Cloud Forensics

Module 10

Designed by Cyber Crime Investigators. Presented by Professionals.

C|HFI™ Computer Hacking Forensic Investigator

Module Objectives

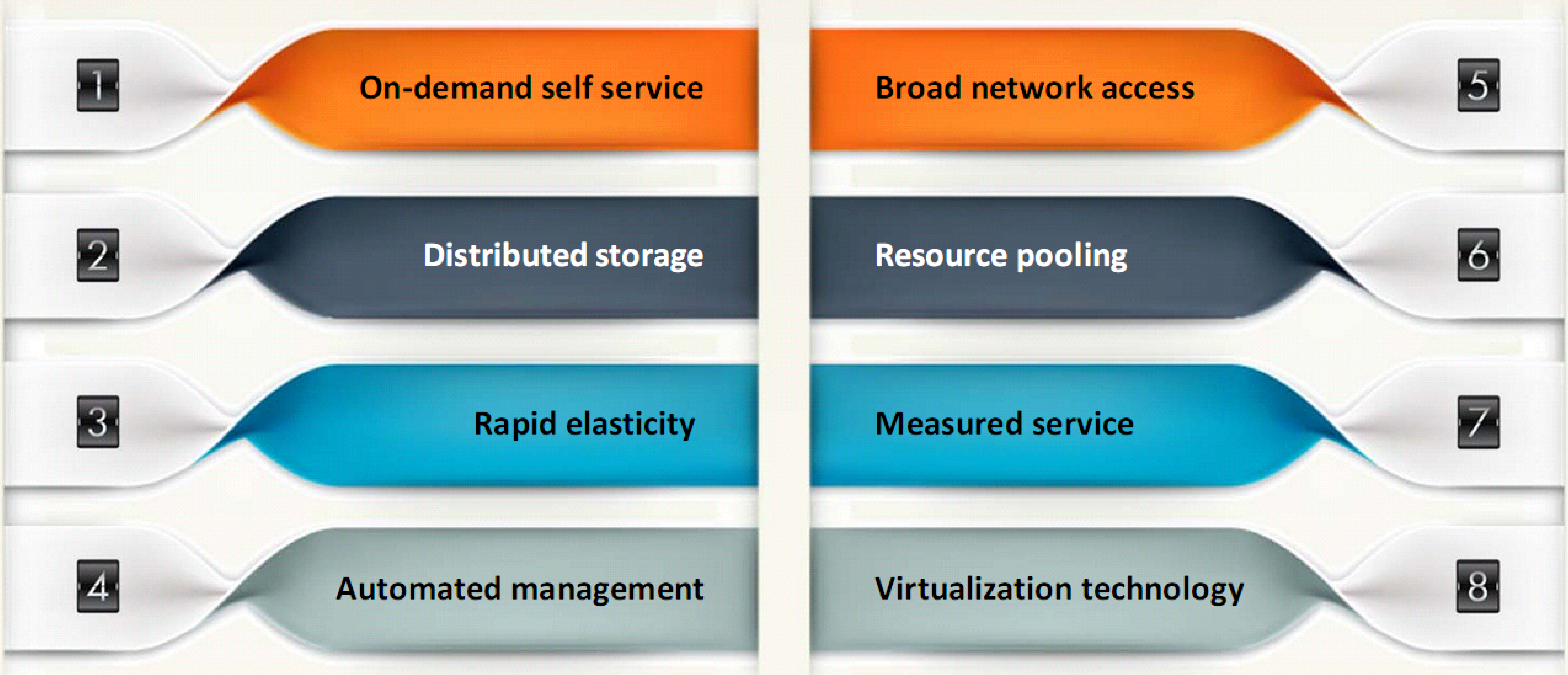
After successfully completing this module, you will be able to:

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

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

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.

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 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**

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)

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

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

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.

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

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

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

Case Study: Cloud as a Tool

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

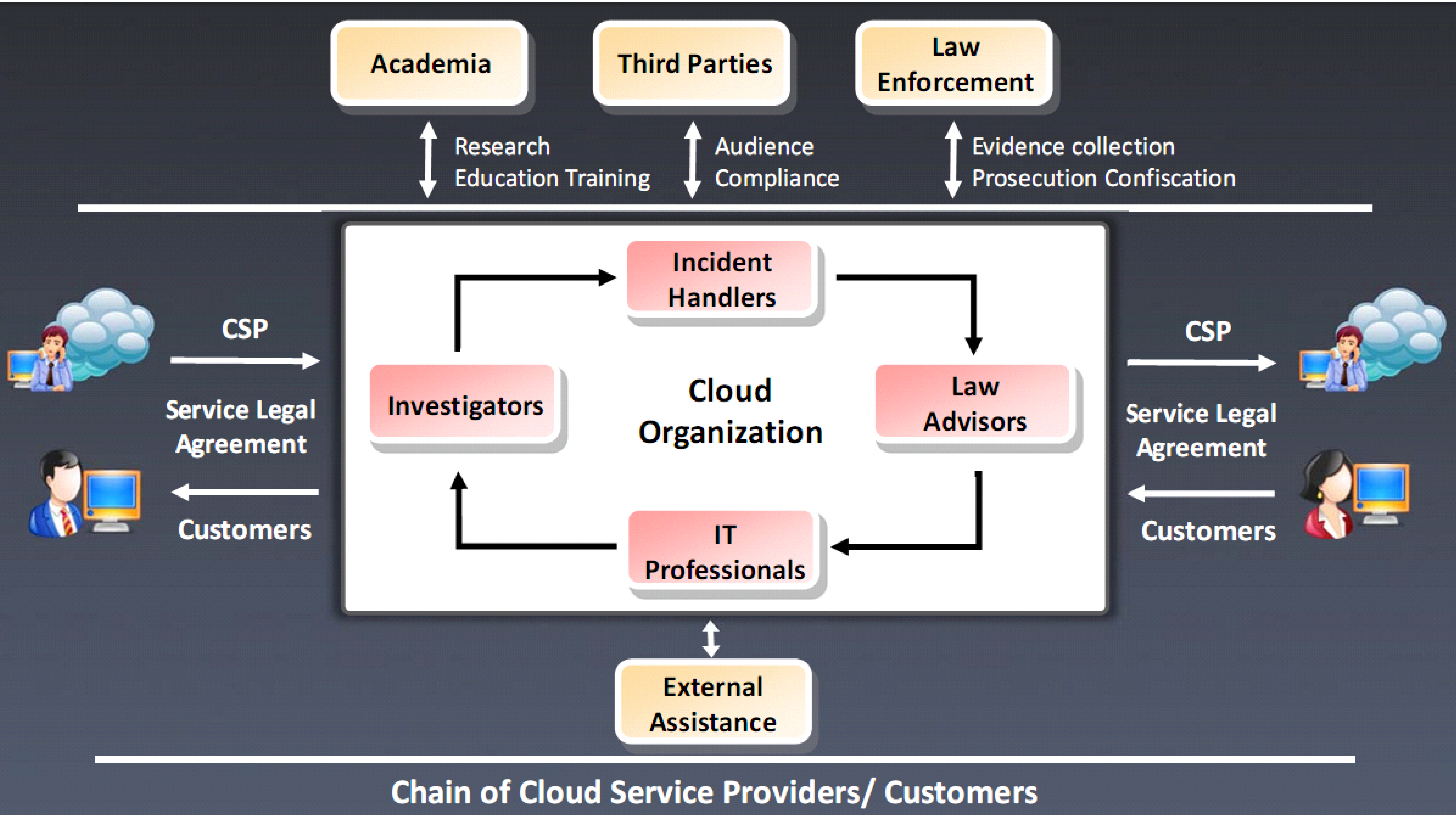
May 02, 2016

- 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

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



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

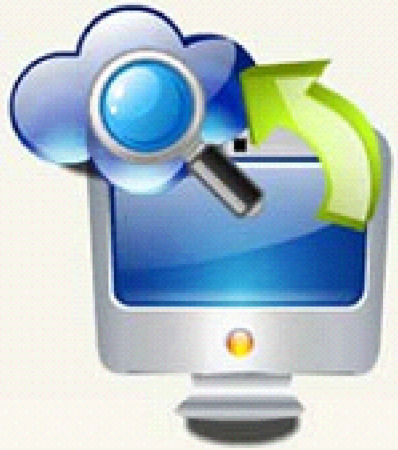
Source: NIST Cloud Computing Forensic Science Challenges (http://csrc.nist.gov)

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

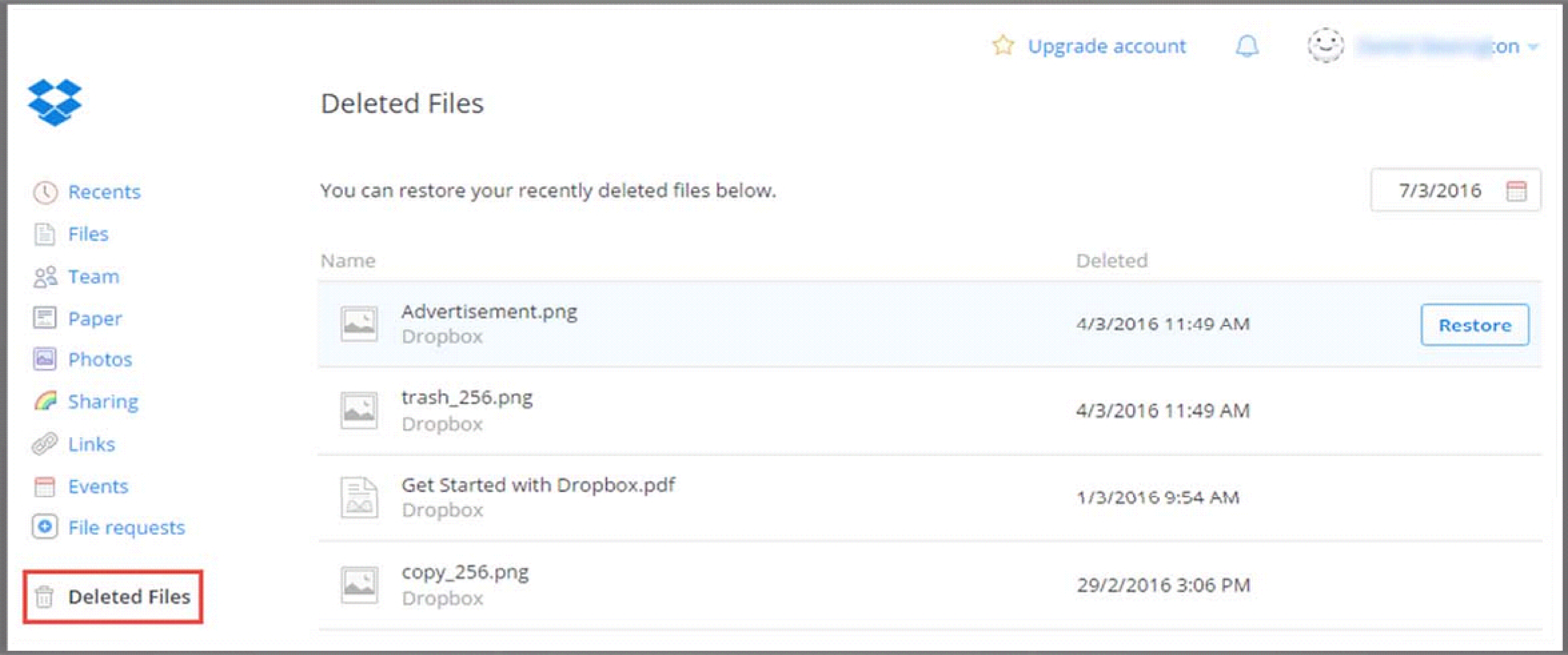


Dropbox

Investigating Dropbox Cloud Storage Service

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

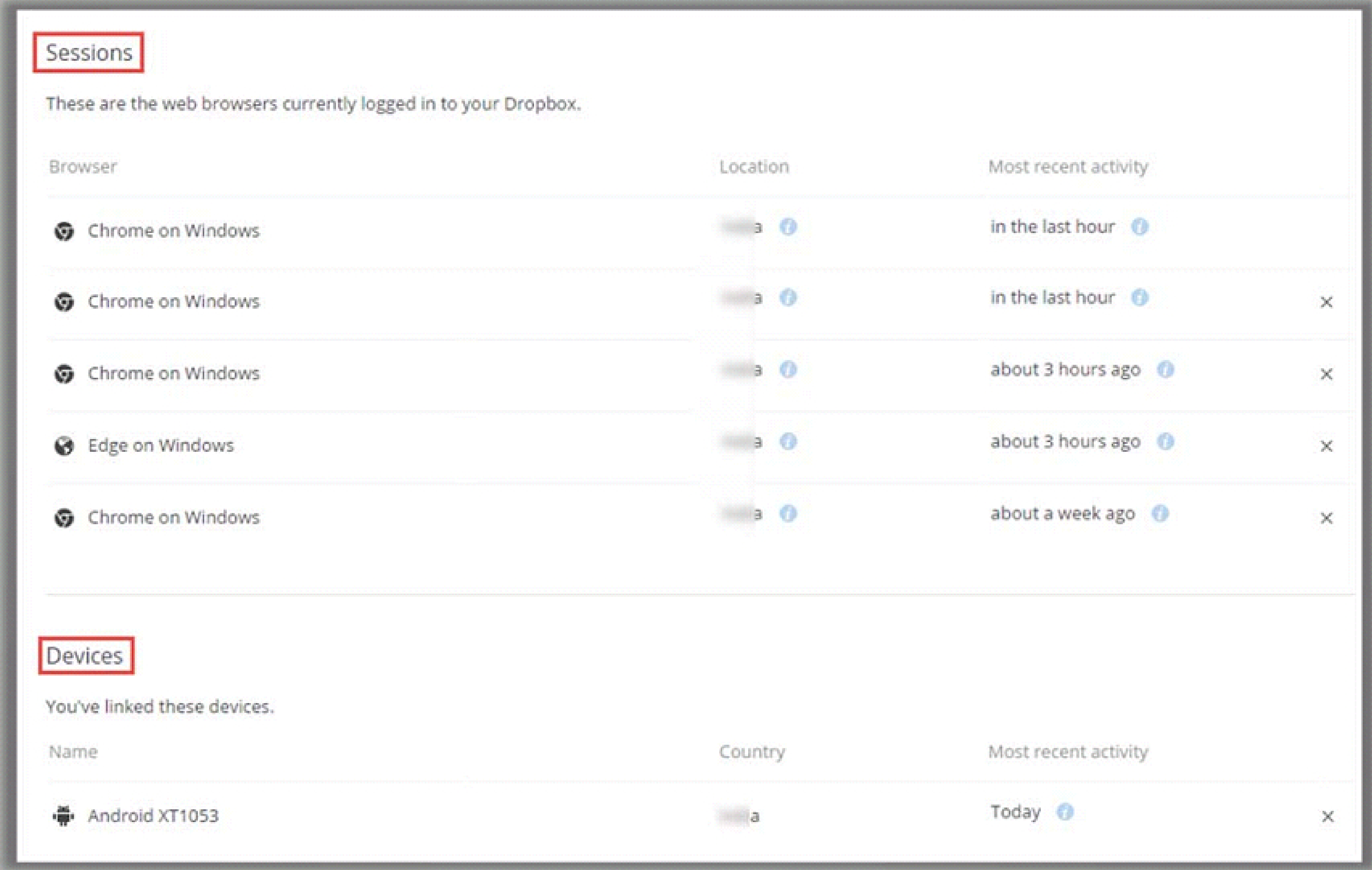
You can restore your recently deleted files below.

7/3/2016

Name	Deleted	
Advertisement.png Dropbox	4/3/2016 11:49 AM	Restore
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	

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	×

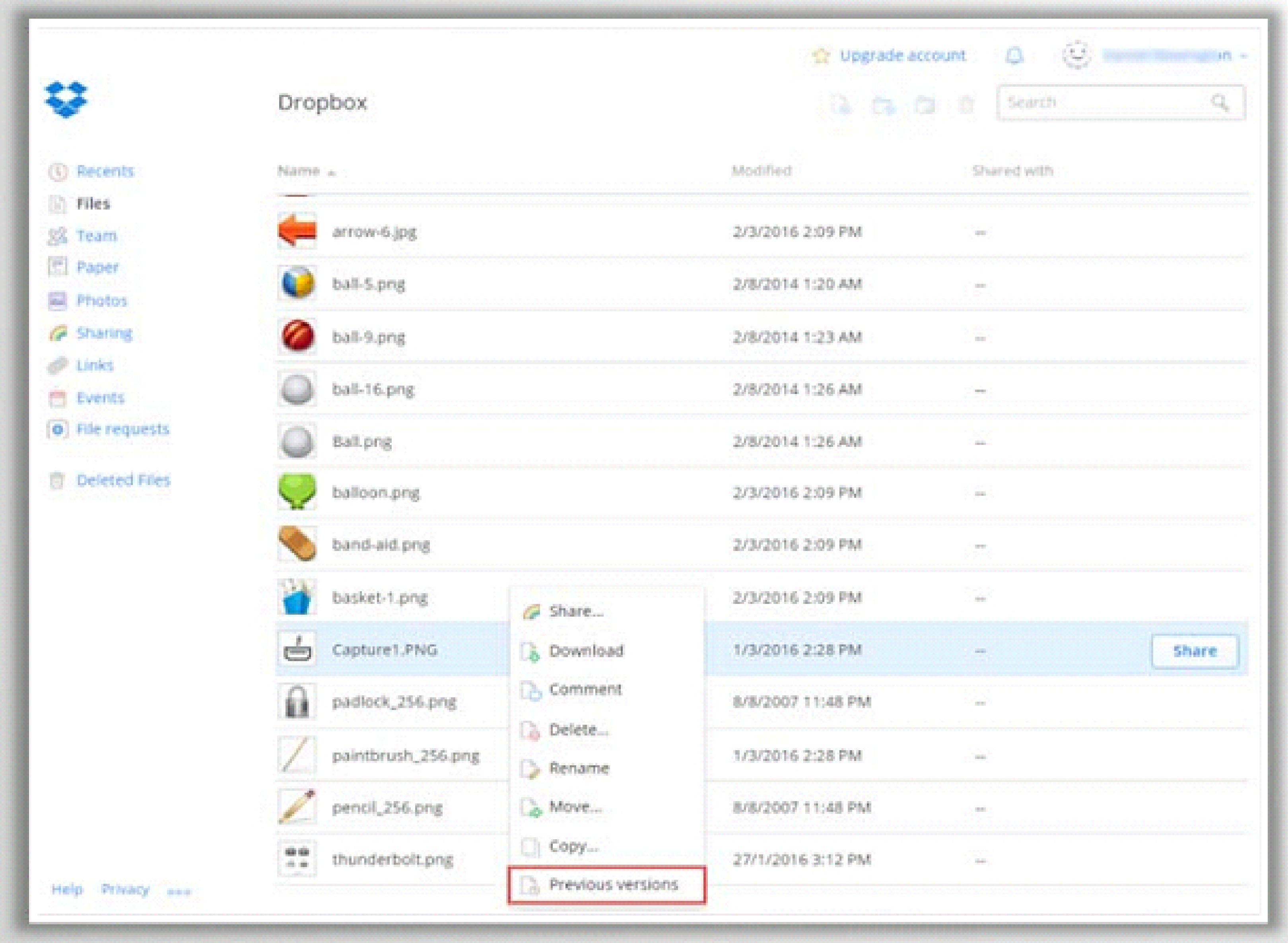
Devices

You've linked these devices.

