modified date, etc. may change when data is moved into and within the cloud and at the time of data gathering process ➤ Consider the impact of cloud on metadata and check if the CSP preserves metadata and is readily accessible for e-discovery purposes
Log capture	➤ Timeline analysis of logs for DHCP log data is a challenge as there is inconsistency from one CSP to the other on how they collect log data

Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)



Cloud Forensics Challenges

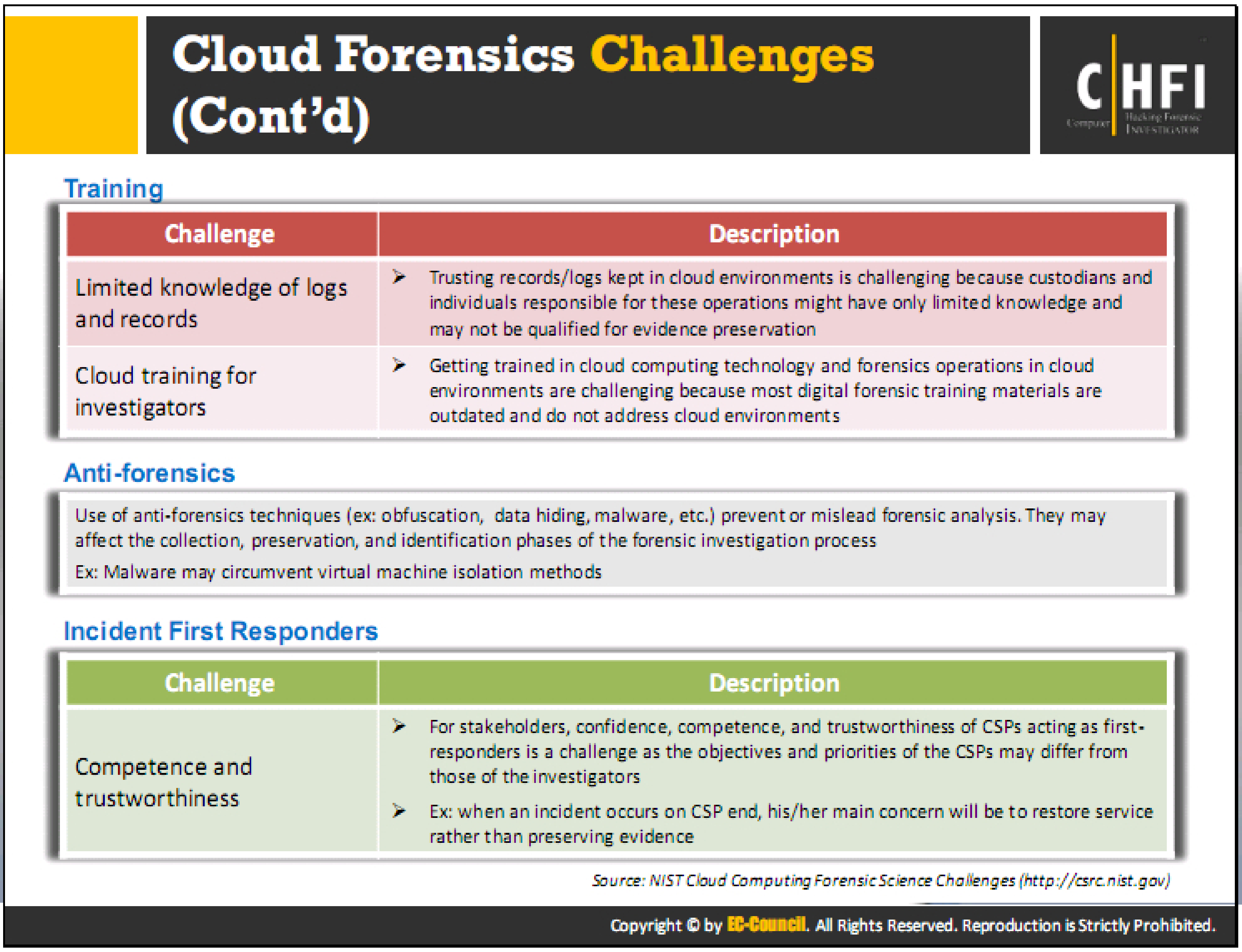
Role Management

Challenge	Description
Identifying account owner	➤ Identifying owner of the account is challenging because the technology or policy does not support sufficient identification of the owner of the account
Fictitious identities	➤ Determining the actual identity of a cloud user (legitimate or illegitimate) is challenging because criminals can often create accounts with fake identities
Decoupling user credentials & physical location	➤ Positively attributing a cloud user's credentials to a physical user is a challenge as there is no mandatory non-repudiation methods implemented in the cloud and sophisticated encryption and network proxy services may raise questions to the validity of network-type metadata
Authentication and access control	➤ Positively identifying the entities that accessed data without being authorized is challenging because the authentication and access control to users' cloud accounts may not meet data protection regulations

Standards

Challenge	Description
Testability, validation, and scientific principles not addressed	➤ Using and/or collecting results from tested and validated tools and techniques is challenging because test beds, test processes, validated techniques, and trained test engineers specializing in cloud environments are rare.
Lack of standard processes & models	➤ Establishing standard procedures and best practices for investigations in the cloud is a challenge because standards and procedures in cloud forensics are much less mature than in traditional forensics and far from being widely adopted

Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)



Cloud Forensics Challenges (Cont'd)

Training

Challenge	Description
Limited knowledge of logs and records	➤ Trusting records/logs kept in cloud environments is challenging because custodians and individuals responsible for these operations might have only limited knowledge and may not be qualified for evidence preservation
Cloud training for investigators	➤ Getting trained in cloud computing technology and forensics operations in cloud environments are challenging because most digital forensic training materials are outdated and do not address cloud environments

Anti-forensics

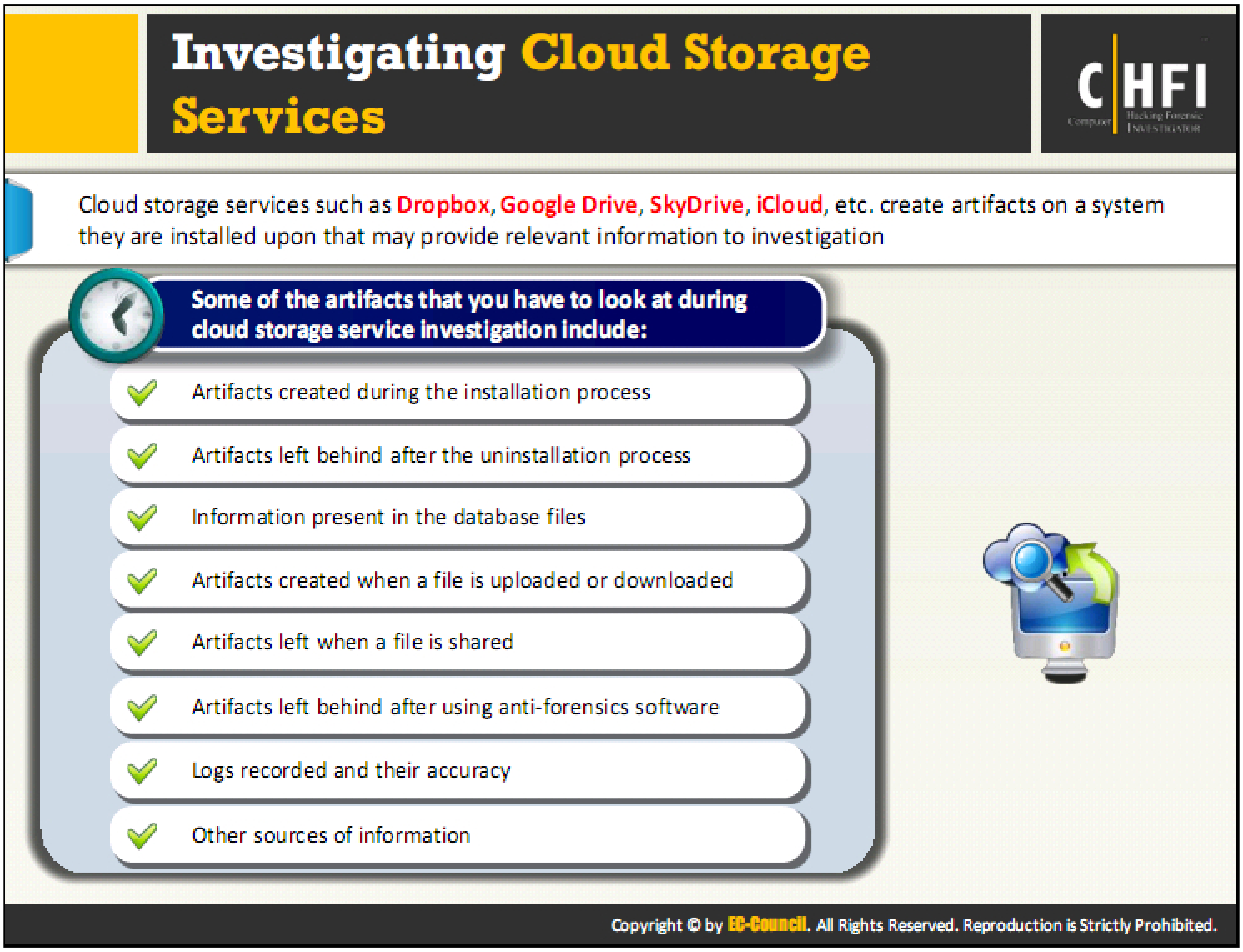
Use of anti-forensics techniques (ex: obfuscation, data hiding, malware, etc.) prevent or mislead forensic analysis. They may affect the collection, preservation, and identification phases of the forensic investigation process

Ex: Malware may circumvent virtual machine isolation methods

Incident First Responders

Challenge	Description
Competence and trustworthiness	➤ For stakeholders, confidence, competence, and trustworthiness of CSPs acting as first-responders is a challenge as the objectives and priorities of the CSPs may differ from those of the investigators ➤ Ex: when an incident occurs on CSP end, his/her main concern will be to restore service rather than preserving evidence

Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)



Investigating Cloud Storage Services

Cloud storage services such as Dropbox, Google Drive, SkyDrive, iCloud, etc. create artifacts on a system they are installed upon that may provide relevant information to investigation

Some of the artifacts that you have to look at during cloud storage service investigation include:

- ✓ Artifacts created during the installation process
- ✓ Artifacts left behind after the uninstallation process
- ✓ Information present in the database files
- ✓ Artifacts created when a file is uploaded or downloaded
- ✓ Artifacts left when a file is shared
- ✓ Artifacts left behind after using anti-forensics software
- ✓ Logs recorded and their accuracy
- ✓ Other sources of information

Cloud Storage Services

Most commonly used cloud storage services include Amazon, Dropbox, Google, AT&T, Iron Mountain, Microsoft, Nirvanix, Rackspace, etc. Users can use these cloud services through the website or by installing a platform based application on their systems. When the clients start using these services, they create folders and save files on the system that can act as evidences or artifacts in case of a security incident.

Public cloud storage service:

This service is usually suited for the unstructured data that does not change regularly. The infrastructure consists of inexpensive storage nodes fitted to commodity drives. Clients can store data on multiple drives for redundancy and access it through internet protocols like Representational State Transfer (REST).

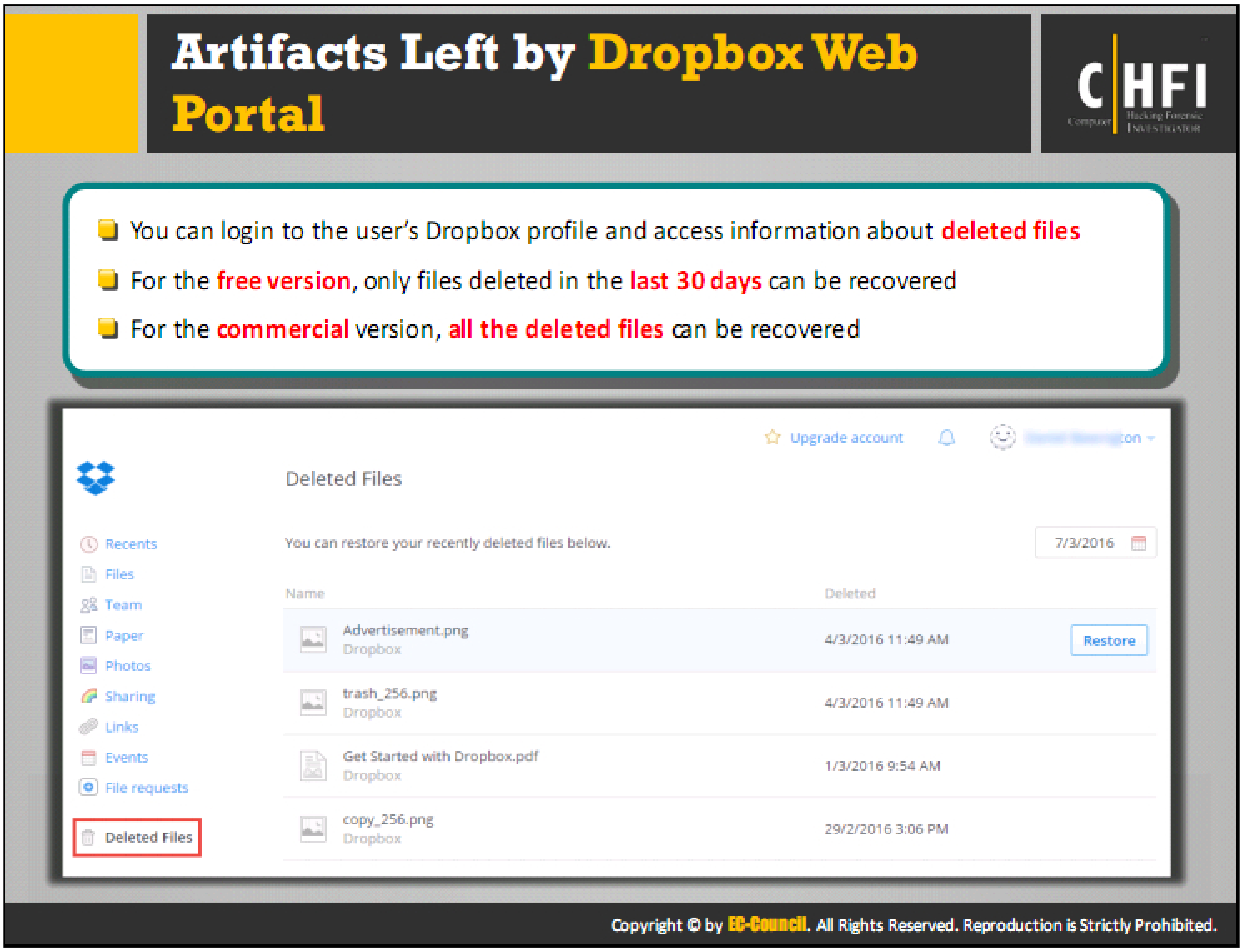
Private cloud storage service:

This service is very well suited for actively used data and for an organizational purpose that needs more control over. The CSP uses dedicated devices for storage of data to ensure better security and performance.

C|HFI
Computer Hacking Forensic Investigator
Dropbox

Investigating Dropbox Cloud Storage Service

Dropbox is an online application that allows users to store their files on a cloud and share them when required. Users can access and use Dropbox through the following methods, website, desktop or mobile application. In both ways, the Dropbox creates artifacts on a system that may provide relevant information for the forensic investigation. Besides, the Dropbox servers also save information such as account history, a user's file history, and logs. These artifacts and log files can help the investigator in conducting a detailed forensic analysis.



Artifacts Left by Dropbox Web Portal

- You can login to the user's Dropbox profile and access information about **deleted files**
- For the **free version**, only files deleted in the **last 30 days** can be recovered
- For the **commercial** version, **all the deleted files** can be recovered

Deleted Files

You can restore your recently deleted files below.

Name	Deleted
Advertisement.png Dropbox	4/3/2016 11:49 AM
trash_256.png Dropbox	4/3/2016 11:49 AM
Get Started with Dropbox.pdf Dropbox	1/3/2016 9:54 AM
copy_256.png Dropbox	29/2/2016 3:06 PM

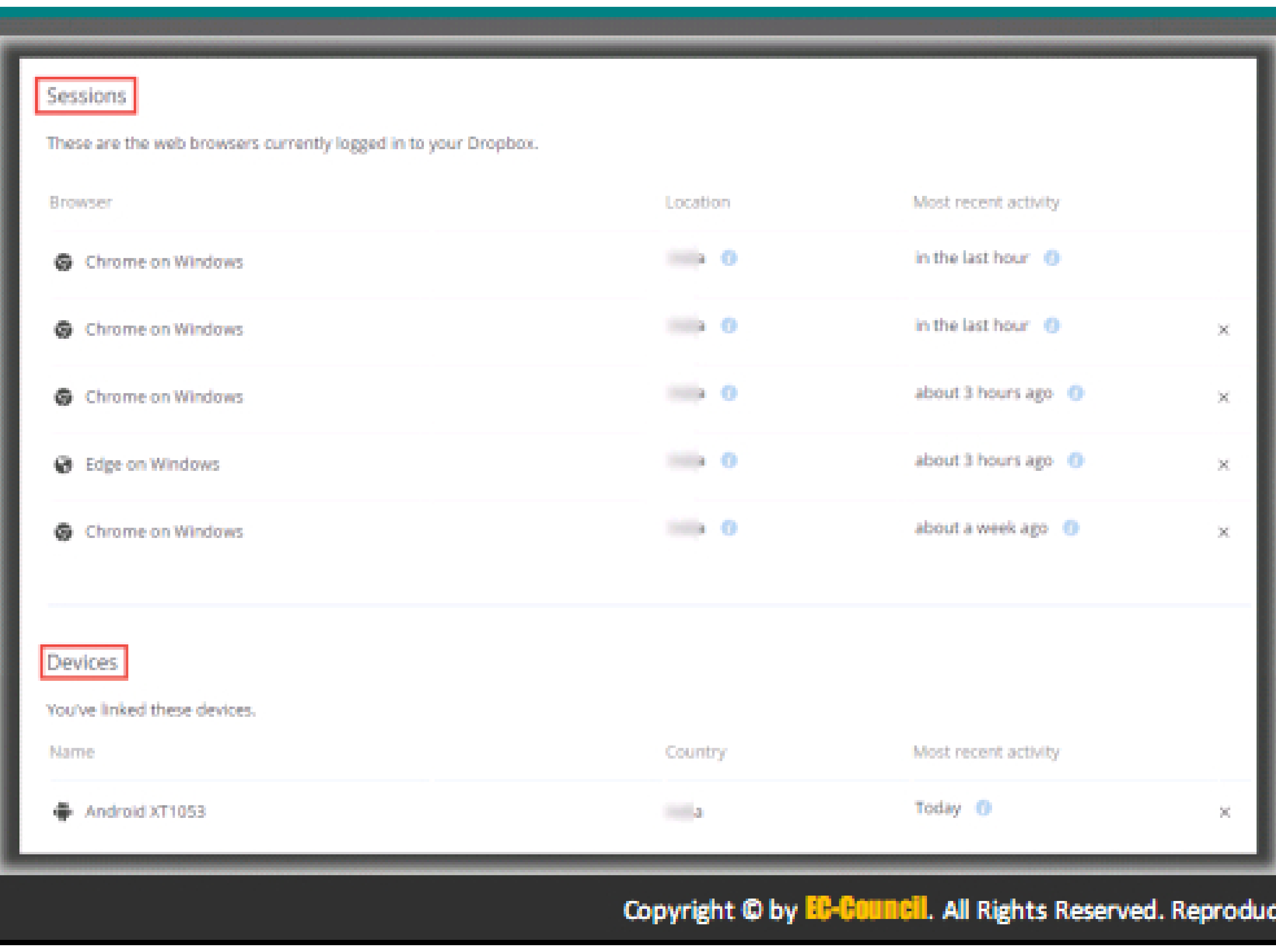
This section will impart knowledge about the evidential data, and artifacts investigators could collect using a web portal of a Dropbox account.

When users delete files from their Dropbox account, they do not erase it entirely as the Dropbox provides an allowance for restoring the deleted files. It stores the deleted file in Deleted Files folder until and unless the user deletes it permanently from the Deleted Files folder.

The investigator can recover the deleted files by logging into the user's Dropbox profile and navigating to the Deleted Files space. For a free version of Dropbox application, the users can recover the files deleted within 30 days; whereas in the commercial version, the Dropbox stores all the deleted files.

Artifacts Left by Dropbox Web Portal (Cont'd)

- You can get information about:
  - last browser sessions
  - devices linked with the Dropbox
  - Apps linked with the Dropbox
- Click on user name in the top-right. From the **menu** → **Settings** → **Security**



Sessions

These are the web browsers currently logged in to your Dropbox.

Browser	Location	Most recent activity	
Chrome on Windows	[redacted]	in the last hour	
Chrome on Windows	[redacted]	in the last hour	×
Chrome on Windows	[redacted]	about 3 hours ago	×
Edge on Windows	[redacted]	about 3 hours ago	×
Chrome on Windows	[redacted]	about a week ago	×

Devices

You've linked these devices.

Name	Country	Most recent activity	
Android XT1053	[redacted]	Today	×

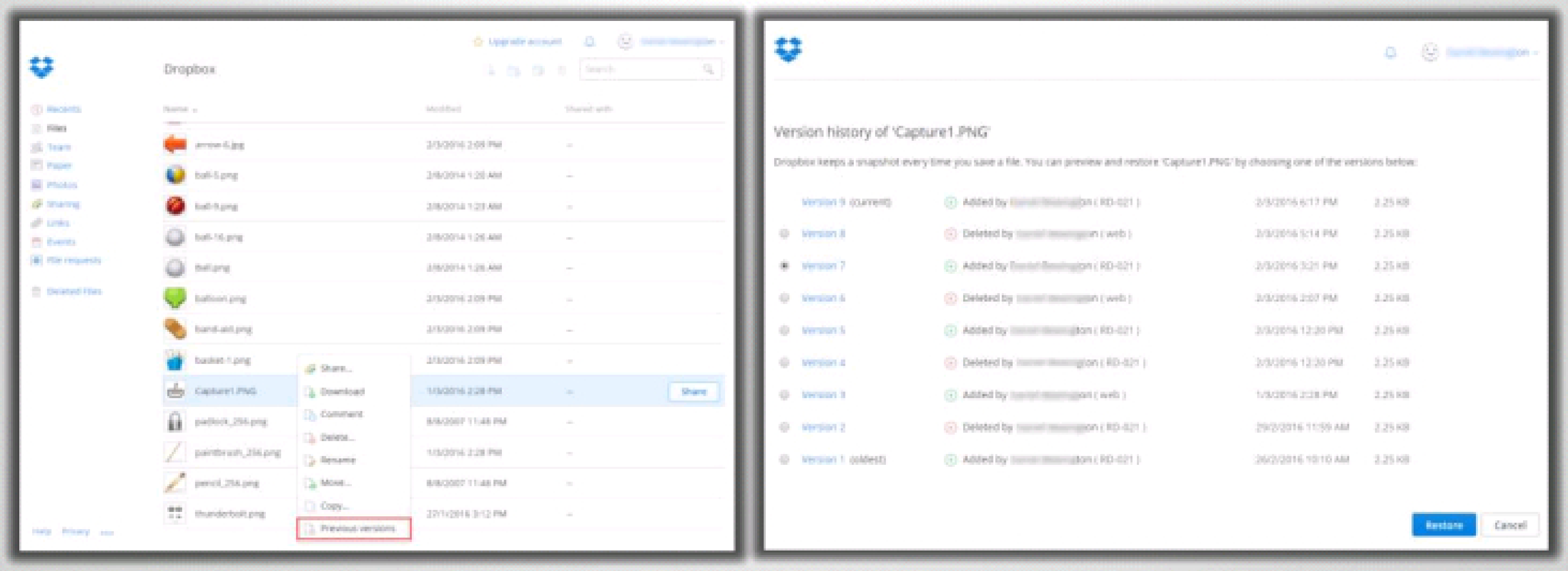
Dropbox stores certain information, which helps the investigators during investigation. Investigators can get the details of the last browser sessions, devices linked with the Dropbox and Apps.

To check for the last browsed sessions and the devices connected to the user's profile when the investigator has logged into the Dropbox account using the website, click on username in the top-right, select Settings from the menu and click on Security.

The site will redirect to a page that shows Sessions and Devices. The sessions section will display information about the logging information such as date, time and location from which the user had logged into the account. The Devices section displays all the linked devices, such as mobiles, laptops, and desktops.

Artifacts Left by Dropbox Web Portal (Cont'd)

- You can view **version history** for each file and can recover previous version of a file
- Right-click the file and select **previous versions**



Dropbox

Name	Modified	Shared with
arrow-6.jpg	2/3/2016 2:09 PM	–
ball-5.png	2/8/2014 1:20 AM	–
ball-9.png	2/8/2014 1:23 AM	–
ball-16.png	2/8/2014 1:26 AM	–
ball.png	2/8/2014 1:26 AM	–
balloon.png	2/3/2016 2:09 PM	–
band-aid.png	2/3/2016 2:09 PM	–
basket-1.png	2/3/2016 2:09 PM	–
Capture1.PNG	1/3/2016 2:28 PM	–
padlock_256.png	8/8/2007 11:48 PM	–
paintbrush_256.png	1/3/2016 2:28 PM	–
pencil_256.png	8/8/2007 11:48 PM	–
thunderbolt.png	22/1/2016 3:12 PM	–

Version history of 'Capture1.PNG'

Dropbox keeps a snapshot every time you save a file. You can preview and restore 'Capture1.PNG' by choosing one of the versions below:

Version 9 (current)	Added by [redacted] (RD-021)	2/3/2016 6:17 PM	2.25 KB
Version 8	Deleted by [redacted] (web)	2/3/2016 5:14 PM	2.25 KB
Version 7	Added by [redacted] (RD-021)	2/3/2016 3:21 PM	2.25 KB
Version 6	Deleted by [redacted] (web)	2/3/2016 2:07 PM	2.25 KB
Version 5	Added by [redacted] (RD-021)	2/3/2016 12:20 PM	2.25 KB
Version 4	Deleted by [redacted] (RD-021)	2/3/2016 12:20 PM	2.25 KB
Version 3	Added by [redacted] (web)	1/3/2016 2:28 PM	2.25 KB
Version 2	Deleted by [redacted] (RD-021)	29/2/2016 11:59 AM	2.25 KB
Version 1 (oldest)	Added by [redacted] (RD-021)	26/2/2016 10:10 AM	2.25 KB

Dropbox comes with a unique feature called extended version history (EVH), which saves all the deleted and previous versions of the files by default. The Dropbox offers this service in two variants, the Dropbox Education or free variant and the Dropbox Pro or paid variant. The main difference is that the trial variant can store the previous versions of deleted files for a limited period of 30 days, while the users who have bought a pro variant can access any version at any given time.

