Temporal Analysis on HFS+ and Mac OS X in Digital Investigation

Mengmeng Sept 23 2012

Abstract

The rules of changes in time, can be used to analyze certain user behaviors like data access, modification or transfer.

The rules differ for different file systems. Some research have already been done on NTFS and FAT file systems, while no analysis of an Mac computer, and (HFS+).

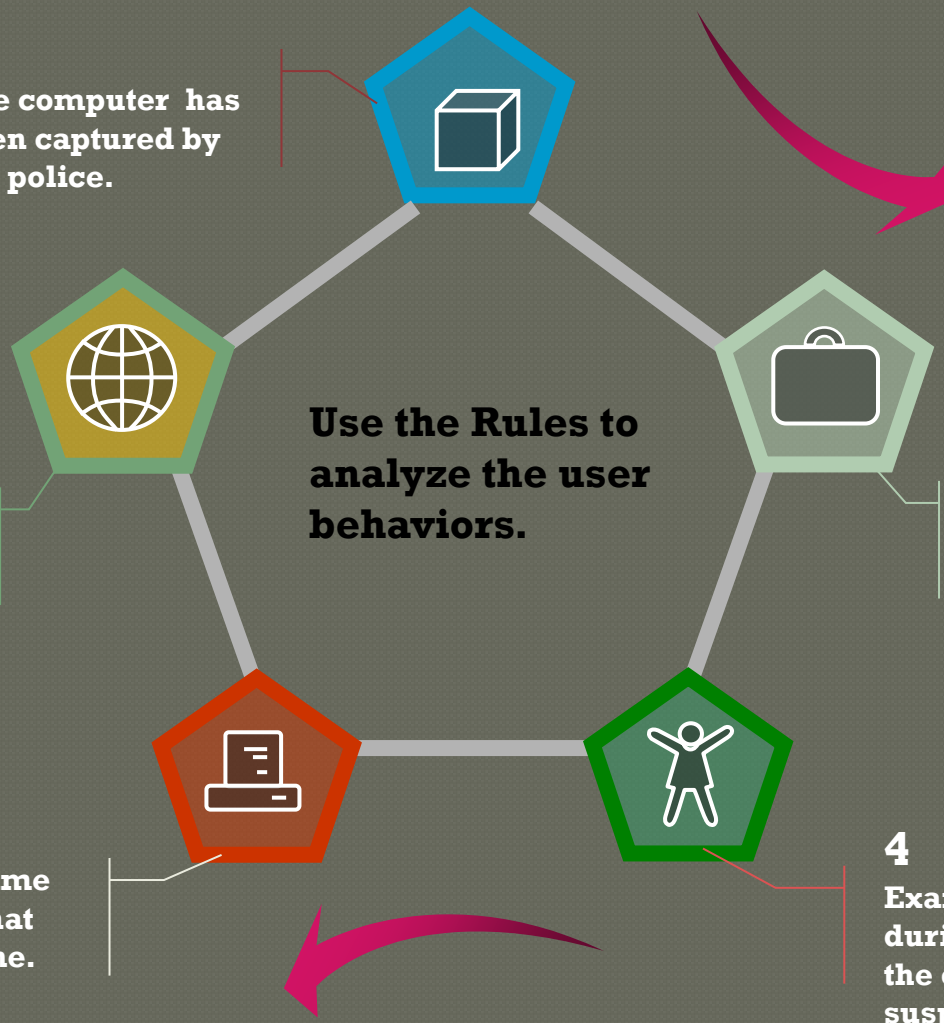
This study analyzes the changes in time attributes on Mac OS X with HFS+, and deduces user behaviors, to help reconstruct crime scene .

