

Mac OS X and iOS Forensics

LOOKING INTO THE PAST WITH FSEVENTS

SANS DFIR SUMMIT 2017

NICOLE IBRAHIM

G-C PARTNERS, LLC

Who am I?

- Digital Forensics Expert at G-C Partners
- Part time researcher
- Part time programmer

Nicole Ibrahim | Consultant | G-C Partners, LLC

nibrahim@g-cpartners.com | @nicoleibrahim

Importance

- Records historical file system activity over time
- Currently not being fully utilized by Mac examiners
- Contains User and OS activity
 - Creations, deletions, renames, permission changes and more.
- Identify names of files that were previously existing but have since been deleted
- Identify what changes occurred to files on interest

Agenda

- Introduction to FSEvents
- Parsing FSEvents
- Interesting artifacts
- Caveats

Introduction to FSEvents



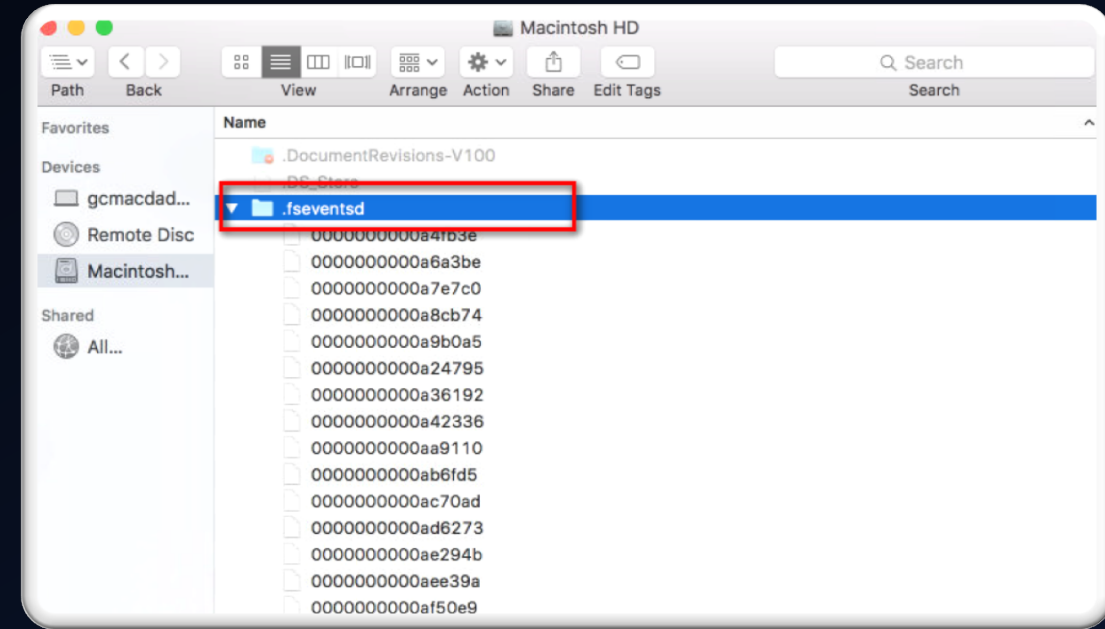
Introduction to FSEvents

- FSEvents or File System Events
- Generated by Apple OS FSEvents API
 - Introduced in 10.5 (Only directory events up to 10.6)
 - In 10.7 file events were introduced
- Stored in FSEvent log files (gzip)
 - Historical events of changes on the file system
 - Logs can span days to months
- Found on iOS, OS X devices, external devices plugged in to a Mac