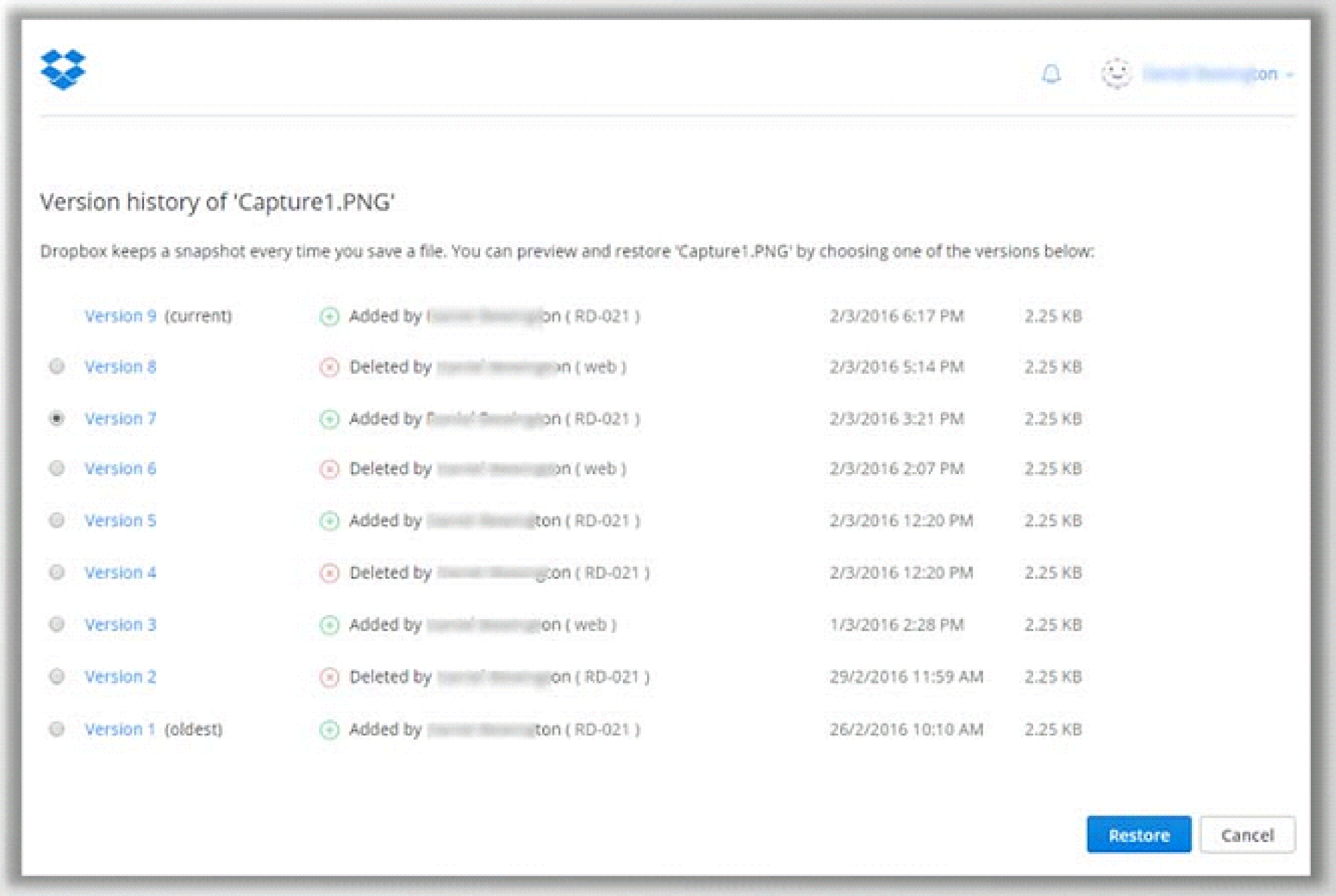
Name	Country	Most recent activity	
Android XT1053	[redacted]	Today	×

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**



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	27/1/2016 3:12 PM	--



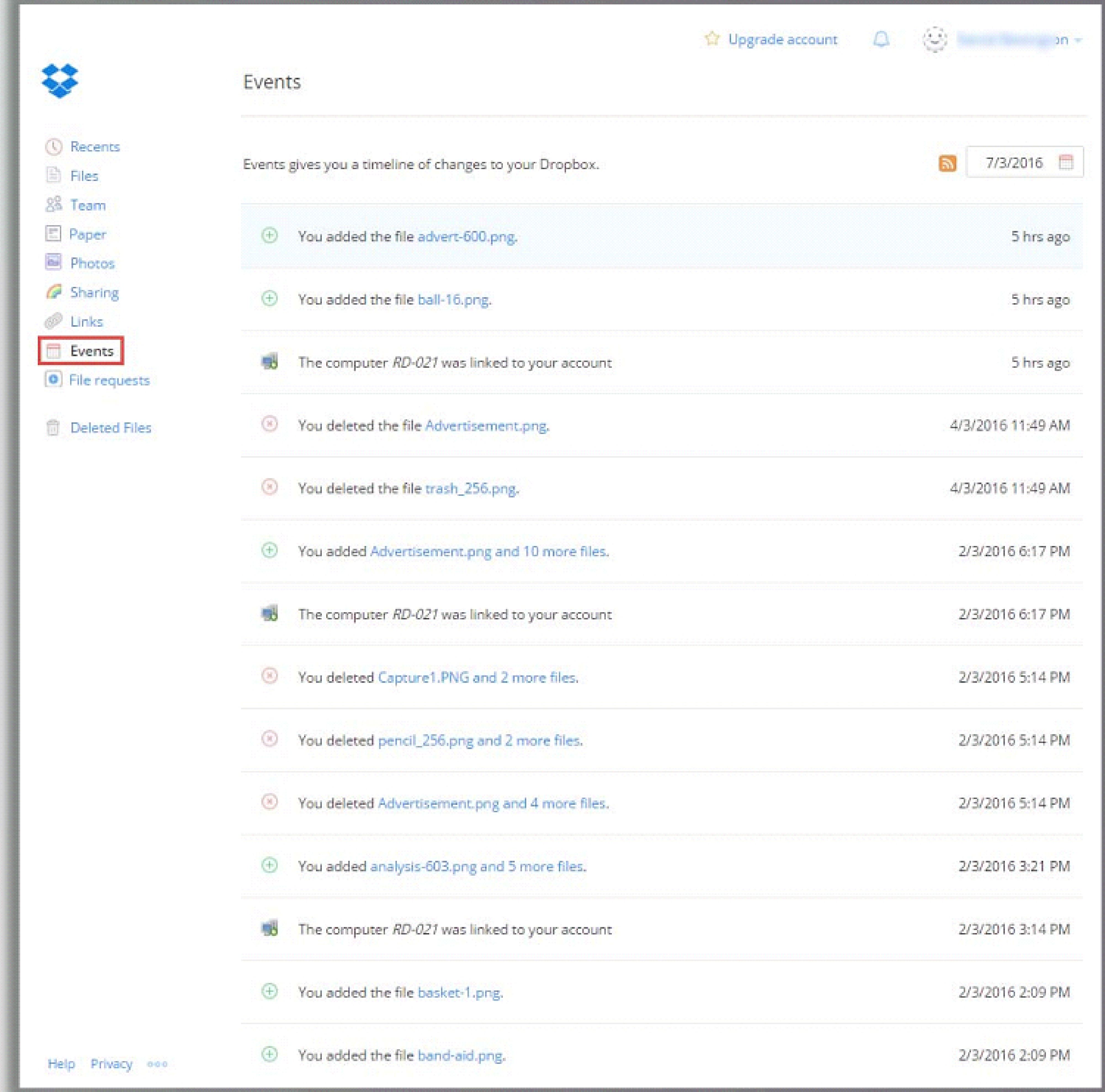
Version history of 'Capture1.PNG'

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

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.

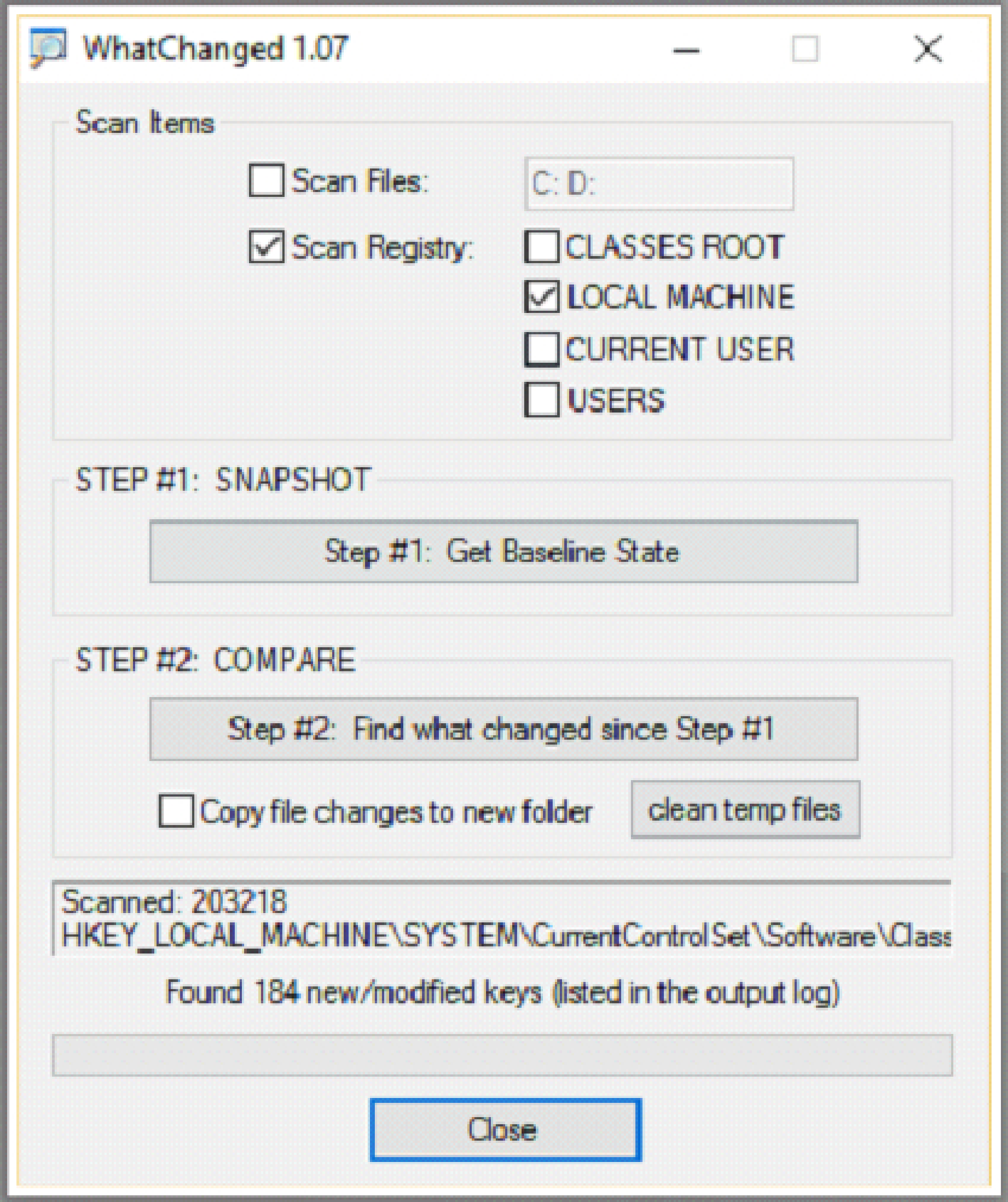
You added the file advert-600.png.	5 hrs ago
You added the file ball-16.png.	5 hrs ago
The computer *RD-021* was linked to your account	5 hrs ago
You deleted the file Advertisement.png.	4/3/2016 11:49 AM
You deleted the file trash_256.png.	4/3/2016 11:49 AM
You added Advertisement.png and 10 more files.	2/3/2016 6:17 PM
The computer *RD-021* 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-021* 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

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**

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
Step #1: Get Baseline State
Step #2: Find what changed since Step #1
clean temp files
Close