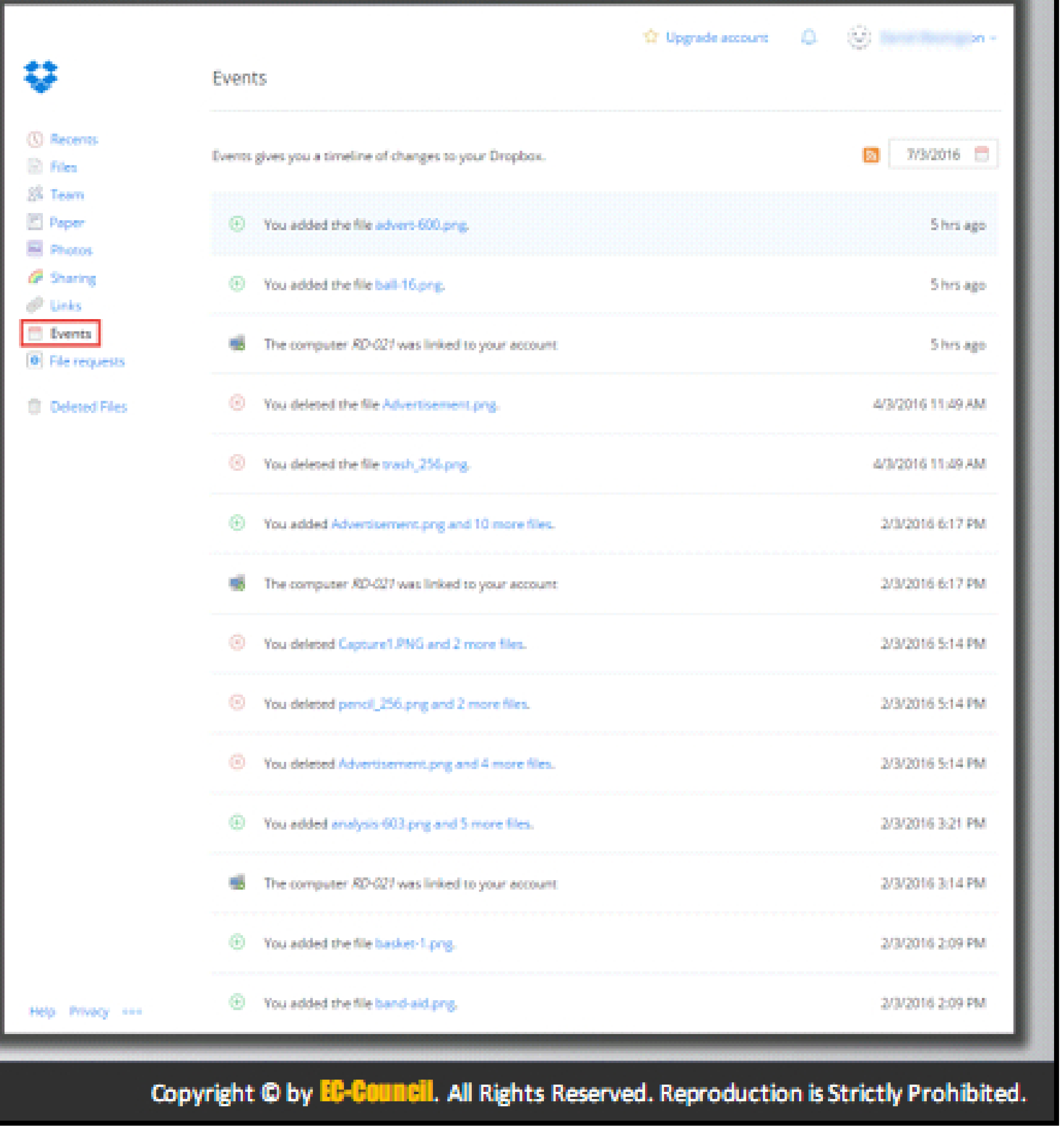
An investigator can use the EVH feature to view version history of each file and recover previous versions of the deleted files from the Dropbox account.

Steps to retrieve a deleted file from Dropbox:

- Login into the web based application
- Select the Files option from the right side menu list
- Right-click over the file from the provided list and select Previous versions from the drop-down menu
- The site will be redirected to the version history page of the selected file, which contains details of all the previous versions
- Select a version from the list and click the Restore button, to restore the version

Artifacts Left by Dropbox Web Portal (Cont'd)

- You can view **Events** section to know the timeline of changes to the Dropbox
- In addition, it also shows which account did the action, what the action was, and the target of the action



Events

Events gives you a timeline of changes to your Dropbox.

7/3/2016

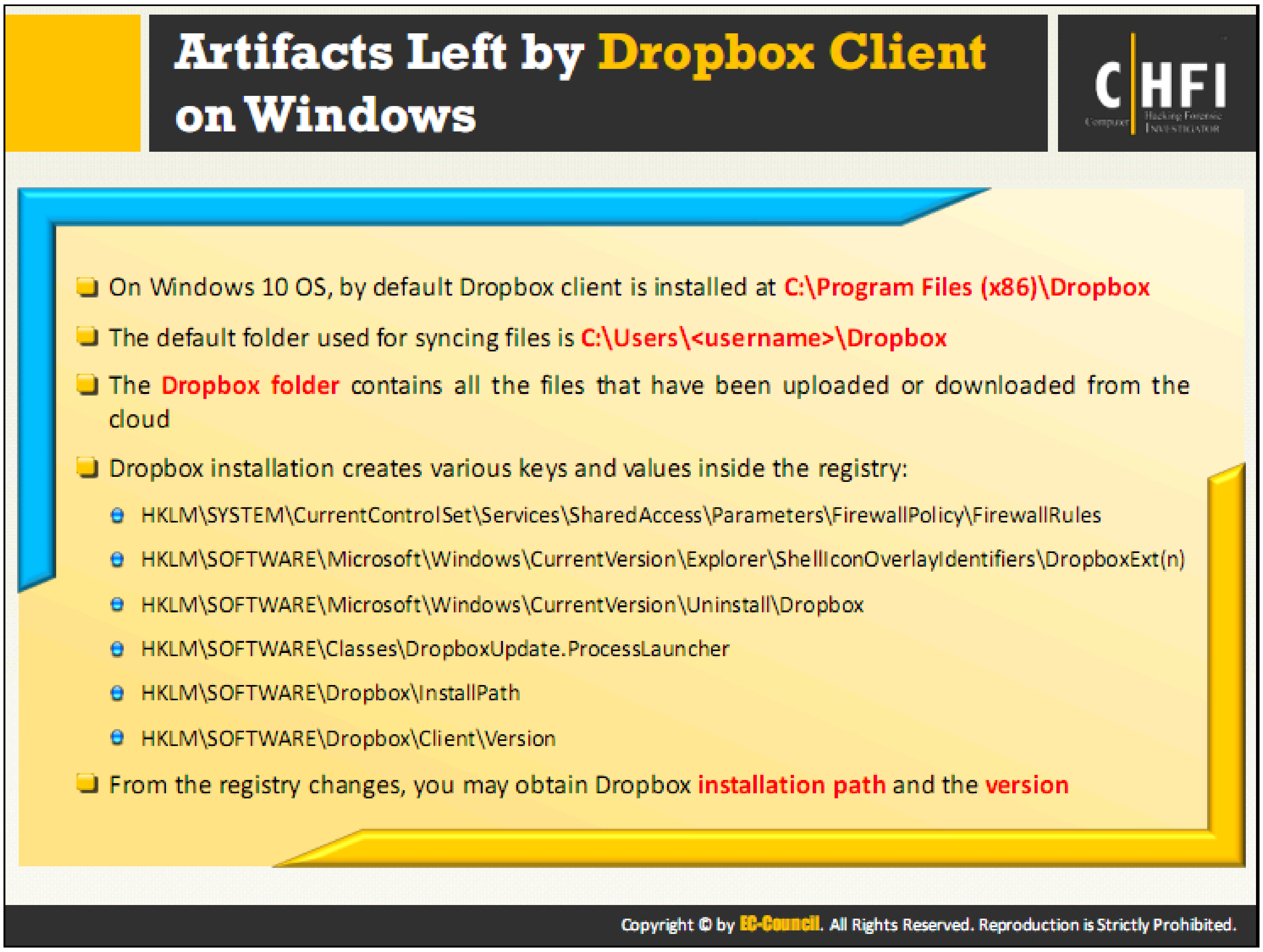
You added the file advert-600.png.	5 hrs ago
You added the file ball-16.png.	5 hrs ago
The computer RD-027 was linked to your account	5 hrs ago
You deleted the file Advertisement.png.	4/3/2016 11:49 AM
You deleted the file trash_256.png.	4/3/2016 11:49 AM
You added Advertisement.png and 10 more files.	2/3/2016 6:17 PM
The computer RD-027 was linked to your account	2/3/2016 6:17 PM
You deleted Capture1.PNG and 2 more files.	2/3/2016 5:14 PM
You deleted pencil_256.png and 2 more files.	2/3/2016 5:14 PM
You deleted Advertisement.png and 4 more files.	2/3/2016 5:14 PM
You added analysis-603.png and 5 more files.	2/3/2016 3:21 PM
The computer RD-027 was linked to your account	2/3/2016 3:14 PM
You added the file basket-1.png.	2/3/2016 2:09 PM
You added the file band-aid.png.	2/3/2016 2:09 PM

Dropbox contains an event log feature that records activities performed on Dropbox folders. Investigators can use this feature to track the account activities. This feature will reveal details such as connected accounts, accounts that made the changes, type of action, targets of the action and the time of action.

Dropbox groups all the actions that had taken place in sync and displays it as a single entry along with a timestamp stating when the action ended. In case, if there is any interruption in the sync process, the Dropbox removes the timestamps for those significant amounts of time.

Steps to see the event logs:

In the Dropbox web portal homepage, select the Events option from the right side menu list. The site will navigate to the events page, which will display events and related details such as time and date of the event, account that performed it, actions performed and file or folders modified.



Artifacts Left by Dropbox Client on Windows

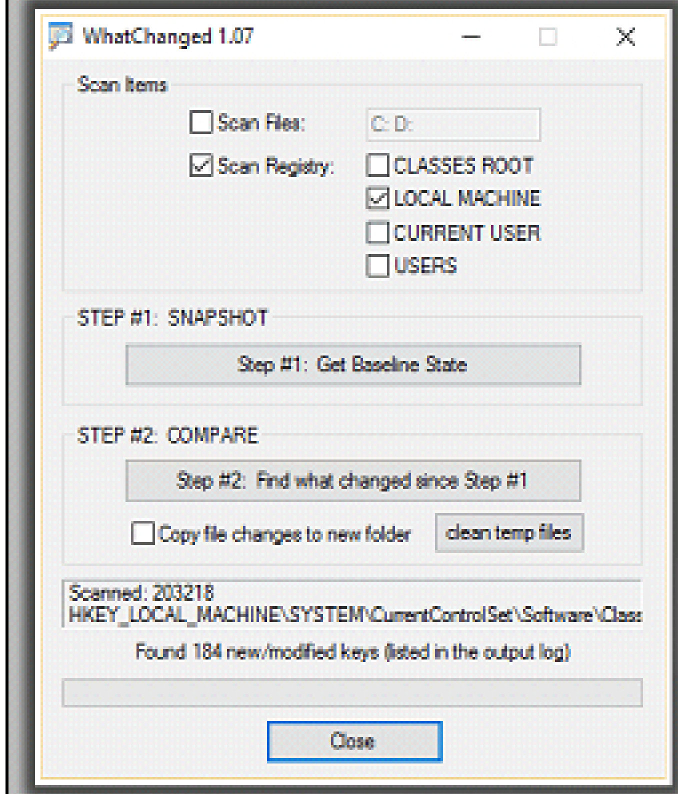
- On Windows 10 OS, by default Dropbox client is installed at **C:\Program Files (x86)\Dropbox**
- The default folder used for syncing files is **C:\Users\<username>\Dropbox**
- The **Dropbox folder** contains all the files that have been uploaded or downloaded from the cloud
- Dropbox installation creates various keys and values inside the registry:
  - HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\DropboxExt(n)
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox
  - HKLM\SOFTWARE\Classes\DropboxUpdate.ProcessLauncher
  - HKLM\SOFTWARE\Dropbox\InstallPath
  - HKLM\SOFTWARE\Dropbox\Client\Version
- From the registry changes, you may obtain Dropbox **installation path** and the **version**

When a user installs a Dropbox application on a desktop running on Windows operating system, the system saves the Dropbox files at the C:\Program Files (x86)\Dropbox location by default. The system uses C:\Users\<*username*>\Dropbox as the default folder used to sync files. The sync location stores all the files that the users upload to or downloads from the Dropbox.

Investigators can use these folders to check the stored files in case they do not have an access to the Dropbox account. The installation process also makes changes in the registry keys and values, which can provide information such as the Dropbox installation path and the version, changes made to the network, ports, and firewall to allow data transfer to and from Dropbox client.

Artifacts Left by Dropbox Client on Windows (Cont'd)

- **WhatChanged Portable** is a system utility that scans for modified files and registry entries. It uses the '**brute-force method**' to check files and the registry.



WhatChanged 1.07

Scan Items

☐ Scan Files: C: D:

☑ Scan Registry: ☐ CLASSES ROOT ☑ LOCAL MACHINE ☐ CURRENT USER ☐ USERS

STEP #1: SNAPSHOT

Step #1: Get Baseline State

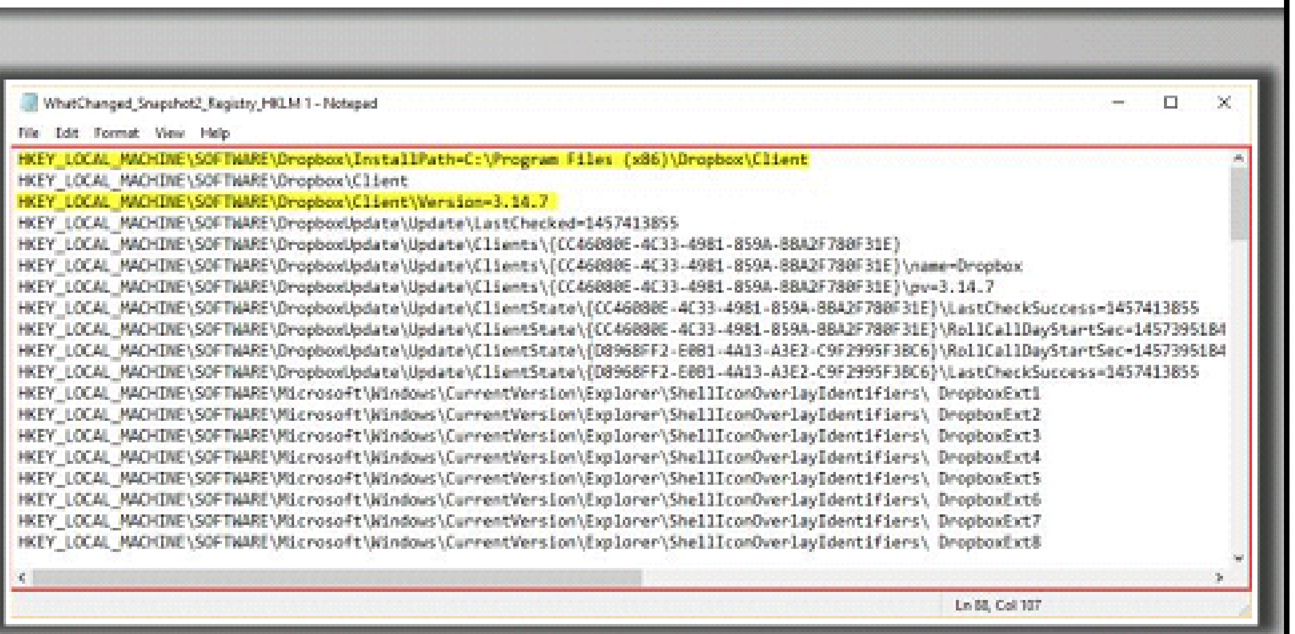
STEP #2: COMPARE

Step #2: Find what changed since Step #1

☐ Copy file changes to new folder

Scanned: 203218
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Software\Class

Found 184 new/modified keys (listed in the output log)



WhatChanged_Snapshot2_Registry_HKLM 1 - Notepad

```
HKEY_LOCAL_MACHINE\SOFTWARE\Dropbox\InstallPath=C:\Program Files (x86)\Dropbox\Client
HKEY_LOCAL_MACHINE\SOFTWARE\Dropbox\Client
HKEY_LOCAL_MACHINE\SOFTWARE\Dropbox\Client\Version=3.14.7
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\LastChecked=1457413855
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Clients\{CC46080E-4C33-4981-859A-8BA2F780F31E}
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Clients\{CC46080E-4C33-4981-859A-8BA2F780F31E}\name=Dropbox
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Clients\{CC46080E-4C33-4981-859A-8BA2F780F31E}\pv=3.14.7
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\ClientState\{CC46080E-4C33-4981-859A-8BA2F780F31E}\LastCheckSuccess=1457413855
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\ClientState\{CC46080E-4C33-4981-859A-8BA2F780F31E}\RollCallDayStartSec=1457395184
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\ClientState\{D8968FF2-E081-4A13-A3E2-C9F2995F38C6}\RollCallDayStartSec=1457395184
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\ClientState\{D8968FF2-E081-4A13-A3E2-C9F2995F38C6}\LastCheckSuccess=1457413855
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ DropboxExt1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ DropboxExt2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ DropboxExt3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ DropboxExt4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ DropboxExt5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ DropboxExt6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ DropboxExt7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\ DropboxExt8
```

http://portableapps.com

Dropbox client imposes many changes in the registry of a system during installation. Investigators can review the registry files the installation process can modify by using WhatChanged Portable tool, which is capable of tracking changes in the registry of a system. Install the tool before installing the Dropbox client and start scanning the registry to find the modified registry keys and values. Copy the changes list to a notepad for ease in referencing.

WhatChanged

Source: http://portableapps.com

WhatChanged portable is useful for checking program installations. It is a system utility that scans for modified files and registry entries. It uses the 'brute-force method' to check files and the registry.

There are two steps for using WhatChanged Portable software:

- First, take a snapshot to get the current state of the computer before installing Dropbox client;
- Second, run it again to check the differences since the previous snapshot, after installing Dropbox client.

  By comparing both the screen shots, investigators can find out the list files modified in the registry and the entries made to the registry.

Artifacts Left by Dropbox Client on Windows (Cont'd)

- **Configuration files are saved inside the Appdata folder in the user profile**

  C:\Users\<username>\AppData\Local\Dropbox\instance(*n*)

- **Executable and libraries are stored at:**

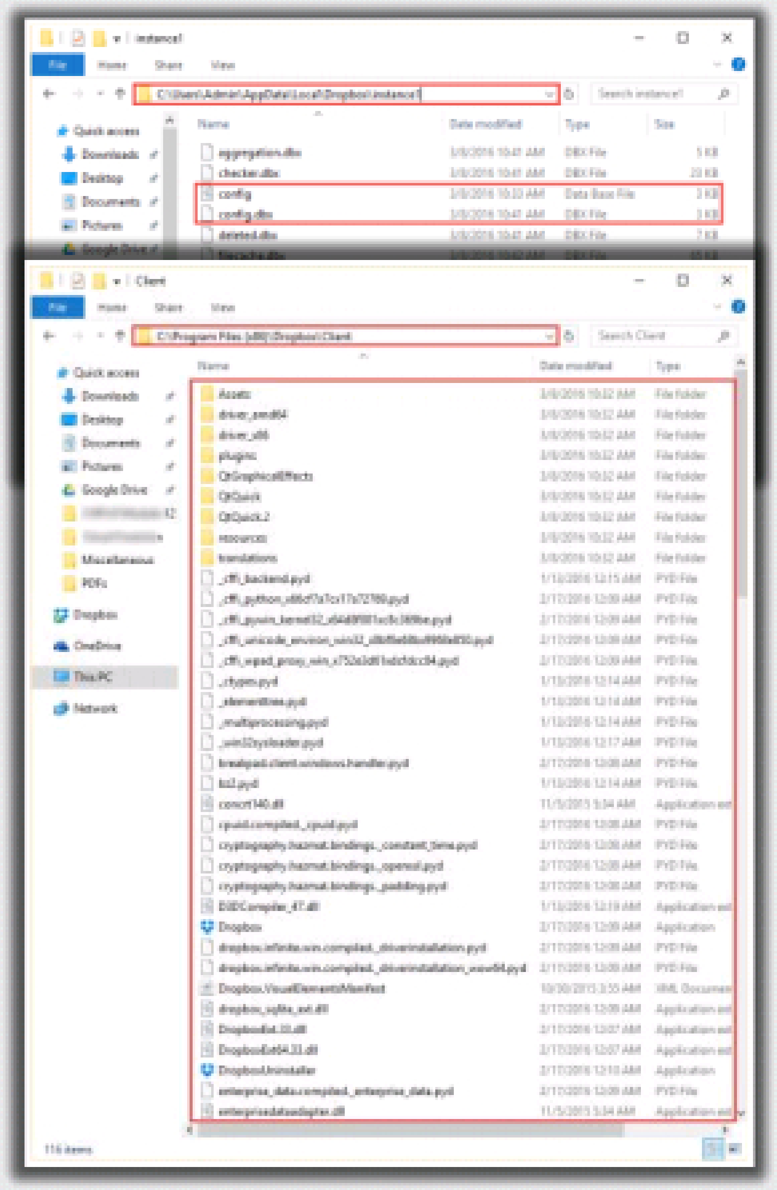
  C:\Program Files (x86)\Dropbox\Client

- **Files created during Dropbox client installation:**
  - **LINK files or Shortcut files:**

    C:\Users\<username>\Desktop\Dropbox.lnk
    C:\Users\<username>\Links\Dropbox.lnk

  - **Prefetch Files:**

    C:\Windows\Prefetch\DROPBOX.EXE-1AFC8E96.pf
    C:\Windows\Prefetch\DROPBOX.EXE-BC41F124.pf
    C:\Windows\Prefetch\DROPBOXCLIENT_3.14.7.EXE-67CA8E4C.pf
    C:\Windows\Prefetch\DROPBOXCLIENT_3.14.7.EXE-68E912D2.pf
    C:\Windows\Prefetch\DROPBOXCRASHHANDLER.EXE-3D55A98C.pf
    C:\Windows\Prefetch\DROPBOXINSTALLER.EXE-1EDCCE18.pf
    C:\Windows\Prefetch\DROPBOXUNINSTALLER.EXE-A866A871.pf
    C:\Windows\Prefetch\DROPBOXUPDATE.EXE-59B5AB7D.pf
    C:\Windows\Prefetch\DROPBOXUPDATE.EXE-48534C67.pf
    C:\Windows\Prefetch\DROPBOXUPDATE.EXE-AA3CC021.pf
    C:\Windows\Prefetch\DROPBOXUPDATEONDEMAND.EXE-229B2726.pf



C:\Users\Admin\AppData\Local\Dropbox\instance1

Name	Date modified	Type	Size
aggregation.dbx	3/8/2016 10:41 AM	DBX File	1 KB
checker.dbx	3/8/2016 10:41 AM	DBX File	20 KB
config	3/8/2016 10:33 AM	Data Base File	3 KB
config.dbx	3/8/2016 10:41 AM	DBX File	3 KB
deleted.dbx	3/8/2016 10:41 AM	DBX File	7 KB
filecache.dbx	[illegible]	DBX File	[illegible]

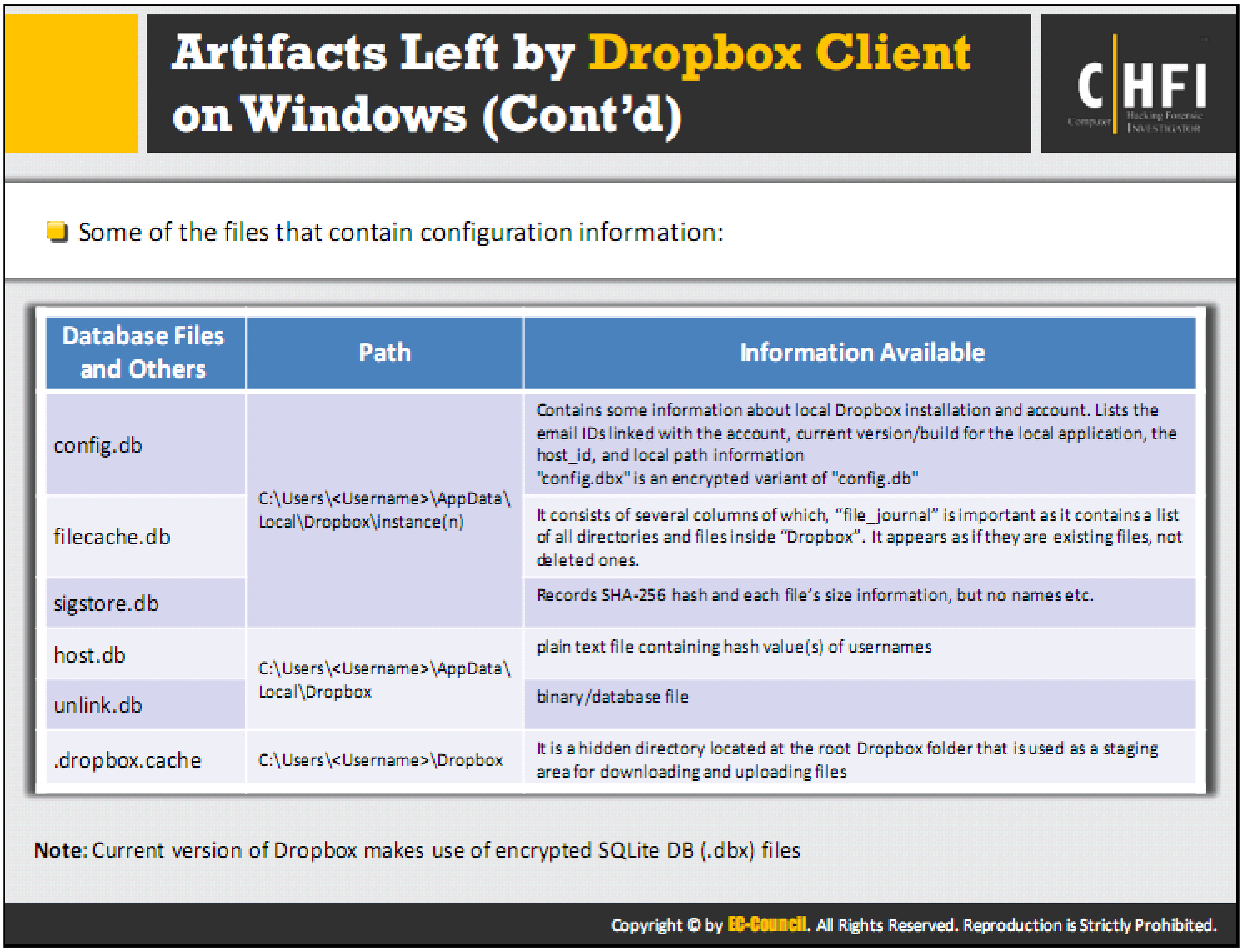
C:\Program Files (x86)\Dropbox\Client

Name	Date modified	Type
Assets	3/8/2016 10:32 AM	File folder
driver_amd64	3/8/2016 10:32 AM	File folder
driver_x86	3/8/2016 10:32 AM	File folder
plugins	3/8/2016 10:32 AM	File folder
QtGraphicalEffects	3/8/2016 10:32 AM	File folder
QtQuick	3/8/2016 10:32 AM	File folder
QtQuick.2	3/8/2016 10:32 AM	File folder
resources	3/8/2016 10:32 AM	File folder
translations	3/8/2016 10:32 AM	File folder
_cffi_backend.pyd	1/13/2016 12:15 AM	PYD File
_cffi_python_[illegible].pyd	2/17/2016 12:09 AM	PYD File
_cffi_pywin_kernel32_[illegible].pyd	2/17/2016 12:09 AM	PYD File
_cffi_unicode_environ_win32_[illegible].pyd	2/17/2016 12:09 AM	PYD File
_cffi_wpad_proxy_win_[illegible].pyd	2/17/2016 12:09 AM	PYD File
_ctypes.pyd	1/13/2016 12:14 AM	PYD File
_elementtree.pyd	1/13/2016 12:14 AM	PYD File
_multiprocessing.pyd	1/13/2016 12:14 AM	PYD File
_win32sysloader.pyd	1/13/2016 12:17 AM	PYD File
breakpad.client.windows.handler.pyd	2/17/2016 12:08 AM	PYD File
bz2.pyd	1/13/2016 12:14 AM	PYD File
concrt140.dll	11/5/2015 5:34 AM	Application ext
cpuid.compiled._cpuid.pyd	2/17/2016 12:08 AM	PYD File
cryptography.hazmat.bindings._constant_time.pyd	2/17/2016 12:08 AM	PYD File
cryptography.hazmat.bindings._openssl.pyd	2/17/2016 12:08 AM	PYD File
cryptography.hazmat.bindings._padding.pyd	2/17/2016 12:08 AM	PYD File
D3DCompiler_47.dll	1/13/2016 12:19 AM	Application ext
Dropbox	2/17/2016 12:09 AM	Application
dropbox.infinite.win.compiled._driverinstallation.pyd	2/17/2016 12:09 AM	PYD File
dropbox.infinite.win.compiled._driverinstallation_wow64.pyd	2/17/2016 12:09 AM	PYD File
Dropbox.VisualElementsManifest	10/30/2015 3:35 AM	XML Document
dropbox_sqlite_ext.dll	2/17/2016 12:09 AM	Application ext
DropboxExt.33.dll	2/17/2016 12:07 AM	Application ext
DropboxExt64.33.dll	2/17/2016 12:07 AM	Application ext
DropboxUninstaller	2/17/2016 12:10 AM	Application
enterprise_data.compiled._enterprise_data.pyd	2/17/2016 12:09 AM	PYD File
enterprisedataadapter.dll	11/5/2015 5:34 AM	Application ext

116 items

During installation, the Dropbox client adds various other files to the system, resulting in multiple changes. The new files include the executables, librairies of the Dropbox client, Program Files, LiNK files, shortcut files of the application and Links of user profiles.