Introduction to FSEvents

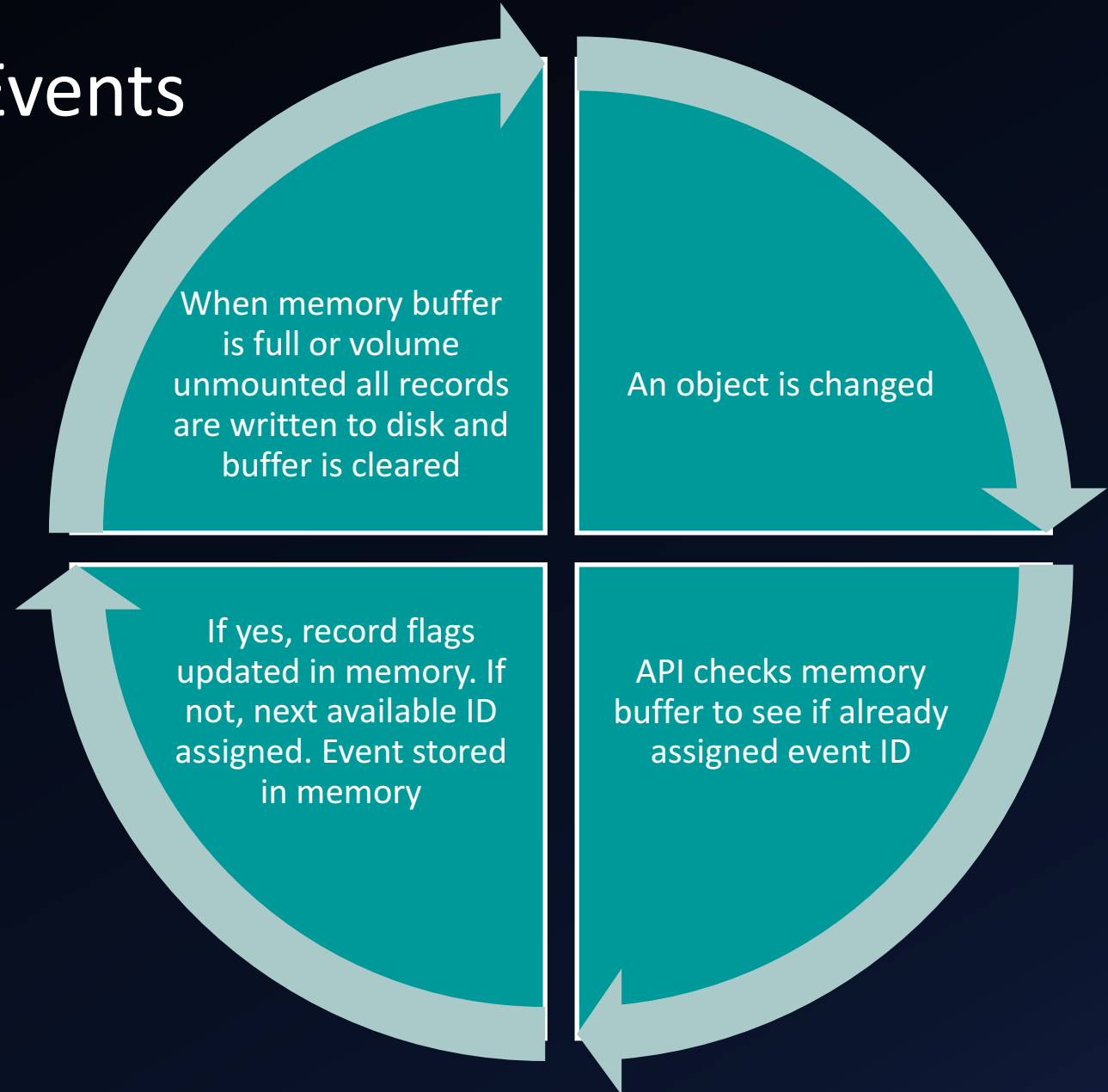
FSEVENT LOGS

- Location in OS X:
 - `/.fseventsd`
- Location in iOS:
 - Data: `/private/var/.fseventsd`
 - System: `/.fseventsd`
 - Developer Patch: `/DeveloperPatch/.fseventsd`
- Gzip archive format
- Name is last Event ID stored in the FSevent log file plus 1.
 - E.g “00000000000a4b3e” or 674,622 decimal



Introduction to FSEvents

LIFECYCLE OF AN FSEVENT RECORD



Decoding FSEvents



Decoding FSEvents

- An uncompressed FSEvent log can contain 1 or more pages with the magic header "1SLD"
- Each log can contain up to 5,000 events
- Events are ordered alphabetically by Full Path
- Each record consists of 3 components

FSEVENT RECORD COMPONENTS

Full Path

- The relative full path to the file system object that incurred a change.

Event ID

- Event ID assigned to full path on first change.

Record Flags

- Record flags indicating the type of object that was changed and what changed for it.

Decoding FSEvents

FSEVENT RECORD FLAGS

- Type flags include:

- File
- Folder
- Hard link
- Symbolic link

- Reason flags include:

- Created
- Removed
- Modified
- Renamed
- Permissions
- Inode metadata
- Finder information
- Mount
- Unmount
- Last hard link removed
- End of transaction
- Document revisions

Offset	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	
00	31	53	4c	44	c1	66	9e	4c	5f	00	00	00	4d	79	5f	46	1SLDÁf.L...My_F
10	69	6c	65	5f	31	2e	74	78	74	00	8d	54	01	00	00	00	ile_1.txt..T...
20	00	00	55	05	80	00	4d	79	5f	46	6f	6c	64	65	72	00	..U...My_Folder.
30	5d	54	01	00	00	00	00	00	c4	07	00	01	4d	79	5f	46]T.....Ä...My_F
40	6f	6c	64	65	72	2f	4d	79	5f	46	69	6c	65	5f	32	2e	older/My_File_2.
50	74	78	74	00	54	54	01	00	00	00	00	00	51	01	80	00	txt.TT.....Q...