Case study

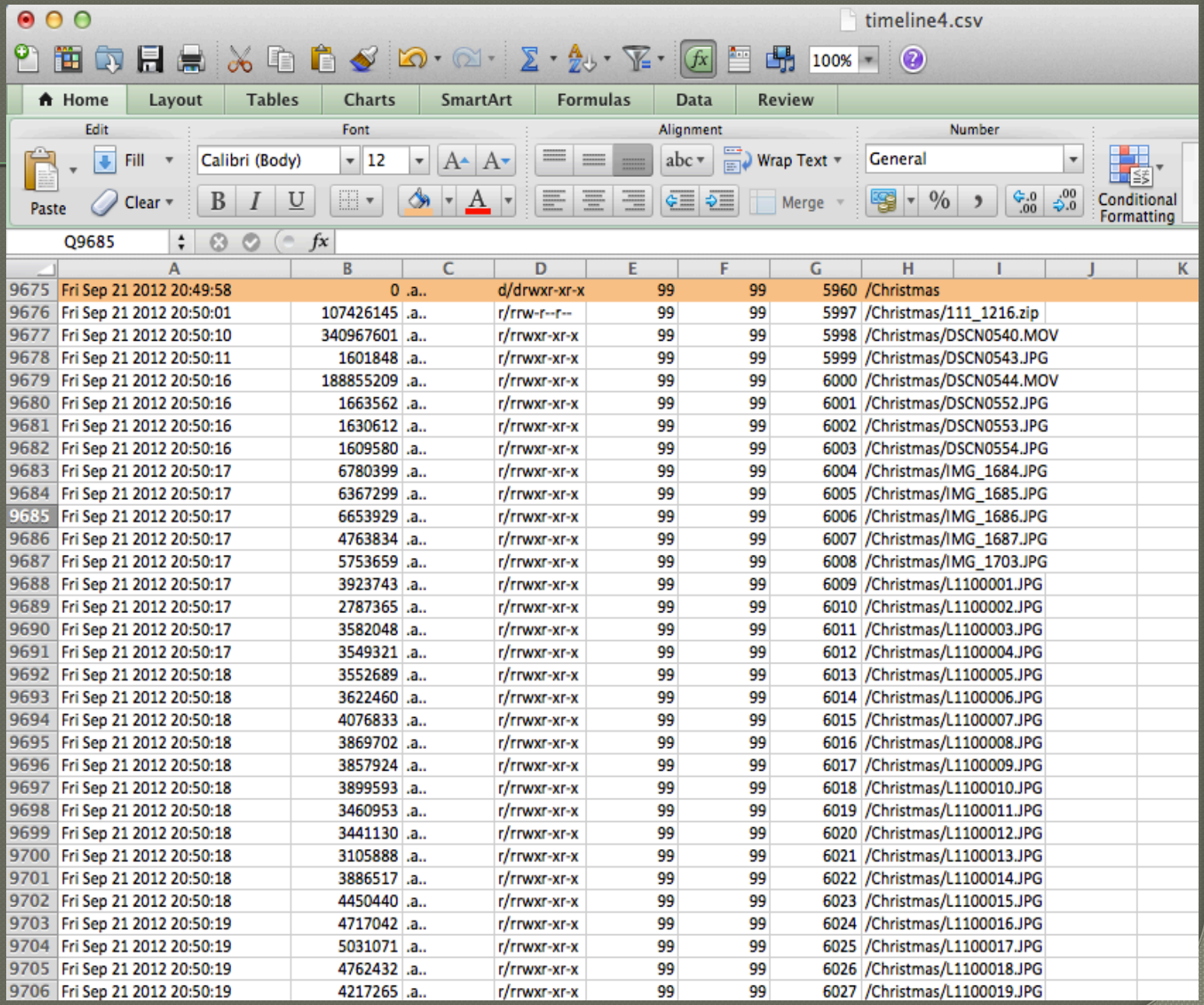
- 1. The victim's(famous TV star) computer is stolen by the suspect. There are some private photos inside the computer. After the computer was captured by the police, all files or folders seem unmodified. But some time stamps of some files and folders are updated.

So what the suspect may have done?

Case Study


2
The computer has been captured by the police.
1
Computer has been stolen by the suspect .
Use the Rules to analyze the user behaviors.
3
Create a clone image of the computer and generate the timeline.
5
Reconstruct the crime scene and know what the suspect has done.
4
Examine the information during the period when the computer is in suspect's use.

We use the Sleuth Kit to generate the timeline



	A	B	C	D	E	F	G	H	I	J	K
9675	Fri Sep 21 2012 20:49:58	0	.a..	d/drwxr-xr-x	99	99	5960	/Christmas			
9676	Fri Sep 21 2012 20:50:01	107426145	.a..	r/rrw-r--r--	99	99	5997	/Christmas/111_1216.zip			
9677	Fri Sep 21 2012 20:50:10	340967601	.a..	r/rrwxr-xr-x	99	99	5998	/Christmas/DSCN0540.MOV			
9678	Fri Sep 21 2012 20:50:11	1601848	.a..	r/rrwxr-xr-x	99	99	5999	/Christmas/DSCN0543.JPG			
9679	Fri Sep 21 2012 20:50:16	188855209	.a..	r/rrwxr-xr-x	99	99	6000	/Christmas/DSCN0544.MOV			
9680	Fri Sep 21 2012 20:50:16	1663562	.a..	r/rrwxr-xr-x	99	99	6001	/Christmas/DSCN0552.JPG			
9681	Fri Sep 21 2012 20:50:16	1630612	.a..	r/rrwxr-xr-x	99	99	6002	/Christmas/DSCN0553.JPG			
9682	Fri Sep 21 2012 20:50:16	1609580	.a..	r/rrwxr-xr-x	99	99	6003	/Christmas/DSCN0554.JPG			
9683	Fri Sep 21 2012 20:50:17	6780399	.a..	r/rrwxr-xr-x	99	99	6004	/Christmas/IMG_1684.JPG			
9684	Fri Sep 21 2012 20:50:17	6367299	.a..	r/rrwxr-xr-x	99	99	6005	/Christmas/IMG_1685.JPG			
9685	Fri Sep 21 2012 20:50:17	6653929	.a..	r/rrwxr-xr-x	99	99	6006	/Christmas/IMG_1686.JPG			
9686	Fri Sep 21 2012 20:50:17	4763834	.a..	r/rrwxr-xr-x	99	99	6007	/Christmas/IMG_1687.JPG			
9687	Fri Sep 21 2012 20:50:17	5753659	.a..	r/rrwxr-xr-x	99	99	6008	/Christmas/IMG_1703.JPG			
9688	Fri Sep 21 2012 20:50:17	3923743	.a..	r/rrwxr-xr-x	99	99	6009	/Christmas/L1100001.JPG			
9689	Fri Sep 21 2012 20:50:17	2787365	.a..	r/rrwxr-xr-x	99	99	6010	/Christmas/L1100002.JPG			
9690	Fri Sep 21 2012 20:50:17	3582048	.a..	r/rrwxr-xr-x	99	99	6011	/Christmas/L1100003.JPG			
9691	Fri Sep 21 2012 20:50:17	3549321	.a..	r/rrwxr-xr-x	99	99	6012	/Christmas/L1100004.JPG			
9692	Fri Sep 21 2012 20:50:18	3552689	.a..	r/rrwxr-xr-x	99	99	6013	/Christmas/L1100005.JPG			
9693	Fri Sep 21 2012 20:50:18	3622460	.a..	r/rrwxr-xr-x	99	99	6014	/Christmas/L1100006.JPG			
9694	Fri Sep 21 2012 20:50:18	4076833	.a..	r/rrwxr-xr-x	99	99	6015	/Christmas/L1100007.JPG			
9695	Fri Sep 21 2012 20:50:18	3869702	.a..	r/rrwxr-xr-x	99	99	6016	/Christmas/L1100008.JPG			
9696	Fri Sep 21 2012 20:50:18	3857924	.a..	r/rrwxr-xr-x	99	99	6017	/Christmas/L1100009.JPG			
9697	Fri Sep 21 2012 20:50:18	3899593	.a..	r/rrwxr-xr-x	99	99	6018	/Christmas/L1100010.JPG			
9698	Fri Sep 21 2012 20:50:18	3460953	.a..	r/rrwxr-xr-x	99	99	6019	/Christmas/L1100011.JPG			
9699	Fri Sep 21 2012 20:50:18	3441130	.a..	r/rrwxr-xr-x	99	99	6020	/Christmas/L1100012.JPG			
9700	Fri Sep 21 2012 20:50:18	3105888	.a..	r/rrwxr-xr-x	99	99	6021	/Christmas/L1100013.JPG			
9701	Fri Sep 21 2012 20:50:18	3886517	.a..	r/rrwxr-xr-x	99	99	6022	/Christmas/L1100014.JPG			
9702	Fri Sep 21 2012 20:50:18	4450440	.a..	r/rrwxr-xr-x	99	99	6023	/Christmas/L1100015.JPG			
9703	Fri Sep 21 2012 20:50:19	4717042	.a..	r/rrwxr-xr-x	99	99	6024	/Christmas/L1100016.JPG			
9704	Fri Sep 21 2012 20:50:19	5031071	.a..	r/rrwxr-xr-x	99	99	6025	/Christmas/L1100017.JPG			
9705	Fri Sep 21 2012 20:50:19	4762432	.a..	r/rrwxr-xr-x	99	99	6026	/Christmas/L1100018.JPG			
9706	Fri Sep 21 2012 20:50:19	4217265	.a..	r/rrwxr-xr-x	99	99	6027	/Christmas/L1100019.JPG			

