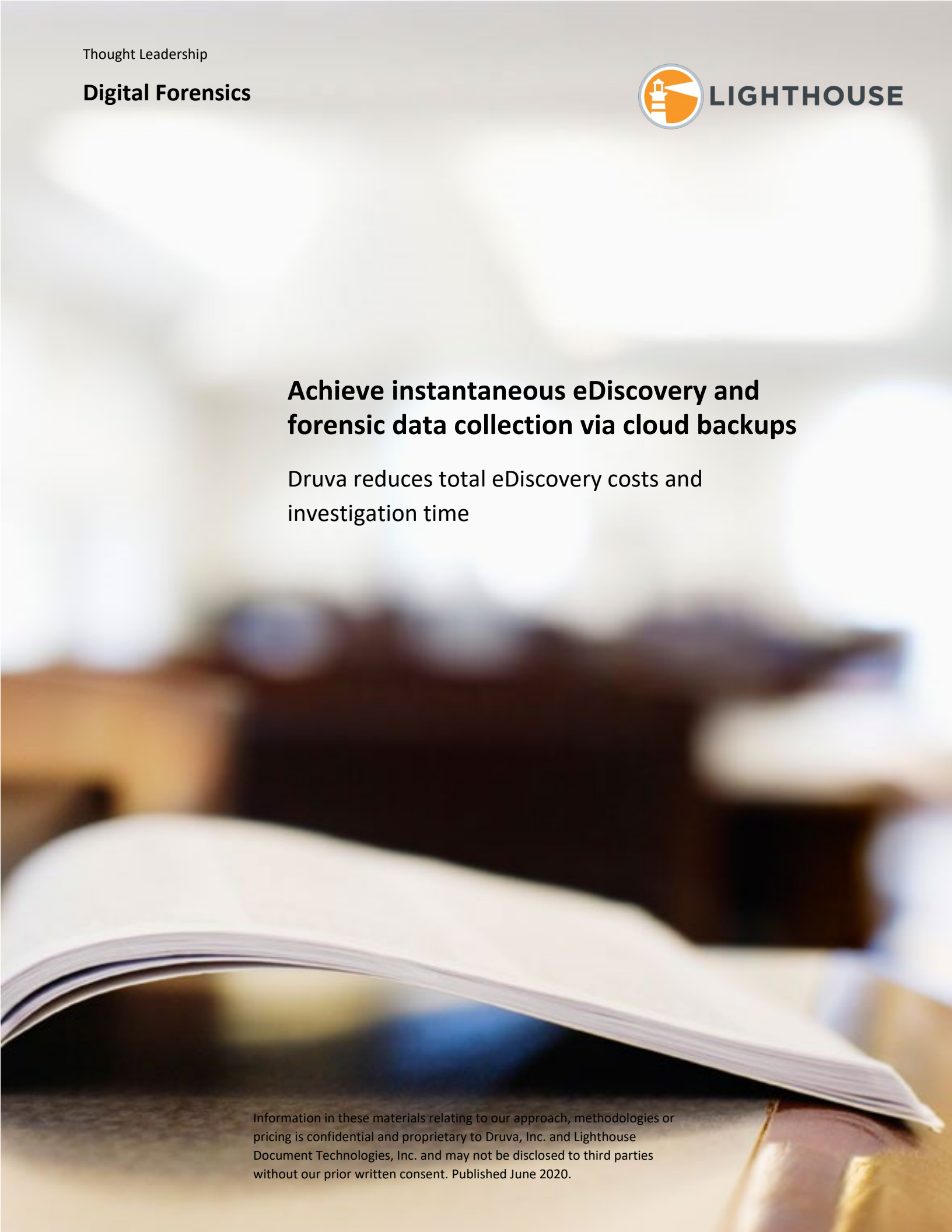
Thought Leadership

Digital Forensics

LIGHTHOUSE

Achieve instantaneous eDiscovery and forensic data collection via cloud backups

Druva reduces total eDiscovery costs and investigation time



Executive Summary

It is a common perception that cloud-based backup copies of endpoints such as laptops are little more than glorified document repositories with minimal forensic significance. We simply download their contents and pass any common user-created file types straight on to our client's favorite eDiscovery platform for review. However, Druva is giving forensic technologists a rich new source of digital artifacts that can be processed using products like OpenText's Encase, Magnet Forensics' Axiom, and Cellebrite's BlackLight software for cases requiring forensic analysis.

Druva's enterprise cloud backup and data protection service preserves and provides a large majority of the forensic artifacts needed by digital forensic investigators in addition to providing a rich version-ed history of files present on the device under investigation from the cloud. Druva eliminates the need for a laptop to be turned in for a forensic investigator to make a copy of the hard drive. Forensic teams can also achieve instantaneous access to the data via the cloud, ultimately reducing eDiscovery data collection time and minimizing the overall cost of the investigation.

