



Collecting & Mining Evidence from the Cloud

Don Vilfer, JD
916-883-2020

Don@DigitalEvidenceVentures.com

www.DigitalEvidenceVentures.com

About Us

Computer Forensics

Cell Phone Forensics and Location Analysis

Fraud Investigation

Employment Investigation

Why Consider the Cloud?

- Many cloud locations may have information that will advance your case.
- Even if a party used a laptop or desktop, all of the data may not reside there.
- A non-company cloud resource may be used to exfiltrate data.
- The cloud may have data when spoliation has occurred on devices.

What is Cloud Forensics?

- A blend of cloud computing and digital forensics.
- The evidence in the cloud can be found anywhere, there is no specific location for cloud data.
- Cloud forensics is the collection of data from a cloud environment in a manner that allows the data to be used as evidence.
- Could involve the investigation of virtual and physical servers, networks, storage devices, applications, and more.



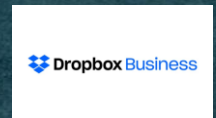
Cloud Examples?

- Some of the more popular cloud storage providers include:

- Google
- Microsoft 365
- Dropbox
- Linode
- Druva Data Resiliency Cloud
- OneDrive
- Amazon
- Social Media



amazon drive



Microsoft 365
Business



What Is Digital Forensics?

Digital forensics is a branch of **forensic** science encompassing the recovery and investigation of material found in **digital** devices, often in relation to **computer** crime. --Wikipedia



Examples of Cloud evidence

- Photos stored in iCloud.
- Spreadsheets from SharePoint.
- Documents uploaded to Google Drive.
- Comments made on Facebook.
- Office365 email.



FORENSIC IMAGE

- The creation of a Forensic Duplicate of the storage media.
- FRE Section 1003: a duplicate is admissible to the same extent as the original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original.



CHARACTERISTICS OF A FORENSIC IMAGE

- Hash Value (Digital Fingerprint)
- Data cannot be changed
- Includes Unallocated Space, Drive Freespace and File Slack
- Difference from Ghost
- Acceptable in court as Best Evidence



What is Metadata?

- Metadata provides data or information about other data.
- It is the fine detail that describe characteristics of a certain thing.
- Metadata is just as valuable if not more so than data.
- Think about the What, When, Where, Who, How, Which and Why—these are the types of details metadata may provide about data.



But How Do We Acquire Cloud Data In A Forensically Sound Manner?

- Cannot just image the computer
- Cannot usually remotely image the server
- A simple download may change metadata
- Security features may prevent access (2fa)
- Complex cloud features may involve complex APIs.



THE USUAL RULES OF EVIDENCE STILL APPLY

- Chain of Custody—must be able to account for the location of the evidence from the moment it was collected.
- Authentication—computer evidence is considered “writings and recordings” under the Rules of Evidence and must be authenticated to be admissible.
- Validation—is it really the same? (Hash files)

Authenticating Digital Evidence

- Federal Rules of Evidence added two categories of self-authenticating digital records:
- **Certified Records Generated by an Electronic Process or System [902(13)]** — A record generated by an electronic process or system that produces an accurate result, as shown by a **certification of a qualified person** that complies with the certification requirements of Rule 902(11) or (12).
- **Certified Data Copied from an Electronic Device, Storage Medium, or File [902(14)]** — Data copied from an electronic device, storage medium or file, if **authenticated by a process of digital identification, as shown by a certification of a qualified person** that complies with the certification requirements of Rule 902(11) or (12).

Authenticating Digital Evidence

- But, even with a question of authenticity, evidence might still be admitted.
- “the court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so.” The possibility of alteration “does not and cannot be the basis for excluding ESI as unauthenticated as a matter of course, any more that it can be the rationale for excluding paper documents.” *United States v. Safavian*, 435 F. Supp. 2d 36, 38 (D.D.C. 2006).



RECENT CASE LAW

State v. Kolanowski, (Wash: Court of Appeals, January 30, 2017). In a case involving the failure to authenticate social media evidence, a criminal defendant unsuccessfully sought to admit a screenshot of Facebook evidence that he maintained would have served as critical impeachment of the prosecutions' main witness. The State successfully argued the screenshot lacked foundation. Metadata that could have been obtained during the collection was not obtained—a simple screenshot did not suffice.