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

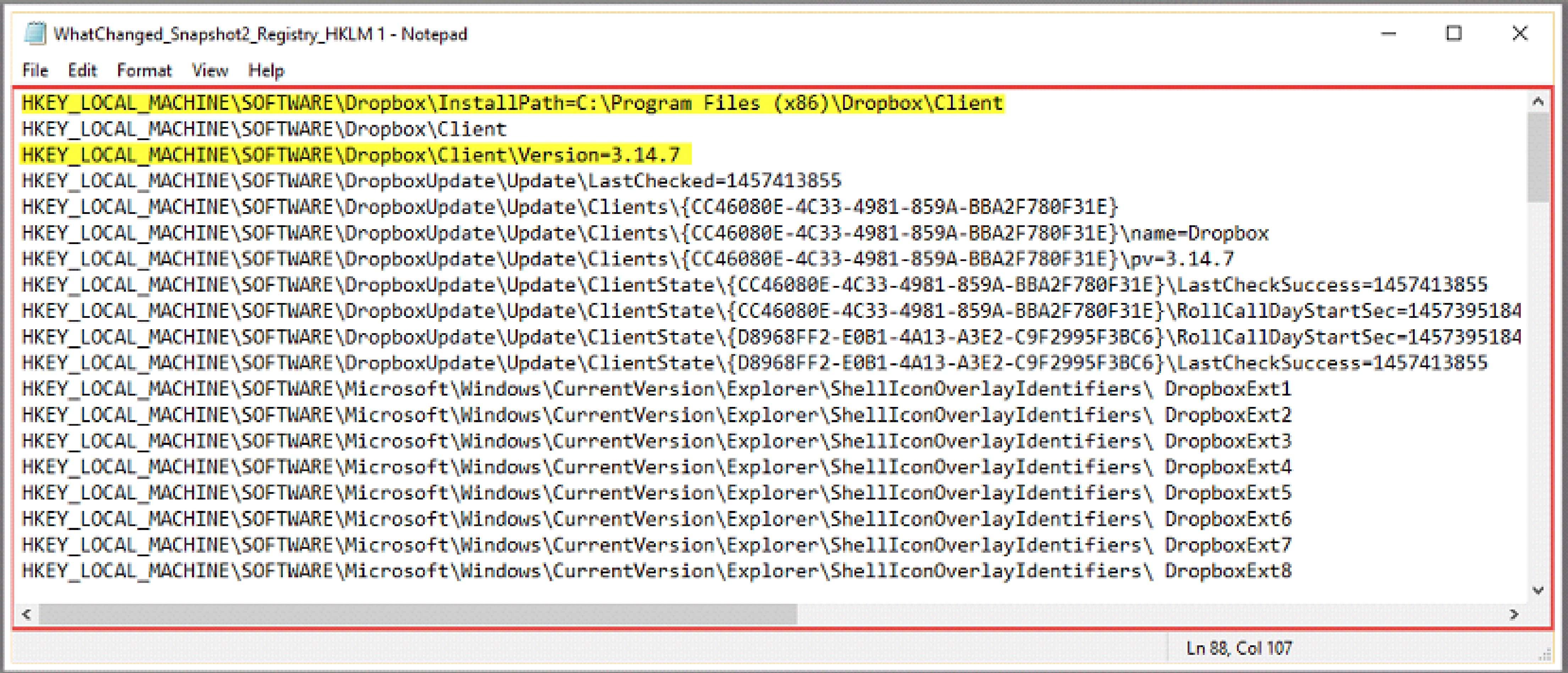
STEP #1: SNAPSHOT

STEP #2: COMPARE

□ 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
File Edit Format View Help
Ln 88, Col 107

```
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-BBA2F780F31E}
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Clients\{CC46080E-4C33-4981-859A-BBA2F780F31E}\name=Dropbox
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\Clients\{CC46080E-4C33-4981-859A-BBA2F780F31E}\pv=3.14.7
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\ClientState\{CC46080E-4C33-4981-859A-BBA2F780F31E}\LastCheckSuccess=1457413855
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\ClientState\{CC46080E-4C33-4981-859A-BBA2F780F31E}\RollCallDayStartSec=1457395184
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\ClientState\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3BC6}\RollCallDayStartSec=1457395184
HKEY_LOCAL_MACHINE\SOFTWARE\DropboxUpdate\Update\ClientState\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3BC6}\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

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:**

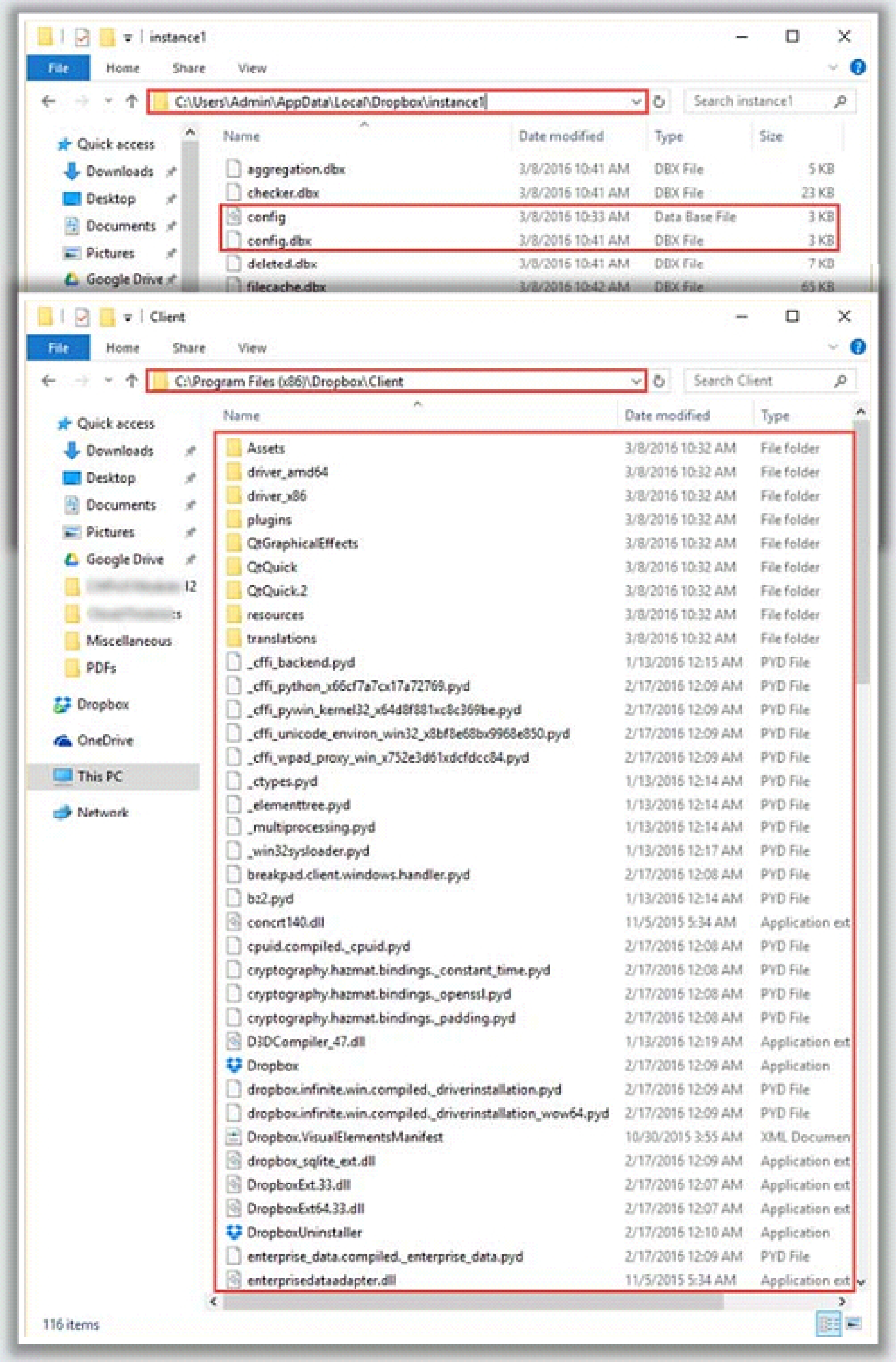
  C:\Program Files (x86)\Dropbox\Client

- **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	5 KB
checker.dbx	3/8/2016 10:41 AM	DBX File	23 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	3/8/2016 10:42 AM	DBX File	65 KB

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_x66cf7a7cx17a72769.pyd	2/17/2016 12:09 AM	PYD File
_cffi_pywin_kernel32_x64d8f881xc8c369be.pyd	2/17/2016 12:09 AM	PYD File
_cffi_unicode_environ_win32_x8bf8e68bx9968e850.pyd	2/17/2016 12:09 AM	PYD File
_cffi_wpad_proxy_win_x752e3d61xdcfdcc84.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 3:55 AM	XML Documen
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

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

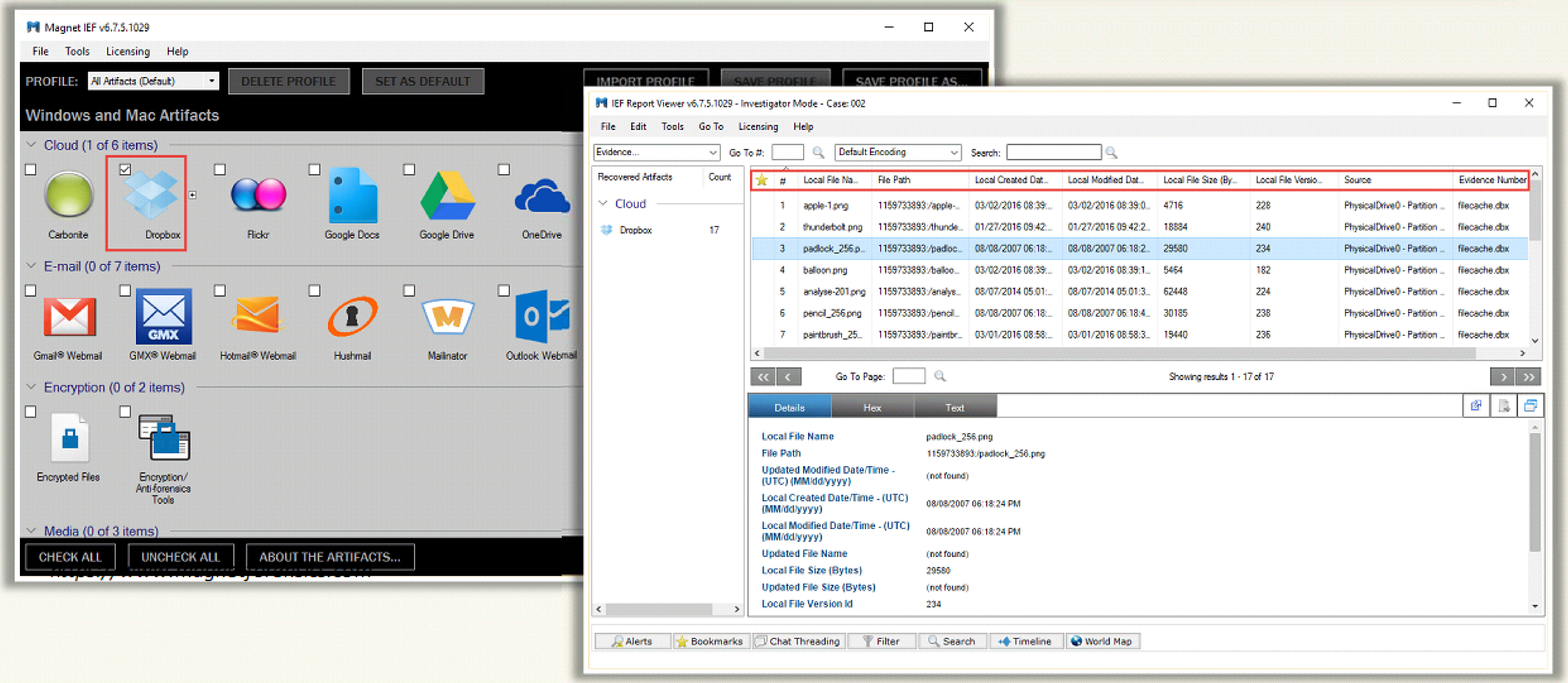
- Some of the files that contain configuration information:

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:/padloc...	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	analyse-201.png	1159733893:/analys...	08/07/2014 05:01:...	08/07/2014 05:01:3...	62448	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

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

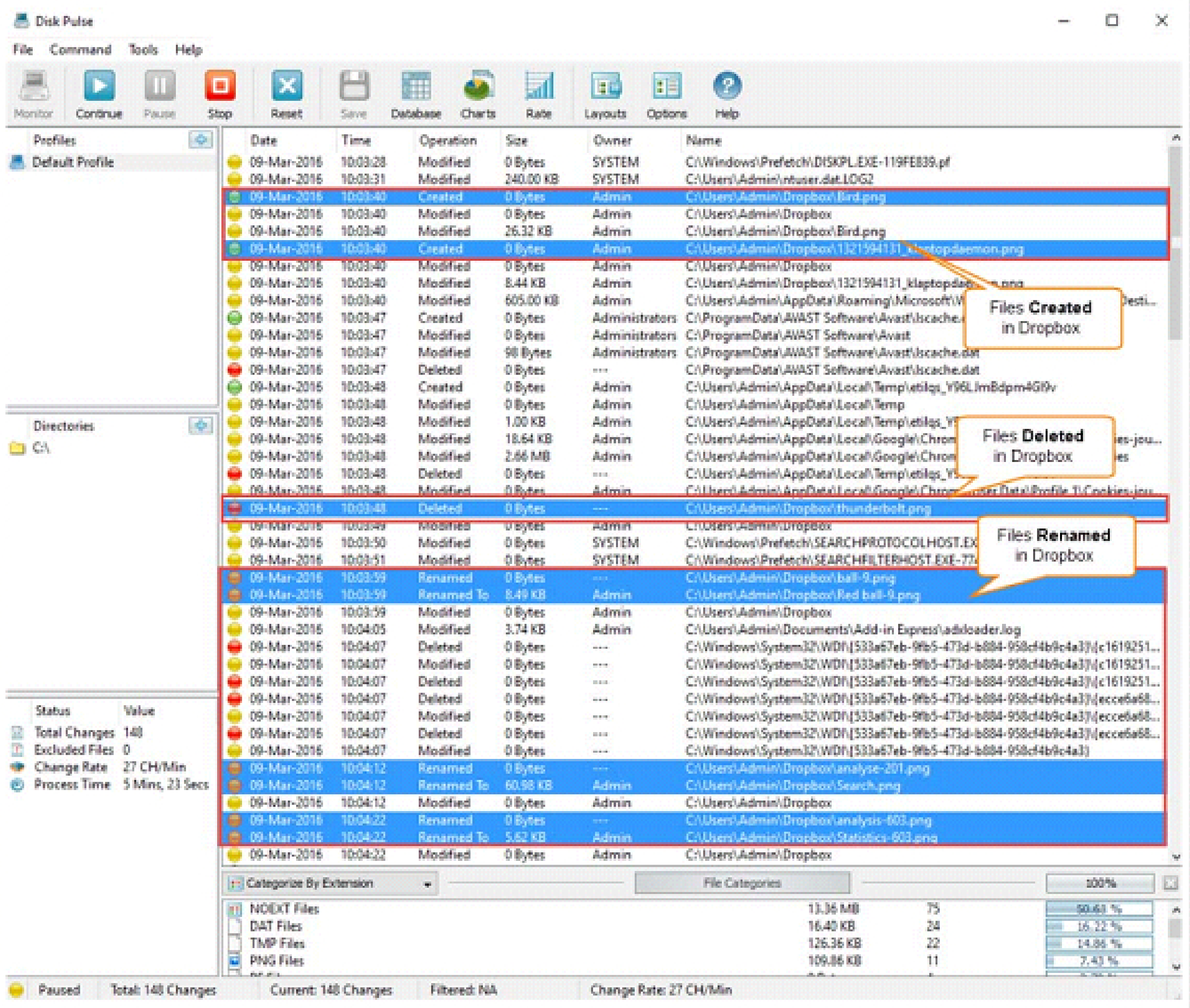
- You can view changes (create, modify/rename, and delete) to the Dropbox using tools such as **DiskPulse**, **Directory Monitor**, etc.

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

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



Date	Time	Operation	Size	Owner	Name
09-Mar-2016	10:03:28	Modified	0 Bytes	SYSTEM	C:\Windows\Prefetch\DISKPL.EXE-119FE839.pf
09-Mar-2016	10:03:31	Modified	240.00 KB	SYSTEM	C:\Users\Admin\ntuser.dat.LOG2
09-Mar-2016	10:03:40	Created	0 Bytes	Admin	C:\Users\Admin\Dropbox\Bird.png
09-Mar-2016	10:03:40	Modified	0 Bytes	Admin	C:\Users\Admin\Dropbox
09-Mar-2016	10:03:40	Modified	26.32 KB	Admin	C:\Users\Admin\Dropbox\Bird.png
09-Mar-2016	10:03:40	Created	0 Bytes	Admin	C:\Users\Admin\Dropbox\1321594131_klaptopdaemon.png
09-Mar-2016	10:03:40	Modified	0 Bytes	Admin	C:\Users\Admin\Dropbox
09-Mar-2016	10:03:40	Modified	8.44 KB	Admin	C:\Users\Admin\Dropbox\1321594131_klaptopda n.png
09-Mar-2016	10:03:40	Modified	605.00 KB	Admin	C:\Users\Admin\AppData\Roaming\Microsoft\W Desti...
09-Mar-2016	10:03:47	Created	0 Bytes	Administrators	C:\ProgramData\AVAST Software\Avast\lscache.
09-Mar-2016	10:03:47	Modified	0 Bytes	Administrators	C:\ProgramData\AVAST Software\Avast
09-Mar-2016	10:03:47	Modified	98 Bytes	Administrators	C:\ProgramData\AVAST Software\Avast\lscache.dat
09-Mar-2016	10:03:47	Deleted	0 Bytes	---	C:\ProgramData\AVAST Software\Avast\lscache.dat
09-Mar-2016	10:03:48	Created	0 Bytes	Admin	C:\Users\Admin\AppData\Local\Temp\etilqs_Y96LImBdpm4GI9v
09-Mar-2016	10:03:48	Modified	0 Bytes	Admin	C:\Users\Admin\AppData\Local\Temp
09-Mar-2016	10:03:48	Modified	1.00 KB	Admin	C:\Users\Admin\AppData\Local\Temp\etilqs_Y
09-Mar-2016	10:03:48	Modified	18.64 KB	Admin	C:\Users\Admin\AppData\Local\Google\Chrom es-jou...
09-Mar-2016	10:03:48	Modified	2.66 MB	Admin	C:\Users\Admin\AppData\Local\Google\Chrom es
09-Mar-2016	10:03:48	Deleted	0 Bytes	---	C:\Users\Admin\AppData\Local\Temp\etilqs_Y
09-Mar-2016	10:03:48	Modified	0 Bytes	Admin	C:\Users\Admin\AppData\Local\Google\Chrom User Data\Profile 1\Cookies-jou...
09-Mar-2016	10:03:48	Deleted	0 Bytes	---	C:\Users\Admin\Dropbox\thunderbolt.png
09-Mar-2016	10:03:49	Modified	0 Bytes	Admin	C:\Users\Admin\Dropbox
09-Mar-2016	10:03:50	Modified	0 Bytes	SYSTEM	C:\Windows\Prefetch\SEARCHPROTOCOLHOST.EX
09-Mar-2016	10:03:51	Modified	0 Bytes	SYSTEM	C:\Windows\Prefetch\SEARCHFILTERHOST.EXE-77
09-Mar-2016	10:03:59	Renamed	0 Bytes	---	C:\Users\Admin\Dropbox\ball-9.png
09-Mar-2016	10:03:59	Renamed To	8.49 KB	Admin	C:\Users\Admin\Dropbox\Red ball-9.png
09-Mar-2016	10:03:59	Modified	0 Bytes	Admin	C:\Users\Admin\Dropbox
09-Mar-2016	10:04:05	Modified	3.74 KB	Admin	C:\Users\Admin\Documents\Add-in Express\adxloader.log
09-Mar-2016	10:04:07	Deleted	0 Bytes	---	C:\Windows\System32\WDI\{533a67eb-9fb5-473d-b884-958cf4b9c4a3}\{c1619251...
09-Mar-2016	10:04:07	Modified	0 Bytes	---	C:\Windows\System32\WDI\{533a67eb-9fb5-473d-b884-958cf4b9c4a3}\{c1619251...
09-Mar-2016	10:04:07	Deleted	0 Bytes	---	C:\Windows\System32\WDI\{533a67eb-9fb5-473d-b884-958cf4b9c4a3}\{c1619251...
09-Mar-2016	10:04:07	Deleted	0 Bytes	---	C:\Windows\System32\WDI\{533a67eb-9fb5-473d-b884-958cf4b9c4a3}\{ecce6a68...
09-Mar-2016	10:04:07	Modified	0 Bytes	---	C:\Windows\System32\WDI\{533a67eb-9fb5-473d-b884-958cf4b9c4a3}\{ecce6a68...
09-Mar-2016	10:04:07	Deleted	0 Bytes	---	C:\Windows\System32\WDI\{533a67eb-9fb5-473d-b884-958cf4b9c4a3}\{ecce6a68...
09-Mar-2016	10:04:07	Modified	0 Bytes	---	C:\Windows\System32\WDI\{533a67eb-9fb5-473d-b884-958cf4b9c4a3}
09-Mar-2016	10:04:12	Renamed	0 Bytes	---	C:\Users\Admin\Dropbox\analyse-201.png
09-Mar-2016	10:04:12	Renamed To	60.98 KB	Admin	C:\Users\Admin\Dropbox\Search.png
09-Mar-2016	10:04:12	Modified	0 Bytes	Admin	C:\Users\Admin\Dropbox
09-Mar-2016	10:04:22	Renamed	0 Bytes	---	C:\Users\Admin\Dropbox\analysis-603.png
09-Mar-2016	10:04:22	Renamed To	5.62 KB	Admin	C:\Users\Admin\Dropbox\Statistics-603.png
09-Mar-2016	10:04:22	Modified	0 Bytes	Admin	C:\Users\Admin\Dropbox

Files **Created** in Dropbox

Files **Deleted** in Dropbox

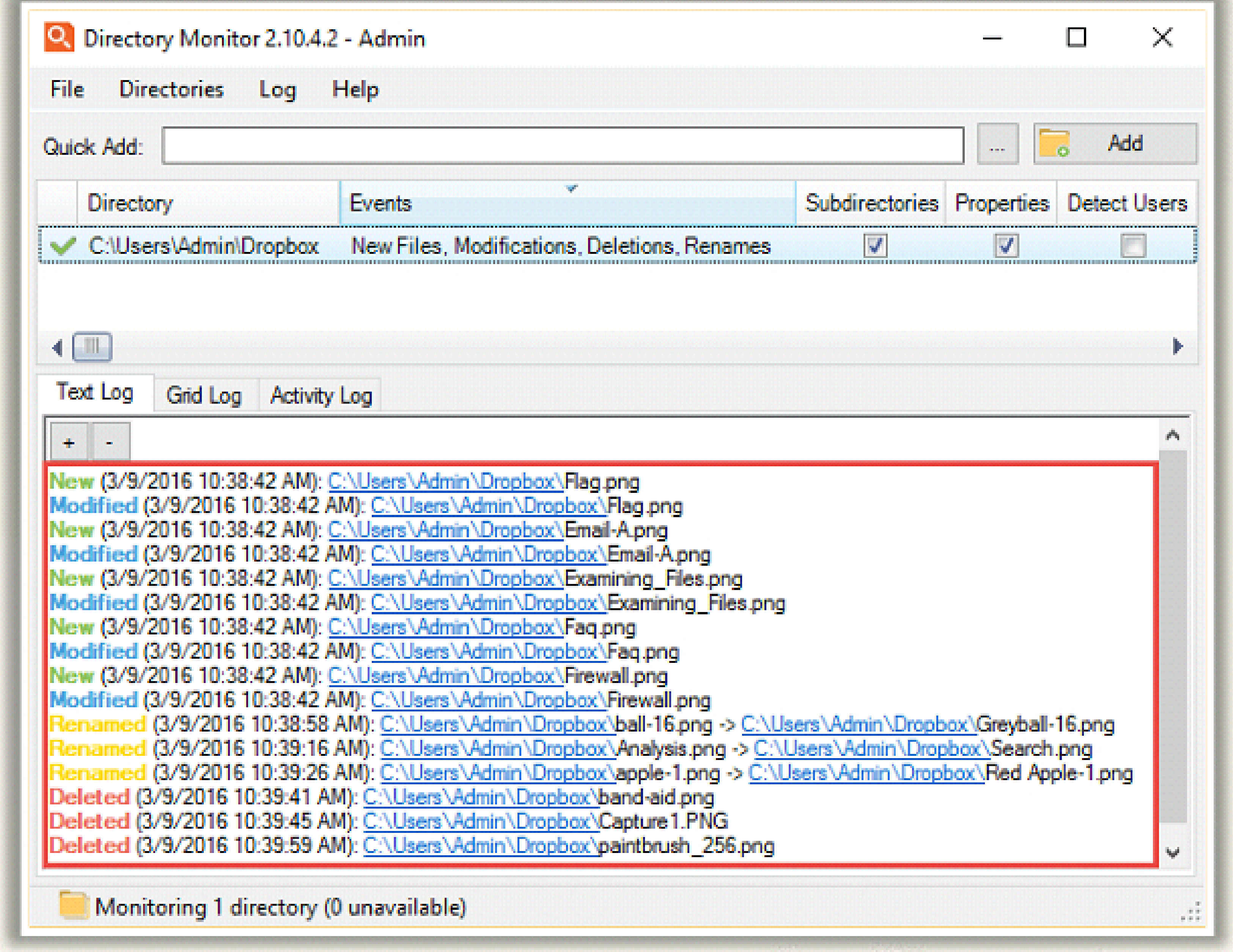
Files **Renamed** in Dropbox

Status	Value
Total Changes	148
Excluded Files	0
Change Rate	27 CH/Min
Process Time	5 Mins, 23 Secs

NOEXT Files	13.36 MB	75	50.63 %
DAT Files	16.40 KB	24	16.22 %
TMP Files	126.36 KB	22	14.86 %
PNG Files	109.86 KB	11	7.43 %

Paused | Total: 148 Changes | Current: 148 Changes | Filtered: NA | Change Rate: 27 CH/Min

http://www.diskpulse.com



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
```

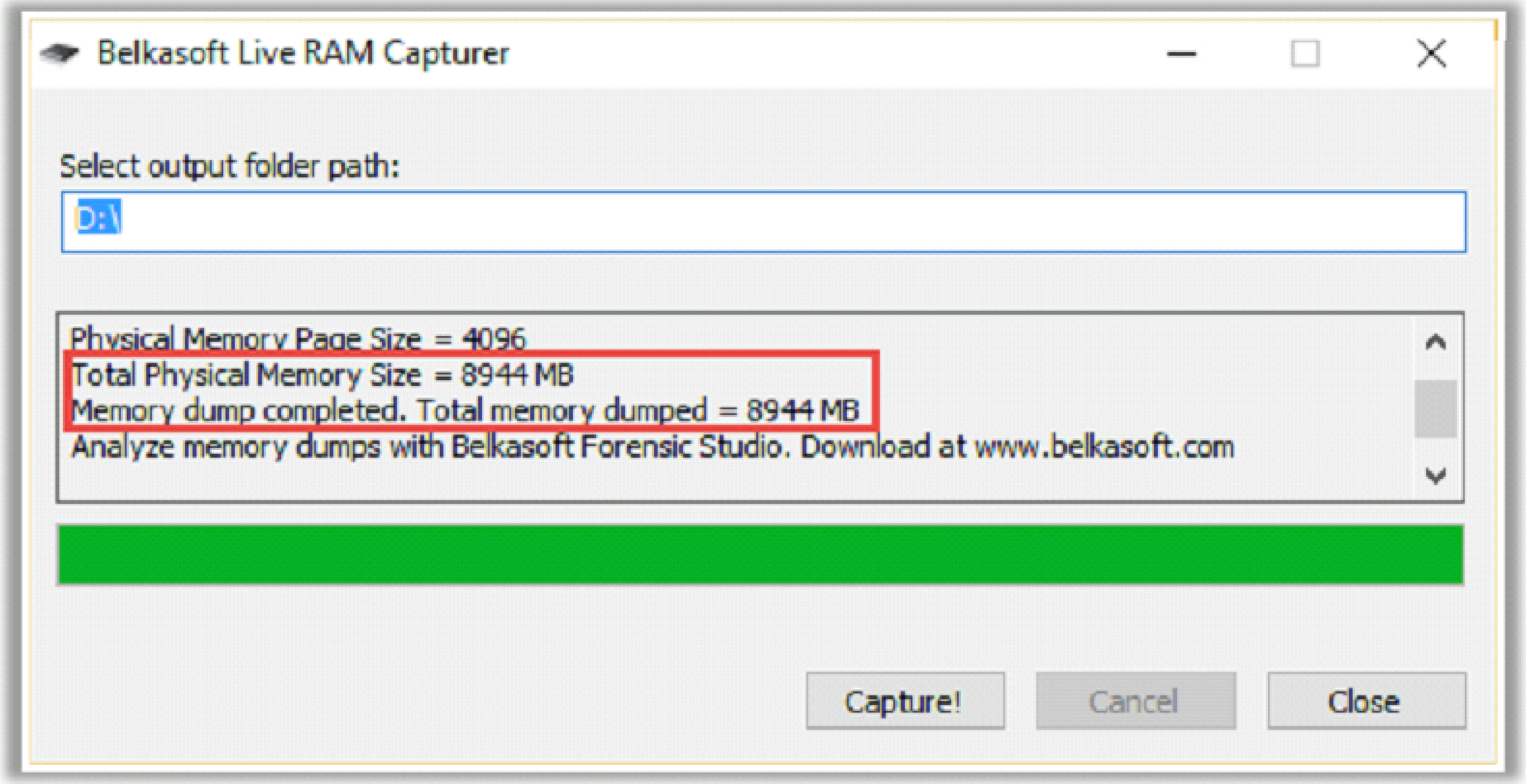
Monitoring 1 directory (0 unavailable)

https://directorymonitor.com

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

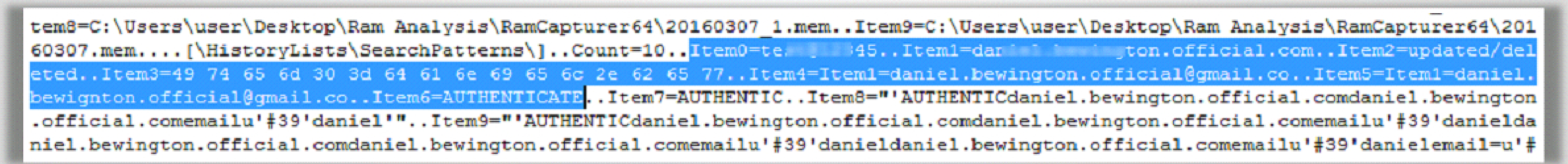
Artifacts Left by Dropbox Client on Windows (Cont'd)

- **HxD:**

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

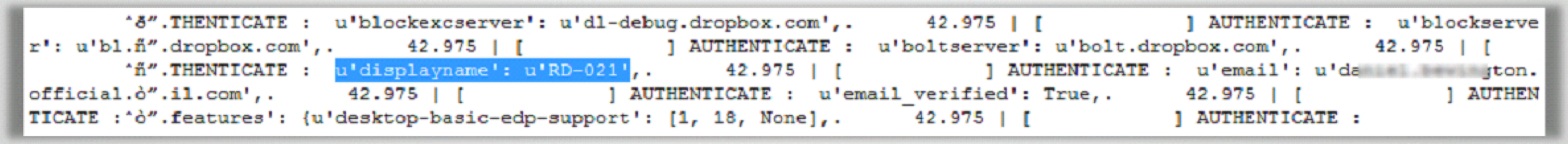
- **Given below are the strings that assists you to find out information of evidentiary value** (such as email ID, display name, filecache.dbx path, Server time, file list, and deleted file):

  - **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=dar[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



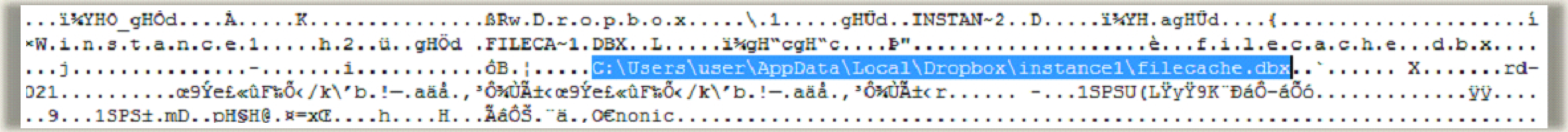
```
      ˆð”.THENTICATE :  u'blockexcserver': u'dl-debug.dropbox.com',.      42.975 | [              ] AUTHENTICATE :  u'blockserve
r': u'bl.ñ”.dropbox.com',.      42.975 | [              ] AUTHENTICATE :  u'boltserver': u'bolt.dropbox.com',.      42.975 | [
      ˆñ”.THENTICATE :  u'displayname': u'RD-021',.      42.975 | [              ] AUTHENTICATE :  u'email': u'da[redacted]gton.
official.ò”.il.com',.      42.975 | [              ] AUTHENTICATE :  u'email_verified': True,.      42.975 | [              ] AUTHEN
TICATE :ˆò”.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:\**

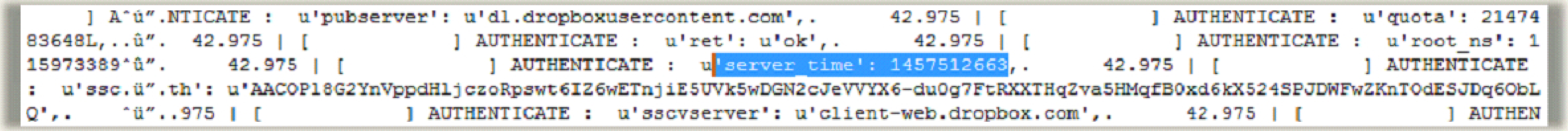
Artifacts Left by Dropbox Client on Windows (Cont'd)

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



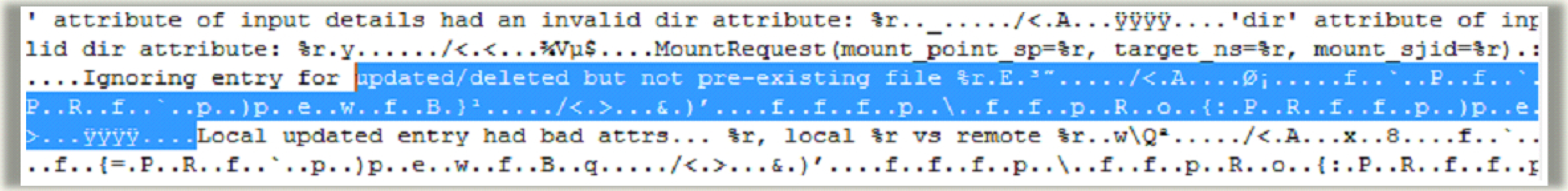
```
...ï¾YHO_gHÔd....À.....K...............ßRw.D.r.o.p.b.o.x.....\.1.....gHÜd..INSTAN~2..D.....ï¾YH.agHÜd....{.....................i
×W.i.n.s.t.a.n.c.e.1.....h.2..ü..gHÖd .FILECA~1.DBX..L.....ï¾gH"cgH"c....Þ"....................è...f.i.l.e.c.a.c.h.e...d.b.x....
...j...............-.......i...........ôB.¦.....C:\Users\user\AppData\Local\Dropbox\instance1\filecache.dbx..`...... X.......rd-
021..........œ9Ýe£«ûF‰Ő‹/k\'b.!—.aää.,³Ô¾ÙÃ±‹œ9Ýe£«ûF‰Ő‹/k\'b.!—.aää.,³Ô¾ÙÃ±‹r...... -...1SPSU(LŸyŸ9K¨ÐáÔ–áŐó............ÿÿ....
..9...1SPS±.mD..pH§H@.¤=xŒ....h....H...ÅâÔŠ.¨ä.,O€nonic.............................................................
```

- **server_time -** provides server time