Case study

- The computer has been in the suspect's control on Sept 21, 2012. So we only check the time slot in the timeline data.
- From the timeline, we can see that the folder /Christmas and the image files inside this folder all have the similar Access time.
- Then, let's specify the folder /Christmas in the timeline to see the other time stamps' value.

Case study

	A	B	C	D	E	F	G	H	I
1	Date	Size	Type	Mode	UID	GID	Meta	File Name	
2540	Sun Jan 22 2012 17:30:38	0	...b	d/drwxr-xr-x	99	99	5960	/Christmas	
9625	Mon Aug 20 2012 00:51:29	0	m.c.	d/drwxr-xr-x	99	99	5960	/Christmas	
9675	Fri Sep 21 2012 20:49:58	0	.a..	d/drwxr-xr-x	99	99	5960	/Christmas	
9753									

2466	Sat Dec 17 2011 00:51:02	3441130	m...	r/rrwxr-xr-x	99	99	6020	/Christmas/L1100012.JPG
2467	Sat Dec 17 2011 00:51:07	3105888	m...	r/rrwxr-xr-x	99	99	6021	/Christmas/L1100013.JPG
2468	Sat Dec 17 2011 00:53:18	3860425	m...	r/rrwxr-xr-x	99	99	6040	/Christmas/L1100031.JPG
2469	Sat Dec 17 2011 00:53:27	3924766	m...	r/rrwxr-xr-x	99	99	6041	/Christmas/L1100032.JPG
2470	Sat Dec 17 2011 00:53:33	3825761	m...	r/rrwxr-xr-x	99	99	6043	/Christmas/L1100034.JPG
2471	Sat Dec 17 2011 00:53:38	4176504	m...	r/rrwxr-xr-x	99	99	6044	/Christmas/L1100035.JPG
2472	Sat Dec 17 2011 00:53:44	3618305	m...	r/rrwxr-xr-x	99	99	6045	/Christmas/L1100036.JPG
2473	Sun Dec 18 2011 01:29:32	6780399	...b	r/rrwxr-xr-x	99	99	6004	/Christmas/IMG_1684.JPG
2474	Sun Dec 18 2011 01:29:42	5753659	...b	r/rrwxr-xr-x	99	99	6008	/Christmas/IMG_1703.JPG
2475	Sun Dec 18 2011 01:30:10	6780399	m...	r/rrwxr-xr-x	99	99	6004	/Christmas/IMG_1684.JPG
2476	Sun Dec 18 2011 01:30:10	6367299	m..b	r/rrwxr-xr-x	99	99	6005	/Christmas/IMG_1685.JPG
2477	Sun Dec 18 2011 01:30:11	5753659	m...	r/rrwxr-xr-x	99	99	6008	/Christmas/IMG_1703.JPG
2478	Sun Dec 18 2011 01:30:12	6653929	m..b	r/rrwxr-xr-x	99	99	6006	/Christmas/IMG_1686.JPG
2479	Sun Dec 18 2011 01:30:14	4763834	m..b	r/rrwxr-xr-x	99	99	6007	/Christmas/IMG_1687.JPG
2526	Sun Jan 22 2012 17:30:38	0	...b	d/drwxr-xr-x	99	99	5960	/Christmas
3659	Tue Jun 12 2012 01:58:52	107426145	...b	r/rrw-r--r--	99	99	5997	/Christmas/111_1216.zip
3660	Tue Jun 12 2012 01:58:59	107426145	m...	r/rrw-r--r--	99	99	5997	/Christmas/111_1216.zip
6314	Sun Jun 17 2012 23:31:23	15364	...b	r/rrw-r--r--	99	99	5962	/Christmas/.DS_Store
7317	Fri Jun 22 2012 00:01:37	107426145	..c.	r/rrw-r--r--	99	99	5997	/Christmas/111_1216.zip
7318	Fri Jun 22 2012 00:02:32	340967601	..c.	r/rrwxr-xr-x	99	99	5998	/Christmas/DSCN0540.MOV
7319	Fri Jun 22 2012 00:02:32	1601848	..c.	r/rrwxr-xr-x	99	99	5999	/Christmas/DSCN0543.JPG
7320	Fri Jun 22 2012 00:03:03	188855209	..c.	r/rrwxr-xr-x	99	99	6000	/Christmas/DSCN0544.MOV
7321	Fri Jun 22 2012 00:03:03	1663562	..c.	r/rrwxr-xr-x	99	99	6001	/Christmas/DSCN0552.JPG
7322	Fri Jun 22 2012 00:03:03	1630612	..c.	r/rrwxr-xr-x	99	99	6002	/Christmas/DSCN0553.JPG
7323	Fri Jun 22 2012 00:03:04	1609580	..c.	r/rrwxr-xr-x	99	99	6003	/Christmas/DSCN0554.JPG
7324	Fri Jun 22 2012 00:03:05	6780399	..c.	r/rrwxr-xr-x	99	99	6004	/Christmas/IMG_1684.JPG
7325	Fri Jun 22 2012 00:03:06	6367299	..c.	r/rrwxr-xr-x	99	99	6005	/Christmas/IMG_1685.JPG
7326	Fri Jun 22 2012 00:03:07	6653929	..c.	r/rrwxr-xr-x	99	99	6006	/Christmas/IMG_1686.JPG
7327	Fri Jun 22 2012 00:03:07	4763834	..c.	r/rrwxr-xr-x	99	99	6007	/Christmas/IMG_1687.JPG
7328	Fri Jun 22 2012 00:03:08	5753659	..c.	r/rrwxr-xr-x	99	99	6008	/Christmas/IMG_1703.JPG
7329	Fri Jun 22 2012 00:03:09	3923743	..c.	r/rrwxr-xr-x	99	99	6009	/Christmas/L1100001.JPG