Finding Relevant Cloud Sources

- Forensic review of the computers.
- Interview of subject, IT staff or business owner.
- Interrogatories and deposition.
- Network traffic analysis/log files.



Case Study: Artifacts on the Computer

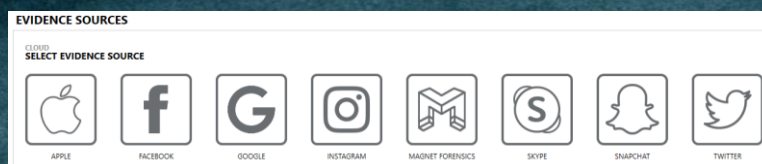
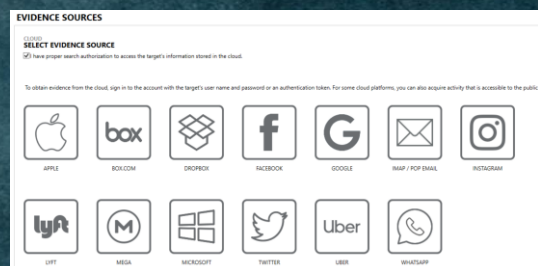
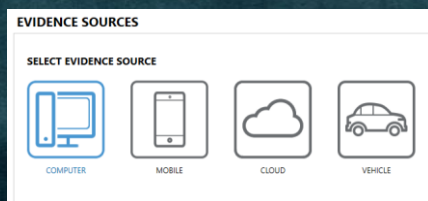
ALL EVIDENCE	662,484
REFINED RESULTS	5,671
Classified URLs	69
Cloud Services URLs	2,436
Credit Cards	1
Facebook URLs	62
Google Analytics First Visit Cookies	16
Google Analytics Referral Cookies	8
Google Analytics Session Cookies	2
Google Analytics URLs	1
Google Searches	944
Identifiers - Device	254
Identifiers - People	104
Locally Accessed Files and Folders	246
Malware/Phishing URLs	3
Parsed Search Queries	361
Passwords and Tokens	65
Rebuilt Desktops - Windows	2
Rebuilt Webpages	496
Social Media URLs	23
Tax Site URLs	1
Web Chat URLs	577

EVIDENCE (2,436)					
Site...	URL	Artifact type	Artifact	Artifact ID	
OneDrive	https://onedrive.live.com	Cloud Services URLs	Potential Browser Activity	82	
Google Drive	https://drive.google.com/file/d/1vuefYolUcobbhd7...	Cloud Services URLs	Potential Browser Activity	454	
Google Drive	https://drive.google.com/drive/settings	Cloud Services URLs	Potential Browser Activity	483	
Google Drive	http://drive.google.com/intents/opensdrivedoc	Cloud Services URLs	Potential Browser Activity	486	
Google Drive	https://drive.google.com/	Cloud Services URLs	Potential Browser Activity	514	
OneDrive	https://onedrive.live.com/default offline_access ope...	Cloud Services URLs	Potential Browser Activity	657	
OneDrive	https://onedrive.live.com/default offline_access ope...	Cloud Services URLs	Potential Browser Activity	661	
Google Drive	https://drive.google.com/drive/folders/17_X9yiwG...	Cloud Services URLs	Potential Browser Activity	742	
Google Drive	https://drive.google.com/drive/folders/1-OQK2vFvG...	Cloud Services URLs	Potential Browser Activity	886	
Google Drive	https://drive.google.com/drive/folders/1I_g22D2usa...	Cloud Services URLs	Potential Browser Activity	895	
Google Drive	https://drive.google.com/drive/folders/1ewy2bVIGq...	Cloud Services URLs	Potential Browser Activity	885	
Google Drive	https://drive.google.com/drive/folders/18CAR573p2...	Cloud Services URLs	Potential Browser Activity	891	