	Description	Offset	Length	Data
	Page Magic Number	0x00	0x04	1SLD
	Page UNKNOWN Value	0x04	0x04	0xc1669e4c (3244727884)
	Page Size	0x08	0x04	0x0000005f (95)
	Record Full Path	0x0c	0x0d Variable	My_File_1.txt
	Null Terminator	0x19	0x01	.
	Record Event ID	0x1a	0x08	87,181
	Record Reason Flags	0x22	0x04	0x55058000
	Record Full Path	0x26	0x09 Variable	My_Folder
	Null Terminator	0x2f	0x01	.
	Record Event ID	0x30	0x08	87,133
	Record Reason Flags	0x38	0x04	0xc4070001
	Record Full Path	0x3c	0x13 Variable	My_Folder/My_File_2.txt
	Null Terminator	0x53	0x01	.
	Record Event ID	0x54	0x08	87,124
	Record Reason Flags	0x5c	0x04	0x51018000

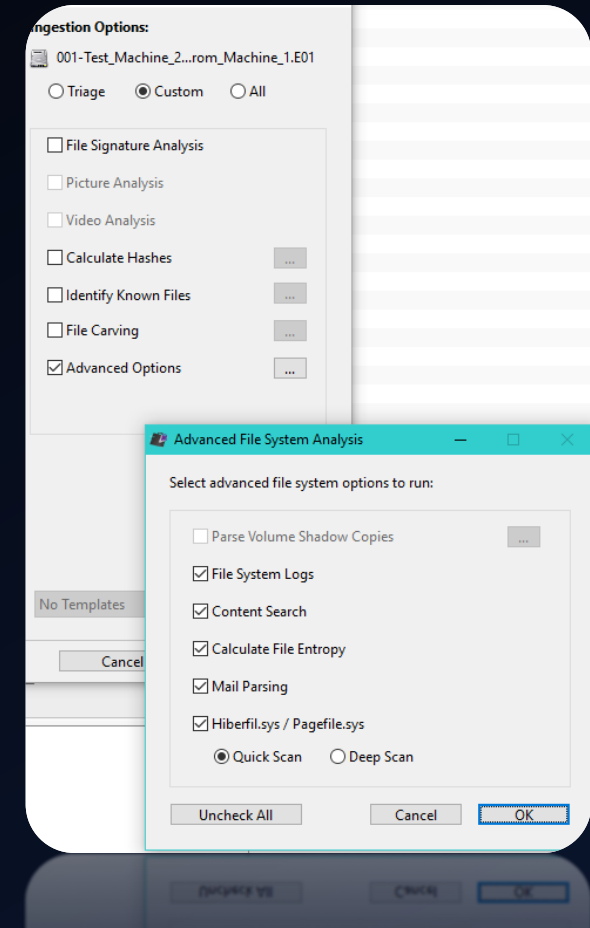
Parsing FSEvents



Parsing FSEvents

BLACKBAG BLACKLIGHT SOFTWARE

- Closed source and paid
- <https://www.blackbagtech.com/software-products/blacklight.html>



Identifier	Source File	Source File Create Date	Source File Modified Date	File Name	File Path	Reasons	Offset
1180070	0000000000120112	2016-10-22 20:45:28 (UTC)	2016-10-22 20:45:28 (UTC)	.		IsDirectory, EndOfTransaction	45
1180069	0000000000120112	2016-10-22 20:45:28 (UTC)	2016-10-22 20:45:28 (UTC)	sl-compat	.fseventsd/sl-compat	IsDirectory	12
1179920	0000000000120111	2016-10-22 20:45:28 (UTC)	2016-10-22 20:45:28 (UTC)	.DS_Store	.DS_Store	InodeMetaMod, Modified, IsFile	25
1179467	0000000000120111	2016-10-22 20:45:28 (UTC)	2016-10-22 20:45:28 (UTC)	.		Mounted	12
1179417	0000000000120111	2016-10-22 20:45:28 (UTC)	2016-10-22 20:45:28 (UTC)	VolumeConfiguration.plist	.Spotlight-V100/VolumeConfiguration.plist	InodeMetaMod, Modified, IsFile	47

Parsing FSEvents

G-C PARTNERS FSEVENTSPARSER SCRIPT

- Open source and free
- Python
- Available at
<https://github.com/dlcowen/FSEventsParser>

```
.\\00-Research\\006-FSEvents\\Code\\Public_Releases>python FSEvents_Parser_V2.1.py -c test2 -s D:\\f -o g:\\

=====
SEParser v 2.1 -- provided by G-C Partners, LLC
Run Time: 06/05/2017 00:42:36 [UTC]
=====

file 1 of 2: Trying 0000000000120111
LD Header found. Parsing records

file 2 of 2: Trying 0000000000120112
LD Header found. Parsing records

-----

FINISHED PARSING: See exceptions log for parsing errors.
11 Files Attempted: 2
11 Parsed Files: 2
0 Files with Errors: 0
1 Records Parsed: 5
```

event_id	filename	mask	mask_hex	record_end_offset	source	source_modified_time	other_dates
1179467	NULL	Mount;	0x00000002	25	D:\\f\\0000000000120111	10/22/2016 14:45	UNKNOWN
1179920	.DS_Store	Modified;InodeMetaMod;FileEvent;	0x14008000	47	D:\\f\\0000000000120111	10/22/2016 14:45	UNKNOWN
1179417	.Spotlight-V100/VolumeConfiguration.plist	Modified;InodeMetaMod;FileEvent;	0x14008000	101	D:\\f\\0000000000120111	10/22/2016 14:45	UNKNOWN
1180069	.fseventsd/sl-compat	FolderEvent;	0x00000001	45	D:\\f\\0000000000120112	10/22/2016 14:45	UNKNOWN
1180070	NULL	FolderEvent;EndOfTransaction;	0x00000021	58	D:\\f\\0000000000120112	10/22/2016 14:45	UNKNOWN