```
    ] Aˆû".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'AACOP18G2YnVppdHljczoRpswt6IZ6wETnjiE5UVk5wDGN2cJeVVYX6-du0g7FtRXXTHqZva5HMqfB0xd6kX524SPJDWFwZKnTOdESJDq6ObL
Q',.    ˆü"..975 | [              ] AUTHENTICATE :  u'sscvserver': u'client-web.dropbox.com',.       42.975 | [              ] AUTHEN
```

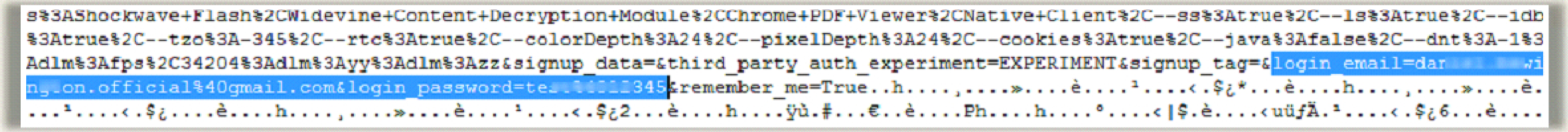
- **updated/deleted -** displays updated/deleted file



```
' 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.³"...../<.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
```

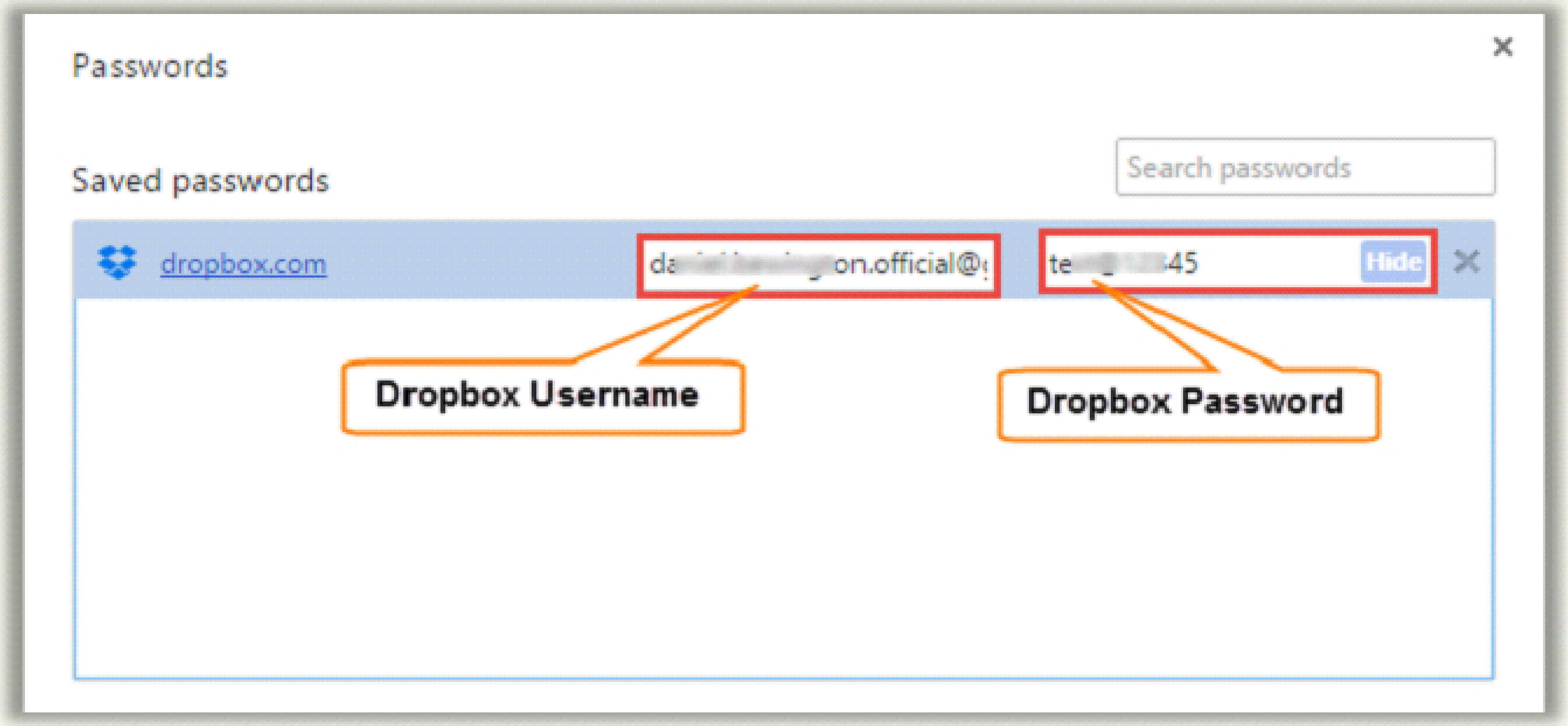
Artifacts Left by Dropbox Client on Windows (Cont'd)

- 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]345&remember_me=True..h....,....»....è....¹....<.$¿*...è....h....,....»....è.
...¹....<.$¿....è....h....,....»....è....¹....<.$¿2...è....h....ÿù.#...€..è....Ph....h....°....<|$.è....<uüƒÄ.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

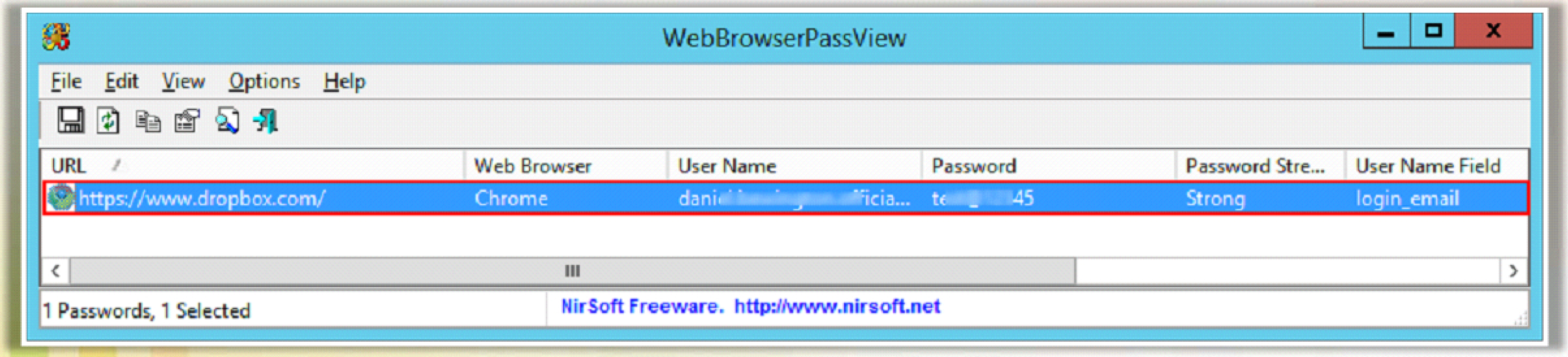


da[redacted]on.official@

te[redacted]45

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

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

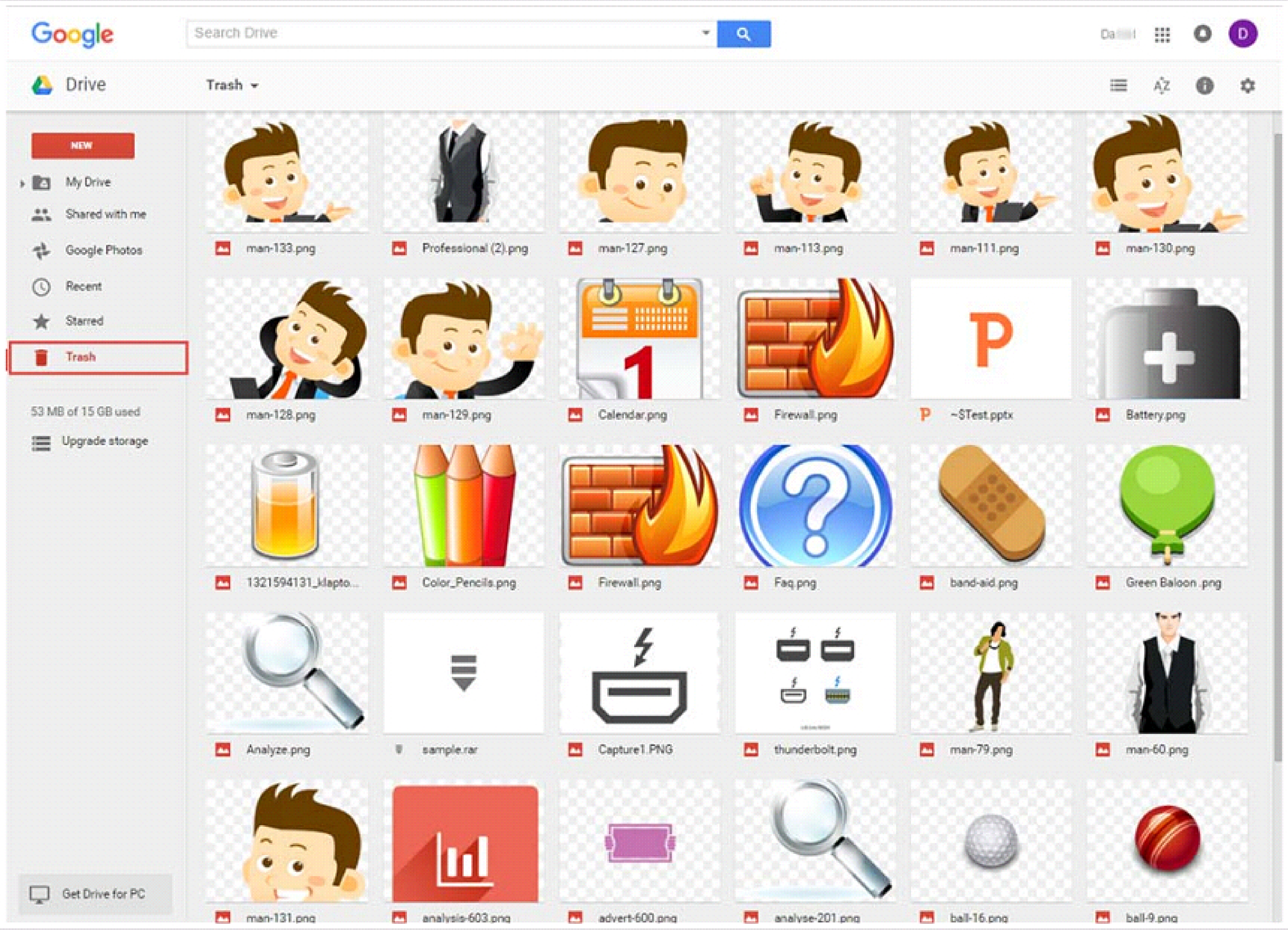
You can also recover information from

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

Investigating Google Drive Cloud Storage Service

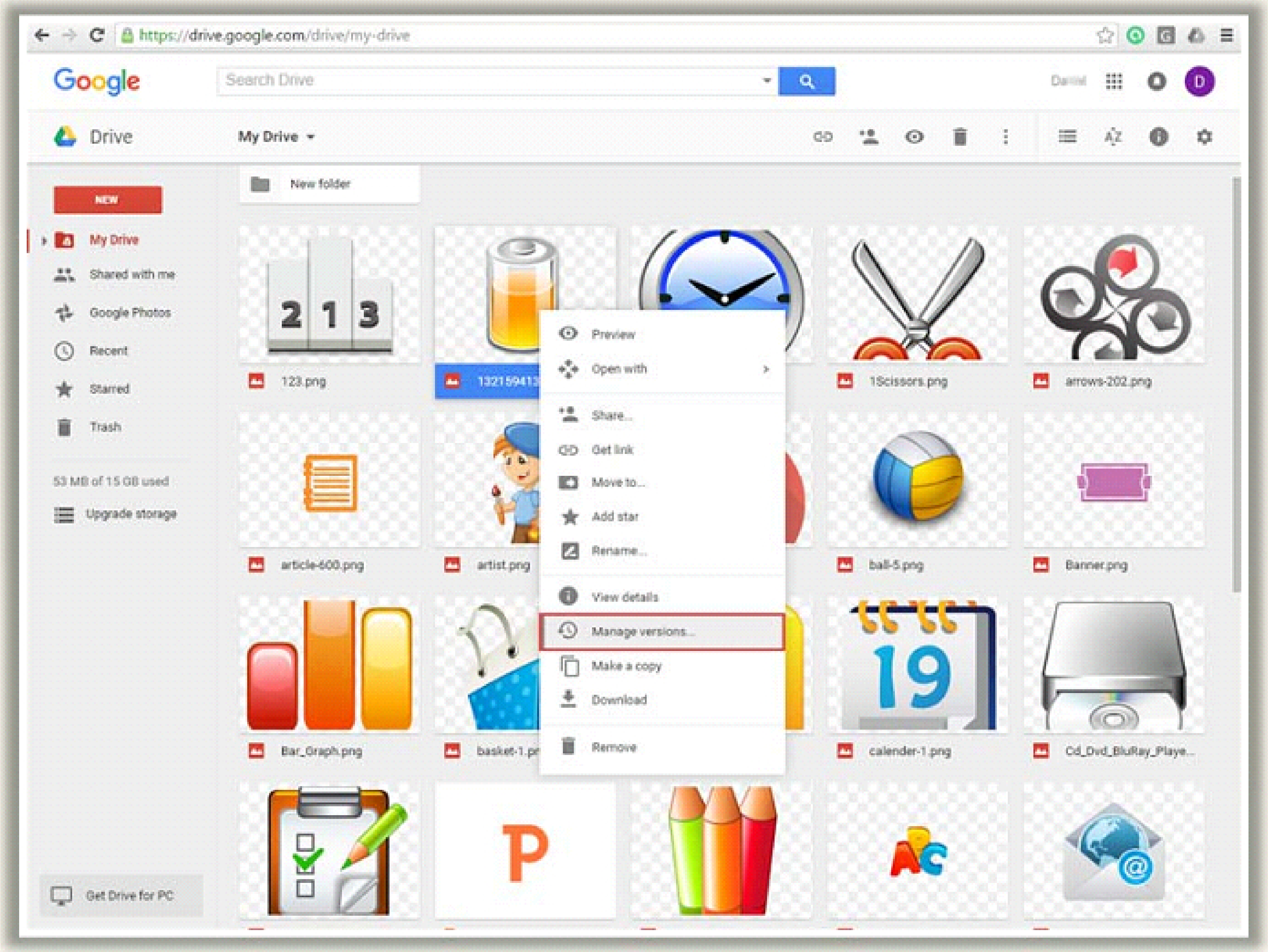
Artifacts Left by Google Drive Web Portal

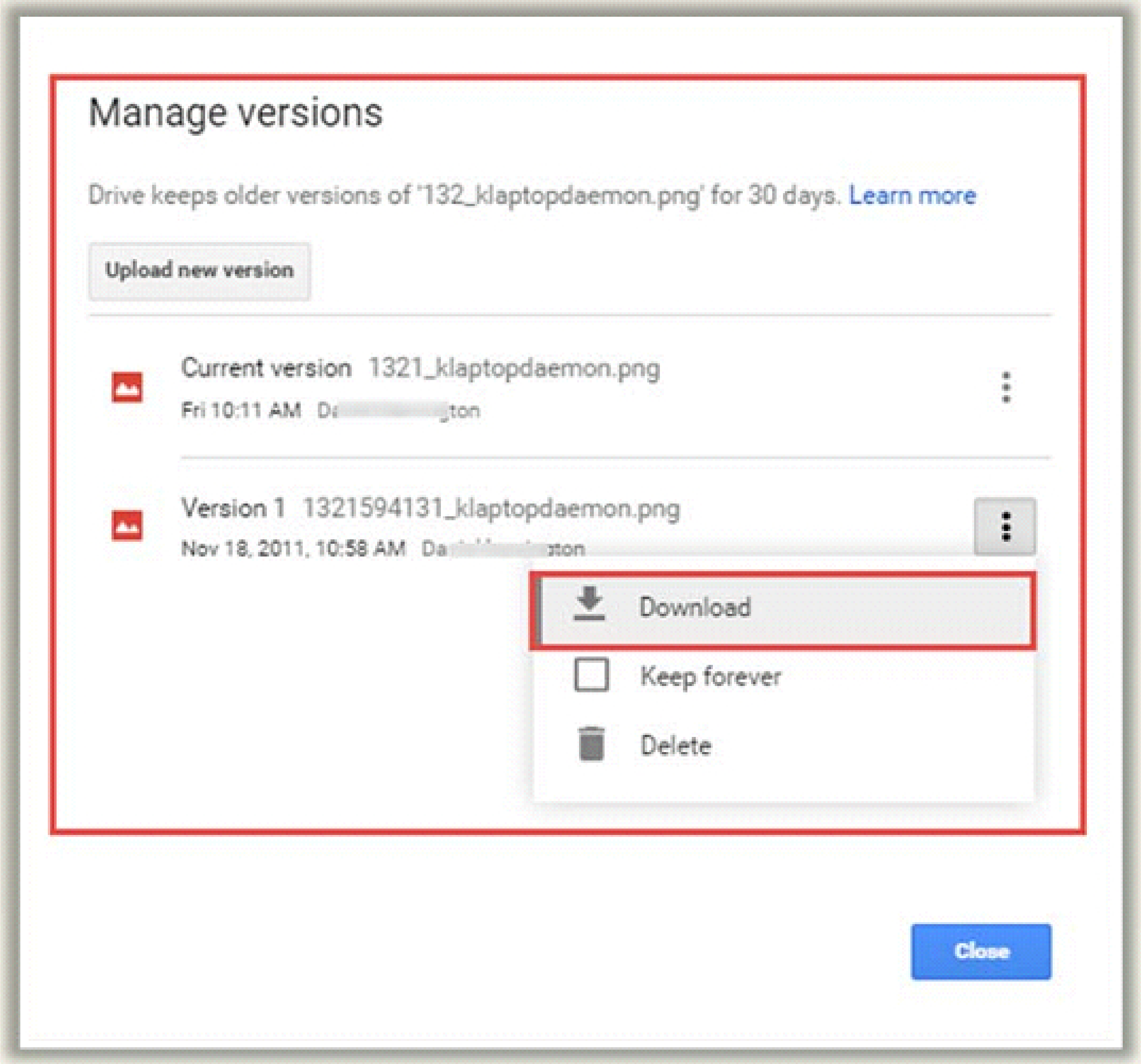
- You can login to the user’s profile and access Google Drive’s information about **deleted files**
- Click on the **Trash** tab to view the deleted files