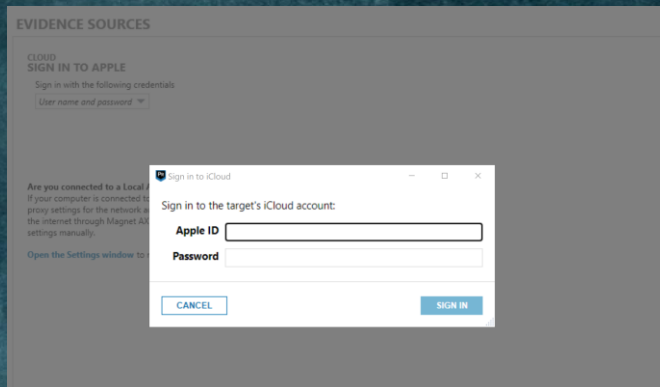
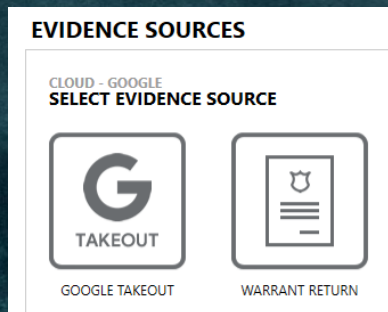
DETAILS	
ARTIFACT INFORMATION	
Site Name	Google Drive
URL	https://drive.google.com/drive/folders/1-OQK2vFvGuj9j3N9VPC8cKx8u85WDgrod7E1ezwbaohapl-gM_ups3hDHeRLwE0homNHhQL
Artifact type	Cloud Services URLs
Item ID	900
Original artifact	Potential Browser Activity



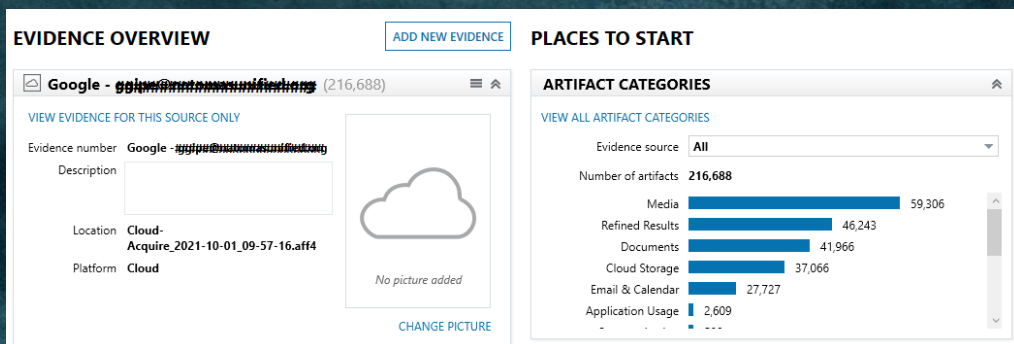
Acquiring From the Cloud



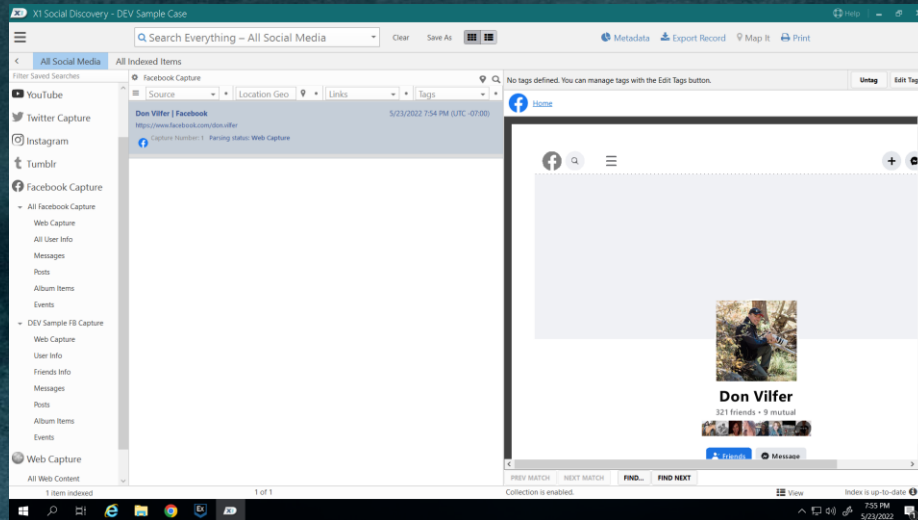
Credentials or Warrant Required



Results!



Social Media Preservation



Questions?

DON VILFER, JD
916-883-2020

DON@DIGITALEVIDENCEVENTURES.COM