Interesting Artifacts



Record Artifacts

OS X

- Just scratching the surface of interesting artifacts:
 - .Trash activity
 - User folders activity
 - Internet activity
 - Mount events

Record Artifacts: OS X

TRASH ACTIVITY

- Files sent to the Trash
- Emptying the Trash

```
SELECT      *, _ROWID_ "NAVICAT_ROWID"
FROM        "fsevents"
WHERE       "filename" LIKE 'Users/%/.Trash/%'
```

rowid	filename	mask
24255026	Users/gc/.Trash/My_Tests/.DS_Store	Modified;InodeMetaMod;Removed;FileEvent;
24255452	Users/gc/.Trash/My_Tests/20160127_Tests	FolderEvent;Removed;
24255029	Users/gc/.Trash/My_Tests/20160127_Tests/.DS_Store	Removed;FileEvent;
24255032	Users/gc/.Trash/My_Tests/20160127_Tests/FSEventMonitor_v0.3_Terminal_log.txt	Removed;FileEvent;
24255449	Users/gc/.Trash/My_Tests/20160127_Tests/FSParser_Reports	FolderEvent;Removed;
24255440	Users/gc/.Trash/My_Tests/20160127_Tests/FSParser_Reports/FSEvents-EXCEPTIONS_LOG.txt	Removed;FileEvent;
24255443	Users/gc/.Trash/My_Tests/20160127_Tests/FSParser_Reports/FSEvents-Parsed_Records-tab_delimited.txt	Removed;FileEvent;
24255446	Users/gc/.Trash/My_Tests/20160127_Tests/FSParser_Reports/fsevents.sqlite	Removed;FileEvent;
24255437	Users/gc/.Trash/My_Tests/20160127_Tests/fsevents	FolderEvent;Removed;
24255035	Users/gc/.Trash/My_Tests/20160127_Tests/fsevents/000000000000094d6	Removed;FileEvent;
24255038	Users/gc/.Trash/My_Tests/20160127_Tests/fsevents/000000000000cf7a	Removed;FileEvent;
24255041	Users/gc/.Trash/My_Tests/20160127_Tests/fsevents/00000000000015233	Removed;FileEvent;
24255044	Users/gc/.Trash/My_Tests/20160127_Tests/fsevents/0000000000002240c	Removed;FileEvent;
24255047	Users/gc/.Trash/My_Tests/20160127_Tests/fsevents/0000000000002240d	Removed;FileEvent;
24255050	Users/gc/.Trash/My_Tests/20160127_Tests/fsevents/00000000000022e55	Removed;FileEvent;

Record Artifacts: OS X

USER FOLDERS ACTIVITY

- Activity in:
 - “Documents”
 - “Downloads”
 - “Desktop”

```
SELECT
    *, _ROWID_ "NAVICAT_ROWID"
FROM
    "fsevents"
WHERE
    "filename" LIKE 'Users/%/Documents/%'
    OR "filename" LIKE 'Users/%/Downloads/%'
    OR "filename" LIKE 'Users/%/Desktop/%'
```

wd	filename	mask
7747658	Users/neiko/Downloads/Microsoft_Office_2016_15.32.17030901_Installer.pkg	Renamed;FileEvent;
7751272	Users/neiko/Downloads/Unconfirmed 148620.crdownload	Modified;Renamed;Created;PermissionChange;ExtendedAttrModified;FileEvent;
7751632	Users/neiko/Downloads/navicat112_sqlite_en.dmg	Renamed;Created;PermissionChange;ExtendedAttrModified;FileEvent;
7730702	Users/neiko/Library/Containers/com.microsoft.Word/Data/Documents/whatsNewJSONCache.plist	Renamed;PermissionChange;FinderInfoMod;FileEvent;
7980785	Users/neiko/Desktop/.DS_Store	Modified;InodeMetaMod;Created;FinderInfoMod;FileEvent;
7978872	Users/neiko/Desktop/.fseventsd	FolderEvent;Renamed;InodeMetaMod;PermissionChange;ExtendedAttrModified;
7975787	Users/neiko/Desktop/.fseventsd/00000000000006211	Modified;Created;PermissionChange;FinderInfoMod;FileEvent;
7975799	Users/neiko/Desktop/.fseventsd/00000000000006212	Modified;Created;PermissionChange;FinderInfoMod;FileEvent;
7975811	Users/neiko/Desktop/.fseventsd/00000000000015401	Modified;Created;PermissionChange;FinderInfoMod;FileEvent;
7975823	Users/neiko/Desktop/.fseventsd/000000000000210fb	Modified;Created;PermissionChange;FinderInfoMod;FileEvent;
7975835	Users/neiko/Desktop/.fseventsd/0000000000002df90	Modified;Created;PermissionChange;FinderInfoMod;FileEvent;
7975847	Users/neiko/Desktop/.fseventsd/0000000000003cdea	Modified;Created;PermissionChange;FinderInfoMod;FileEvent;
7975859	Users/neiko/Desktop/.fseventsd/0000000000004b3f0	Modified;Created;PermissionChange;FinderInfoMod;FileEvent;