Case study

Finder information for the folder and files

Name	Date Modified	Date Created	Last Opened	Date Added
Christmas	20 Aug, 2012 12:51 AM	22 Jan, 2012 5:30 PM	Yesterday 8:48 PM	22 Jun, 2012 12:00 AM

Name	Date Modified	Date Created	Last Opened	Date Added
DSCN0540.MOV	17 Dec, 2011 12:01 AM	16 Dec, 2011 11:52 PM	17 Dec, 2011 12:01 AM	22 Jun, 2012 12:01 AM
DSCN0543.JPG	16 Dec, 2011 11:45 PM	16 Dec, 2011 11:45 PM	16 Dec, 2011 11:45 PM	22 Jun, 2012 12:02 AM
DSCN0544.MOV	16 Dec, 2011 11:51 PM	16 Dec, 2011 11:46 PM	16 Dec, 2011 11:51 PM	22 Jun, 2012 12:02 AM
DSCN0552.JPG	16 Dec, 2011 11:45 PM	16 Dec, 2011 11:45 PM	16 Dec, 2011 11:45 PM	22 Jun, 2012 12:03 AM
DSCN0553.JPG	16 Dec, 2011 11:44 PM	16 Dec, 2011 11:44 PM	16 Dec, 2011 11:44 PM	22 Jun, 2012 12:03 AM
DSCN0554.JPG	16 Dec, 2011 11:45 PM	16 Dec, 2011 11:45 PM	16 Dec, 2011 11:45 PM	22 Jun, 2012 12:03 AM
IMG_1684.JPG	18 Dec, 2011 1:30 AM	18 Dec, 2011 1:29 AM	18 Dec, 2011 1:30 AM	22 Jun, 2012 12:03 AM
IMG_1685.JPG	18 Dec, 2011 1:30 AM	18 Dec, 2011 1:30 AM	18 Dec, 2011 1:30 AM	22 Jun, 2012 12:03 AM
IMG_1686.JPG	18 Dec, 2011 1:30 AM	18 Dec, 2011 1:30 AM	18 Dec, 2011 1:30 AM	22 Jun, 2012 12:03 AM
IMG_1687.JPG	18 Dec, 2011 1:30 AM	18 Dec, 2011 1:30 AM	18 Dec, 2011 1:30 AM	22 Jun, 2012 12:03 AM
IMG_1703.JPG	18 Dec, 2011 1:30 AM	18 Dec, 2011 1:29 AM	18 Dec, 2011 1:30 AM	22 Jun, 2012 12:03 AM
L1100001.JPG	16 Dec, 2011 6:43 PM	16 Dec, 2011 6:43 PM	16 Dec, 2011 6:43 PM	22 Jun, 2012 12:03 AM
L1100002.JPG	16 Dec, 2011 6:43 PM	16 Dec, 2011 6:43 PM	16 Dec, 2011 6:43 PM	22 Jun, 2012 12:03 AM
L1100003.JPG	17 Dec, 2011 12:50 AM	17 Dec, 2011 12:48 AM	17 Dec, 2011 12:50 AM	22 Jun, 2012 12:03 AM
L1100004.JPG	17 Dec, 2011 12:50 AM	17 Dec, 2011 12:48 AM	17 Dec, 2011 12:50 AM	22 Jun, 2012 12:03 AM
L1100005.JPG	17 Dec, 2011 12:50 AM	17 Dec, 2011 12:48 AM	17 Dec, 2011 12:50 AM	22 Jun, 2012 12:03 AM
L1100006.JPG	17 Dec, 2011 12:50 AM	17 Dec, 2011 12:48 AM	17 Dec, 2011 12:50 AM	22 Jun, 2012 12:03 AM
L1100007.JPG	16 Dec, 2011 6:43 PM	16 Dec, 2011 6:43 PM	16 Dec, 2011 6:43 PM	22 Jun, 2012 12:03 AM
L1100008.JPG	16 Dec, 2011 6:44 PM	16 Dec, 2011 6:44 PM	16 Dec, 2011 6:44 PM	22 Jun, 2012 12:03 AM

