Yogesh Khatri

mac_apt

MACOS ARTIFACT PARSING TOOL

YOGESH KHATRI

CHAMPLAIN COLLEGE

@SWIFTFORENSICS

Need and Goals

Could not find platform independent open source tool for macOS processing

- Other FOSS tools depended on obj-C or .NET or other non-free tools

Till a few months ago, Autopsy / Sleuthkit could not read lzvn compressed files (30-50% on El Capitan)

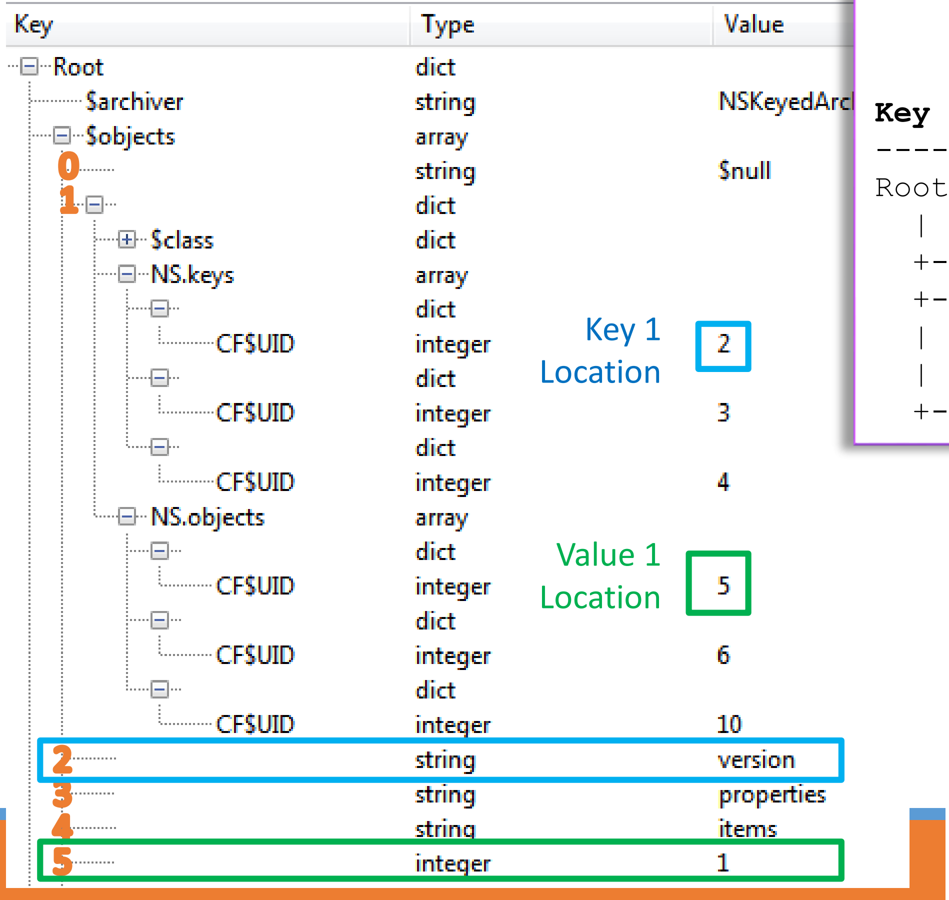
- Only one commercial tool could!

Wanted to learn mac forensic analysis from the ground up

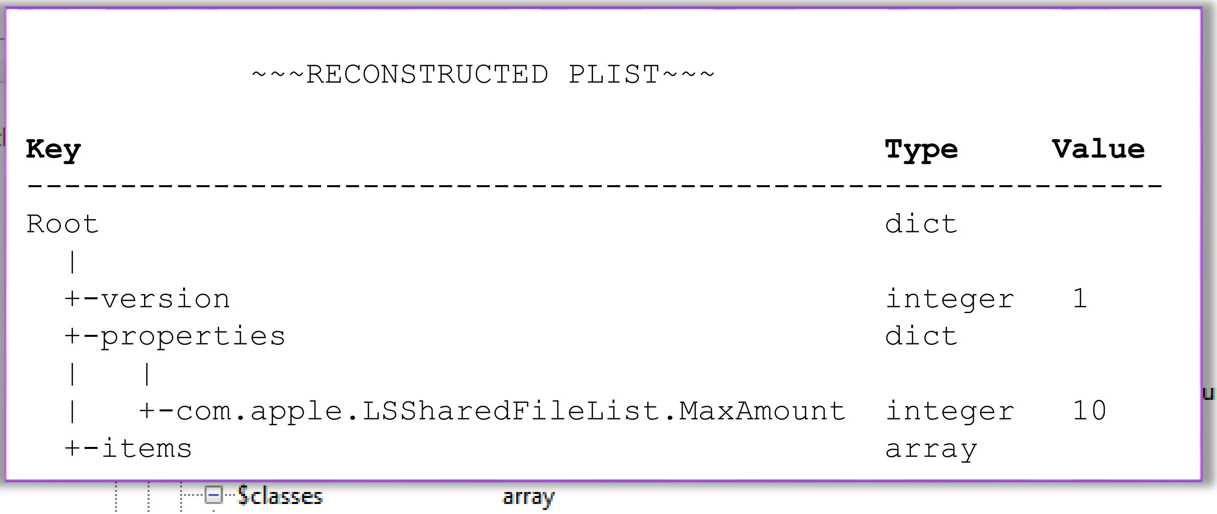
Manual analysis of artifacts is very slow!

- Several thousand plists to look at..
- Manual analysis is not always possible!

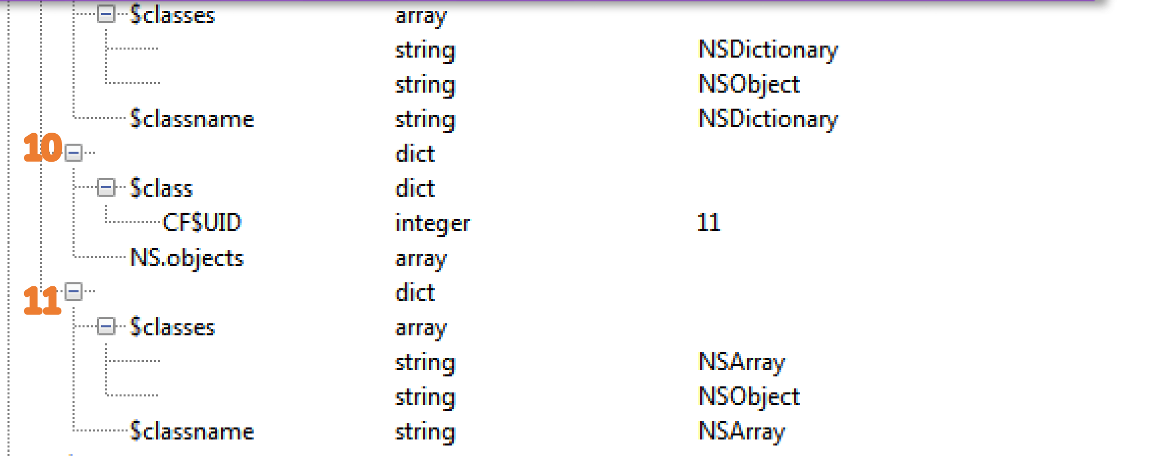
Manual analysis fail - SFL plist files



```
Key                         Type       Value
Root                        dict
   $archiver                string     NSKeyedArc
   $objects                 array
0                           string     $null
1                           dict
      $class                dict
      NS.keys               array
                            dict
            CF$UID          integer    2
                            dict
            CF$UID          integer    3
                            dict
            CF$UID          integer    4
      NS.objects            array
                            dict
            CF$UID          integer    5
                            dict
            CF$UID          integer    6
                            dict
            CF$UID          integer    10
2                           string     version
3                           string     properties
4                           string     items
5                           integer    1
```



```
                   ~~~RECONSTRUCTED PLIST~~~

Key                                             Type       Value
---------------------------------------------------------------
Root                                            dict
   |
   +-version                                    integer    1
   +-properties                                 dict
   |    |
   |    +-com.apple.LSSharedFileList.MaxAmount  integer    10
   +-items                                      array
```



```
      $classes              array
                            string     NSDictionary
                            string     NSObject
      $classname            string     NSDictionary
10                          dict
      $class                dict
         CF$UID             integer    11
      NS.objects            array
11                          dict
      $classes              array
                            string     NSArray
                            string     NSObject
      $classname            string     NSArray
```

The Design -
By forensic analysts For forensic analysts

Works with popular/common disk image formats

- Also works on mounted volumes or individual artifact files/databases

Spreadsheet-like output (XLSX, SQLite) for easily filtering, sorting and sifting of data

Every piece of output data references its source

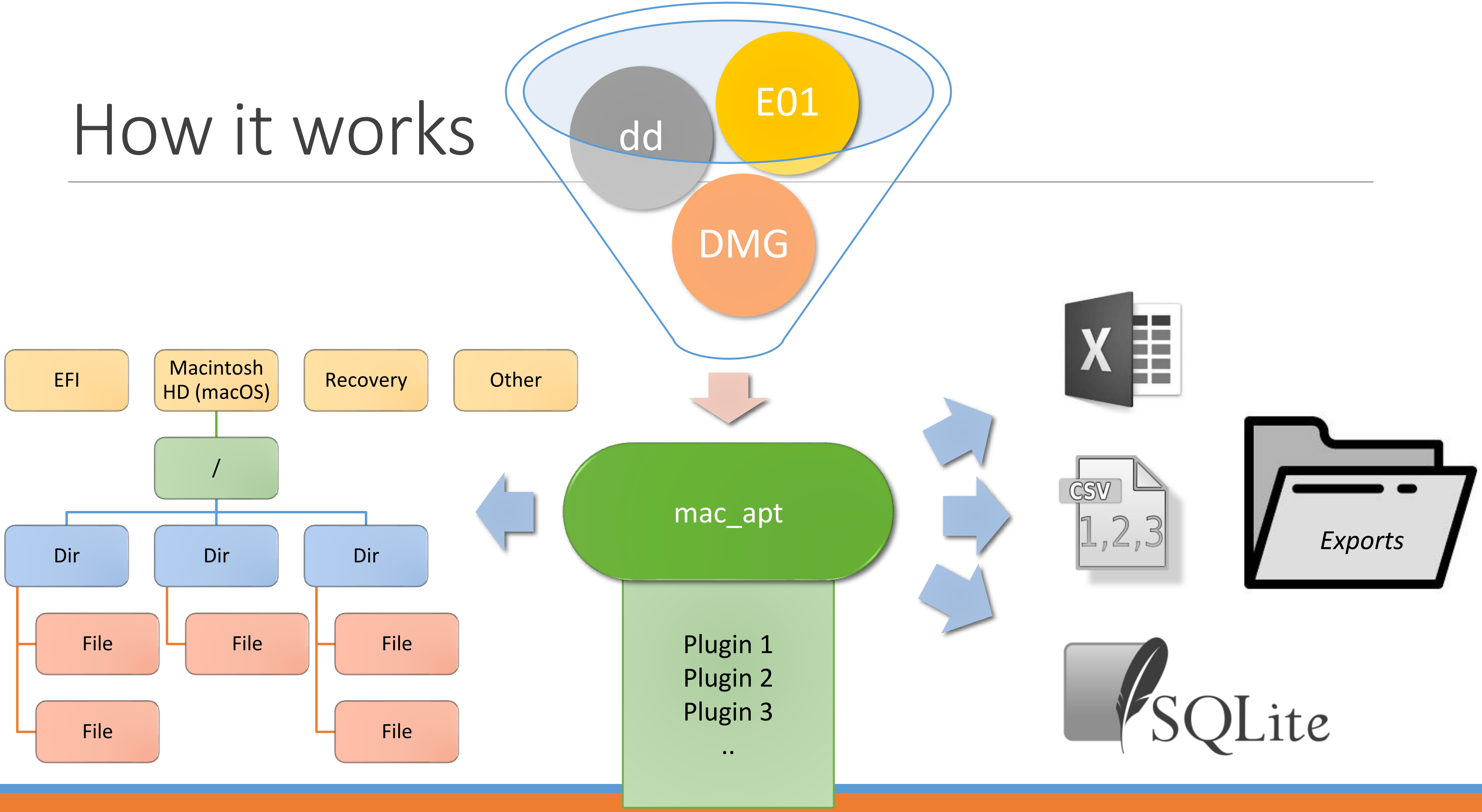
Exports analyzed files for manual review

Completely Open source using libraries available for Linux, Windows & macOS

Native file system parsers - HFS+ (with lzvn support) & APFS for robustness when dependent libraries fail