Record Artifacts: OS X

INTERNET ACTIVITY

- Websites visited
 - Chrome
 - Safari

```
SELECT
    *, _ROWID_ "NAVICAT_ROWID"
FROM
    "fsevents"
WHERE
    "filename" LIKE
    'Users/%/Library/Caches/Metadata/Safari/History/%'
    OR "filename" LIKE 'Users/%/Library/Application
    Support/Google/Chrome/Default/Local Storage/%'
```

rowid	filename	mask
5408233	Users/other/Library/Application Support/Google/Chrome/Default/Local Storage/https_www.netflix.com_0.localstorage-journal	Modified;InodeMetaMod;FileEvent;
5325097	Users/other/Library/Application Support/Google/Chrome/Default/Local Storage/https_www.youtube.com_0.localstorage	InodeMetaMod;Created;ExtendedAttrModified;FileEvent;
5325109	Users/other/Library/Application Support/Google/Chrome/Default/Local Storage/https_www.youtube.com_0.localstorage-journal	Modified;InodeMetaMod;Created;ExtendedAttrModified;FileEvent;
5463881	Users/other/Library/Application Support/Google/Chrome/Default/Local Storage/chrome-extension_pkedcjkdefgdpelpbcbmbmeomcjbemfm_0.localstor	Modified;InodeMetaMod;FileEvent;
5408467	Users/other/Library/Application Support/Google/Chrome/Default/Local Storage/https_www.amazon.com_0.localstorage-journal	Modified;InodeMetaMod;FileEvent;
5409287	Users/other/Library/Application Support/Google/Chrome/Default/Local Storage/https_www.netflix.com_0.localstorage	InodeMetaMod;FileEvent;
5412791	Users/other/Library/Application Support/Google/Chrome/Default/Local Storage/https_www.netflix.com_0.localstorage-journal	Modified;InodeMetaMod;FileEvent;
5481704	Users/nikki/Library/Caches/Metadata/Safari/History/http:%2F%2Fwfaa.com%2F.webhistory	Modified;Created;ExtendedAttrModified;ExtendedAttrRemoved;FileEvent;
5481716	Users/nikki/Library/Caches/Metadata/Safari/History/http:%2F%2Fwww.wfaa.com%2F.webhistory	Modified;Created;ExtendedAttrModified;ExtendedAttrRemoved;FileEvent;
5491733	Users/nikki/Library/Caches/Metadata/Safari/History/http:%2F%2Fwww.wfaa.com%2Fweather%2Fradars.webhistory	Modified;Created;ExtendedAttrModified;ExtendedAttrRemoved;FileEvent;
5493889	Users/nikki/Library/Caches/Metadata/Safari/History/http:%2F%2Fwww.wfaa.com%2Fweather%2Ftexas-radar.webhistory	Modified;Created;ExtendedAttrModified;ExtendedAttrRemoved;FileEvent;
5486606	Users/nikki/Library/Caches/Metadata/Safari/History/http:%2F%2Fwww.wfaa.com%2Fweather%2Fwfaa-weather-large-hail-damaging-wind-possible-to	Modified;Created;ExtendedAttrModified;ExtendedAttrRemoved;FileEvent;
5504075	Users/nikki/Library/Caches/Metadata/Safari/History/https:%2F%2Fen.wikipedia.org%2Fwiki%2FWind_shear.webhistory	Modified;Created;ExtendedAttrModified;ExtendedAttrRemoved;FileEvent;
5498048	Users/nikki/Library/Caches/Metadata/Safari/History/https:%2F%2Fwww.google.com%2Fsearch?client=safari&rls=en&q=weather&ie=UTF-8&oe=UTF-8	Modified;Created;ExtendedAttrModified;ExtendedAttrRemoved;FileEvent;

Record Artifacts: OS X

MOUNT ACTIVITY

- Mount activity related to:
 - DMGs
 - External devices
 - Shared network drives

```
SELECT
    *, _ROWID_ "NAVICAT_ROWID"
FROM
    "fsevents"
WHERE
    "mask" LIKE '%mount%'
```