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

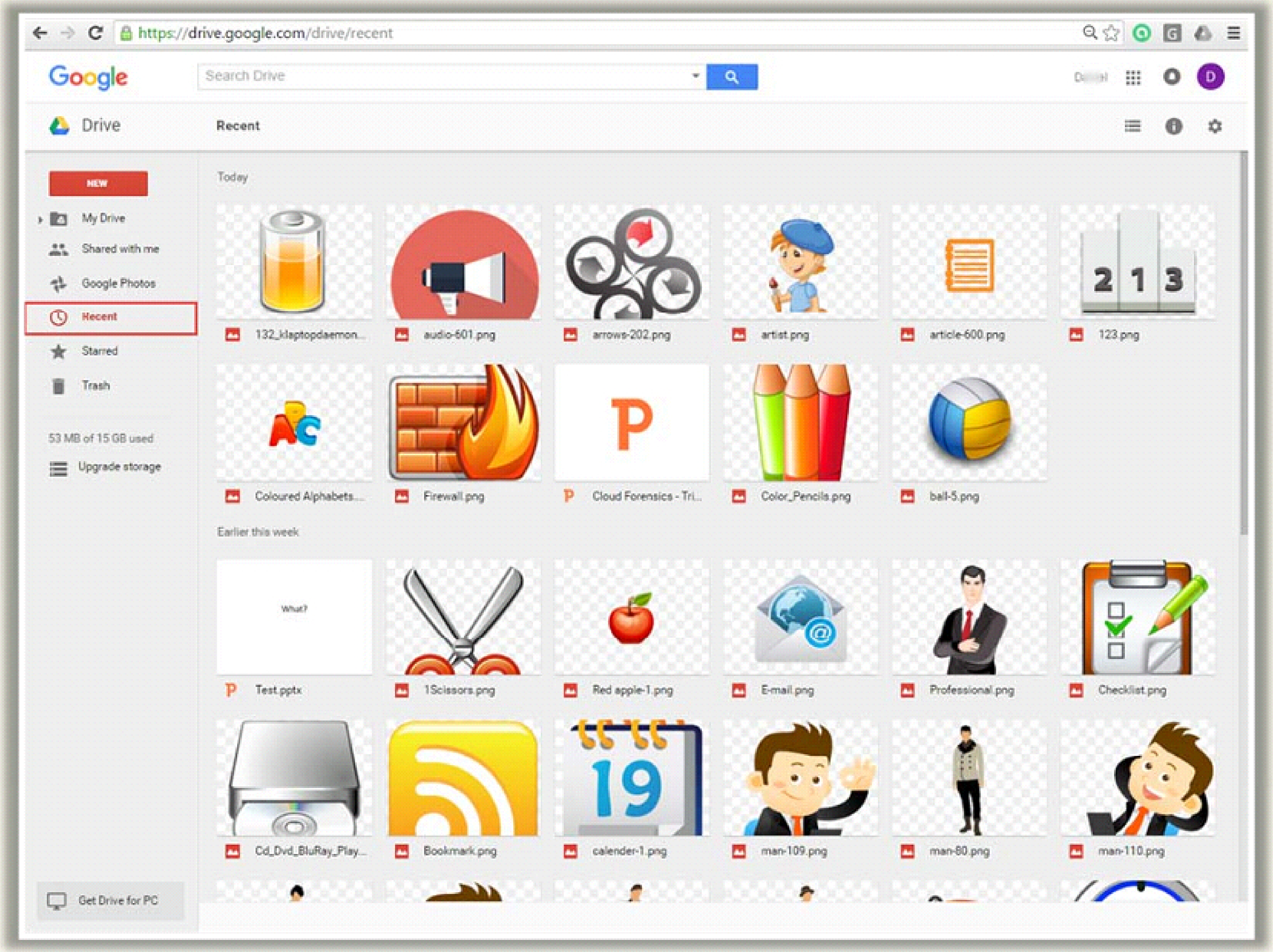
Upload new version

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

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

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

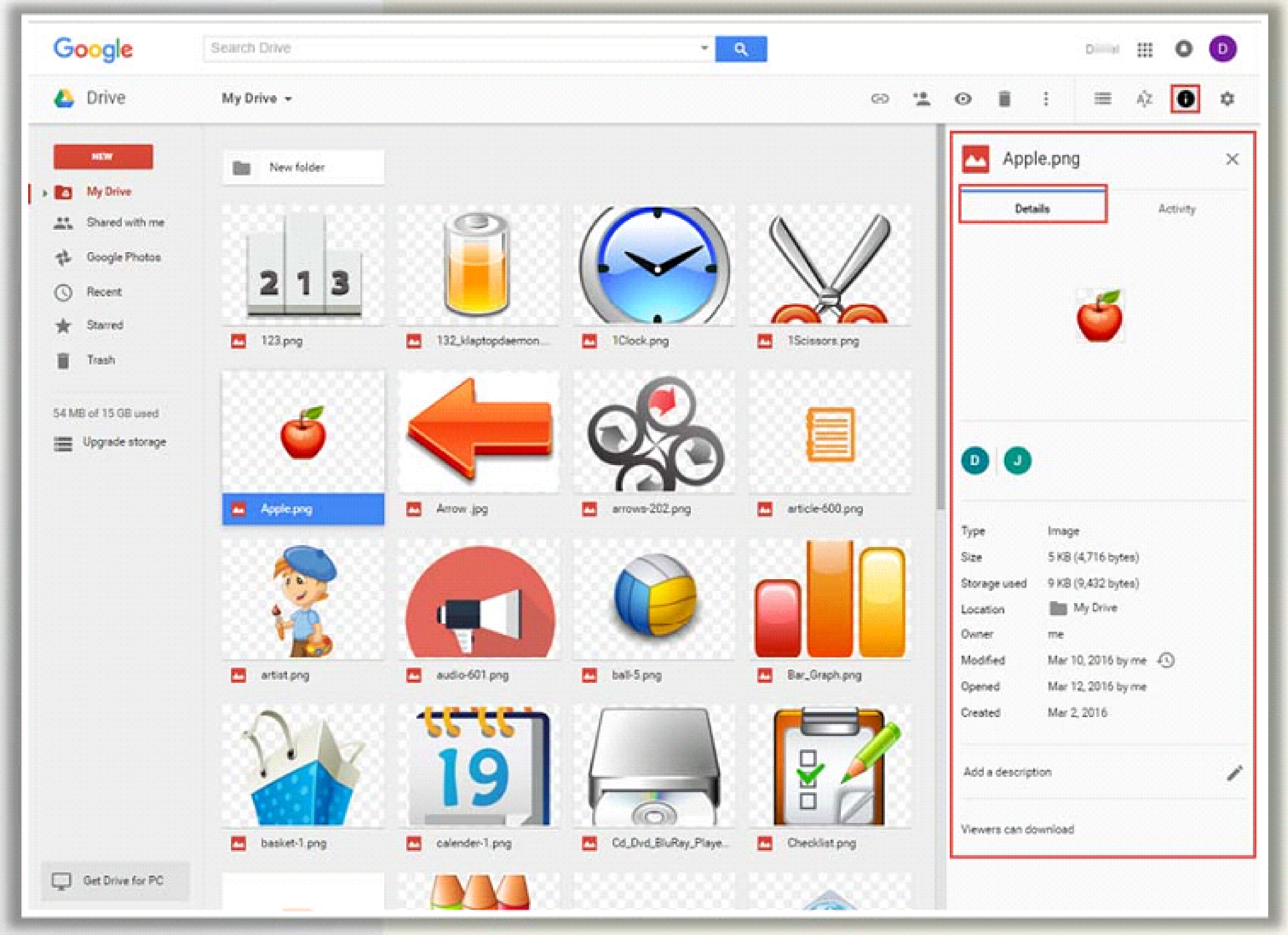
You can view the recent visits by clicking the **Recent** tab



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 (ℹ) 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.



Type Image
Size 5 KB (4,716 bytes)
Storage used 9 KB (9,432 bytes)
Location My Drive
Owner me
Modified Mar 10, 2016 by me
Opened Mar 12, 2016 by me
Created Mar 2, 2016

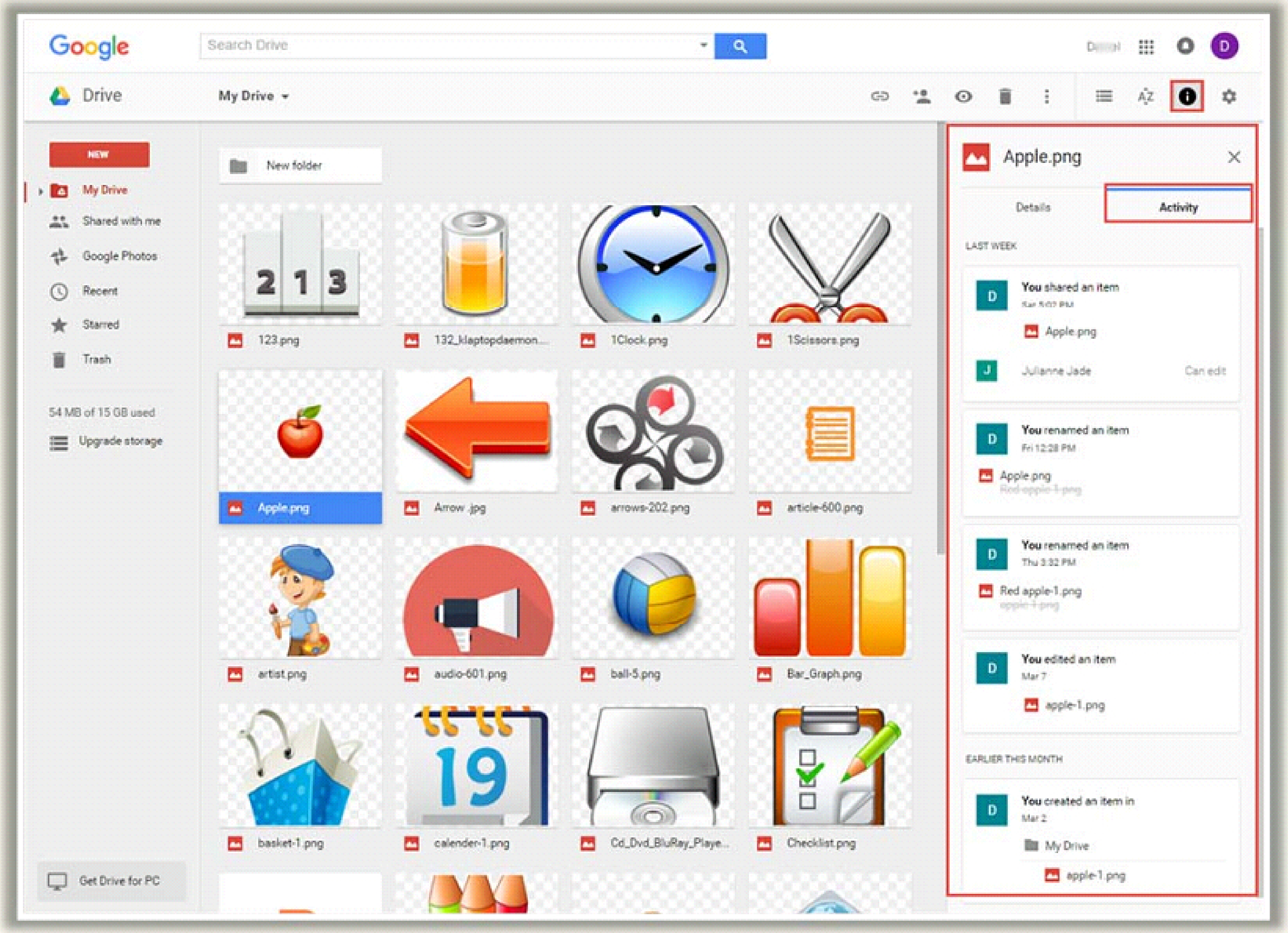
Add a description

Viewers can download

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



Apple.png

Details | Activity

LAST WEEK

You shared an item
Sat 5:02 PM
Apple.png
Julianne Jade — Can edit

You renamed an item
Fri 12:28 PM
Apple.png
~~Red-apple-1.png~~

You renamed an item
Thu 3:32 PM
Red apple-1.png
~~apple-1.png~~

You edited an item
Mar 7
apple-1.png

EARLIER THIS MONTH

You created an item in
Mar 2
My Drive
apple-1.png

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."

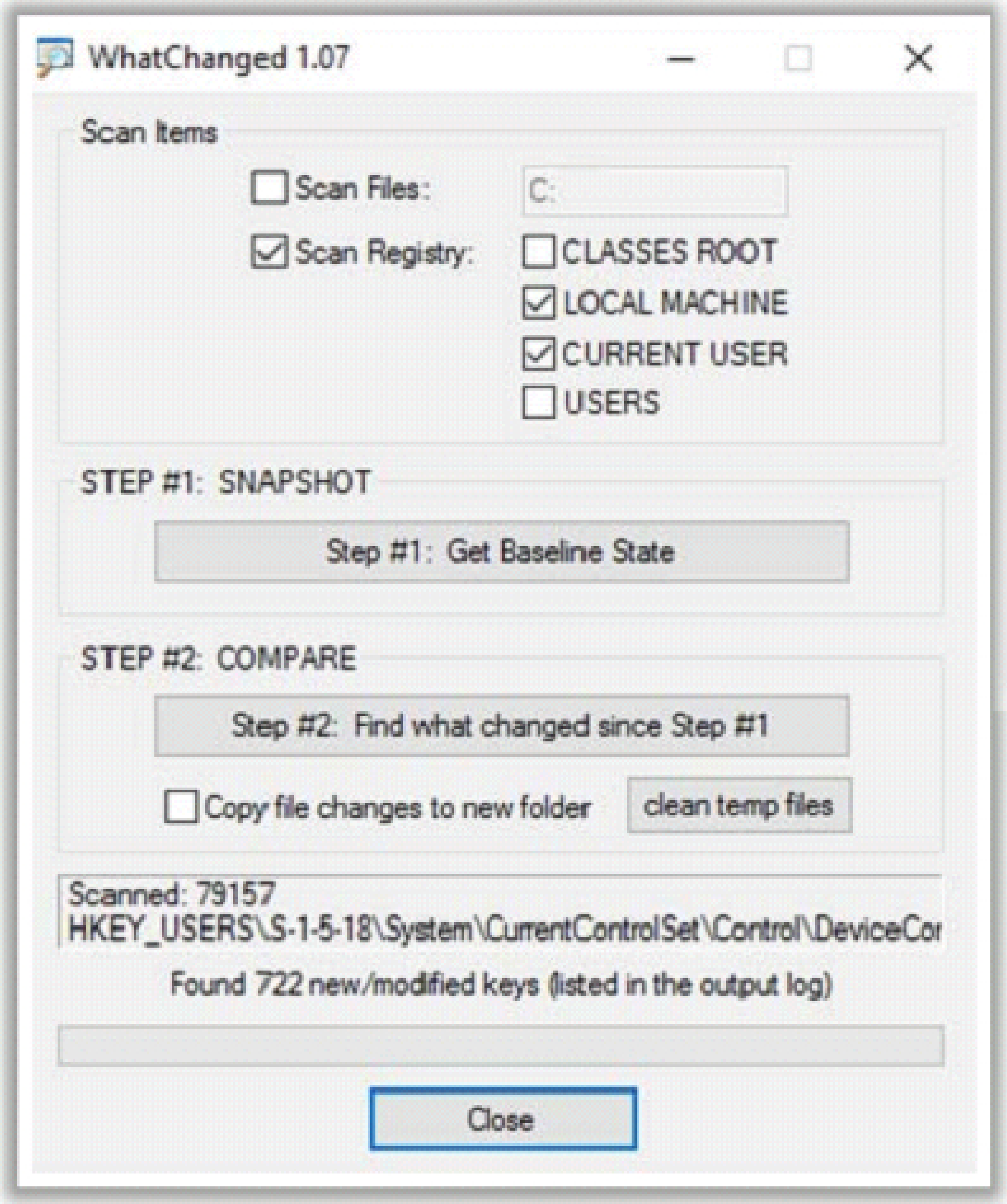
Artifacts Left by Google Drive Client on Windows

- 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**

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

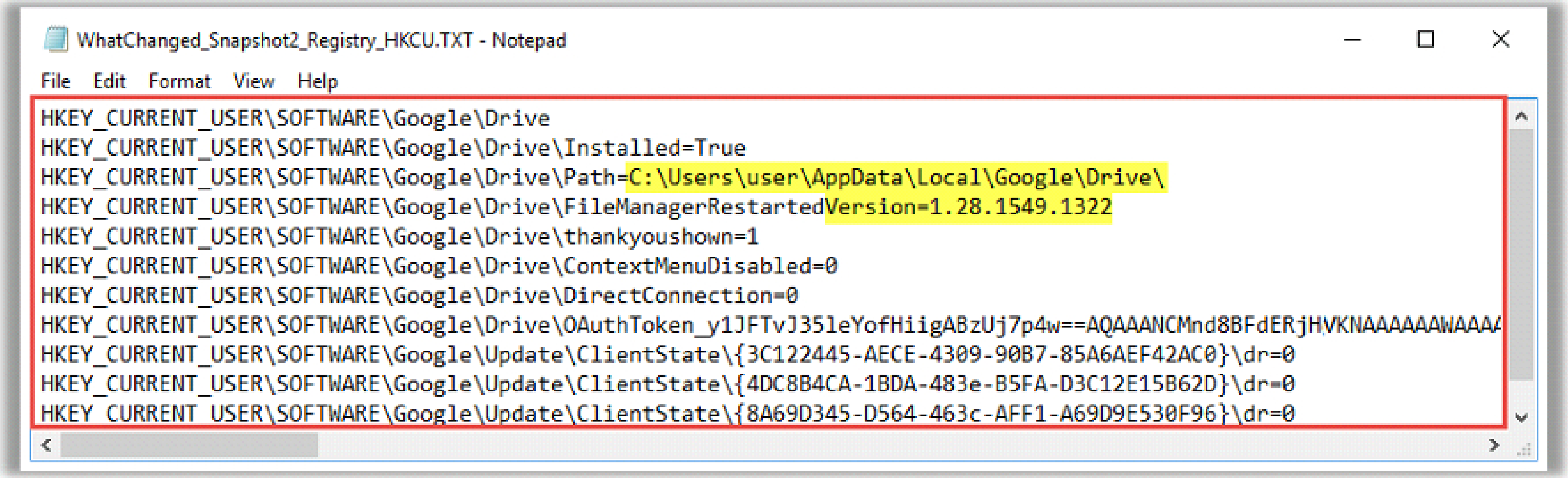
□ Copy file changes to new folder

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