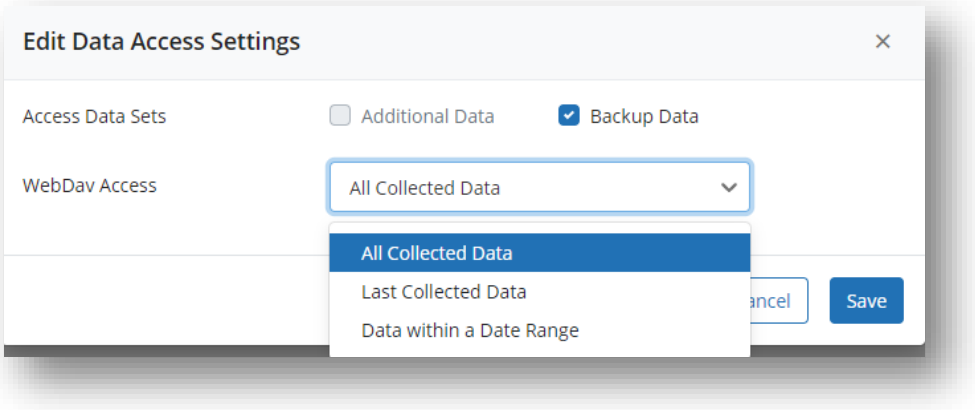
Druva Backup and Restore

Druva asked our Lighthouse Digital's Forensics team to do a feasibility study on whether data backed-up by their service was a viable source of defensible artifacts suitable for forensic analysis. The answer is affirmative.

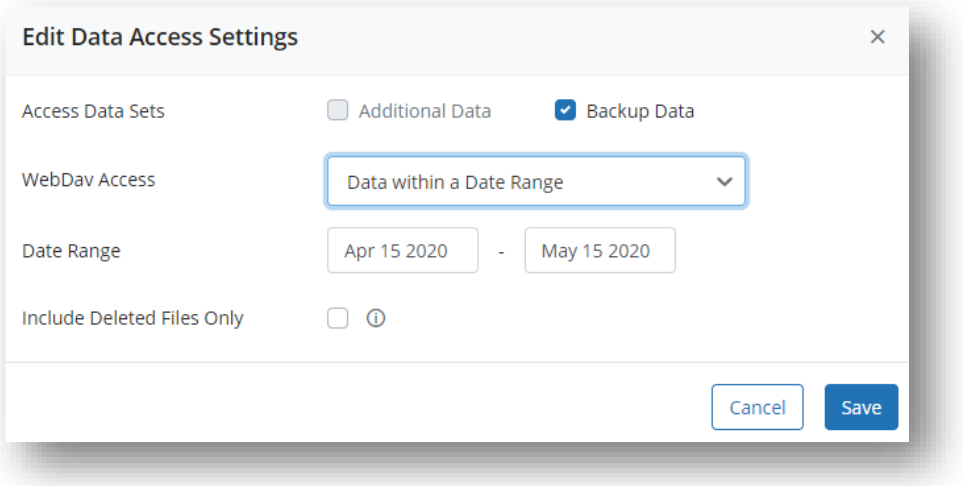
To start, we created a list of the most common Windows and MacOS artifacts exposed and consumed for analysis by forensic analysis tools such as EnCase, Axiom and BlackLight. We also asked Druva to set up several test systems for us to examine, one being a Mac and the other a PC. Next, Lighthouse had Druva perform a series of tasks in order to create a suitable number of artifacts for our tools to decode. We then created full E01 images of each system's hard drive and downloaded the corresponding Druva backup set for each machine. This gave us the requisite information we needed to perform a detailed comparison between the backup datasets and the original source material.

Druva gives you three flavors of restored data:

- *Most Recent - Latest copy of backup*
- *Versioned - All copies of backup or within a date range*
- 'Deleted Only' within a *date range*



If you simply want the most recent backup set, then Druva can produce this without any versioning modifications to the file names. Moreover, if you want to recover only those files that have been deleted off the target computer, then there is a recovery mode for that as well.



Versioned restores have data appended to folder/file names, so that multiple iterations of identically named objects can reside in the same location:

Name

- SysWOW64,v1
- Tasks,v1
- TextInput,v1
- twain_32,v1
- UpdateAssistant,v1
- UpdateAssistantV2,v1
- Vss,v1
- WaaS,v14
- Web,v1
- WinSxS,v1
- bfsvc,v1.exe
- bfsvc,v14.exe
- bootstat,v1.dat
- bootstat,v10.dat
- bootstat,v14.dat
- bootstat,v19.dat
- bootstat,v25.dat
- bootstat,v31.dat
- comsetup,v1.log
- comsetup,v14.log

This type of restore is useful for quickly identifying historical changes to specific files, which is never available to investigators from the image of a hard disk. While the versioned files are extremely valuable in certain types of investigations, the current set of forensic investigative tools such as EnCase / Axiom / BlackLight are not able to process them, since the versioning details mask the original artifact's name and location that the software needs to identify it.