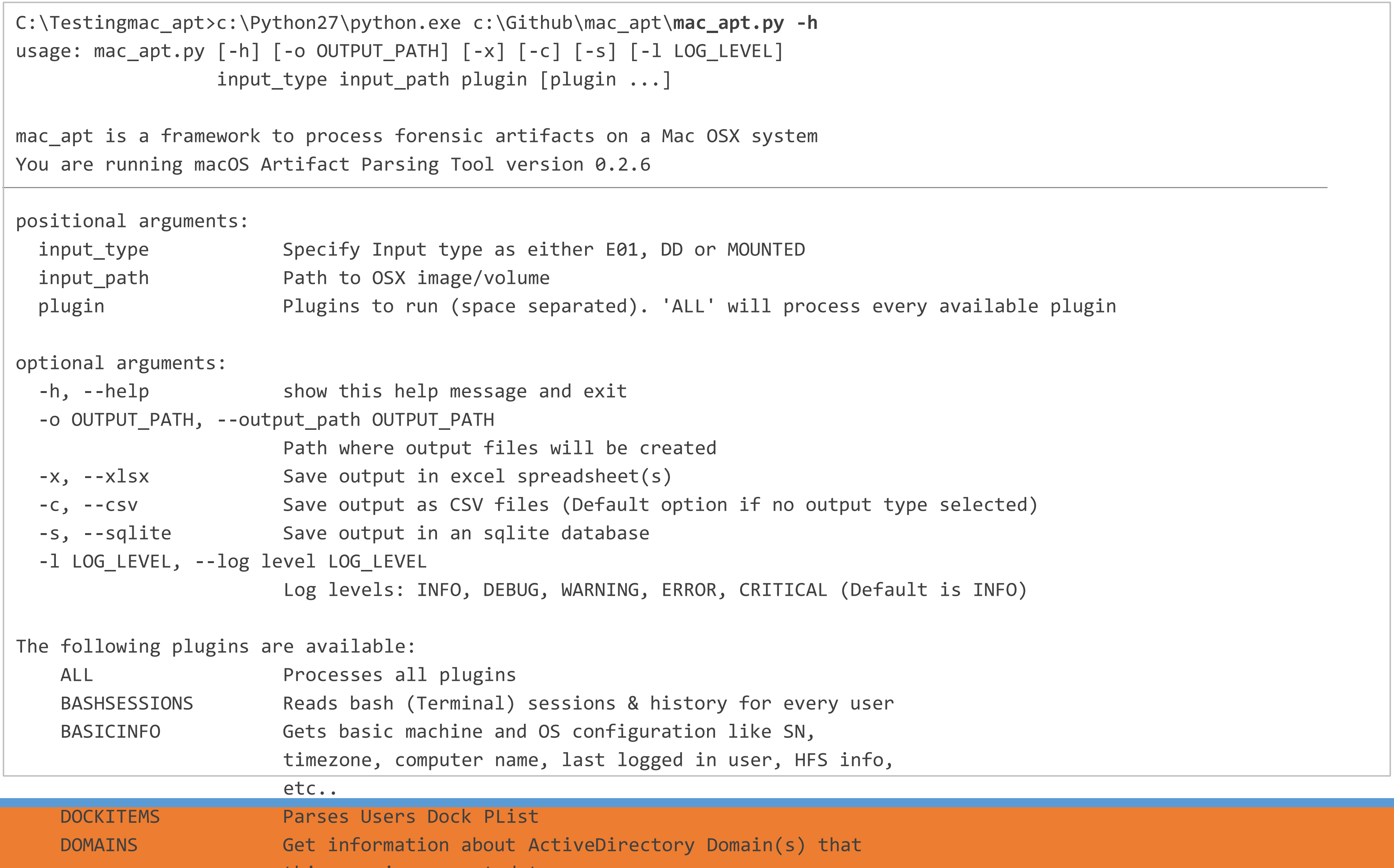
Plugin based architecture for expansion

How it works



dd
E01
DMG
EFI
Macintosh HD (macOS)
Recovery
Other
/
Dir
Dir
Dir
File
File
File
File
File
mac_apt
Plugin 1
Plugin 2
Plugin 3
..
CSV
1,2,3
Exports
SQLite

mac_apt -h

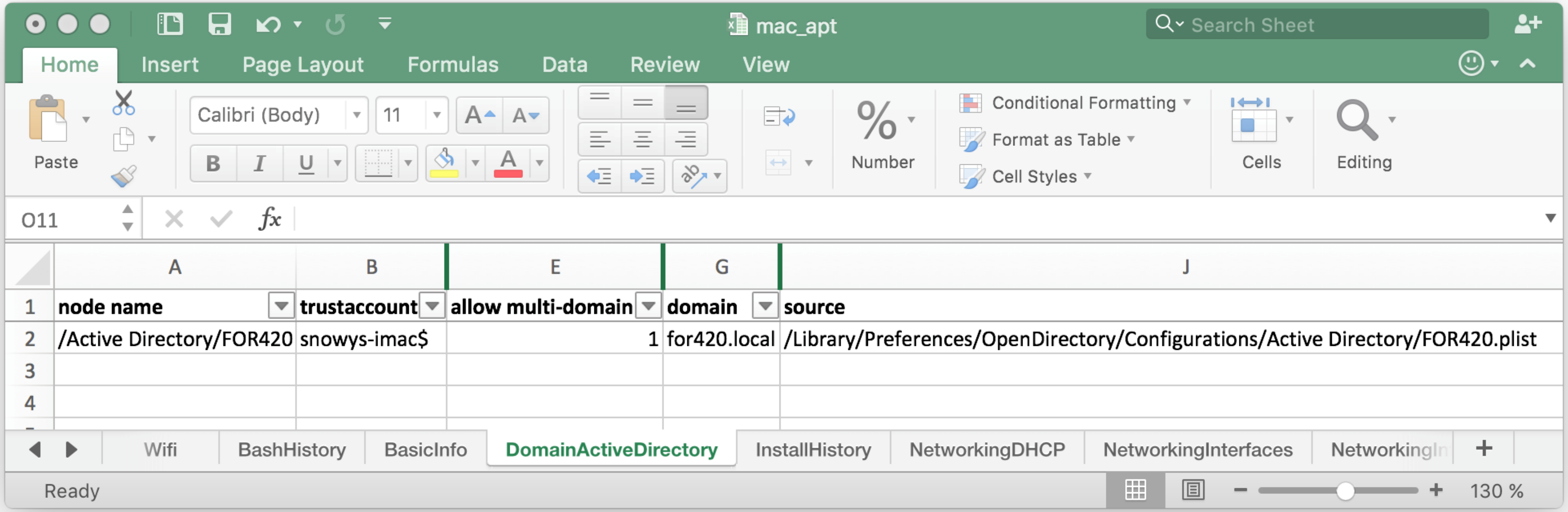


```
C:\Testingmac_apt>c:\Python27\python.exe c:\Github\mac_apt\mac_apt.py -h
usage: mac_apt.py [-h] [-o OUTPUT_PATH] [-x] [-c] [-s] [-l LOG_LEVEL]
                  input_type input_path plugin [plugin ...]

mac_apt is a framework to process forensic artifacts on a Mac OSX system
You are running macOS Artifact Parsing Tool version 0.2.6

positional arguments:
  input_type            Specify Input type as either E01, DD or MOUNTED
  input_path            Path to OSX image/volume
  plugin                Plugins to run (space separated). 'ALL' will process every available plugin

optional arguments:
  -h, --help            show this help message and exit
  -o OUTPUT_PATH, --output_path OUTPUT_PATH
                        Path where output files will be created
  -x, --xlsx            Save output in excel spreadsheet(s)
  -c, --csv             Save output as CSV files (Default option if no output type selected)
  -s, --sqlite          Save output in an sqlite database
  -l LOG_LEVEL, --log level LOG_LEVEL
                        Log levels: INFO, DEBUG, WARNING, ERROR, CRITICAL (Default is INFO)

The following plugins are available:
    ALL                 Processes all plugins
    BASHSESSIONS        Reads bash (Terminal) sessions & history for every user
    BASICINFO           Gets basic machine and OS configuration like SN,
                        timezone, computer name, last logged in user, HFS info,
                        etc..
    DOCKITEMS           Parses Users Dock PList
    DOMAINS             Get information about ActiveDirectory Domain(s) that
```

Running mac_apt

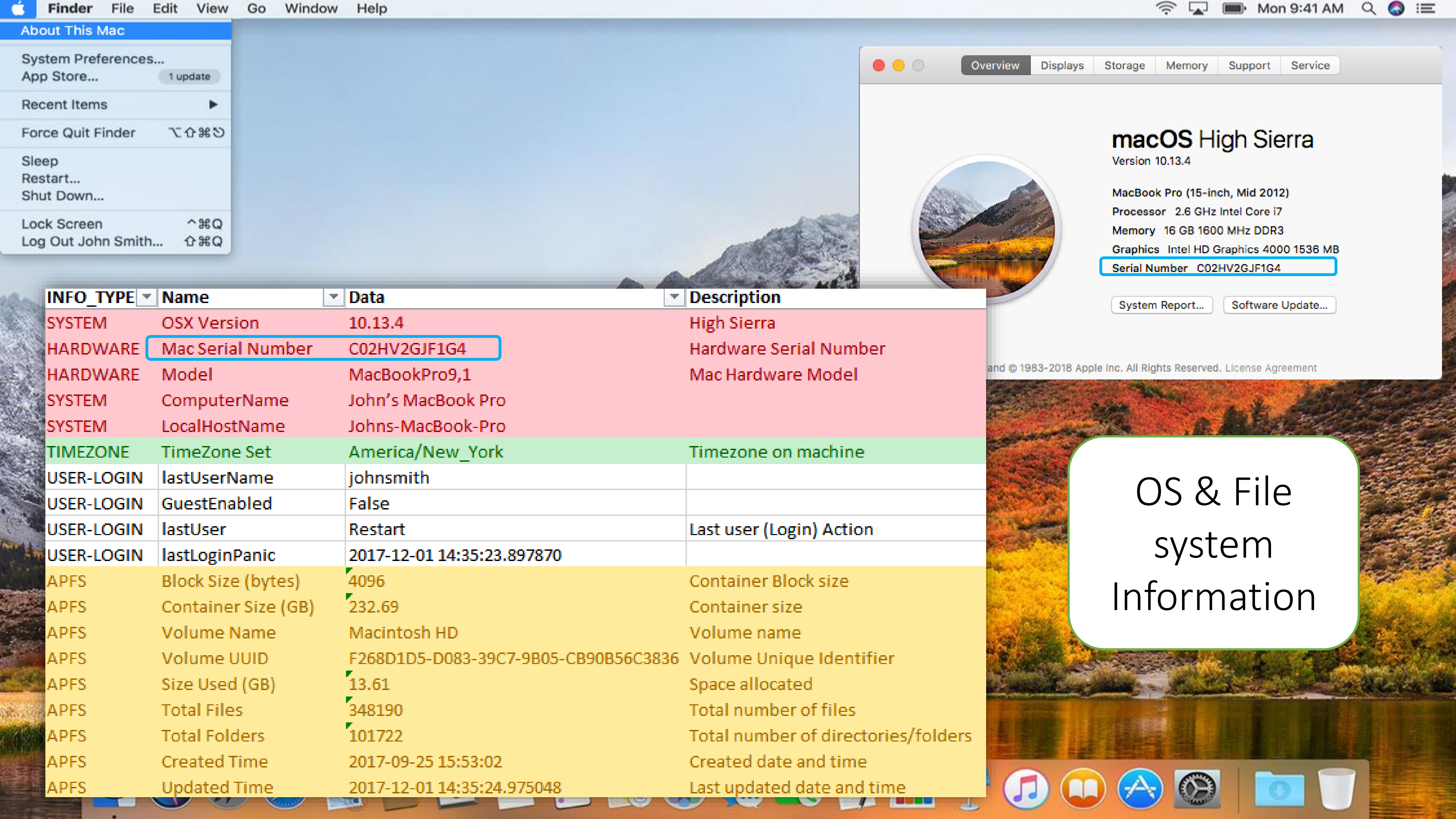
```
C:\>python.exe mac_apt.py -o c:\Output -s -x DD “D:\Mac Project\Images\HighSierra\HighSierra.dd” ALL
MAIN|INFO|Started macOS Artifact Parsing Tool, version 0.2.6
MAIN|INFO|Dates and times are in UTC unless the specific artifact being parsed saves it as local time!
MAIN|INFO|Pytsk version = 20160721
MAIN|INFO|Pyewf version = 20140608
MAIN|INFO|Opened image D:\Mac Project\Images\HighSierra\HighSierra.dd
MAIN|INFO|Looking at FS with volume label 'Untitled'  @ offset 209735680
MAIN|INFO|Found an APFS container with uuid: 405BD9B5-7303-44C1-9D77-EBD57DB77F5D
MAIN|INFO|Reading APFS volumes from container, this may take a few minutes ...
MAIN|INFO|Found valid OSX/macOS kernel
MAIN.HELPERS.MACINFO|INFO|OSX version detected is: High Sierra (10.13)
MAIN.DISK_REPORT|INFO|Disk info
MAIN.DISK_REPORT|INFO|Disk Size   = 232.89 GB (250059350016 bytes)
MAIN.DISK_REPORT|INFO|Part Scheme = GPT
MAIN.DISK_REPORT|INFO|Block size  = 512 bytes
MAIN.DISK_REPORT|INFO|Num Sectors = 488397168.0
MAIN|INFO|---------------------------------------------------
MAIN|INFO|Running plugin BASHSESSIONS
MAIN|INFO|---------------------------------------------------
MAIN|INFO|Running plugin BASICINFO
...
```

Output snippet



	A	B	E	G	J
1	node name	trustaccount	allow multi-domain	domain	source
2	/Active Directory/FOR420	snowys-imac$	1	for420.local	/Library/Preferences/OpenDirectory/Configurations/Active Directory/FOR420.plist
3					
4					

OS & File system Information



macOS High Sierra

Version 10.13.4

MacBook Pro (15-inch, Mid 2012)

Processor 2.6 GHz Intel Core i7

Memory 16 GB 1600 MHz DDR3

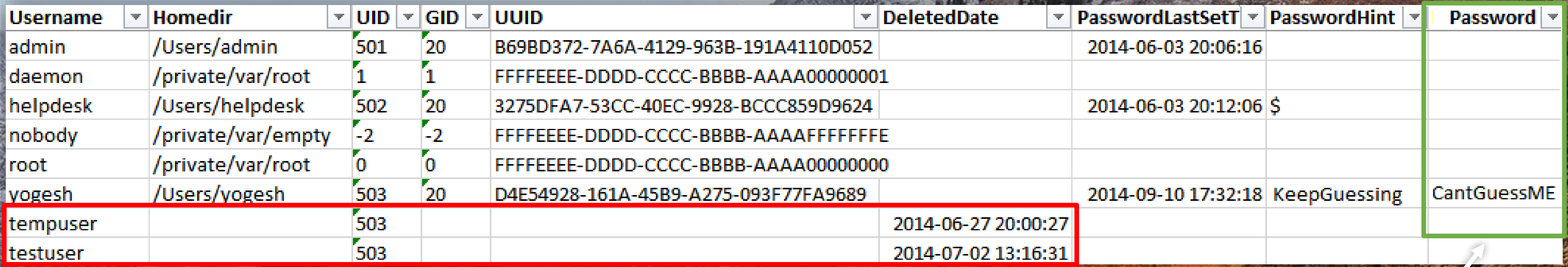
Graphics Intel HD Graphics 4000 1536 MB

Serial Number C02HV2GJF1G4

and © 1983-2018 Apple Inc. All Rights Reserved. License Agreement

INFO_TYPE	Name	Data	Description
SYSTEM	OSX Version	10.13.4	High Sierra
HARDWARE	Mac Serial Number	C02HV2GJF1G4	Hardware Serial Number
HARDWARE	Model	MacBookPro9,1	Mac Hardware Model
SYSTEM	ComputerName	John's MacBook Pro	
SYSTEM	LocalHostName	Johns-MacBook-Pro	
TIMEZONE	TimeZone Set	America/New_York	Timezone on machine
USER-LOGIN	lastUserName	johnsmith	
USER-LOGIN	GuestEnabled	False	
USER-LOGIN	lastUser	Restart	Last user (Login) Action
USER-LOGIN	lastLoginPanic	2017-12-01 14:35:23.897870	
APFS	Block Size (bytes)	4096	Container Block size
APFS	Container Size (GB)	232.69	Container size
APFS	Volume Name	Macintosh HD	Volume name
APFS	Volume UUID	F268D1D5-D083-39C7-9B05-CB90B56C3836	Volume Unique Identifier
APFS	Size Used (GB)	13.61	Space allocated
APFS	Total Files	348190	Total number of files
APFS	Total Folders	101722	Total number of directories/folders
APFS	Created Time	2017-09-25 15:53:02	Created date and time
APFS	Updated Time	2017-12-01 14:35:24.975048	Last updated date and time