event_id	filename	mask	mask_hex	source_modified_time
6698195	/Volumes/Recovery HD	FolderEvent;Unmount;Removed;	0x02000005	2017-03-24 17:46:32
6691374	/home	Mount;	0x00000002	2017-03-24 17:46:32
6690718	/net	Mount;	0x00000002	2017-03-24 17:46:32
6727297	/Volumes/Recovery HD	Unmount;	0x00000004	2017-03-24 20:56:02
6757329	/private/var/setup	FolderEvent;Mount;Unmount;PermissionChange;Removed;	0x02010007	2017-03-24 20:56:02
6767834	/Volumes/Recovery HD	FolderEvent;Mount;Unmount;Removed;	0x02000007	2017-03-25 01:09:45
10629284	/Volumes/MachOView	Mount;	0x00000002	2016-03-21 15:29:44
444876	/Volumes/OSX_108TEST	FolderEvent;Unmount;FolderCreated;	0x80000005	2016-03-21 15:29:44
245516	/Volumes/OSX_108TEST 1	Mount;Unmount;	0x00000006	2016-03-21 15:29:44
10576968	/Volumes/TEST	FolderEvent;Unmount;FolderCreated;	0x80000005	2016-03-21 15:29:44
10535360	/Volumes/Test_Folder_Actions	FolderEvent;Mount;Unmount;FolderCreated;Removed;	0x82000007	2016-03-21 15:29:44
10576969	/Volumes/UNTITLED	FolderEvent;Unmount;Removed;	0x02000005	2016-03-21 15:29:44
10625760	/Volumes/Untitled	Unmount;	0x00000004	2016-03-21 15:29:44
1419	/home	Mount;	0x00000002	2016-03-21 15:29:44
1418	/net	Mount;	0x00000002	2016-03-21 15:29:44
10640527	/Volumes/Recovery HD	FolderEvent;Mount;Unmount;Removed;	0x02000007	2016-03-23 09:58:48
10686244	/Volumes/artifacts-20160114.pkg	Mount;Unmount;	0x00000006	2016-03-23 09:58:48
10686248	/Volumes/bencode-1.0.pkg	Mount;Unmount;	0x00000006	2016-03-23 09:58:48

Artifacts

IOS

- iCloud synced files
- Internet activity
- Email activity

Record Artifacts: iOS

ICLOUD SYNCED FILES

- iCloud synced files from other devices

```
SELECT
    *, _ROWID_ "NAVICAT_ROWID"
FROM
    "fsevents"
WHERE
    "filename" LIKE 'mobile/Library/Mobile
Documents/com~apple~CloudDocs/%'
```

event_id	filename	mask
33604138	mobile/Library/Mobile Documents/com~apple~CloudDocs/.Trash/_fseventsd 5.30.19 PM/.00000000020d4441.icloud	Renamed;FileEvent;
33605361	mobile/Library/Mobile Documents/com~apple~CloudDocs/.Trash/_fseventsd 5.30.19 PM/.00000000020d9d05.icloud	Renamed;FileEvent;
33605341	mobile/Library/Mobile Documents/com~apple~CloudDocs/.Trash/_fseventsd 5.30.19 PM/.00000000020dea0e.icloud	Renamed;FileEvent;
33605331	mobile/Library/Mobile Documents/com~apple~CloudDocs/.Trash/_fseventsd 5.30.19 PM/.00000000020e5586.icloud	Renamed;FileEvent;
33603451	mobile/Library/Mobile Documents/com~apple~CloudDocs/.Trash/_fseventsd 5.30.19 PM/.00000000020f16ac.icloud	Renamed;FileEvent;
33604219	mobile/Library/Mobile Documents/com~apple~CloudDocs/.Trash/_fseventsd 5.30.19 PM/.00000000020f6e68.icloud	Renamed;FileEvent;
33604177	mobile/Library/Mobile Documents/com~apple~CloudDocs/.Trash/_fseventsd 5.30.19 PM/.0000000002100c5f.icloud	Renamed;FileEvent;
33604258	mobile/Library/Mobile Documents/com~apple~CloudDocs/.Trash/_fseventsd 5.30.19 PM/.0000000002107919.icloud	Renamed;FileEvent;
33604893	mobile/Library/Mobile Documents/com~apple~CloudDocs/.Trash/_fseventsd 5.30.19 PM/.000000000210bacb.icloud	Renamed;FileEvent;
33605381	mobile/Library/Mobile Documents/com~apple~CloudDocs/.Trash/_fseventsd 5.30.19 PM/.000000000210ff8b.icloud	Renamed;FileEvent;
33603361	mobile/Library/Mobile Documents/com~apple~CloudDocs/.Trash/_fseventsd 5.30.19 PM/.0000000002113bd4.icloud	Renamed;FileEvent;

Record Artifacts: iOS

INTERNET ACTIVITY

- Websites visited?

```
SELECT
    *, _ROWID_ "NAVICAT_ROWID"
FROM
    "fsevents"
WHERE
    "filename" LIKE '%websitedata/local%'
```