Case study

- From above information, we can see that for folder /Christmas, Access>Modify=Change>Birth
- For the files inside this folder, Access>Change>Modify=Birth. And Date Added=Change>Last Opened=Modify=Birth,
- And the folder's Access time is same with the files' Access time.

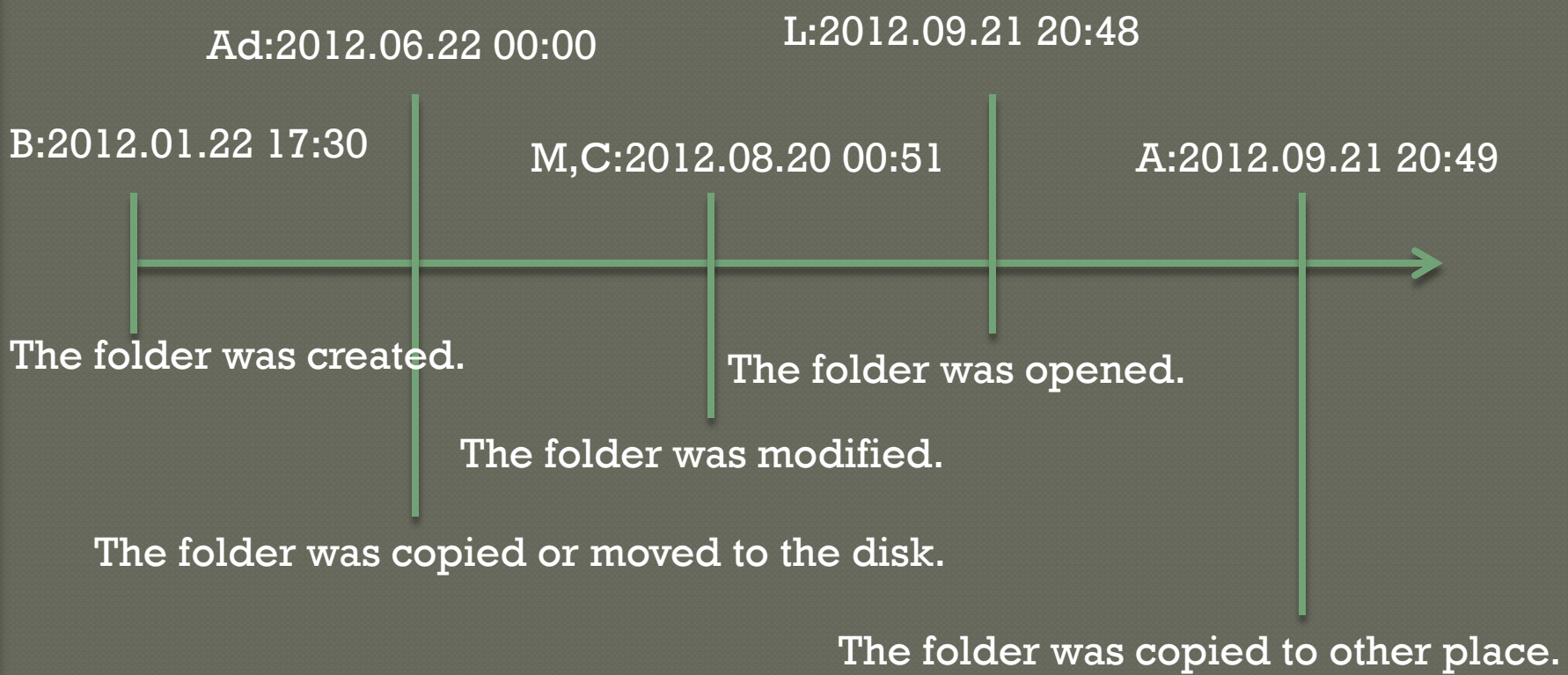
Based on the Rule No.5 for folder, the folder has been copied to another location or compressed.

Based on the Rule No. 6 for files, the image files inside the folder have been accessed, copied to other location or compressed, and before that, these files may be extracted or downloaded or copied or moved from other location.