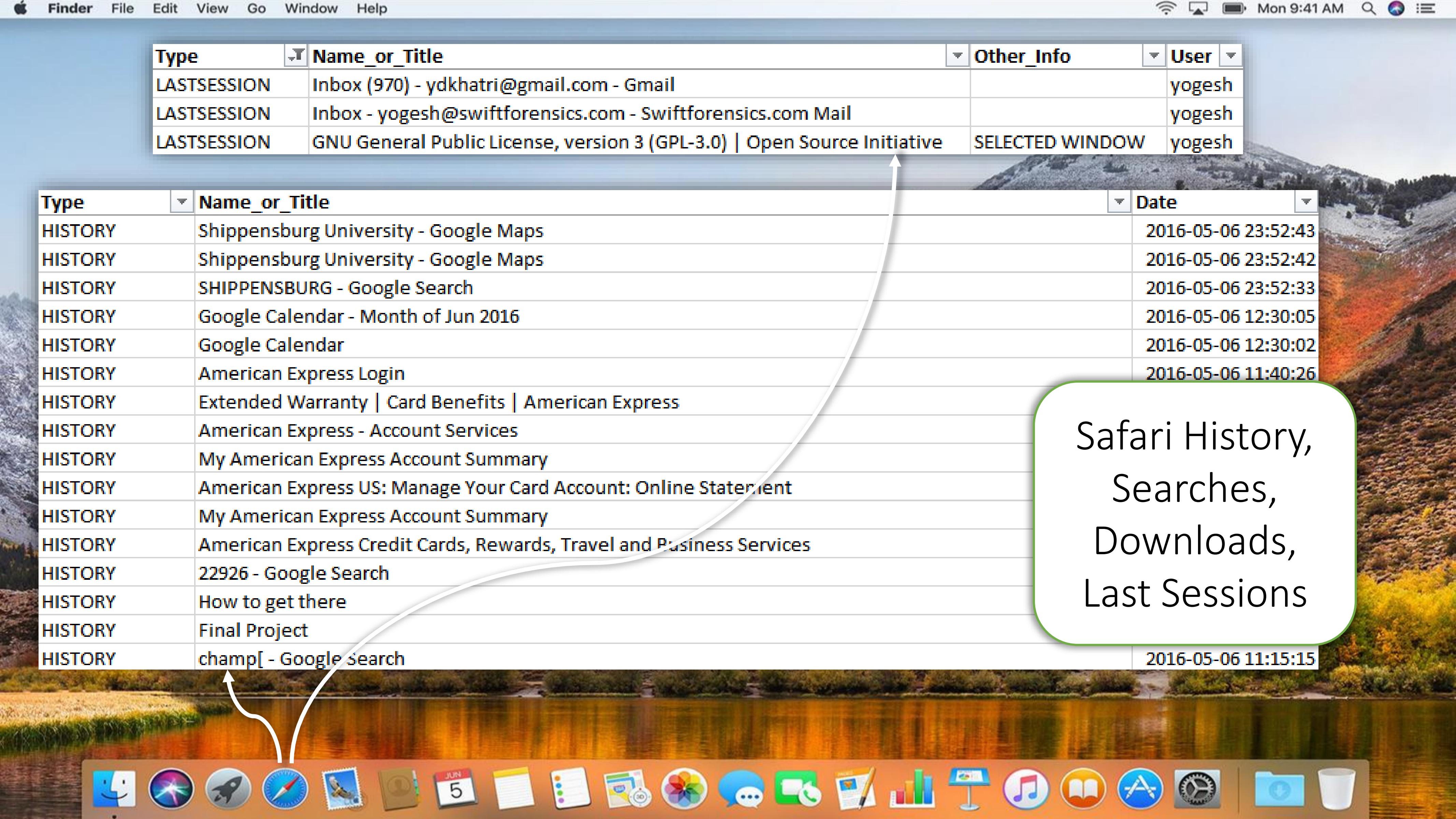
User Info



Username	Homedir	UID	GID	UUID	DeletedDate	PasswordLastSetT	PasswordHint	Password
admin	/Users/admin	501	20	B69BD372-7A6A-4129-963B-191A4110D052		2014-06-03 20:06:16		
daemon	/private/var/root	1	1	FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000001				
helpdesk	/Users/helpdesk	502	20	3275DFA7-53CC-40EC-9928-BCCC859D9624		2014-06-03 20:12:06	$	
nobody	/private/var/empty	-2	-2	FFFFEEEE-DDDD-CCCC-BBBB-AAAAFFFFFFFE				
root	/private/var/root	0	0	FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000000				
yogesh	/Users/yogesh	503	20	D4E54928-161A-45B9-A275-093F77FA9689		2014-09-10 17:32:18	KeepGuessing	CantGuessME
tempuser		503			2014-06-27 20:00:27			
testuser		503			2014-07-02 13:16:31			

Deleted users

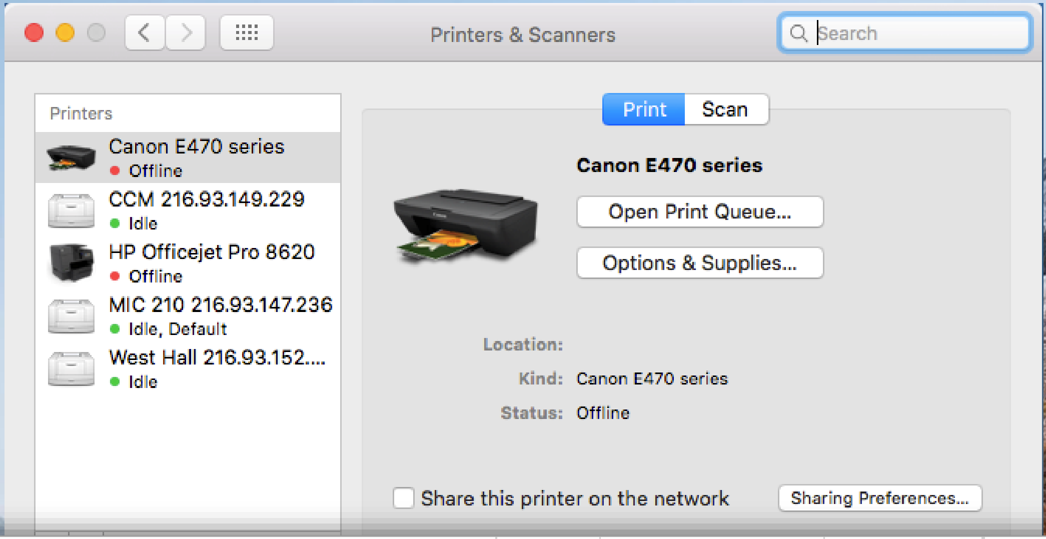
If Auto-login is set, password is stored in obfuscated form. mac_apt will retrieve and display it here.



Type	Name_or_Title	Other_Info	User
LASTSESSION	Inbox (970) - ydkhatri@gmail.com - Gmail		yogesh
LASTSESSION	Inbox - yogesh@swiftforensics.com - Swiftforensics.com Mail		yogesh
LASTSESSION	GNU General Public License, version 3 (GPL-3.0) | Open Source Initiative	SELECTED WINDOW	yogesh

Type	Name_or_Title	Date
HISTORY	Shippensburg University - Google Maps	2016-05-06 23:52:43
HISTORY	Shippensburg University - Google Maps	2016-05-06 23:52:42
HISTORY	SHIPPENSBURG - Google Search	2016-05-06 23:52:33
HISTORY	Google Calendar - Month of Jun 2016	2016-05-06 12:30:05
HISTORY	Google Calendar	2016-05-06 12:30:02
HISTORY	American Express Login	2016-05-06 11:40:26
HISTORY	Extended Warranty | Card Benefits | American Express	
HISTORY	American Express - Account Services	
HISTORY	My American Express Account Summary	
HISTORY	American Express US: Manage Your Card Account: Online Statement	
HISTORY	My American Express Account Summary	
HISTORY	American Express Credit Cards, Rewards, Travel and Business Services	
HISTORY	22926 - Google Search	
HISTORY	How to get there	
HISTORY	Final Project	
HISTORY	champ[- Google Search	2016-05-06 11:15:15

Safari History, Searches, Downloads, Last Sessions



Printers

- Canon E470 series — Offline
- CCM 216.93.149.229 — Idle
- HP Officejet Pro 8620 — Offline
- MIC 210 216.93.147.236 — Idle, Default
- West Hall 216.93.152.... — Idle

Canon E470 series

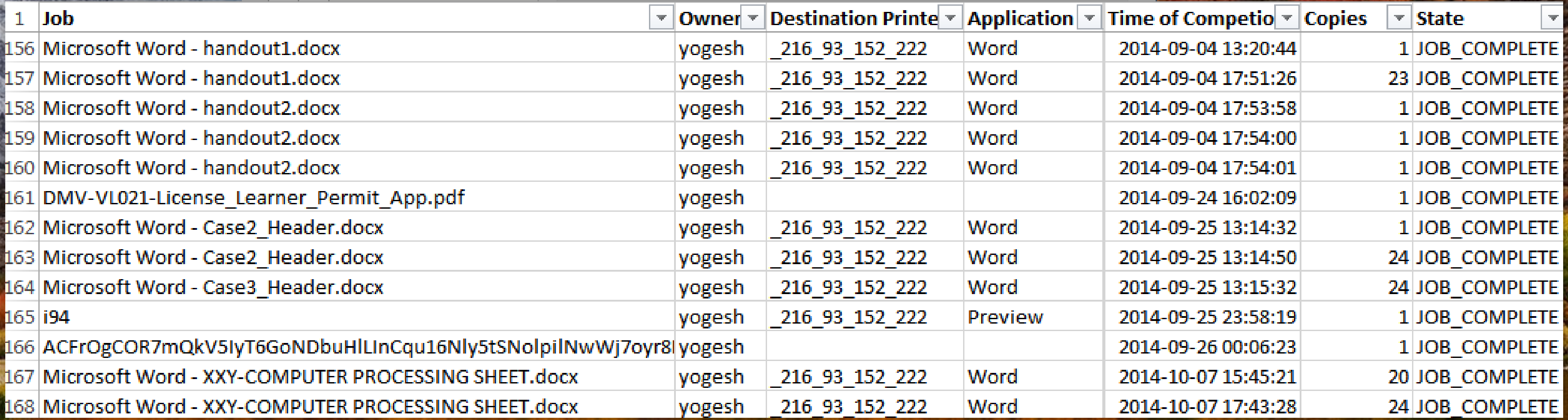
Location:

Kind: Canon E470 series

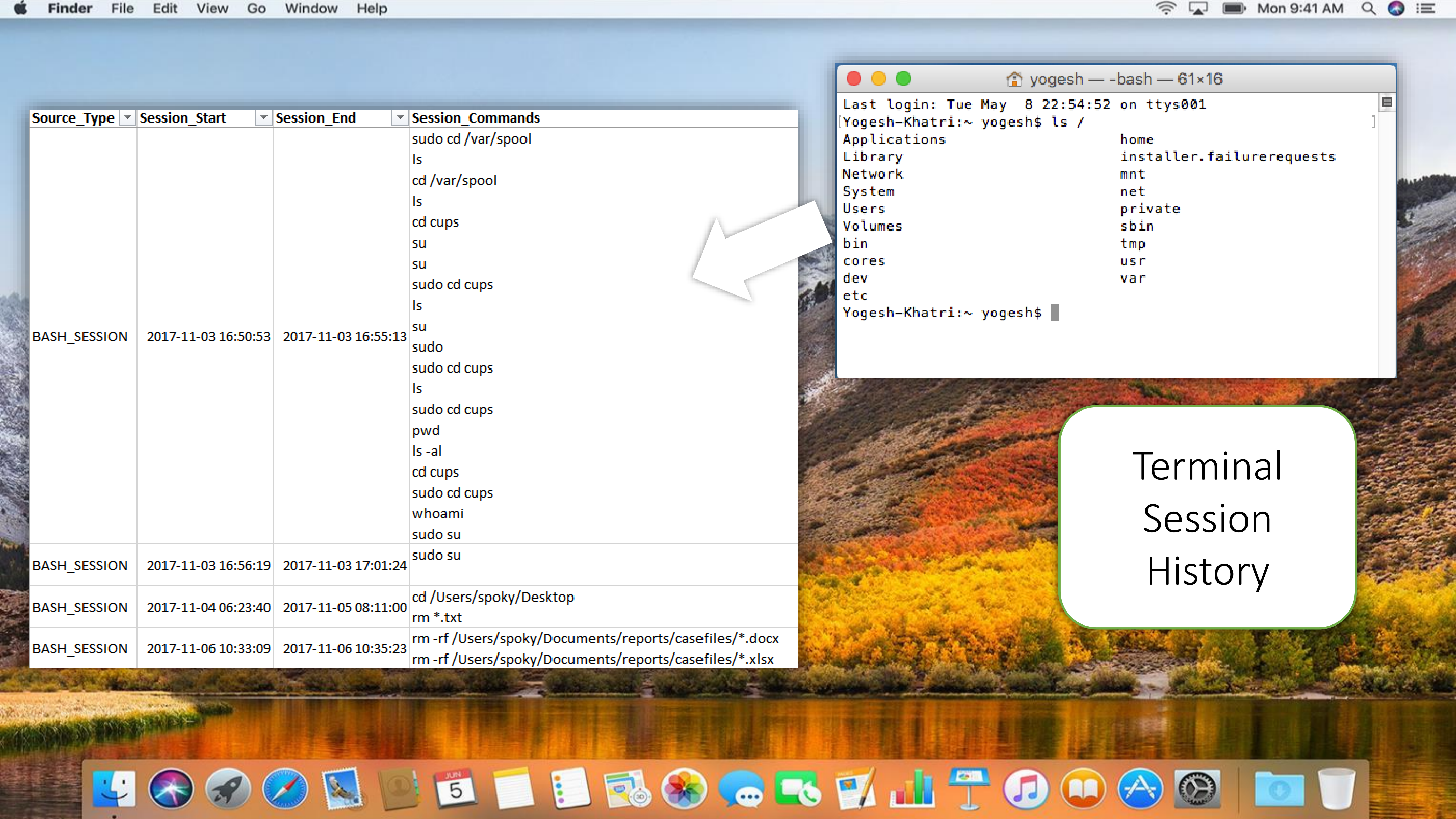
Status: Offline

□ Share this printer on the network

Print Job History



1	Job	Owner	Destination Printe	Application	Time of Competio	Copies	State
156	Microsoft Word - handout1.docx	yogesh	_216_93_152_222	Word	2014-09-04 13:20:44	1	JOB_COMPLETE
157	Microsoft Word - handout1.docx	yogesh	_216_93_152_222	Word	2014-09-04 17:51:26	23	JOB_COMPLETE
158	Microsoft Word - handout2.docx	yogesh	_216_93_152_222	Word	2014-09-04 17:53:58	1	JOB_COMPLETE
159	Microsoft Word - handout2.docx	yogesh	_216_93_152_222	Word	2014-09-04 17:54:00	1	JOB_COMPLETE
160	Microsoft Word - handout2.docx	yogesh	_216_93_152_222	Word	2014-09-04 17:54:01	1	JOB_COMPLETE
161	DMV-VL021-License_Learner_Permit_App.pdf	yogesh			2014-09-24 16:02:09	1	JOB_COMPLETE
162	Microsoft Word - Case2_Header.docx	yogesh	_216_93_152_222	Word	2014-09-25 13:14:32	1	JOB_COMPLETE
163	Microsoft Word - Case2_Header.docx	yogesh	_216_93_152_222	Word	2014-09-25 13:14:50	24	JOB_COMPLETE
164	Microsoft Word - Case3_Header.docx	yogesh	_216_93_152_222	Word	2014-09-25 13:15:32	24	JOB_COMPLETE
165	i94	yogesh	_216_93_152_222	Preview	2014-09-25 23:58:19	1	JOB_COMPLETE
166	ACFrOgCOR7mQkV5IyT6GoNDbuHlLInCqu16Nly5tSNolpilNwWj7oyr8l	yogesh			2014-09-26 00:06:23	1	JOB_COMPLETE
167	Microsoft Word - XXY-COMPUTER PROCESSING SHEET.docx	yogesh	_216_93_152_222	Word	2014-10-07 15:45:21	20	JOB_COMPLETE
168	Microsoft Word - XXY-COMPUTER PROCESSING SHEET.docx	yogesh	_216_93_152_222	Word	2014-10-07 17:43:28	24	JOB_COMPLETE

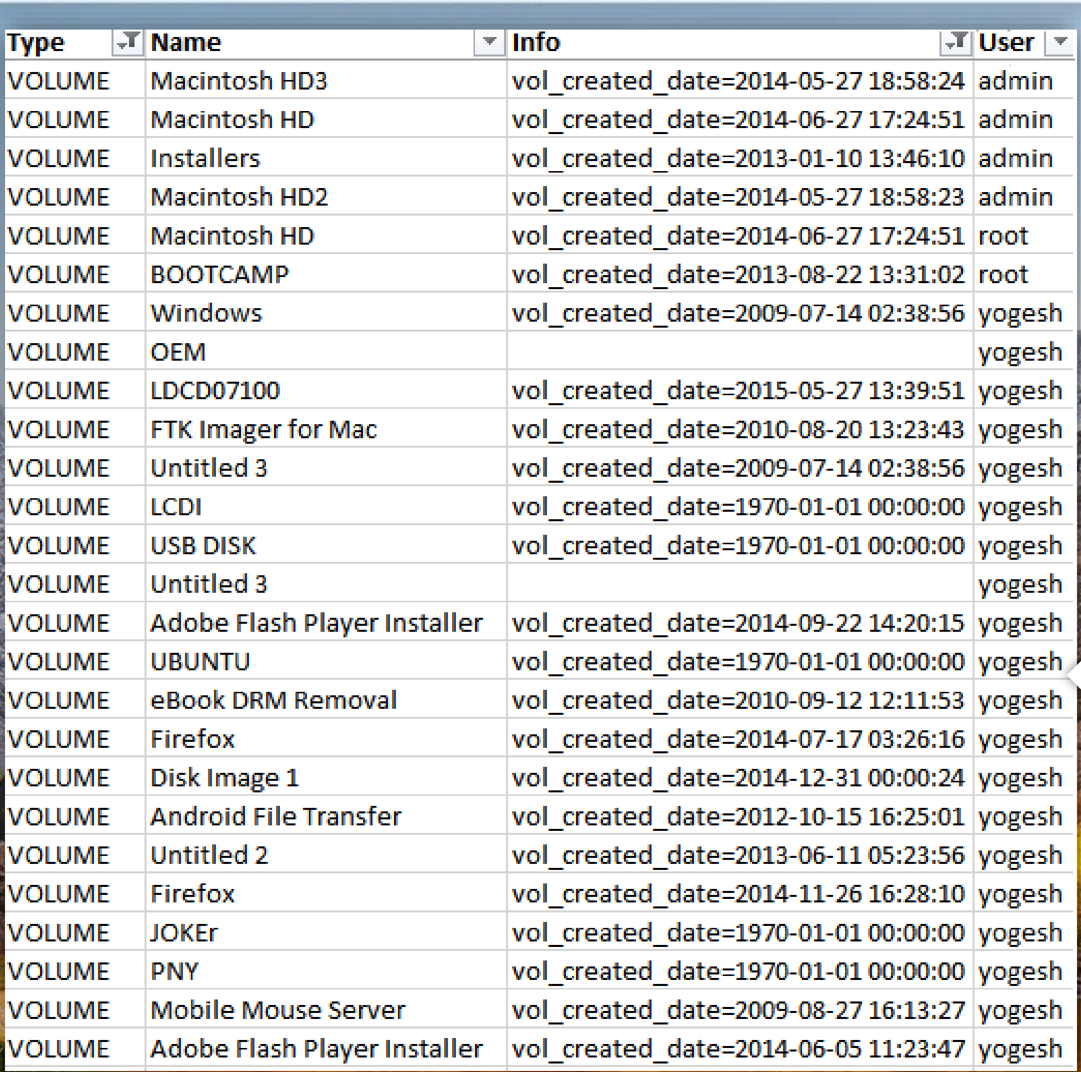


Terminal Session History

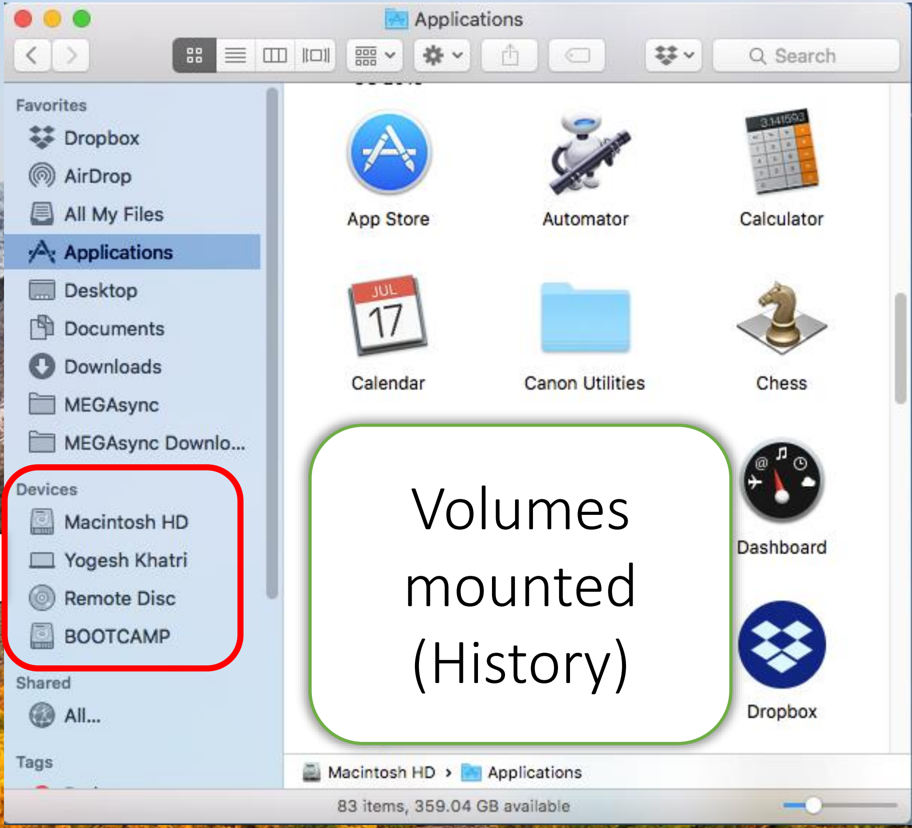
Source_Type	Session_Start	Session_End	Session_Commands
BASH_SESSION	2017-11-03 16:50:53	2017-11-03 16:55:13	sudo cd /var/spool ls cd /var/spool ls cd cups su su sudo cd cups ls su sudo sudo cd cups ls sudo cd cups pwd ls -al cd cups sudo cd cups whoami sudo su
BASH_SESSION	2017-11-03 16:56:19	2017-11-03 17:01:24	sudo su
BASH_SESSION	2017-11-04 06:23:40	2017-11-05 08:11:00	cd /Users/spoky/Desktop rm *.txt
BASH_SESSION	2017-11-06 10:33:09	2017-11-06 10:35:23	rm -rf /Users/spoky/Documents/reports/casefiles/*.docx rm -rf /Users/spoky/Documents/reports/casefiles/*.xlsx

yogesh — -bash — 61×16

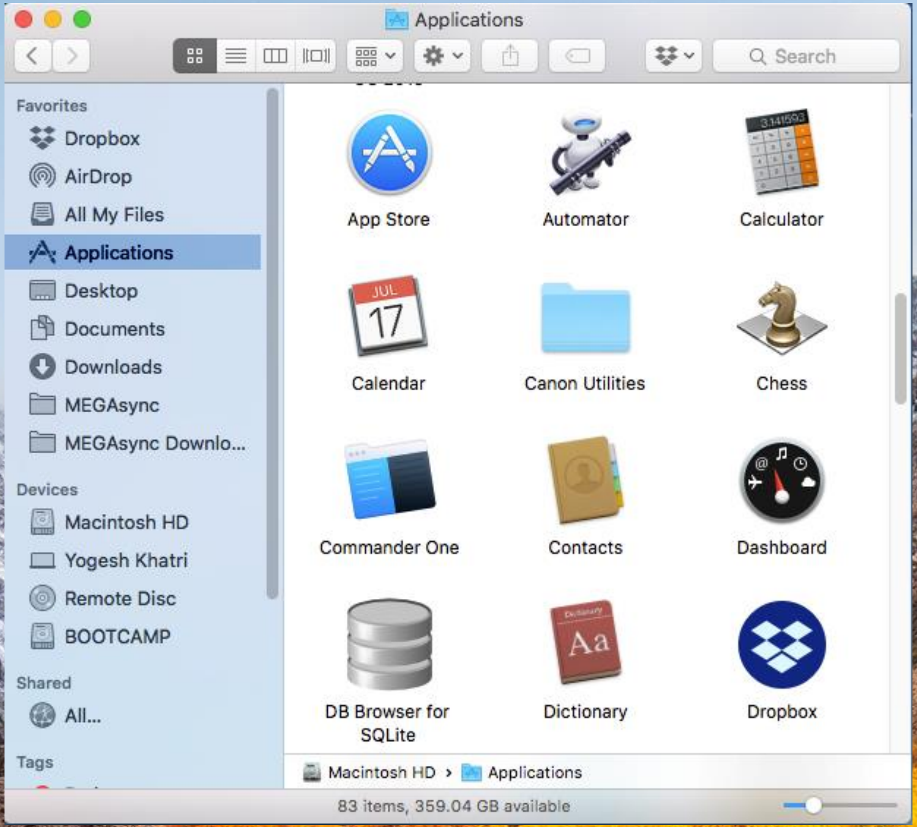
```
Last login: Tue May  8 22:54:52 on ttys001
Yogesh-Khatri:~ yogesh$ ls /
Applications                    home
Library                         installer.failurerequests
Network                         mnt
System                          net
Users                           private
Volumes                         sbin
bin                             tmp
cores                           usr
dev                             var
etc
Yogesh-Khatri:~ yogesh$ 
```