Investigators should gather information about the files and folders the application creates on a desktop and understand how it can act as evidence. The files and folders an application adds during installation include the ones mentioned in the slide.



Artifacts Left by Dropbox Client on Windows (Cont'd)

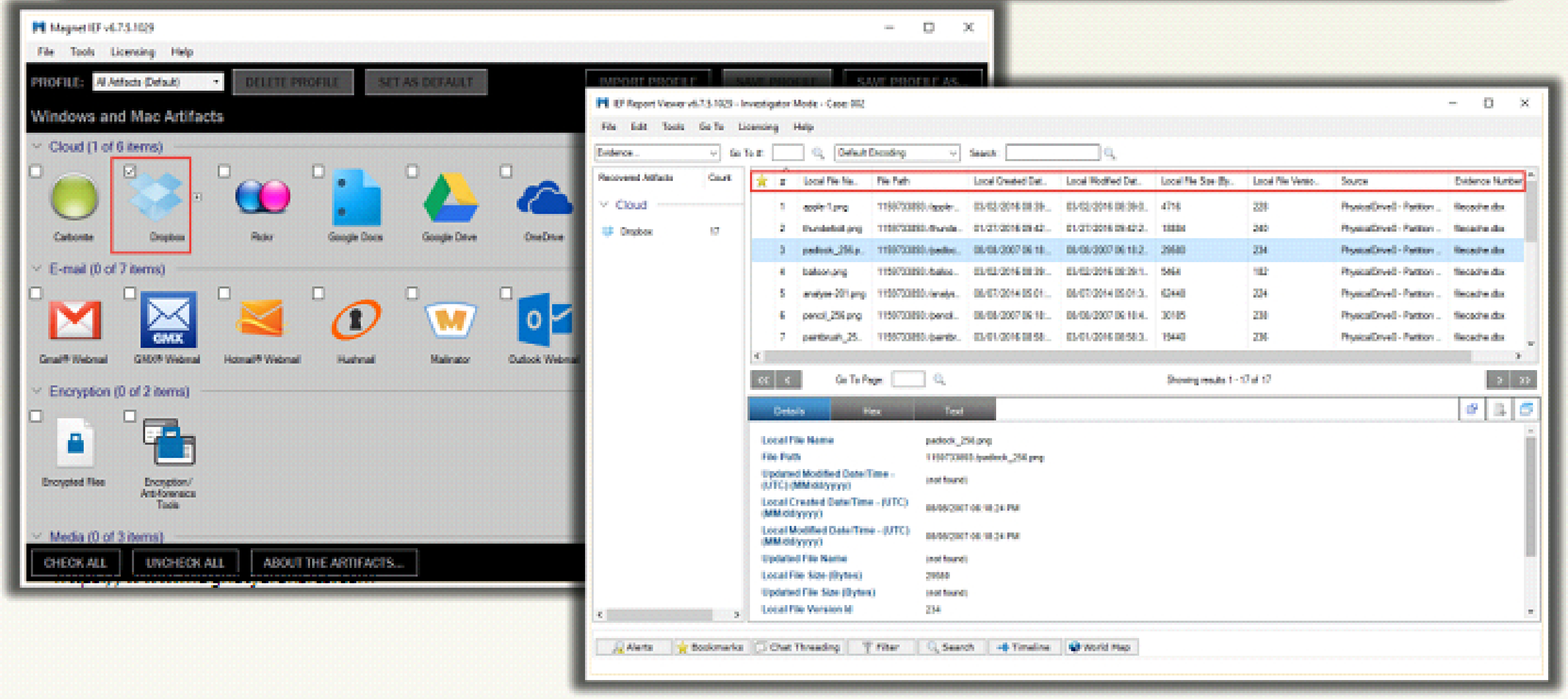
- Some of the files that contain configuration information:

Database Files and Others	Path	Information Available
config.db	C:\Users\<Username>\AppData\Local\Dropbox\instance(n)	Contains some information about local Dropbox installation and account. Lists the email IDs linked with the account, current version/build for the local application, the host_id, and local path information "config.dbx" is an encrypted variant of "config.db"
filecache.db		It consists of several columns of which, "file_journal" is important as it contains a list of all directories and files inside "Dropbox". It appears as if they are existing files, not deleted ones.
sigstore.db		Records SHA-256 hash and each file's size information, but no names etc.
host.db	C:\Users\<Username>\AppData\Local\Dropbox	plain text file containing hash value(s) of usernames
unlink.db		binary/database file
.dropbox.cache	C:\Users\<Username>\Dropbox	It is a hidden directory located at the root Dropbox folder that is used as a staging area for downloading and uploading files

Note: Current version of Dropbox makes use of encrypted SQLite DB (.dbx) files

Artifacts Left by Dropbox Client on Windows (Cont'd)

- MAGNET IEF can be used by forensics professionals to **find**, **analyze**, and **report on the digital evidence** from computers, smartphones, and tablets
- It can **recover evidence from a variety of data sources** (ex: here Dropbox) and integrate them into a single Magnet IEF case file



☆	#	Local File Na...	File Path	Local Created Dat...	Local Modified Dat...	Local File Size (By...	Local File Versio...	Source	Evidence Number
	1	apple-1.png	1159733893./apple...	03/02/2016 08:39...	03/02/2016 08:39:0...	4716	228	PhysicalDrive0 - Partition ...	filecache.dbx
	2	thunderbolt.png	1159733893./thunde...	01/27/2016 09:42...	01/27/2016 09:42:2...	18884	240	PhysicalDrive0 - Partition ...	filecache.dbx
	3	padlock_256.p...	1159733893./padlo...	08/08/2007 06:18...	08/08/2007 06:18:2...	29580	234	PhysicalDrive0 - Partition ...	filecache.dbx
	4	balloon.png	1159733893./balloo...	03/02/2016 08:39...	03/02/2016 08:39:1...	5464	182	PhysicalDrive0 - Partition ...	filecache.dbx
	5	analyze-201.png	1159733893./analy...	06/07/2014 05:01...	06/07/2014 05:01:3...	62440	224	PhysicalDrive0 - Partition ...	filecache.dbx
	6	pencil_256.png	1159733893./pencil...	08/08/2007 06:18...	08/08/2007 06:18:4...	30185	238	PhysicalDrive0 - Partition ...	filecache.dbx
	7	paintbrush_25...	1159733893./paintbr...	03/01/2016 08:58...	03/01/2016 08:58:3...	19440	236	PhysicalDrive0 - Partition ...	filecache.dbx

Local File Name	padlock_256.png
File Path	1159733893./padlock_256.png
Updated Modified Date/Time - (UTC) (MM/dd/yyyy)	(not found)
Local Created Date/Time - (UTC) (MM/dd/yyyy)	08/08/2007 06:18:24 PM
Local Modified Date/Time - (UTC) (MM/dd/yyyy)	08/08/2007 06:18:24 PM
Updated File Name	(not found)
Local File Size (Bytes)	29580
Updated File Size (Bytes)	(not found)
Local File Version Id	234

Source: *https://www.magnetforensics.com*

The tool processes the raw, unstructured and disparate data in the forensic image, or file dump and extracts the meaningful data for each supported artifact type. It searches for the artifacts of multiple categories from allocated and unallocated space over the computer devices.

Investigators use Magnet IEF to find, analyze and report on the digital evidence from computers, Smartphones, and tablets. It automates the digital forensic evidence.

The tool can recover artifacts from unallocated space by extracting data from the files that are not sequential, out of order, or missing entirely irrespective of the disk sizes and integrates them into a single Magnet IEF case file.

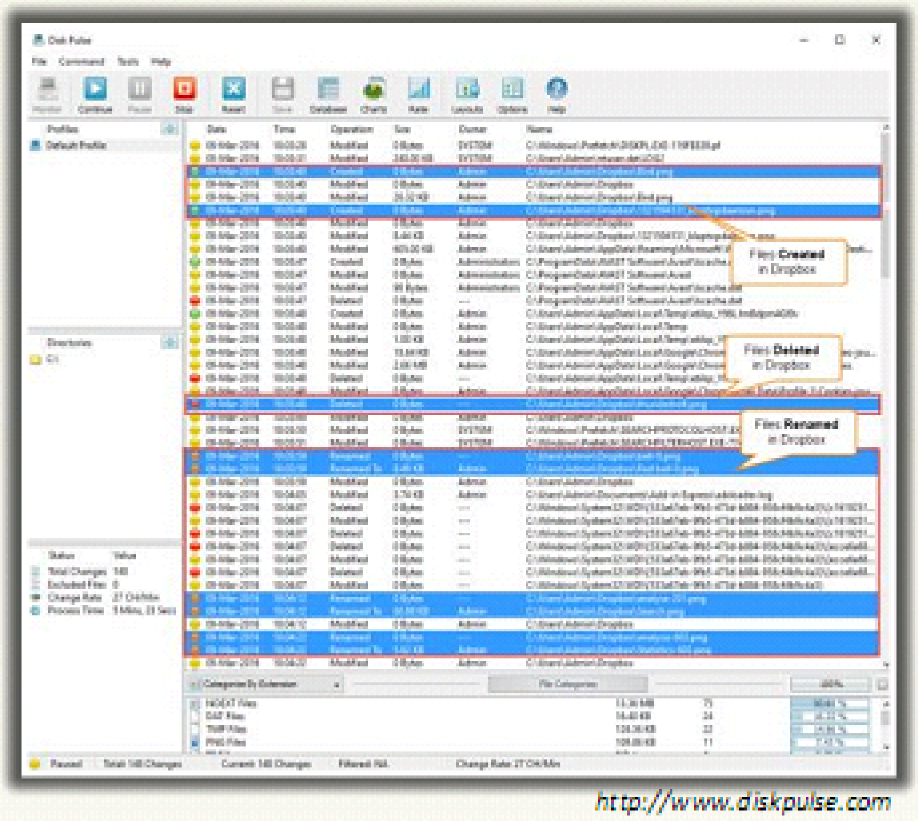
All the digital evidence recovered by a MAGNET IEF search is organized and stored in an IEF Case File, a database comprised of distinct artifact tables for each supported artifact type.

Artifacts Left by Dropbox Client on Windows (Cont'd)

- You can view changes (create, modify/rename, and delete) to the Dropbox using tools such as DiskPulse, Directory Monitor, etc.

DiskPulse

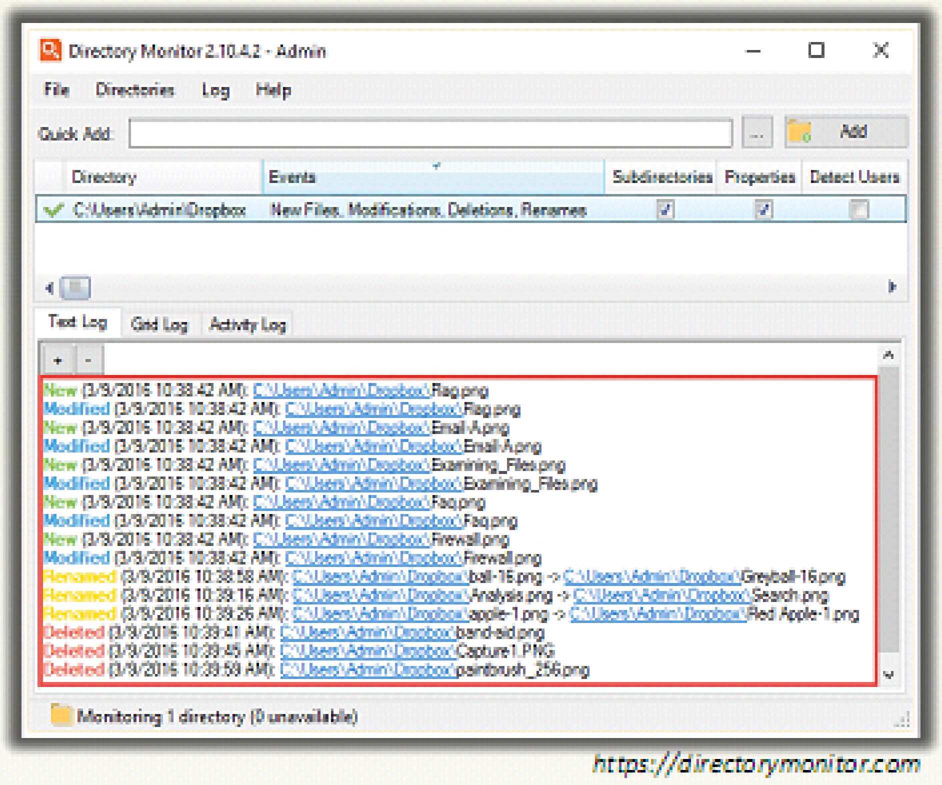
Monitors the disks or directories, saves reports and disk change monitoring statistics, executes custom commands, and sends E-Mail notifications when unauthorized changes are detected in critical system files



http://www.diskpulse.com

Directory Monitor

Monitors and detects changes to the directories and/or network shares and will notify user of file changes/access, deletions, modifications, and new files



Directory	Events	Subdirectories	Properties	Detect Users
✓ C:\Users\Admin\Dropbox	New Files, Modifications, Deletions, Renames	☑	☑	□

```
New (3/9/2016 10:38:42 AM): C:\Users\Admin\Dropbox\Flag.png
Modified (3/9/2016 10:38:42 AM): C:\Users\Admin\Dropbox\Flag.png
New (3/9/2016 10:38:42 AM): C:\Users\Admin\Dropbox\Email-A.png
Modified (3/9/2016 10:38:42 AM): C:\Users\Admin\Dropbox\Email-A.png
New (3/9/2016 10:38:42 AM): C:\Users\Admin\Dropbox\Examining_Files.png
Modified (3/9/2016 10:38:42 AM): C:\Users\Admin\Dropbox\Examining_Files.png
New (3/9/2016 10:38:42 AM): C:\Users\Admin\Dropbox\Faq.png
Modified (3/9/2016 10:38:42 AM): C:\Users\Admin\Dropbox\Faq.png
New (3/9/2016 10:38:42 AM): C:\Users\Admin\Dropbox\Firewall.png
Modified (3/9/2016 10:38:42 AM): C:\Users\Admin\Dropbox\Firewall.png
Renamed (3/9/2016 10:38:58 AM): C:\Users\Admin\Dropbox\ball-16.png -> C:\Users\Admin\Dropbox\Greyball-16.png
Renamed (3/9/2016 10:39:16 AM): C:\Users\Admin\Dropbox\Analysis.png -> C:\Users\Admin\Dropbox\Search.png
Renamed (3/9/2016 10:39:26 AM): C:\Users\Admin\Dropbox\apple-1.png -> C:\Users\Admin\Dropbox\Red Apple-1.png
Deleted (3/9/2016 10:39:41 AM): C:\Users\Admin\Dropbox\band-aid.png
Deleted (3/9/2016 10:39:45 AM): C:\Users\Admin\Dropbox\Capture1.PNG
Deleted (3/9/2016 10:39:59 AM): C:\Users\Admin\Dropbox\paintbrush_256.png
```

Monitoring 1 directory (0 unavailable)

https://directorymonitor.com

Investigators can view changes in a Dropbox account using tools such as DiskPulse, Directory Monitor, etc.

DiskPulse

Source: http://www.diskpulse.com

DiskPulse is a disk change monitoring solution allowing investigators to monitor changes in one or more disks and directories, send E-Mail notifications, save various types of reports, generate statistical pie charts, export detected changes to an SQL database, send error messages to the system event log and execute custom commands when a user-specified number of changes detected.

The tool intercepts file system change notifications issued by the operating system and detects newly created files, modified files, deleted files and renamed files. All file system changes are detected in real-time allowing one to send an E-Mail notification, execute a custom command and save a disk change monitoring report within a couple of seconds after one or more critical changes detected.

The Investigator is provided with the ability to review, categorize and filter detected file system changes, generate various types of statistical reports showing the number of changes per file extension, the number of changes per change type, the number of changes per user, etc.

Directory Monitor

Source: https://directorymonitor.com

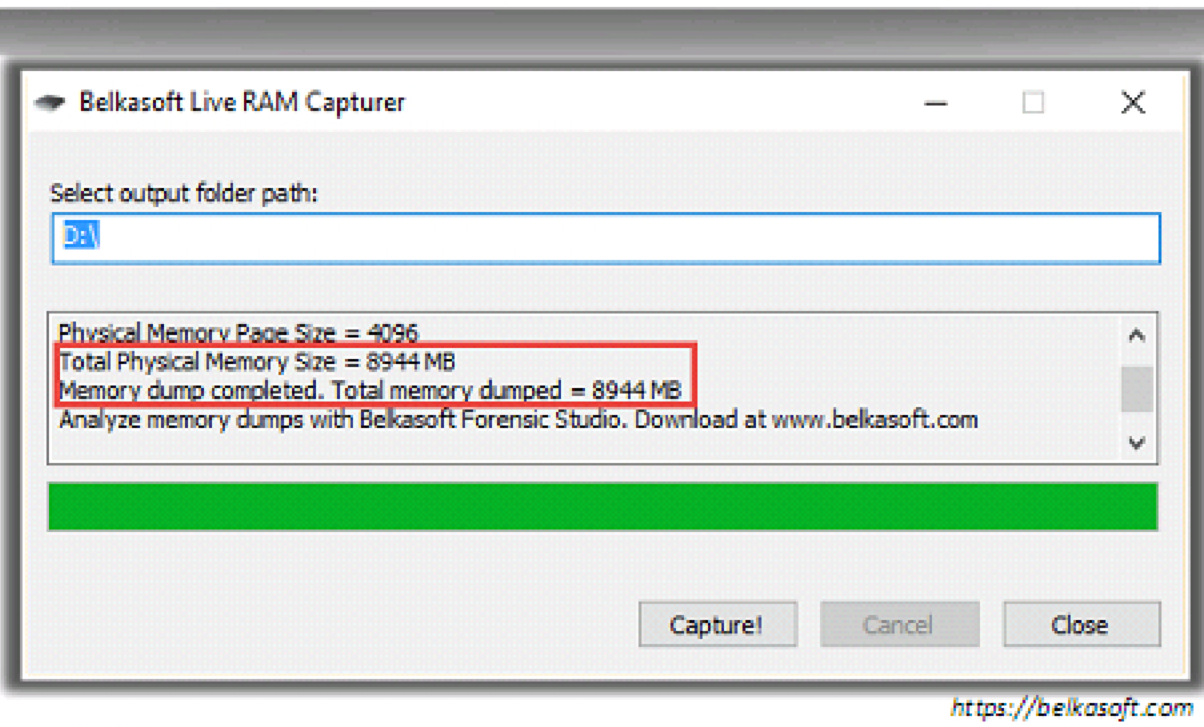
Directory Monitor can be used by the investigators for the surveillance of certain directories and network shares and will notify the investigator of file changes/access, deletions, modifications, and new files in real-time. Users and processes making the changes can also be detected. It provides text logs, automation via script/application execution, emailing, writing to a database, sound notifications, etc.

The tool monitors local directories or network shares including hidden/private shares, enable snapshots to ensure changes can be detected while the network is down and even during power outages.

Artifacts Left by Dropbox Client on Windows (Cont'd)

- If the Dropbox client is installed on the PC, you can find information about the **sessions in RAM**. For this, first you need to run tools such as RAM Capturer to dump the RAM contents and then use a hex editor tool to analyze the RAM contents
- **RAM Capturer:**

  Forensic tool that allows to reliably extract the entire contents of computer's volatile memory – even if protected by an active anti-debugging or anti-dumping system



Select output folder path: D:\

```
Physical Memory Page Size = 4096
Total Physical Memory Size = 8944 MB
Memory dump completed. Total memory dumped = 8944 MB
Analyze memory dumps with Belkasoft Forensic Studio. Download at www.belkasoft.com
```

https://belkasoft.com

RAM Capturer

Source: https://belkasoft.com

Investigators can find out the information about the sessions of a Dropbox client from the RAM analysis. For this, the investigator can run RAM Capturer tool to dump the RAM contents, and then use a hex editor tool to analyze the captured RAM contents.

RAM Capturer allows investigator to reliably extract the entire contents of computer's volatile memory to the required drive – even if protected by an active anti-debugging or anti-dumping system. The tool allows investigators with the ability to take snapshots of the computer's volatile memory (memory dumps) even if an anti-dumping protection is active for the drive.

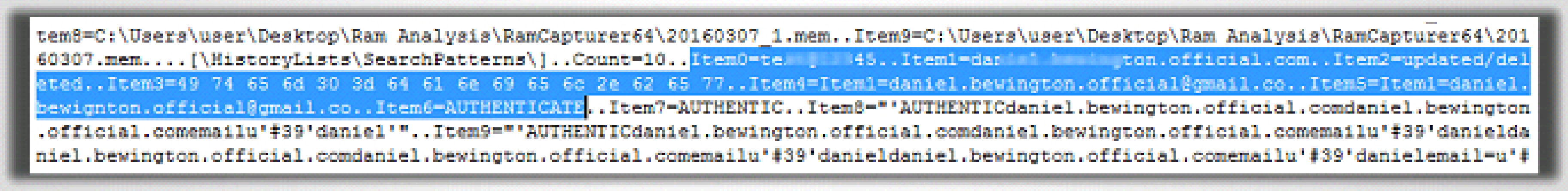
Artifacts Left by Dropbox Client on Windows (Cont'd)

- **HxD**:

  HxD is a hex editor which, additionally to raw disk editing and modifying of main memory (RAM), handles files of any size

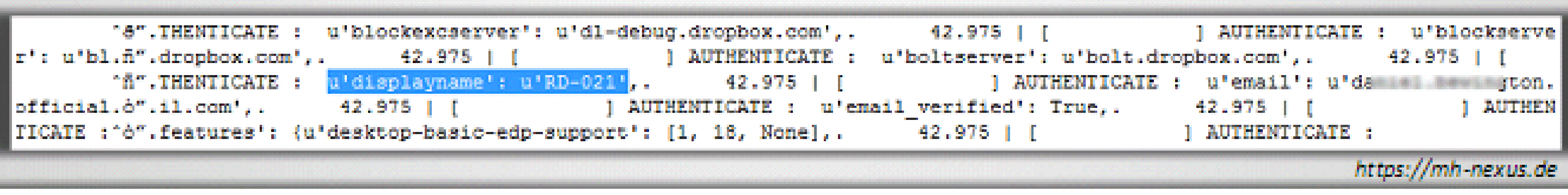
- **Given below are the strings that assists you to find out information of evidentiary value** (such as email ID, display name, filecache.dbx path, Server time, file list, and deleted file):

  - **AUTHENTICATE –** provides login credentials



```
tem8=C:\Users\user\Desktop\Ram Analysis\RamCapturer64\20160307_1.mem..Item9=C:\Users\user\Desktop\Ram Analysis\RamCapturer64\201
60307.mem....[\HistoryLists\SearchPatterns\]..Count=10..Item0=te[redacted]45..Item1=da[redacted]ton.official.com..Item2=updated/del
eted..Item3=49 74 65 6d 30 3d 64 61 6e 69 65 6c 2e 62 65 77..Item4=Item1=daniel.bewington.official@gmail.co..Item5=Item1=daniel.
bewignton.official@gmail.co..Item6=AUTHENTICATE..Item7=AUTHENTIC..Item8="'AUTHENTICdaniel.bewington.official.comdaniel.bewington
.official.comemailu'#39'daniel'"..Item9="'AUTHENTICdaniel.bewington.official.comdaniel.bewington.official.comemailu'#39'danielda
niel.bewington.official.comdaniel.bewington.official.comemailu'#39'danieldaniel.bewington.official.comemailu'#39'danielemail=u'#
```

  - **DisplayName –** provides logged in user's name



```
       ^ê".THENTICATE :  u'blockexcserver': u'dl-debug.dropbox.com',.      42.975 | [              ] AUTHENTICATE :  u'blockserve
r': u'bl.ñ".dropbox.com',.      42.975 | [              ] AUTHENTICATE :  u'boltserver': u'bolt.dropbox.com',.      42.975 | [
       ^ñ".THENTICATE :  u'displayname': u'RD-021',.      42.975 | [              ] AUTHENTICATE :  u'email': u'da[redacted]gton.
official.ò".il.com',.      42.975 | [              ] AUTHENTICATE :  u'email_verified': True,.      42.975 | [              ] AUTHEN
TICATE :^ò".features': {u'desktop-basic-edp-support': [1, 18, None],.      42.975 | [              ] AUTHENTICATE :
```

https://mh-nexus.de

Note: Also, the information mentioned above can be obtained from within **Hiberfil.sys** and **Pagefile.sys** located in **C:\**

HXD

Source: https://mh-nexus.de

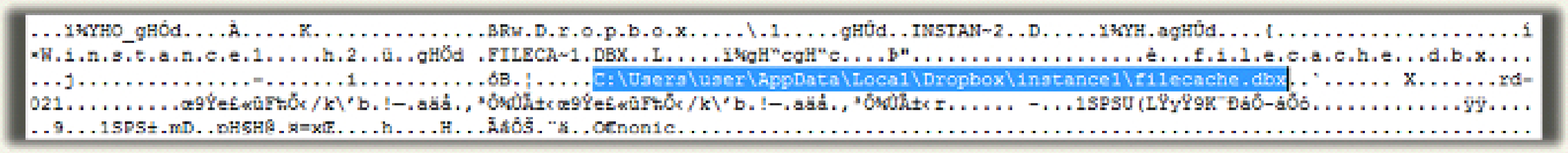
HXD is a hex editor allowing users to edit, modify the raw binary content of a file or a disk of any size.

The tool features; operations such as searching, replacing, exporting, checksums/ digests, insertion of byte patterns, a file shredder, concatenation or splitting of files, statistics, analyze malware, patch programmers, repair hard drive tables, perform file comparisons, create cheats, etc. The tool assists investigators in finding out information of evidentiary value such as email ID, display name, filecache.dbx path, Server_time, file list, and updated/deleted files.