Case study

- Reconstruct the user behavior

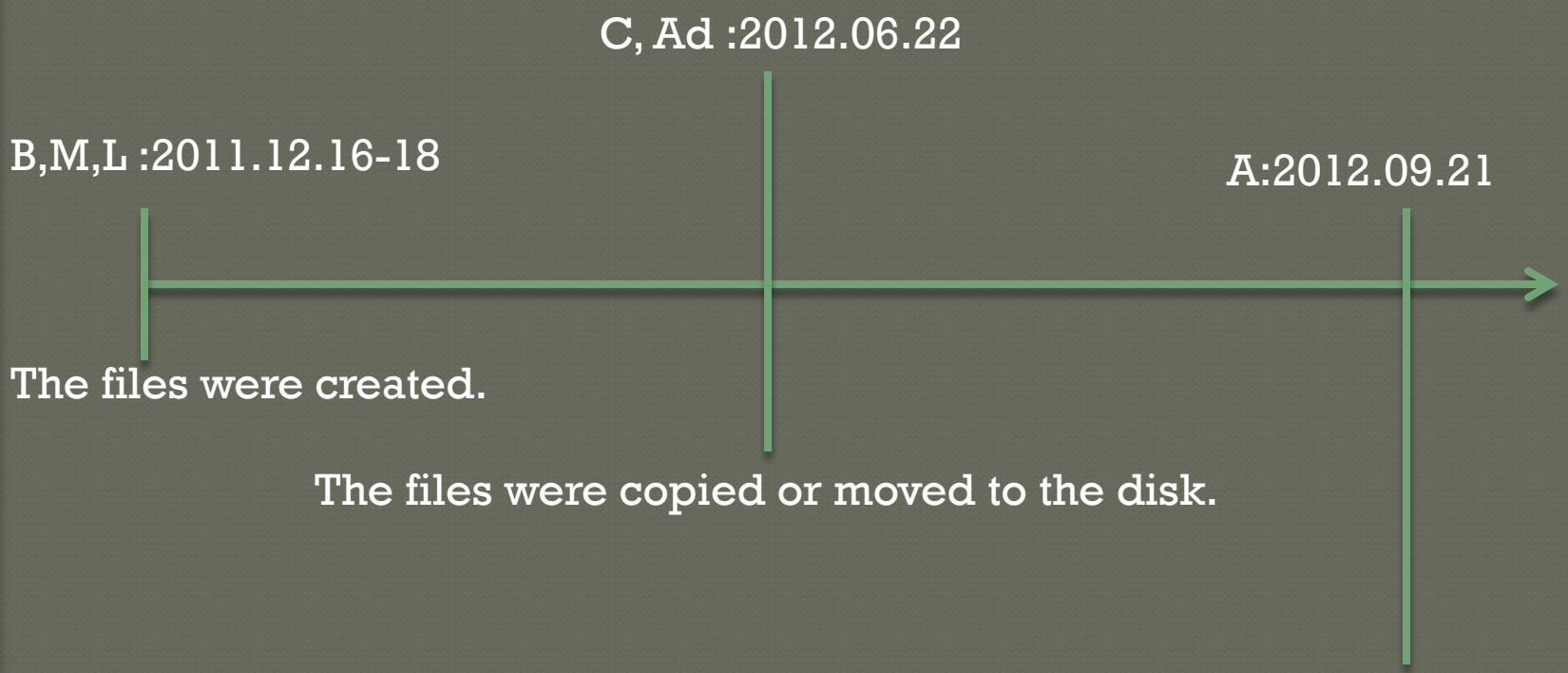
For folder:



Case study

- Reconstruct the user behavior

For files inside the folder:



Contents

Related work

Time analysis

K.P. Chow et al. :
Rules to determine the behavioral characteristics of MAC times on NTFS file system.
Bang et al. :
More research work on time information changes about NTFS files and folders as well as FAT files and folders.

Mac Forensic

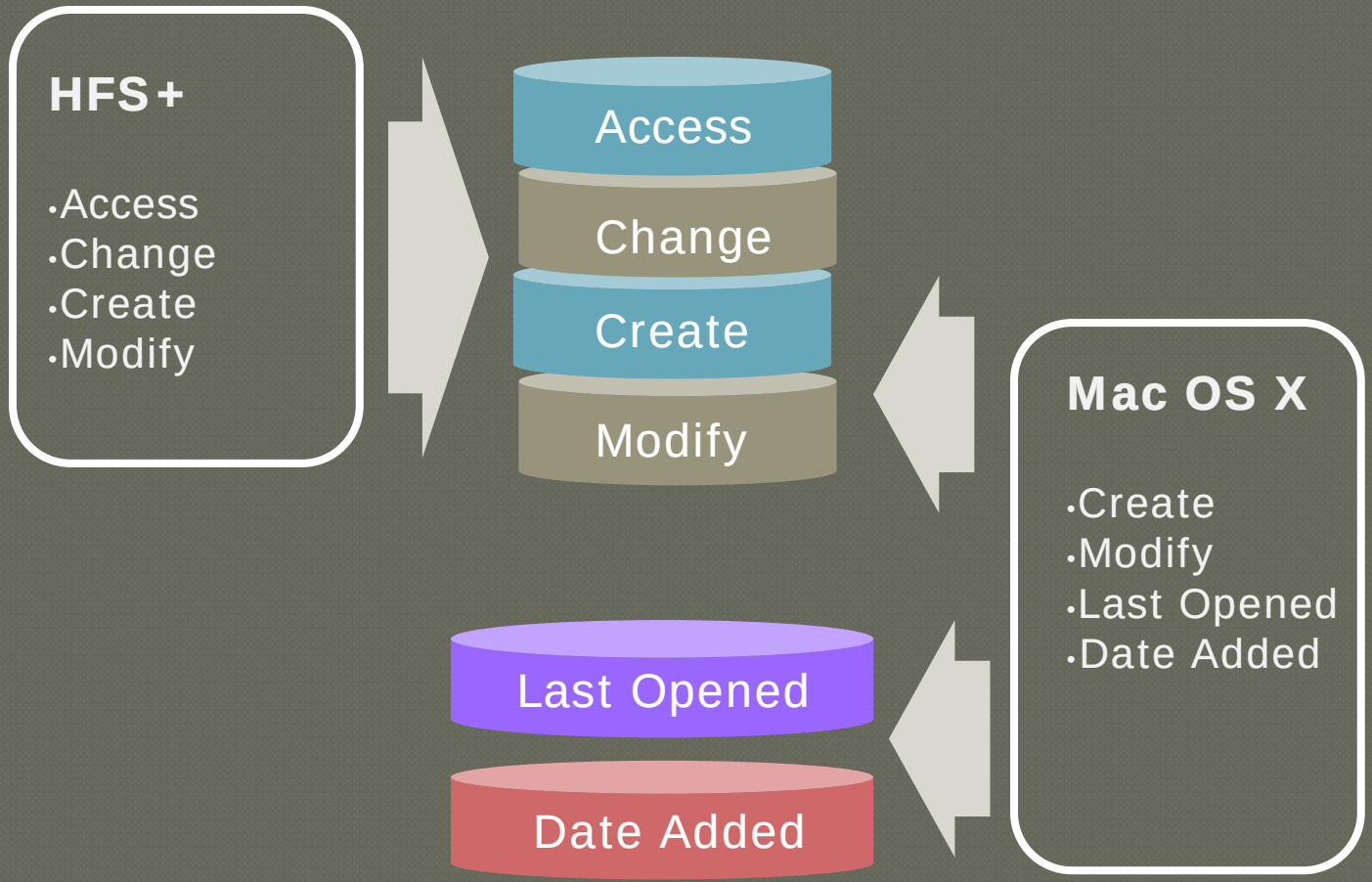
Florian Buchholz:
The role file system metadata plays in data forensics. A graphical timeline editor named Zeitline.
Brian Carrier:
The Sleuth Kit also can do file system analysis and give timeline about the files on the disk.