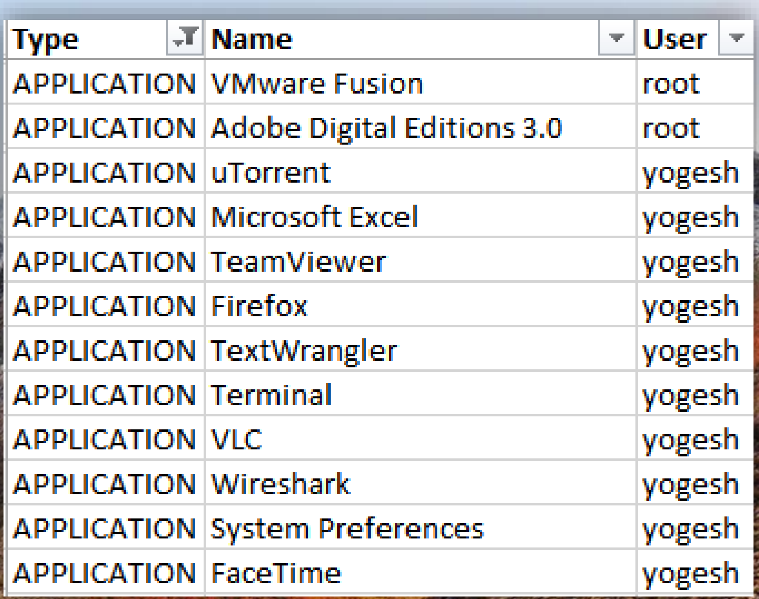


Type	Name	Info	User
VOLUME	Macintosh HD3	vol_created_date=2014-05-27 18:58:24	admin
VOLUME	Macintosh HD	vol_created_date=2014-06-27 17:24:51	admin
VOLUME	Installers	vol_created_date=2013-01-10 13:46:10	admin
VOLUME	Macintosh HD2	vol_created_date=2014-05-27 18:58:23	admin
VOLUME	Macintosh HD	vol_created_date=2014-06-27 17:24:51	root
VOLUME	BOOTCAMP	vol_created_date=2013-08-22 13:31:02	root
VOLUME	Windows	vol_created_date=2009-07-14 02:38:56	yogesh
VOLUME	OEM		yogesh
VOLUME	LDCD07100	vol_created_date=2015-05-27 13:39:51	yogesh
VOLUME	FTK Imager for Mac	vol_created_date=2010-08-20 13:23:43	yogesh
VOLUME	Untitled 3	vol_created_date=2009-07-14 02:38:56	yogesh
VOLUME	LCDI	vol_created_date=1970-01-01 00:00:00	yogesh
VOLUME	USB DISK	vol_created_date=1970-01-01 00:00:00	yogesh
VOLUME	Untitled 3		yogesh
VOLUME	Adobe Flash Player Installer	vol_created_date=2014-09-22 14:20:15	yogesh
VOLUME	UBUNTU	vol_created_date=1970-01-01 00:00:00	yogesh
VOLUME	eBook DRM Removal	vol_created_date=2010-09-12 12:11:53	yogesh
VOLUME	Firefox	vol_created_date=2014-07-17 03:26:16	yogesh
VOLUME	Disk Image 1	vol_created_date=2014-12-31 00:00:24	yogesh
VOLUME	Android File Transfer	vol_created_date=2012-10-15 16:25:01	yogesh
VOLUME	Untitled 2	vol_created_date=2013-06-11 05:23:56	yogesh
VOLUME	Firefox	vol_created_date=2014-11-26 16:28:10	yogesh
VOLUME	JOKEr	vol_created_date=1970-01-01 00:00:00	yogesh
VOLUME	PNY	vol_created_date=1970-01-01 00:00:00	yogesh
VOLUME	Mobile Mouse Server	vol_created_date=2009-08-27 16:13:27	yogesh
VOLUME	Adobe Flash Player Installer	vol_created_date=2014-06-05 11:23:47	yogesh



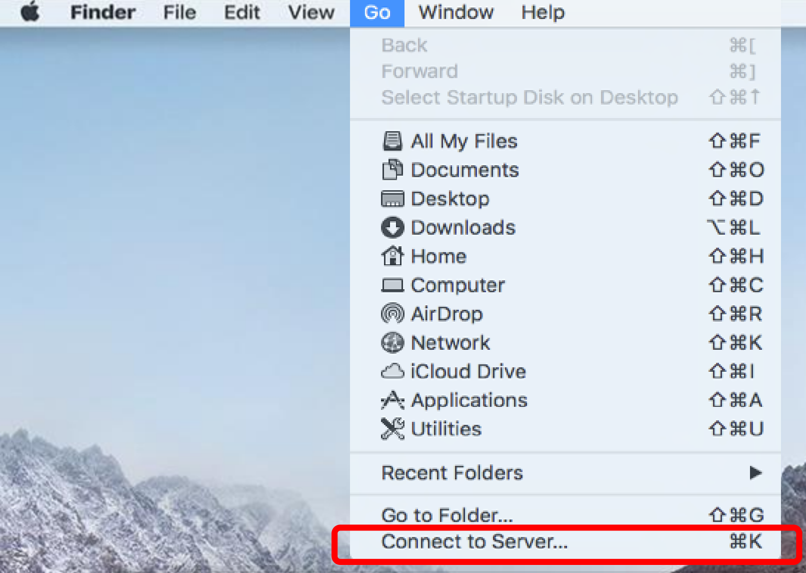
Volumes mounted (History)





Type	Name	User
APPLICATION	VMware Fusion	root
APPLICATION	Adobe Digital Editions 3.0	root
APPLICATION	uTorrent	yogesh
APPLICATION	Microsoft Excel	yogesh
APPLICATION	TeamViewer	yogesh
APPLICATION	Firefox	yogesh
APPLICATION	TextWrangler	yogesh
APPLICATION	Terminal	yogesh
APPLICATION	VLC	yogesh
APPLICATION	Wireshark	yogesh
APPLICATION	System Preferences	yogesh
APPLICATION	FaceTime	yogesh

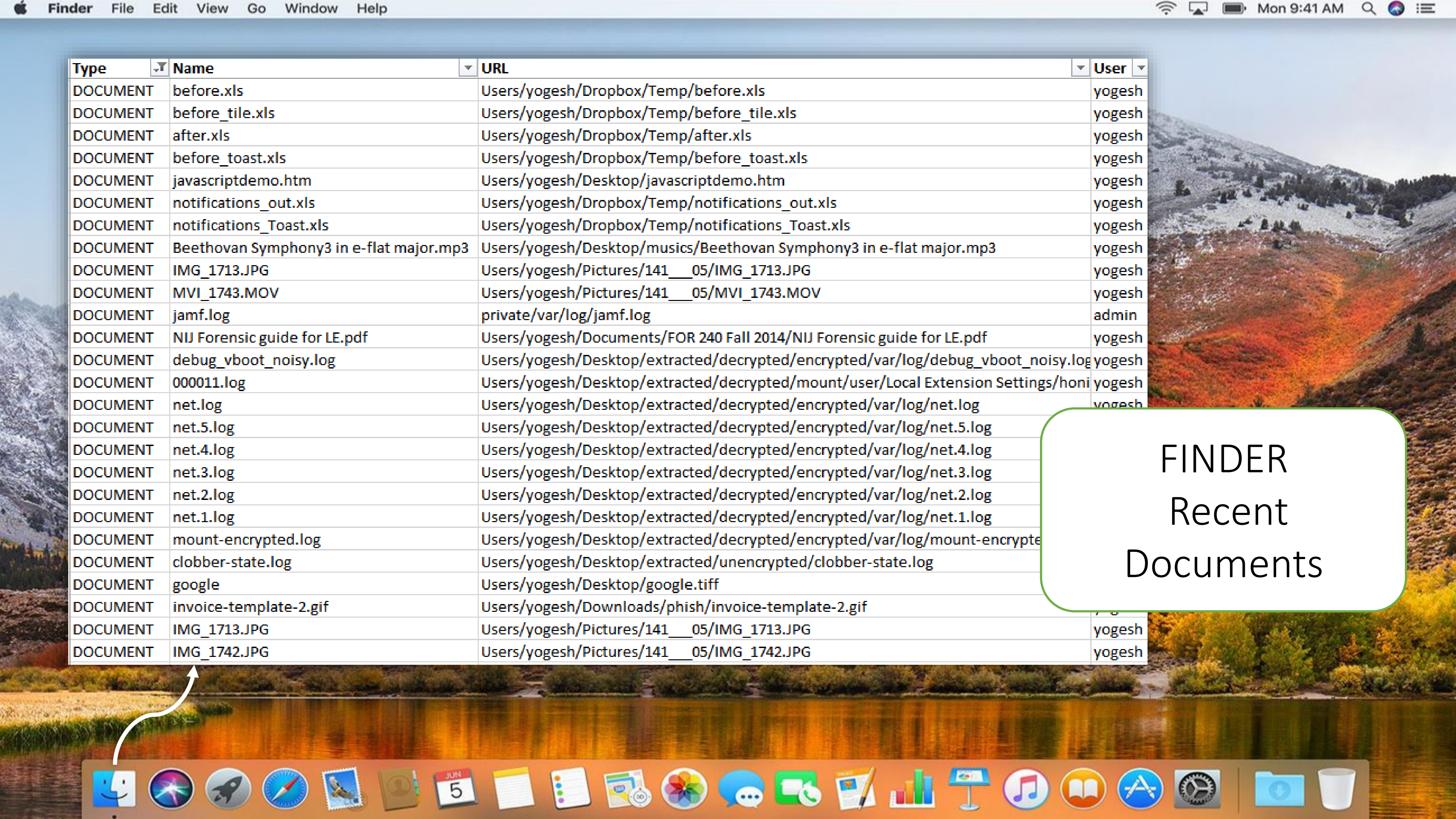
Applications used recently



Type	Name	User
HOST	cosmos.champlain.edu	yogesh
HOST	192.168.0.12	yogesh
HOST	mansarovar	yogesh
HOST	readyshare	yogesh
HOST	192.168.191.193	yogesh
HOST	216.93.147.35	yogesh
HOST	saturn	yogesh
HOST	192.168.0.11	yogesh

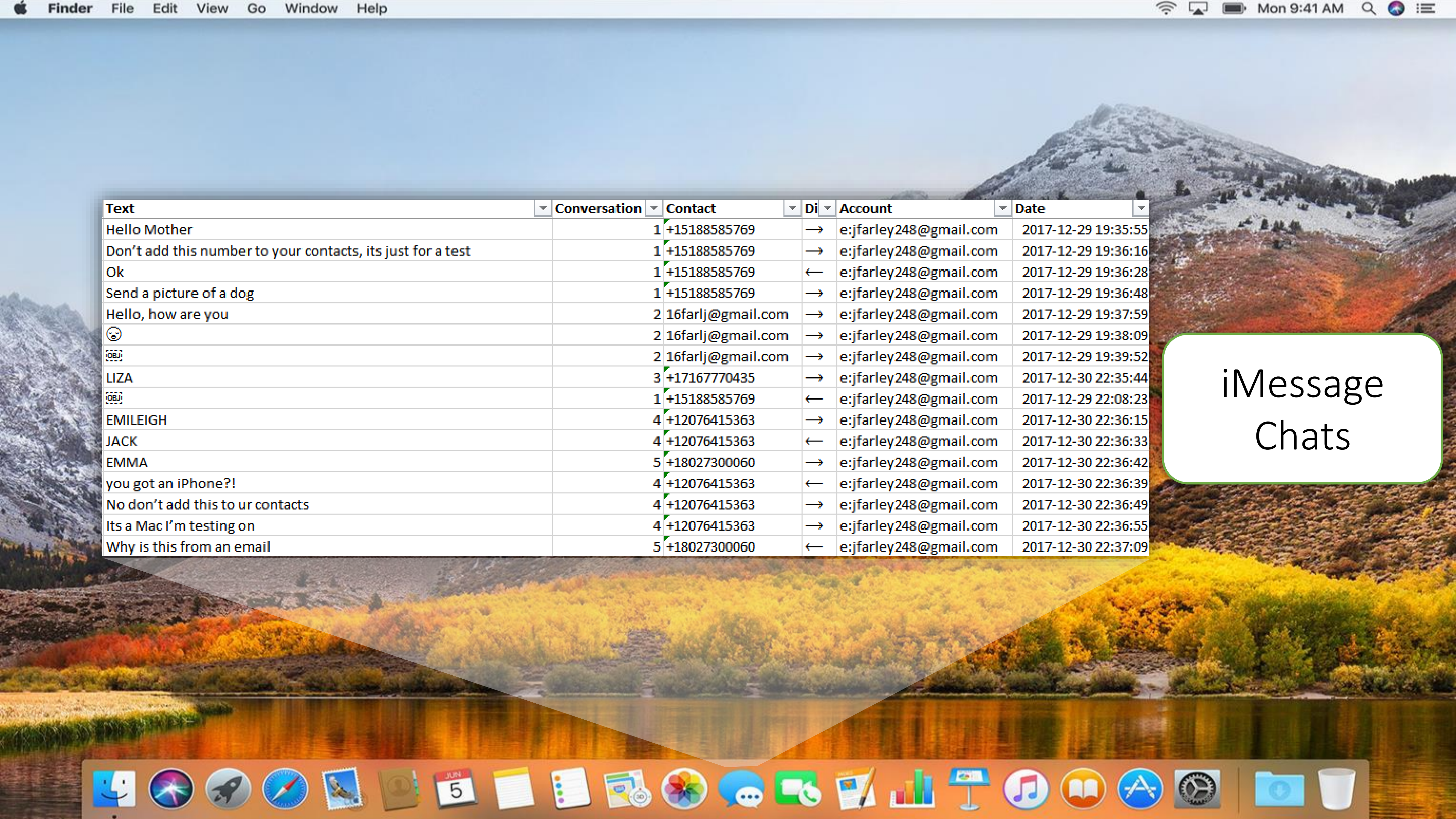
Type	Name	URL
SERVER	khatri	smb://Khatri@cosmos.champlain.edu/studentshared/khatri
SERVER	AdminHome	smb://Khatri@cosmos.champlain.edu/AdminHome
SERVER	StudentShared	smb://Khatri@cosmos.champlain.edu/StudentShared
SERVER	SD Card	smb://GUEST:@192.168.0.12:7777/SD%20Card
SERVER	external_SD	smb://GUEST@192.168.0.12:7777/external_SD
SERVER	yogesh	smb://GUEST:@mansarovar/yogesh
SERVER	USB_Storage	smb://GUEST:@readyshare/USB_Storage
SERVER	frank@192.168.191.193	ftp://frank@192.168.191.193/
SERVER	c$	smb://khatri@216.93.147.35/c$
SERVER	WebDirs	smb://Khatri@cosmos.champlain.edu/WebDirs
SERVER		smb://cosmos.champlain.edu/studentshared/khatri
SERVER	smb://cosmos.champlain.edu/studentshared/khatri	smb://cosmos.champlain.edu/studentshared/khatri
SERVER	smb://192.168.0.12:7777/SD Card	smb://192.168.0.12:7777/SD%20Card
SERVER	smb://192.168.0.11	smb://192.168.0.11
SERVER	smb://cosmos.champlain.edu	smb://cosmos.champlain.edu