Investigators can track the logged in credentials of the required Dropbox account by searching the RAM dump using the string AUTHENTICATE and the logged in user's name can be obtained using the string DisplayName.

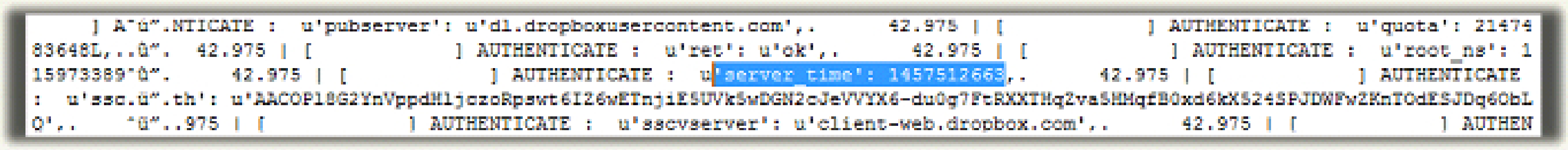
Artifacts Left by Dropbox Client on Windows (Cont'd)

- **filecache.dbx -** displays path for filecache.dbx



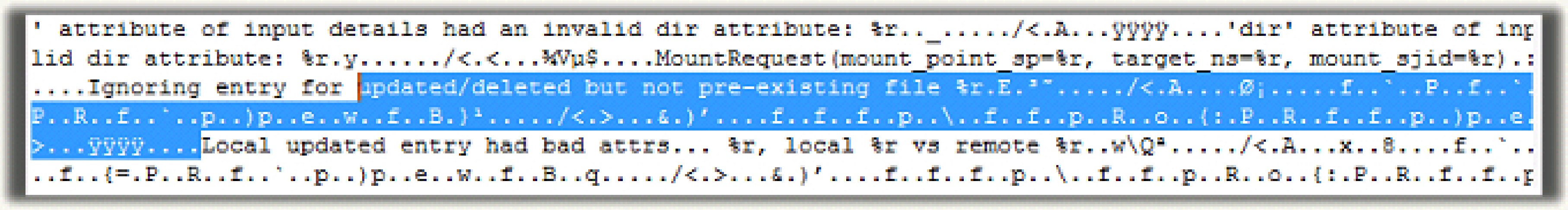
```
...ì¾YHO_gHÓd....À.....K...............BRw.D.r.o.p.b.o.x.....\.1.....gHÚd..INSTAN~2..D.....ì¾YH.agHÚd....(.....................i
•W.i.n.s.t.a.n.c.e.1.....h.2..ü..gHÖd .FILECA~1.DBX..L.....ì¾gH"cgH"c....Þ"...................è...f.i.l.e.c.a.c.h.e...d.b.x....
...j................-.......i...........óB.¦.....C:\Users\user\AppData\Local\Dropbox\instance1\filecache.dbx..`...... X.......rd-
021..........œ9Ÿe£«ûF‰Õ‹/k\'b.!—.aää.,*Ô¾ÚÅ±‹œ9Ÿe£«ûF‰Õ‹/k\'b.!—.aää.,*Ô¾ÚÅ±‹r...... -...1SPSU(LŸyŸ9K¯ÐáÕ-áÕõ.............ÿÿ....
..9...1SPS±.mD..pH§H®.æ=xE....h....H...ÃáÕŠ.¨ä..Œnonic..................................................................
```

- **server_time -** provides server time



```
    ] A¯ü".NTICATE :  u'pubserver': u'dl.dropboxusercontent.com',.      42.975 | [             ] AUTHENTICATE :  u'quota': 21474
83648L,..û".  42.975 | [             ] AUTHENTICATE :  u'ret': u'ok',.      42.975 | [             ] AUTHENTICATE :  u'root_ns': 1
15973389ˆû".     42.975 | [             ] AUTHENTICATE :  u'server_time': 1457512663,.      42.975 | [             ] AUTHENTICATE
:  u'ssc.ü".th': u'AACOP18G2YnVppdH1jczoRpswt6I26wETnjiESUVk5wDGN2cJeVVYX6-du0g7FtRXXTHq2va5HMqfB0xd6kX524SPJDWFw2KnTOdESJDq6ObL
Q',.    ˆû"..975 | [             ] AUTHENTICATE :  u'sscvserver': u'client-web.dropbox.com',.      42.975 | [             ] AUTHEN
```

- **updated/deleted -** displays updated/deleted file



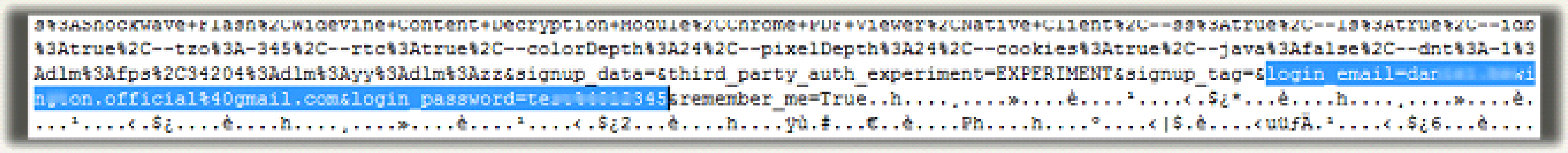
```
' attribute of input details had an invalid dir attribute: %r.._...../<.A...ÿÿÿÿ....'dir' attribute of inp
lid dir attribute: %r.y....../<.<...¾Vµ$....MountRequest(mount_point_sp=%r, target_ns=%r, mount_sjid=%r).:
....Ignoring entry for updated/deleted but not pre-existing file %r.E.²˜...../<.A....Ø¡.....f..`..P..f..`.
P..R..f..`..p..)p..e..w..f..B.)¹...../<.>...&.)'....f..f..f..p..\..f..f..p..R..o..{:.P..R..f..f..p..)p..e.
>...ÿÿÿÿ....Local updated entry had bad attrs... %r, local %r vs remote %r..w\Qª...../<.A...x..8....f..`..
..f..{=.P..R..f..`..p..)p..e..w..f..B..q...../<.>...&.)'....f..f..f..p..\..f..f..p..R..o..{:.P..R..f..f..p
```

Investigators can trace the path of filecache.dbx by searching the RAM dump using hex editor with the string filecache.dbx, use the string server_time to trace the server time of a particular instance and use the string updated/deleted to find the updated and deleted files.

The configuration files of a Dropbox, stored in SQLite database filesare located within the instance (n) of Dropbox folder in Appdata of Users profile. Filecache.dbx and config.dbx file are encrypted SQLite databases that store the information of files synced to cloud using Dropbox. SQLite browser can display these files when decrypted. Current version of Dropbox makes use of encrypted SQLite DB files.

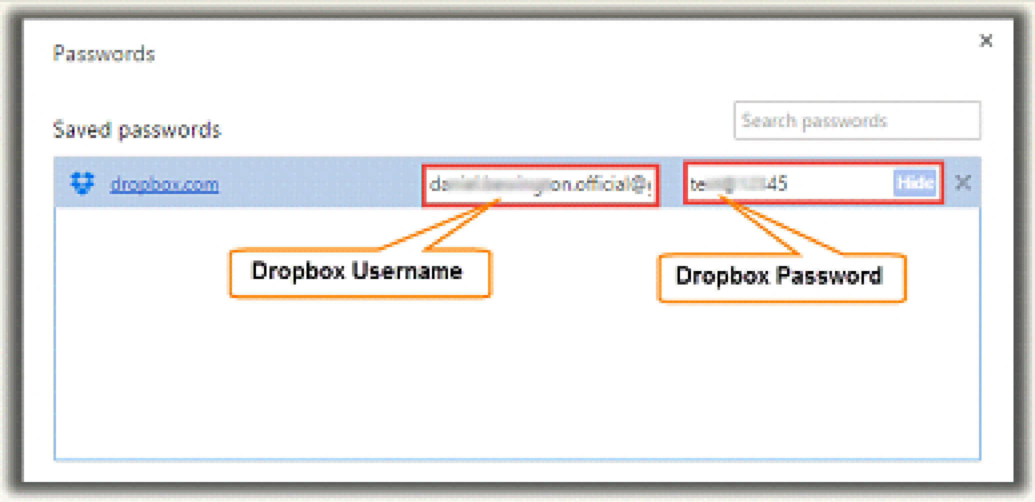
Artifacts Left by Dropbox Client on Windows (Cont'd)

- In case of Web-based Dropbox, you can find the username and password in clear from RAM dump using strings:
  - **login_email**
  - **login_password**



```
s%3AShockwave+Flash%2CWidevine+Content+Decryption+Module%2CChrome+PDF+Viewer%2CNative+Client%2C--ss%3Atrue%2C--ls%3Atrue%2C--idb
%3Atrue%2C--tzo%3A-345%2C--rtc%3Atrue%2C--colorDepth%3A24%2C--pixelDepth%3A24%2C--cookies%3Atrue%2C--java%3Afalse%2C--dnt%3A-1%3
Adlm%3Afps%2C34204%3Adlm%3Ayy%3Adlm%3Azz&signup_data=&third_party_auth_experiment=EXPERIMENT&signup_tag=&login_email=dar[redacted]wi
n[redacted]on.official%40gmail.com&login_password=te[redacted]12345&remember_me=True..h....,....»....è....¹....‹.$¿*...è....h....,....»....è.
...¹....‹.$¿....è....h....,....»....è....¹....‹.$¿2...è....h....ÿù.#...€..è....Ph....h....°....‹|$.è....‹uûfÃ.¹....‹.$¿6...è....
```

- Also, you can find the Web-based Dropbox login credentials stored somewhere in the PC (ex: browser). Screenshot below is with respect to the Chrome

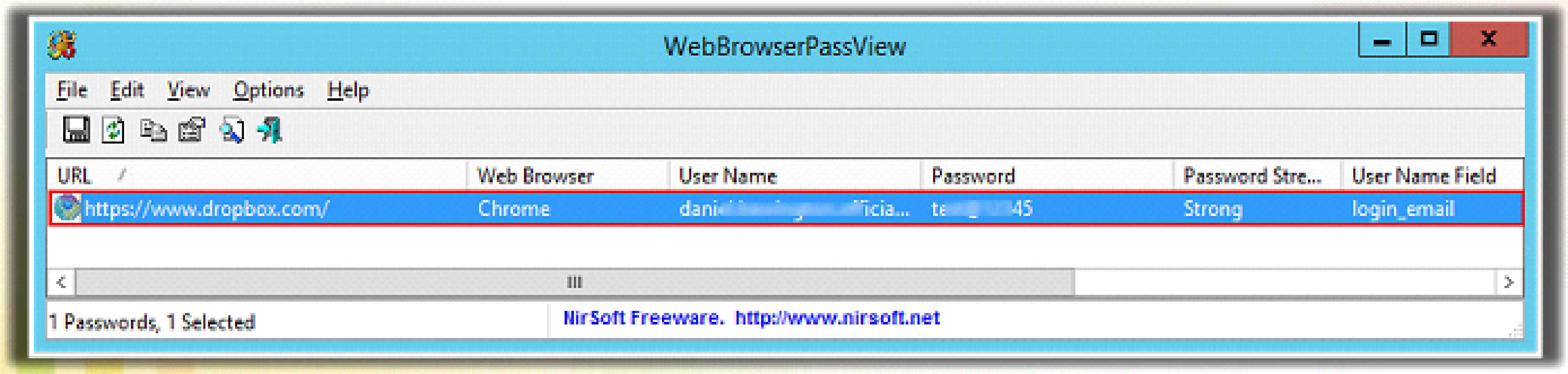


Investigators can find out the logged in Dropbox credentials of a web-based application by exploring RAM dump using the strings login_email for the user's email ID and login_password for the password of the account.

Investigators can also trace the stored credentials of the web-based Dropbox application within the PC from the sources like browsers.

Artifacts Left by Dropbox Client on Windows (Cont'd)

- You can use tools such as **WebBrowserPassView**, a password recovery tool that reveals the passwords stored by the following Web browsers: Internet Explorer (Version 4.0 - 11.0), Mozilla Firefox, Google Chrome, Safari, and Opera



URL	Web Browser	User Name	Password	Password Stre...	User Name Field
https://www.dropbox.com/	Chrome	dani[redacted]ficia...	te[redacted]45	Strong	login_email

1 Passwords, 1 Selected | NirSoft Freeware. http://www.nirsoft.net

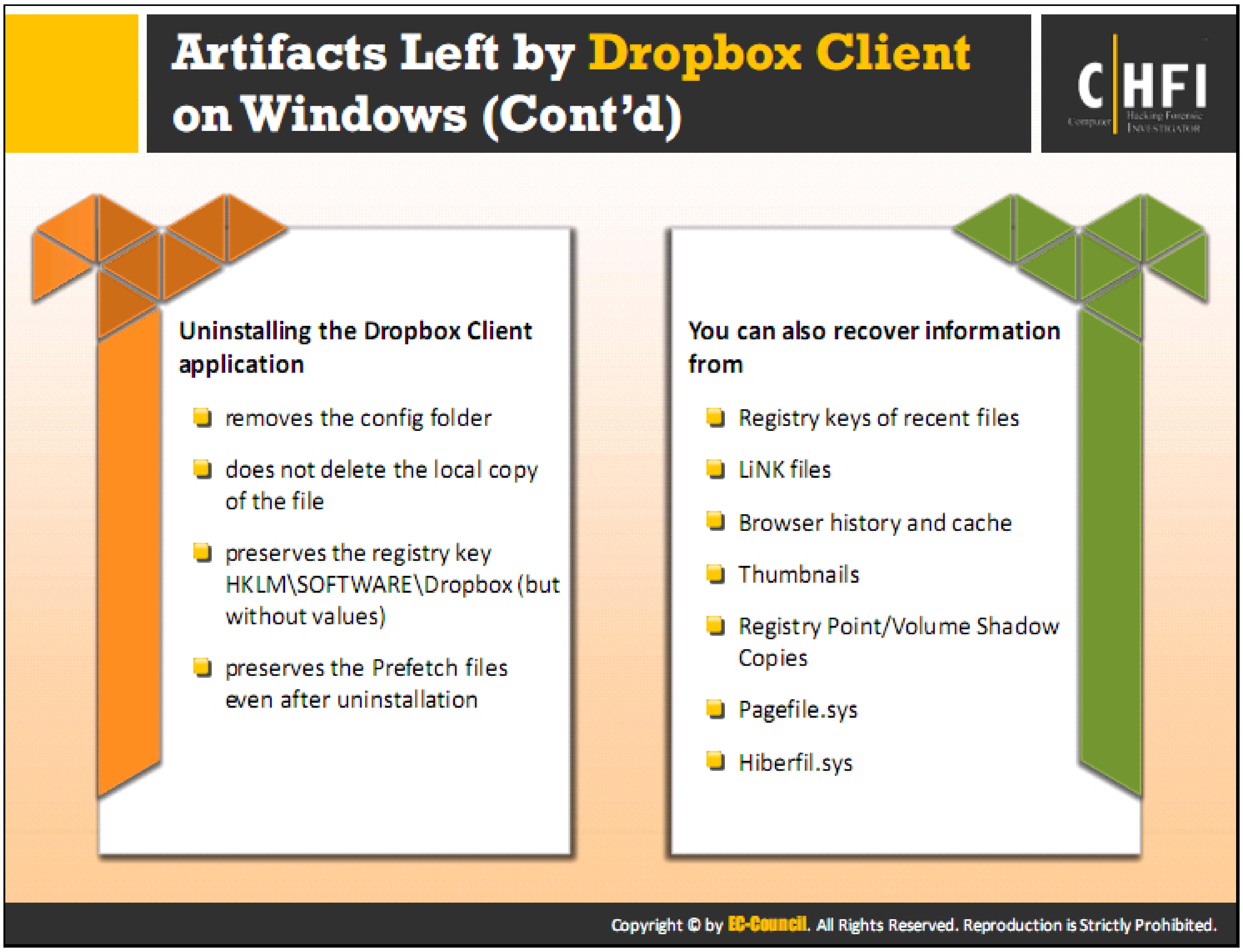
http://www.nirsoft.net

WebBrowserPassView

Source: http://www.nirsoft.net

Investigators can use tools such as WebBrowserPassView, a password recovery tool that reveals the passwords stored by the following Web browsers: Internet Explorer (Version 4.0 - 11.0), Mozilla Firefox, Google Chrome, Safari, and Opera.

The tool can also be used to recover the lost/forgotten password of any website be it Facebook, Google, Yahoo as long as it is stored in the user's browser. The retrieved passwords can be saved in text/html/csv/xml file by using the Save Selected Items.



Artifacts Left by Dropbox Client on Windows (Cont'd)

Uninstalling the Dropbox Client application

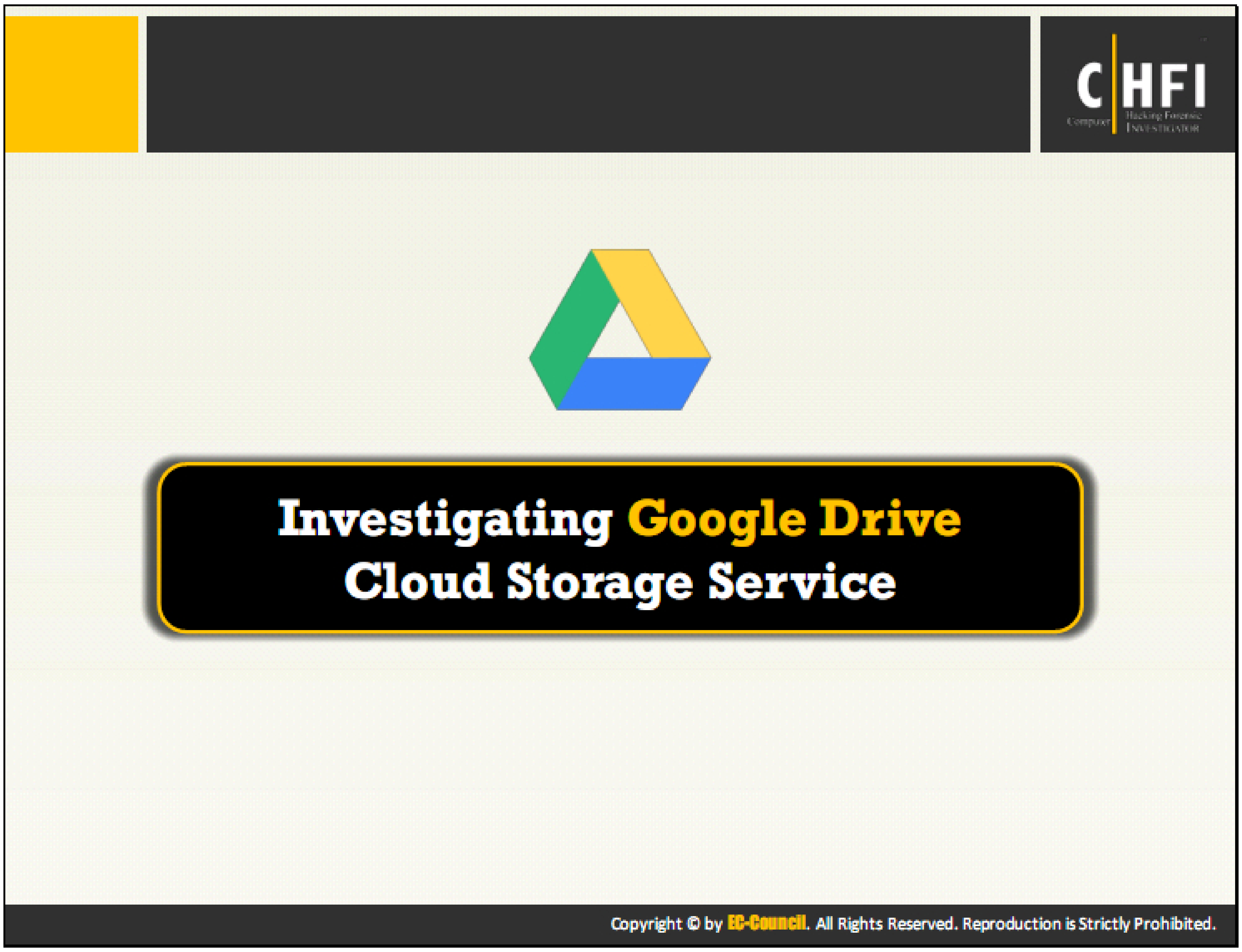
- removes the config folder
- does not delete the local copy of the file
- preserves the registry key HKLM\SOFTWARE\Dropbox (but without values)
- preserves the Prefetch files even after uninstallation

You can also recover information from

- Registry keys of recent files
- LiNK files
- Browser history and cache
- Thumbnails
- Registry Point/Volume Shadow Copies
- Pagefile.sys
- Hiberfil.sys

If a user uninstalls an application or a client, the system deletes it files and folders from the local disks. However, some files stay even after uninstalling the application, such as local copy, Prefetch files, registry keys without the values, etc.

Investigators can recover information related to Dropbox from the registry keys of recent files, LiNK files, Browser history and cache, thumbnails, etc., which remain in the system even after the user has uninstalled the application.



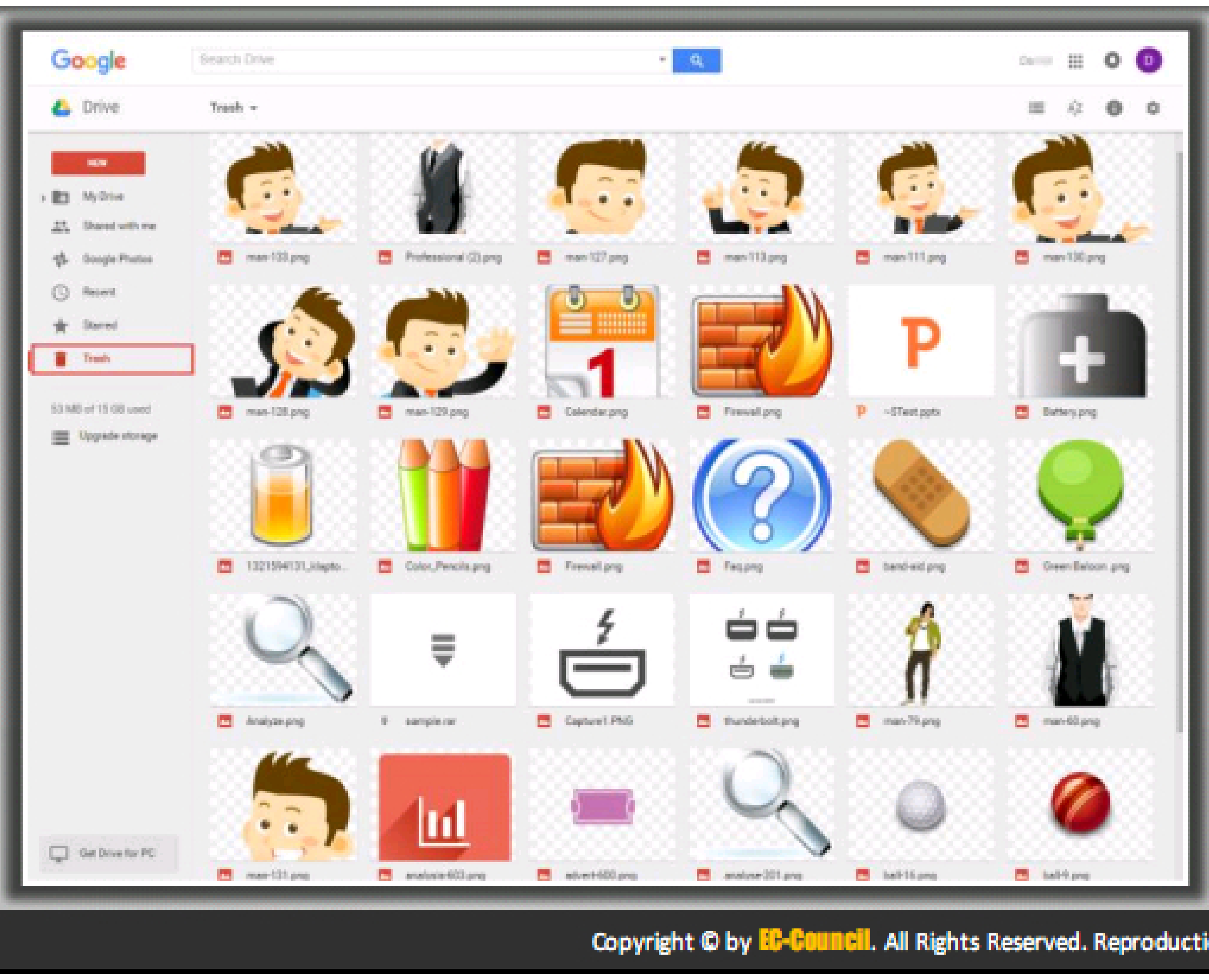
Investigating Google Drive Cloud Storage Service

Google drive is online file storage and sharing service from Google that supports sharing of different types of files such as pictures, videos, documents, spreadsheets, presentations, etc. The service supports various devices including desktops, mobiles, etc. through different modes such as desktop client, web portal, mobile application, etc.

The users can also invite others to view, download and collaborate on the files. The storage works in collaboration with Google Docs, Sheets, and Slides, an office suite that allows users to editing the documents, spreadsheets, presentations, drawings, forms, and more online.

Artifacts Left by Google Drive Web Portal

- You can login to the user's profile and access Google Drive's information about deleted files
- Click on the Trash tab to view the deleted files



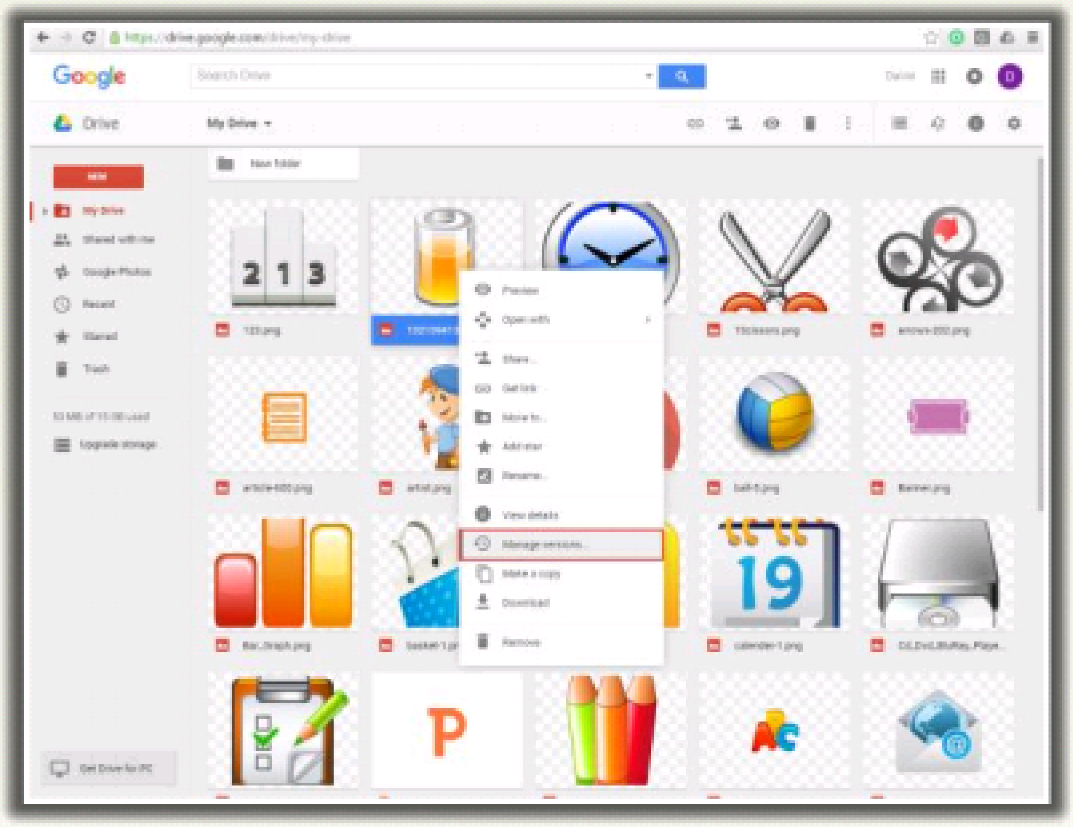
Google Drive does not discard the files completely when the users delete them from their accounts instead it keeps them in the Trash folder temporarily. Investigators can check the Trash folder in the drive account to recover these files, as they can contain crucial evidence. Analysis of the deleted files can provide details such as the author of the file, date of creation and modification, etc.