Macintosh computer investigation:

- Shortage of documentation on how the timestamps in file system are handled.
- No systematic documentation on the behavioral characteristics of file or folder timestamps under different operations.

Contents

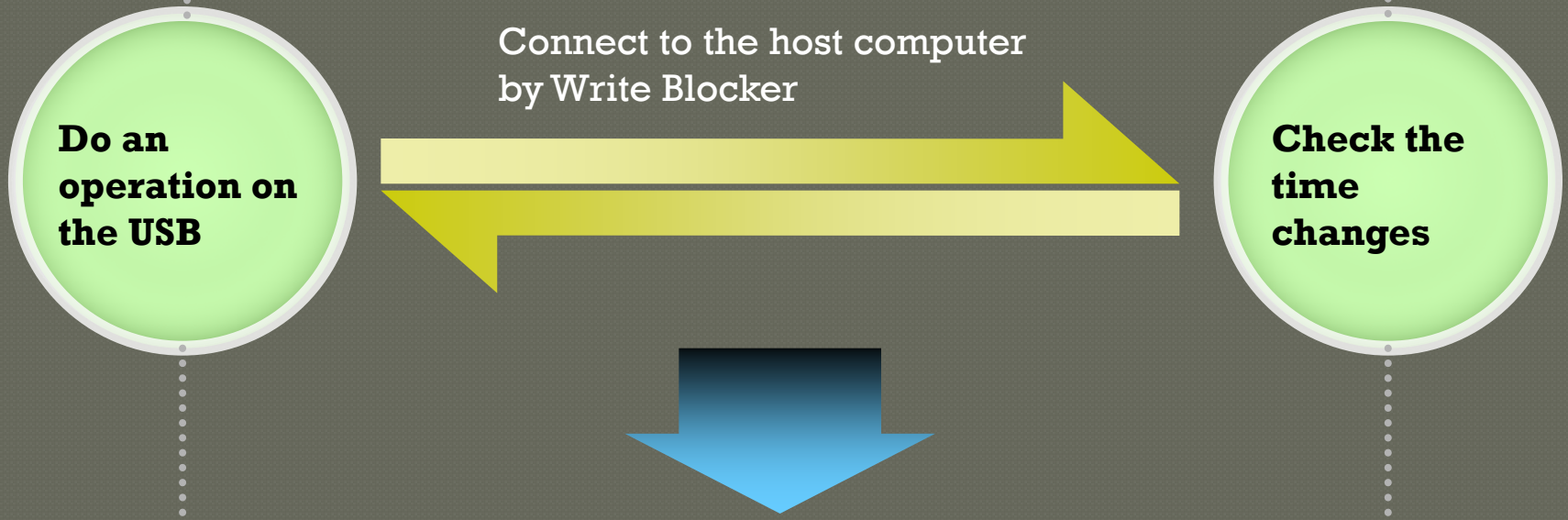
HFS+ and Mac OS X



Contents

Experiments

A Macbook pro with the Mac OS X 10.7.3 as the host computer
Erase a USB disk as "HFS+"using the Disk Utility in the computer



Creation, Modification, Change, and Access times-- command line Last Opened, Date Added times --- Finder window

Time attributes changes

Empty: Unchanged;
Y: Changed;
*: Depends on what application is used;
^: Only for .txt files accessed by the first time;
N/Y: sometimes change, sometimes not;
Y (d): Changed to the time when the file was deleted;
Y (s): Changed to the time when the item was saved after modification;
Y (o1): Changed to the time when the file was opened;
Y (o2): Changed to the time when the folder was opened;
Y (b): Changed to the time when the action began;
Y (f): Changed to the time when the action was finished;
B: Creation time/Birth time;
M: Modification time;
A: Access time;
C: Change time;
L: Last Opened time;
Ad: Date Added time.