```
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==AQAAANCMnd8BFdERjHVKNAAAAAWAAAA
HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{3C122445-AECE-4309-90B7-85A6AEF42AC0}\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
```

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:

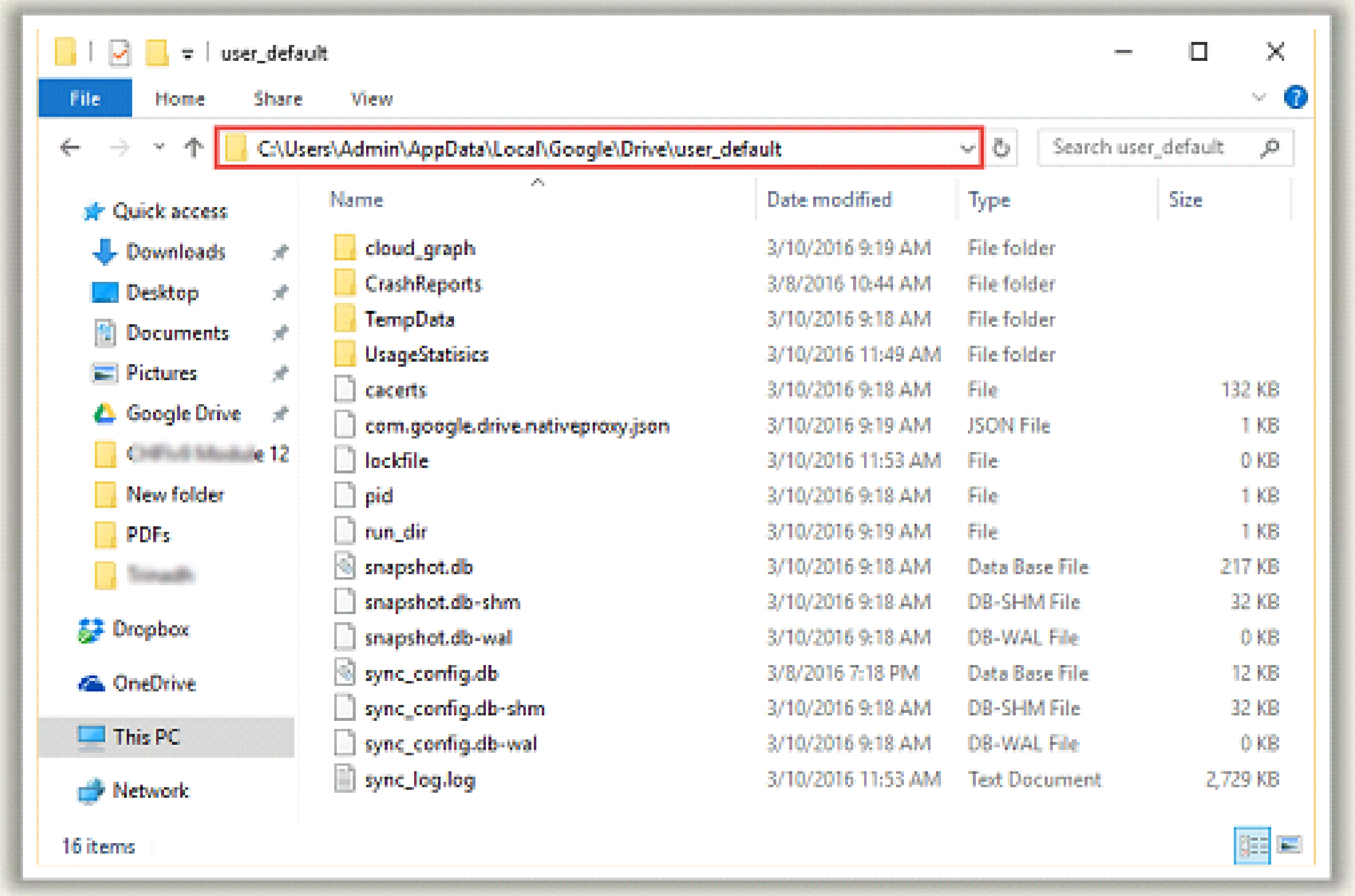
C:\Users\<username>\Desktop\Google Drive.lnk

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

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

Prefetch Files:

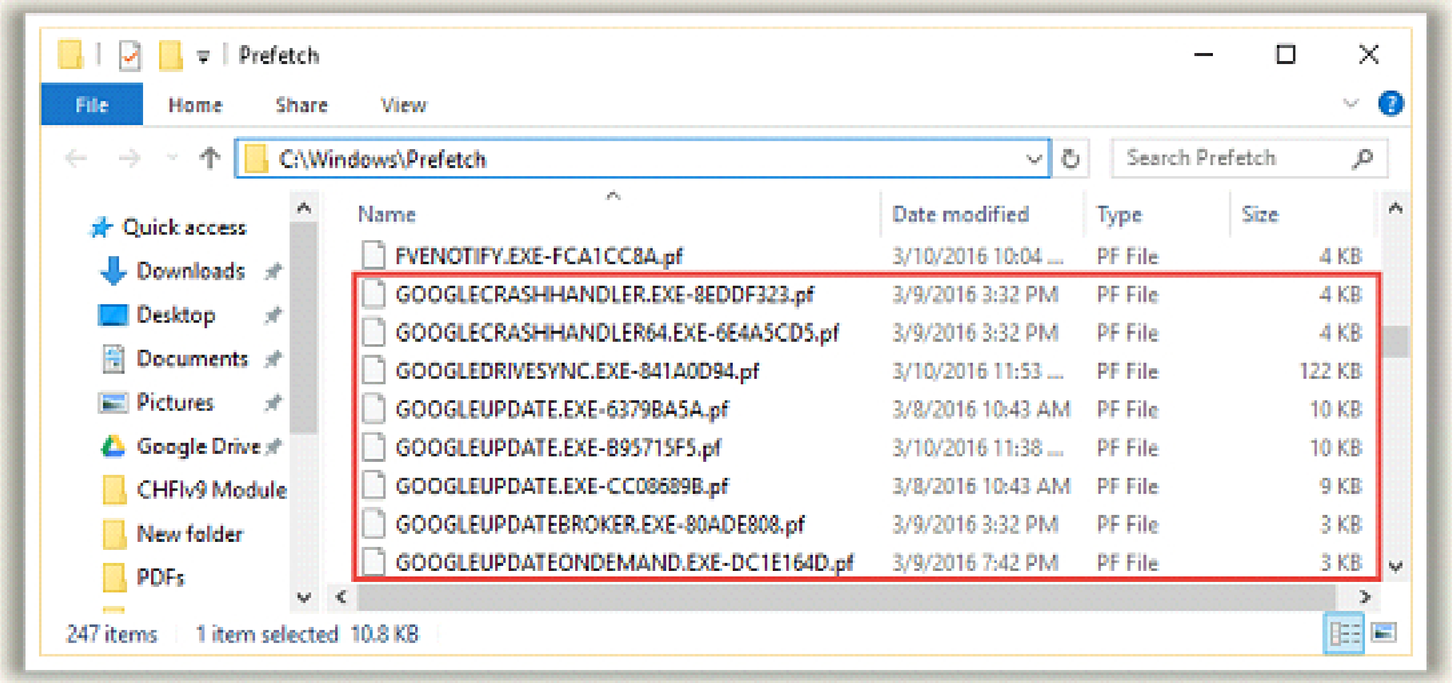
Located at C:\Windows\Prefetch



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

Name	Date modified	Type	Size
cloud_graph	3/10/2016 9:19 AM	File folder	
CrashReports	3/8/2016 10:44 AM	File folder	
TempData	3/10/2016 9:18 AM	File folder	
UsageStatisics	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 9:18 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	3/8/2016 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 11:53 AM	Text Document	2,729 KB

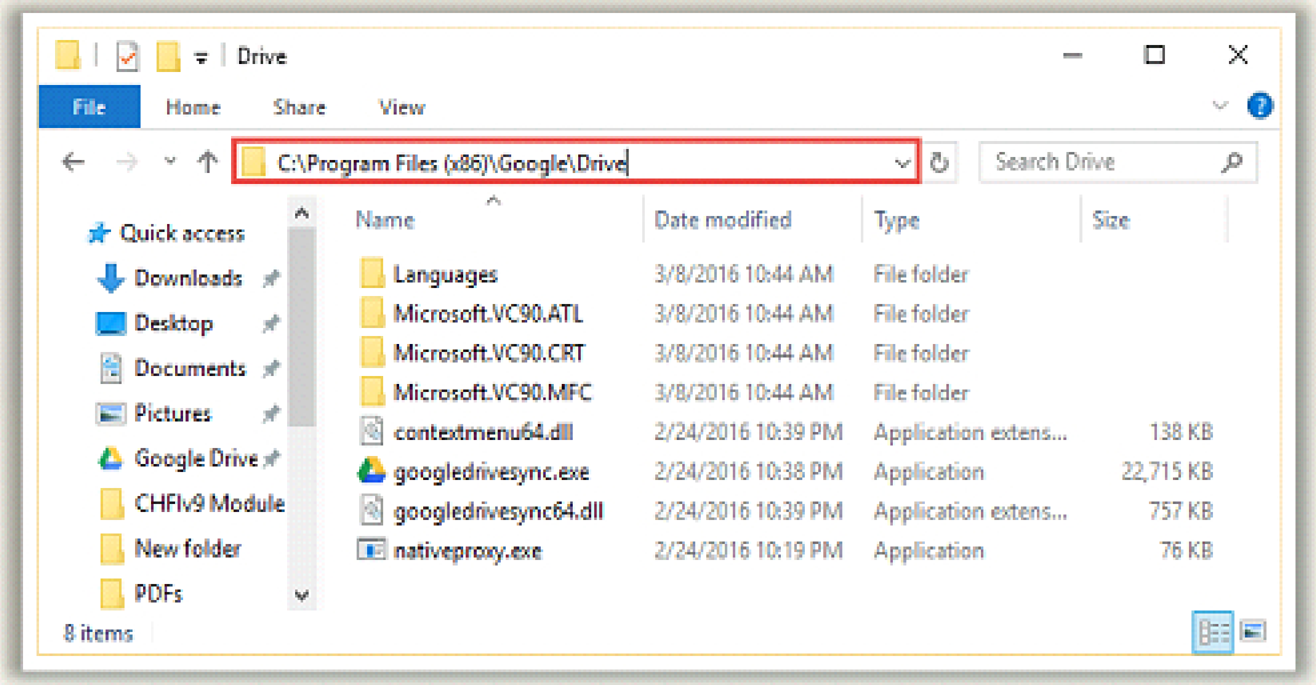
16 items



C:\Windows\Prefetch

Name	Date modified	Type	Size
FVENOTIFY.EXE-FCA1CC8A.pf	3/10/2016 10:04 ...	PF File	4 KB
GOOGLECRASHHANDLER.EXE-8EDDF323.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-6379BA5A.pf	3/8/2016 10:43 AM	PF File	10 KB
GOOGLEUPDATE.EXE-895715F5.pf	3/10/2016 11:38 ...	PF File	10 KB
GOOGLEUPDATE.EXE-CC08689B.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



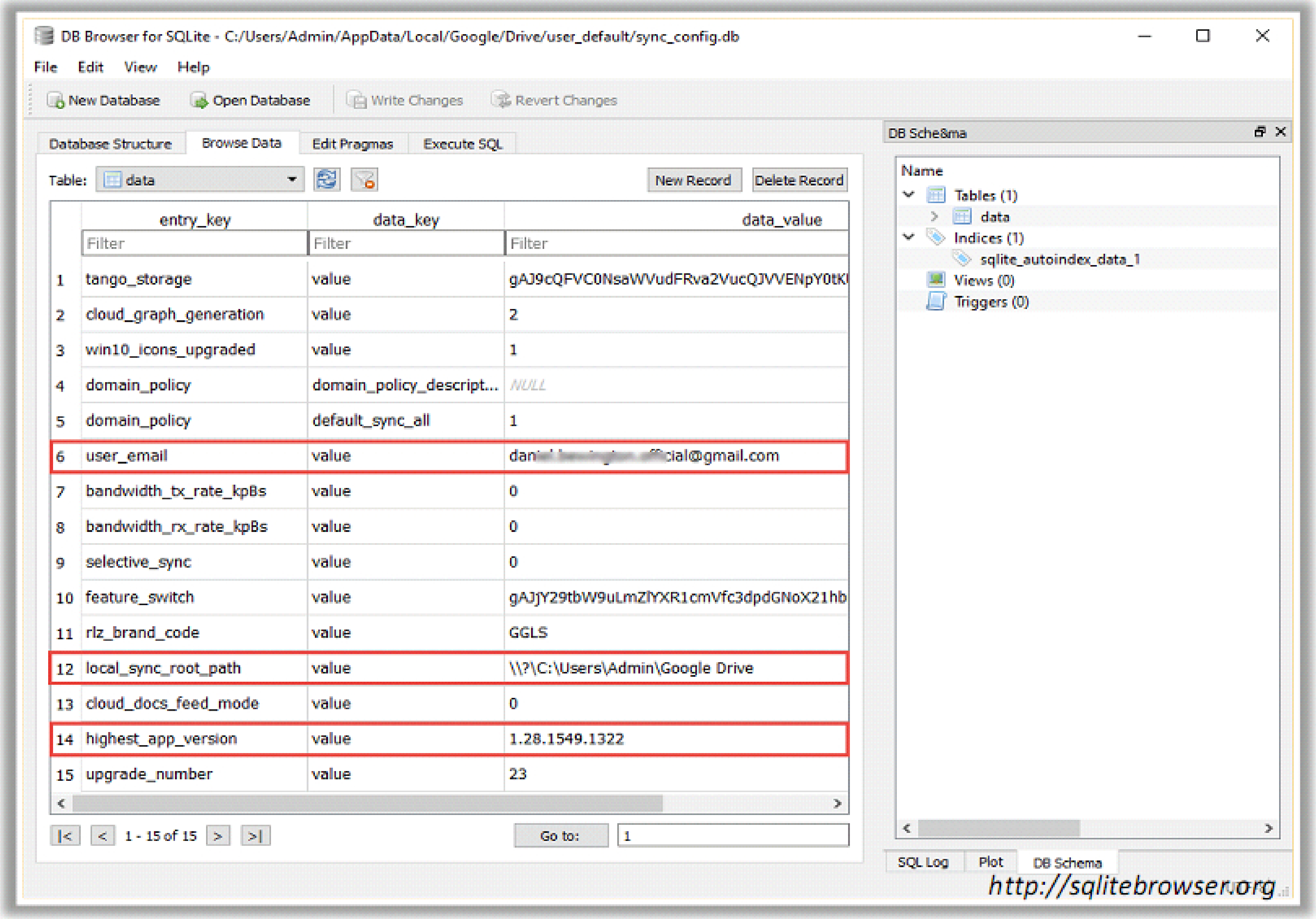
C:\Program Files (x86)\Google\Drive

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

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

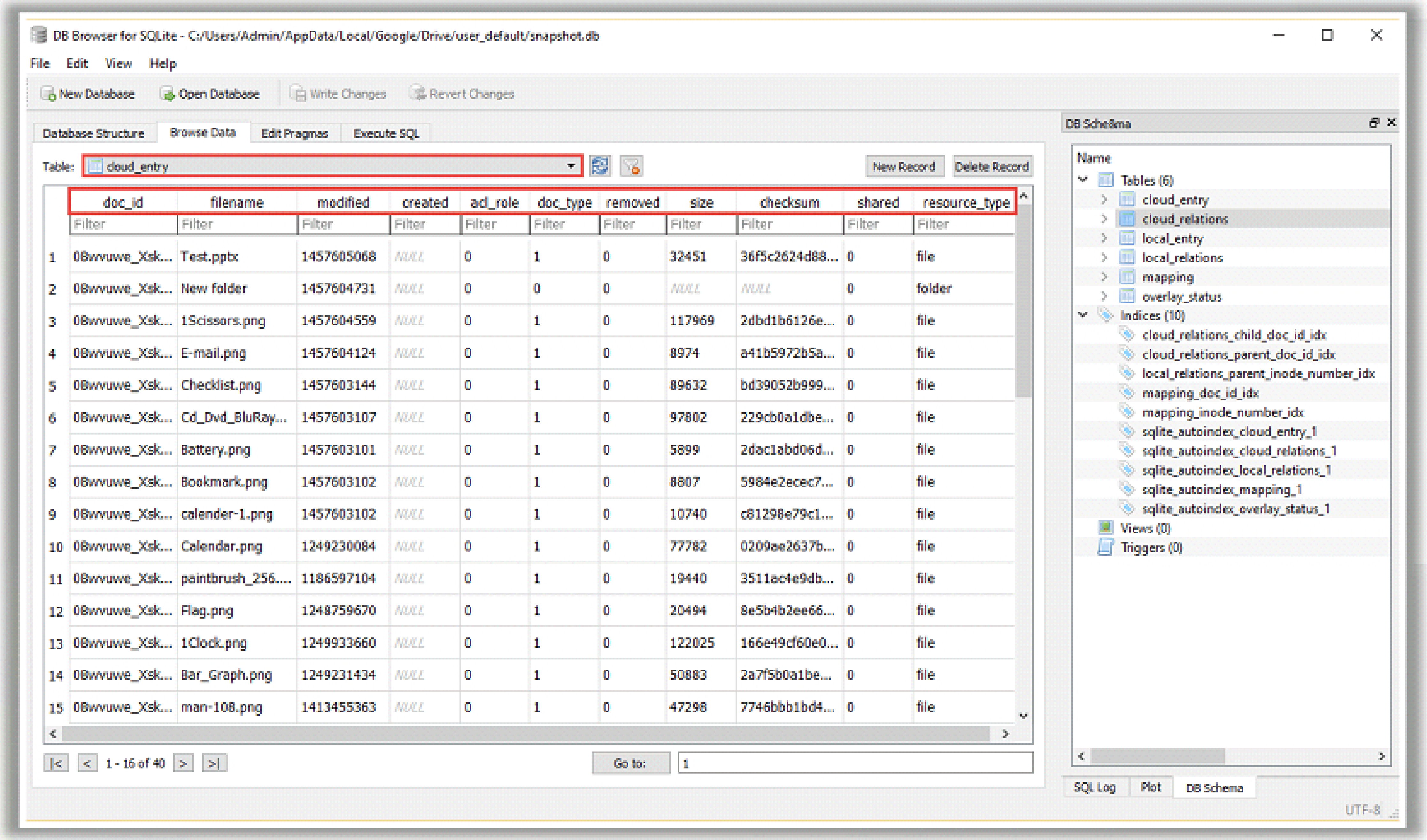


	entry_key	data_key	data_value
1	tango_storage	value	gAJ9cQFVC0NsaWVudFRva2VucQJVVENpY0tK
2	cloud_graph_generation	value	2
3	win10_icons_upgraded	value	1
4	domain_policy	domain_policy_descript...	NULL
5	domain_policy	default_sync_all	1
6	user_email	value	dani[redacted]cial@gmail.com
7	bandwidth_tx_rate_kpBs	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

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

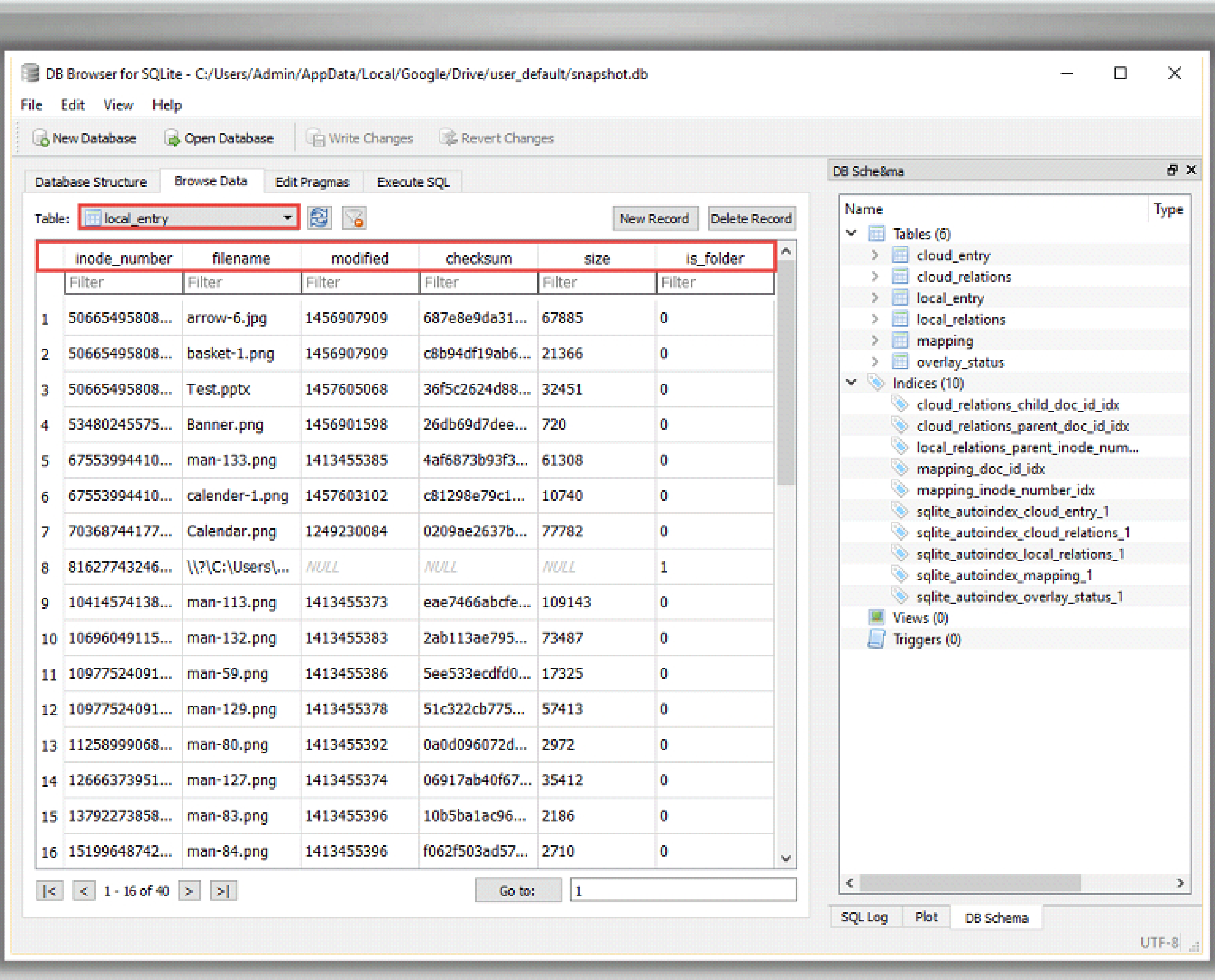
- Files given below are in SQlite3 format and can be accessed using SQlite browsers:
  - snapshot.db
  - sync_config.db
- You can run tools such as **DB Browser for SQLite** to find information about **local entry** and **cloud entry** in the **Snapshot.db**
- Given below is the snapshot for **cloud 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
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	0Bwvuwe_Xsk...	Test.pptx	1457605068	NULL	0	1	0	32451	36f5c2624d88...	0	file
2	0Bwvuwe_Xsk...	New folder	1457604731	NULL	0	0	0	NULL	NULL	0	folder
3	0Bwvuwe_Xsk...	1Scissors.png	1457604559	NULL	0	1	0	117969	2dbd1b6126e...	0	file
4	0Bwvuwe_Xsk...	E-mail.png	1457604124	NULL	0	1	0	8974	a41b5972b5a...	0	file
5	0Bwvuwe_Xsk...	Checklist.png	1457603144	NULL	0	1	0	89632	bd39052b999...	0	file
6	0Bwvuwe_Xsk...	Cd_Dvd_BluRay...	1457603107	NULL	0	1	0	97802	229cb0a1dbe...	0	file
7	0Bwvuwe_Xsk...	Battery.png	1457603101	NULL	0	1	0	5899	2dac1abd06d...	0	file
8	0Bwvuwe_Xsk...	Bookmark.png	1457603102	NULL	0	1	0	8807	5984e2ecec7...	0	file
9	0Bwvuwe_Xsk...	calender-1.png	1457603102	NULL	0	1	0	10740	c81298e79c1...	0	file
10	0Bwvuwe_Xsk...	Calendar.png	1249230084	NULL	0	1	0	77782	0209ae2637b...	0	file
11	0Bwvuwe_Xsk...	paintbrush_256....	1186597104	NULL	0	1	0	19440	3511ac4e9db...	0	file
12	0Bwvuwe_Xsk...	Flag.png	1248759670	NULL	0	1	0	20494	8e5b4b2ee66...	0	file
13	0Bwvuwe_Xsk...	1Clock.png	1249933660	NULL	0	1	0	122025	166e49cf60e0...	0	file
14	0Bwvuwe_Xsk...	Bar_Graph.png	1249231434	NULL	0	1	0	50883	2a7f5b0a1be...	0	file
15	0Bwvuwe_Xsk...	man-108.png	1413455363	NULL	0	1	0	47298	7746bbb1bd4...	0	file

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

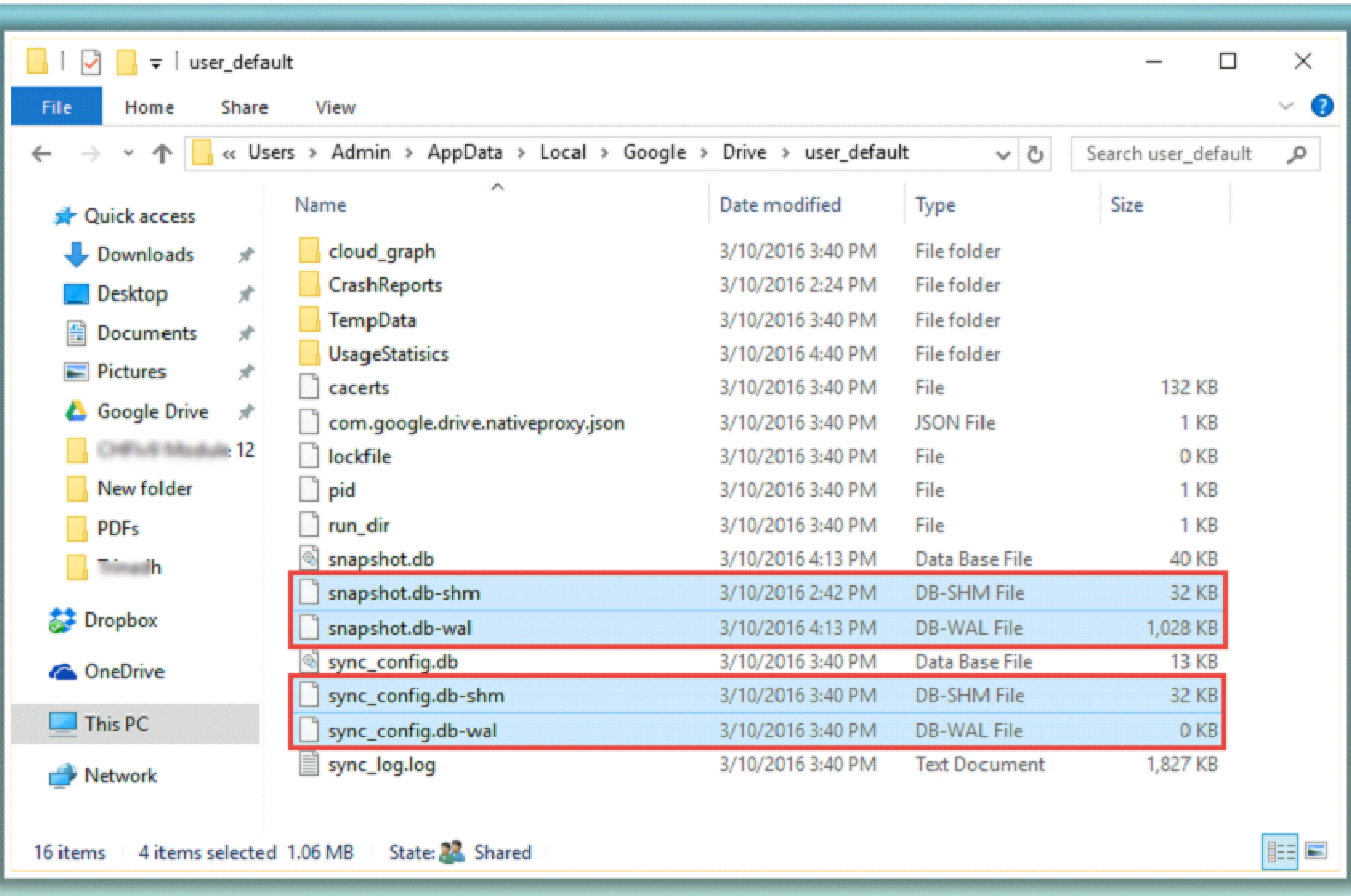


	inode_number	filename	modified	checksum	size	is_folder
	Filter	Filter	Filter	Filter	Filter	Filter
1	50665495808...	arrow-6.jpg	1456907909	687e8e9da31...	67885	0
2	50665495808...	basket-1.png	1456907909	c8b94df19ab6...	21366	0
3	50665495808...	Test.pptx	1457605068	36f5c2624d88...	32451	0
4	53480245575...	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	0209ae2637b...	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	5ee533ecdfd0...	17325	0
12	10977524091...	man-129.png	1413455378	51c322cb775...	57413	0
13	11258999068...	man-80.png	1413455392	0a0d096072d...	2972	0
14	12666373951...	man-127.png	1413455374	06917ab40f67...	35412	0
15	13792273858...	man-83.png	1413455396	10b5ba1ac96...	2186	0
16	15199648742...	man-84.png	1413455396	f062f503ad57...	2710	0

Name	Type
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_num...	
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)	

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

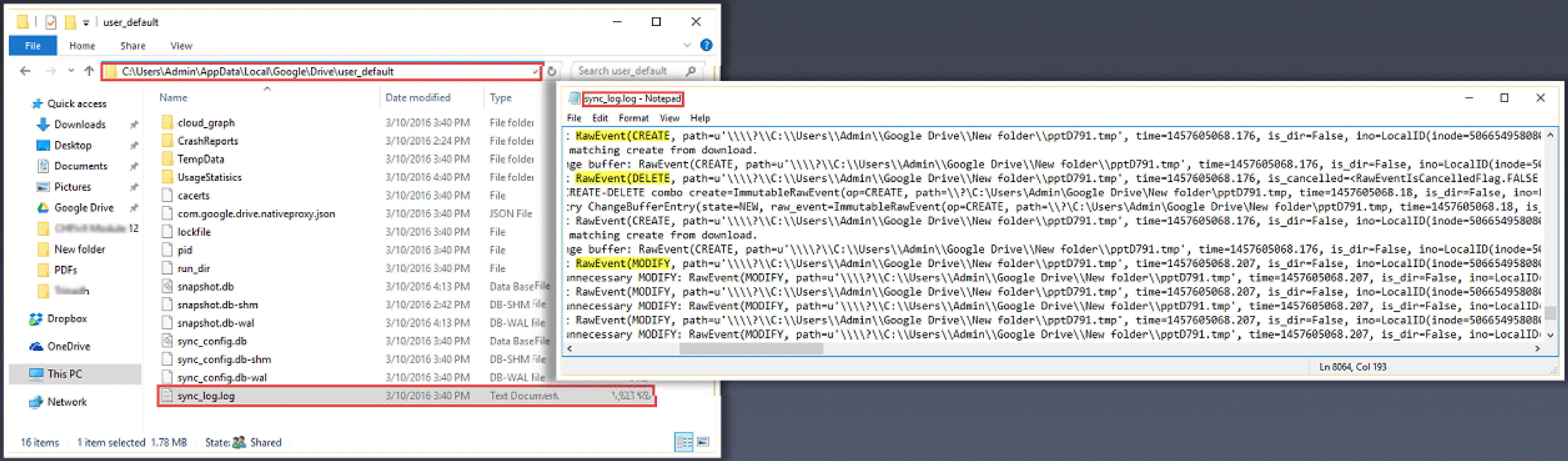


Name	Date modified	Type	Size
cloud_graph	3/10/2016 3:40 PM	File folder	
CrashReports	3/10/2016 2:24 PM	File folder	
TempData	3/10/2016 3:40 PM	File folder	
UsageStatisics	3/10/2016 4:40 PM	File folder	
cacerts	3/10/2016 3:40 PM	File	132 KB
com.google.drive.nativeproxy.json	3/10/2016 3:40 PM	JSON File	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

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



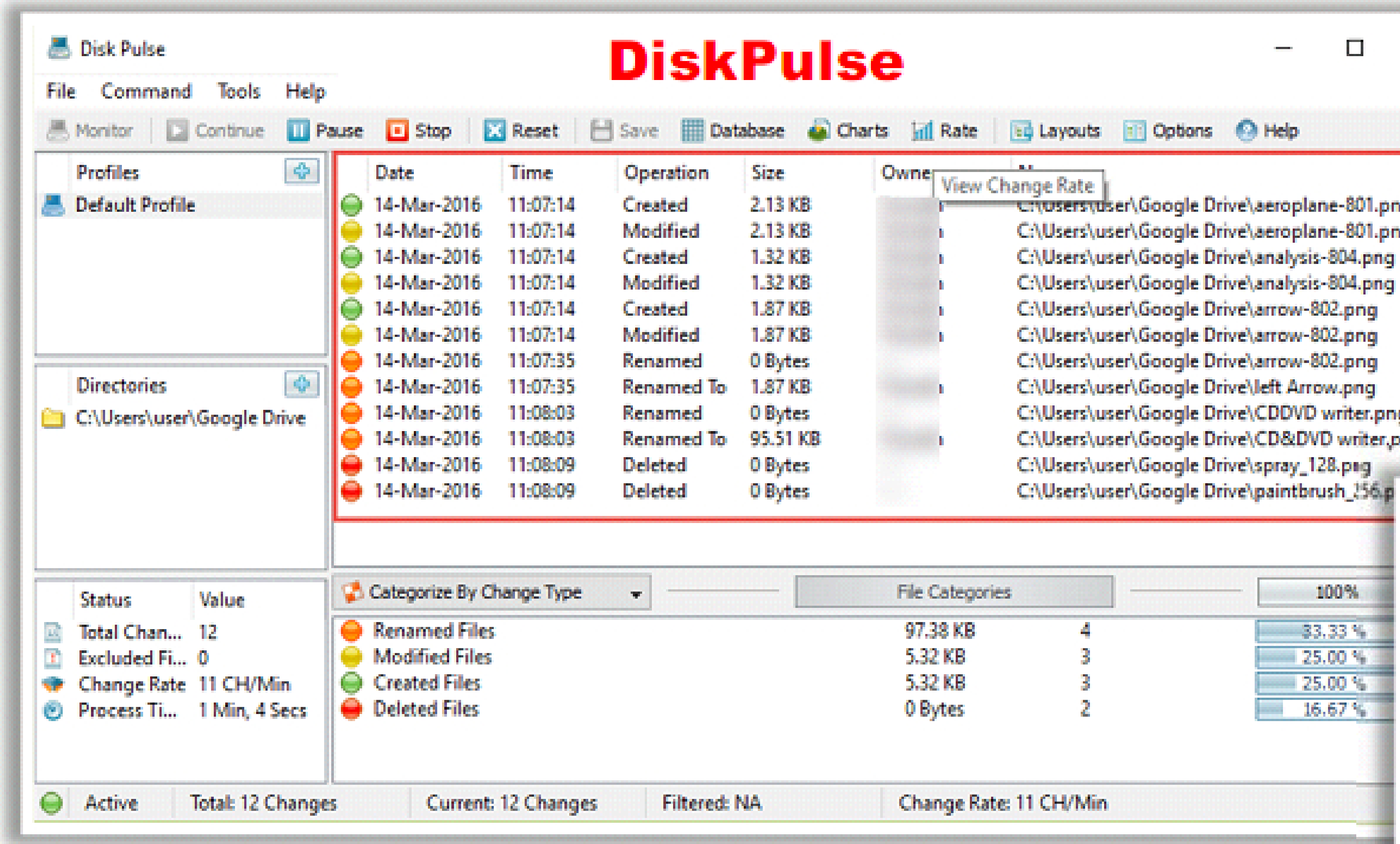
Name	Date modified	Type	
cloud_graph	3/10/2016 3:40 PM	File folde	
CrashReports	3/10/2016 2:24 PM	File folde	
TempData	3/10/2016 3:40 PM	File folde	
UsageStatisics	3/10/2016 4:40 PM	File folde	
cacerts	3/10/2016 3:40 PM	File	
com.google.drive.nativeproxy.json	3/10/2016 3:40 PM	JSON File	
lockfile	3/10/2016 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	1,923 KB

16 items 1 item selected 1.78 MB State: Shared