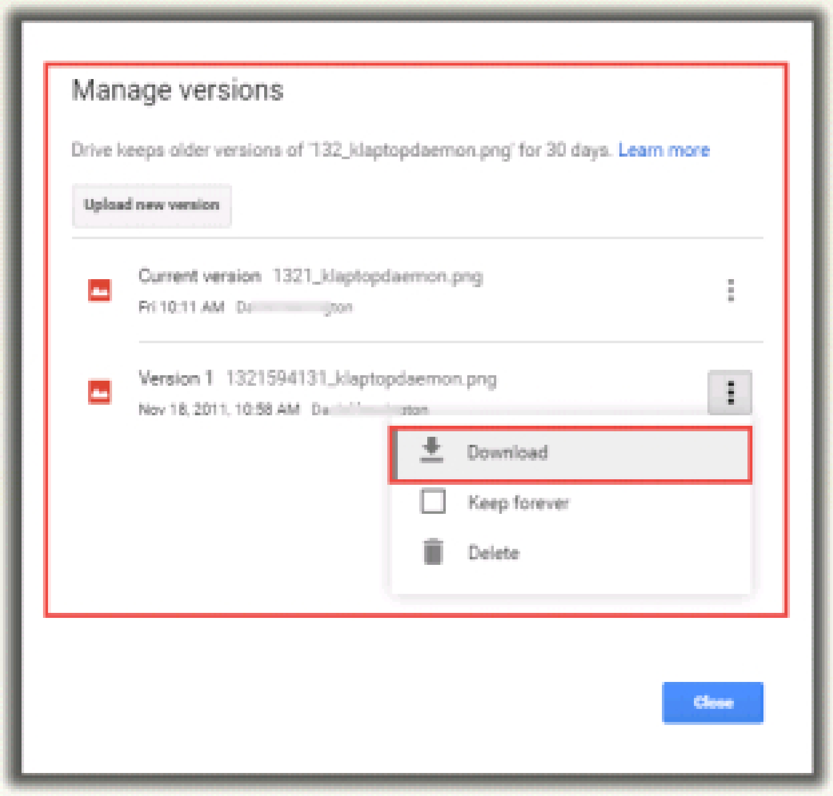
To recover the deleted files in a Google Drive account:

- First login to the account
- Select the Trash folder from the left side menu list of the account
- Right click on file required to restore and select the Restore option from the menu

Artifacts Left by Google Drive Web Portal (Cont'd)

- You can view version history for each file and can recover previous version of a file
- Right-click the file and select Manage versions...




Manage versions

Drive keeps older versions of '132_klaptopdaemon.png' for 30 days. Learn more

Upload new version

Current version 1321_klaptopdaemon.png
Fri 10:11 AM [redacted]

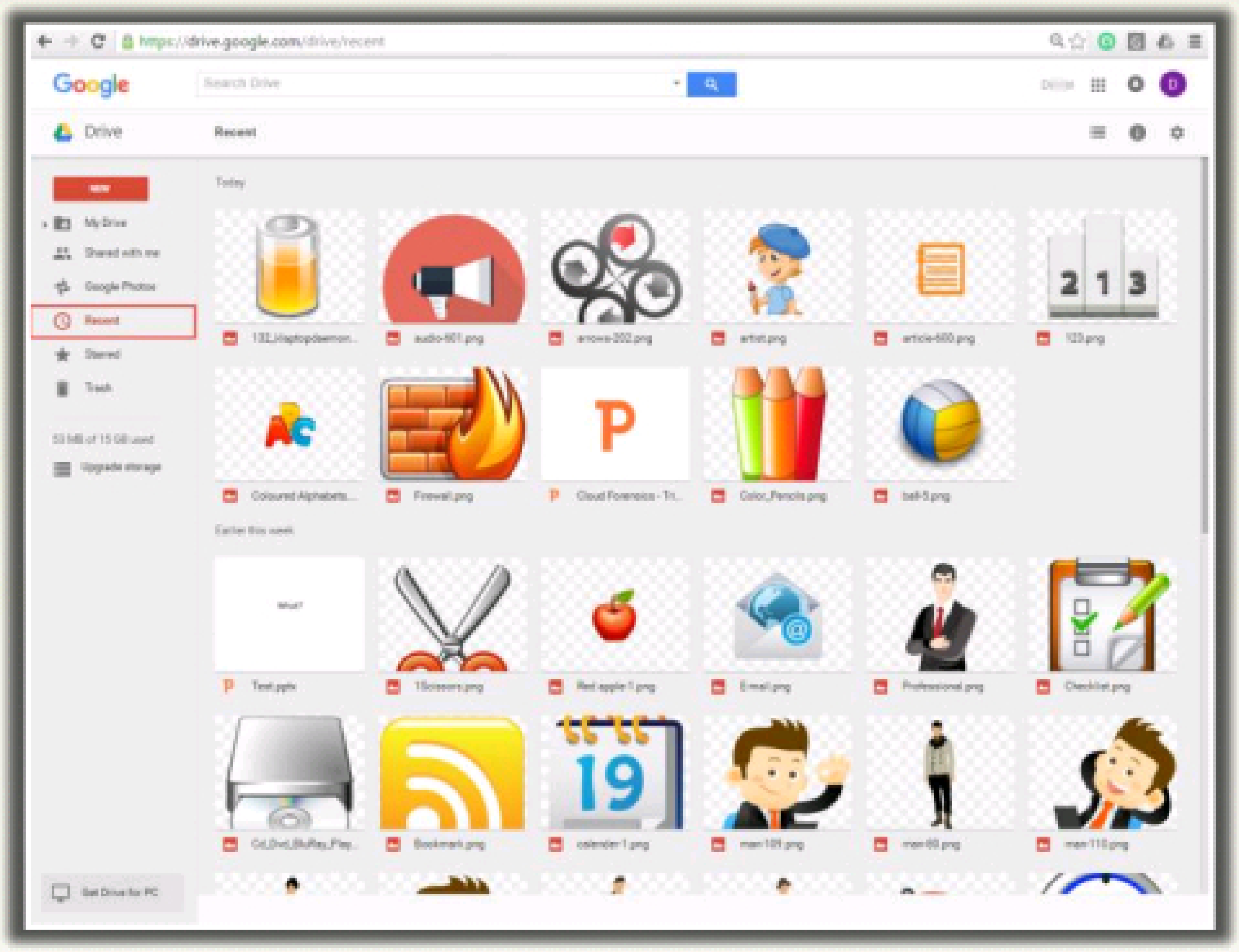
Version 1 1321594131_klaptopdaemon.png
Nov 18, 2011, 10:58 AM [redacted]

Google Drive stores versions of the file, when users edit it and also tracks if the user moves a file to another location. Using this feature, the investigators can download previous versions of files available to the files modified during the security incident.

- In the Google Drive account homepage, right click on the required file
- Select Manage versions... option from the drop down menu
- In the Manage versions window, select the version required to analyze
- Click the options ⋮ button present at the end of the file name
- Click the Download option from the list

Artifacts Left by Google Drive Web Portal (Cont'd)

You can view the recent visits by clicking the Recent tab



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Google Drive stores logs of the recent activities as well as sorts the stored files in order of the activity performed on them. Investigators can check these features to view which files the users or attackers had finally accessed and what kind of activity they had carried out on their visit.

Step to view the recently modified files:

- Login to the account
- Select the Recent menu option from the left side menu list
- The website will sort the files in order of activity
- To view more details of the activity performed, right-click the file and select view details option from the drop down list

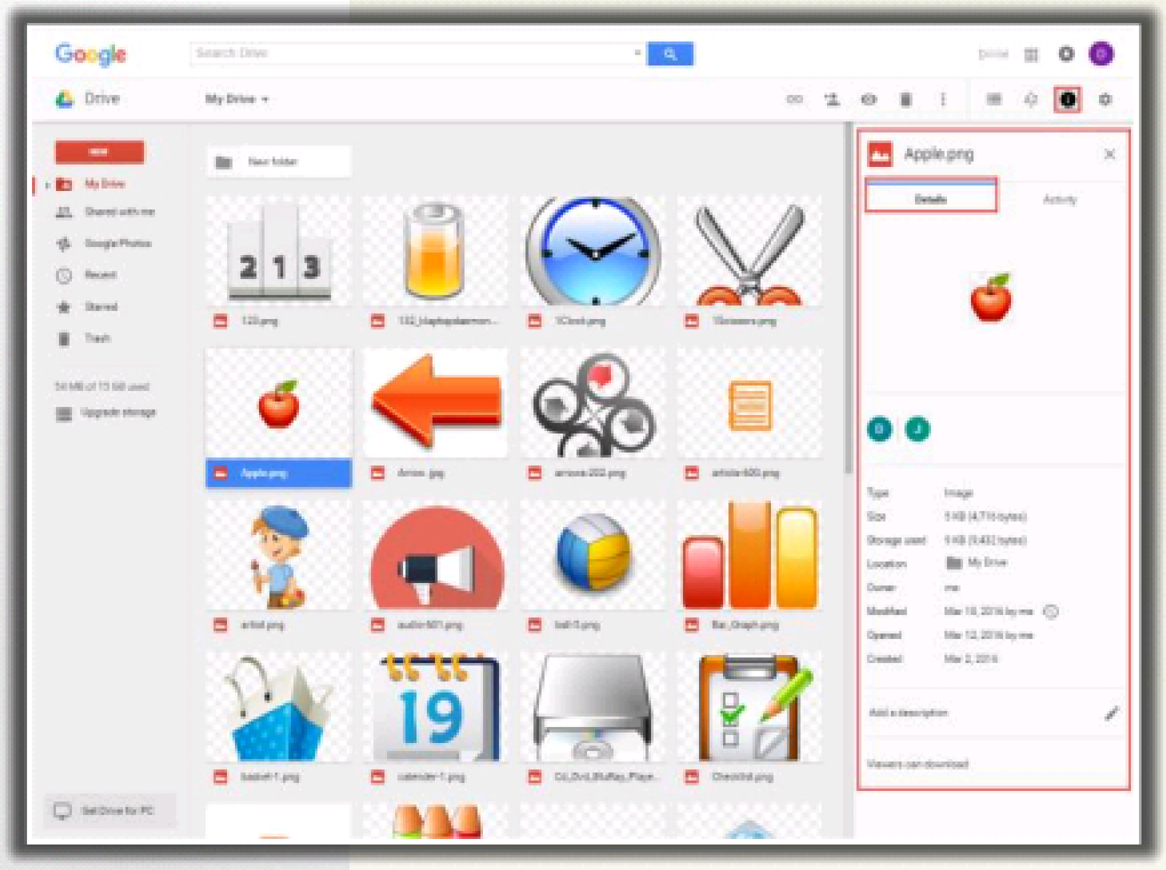
Steps to view the recent activity:

- In the account, the click on the view details ⓘ button from the top right side of the homepage
- The page will display all the recent activities and the users associated with it, if any

Artifacts Left by Google Drive Web Portal (Cont'd)

- You can view valuable information of a particular item by selecting the item and clicking on the information button (●) on the top-right
- For each item, there exists 2 panes: Details and Activity

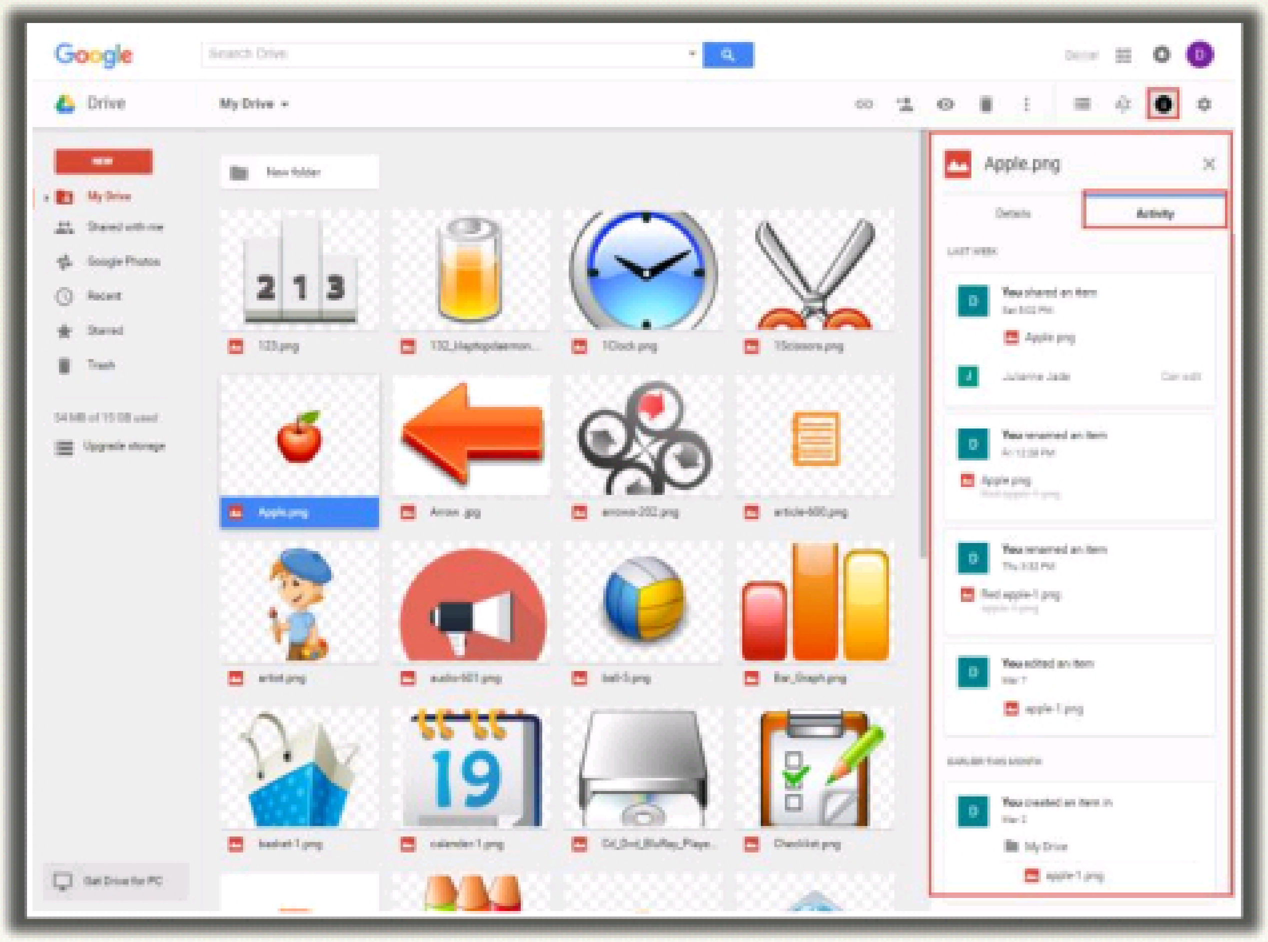
Details pane – Contains information about the selected item such as the owner, the size of the file, when it was created, opened, modified, etc.



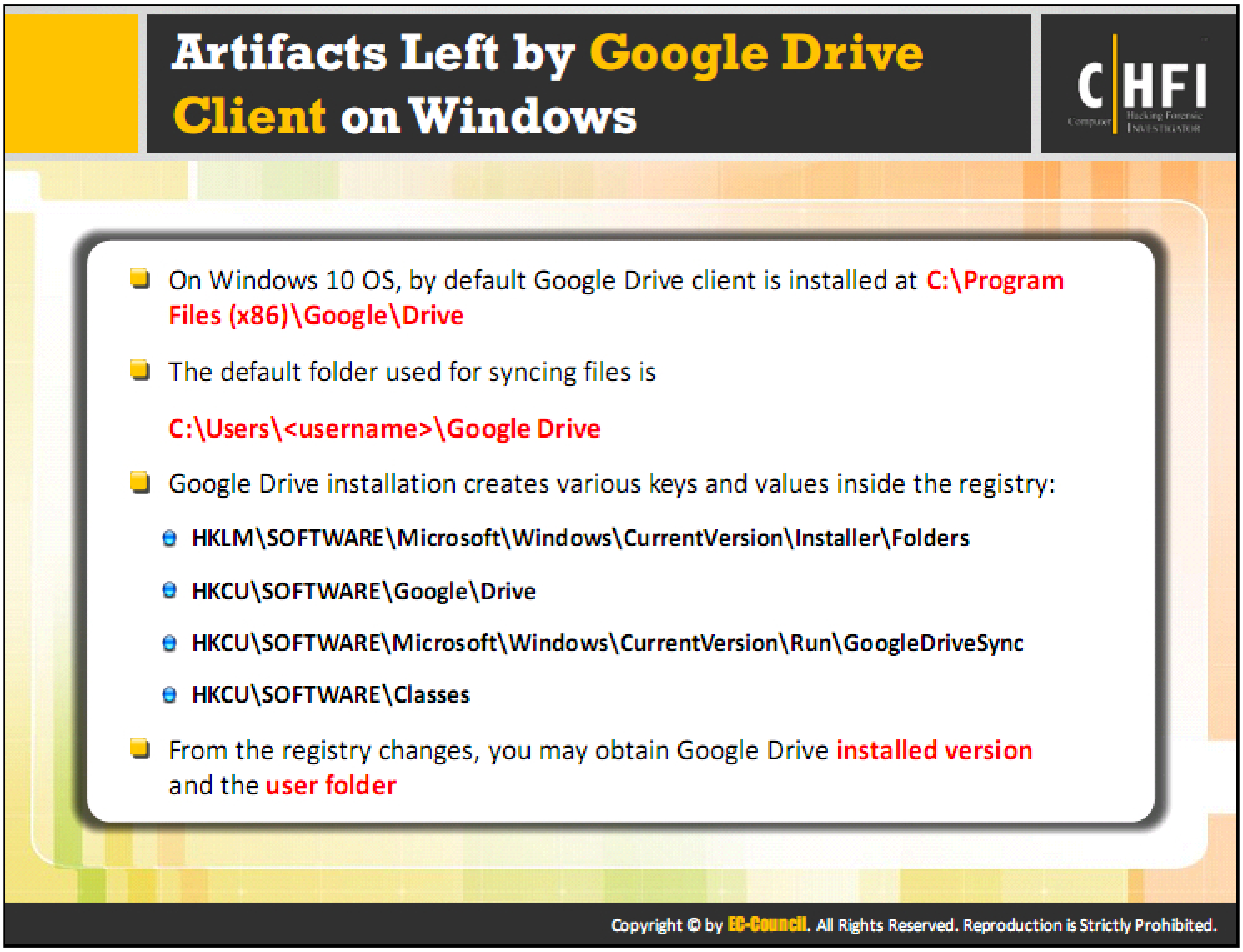
Artifacts Left by Google Drive Web Portal (Cont'd)

Activity Pane

Activity pane – shows activities performed on a selected item such as moving and removing, renaming, uploading, sharing and unsharing, editing and commenting



Note: You can click My Drive in the left-hand navigation, then information button on the top-right to view details and track activity of all items created in, or uploaded to, "My Drive."



Artifacts Left by Google Drive Client on Windows

- On Windows 10 OS, by default Google Drive client is installed at **C:\Program Files (x86)\Google\Drive**
- The default folder used for syncing files is

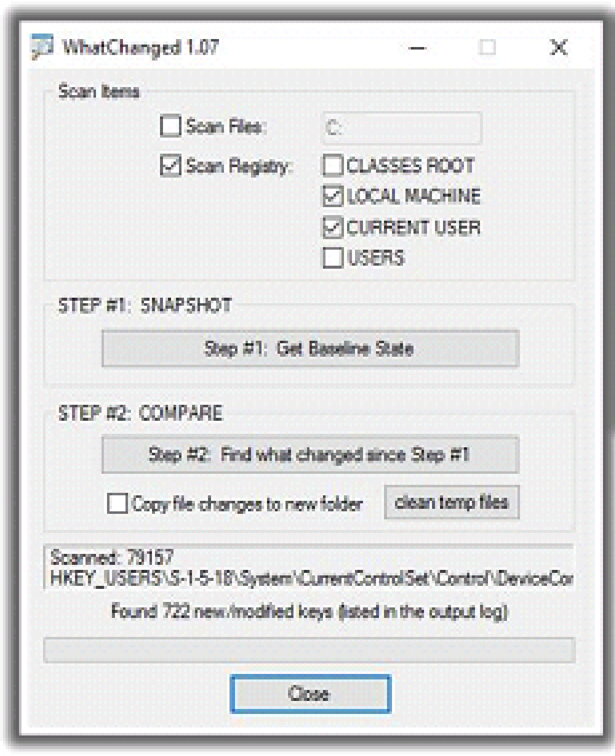
  C:\Users\<username>\Google Drive
- Google Drive installation creates various keys and values inside the registry:
  - **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders**
  - **HKCU\SOFTWARE\Google\Drive**
  - **HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\GoogleDriveSync**
  - **HKCU\SOFTWARE\Classes**
- From the registry changes, you may obtain Google Drive **installed version** and the **user folder**

All applications store their data in specific folders in the system. When users install the Google Drive client on their devices, it uses space to store application specific files and folders, which store the cache, thumbnails, and other files an application requires to perform well.

The default installation path of Google Drive client in Windows 10 OS is C:\Program Files (x86)\Google\Drive. The default folder used in syncing is C:\Users\<username>\Google Drive. The installation creates various keys and values inside the registry from these investigators can make out the installed version and the user folder from the registry changes for their investigation.

Artifacts Left by Google Drive Client on Windows (Cont'd)

You can use tools such as **WhatChanged Portable** to scan for modified files and registry entries


WhatChanged 1.07

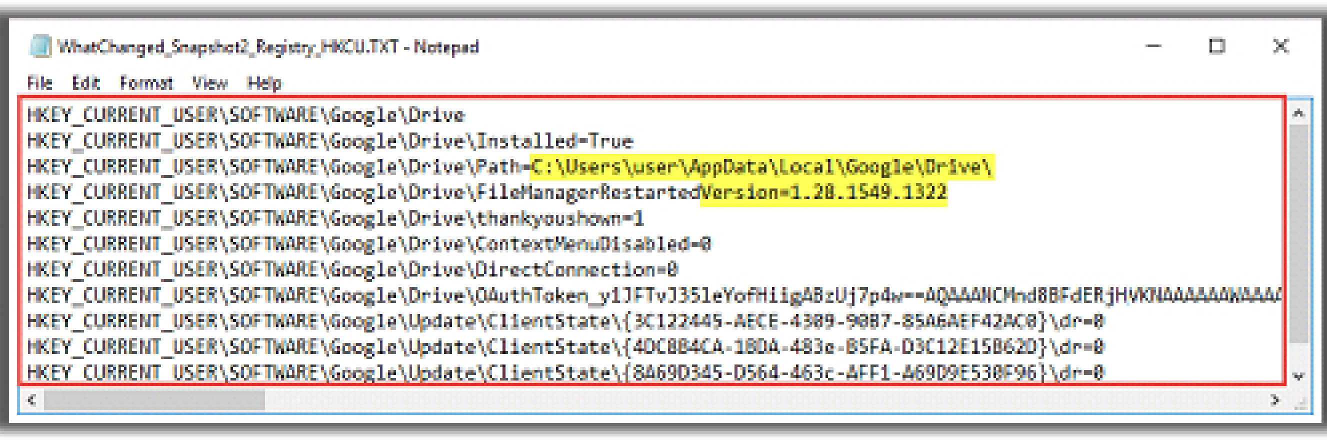
Scan Items
□ Scan Files: C:
☑ Scan Registry: □ CLASSES ROOT
☑ LOCAL MACHINE
☑ CURRENT USER
□ USERS

STEP #1: SNAPSHOT
Step #1: Get Baseline State

STEP #2: COMPARE
Step #2: Find what changed since Step #1
□ Copy file changes to new folder
clean temp files

```
Scanned: 79157
HKEY_USERS\S-1-5-18\System\CurrentControlSet\Control\DeviceCor
Found 722 new/modified keys (listed in the output log)
```

Close


WhatChanged_Snapshot2_Registry_HKCU.TXT - Notepad

File Edit Format View Help

```
HKEY_CURRENT_USER\SOFTWARE\Google\Drive
HKEY_CURRENT_USER\SOFTWARE\Google\Drive\Installed=True
HKEY_CURRENT_USER\SOFTWARE\Google\Drive\Path=C:\Users\user\AppData\Local\Google\Drive\
HKEY_CURRENT_USER\SOFTWARE\Google\Drive\FileManagerRestartedVersion=1.28.1549.1322
HKEY_CURRENT_USER\SOFTWARE\Google\Drive\thankyoushown=1
HKEY_CURRENT_USER\SOFTWARE\Google\Drive\ContextMenuDisabled=0
HKEY_CURRENT_USER\SOFTWARE\Google\Drive\DirectConnection=0
HKEY_CURRENT_USER\SOFTWARE\Google\Drive\OAuthToken_y1JFTvJ35leYofHiigABzUj7p4w==AQAAANCMnd8BFdERjHVKNAAAAAAWAAAA
HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{3C122445-AECE-4309-9087-85A6AEF42AC0}\dr=0
HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{4DC8B4CA-1BDA-483e-B5FA-D3C12E15B62D}\dr=0
HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}\dr=0
```

After the installation of Google Drive client in Windows 10 OS few changes occur in the registry. Investigators can use WhatChanged Portable to track the modified files and the registry entries.

WhatChanged Portable is useful for checking program installations. It is a system utility that scans for modified files and registry entries. It uses the 'brute-force method' to check files and the registry.

There are two steps for using What Changed Portable software:

- First, take a snapshot to get the current state of the computer before installing Google Drive client;
- Second, run it again to check the differences since the previous snapshot, after installing Google Drive client.

  By comparing both the screen shots, investigators can find out the list files modified in the registry and the entries made to the registry.

WhatChanged

Source: http://portableapps.com

What Changed is a system utility that scans for modified files and registry entries. It is useful for checking program installations. There are two steps for using What Changed: 1) First, take a snapshot to get the current state of the computer; 2) Second, run it again to check the differences since the previous snapshot. What Changed uses the 'brute force method' to check files and the registry.