Recent Hosts & Servers Accessed



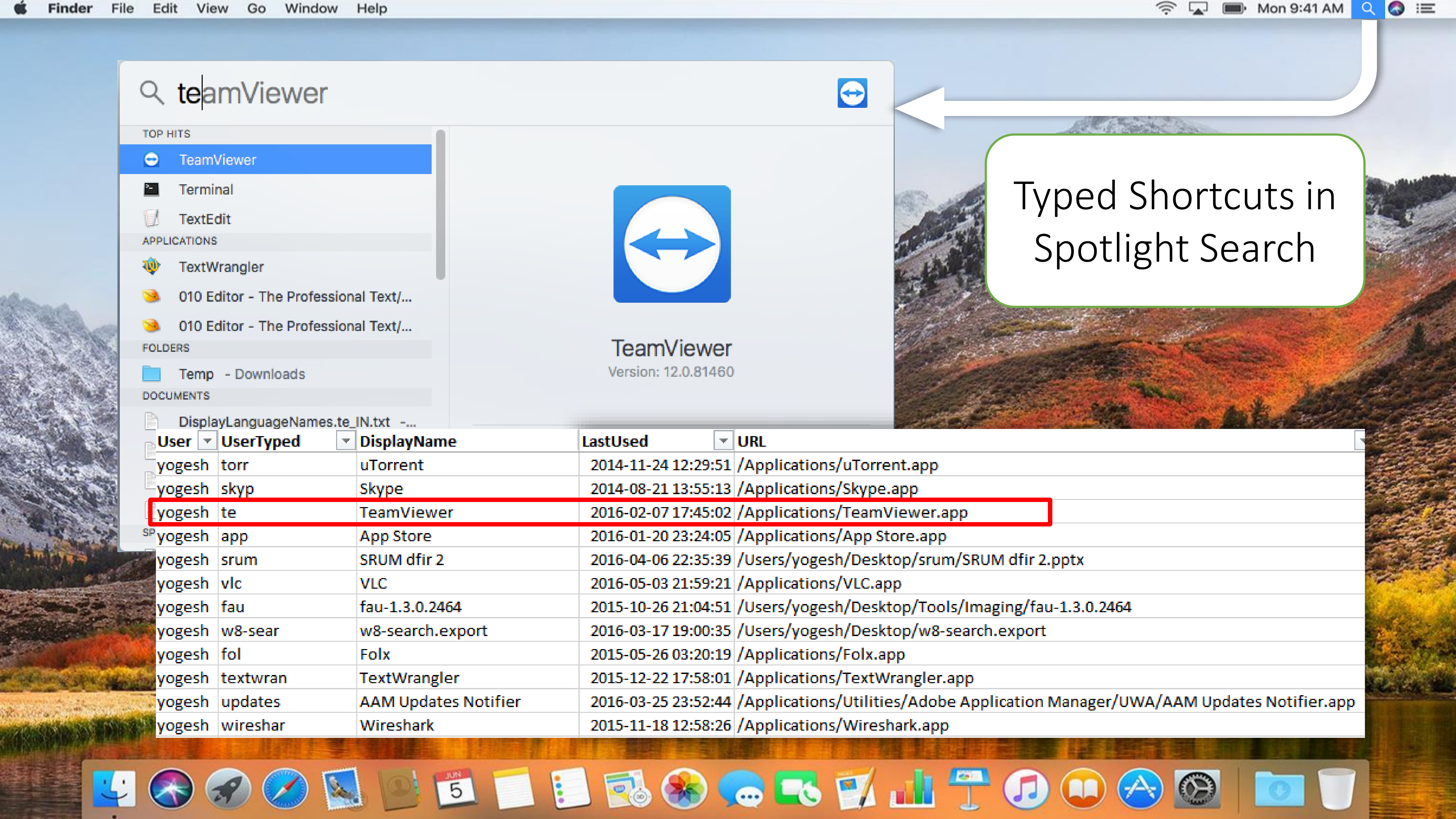
Type	Name	URL	User
DOCUMENT	before.xls	Users/yogesh/Dropbox/Temp/before.xls	yogesh
DOCUMENT	before_tile.xls	Users/yogesh/Dropbox/Temp/before_tile.xls	yogesh
DOCUMENT	after.xls	Users/yogesh/Dropbox/Temp/after.xls	yogesh
DOCUMENT	before_toast.xls	Users/yogesh/Dropbox/Temp/before_toast.xls	yogesh
DOCUMENT	javascriptdemo.htm	Users/yogesh/Desktop/javascriptdemo.htm	yogesh
DOCUMENT	notifications_out.xls	Users/yogesh/Dropbox/Temp/notifications_out.xls	yogesh
DOCUMENT	notifications_Toast.xls	Users/yogesh/Dropbox/Temp/notifications_Toast.xls	yogesh
DOCUMENT	Beethovan Symphony3 in e-flat major.mp3	Users/yogesh/Desktop/musics/Beethovan Symphony3 in e-flat major.mp3	yogesh
DOCUMENT	IMG_1713.JPG	Users/yogesh/Pictures/141___05/IMG_1713.JPG	yogesh
DOCUMENT	MVI_1743.MOV	Users/yogesh/Pictures/141___05/MVI_1743.MOV	yogesh
DOCUMENT	jamf.log	private/var/log/jamf.log	admin
DOCUMENT	NIJ Forensic guide for LE.pdf	Users/yogesh/Documents/FOR 240 Fall 2014/NIJ Forensic guide for LE.pdf	yogesh
DOCUMENT	debug_vboot_noisy.log	Users/yogesh/Desktop/extracted/decrypted/encrypted/var/log/debug_vboot_noisy.log	yogesh
DOCUMENT	000011.log	Users/yogesh/Desktop/extracted/decrypted/mount/user/Local Extension Settings/honi	yogesh
DOCUMENT	net.log	Users/yogesh/Desktop/extracted/decrypted/encrypted/var/log/net.log	yogesh
DOCUMENT	net.5.log	Users/yogesh/Desktop/extracted/decrypted/encrypted/var/log/net.5.log	
DOCUMENT	net.4.log	Users/yogesh/Desktop/extracted/decrypted/encrypted/var/log/net.4.log	
DOCUMENT	net.3.log	Users/yogesh/Desktop/extracted/decrypted/encrypted/var/log/net.3.log	
DOCUMENT	net.2.log	Users/yogesh/Desktop/extracted/decrypted/encrypted/var/log/net.2.log	
DOCUMENT	net.1.log	Users/yogesh/Desktop/extracted/decrypted/encrypted/var/log/net.1.log	
DOCUMENT	mount-encrypted.log	Users/yogesh/Desktop/extracted/decrypted/encrypted/var/log/mount-encrypte	
DOCUMENT	clobber-state.log	Users/yogesh/Desktop/extracted/unencrypted/clobber-state.log	
DOCUMENT	google	Users/yogesh/Desktop/google.tiff	
DOCUMENT	invoice-template-2.gif	Users/yogesh/Downloads/phish/invoice-template-2.gif	
DOCUMENT	IMG_1713.JPG	Users/yogesh/Pictures/141___05/IMG_1713.JPG	yogesh
DOCUMENT	IMG_1742.JPG	Users/yogesh/Pictures/141___05/IMG_1742.JPG	yogesh

FINDER
Recent
Documents



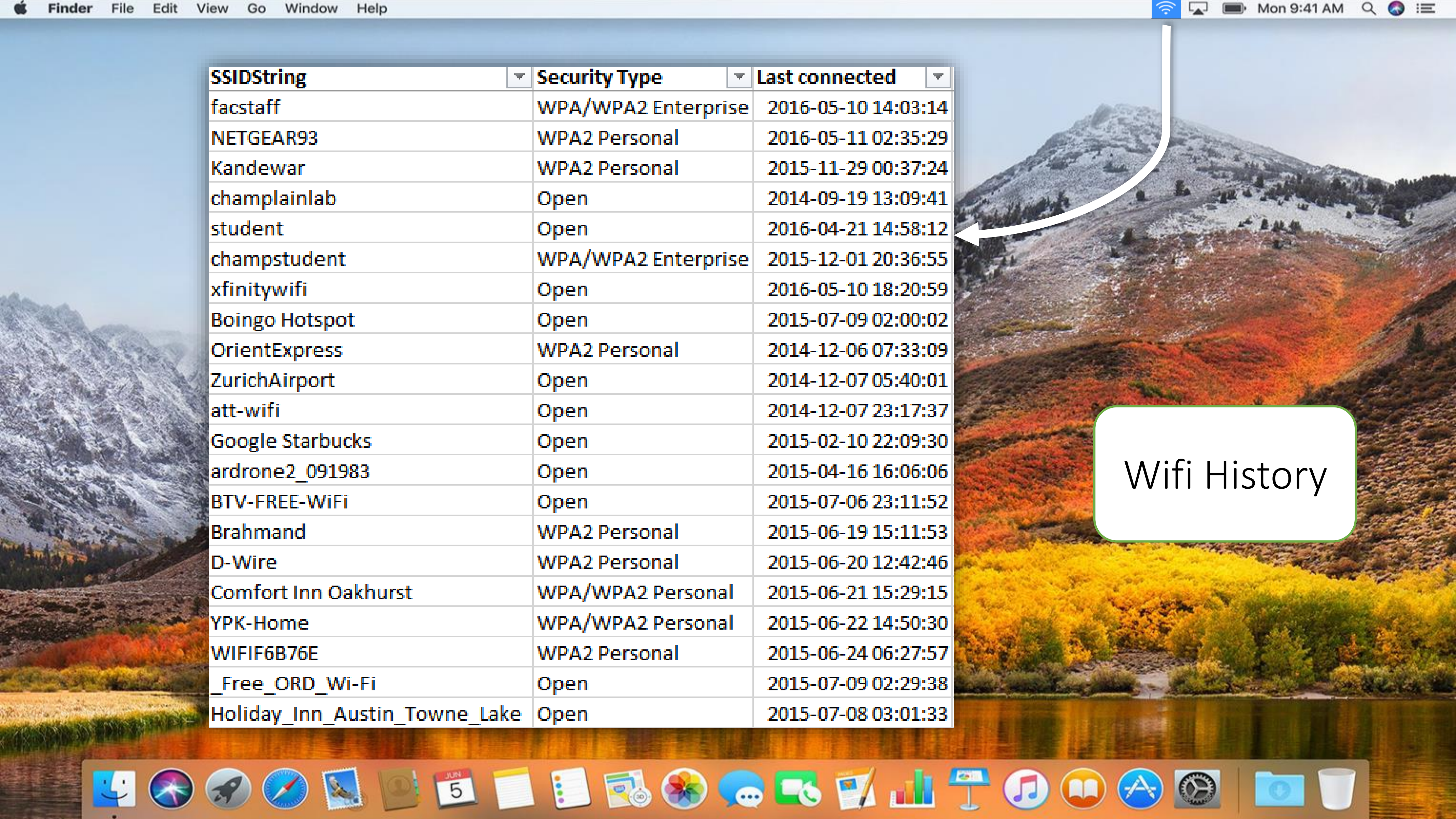
Text	Conversation	Contact	Di	Account	Date
Hello Mother	1	+15188585769	→	e:jfarley248@gmail.com	2017-12-29 19:35:55
Don’t add this number to your contacts, its just for a test	1	+15188585769	→	e:jfarley248@gmail.com	2017-12-29 19:36:16
Ok	1	+15188585769	←	e:jfarley248@gmail.com	2017-12-29 19:36:28
Send a picture of a dog	1	+15188585769	→	e:jfarley248@gmail.com	2017-12-29 19:36:48
Hello, how are you	2	16farlj@gmail.com	→	e:jfarley248@gmail.com	2017-12-29 19:37:59
😧	2	16farlj@gmail.com	→	e:jfarley248@gmail.com	2017-12-29 19:38:09
￼	2	16farlj@gmail.com	→	e:jfarley248@gmail.com	2017-12-29 19:39:52
LIZA	3	+17167770435	→	e:jfarley248@gmail.com	2017-12-30 22:35:44
￼	1	+15188585769	←	e:jfarley248@gmail.com	2017-12-29 22:08:23
EMILEIGH	4	+12076415363	→	e:jfarley248@gmail.com	2017-12-30 22:36:15
JACK	4	+12076415363	←	e:jfarley248@gmail.com	2017-12-30 22:36:33
EMMA	5	+18027300060	→	e:jfarley248@gmail.com	2017-12-30 22:36:42
you got an iPhone?!	4	+12076415363	←	e:jfarley248@gmail.com	2017-12-30 22:36:39
No don’t add this to ur contacts	4	+12076415363	→	e:jfarley248@gmail.com	2017-12-30 22:36:49
Its a Mac I’m testing on	4	+12076415363	→	e:jfarley248@gmail.com	2017-12-30 22:36:55
Why is this from an email	5	+18027300060	←	e:jfarley248@gmail.com	2017-12-30 22:37:09

iMessage Chats


Finder File Edit View Go Window Help
Mon 9:41 AM
teamViewer
TOP HITS
TeamViewer
Terminal
TextEdit
APPLICATIONS
TextWrangler
010 Editor - The Professional Text/...
010 Editor - The Professional Text/...
FOLDERS
Temp - Downloads
DOCUMENTS
DisplayLanguageNames.te_IN.txt -...
TeamViewer
Version: 12.0.81460