In line with good defensibility practices, all restore modes produce a document in a CSV format that contains key metadata, including original file names, paths, creation/last accessed/last modified dates/times, SHA1 hash values, file sizes, assigned owner, content type, etc.

C	D	E	F	G	H	I	J	K
Display Name	Last Modified Timestamp (GMT)	Last Accessed Timestamp (GMT)	Creation Timestamp (GMT)	Checksum(SHA1)	File Path	File Name	Owner	Content Type
bootstat,v1.dat	2019-08-05 23:38:40	2019-08-05 23:33:09	2019-08-05 23:33:09	7b82767a5ee88a3163db891c6fc4f7725e00cafa	C:\Windows\bootstat.dat	bootstat.dat	NT AUTHORITY\SYSTEM	application/octet-stream
bootstat,v10.dat	2019-08-14 03:11:22	2019-08-05 23:33:09	2019-08-05 23:33:09	0ff15e9e98f4555cc66c43bf37040f5f65f874a8	C:\Windows\bootstat.dat	bootstat.dat	NT AUTHORITY\SYSTEM	application/octet-stream
bootstat,v14.dat	2019-10-10 04:12:37	2019-10-10 04:12:37	2019-10-10 02:07:58	984a4af26b6d1869c93f3c28242982bfb1c44759	C:\Windows\bootstat.dat	bootstat.dat	NT AUTHORITY\SYSTEM	application/octet-stream
bootstat,v19.dat	2019-10-14 20:16:45	2019-10-14 20:16:45	2019-10-10 02:07:58	cbe5584ce6b2f81693a8b6f040b748270ea7bd79	C:\Windows\bootstat.dat	bootstat.dat	NT AUTHORITY\SYSTEM	application/octet-stream
bootstat,v25.dat	2019-10-21 03:36:48	2019-10-21 03:36:48	2019-10-10 02:07:58	4c16188049018bb1374e84951f774f273a85ca08	C:\Windows\bootstat.dat	bootstat.dat	NT AUTHORITY\SYSTEM	application/octet-stream
bootstat,v31.dat	2019-10-27 15:56:10	2019-10-27 15:56:10	2019-10-10 02:07:58	275a62bad36ca40325bae04bd11135cb5c61ff1f	C:\Windows\bootstat.dat	bootstat.dat	NT AUTHORITY\SYSTEM	application/octet-stream

We can plug this metadata into a free app like Bulk Rename utility to selectively rename, *en masse*, the versioning periods that are relevant to our customers' cases. However, if one simply wants the most recent backup set, then Druva can produce this without any versioning modifications to the file names. Moreover, if we want to recover only those files that have been deleted off the target computer, then there is a recovery mode for that as well. We found this to be interesting as in some types of investigations, it helps identify the deleted artifacts very quickly, while recovering the complete file, versus just fragments of a file.


A19

Design of Experiment

Our Lighthouse Digital Forensics team took the restored data from the two test systems and laid them each out on blank hard drives, mimicking the path structures of the original media. We then created L01 logical images and used these as the source data for our analysis using EnCase, Axiom and BlackLight. The appendix to this case study illustrates the wide array of artifacts pulled from the restores and rendered suitable for review. Here is a partial list of the artifacts recovered:

Windows OS

- Detailed metadata listings, including SHA1 hash values, for Mac and PC file systems
- Windows and Mac Internet browsing history
- Windows Registry files
- Windows Event logs
- Windows Link and URL files
- Windows Recycle Bin artifacts

Mac OS

- Mac PLIST files
- Full contents of Mac /var/log/* and /var/db/* folders
- Files under /Library/Preference/* and /Library/Logs/* Mac Users folders

Druva will make our test images and corresponding case files available upon request.

Real-World Findings

In summary, Druva's fast and secure enterprise cloud backup are replete with forensically viable information. Although we do not get a traditional universe of artifact data with cloud-based backups as we would with a physical bit stream image of a hard drive, the artifacts that Druva captures along with the version tracking features (unique to Druva) provide a high-quality historical picture of user behavior on par or better than what we would get by examining the physical image alone. This approach provides a unique added perspective for forensic investigations.

The data captured by Druva not only enhances forensic investigations, but also helps accelerate the overall process. With instantaneous access to the data for examination vs. the traditional method of eDiscovery data collection (i.e. handing over a laptop to the forensic investigator to image the system), forensic teams can drive down the overall investigation time and cost of the investigation.