Artifacts Left by Google Drive Client on Windows (Cont'd)

Configuration files are saved inside the installation folder in the user profile

C:\Users\<*username*>\AppData\Local\Google\Drive\user_default

Executable and libraries are stored at:

C:\Program Files (x86)\Google\Drive

Files created during Google Drive client installation:

LiNK files or Shortcut files:

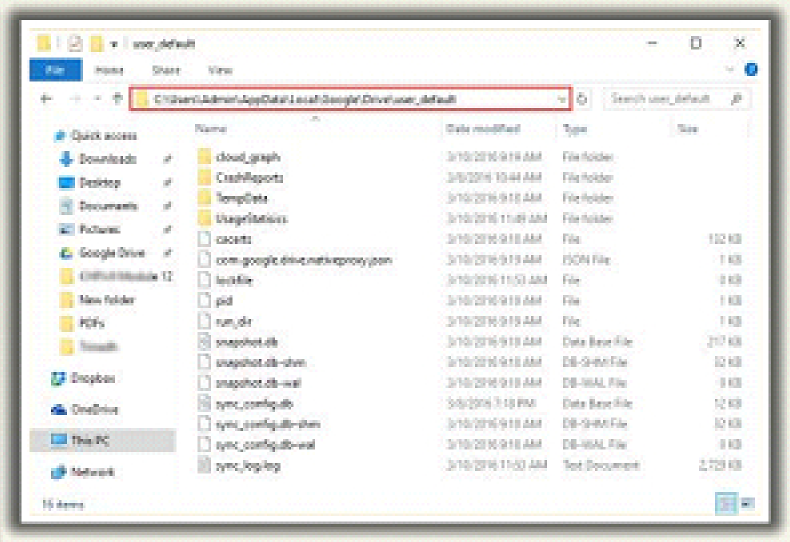
C:\Users\<username>\Desktop\Google Drive.lnk

C:\Users\<username>\Links\Google Drive.lnk

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Google Drive\Google Drive.lnk

Prefetch Files:

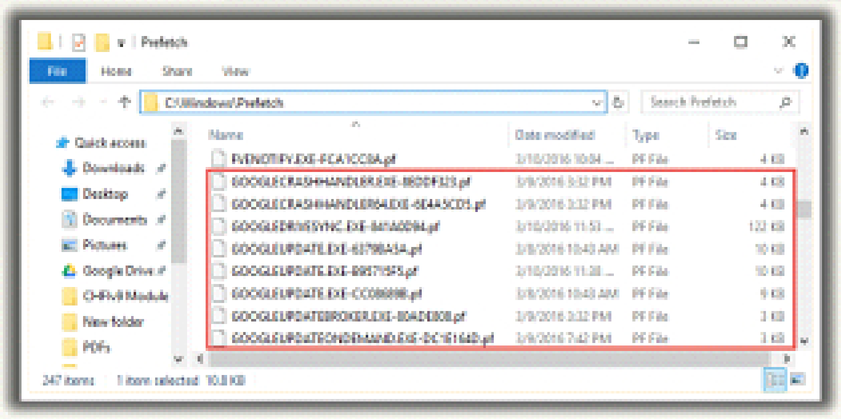
Located at C:\Windows\Prefetch



C:\Users\Admin\AppData\Local\Google\Drive\user_default

Name	Date modified	Type	Size
cloud_graph	3/10/2016 9:18 AM	File folder	
CrashReports	3/9/2016 10:44 AM	File folder	
TempData	3/10/2016 9:18 AM	File folder	
UsageStatistics	3/10/2016 11:49 AM	File folder	
cacerts	3/10/2016 9:18 AM	File	132 KB
com.google.drive.nativeproxy.json	3/10/2016 9:19 AM	JSON File	1 KB
lockfile	3/10/2016 11:53 AM	File	0 KB
pid	3/10/2016 9:19 AM	File	1 KB
run_dir	3/10/2016 9:19 AM	File	1 KB
snapshot.db	3/10/2016 9:18 AM	Data Base File	217 KB
snapshot.db-shm	3/10/2016 9:18 AM	DB-SHM File	32 KB
snapshot.db-wal	3/10/2016 9:18 AM	DB-WAL File	0 KB
sync_config.db	3/9/2016 7:18 PM	Data Base File	12 KB
sync_config.db-shm	3/10/2016 9:18 AM	DB-SHM File	32 KB
sync_config.db-wal	3/10/2016 9:18 AM	DB-WAL File	0 KB
sync_log.log	3/10/2016 11:50 AM	Text Document	2,729 KB

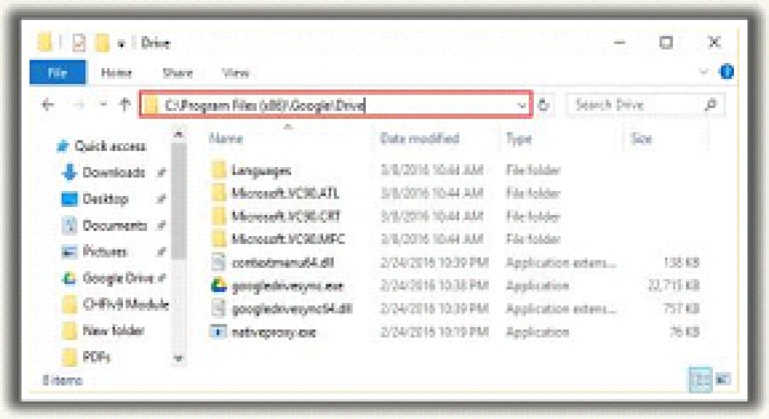
16 items



C:\Windows\Prefetch

Name	Date modified	Type	Size
FVENOTIFY.EXE-FCA1CC0A.pf	3/10/2016 10:04 ...	PF File	4 KB
GOOGLECRASHHANDLER.EXE-8BDDF323.pf	3/9/2016 3:32 PM	PF File	4 KB
GOOGLECRASHHANDLER64.EXE-6E4A5CD5.pf	3/9/2016 3:32 PM	PF File	4 KB
GOOGLEDRIVESYNC.EXE-841A0D94.pf	3/10/2016 11:53 ...	PF File	122 KB
GOOGLEUPDATE.EXE-63798A5A.pf	3/8/2016 10:43 AM	PF File	10 KB
GOOGLEUPDATE.EXE-B9571SF5.pf	3/10/2016 11:38 ...	PF File	10 KB
GOOGLEUPDATE.EXE-CC08698.pf	3/8/2016 10:43 AM	PF File	9 KB
GOOGLEUPDATEBROKER.EXE-80ADE808.pf	3/9/2016 3:32 PM	PF File	3 KB
GOOGLEUPDATEONDEMAND.EXE-DC1E164D.pf	3/9/2016 7:42 PM	PF File	3 KB

247 items 1 item selected 10.8 KB



C:\Program Files (x86)\Google\Drive

Name	Date modified	Type	Size
Languages	3/8/2016 10:44 AM	File folder	
Microsoft.VC90.ATL	3/8/2016 10:44 AM	File folder	
Microsoft.VC90.CRT	3/8/2016 10:44 AM	File folder	
Microsoft.VC90.MFC	3/8/2016 10:44 AM	File folder	
contextmenu64.dll	2/24/2016 10:39 PM	Application extens...	138 KB
googledrivesync.exe	2/24/2016 10:38 PM	Application	22,715 KB
googledrivesync64.dll	2/24/2016 10:39 PM	Application extens...	757 KB
nativeproxy.exe	2/24/2016 10:19 PM	Application	76 KB

8 items

During installation, Google Drive Client makes multiple changes in Windows 10 OS to accommodate the application settings. The application saves the configuration files and folders, storing of the executables and libraries required for running the application, as well as links and shortcut files. All these files contain information regarding the google drive account and its content. Therefore, they prove to be good evidence.

Artifacts Left by Google Drive Client on Windows (Cont'd)

- You can run tools such as DB Browser to view evidentiary data in the Sync_config.db
- **Information includes:**
  - Client version installed
  - Local Sync Root Path
  - User email ID

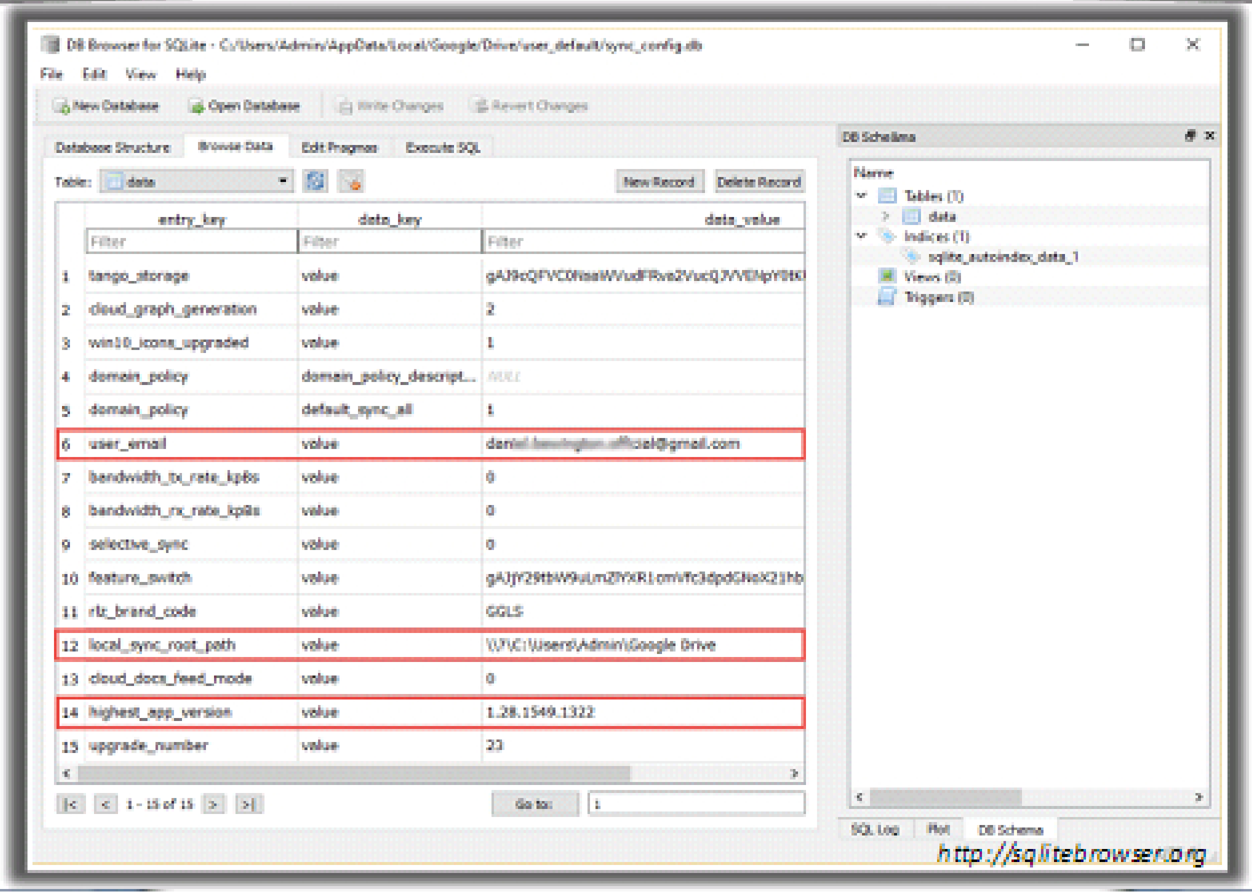


Table: data

	entry_key	data_key	data_value
1	tango_storage	value	gAJ9cQFVC0NaaWVudFRva2VucQJVVENpY0tK
2	cloud_graph_generation	value	2
3	win10_icons_upgraded	value	1
4	domain_policy	domain_policy_descript...	NULL
5	domain_policy	default_sync_all	1
6	user_email	value	daniel[redacted]cial@gmail.com
7	bandwidth_tx_rate_kpbs	value	0
8	bandwidth_rx_rate_kpbs	value	0
9	selective_sync	value	0
10	feature_switch	value	gAJjY29tbW9uLmZlYXR1cmVfc3dpdGNoX21hb
11	rlz_brand_code	value	GGLS
12	local_sync_root_path	value	\\?\C:\Users\Admin\Google Drive
13	cloud_docs_feed_mode	value	0
14	highest_app_version	value	1.28.1549.1322
15	upgrade_number	value	23

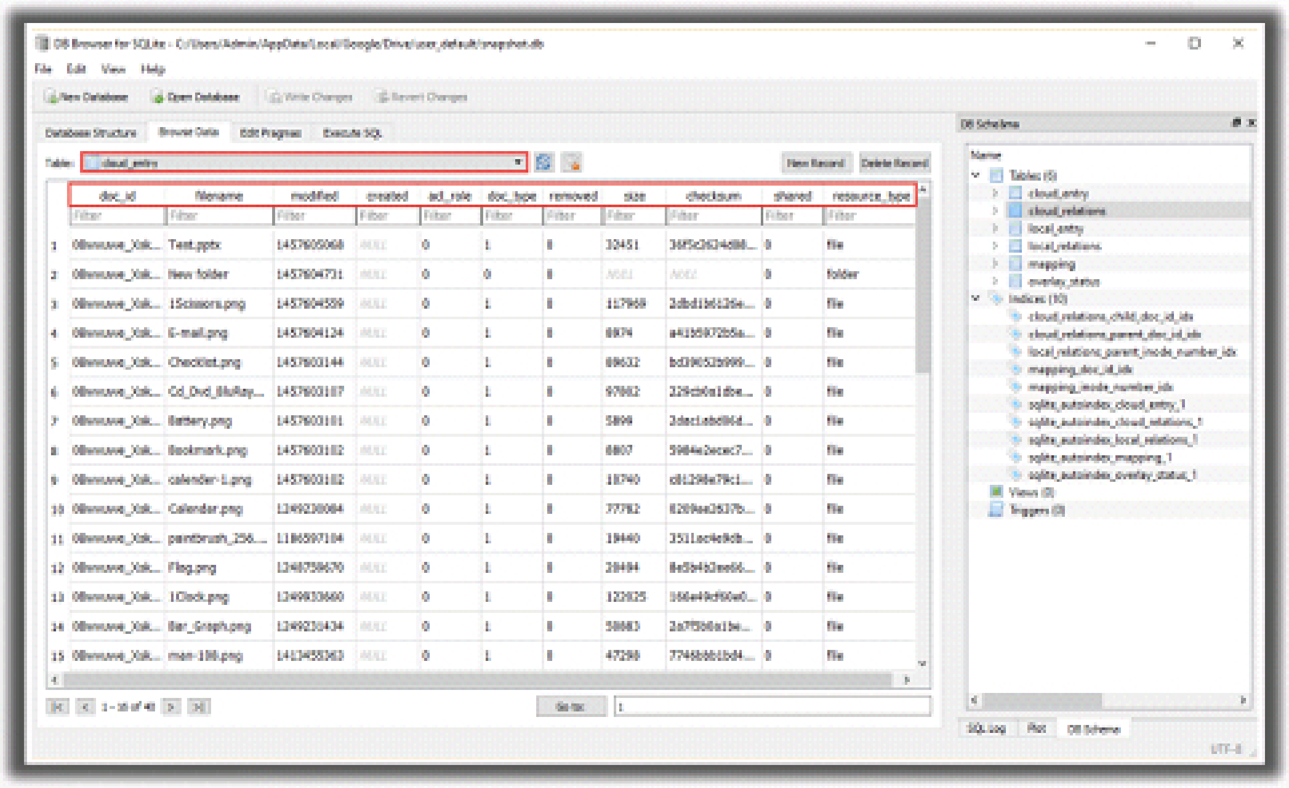
http://sqlitebrowser.org

Sync_config.db is a database file of Google Drive Client containing several records including the Google Drive version, the local sync root path, and the user's email address. Investigators can read the database files using the DB Browser for SQLite tools to extract the required information and also use the file to recreate the databases and search them for the data.

DB browser uses a familiar spreadsheet-like interface, and easy to use. The investigator can make out the client version installed in the machine, the Local Sync Root Path, and the Email ID.

Artifacts Left by Google Drive Client on Windows (Cont'd)

- Files given below are in SQlite3 format and can be accessed using SQlite browsers:
  - snapshot.db
  - sync_config.db
- You can run tools such as DB Browser for SQLite to find information about local entry and cloud entry in the Snapshot.db
- Given below is the snapshot for cloud entry, displaying information: file name, created, modified, removed, size, checksum, shared, resource_type, etc.



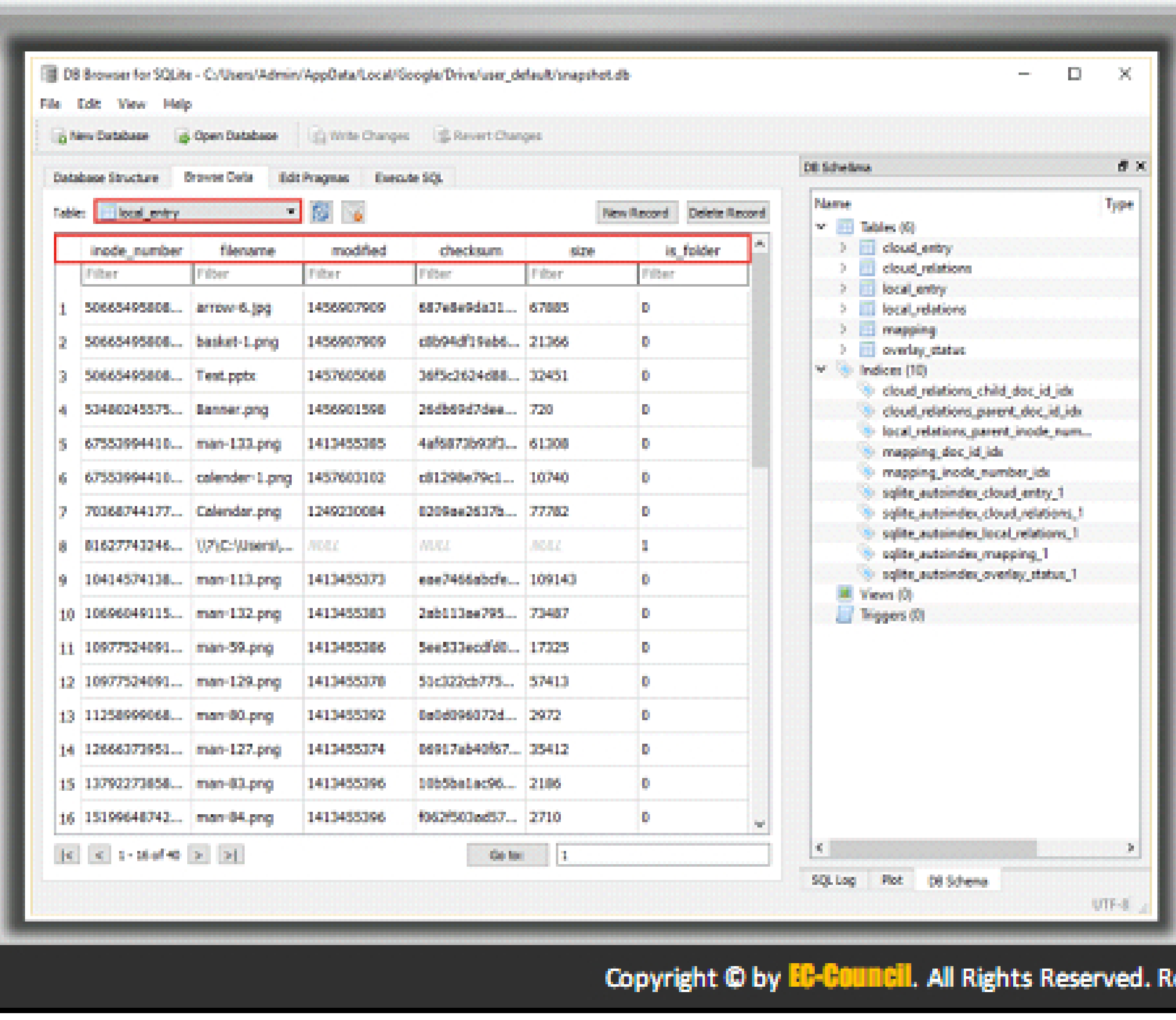
	doc_id	filename	modified	created	acl_role	doc_type	removed	size	checksum	shared	resource_type
1	0Bwwuwe_Xsk...	Test.pptx	1457605068	NULL	0	1	0	32451	36f5c2624d88...	0	file
2	0Bwwuwe_Xsk...	New folder	1457604731	NULL	0	0	0	NULL	NULL	0	folder
3	0Bwwuwe_Xsk...	1Scissors.png	1457604559	NULL	0	1	0	117969	2dbd1b6126e...	0	file
4	0Bwwuwe_Xsk...	E-mail.png	1457604124	NULL	0	1	0	8874	a41b5972b5a...	0	file
5	0Bwwuwe_Xsk...	Checklist.png	1457603144	NULL	0	1	0	89632	bd39652b999...	0	file
6	0Bwwuwe_Xsk...	Cd_Dvd_BluRay...	1457603107	NULL	0	1	0	97002	229cb0a1dbe...	0	file
7	0Bwwuwe_Xsk...	Battery.png	1457603101	NULL	0	1	0	5899	2dec1ebd86d...	0	file
8	0Bwwuwe_Xsk...	Bookmark.png	1457603102	NULL	0	1	0	8807	5984e2ecec7...	0	file
9	0Bwwuwe_Xsk...	calender-1.png	1457603102	NULL	0	1	0	18740	c81298e79c1...	0	file
10	0Bwwuwe_Xsk...	Calender.png	1249230084	NULL	0	1	0	77782	8209ae2637b...	0	file
11	0Bwwuwe_Xsk...	paintbrush_256...	1186597104	NULL	0	1	0	19440	3511ec4e9cb...	0	file
12	0Bwwuwe_Xsk...	Flag.png	1248758670	NULL	0	1	0	28494	8e5b4b2ee66...	0	file
13	0Bwwuwe_Xsk...	1Clock.png	1249933660	NULL	0	1	0	122025	166e49cf60e0...	0	file
14	0Bwwuwe_Xsk...	Bar_Graph.png	1249231434	NULL	0	1	0	58683	2a7f5b6a1be...	0	file
15	0Bwwuwe_Xsk...	man-198.png	1413455363	NULL	0	1	0	47298	7746bbb1bd4...	0	file

Name
- Tables (6)
  - cloud_entry
  - cloud_relations
  - local_entry
  - local_relations
  - mapping
  - overlay_status
- Indices (10)
  - cloud_relations_child_doc_id_idx
  - cloud_relations_parent_doc_id_idx
  - local_relations_parent_inode_number_idx
  - mapping_doc_id_idx
  - mapping_inode_number_idx
  - sqlite_autoindex_cloud_entry_1
  - sqlite_autoindex_cloud_relations_1
  - sqlite_autoindex_local_relations_1
  - sqlite_autoindex_mapping_1
  - sqlite_autoindex_overlay_status_1
- Views (0)
- Triggers (0)

The files snapshot.db and sync_config.db are database format files that store details about local entry and cloud entry. Investigators can also obtain the details of file information like file name, date of files created, removed, and modified, size, checksum, shared, resource_type, etc. by selecting cloud_entry from Table in DB browser.

Artifacts Left by Google Drive Client on Windows (Cont'd)

- Given below is the snapshot for local entry, displaying information: file name, modified, checksum, size, and is_folder

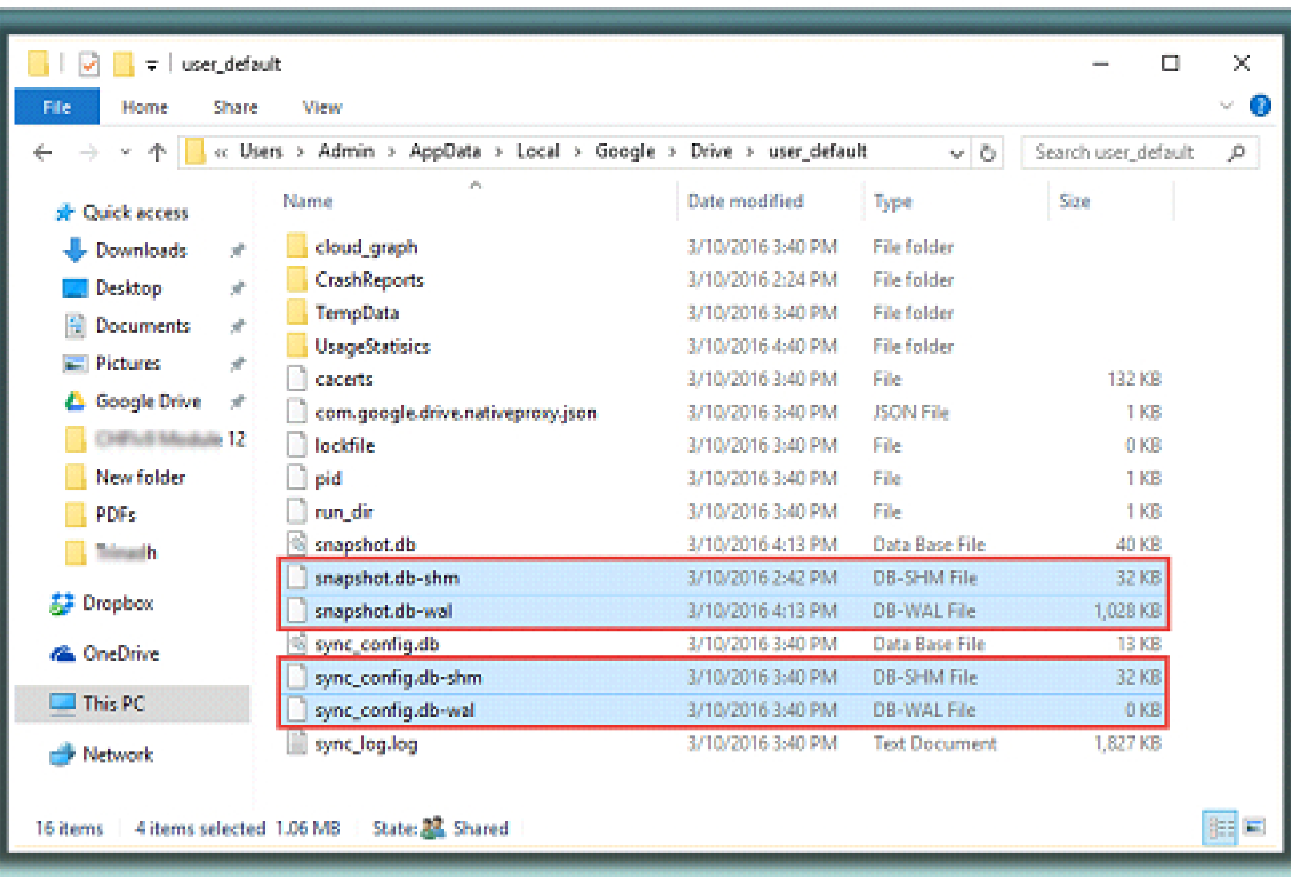


	inode_number	filename	modified	checksum	size	is_folder
	Filter	Filter	Filter	Filter	Filter	Filter
1	50665495808...	arrow-6.jpg	1456907909	687e8e9da31...	67885	0
2	50665495808...	basket-1.png	1456907909	d8b94df19ab6...	21366	0
3	50665495808...	Test.pptx	1457605068	36f5c2624d88...	32451	0
4	53480245575...	Banner.png	1456901598	26db69d7dee...	720	0
5	67553994410...	man-133.png	1413455385	4af6873b93f3...	61308	0
6	67553994410...	calender-1.png	1457603102	c81298e79c1...	10740	0
7	70368744177...	Calendar.png	1249230084	8208ae2637b...	77782	0
8	81627743246...	\\?\C:\Users\...	NULL	NULL	NULL	1
9	10414574138...	man-113.png	1413455373	eae7466abcfe...	109143	0
10	10696049115...	man-132.png	1413455383	2ab113ae795...	73487	0
11	10977524091...	man-59.png	1413455386	5ee533ecdf80...	17325	0
12	10977524091...	man-129.png	1413455378	53c322cb775...	57413	0
13	11258999068...	man-80.png	1413455392	8a0d096072d...	2972	0
14	12666373951...	man-127.png	1413455374	86917ab40f67...	35412	0
15	13792273858...	man-83.png	1413455396	10b5ba1ac96...	2186	0
16	15199648742...	man-84.png	1413455396	f062f503ed57...	2710	0

Investigators can pull out the values like inode number, file name, modified, checksum, size, and is_folder by selecting local_entry from the Table in DB browser.