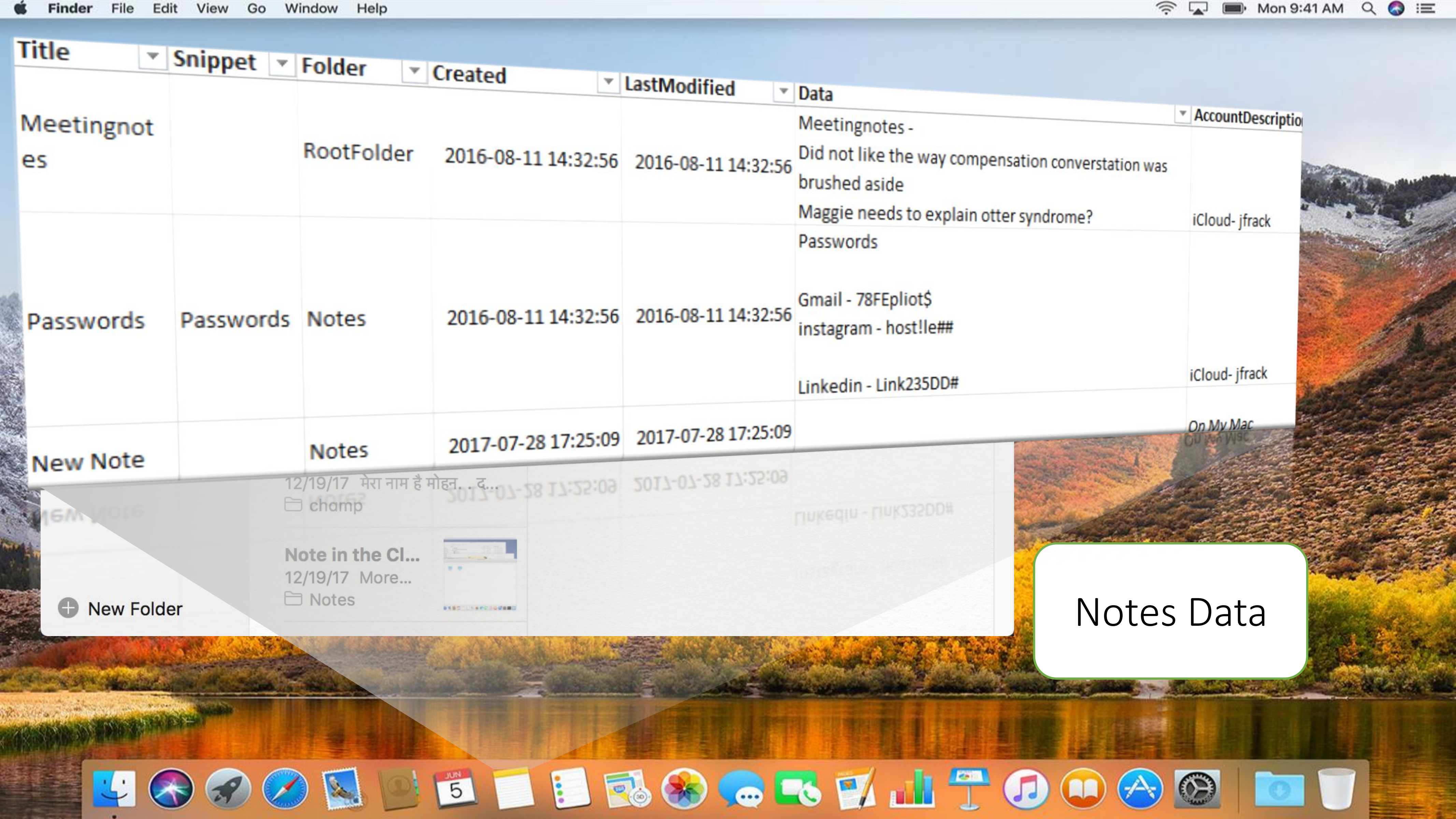
Typed Shortcuts in Spotlight Search

User	UserTyped	DisplayName	LastUsed	URL
yogesh	torr	uTorrent	2014-11-24 12:29:51	/Applications/uTorrent.app
yogesh	skyp	Skype	2014-08-21 13:55:13	/Applications/Skype.app
yogesh	te	TeamViewer	2016-02-07 17:45:02	/Applications/TeamViewer.app
yogesh	app	App Store	2016-01-20 23:24:05	/Applications/App Store.app
yogesh	srum	SRUM dfir 2	2016-04-06 22:35:39	/Users/yogesh/Desktop/srum/SRUM dfir 2.pptx
yogesh	vlc	VLC	2016-05-03 21:59:21	/Applications/VLC.app
yogesh	fau	fau-1.3.0.2464	2015-10-26 21:04:51	/Users/yogesh/Desktop/Tools/Imaging/fau-1.3.0.2464
yogesh	w8-sear	w8-search.export	2016-03-17 19:00:35	/Users/yogesh/Desktop/w8-search.export
yogesh	fol	Folx	2015-05-26 03:20:19	/Applications/Folx.app
yogesh	textwran	TextWrangler	2015-12-22 17:58:01	/Applications/TextWrangler.app
yogesh	updates	AAM Updates Notifier	2016-03-25 23:52:44	/Applications/Utilities/Adobe Application Manager/UWA/AAM Updates Notifier.app
yogesh	wireshar	Wireshark	2015-11-18 12:58:26	/Applications/Wireshark.app



SSIDString	Security Type	Last connected
facstaff	WPA/WPA2 Enterprise	2016-05-10 14:03:14
NETGEAR93	WPA2 Personal	2016-05-11 02:35:29
Kandewar	WPA2 Personal	2015-11-29 00:37:24
champlainlab	Open	2014-09-19 13:09:41
student	Open	2016-04-21 14:58:12
champstudent	WPA/WPA2 Enterprise	2015-12-01 20:36:55
xfinitywifi	Open	2016-05-10 18:20:59
Boingo Hotspot	Open	2015-07-09 02:00:02
OrientExpress	WPA2 Personal	2014-12-06 07:33:09
ZurichAirport	Open	2014-12-07 05:40:01
att-wifi	Open	2014-12-07 23:17:37
Google Starbucks	Open	2015-02-10 22:09:30
ardrone2_091983	Open	2015-04-16 16:06:06
BTV-FREE-WiFi	Open	2015-07-06 23:11:52
Brahmand	WPA2 Personal	2015-06-19 15:11:53
D-Wire	WPA2 Personal	2015-06-20 12:42:46
Comfort Inn Oakhurst	WPA/WPA2 Personal	2015-06-21 15:29:15
YPK-Home	WPA/WPA2 Personal	2015-06-22 14:50:30
WIFIF6B76E	WPA2 Personal	2015-06-24 06:27:57
_Free_ORD_Wi-Fi	Open	2015-07-09 02:29:38
Holiday_Inn_Austin_Towne_Lake	Open	2015-07-08 03:01:33

Wifi History

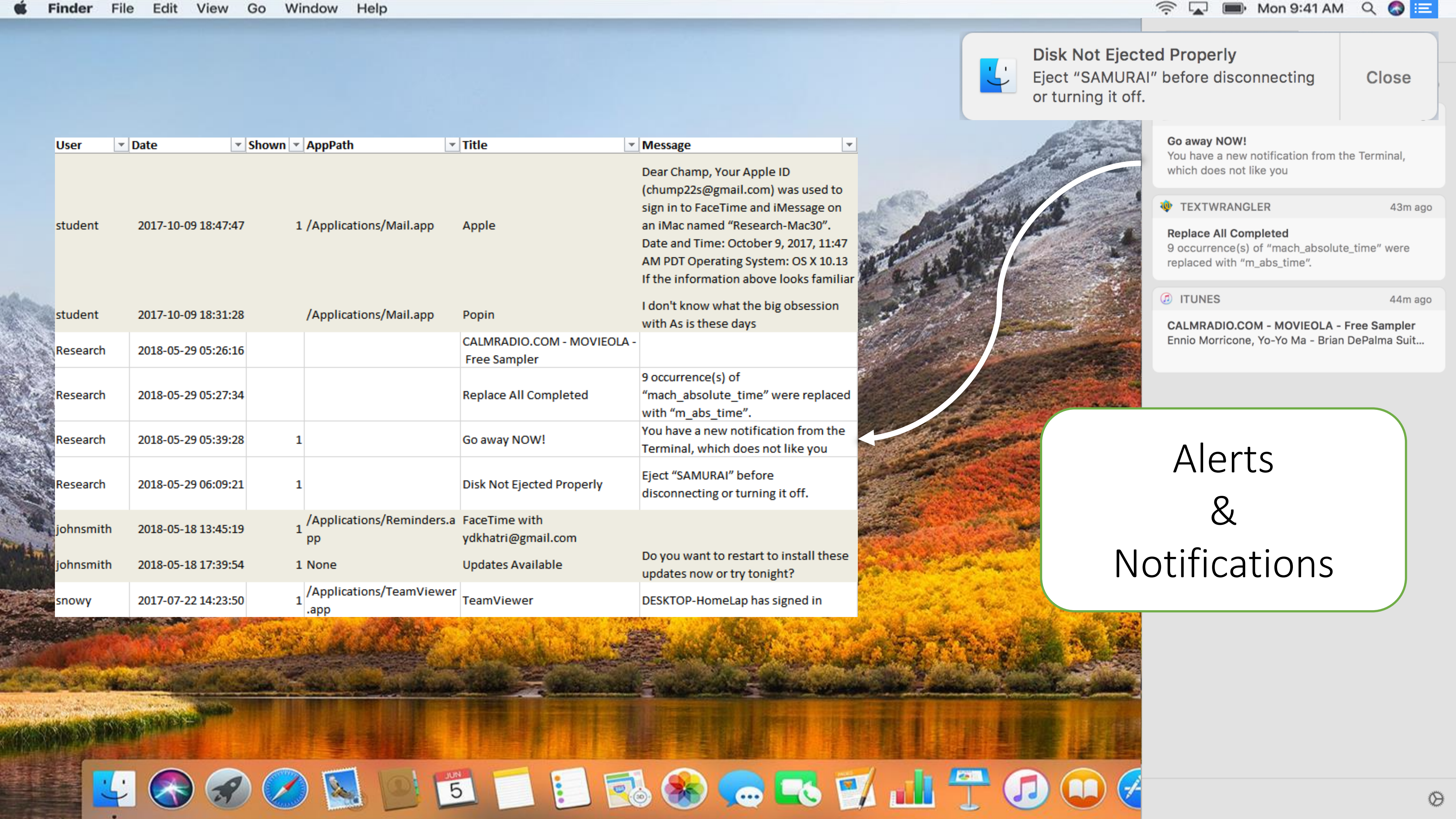


Title	Snippet	Folder	Created	LastModified	Data	AccountDescriptio
Meetingnotes		RootFolder	2016-08-11 14:32:56	2016-08-11 14:32:56	Meetingnotes - Did not like the way compensation converstation was brushed aside Maggie needs to explain otter syndrome?	iCloud- jfrack
Passwords	Passwords	Notes	2016-08-11 14:32:56	2016-08-11 14:32:56	Passwords Gmail - 78FEpliot$ instagram - host!le## Linkedin - Link235DD#	iCloud- jfrack
New Note		Notes	2017-07-28 17:25:09	2017-07-28 17:25:09		On My Mac

12/19/17 मेरा नाम है मोहन. . द...
champ

Note in the Cl...
12/19/17 More...
Notes

Notes Data



Disk Not Ejected Properly
Eject “SAMURAI” before disconnecting or turning it off.

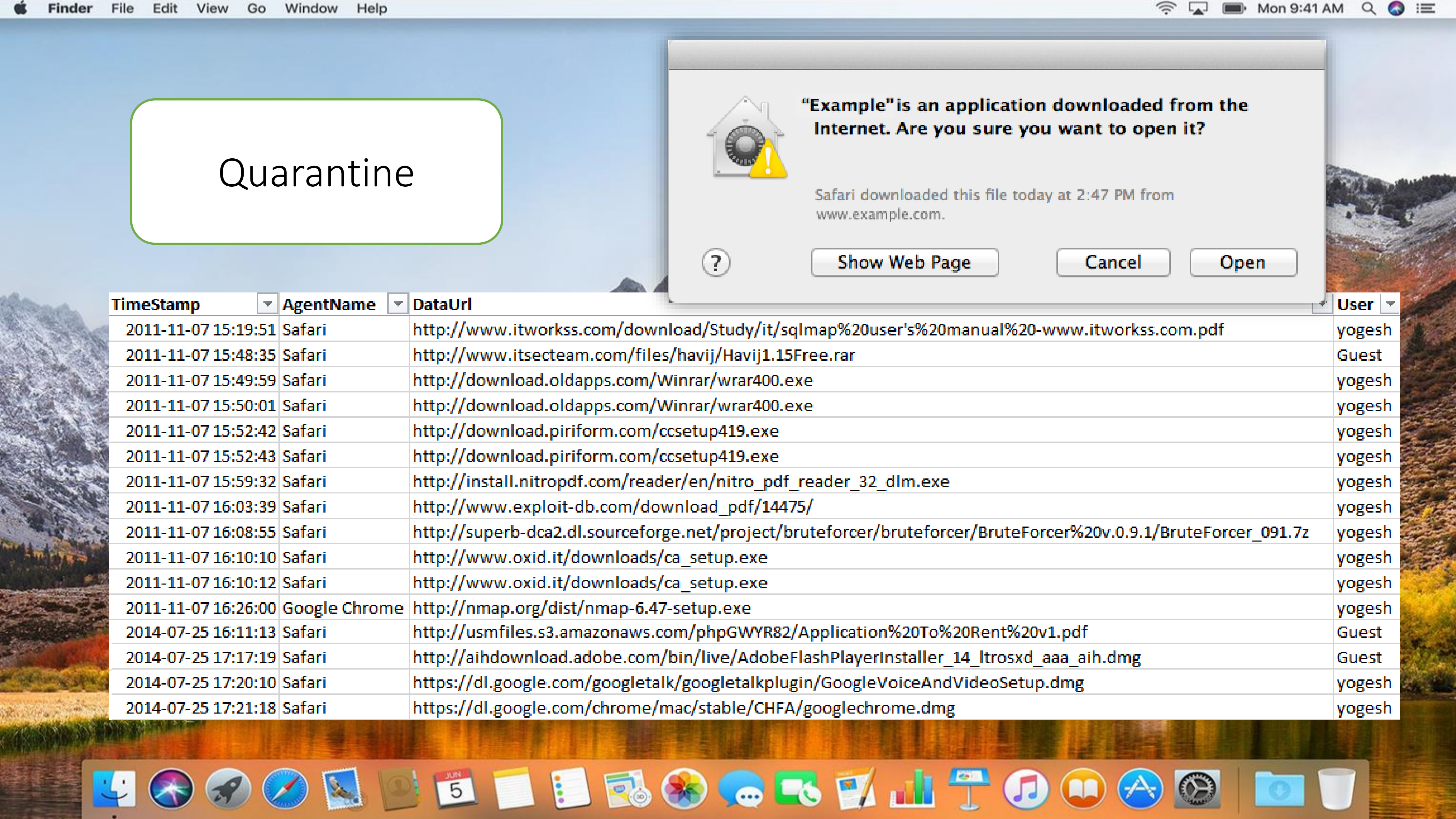
User	Date	Shown	AppPath	Title	Message
student	2017-10-09 18:47:47	1	/Applications/Mail.app	Apple	Dear Champ, Your Apple ID (chump22s@gmail.com) was used to sign in to FaceTime and iMessage on an iMac named “Research-Mac30”. Date and Time: October 9, 2017, 11:47 AM PDT Operating System: OS X 10.13 If the information above looks familiar
student	2017-10-09 18:31:28		/Applications/Mail.app	Popin	I don't know what the big obsession with As is these days
Research	2018-05-29 05:26:16			CALMRADIO.COM - MOVIEOLA - Free Sampler	
Research	2018-05-29 05:27:34			Replace All Completed	9 occurrence(s) of “mach_absolute_time” were replaced with “m_abs_time”.
Research	2018-05-29 05:39:28	1		Go away NOW!	You have a new notification from the Terminal, which does not like you
Research	2018-05-29 06:09:21	1		Disk Not Ejected Properly	Eject “SAMURAI” before disconnecting or turning it off.
johnsmith	2018-05-18 13:45:19	1	/Applications/Reminders.app	FaceTime with ydkhatri@gmail.com	
johnsmith	2018-05-18 17:39:54	1	None	Updates Available	Do you want to restart to install these updates now or try tonight?
snowy	2017-07-22 14:23:50	1	/Applications/TeamViewer.app	TeamViewer	DESKTOP-HomeLap has signed in

Go away NOW!
You have a new notification from the Terminal, which does not like you

TEXTWRANGLER 43m ago
Replace All Completed
9 occurrence(s) of “mach_absolute_time” were replaced with “m_abs_time”.