Our Lighthouse team put these unique features to the test on a recent theft of intellectual property matter. Our client discovered months earlier that an employee was blatantly creating sensitive documents for a competitor. The company initiated a series of discreet backups over the course of the investigation, unbeknownst to the subject, which clearly showed subject authorship, unauthorized transferal, and subsequent deletion of confidential materials to mask the illegal activity. We even found hard evidence of the subject visiting our client's competitor's facilities overseas, complete with GPS coordinates of the subject's foreign travels. Most of this evidence was no longer present on the subject's work computers by the time law enforcement became involved and the drives were imaged after the fact. Druva's expanded enterprise cloud backup approach of supplying remotely available, on-demand logical backups that capture forensic artifact information on a continual basis at the touch of a button, creates a serious use case for forensic examinations. Druva's enterprise cloud backup becomes a compelling data source to include in any investigation to corroborate findings and potentially uncover "smoking-gun" evidence.

Start reducing data collection time and costs, visit: http://druva.com/ediscovery

Appendix

Artifacts verified in Druva Backups.

Windows OS

Type	Attribute/File	Prominent Use
Full file listing to include	File Name	eDiscovery
	File Extension	eDiscovery
	Logical Size	eDiscovery
	Created date / time	eDiscovery
	Last Accessed date / time	eDiscovery
	Last Written (or Modified) date / time	eDiscovery
	Full path of the file / folder	eDiscovery
	An indicator if the item is a file or folder object	eDiscovery
	MD5 (or SHA) hash value for files	eDiscovery
File and Directories	All Registry (*.reg | *.dat | SAM | SECURITY | SOFTWARE | SYSTEM) files.	Forensics
	All Link (*.lnk) files	eDiscovery
	All Event (*.evt | *.evtx) logs	eDiscovery
	All URL (*.url) files	eDiscovery
	All Jump Lists (*.automaticDestinations-ms | *.customDestinations-ms) files	Forensics
	All files located beneath the following path: \Windows\Prefetch*	Forensics
	Recycle Bin (INFO2 | $I*) files	Forensics
	Cache (Amcache.hve | RecentFileCache.bcf) files	Forensics
	Setupapi (Setupapi*.*) logs	Forensics
	Desktop.ini files	Forensics
Microsoft Edge Browser History	\Users*\AppData\Local\MicrosoftEdge*	Forensics
	\Users*\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe*	Forensics
Internet Explorer Browser History	\Users*\AppData\Local\Microsoft\Internet Explorer*	Forensics
	\Users*\AppData\LocalLow\Microsoft\Internet Explorer*	Forensics
	\Users*\AppData\Local\Microsoft\Windows*	Forensics
Google Chrome Browser History	\Users*\AppData\Local\Google\Chrome*	Forensics
Mozilla Firefox Browser History	\Users*\AppData\Local\Mozilla\Firefox*	Forensics
	\Users*\AppData\Roaming\Mozilla\Firefox*	Forensics

* Additional app related artifacts could be collected from their respective app folder

Mac OS

Type	Attribute/File	Prominent Use
Full file listing to include	File Extension	eDiscovery
	Logical Size	eDiscovery
	Created date / time	eDiscovery
	Last Accessed date / time	eDiscovery
	Last Written (or Modified) date / time	eDiscovery
	Full path of the file / folder	eDiscovery
	An indicator if the item is a file or folder object	Forensics
	MD5 hash value for files (SHA1)	eDiscovery
File and Directories	All .bash_history files	eDiscovery
	All Plist (*.plist) files	Forensics
	All files under Thumbnail Cache folders (*/com.apple.QuickLook.thumbnailcache/*)	Forensics
	All files under */var/log/*	eDiscovery
	All files under */var/db/*	Forensics
	All files under /Users/*/Library/Preferences	eDiscovery
	All files under /Users/*/Library/Logs	eDiscovery
	/etc/hostconfig	Forensics
	/etc/localtime	Forensics
Apple Safari Browser History	/Library/Safari/*	Forensics
	/Users/*/Library/Safari/*	Forensics
	/Users/*/Library/Caches/com.apple.Safari/*	Forensics
	/Users/*/Library/Caches/Metadata/Safari/*	Forensics
	/Users/*/Library/Cookies/*	Forensics
Google Chrome Browser History	/Library/Application Support/Google/Chrome/*	Forensics
	/Users/*/Library/Application Support/Google/Chrome/*	Forensics
	/Users/*/Caches/Google/Chrome/*	Forensics
	/Users/*/Library/Caches/com.google.Chrome/*	Forensics
Mozilla Firefox Browser History	/Library/Application Support/Firefox/*	Forensics
	/Library/Caches/Firefox/*	Forensics
	/Users/*/Library/Application Support/Firefox/*	Forensics

* Additional app related artifacts could be collected from their respective app folder