Artifacts Left by Google Drive Client on Windows (Cont'd)

- An additional 4 files are created in the default database path directory `C\Users\<username>\AppData\Local\Google\Drive\user_default` after data is added and synced into Google Drive
- They are temporary files created by SQLite, mainly used for transaction logging such as rollback changes when a transaction fails



« Users › Admin › AppData › Local › Google › Drive › user_default

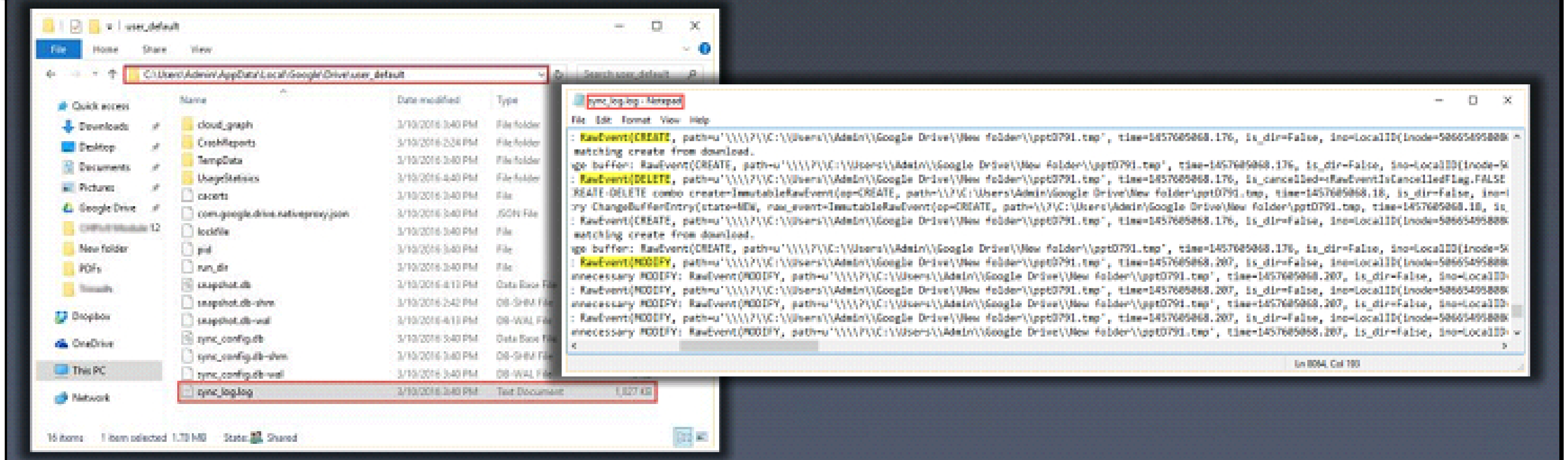
Name	Date modified	Type	Size
cloud_graph	3/10/2016 3:40 PM	File folder	
CrashReports	3/10/2016 2:24 PM	File folder	
TempData	3/10/2016 3:40 PM	File folder	
UsageStatisics	3/10/2016 4:40 PM	File folder	
cacerts	3/10/2016 3:40 PM	File	132 KB
com.google.drive.nativeproxy.json	3/10/2016 3:40 PM	JSON File	1 KB
lockfile	3/10/2016 3:40 PM	File	0 KB
pid	3/10/2016 3:40 PM	File	1 KB
run_dir	3/10/2016 3:40 PM	File	1 KB
snapshot.db	3/10/2016 4:13 PM	Data Base File	40 KB
snapshot.db-shm	3/10/2016 2:42 PM	DB-SHM File	32 KB
snapshot.db-wal	3/10/2016 4:13 PM	DB-WAL File	1,028 KB
sync_config.db	3/10/2016 3:40 PM	Data Base File	13 KB
sync_config.db-shm	3/10/2016 3:40 PM	DB-SHM File	32 KB
sync_config.db-wal	3/10/2016 3:40 PM	DB-WAL File	0 KB
sync_log.log	3/10/2016 3:40 PM	Text Document	1,827 KB

16 items 4 items selected 1.06 MB State: Shared

The installation process of Google drive client creates some temporary files in the user profile that SQLite uses for storing the changes temporarily in case of sync failures and roll them back later. Investigators should search for such files and extract the information to check for the presence of any information useful for investigation. These files are in database format and readable using various tools.

Artifacts Left by Google Drive Client on Windows (Cont'd)

- You can obtain information about the client sync session from the Sync_log.log file
- Information available includes: sync sessions, file created, file modified, and file deleted
- Open the Sync_log.log file located at C:\Users\<Username>\AppData\Local\Google\Drive\user_default and use the strings given below:
  - RawEvent(CREATE
  - RawEvent(DELETE
  - RawEvent(MODIFY



Name	Date modified	Type	
cloud_graph	3/10/2016 3:40 PM	File folder	
CrashReports	3/10/2016 2:24 PM	File folder	
TempData	3/10/2016 3:40 PM	File folder	
UsageStatistics	3/10/2016 4:40 PM	File folder	
cacerts	3/10/2016 3:40 PM	File	
com.google.drive.nativeproxy.json	3/10/2016 3:40 PM	JSON File	
lockfile	3/10/2016 3:40 PM	File	
pid	3/10/2016 3:40 PM	File	
run_dir	3/10/2016 3:40 PM	File	
snapshot.db	3/10/2016 4:13 PM	Data Base File	
snapshot.db-shm	3/10/2016 2:42 PM	DB-SHM File	
snapshot.db-wal	3/10/2016 4:13 PM	DB-WAL File	
sync_config.db	3/10/2016 3:40 PM	Data Base File	
sync_config.db-shm	3/10/2016 3:40 PM	DB-SHM File	
sync_config.db-wal	3/10/2016 3:40 PM	DB-WAL File	
sync_log.log	3/10/2016 3:40 PM	Text Document	1,827 KB

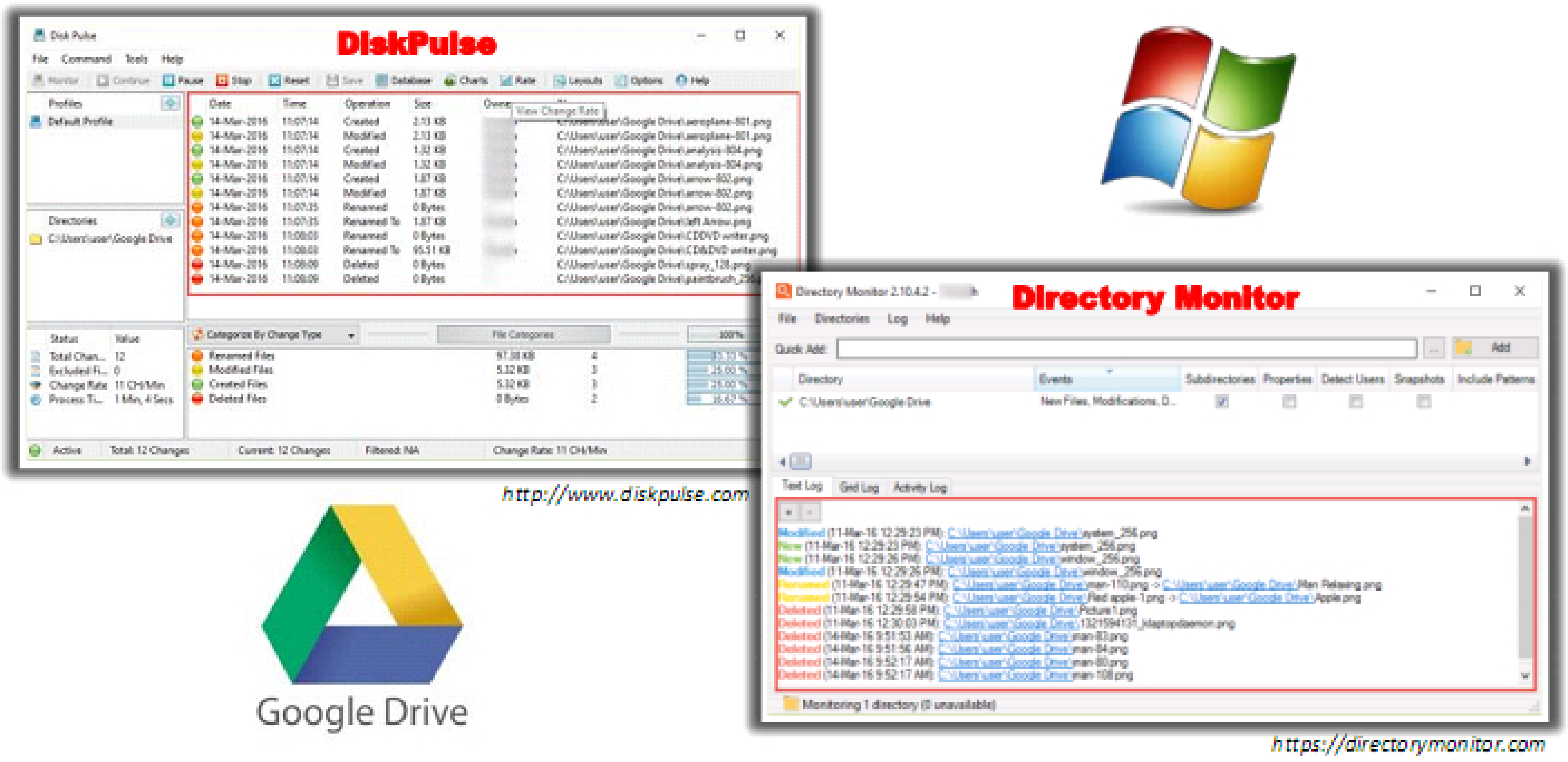
```
: RawEvent(CREATE, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\ppt0791.tmp', time=1457605068.176, is_dir=False, ino=LocalID(inode=50665495808
 matching create from download.
ge buffer: RawEvent(CREATE, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\ppt0791.tmp', time=1457605068.176, is_dir=False, ino=LocalID(inode=5
: RawEvent(DELETE, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\ppt0791.tmp', time=1457605068.176, is_cancelled=<RawEventIsCancelledFlag.FALSE
REATE-DELETE combo create=ImmutableRawEvent(op=CREATE, path=\\?\C:\Users\Admin\Google Drive\New folder\ppt0791.tmp, time=1457605068.18, is_dir=False, ino=
ry ChangeBufferEntry(state=NEW, raw_event=ImmutableRawEvent(op=CREATE, path=\\?\C:\Users\Admin\Google Drive\New folder\ppt0791.tmp, time=1457605068.18, is
: RawEvent(CREATE, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\ppt0791.tmp', time=1457605068.176, is_dir=False, ino=LocalID(inode=50665495808
 matching create from download.
ge buffer: RawEvent(CREATE, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\ppt0791.tmp', time=1457605068.176, is_dir=False, ino=LocalID(inode=5
: RawEvent(MODIFY, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\ppt0791.tmp', time=1457605068.207, is_dir=False, ino=LocalID(inode=50665495808
nnecessary MODIFY: RawEvent(MODIFY, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\ppt0791.tmp', time=1457605068.207, is_dir=False, ino=LocalID
: RawEvent(MODIFY, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\ppt0791.tmp', time=1457605068.207, is_dir=False, ino=LocalID(inode=50665495808
nnecessary MODIFY: RawEvent(MODIFY, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\ppt0791.tmp', time=1457605068.207, is_dir=False, ino=LocalID
: RawEvent(MODIFY, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\ppt0791.tmp', time=1457605068.207, is_dir=False, ino=LocalID(inode=50665495808
nnecessary MODIFY: RawEvent(MODIFY, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\ppt0791.tmp', time=1457605068.207, is_dir=False, ino=LocalID
```

Installing the Google Drive Client version in windows10 OS, creates Sync_log.log file in a user_default folder of Drive. The log file contains the information about the client sync session.

The investigator can find the information about sync sessions, files created, saved and deleted from the Sync_log.log file by opening the file in the notepad and searching it with the strings RAWEVENT[CREATE, RAWEVENT[DELETE, RAWEVENT[MODIFY. These events will help the investigators in cross-checking the information with details found on the client and check for suspicious modifications.

Artifacts Left by Google Drive Client on Windows (Cont'd)

- You can view changes (create, modify/rename, and delete) to the Google Drive using tools such as DiskPulse, Directory Monitor, etc.


DiskPulse
Disk Pulse
File Command Tools Help
Monitor Continue Pause Stop Reset Save Database Charts Rate Layouts Options Help
Profiles
Default Profile
Directories
C:\Users\user\Google Drive
View Change Rate
Categorize By Change Type
File Categories
100%
Google Drive
Directory Monitor
Directory Monitor 2.10.4.2 - [redacted]h
File Directories Log Help
Quick Add:
Add
Text Log Grid Log Activity Log

Date	Time	Operation	Size	Owner	Name
14-Mar-2016	11:07:14	Created	2.13 KB	[redacted]	C:\Users\user\Google Drive\aeroplane-801.png
14-Mar-2016	11:07:14	Modified	2.13 KB	[redacted]	C:\Users\user\Google Drive\aeroplane-801.png
14-Mar-2016	11:07:14	Created	1.32 KB	[redacted]	C:\Users\user\Google Drive\analysis-804.png
14-Mar-2016	11:07:14	Modified	1.32 KB	[redacted]	C:\Users\user\Google Drive\analysis-804.png
14-Mar-2016	11:07:14	Created	1.87 KB	[redacted]	C:\Users\user\Google Drive\arrow-802.png
14-Mar-2016	11:07:14	Modified	1.87 KB	[redacted]	C:\Users\user\Google Drive\arrow-802.png
14-Mar-2016	11:07:35	Renamed	0 Bytes	[redacted]	C:\Users\user\Google Drive\arrow-802.png
14-Mar-2016	11:07:35	Renamed To	1.87 KB	[redacted]	C:\Users\user\Google Drive\left Arrow.png
14-Mar-2016	11:08:03	Renamed	0 Bytes	[redacted]	C:\Users\user\Google Drive\CDDVD writer.png
14-Mar-2016	11:08:03	Renamed To	95.51 KB	[redacted]	C:\Users\user\Google Drive\CD&DVD writer.png
14-Mar-2016	11:08:09	Deleted	0 Bytes		C:\Users\user\Google Drive\spray_128.png
14-Mar-2016	11:08:09	Deleted	0 Bytes		C:\Users\user\Google Drive\paintbrush_256

Status	Value
Total Chan...	12
Excluded Fi...	0
Change Rate	11 CH/Min
Process Ti...	1 Min, 4 Secs

Categorize By Change Type			
Renamed Files	97.38 KB	4	33.33 %
Modified Files	5.32 KB	3	25.00 %
Created Files	5.32 KB	3	25.00 %
Deleted Files	0 Bytes	2	16.67 %

Active | Total: 12 Changes | Current: 12 Changes | Filtered: NA | Change Rate: 11 CH/Min

http://www.diskpulse.com

Directory	Events	Subdirectories	Properties	Detect Users	Snapshots	Include Patterns
✓ C:\Users\user\Google Drive	New Files, Modifications, D...	☑	□	□	□	

```
Modified (11-Mar-16 12:29:23 PM): C:\Users\user\Google Drive\system_256.png
New (11-Mar-16 12:29:23 PM): C:\Users\user\Google Drive\system_256.png
New (11-Mar-16 12:29:26 PM): C:\Users\user\Google Drive\window_256.png
Modified (11-Mar-16 12:29:26 PM): C:\Users\user\Google Drive\window_256.png
Renamed (11-Mar-16 12:29:47 PM): C:\Users\user\Google Drive\man-110.png -> C:\Users\user\Google Drive\Man Relaxing.png
Renamed (11-Mar-16 12:29:54 PM): C:\Users\user\Google Drive\Red apple-1.png -> C:\Users\user\Google Drive\Apple.png
Deleted (11-Mar-16 12:29:58 PM): C:\Users\user\Google Drive\Picture1.png
Deleted (11-Mar-16 12:30:03 PM): C:\Users\user\Google Drive\1321594131_klaptopdaemon.png
Deleted (14-Mar-16 9:51:53 AM): C:\Users\user\Google Drive\man-83.png
Deleted (14-Mar-16 9:51:56 AM): C:\Users\user\Google Drive\man-84.png
Deleted (14-Mar-16 9:52:17 AM): C:\Users\user\Google Drive\man-80.png
Deleted (14-Mar-16 9:52:17 AM): C:\Users\user\Google Drive\man-108.png
```

Monitoring 1 directory (0 unavailable)

https://directorymonitor.com

DiskPulse

Source: http://www.diskpulse.com

DiskPulse is a disk change monitoring solution allowing investigators to monitor changes in one or more disks and directories, send E-Mail notifications, save various types of reports, generate statistical pie charts, export detected changes to an SQL database, send error messages to the system event log and execute custom commands when a user-specified number of changes detected. The tool intercepts file system change notifications issued by the operating system and detects newly created files, modified files, deleted files and renamed files. All file system changes are detected in real-time allowing one to send an E-Mail notification, execute a custom command and/or save a disk change monitoring report within a couple of seconds after one or more critical changes detected.

Directory Monitor:

Source: https://directorymonitor.com

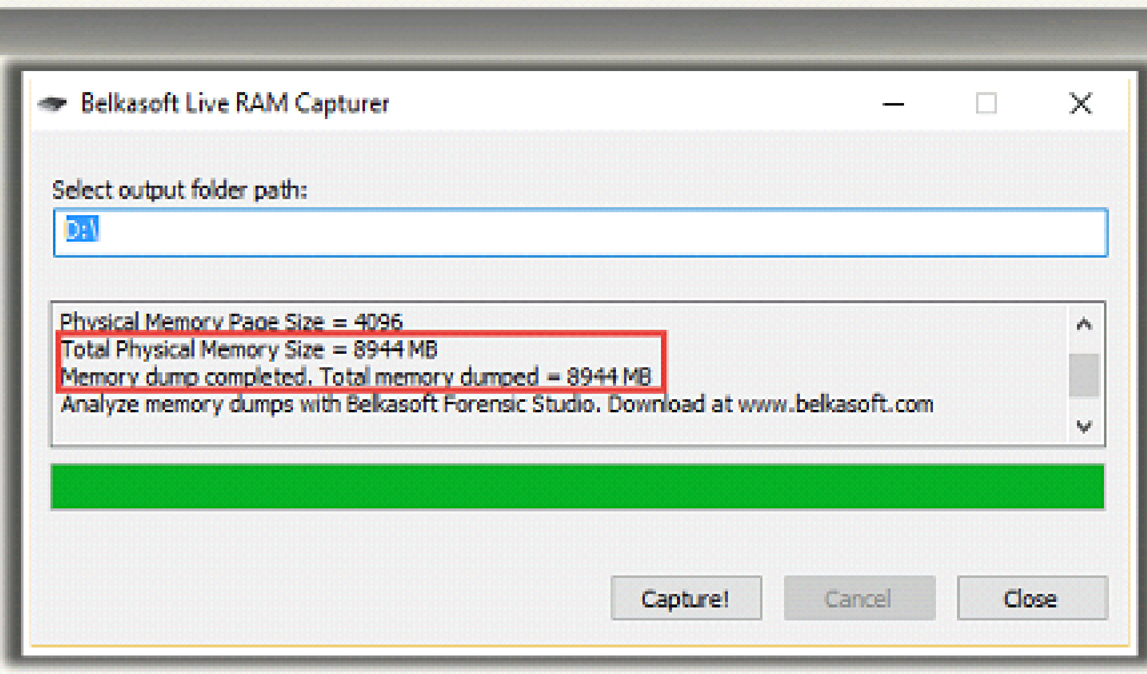
Directory Monitor can be used by the investigators for the surveillance of certain directories and/or network shares and will notify the investigator of file changes/access, deletions, modifications, and new files in real-time. Users and processes making the changes can also be detected. It provides text logs, automation via script/application execution, emailing, writing to a database, sound notifications, etc. The tool monitors local directories or network shares including hidden/private shares, enable snapshots to ensure changes can be detected while the network is down and even during power outages.

Artifacts Left by Google Drive Client on Windows (Cont'd)

- If the Google Drive client is installed on the PC, you can find information about the **sessions in RAM**
- For this, first you need to run tools such as **RAM Capturer** to dump the RAM contents and then use a hex editor tool to analyze the RAM contents

RAM Capturer:

Forensic tool that allows to reliably extract the entire contents of computer's volatile memory – even if protected by an active anti-debugging or anti-dumping system



```
Physical Memory Page Size = 4096
Total Physical Memory Size = 8944 MB
Memory dump completed. Total memory dumped = 8944 MB
Analyze memory dumps with Belkasoft Forensic Studio. Download at www.belkasoft.com
```

https://belkasoft.com

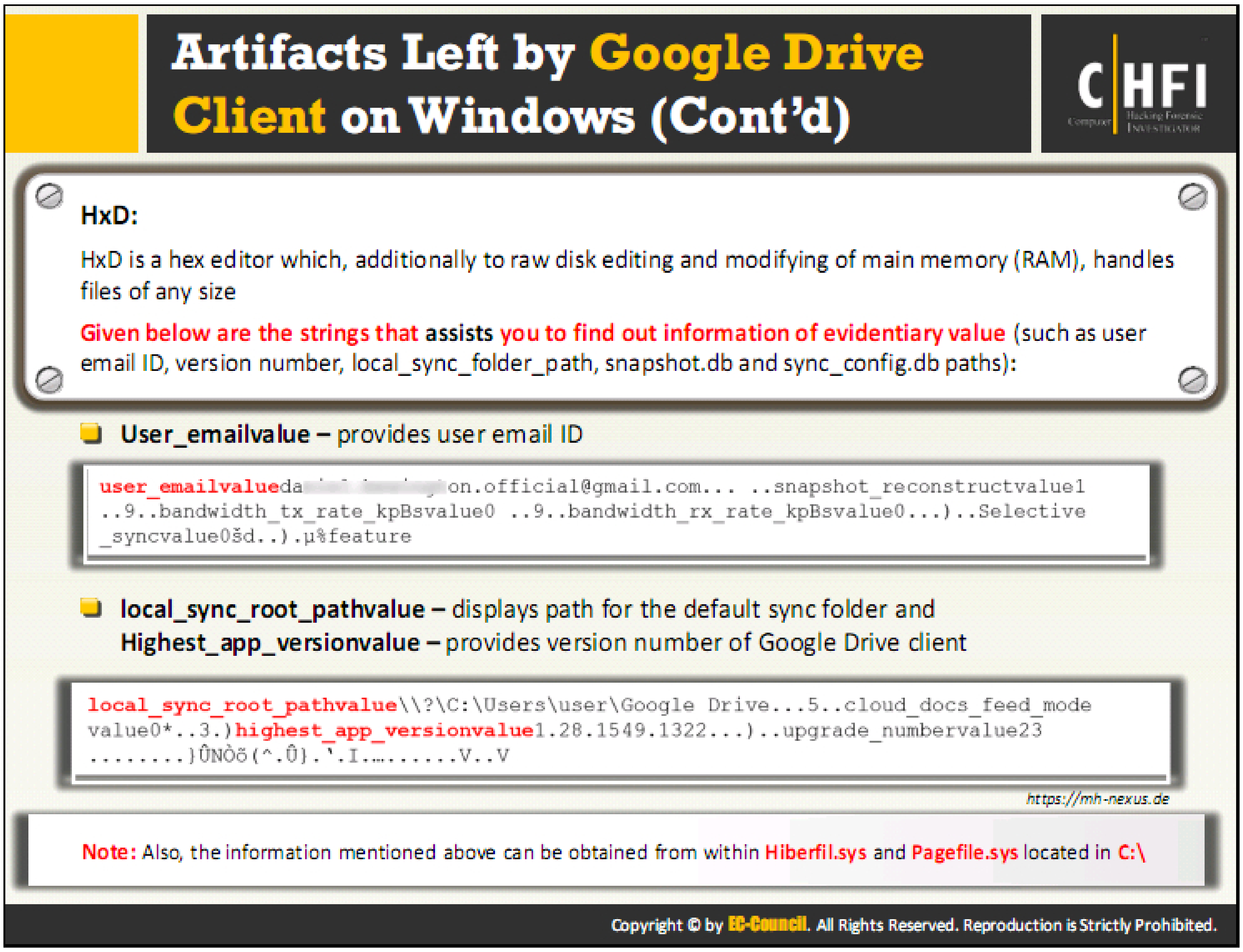
Investigators can find out the information about the sessions of a Google Drive client from the RAM analysis. In cases where the investigator has to extract information from a dead system and has to find out if the user or attacker had used a cloud environment on the system, the investigator can use the data stored in RAM. The process refers to RAM analysis. For this, the investigator can run RAM Capturer tool to dump the RAM contents, and then use a hex editor tool to analyze the captured RAM contents.

RAM Capturer allows the investigator to reliably extract the entire contents of computer's volatile memory to the required drive – even if protected by an active anti-debugging or anti-dumping system. The tool allows investigators with the ability to take snapshots of the computer's volatile memory (memory dumps) even if an anti-dumping protection is active for the drive.

Belkasoft Live RAM Capturer

Source: https://belkasoft.com

Belkasoft Live RAM Capturer is a forensic tool that allows extracting the entire contents of computer's volatile memory – even if protected by an active anti-debugging or anti-dumping system. Separate 32-bit and 64-bit builds are available to minimize the tool's footprint as much as possible. Memory dumps captured with Belkasoft Live RAM Capturer can be analyzed with Live RAM Analysis in Belkasoft Evidence Center.