ITUNES 44m ago
CALMRADIO.COM - MOVIEOLA - Free Sampler
Ennio Morricone, Yo-Yo Ma - Brian DePalma Suit...

Alerts & Notifications



Quarantine

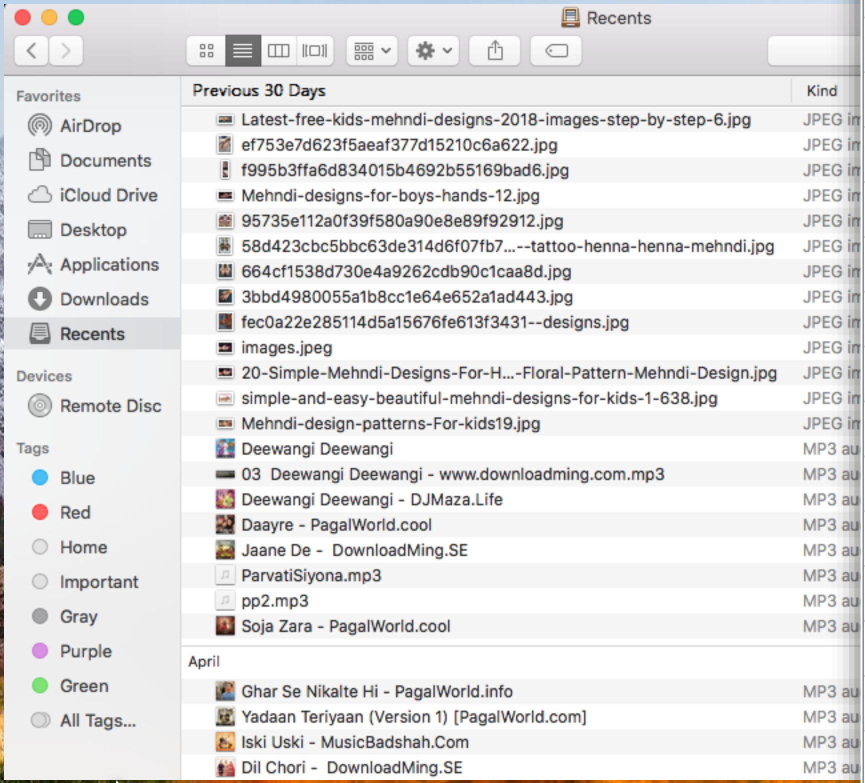
"Example" is an application downloaded from the Internet. Are you sure you want to open it?

Safari downloaded this file today at 2:47 PM from www.example.com.

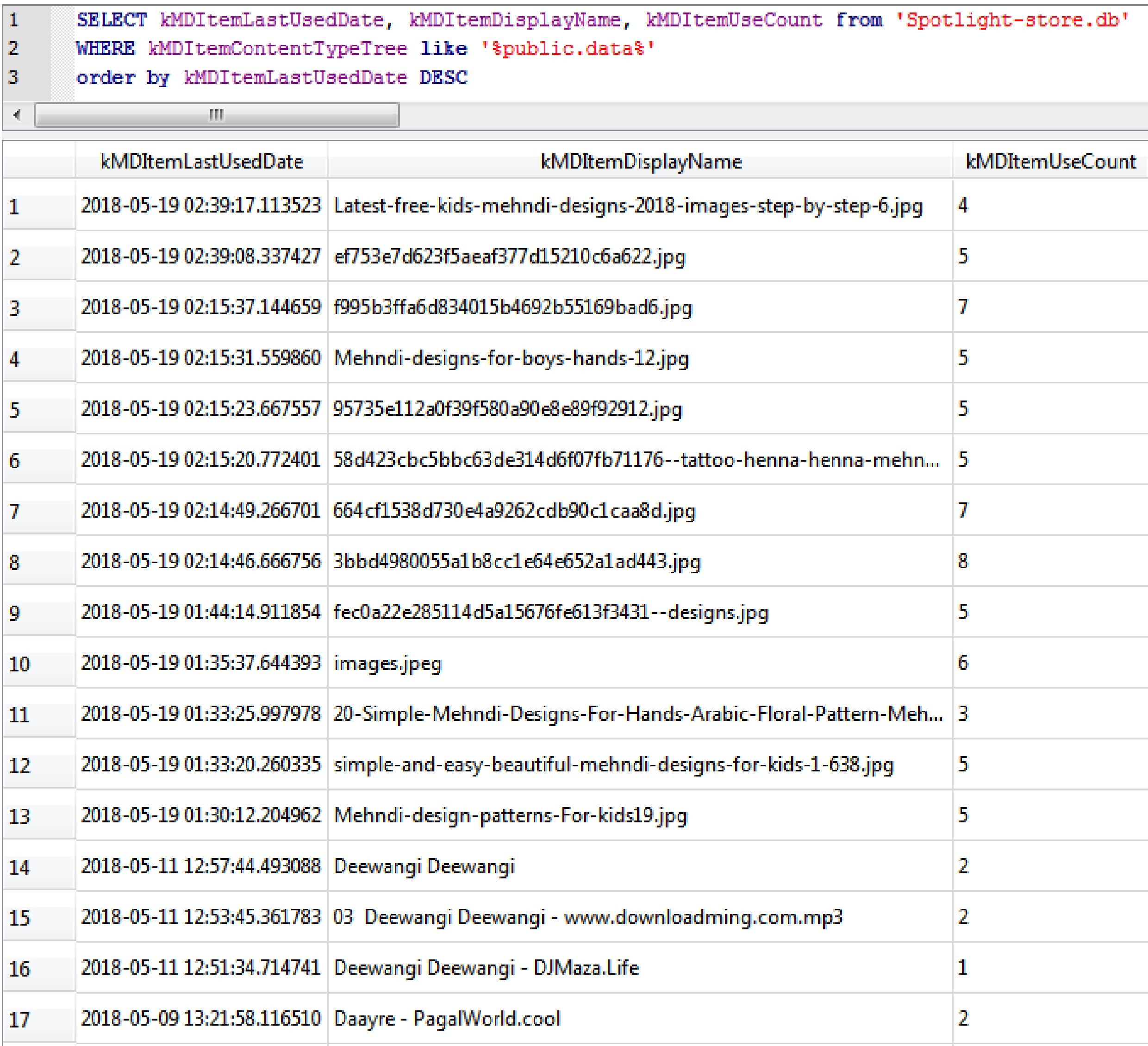
TimeStamp	AgentName	DataUrl	User
2011-11-07 15:19:51	Safari	http://www.itworkss.com/download/Study/it/sqlmap%20user's%20manual%20-www.itworkss.com.pdf	yogesh
2011-11-07 15:48:35	Safari	http://www.itsecteam.com/files/havij/Havij1.15Free.rar	Guest
2011-11-07 15:49:59	Safari	http://download.oldapps.com/Winrar/wrar400.exe	yogesh
2011-11-07 15:50:01	Safari	http://download.oldapps.com/Winrar/wrar400.exe	yogesh
2011-11-07 15:52:42	Safari	http://download.piriform.com/ccsetup419.exe	yogesh
2011-11-07 15:52:43	Safari	http://download.piriform.com/ccsetup419.exe	yogesh
2011-11-07 15:59:32	Safari	http://install.nitropdf.com/reader/en/nitro_pdf_reader_32_dlm.exe	yogesh
2011-11-07 16:03:39	Safari	http://www.exploit-db.com/download_pdf/14475/	yogesh
2011-11-07 16:08:55	Safari	http://superb-dca2.dl.sourceforge.net/project/bruteforcer/bruteforcer/BruteForcer%20v.0.9.1/BruteForcer_091.7z	yogesh
2011-11-07 16:10:10	Safari	http://www.oxid.it/downloads/ca_setup.exe	yogesh
2011-11-07 16:10:12	Safari	http://www.oxid.it/downloads/ca_setup.exe	yogesh
2011-11-07 16:26:00	Google Chrome	http://nmap.org/dist/nmap-6.47-setup.exe	yogesh
2014-07-25 16:11:13	Safari	http://usmfiles.s3.amazonaws.com/phpGWYR82/Application%20To%20Rent%20v1.pdf	Guest
2014-07-25 17:17:19	Safari	http://aihdownload.adobe.com/bin/live/AdobeFlashPlayerInstaller_14_ltrosxd_aaa_aih.dmg	Guest
2014-07-25 17:20:10	Safari	https://dl.google.com/googletalk/googletalkplugin/GoogleVoiceAndVideoSetup.dmg	yogesh
2014-07-25 17:21:18	Safari	https://dl.google.com/chrome/mac/stable/CHFA/googlechrome.dmg	yogesh

New

Spotlight Data



Previous 30 Days	Kind
Latest-free-kids-mehndi-designs-2018-images-step-by-step-6.jpg	JPEG im
ef753e7d623f5aeaf377d15210c6a622.jpg	JPEG im
f995b3ffa6d834015b4692b55169bad6.jpg	JPEG im
Mehndi-designs-for-boys-hands-12.jpg	JPEG im
95735e112a0f39f580a90e8e89f92912.jpg	JPEG im
58d423cbc5bbc63de314d6f07fb7...--tattoo-henna-henna-mehndi.jpg	JPEG im
664cf1538d730e4a9262cdb90c1caa8d.jpg	JPEG im
3bbd4980055a1b8cc1e64e652a1ad443.jpg	JPEG im
fec0a22e285114d5a15676fe613f3431--designs.jpg	JPEG im
images.jpeg	JPEG im
20-Simple-Mehndi-Designs-For-H...-Floral-Pattern-Mehndi-Design.jpg	JPEG im
simple-and-easy-beautiful-mehndi-designs-for-kids-1-638.jpg	JPEG im
Mehndi-design-patterns-For-kids19.jpg	JPEG im
Deewangi Deewangi	MP3 au
03 Deewangi Deewangi - www.downloadming.com.mp3	MP3 au
Deewangi Deewangi - DJMaza.Life	MP3 au
Daayre - PagalWorld.cool	MP3 au
Jaane De - DownloadMing.SE	MP3 au
ParvatiSiyona.mp3	MP3 au
pp2.mp3	MP3 au
Soja Zara - PagalWorld.cool	MP3 au
April	
Ghar Se Nikalte Hi - PagalWorld.info	MP3 au
Yadaan Teriyaan (Version 1) [PagalWorld.com]	MP3 au
Iski Uski - MusicBadshah.Com	MP3 au
Dil Chori - DownloadMing.SE	MP3 au



```
SELECT kMDItemLastUsedDate, kMDItemDisplayName, kMDItemUseCount from 'Spotlight-store.db'
WHERE kMDItemContentTypeTree like '%public.data%'
order by kMDItemLastUsedDate DESC
```

	kMDItemLastUsedDate	kMDItemDisplayName	kMDItemUseCount
1	2018-05-19 02:39:17.113523	Latest-free-kids-mehndi-designs-2018-images-step-by-step-6.jpg	4
2	2018-05-19 02:39:08.337427	ef753e7d623f5aeaf377d15210c6a622.jpg	5
3	2018-05-19 02:15:37.144659	f995b3ffa6d834015b4692b55169bad6.jpg	7
4	2018-05-19 02:15:31.559860	Mehndi-designs-for-boys-hands-12.jpg	5
5	2018-05-19 02:15:23.667557	95735e112a0f39f580a90e8e89f92912.jpg	5
6	2018-05-19 02:15:20.772401	58d423cbc5bbc63de314d6f07fb71176--tattoo-henna-henna-mehn...	5
7	2018-05-19 02:14:49.266701	664cf1538d730e4a9262cdb90c1caa8d.jpg	7
8	2018-05-19 02:14:46.666756	3bbd4980055a1b8cc1e64e652a1ad443.jpg	8
9	2018-05-19 01:44:14.911854	fec0a22e285114d5a15676fe613f3431--designs.jpg	5
10	2018-05-19 01:35:37.644393	images.jpeg	6
11	2018-05-19 01:33:25.997978	20-Simple-Mehndi-Designs-For-Hands-Arabic-Floral-Pattern-Meh...	3
12	2018-05-19 01:33:20.260335	simple-and-easy-beautiful-mehndi-designs-for-kids-1-638.jpg	5
13	2018-05-19 01:30:12.204962	Mehndi-design-patterns-For-kids19.jpg	5
14	2018-05-11 12:57:44.493088	Deewangi Deewangi	2
15	2018-05-11 12:53:45.361783	03 Deewangi Deewangi - www.downloadming.com.mp3	2
16	2018-05-11 12:51:34.714741	Deewangi Deewangi - DJMaza.Life	1
17	2018-05-09 13:21:58.116510	Daayre - PagalWorld.cool	2

Full list of plugins

BASICINFO

BASHSESSIONS

DOMAINS

IMESSAGE

INETACCOUNTS

INSTALLHISTORY

NETUSAGE

NETWORKING

NOTES

NOTIFICATIONS

PRINTJOBS

QUARANTINE

RECENTITEMS

SAFARI

SPOTLIGHT

SPOTLIGHTSHORTCUTS

USERS

WIFI

In the near future..

Code upgrade to Python 3

Plugins for

- Apple Unified Logs
- fseventsd
- FaceTime
- iDevice Backup data
- Dock items
- Microsoft Office 365
- Safari Cookies
- More apps..

Thanks for listening! Time for Questions..

Thanks also to my students who helped in generating data, in research and writing some of the plugins - Austin Truax, Jake Nicastro, TJ Dalzell, Noah Sidall, Michael Geyer, Adam Ferrante, Jack Farley

GitHub https://github.com/ydkhatri/mac_apt

✉ yogesh@swiftforensics.com

@swiftforensics

Send us your bug reports, requests or contribute with code !