```
: RawEvent(CREATE, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\pptD791.tmp', time=1457605068.176, is_dir=False, ino=LocalID(inode=50665495808
 matching create from download.
ıge buffer: RawEvent(CREATE, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\pptD791.tmp', time=1457605068.176, is_dir=False, ino=LocalID(inode=5
: RawEvent(DELETE, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\pptD791.tmp', time=1457605068.176, is_cancelled=<RawEventIsCancelledFlag.FALSE
:REATE-DELETE combo create=ImmutableRawEvent(op=CREATE, path=\\?\C:\Users\Admin\Google Drive\New folder\pptD791.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\pptD791.tmp, time=1457605068.18, is_
: RawEvent(CREATE, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\pptD791.tmp', time=1457605068.176, is_dir=False, ino=LocalID(inode=50665495808
 matching create from download.
ıge buffer: RawEvent(CREATE, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\pptD791.tmp', time=1457605068.176, is_dir=False, ino=LocalID(inode=5
: RawEvent(MODIFY, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\pptD791.tmp', time=1457605068.207, is_dir=False, ino=LocalID(inode=50665495808
ınnecessary MODIFY: RawEvent(MODIFY, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\pptD791.tmp', time=1457605068.207, is_dir=False, ino=LocalID
: RawEvent(MODIFY, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\pptD791.tmp', time=1457605068.207, is_dir=False, ino=LocalID(inode=50665495808
ınnecessary MODIFY: RawEvent(MODIFY, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\pptD791.tmp', time=1457605068.207, is_dir=False, ino=LocalID
: RawEvent(MODIFY, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\pptD791.tmp', time=1457605068.207, is_dir=False, ino=LocalID(inode=50665495808
ınnecessary MODIFY: RawEvent(MODIFY, path=u'\\\\?\\C:\\Users\\Admin\\Google Drive\\New folder\\pptD791.tmp', time=1457605068.207, is_dir=False, ino=LocalID
```

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%

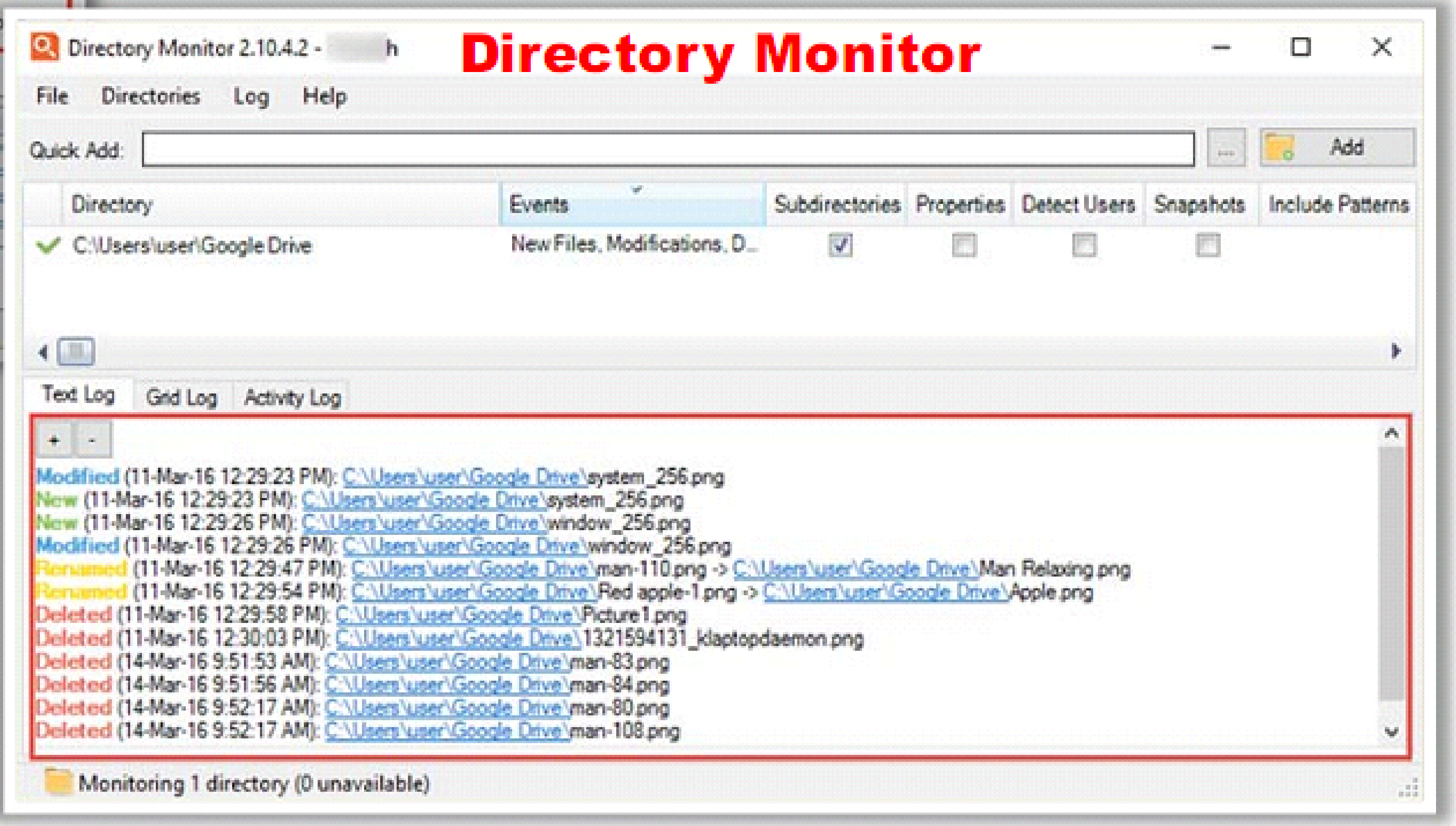
	Date	Time	Operation	Size	Owne	N
●	14-Mar-2016	11:07:14	Created	2.13 KB	[redacted]	C:\Users\user\Google Drive\aeroplane-801.png
●	14-Mar-2016	11:07:14	Modified	2.13 KB	[redacted]	C:\Users\user\Google Drive\aeroplane-801.png
●	14-Mar-2016	11:07:14	Created	1.32 KB	[redacted]	C:\Users\user\Google Drive\analysis-804.png
●	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	[redacted]	C:\Users\user\Google Drive\spray_128.png
●	14-Mar-2016	11:08:09	Deleted	0 Bytes	[redacted]	C:\Users\user\Google Drive\paintbrush_256.p

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

●	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 Monitor

Directory Monitor 2.10.4.2 - [redacted]h
File Directories Log Help
Quick Add:
...
Add
Text Log
Grid Log
Activity Log
+
-

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)

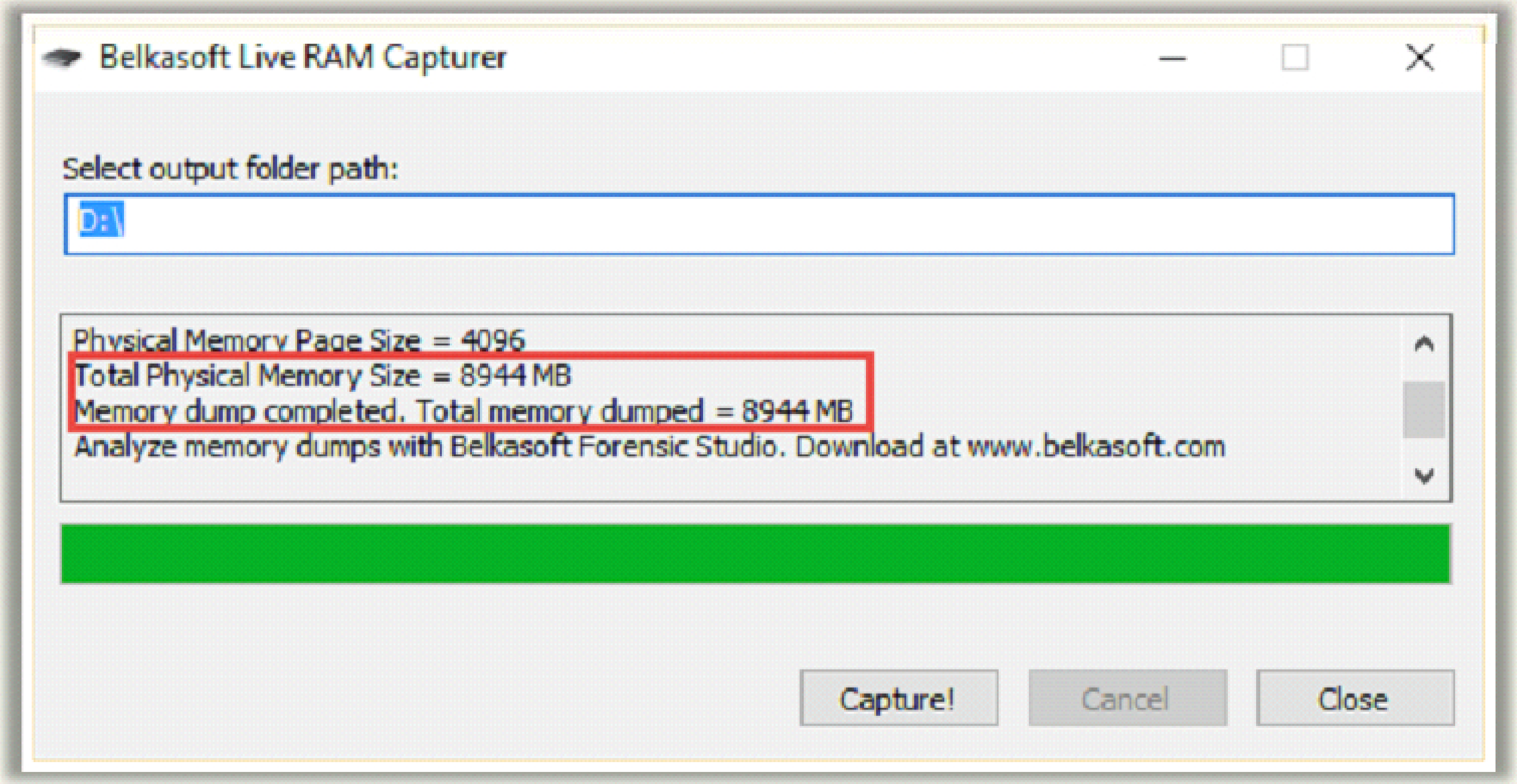
https://directorymonitor.com

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



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

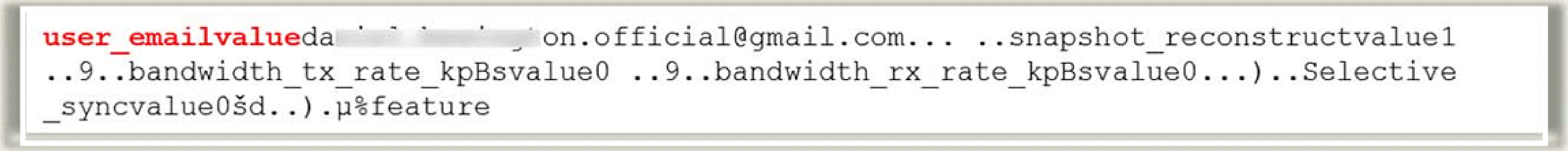
Artifacts Left by Google Drive Client on Windows (Cont'd)

HxD:

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

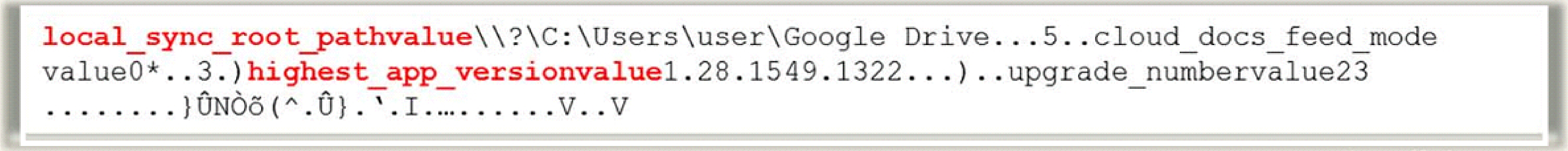
Given below are the strings that **assists** you to find out information of evidentiary value (such as user email ID, version number, local_sync_folder_path, snapshot.db and sync_config.db paths):

- **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



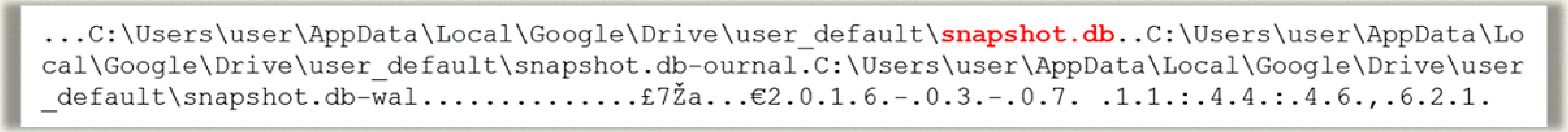
```
local_sync_root_pathvalue\\?\C:\Users\user\Google Drive...5..cloud_docs_feed_mode
value0*..3.)highest_app_versionvalue1.28.1549.1322...)..upgrade_numbervalue23
........}ÛNÒõ(^.Û}.`.I.…......V..V
```

https://mh-nexus.de

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

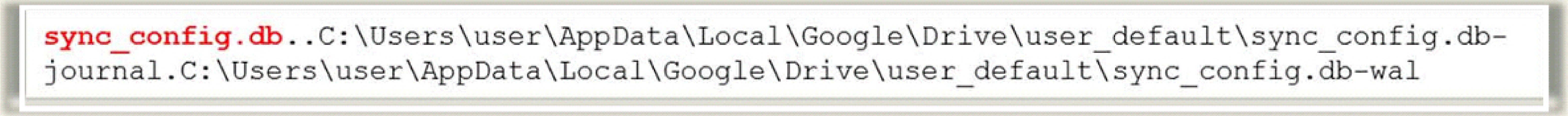
Artifacts Left by Google Drive Client on Windows (Cont'd)

- **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

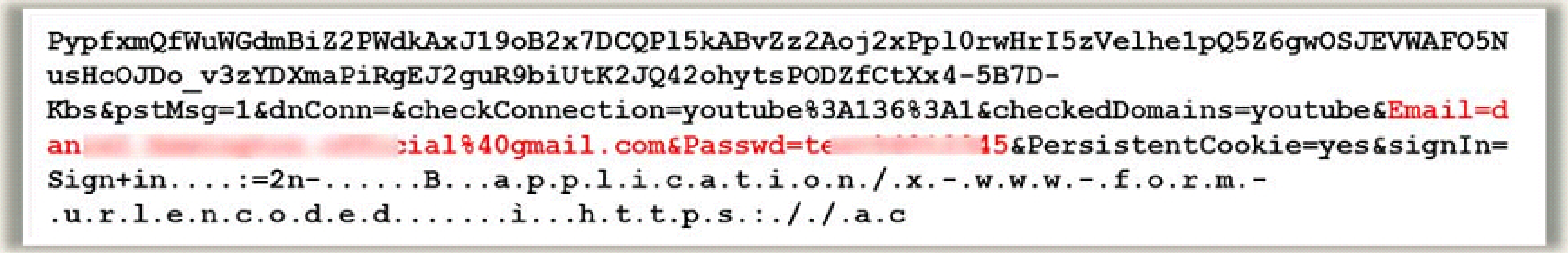