Artifacts Left by Google Drive Client on Windows (Cont'd)

HxD:

HxD is a hex editor which, additionally to raw disk editing and modifying of main memory (RAM), handles files of any size

Given below are the strings that assists you to find out information of evidentiary value (such as user email ID, version number, local_sync_folder_path, snapshot.db and sync_config.db paths):

- **User_emailvalue –** provides user email ID

```
user_emailvalueda[redacted]on.official@gmail.com... ..snapshot_reconstructvalue1
..9..bandwidth_tx_rate_kpBsvalue0 ..9..bandwidth_rx_rate_kpBsvalue0...)..Selective
_syncvalue0šd..).µ%feature
```

- **local_sync_root_pathvalue –** displays path for the default sync folder and **Highest_app_versionvalue –** provides version number of Google Drive client

```
local_sync_root_pathvalue\\?\C:\Users\user\Google Drive...5..cloud_docs_feed_mode
value0*..3.)highest_app_versionvalue1.28.1549.1322...)..upgrade_numbervalue23
........)ÛNÒõ(^.Û).`.I.…......V..V
```

https://mh-nexus.de

Note: Also, the information mentioned above can be obtained from within Hiberfil.sys and Pagefile.sys located in C:\

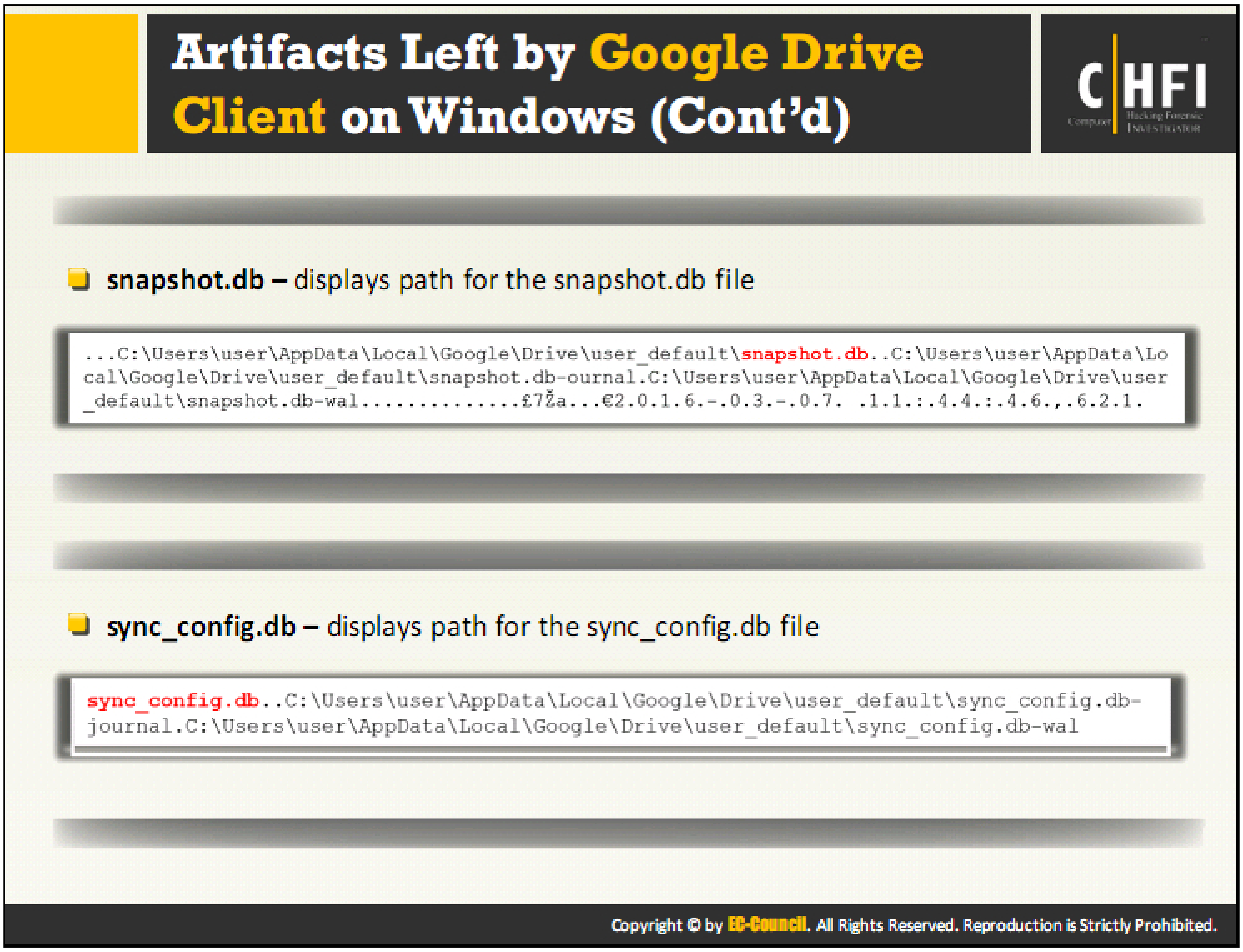
HXD

Source: https://mh-nexus.de

HXD is a hex editor allowing users to edit, modify the raw binary content of a file or a disk of any size.

The tool features; operations such as searching, replacing, exporting, checksums/ digests, insertion of byte patterns, a file shredder, concatenation or splitting of files, statistics, analyze malware, patch programmers, repair hard drive tables, perform file comparisons, create cheats, etc. The tool assists investigators in finding out information of evidentiary value such as email ID, display name, filecache.dbx path, Server_time, file list, and updated/deleted files.

Investigators can track the email ID the required Google Drive account by searching the RAM dump using the string user_emailvalue and the sync path, and the app version can be obtained using the strings local_sync_root_pathvalue and Highest_app_versionvalue.



Artifacts Left by Google Drive Client on Windows (Cont'd)

CHFI
Computer Hacking Forensic Investigator

- **snapshot.db –** displays path for the snapshot.db file

```
...C:\Users\user\AppData\Local\Google\Drive\user_default\snapshot.db..C:\Users\user\AppData\Lo
cal\Google\Drive\user_default\snapshot.db-ournal.C:\Users\user\AppData\Local\Google\Drive\user
_default\snapshot.db-wal..............£7Ža...€2.0.1.6.-.0.3.-.0.7. .1.1.:.4.4.:.4.6.,.6.2.1.
```

- **sync_config.db –** displays path for the sync_config.db file

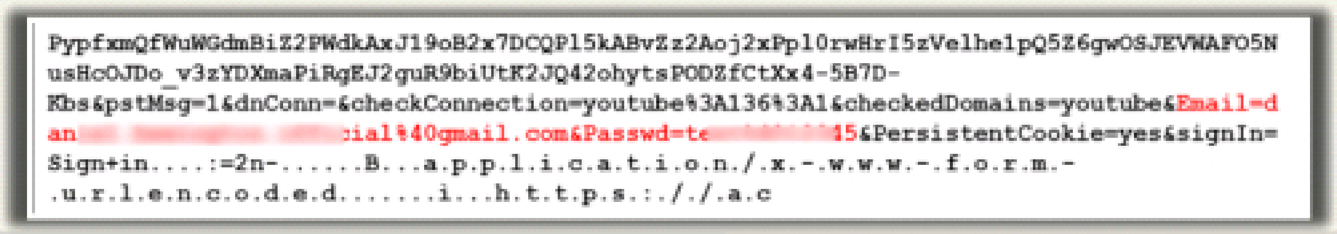
```
sync_config.db..C:\Users\user\AppData\Local\Google\Drive\user_default\sync_config.db-
journal.C:\Users\user\AppData\Local\Google\Drive\user_default\sync_config.db-wal
```

The investigators can search the path of file snapshot.db by searching the RAM dump using hex editor with the string snapshot.db and path of sync config.db file with the string sync_config.db.

Artifacts Left by Google Drive Client on Windows (Cont'd)

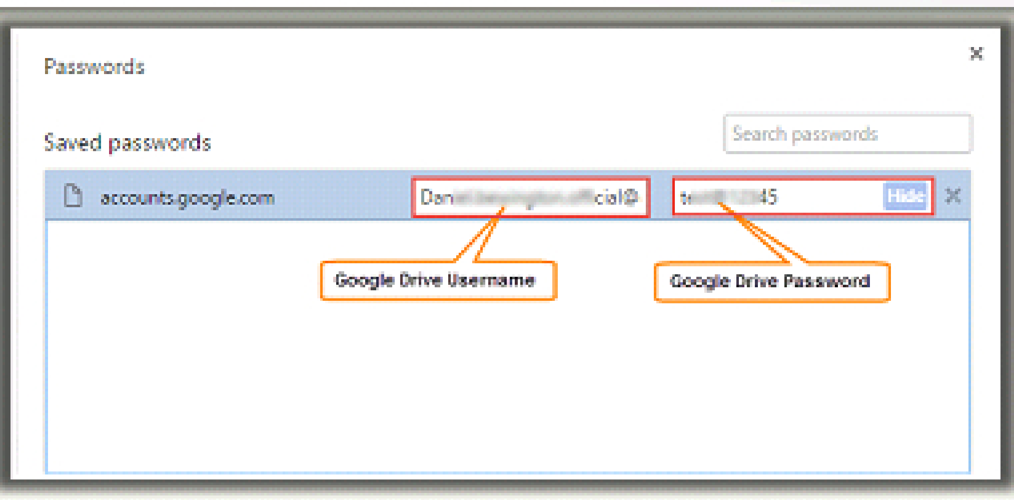
In case of Web-based Google Drive, you can find the **username** and **password** in clear from **RAM dump** using strings:

- "Email= "
- "Passwd="



```
PypfxmQfWuWGdmBiZ2PWdkAxJ19oB2x7DCQPl5kABvZz2Aoj2xPpl0rwHrI5zVelhe1pQ5Z6gwOSJEVWAFO5N
usHcOJDo_v3zYDXmaPiRgEJ2guR9biUtK2JQ42ohytsPODZfCtXx4-5B7D-
Kbs&pstMsg=1&dnConn=&checkConnection=youtube%3A136%3A1&checkedDomains=youtube&Email=d
an[redacted]cial%40gmail.com&Passwd=te[redacted]45&PersistentCookie=yes&signIn=
Sign+in....:=2n-......B...a.p.p.l.i.c.a.t.i.o.n./.x.-.w.w.w.-.f.o.r.m.-
.u.r.l.e.n.c.o.d.e.d.......i...h.t.t.p.s.:./././.a.c
```

Also, you can find the Web-based Google Drive **login credentials** stored somewhere in the PC (ex: browser). Screenshot below is with respect to the **Chrome**

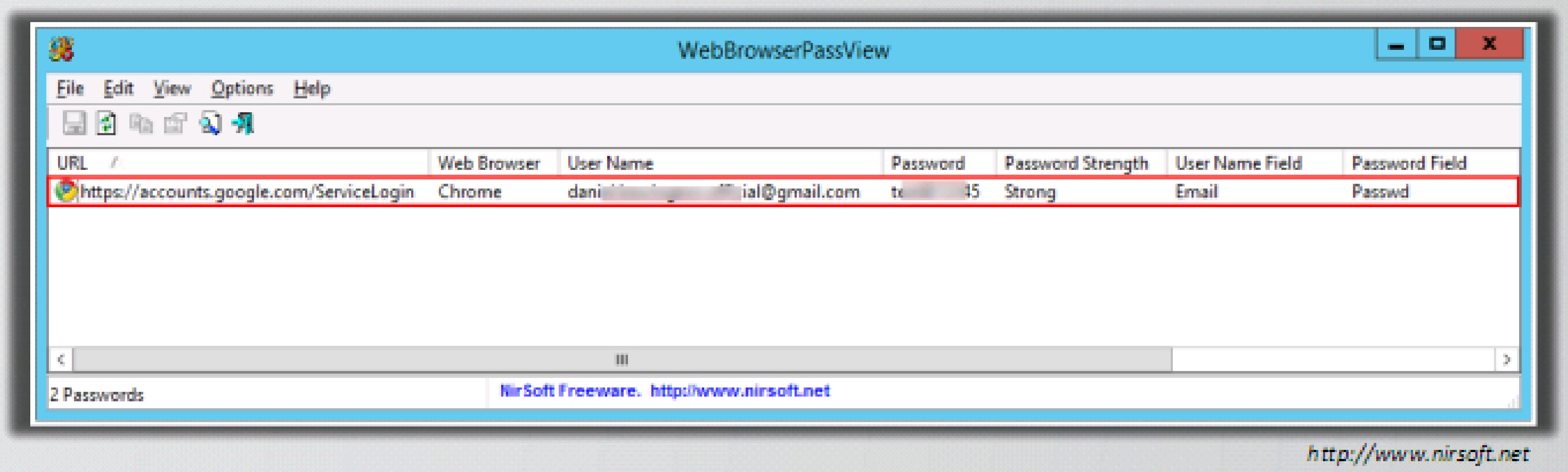


The credentials of a web-based Google Drive account can be tracked in clear-text by the investigators, by exploring the RAM dump using hex editor with the strings like EMAIL= for the user's email id and Passwd= for the password.

Investigators can also trace the stored credentials of the web-based Google Drive application within the PC from the sources like browsers.

Artifacts Left by Google Drive Client on Windows (Cont'd)

You can use tools such as **WebBrowserPassView**, a password recovery tool that reveals the passwords stored by the following Web browsers: Internet Explorer (Version 4.0 - 11.0), Mozilla Firefox, Google Chrome, Safari, and Opera


WebBrowserPassView
File Edit View Options Help
2 Passwords
NirSoft Freeware. http://www.nirsoft.net

URL	Web Browser	User Name	Password	Password Strength	User Name Field	Password Field
https://accounts.google.com/ServiceLogin	Chrome	dani[redacted]ial@gmail.com	te[redacted]45	Strong	Email	Passwd

http://www.nirsoft.net

Investigators can use tools such as WebBrowserPassView, a password recovery tool that reveals the passwords stored by the following Web browsers: Internet Explorer (Version 4.0 - 11.0), Mozilla Firefox, Google Chrome, Safari, and Opera.

The tool can also be used to recover the lost/forgotten password of any website be it Facebook, Google, Yahoo as long as it is stored in the user's browser. The tool allows users to save retrieved passwords in text/html/csv/xml file by using the Save Selected Items option.

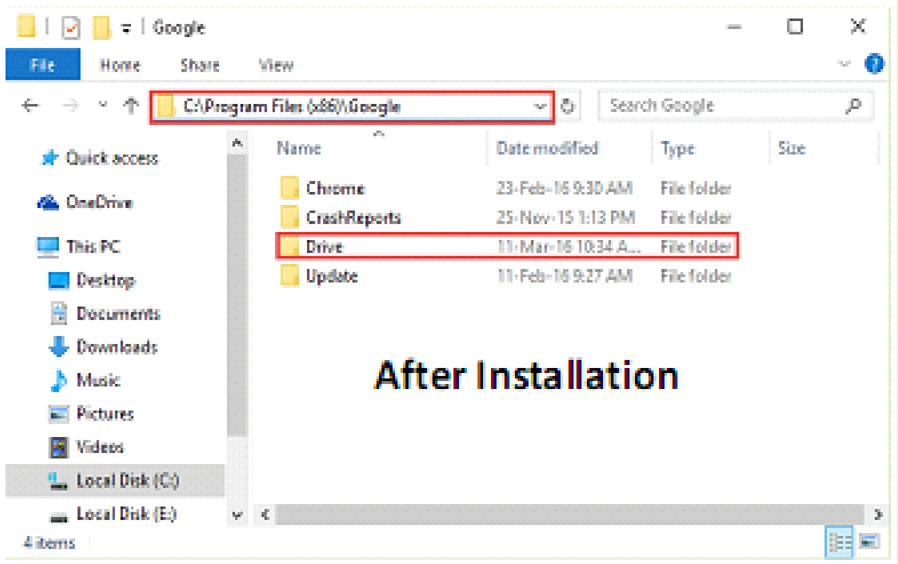
Artifacts Left by Google Drive Client on Windows (Cont'd)

Uninstalling the Google Drive Client application:

- removes the client config folder (sync_config.db)
- Sync_log.log entries are identified from unallocated space
- does not delete the local copy of the file
- preserves the Prefetch files even after uninstallation

You can also recover information from:

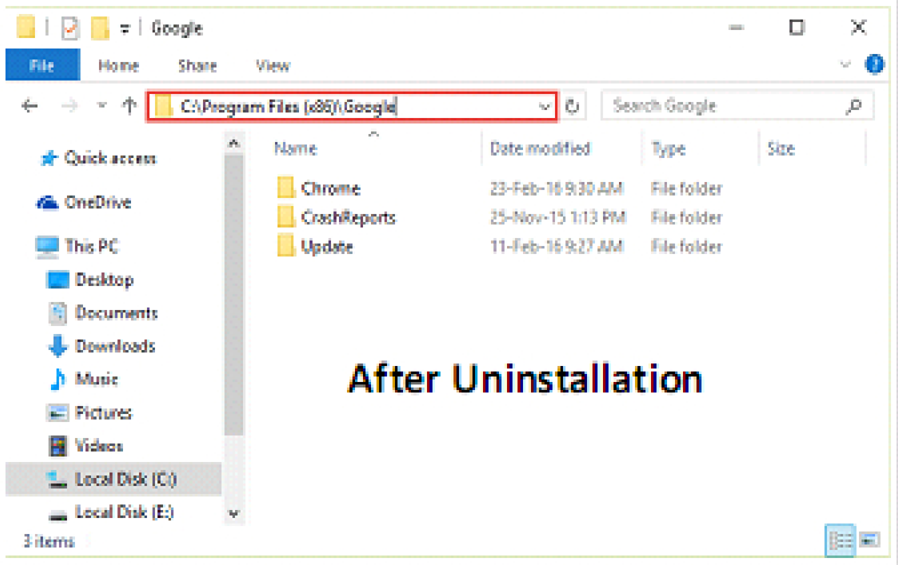
- Registry keys of recent files
- LiNK files
- Browser history and cache
- Thumbnails
- Registry Point/Volume Shadow Copies
- Pagefile.sys
- Hiberfil.sys



C:\Program Files (x86)\Google

Name	Date modified	Type	Size
Chrome	23-Feb-16 9:30 AM	File folder	
CrashReports	25-Nov-15 1:13 PM	File folder	
Drive	11-Mar-16 10:34 A...	File folder	
Update	11-Feb-16 9:27 AM	File folder	

After Installation



C:\Program Files (x86)\Google

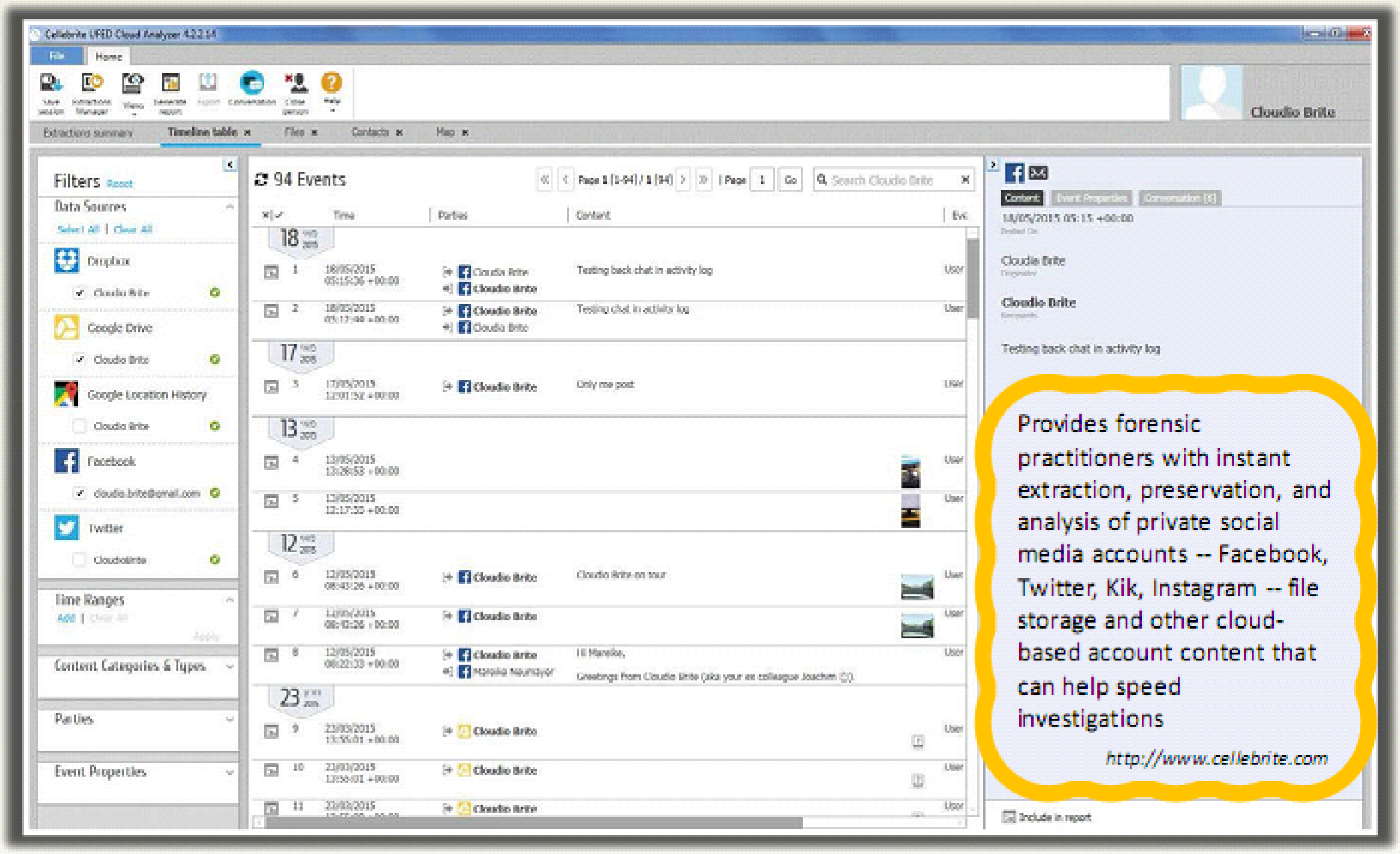
Name	Date modified	Type	Size
Chrome	23-Feb-16 9:30 AM	File folder	
CrashReports	25-Nov-15 1:13 PM	File folder	
Update	11-Feb-16 9:27 AM	File folder	

After Uninstallation

The process of uninstalling an application includes removal of the application along with deletion of various files related to that application. One such file is the Drive file, which the Google Drive client creates in Program Files on installation and removes during uninstalling. While uninstalling the application, the system will also remove config folder, but preserves the local copy and Prefetch files.

Investigators should have the knowledge of files that the system removes and keeps to easily identify the files that can be helpful in investigation. Even after the user has uninstalled the application, the investigator can recover the information related to the application from multiple sources like the Registry keys, LiNK files, browser history and cache, Thumbnails, etc.

Cloud Forensics Tools: UFED Cloud Analyzer



	Time	Parties	Content	Ev
1	18/05/2015 05:15:36 +00:00	Cloudio Brite Cloudio Brite	Testing back chat in activity log	User
2	18/05/2015 05:17:44 +00:00	Cloudio Brite Cloudio Brite	Testing chat in activity log	User
3	17/05/2015 12:01:52 +00:00	Cloudio Brite	Only me post	User
4	13/05/2015 13:28:53 +00:00			User
5	13/05/2015 12:17:32 +00:00			User
6	12/05/2015 08:43:26 +00:00	Cloudio Brite	Cloudio Brite on tour	User
7	12/05/2015 08:42:26 +00:00	Cloudio Brite		User
8	12/05/2015 08:22:33 +00:00	Cloudio Brite Mareike Naumayer	Hi Mareike, Greetings from Cloudio Brite (aka your ex colleague Joachim ☺).	User
9	23/03/2015 13:55:01 +00:00	Cloudio Brite		User
10	23/03/2015 13:56:01 +00:00	Cloudio Brite		User
11	23/03/2015	Cloudio Brite		User

18/05/2015 05:15 +00:00

Cloudio Brite

Cloudio Brite

Testing back chat in activity log

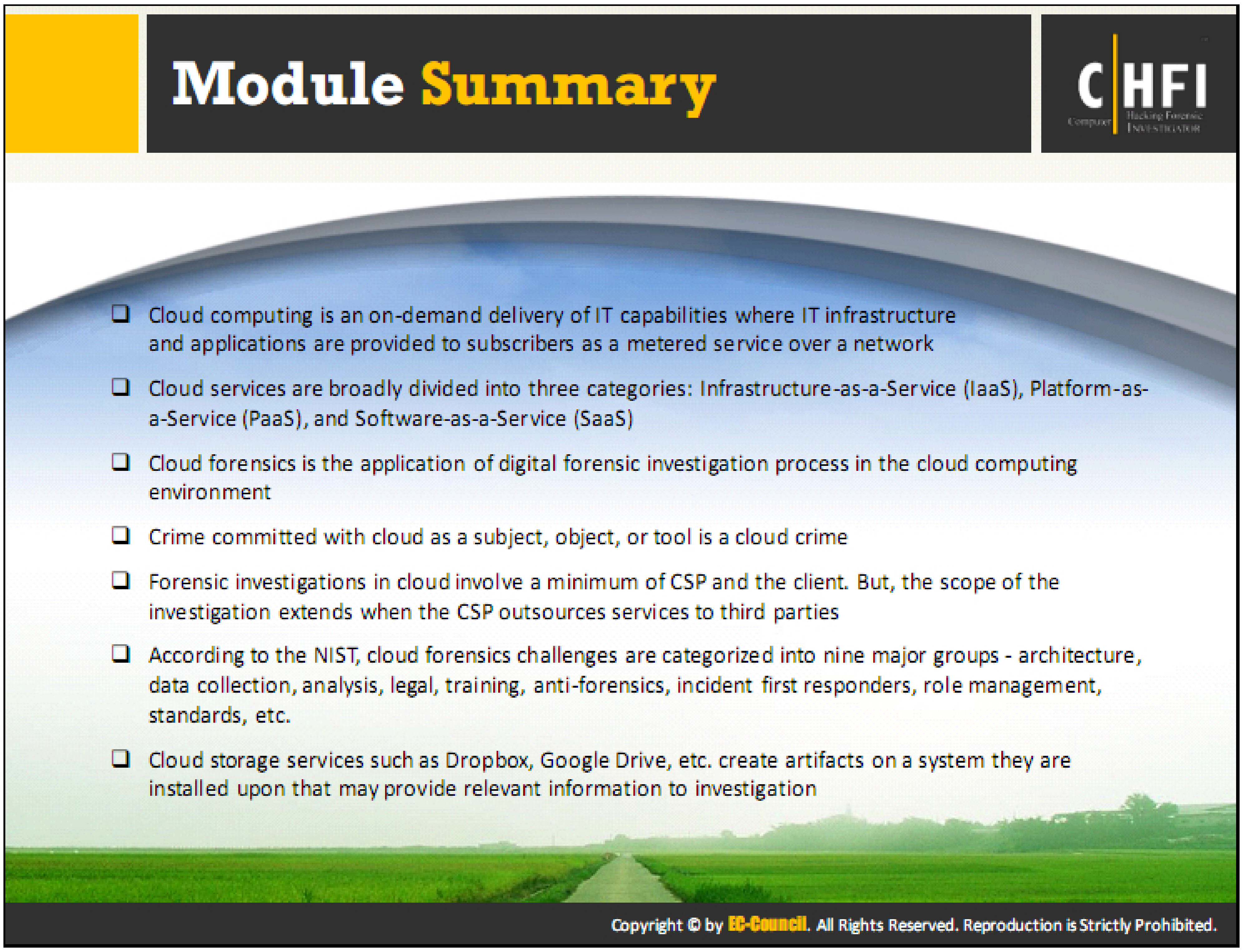
Provides forensic practitioners with instant extraction, preservation, and analysis of private social media accounts -- Facebook, Twitter, Kik, Instagram -- file storage and other cloud-based account content that can help speed investigations

http://www.cellebrite.com

Source: http://www.cellebrite.com

Cloud data sources represent a virtual goldmine of potential evidence for forensic investigators. Together with mobile device data, they often capture the details and critical connections investigators need to solve crimes. However, access remains a challenge. The tool provides forensic practitioners with instant extraction, preservation, and analysis of private social media accounts -- Facebook, Twitter, Kik, Instagram -- file storage and other cloud-based account content that can help speed investigations.

The tool automatically collects both existing cloud data and metadata and packages it in a forensically sound manner. Allows investigators to search, filter and sort data and identify the required details to advance their investigations.



Module Summary

CHFI Computer Hacking Forensic Investigator

- ❑ Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network
- ❑ Cloud services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS)
- ❑ Cloud forensics is the application of digital forensic investigation process in the cloud computing environment
- ❑ Crime committed with cloud as a subject, object, or tool is a cloud crime
- ❑ Forensic investigations in cloud involve a minimum of CSP and the client. But, the scope of the investigation extends when the CSP outsources services to third parties
- ❑ According to the NIST, cloud forensics challenges are categorized into nine major groups - architecture, data collection, analysis, legal, training, anti-forensics, incident first responders, role management, standards, etc.
- ❑ Cloud storage services such as Dropbox, Google Drive, etc. create artifacts on a system they are installed upon that may provide relevant information to investigation

This module discusses the working of Cloud Storage Services, its types, major threats and attacks it faces, and the process of investigating the cloud in a concise manner. The module educates on various cloud storage services, their working, how they store files and folders, etc.

Additionally, it discusses the process investigators should follow to investigate cloud services such as Dropbox and Google Drive, as well as the tools that can help in conducting an investigation and analyzing the evidence data.

The next module will discuss about malware forensics, artifacts malware produce, detection, and analysis, etc.