event_id	filename	mask
3688334	mobile/Containers/Data/Application/4B88FE56-DDDE-42D9-BE34-54F61FED2D57/Library/WebKit/WebsiteData/LocalStorage/http_www.redsn0w.us_0.localstorage-journal	Modified;Created;Removed;FileEvent;
3732012	mobile/Containers/Data/Application/4B88FE56-DDDE-42D9-BE34-54F61FED2D57/Library/WebKit/WebsiteData/LocalStorage/StorageTracker.db-journal	Modified;Created;Removed;FileEvent;
3702270	mobile/Containers/Data/Application/4B88FE56-DDDE-42D9-BE34-54F61FED2D57/Library/WebKit/WebsiteData/LocalStorage/http_www.npr.org_0.localstorage	Modified;FileEvent;
3790959	mobile/Containers/Data/Application/4B88FE56-DDDE-42D9-BE34-54F61FED2D57/Library/WebKit/WebsiteData/LocalStorage/StorageTracker.db-journal	Modified;Created;Removed;FileEvent;
3790962	mobile/Containers/Data/Application/4B88FE56-DDDE-42D9-BE34-54F61FED2D57/Library/WebKit/WebsiteData/LocalStorage/https_www.instagram.com_0.localstorage	Modified;Created;Removed;FileEvent;
3790860	mobile/Containers/Data/Application/4B88FE56-DDDE-42D9-BE34-54F61FED2D57/Library/WebKit/WebsiteData/LocalStorage/https_www.instagram.com_0.localstorage-journal	Modified;Created;Removed;FileEvent;
3847710	mobile/Containers/Data/Application/E2DD4CDC-722A-480C-86B3-1F5BCD1E8F2F/Library/WebKit/WebsiteData/LocalStorage/StorageTracker.db-journal	Modified;Created;Removed;FileEvent;
3847983	mobile/Containers/Data/Application/E2DD4CDC-722A-480C-86B3-1F5BCD1E8F2F/Library/WebKit/WebsiteData/LocalStorage/https_m.youtube.com_0.localstorage-journal	Modified;Created;Removed;FileEvent;
3806827	mobile/Containers/Data/Application/F6142168-1D6B-44CC-8CD1-C306ED328B0C/Library/WebKit/WebsiteData/LocalStorage/StorageTracker.db-journal	Modified;Created;Removed;FileEvent;
3807598	mobile/Containers/Data/Application/F6142168-1D6B-44CC-8CD1-C306ED328B0C/Library/WebKit/WebsiteData/LocalStorage/http_pubads.g.doubleclick.net_0.localstorage	Modified;Created;FileEvent;
3806733	mobile/Containers/Data/Application/F6142168-1D6B-44CC-8CD1-C306ED328B0C/Library/WebKit/WebsiteData/LocalStorage/http_pubads.g.doubleclick.net_0.localstorage-journal	Modified;Created;Removed;FileEvent;
3807607	mobile/Containers/Data/Application/F6142168-1D6B-44CC-8CD1-C306ED328B0C/Library/WebKit/WebsiteData/LocalStorage/http_www.vox.com_0.localstorage	Modified;Created;FileEvent;
3807349	mobile/Containers/Data/Application/F6142168-1D6B-44CC-8CD1-C306ED328B0C/Library/WebKit/WebsiteData/LocalStorage/http_www.vox.com_0.localstorage-journal	Modified;Created;Removed;FileEvent;
3845403	mobile/Containers/Data/Application/C8F70FFA-7504-49A0-B1A9-1A5C5A7B60FB/Library/WebKit/WebsiteData/LocalStorage/StorageTracker.db-shm	InodeMetaMod;FileEvent;
3845439	mobile/Containers/Data/Application/C8F70FFA-7504-49A0-B1A9-1A5C5A7B60FB/Library/WebKit/WebsiteData/LocalStorage/https_m.facebook.com_0.localstorage-shm	Modified;InodeMetaMod;FileEvent;
3885979	mobile/Containers/Data/Application/E2DD4CDC-722A-480C-86B3-1F5BCD1E8F2F/Library/WebKit/WebsiteData/LocalStorage/StorageTracker.db-journal	Modified;Created;Removed;FileEvent;
3886855	mobile/Containers/Data/Application/E2DD4CDC-722A-480C-86B3-1F5BCD1E8F2F/Library/WebKit/WebsiteData/LocalStorage/https_m.youtube.com_0.localstorage	Modified;FileEvent;
3886308	mobile/Containers/Data/Application/E2DD4CDC-722A-480C-86B3-1F5BCD1E8F2F/Library/WebKit/WebsiteData/LocalStorage/https_www.google.com_0.localstorage-journal	Modified;Created;Removed;FileEvent;

Record Artifacts: iOS

EMAIL ACTIVITY

- Inbox
- Sent
- Attachments

```
SELECT
    *, _ROWID_ "NAVICAT_ROWID"
FROM
    "fsevents"
WHERE
    "filename" LIKE 'mobile/Library/Mail/%'
```