```
sync_config.db..C:\Users\user\AppData\Local\Google\Drive\user_default\sync_config.db-
journal.C:\Users\user\AppData\Local\Google\Drive\user_default\sync_config.db-wal
```

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

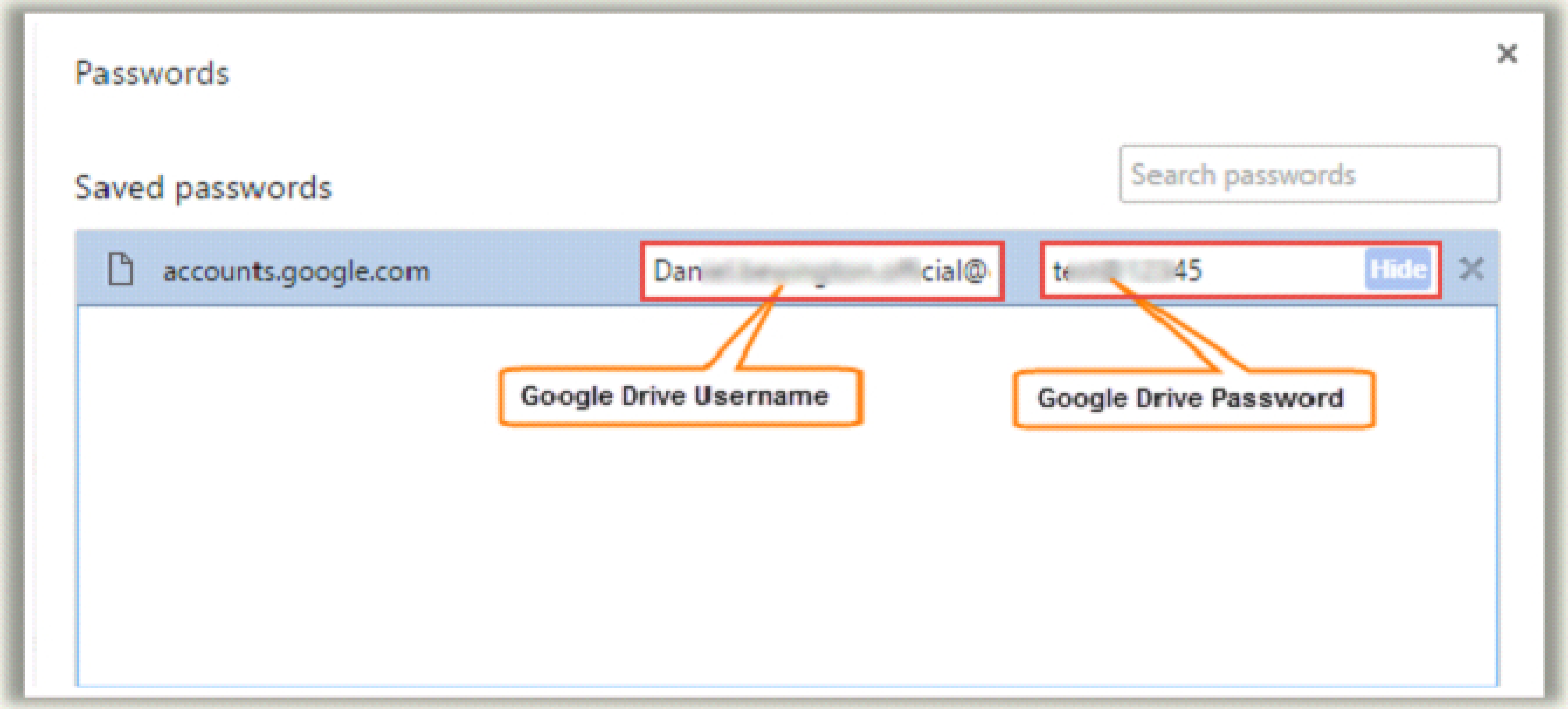
In case of Web-based Google Drive, you can find the **username** and **password** in clear from **RAM dump** using strings:

- "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**



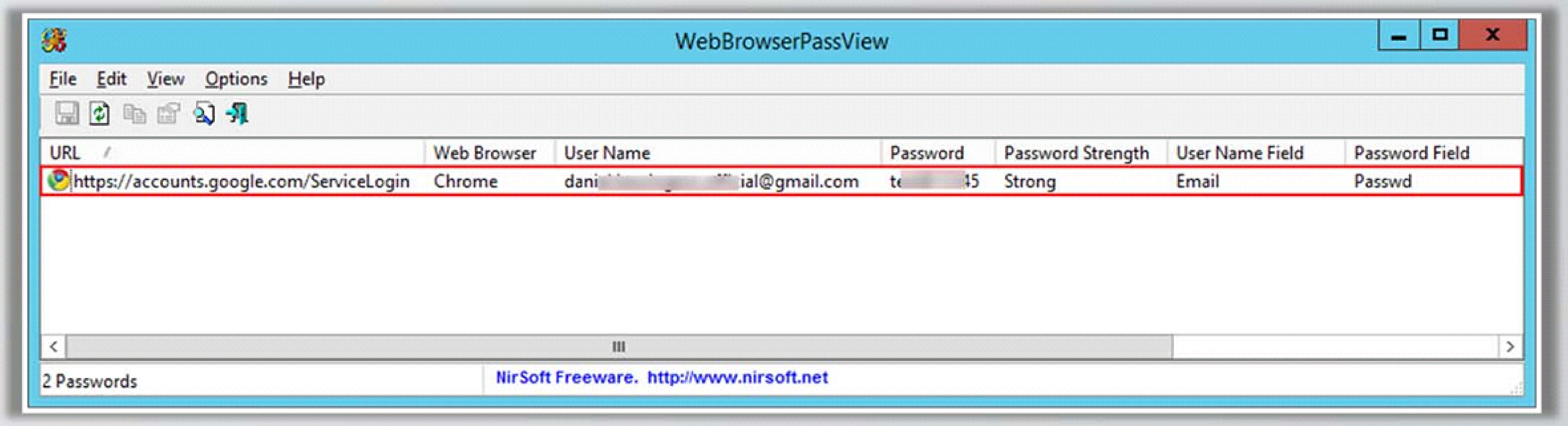
accounts.google.com Dan[redacted]cial@ te[redacted]45

Google Drive Username

Google Drive Password

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



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

2 Passwords

NirSoft Freeware. http://www.nirsoft.net

http://www.nirsoft.net

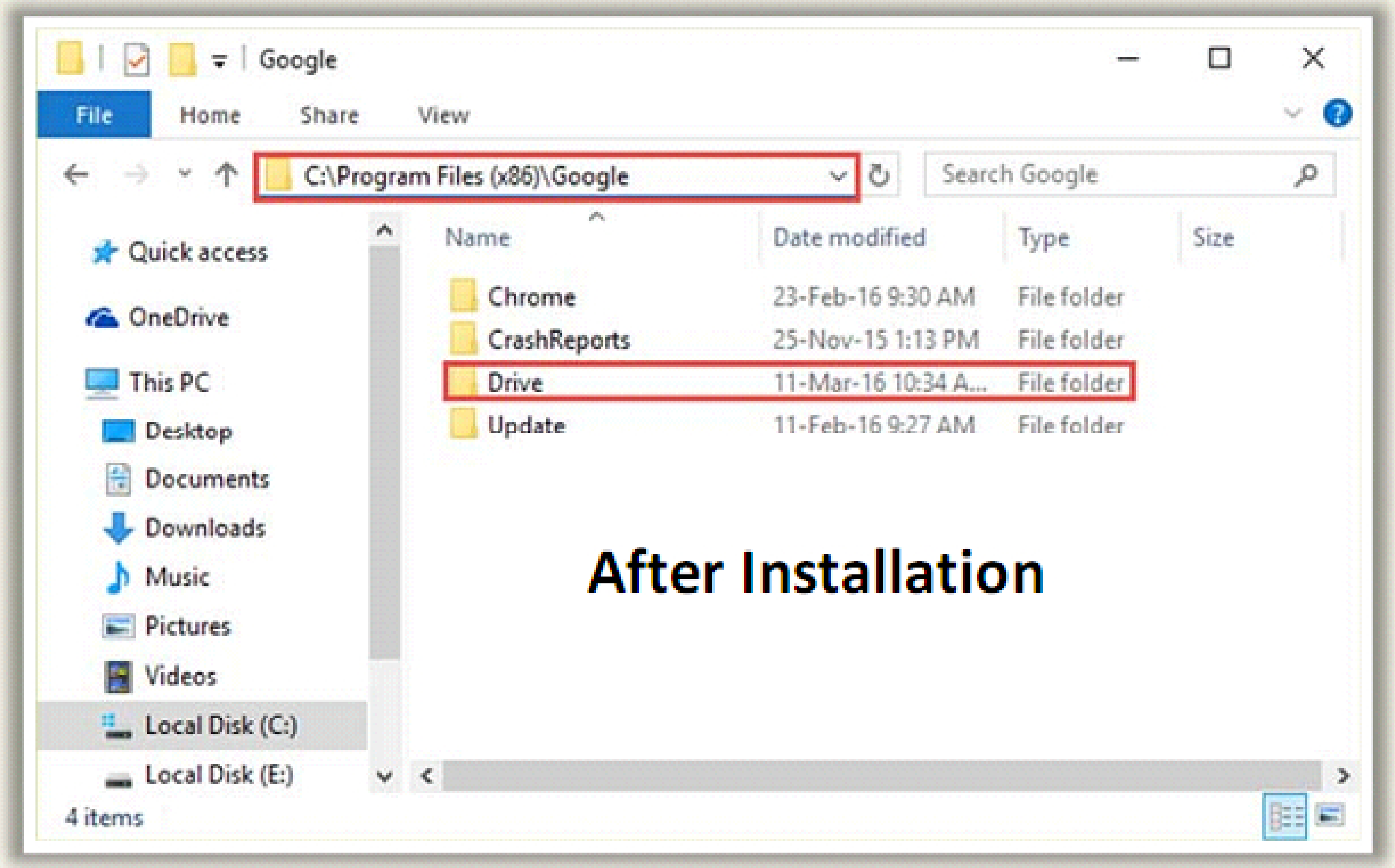
Artifacts Left by Google Drive Client on Windows (Cont'd)

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:

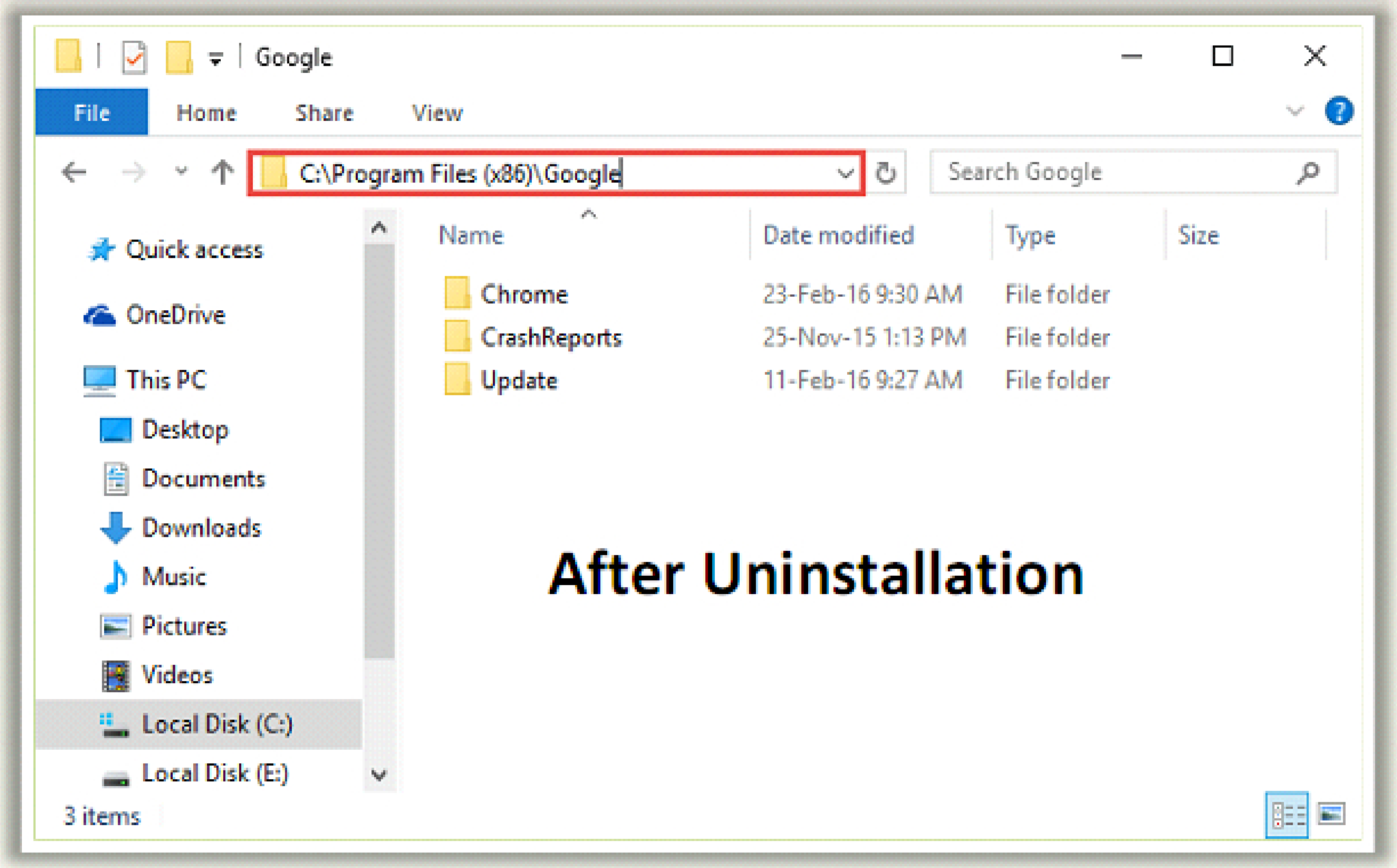
- Registry keys of recent files
- LiNK files
- Browser history and cache
- Thumbnails
- Registry Point/Volume Shadow Copies
- Pagefile.sys
- Hiberfil.sys



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

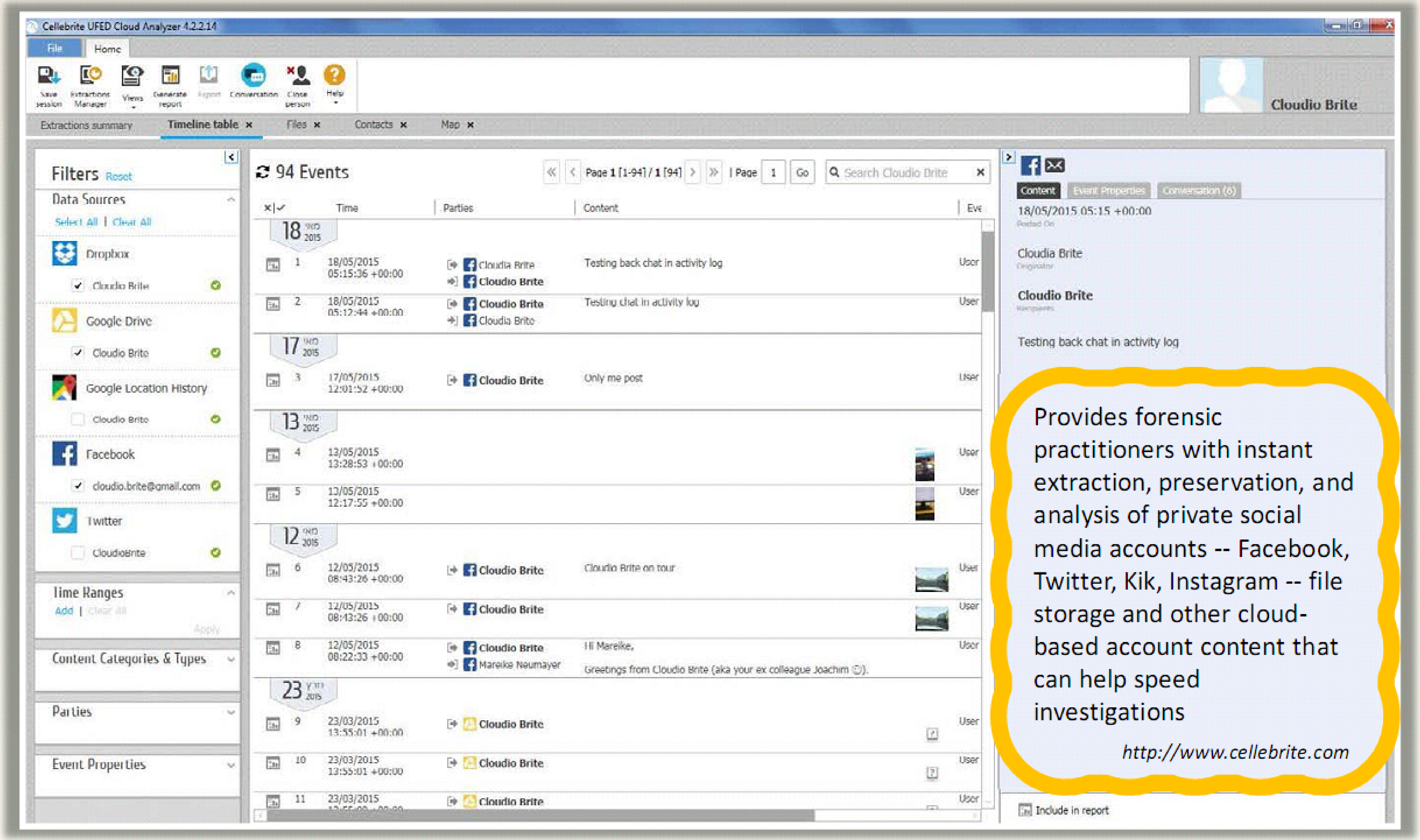


C:\Program Files (x86)\Google

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

Cloud Forensics Tools:
UFED Cloud Analyzer



94 Events

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

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

Cloudia Brite
Originator

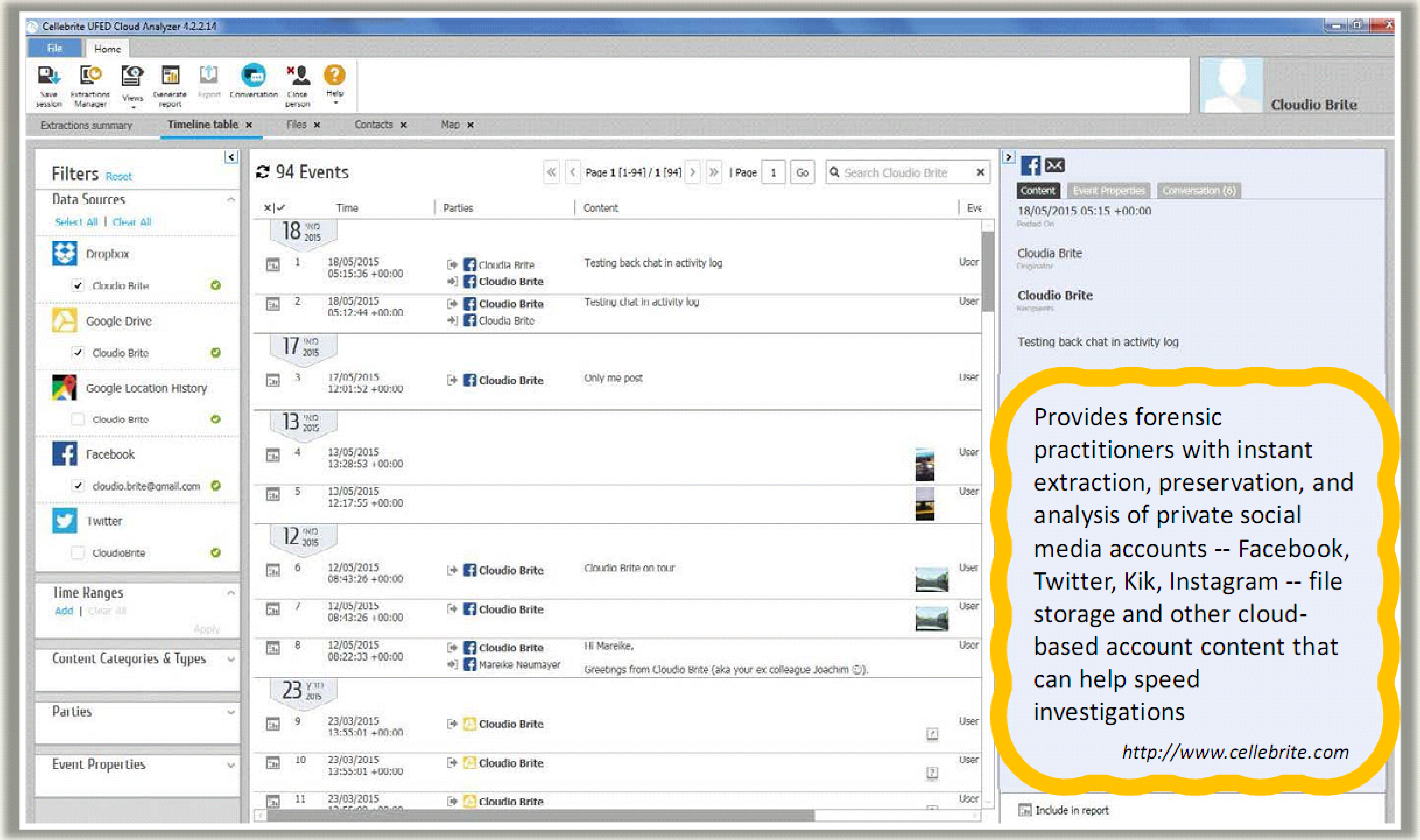
Cloudio Brite
Recipients

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

Cloud Forensics Tools: UFED Cloud Analyzer



94 Events

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

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

Cloudia Brite
Originator

Cloudio Brite
Recipients

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