event_id	filename	mask
5428567	mobile/Library/Mail/IMAP-[REDACTED]/INBOX.imapmbox/Attachments/55212/4/shield.png	Renamed;FileEvent;
5428634	mobile/Library/Mail/IMAP-[REDACTED]@imap.gmail.com/INBOX.imapmbox/Attachments/55214/2/unknown_device.png	Renamed;FileEvent;
5428589	mobile/Library/Mail/IMAP-[REDACTED]@imap.gmail.com/INBOX.imapmbox/Attachments/55214/3/google_logo.png	Renamed;FileEvent;
5428653	mobile/Library/Mail/IMAP-[REDACTED]@imap.gmail.com/INBOX.imapmbox/Attachments/55214/4/shield.png	Renamed;FileEvent;
33902492	mobile/Library/Mail/IMAP-[REDACTED]/INBOX.imapmbox/Attachments/64567/2/FSEvents_Documentation.docx	Renamed;FileEvent;
33905154	mobile/Library/Mail/IMAP-[REDACTED]/INBOX.imapmbox/Attachments/64573/2/mime-attachment.jpg	Renamed;FileEvent;
33905245	mobile/Library/Mail/IMAP-[REDACTED]/INBOX.imapmbox/Attachments/64573/3/mime-attachment.jpg	Renamed;FileEvent;
33905294	mobile/Library/Mail/IMAP-[REDACTED]/INBOX.imapmbox/Attachments/64573/4/mime-attachment.jpg	Renamed;FileEvent;
33905343	mobile/Library/Mail/IMAP-[REDACTED]/INBOX.imapmbox/Attachments/64573/5/mime-attachment.jpg	Renamed;FileEvent;
33905114	mobile/Library/Mail/IMAP-[REDACTED]/INBOX.imapmbox/Attachments/64573/6/mime-attachment.gif	Renamed;FileEvent;
34392427	mobile/Library/Mail/IMAP-[REDACTED]/INBOX.imapmbox/Attachments/64618/2/[REDACTED].xls	Renamed;FileEvent;
36504866	mobile/Library/Mail/IMAP-[REDACTED]/INBOX.imapmbox/Attachments/39892/2/[REDACTED].xls	Removed;FileEvent;
36504854	mobile/Library/Mail/IMAP-[REDACTED]/INBOX.imapmbox/Attachments/49134/2/IMG_1957.JPG	Removed;FileEvent;
36504818	mobile/Library/Mail/IMAP-[REDACTED]/INBOX.imapmbox/Attachments/50064/1.2	FolderEvent;Removed;
36504815	mobile/Library/Mail/IMAP-[REDACTED]/INBOX.imapmbox/Attachments/50064/1.2/Screen Shot 2017-05-03 at 10.14.40 AM.png	Removed;FileEvent;

Caveats



Caveats

- Lost FSEvents
- Lack of timestamps
- External devices
- Anti-forensics
- Coalescing of multiple changes

Caveats: Lost FSEvents

PROBLEM

- FSEvents are lost due to either:
 - A hard reset of a system
 - A system crash
 - Not properly unmounting a volume
 - System upgrades

REMEDIES

- Carve for gzip files

Caveats: Lack of Timestamps



PROBLEM

- FSEvent Records consist of:
 - Event ID
 - Full Path
 - Flags
- Note timestamps are not mentioned

REMEDIES

- Use temporal data from the names of logs

wd	filename	mask	mask_hex	source_modified_time	other_dates
1054	private/var/log/DiagnosticMessages/2017.05.13.asl	Created;PermissionChange;ExtendedAttrModified;FileEvent;	0x01038000	2017-05-13 13:02:26	2017.05.13
426	private/var/log/asl/2017.05.13.G80.asl	Created;PermissionChange;ExtendedAttrModified;FileEvent;	0x01038000	2017-05-13 13:02:26	2017.05.13
519	private/var/log/powermanagement/2017.05.13.asl	Modified;Created;PermissionChange;ExtendedAttrModified;FileEvent;	0x11038000	2017-05-13 13:02:26	2017.05.13
209338	private/var/log/powermanagement/2017.05.13.asl	Modified;FileEvent;	0x10008000	2017-05-13 14:39:47	UNKNOWN
1124380	private/var/log/DiagnosticMessages/2017.05.13.asl	Modified;FileEvent;	0x10008000	2017-05-13 16:06:22	UNKNOWN
3796573	private/var/log/DiagnosticMessages/2017.05.13.asl	Modified;FileEvent;	0x10008000	2017-05-13 16:26:37	UNKNOWN
5079026	private/var/log/DiagnosticMessages/2017.05.13.asl	Modified;FileEvent;	0x10008000	2017-05-14 09:22:29	2017.05.13,2017.05.14
5078975	private/var/log/asl/2017.05.13.G80.asl	Modified;FileEvent;	0x10008000	2017-05-14 09:22:29	2017.05.13,2017.05.14
5079020	private/var/log/powermanagement/2017.05.13.asl	Modified;FileEvent;	0x10008000	2017-05-14 09:22:29	2017.05.13,2017.05.14

Caveats: External Devices

PROBLEM

- Unsafe removal results in lost events
- Safe removal was performed, but FSEvents not finished writing to disk
- File system compatibility issues results in lost events

REMEDIES

- Hope that the user has properly unmounted their devices
 - Carving for those lost events might not be possible due to FSEvents being stored in memory

Caveats: Coalescing of multiple changes


PROBLEM

- The FSEvents API coalesces multiple changes into a single record resulting in:
 - Inability to determine order of changes
 - Inability to determine frequency of changes

REMEDIES

- None

This file may have been created 3 times and removed twice, but we will never know



Event ID	Record Full Path	Event Reason Flags
123	Users/GC/Desktop/My_Test_File.txt	Created,Removed,Modified,FileEvent

Caveats: Anti-Forensics

PROBLEM

- A no_log file was placed in the .fseventsd directory
 - FSEvents are not recorded for the volume

REMEDIES

- None. However, this scenario is unlikely and requires root privileges and advanced knowledge of FSEvents



Questions?

Nicole Ibrahim | Consultant | G-C Partners, LLC

nibrahim@g-cpartners.com | @nicoleibrahim