Time attributes changes

Action	B	M	A	C	L	Ad	Rule
File Created	Y	Y	Y	Y	*Y	Y	B=M=A=C=Ad ≤ L
File Accessed			Y(o1)	^Y	*Y		B ≤M, Ad, C≤A≤L
"Get info"			Y				B≤M, C, L, Ad<A
File content Modified		Y(s)	Y(s)	Y(s)	*Y	*N/Y	B ≤ Ad ≤L ≤M =A=C
File property changed (command)				Y			B≤ M, A, L, Ad<C
File property changed(get info)			Y	Y			B≤ M, L, Ad<A≤ C
File renamed						Y	B≤ M, L, A, C<Ad
File copy (original file)			Y				B≤ M, C, L, Ad<A
File copy (new file)			Y(b)	Y(f)	N/Y	Y(b)	B≤ M≤ L<A =Ad≤ C
File downloaded from email or from some websites	Y(b)	Y(f)	Y(b)	Y(f)	Y(f)	Y(f)	B≤ M=A=C=Ad=L
File downloaded from internet(the other result from last one)			Y(b)	Y(f)		Y(b)	B≤ M, L<A =Ad≤ C
File moved within same volume						Y	B≤ M, L, A, C<Ad
File moved to different volume			Y(b)	Y(f)		Y(b)	B≤ M, L<A =Ad≤ C
File compress(original files)			Y				B≤ M, L, C, Ad<A
File extracted				Y(f)		Y(b)	B≤ M, L, A< Ad≤ C
Image/Videos previewed			N/Y				B≤ M, C, L, Ad≤ A

Time attributes changes

Action	B	M	A	C	L	Ad	Rule
Folder Created	Y	Y	Y	Y	Y	Y	All same
Folder Accessed					Y(o2)		B ≤ M≤ C, Ad ,A≤ L
"Get info"							B≤ M, C, L, Ad, A
Folder Modified (create internal file)		Y	Y	Y	N/Y		B≤ Ad≤ L≤ M =C=A
File content Modified inside folder		Y(s)	Y(o1)	Y(s)	Y(o2)		B≤ Ad< L≤ A<M=C
File deleted inside folder		Y(d)		Y(d)	Y(o2)		B≤ A, Ad< L≤ M =C
Folder created, modified, deleted inside folder		Y		Y	Y		B≤ A, Ad< L≤ M =C
Folder property changed				Y			B≤ M, A, L, Ad<C
Folder renamed						Y	B≤M, L, A, C<Ad
Folder copy (original folder)			Y				B≤ M, C, L, Ad<A
Folder copy (new folder)			Y(b)	Y(f)	N/Y	Y(b)	B≤ M≤ L<A =Ad≤ C
Folder moved within same volume						Y	B≤ M, L, A, C<Ad
File moved to different volume			Y(b)	Y(f)		Y(b)	B≤ M, L<A =Ad≤ C
Folder compress(original folder)			Y				B≤ M, L, C, Ad<A
Folder extracted	N/Y	N/Y	N/Y	Y	N/Y	Y	B≤ M, L, A≤ Ad≤ C

Rules for files

Rule No.1: B=M=A=C=Ad,
the file may be just created or downloaded without any modification or access.
<*kMDItemWhereFroms*>

Rule No.2: A > (B, M, C),
accessed, copied to other location or compressed.

Last Opened ≥Access time, →accessed.
If several files' Access times are very close, then these files may be copied to other location in a batch or compressed together.

Rules for files

Rule No.3: M>B, the file's content has been modified.

Rule No.4: C > (B, M, A),
changed in the property or extracted
check the Date Added time,
Ad=C or C time is a little delayed to Ad , → extracted

If several files' Change times are the same as well as the Date Added times are very close, → extracted in a batch.

Date Added time ≠Change time, →changed in the property.

Rules for files

Rule No.5: C =A > (B, M),
check the Date Added time,
C=Ad, copied from other location or moved from other volume or downloaded from Internet.
C>Ad, then the file's property has been modified.

Rule No.6: A >C > (B, M),
several files have the similar situation → before the files are accessed, copied to other location or compressed---extracted or downloaded or copied or moved from other location.
We can then apply the Rule No. 4 or 5 to analyze the details without the Access time.

Rules for files

Rule No.7: Ad > (B, M, C, L),
renamed or moved from other place within the same volume.
Several files' Date Added times are very close, →moved in a batch from other location but the same volume.

Rule No. 8: For image and video files, the Last Opened time cannot be proof as the last time the files are viewed by the user, which means that the suspect cannot use the Last Opened time to claim that he does not view the file.
(The image and video files should be examined carefully as they may have some special cases.)

Rules for folders

Rule No.1: B=M=A=C=Ad,
created or just extracted without any modification.

Rule No.2: L > (B, M, A, C, Ad),
opened without any modification.

Rule No.3: M=A=C>B,
modified by creating internal files.

Rule No.4: M=C > (A, B),
deleted some file(s) inside the folder or modified the internal files' contents or done some operations on folders inside this folder.

Rules for folders

Rule No.5: A > (B, M, C),
copied to another location or compressed.

Rule No.6: C > (B, M, A),
check the Date Added time, if C=Ad, then the folder has just been extracted; if not, the folder's properties have been changed.

Rule No.7: C =A > (B, M),
copied from another location or moved from another volume or extracted.

Rules for folders

Rule No.8: A >C > (B, M),
check the Date Added time,
C=Ad, combine Rule No.5 and No.7, before the folder is copied to another location or compressed, the folder may be extracted or copied or moved from other location.

Rule No.9: Ad > (B, M, A, C, L),
renamed or moved from another location within the same volume.

Contents

Case Study

Step 1

• Only interested in some specific files or folders that may be related with the crime.

Step 2

• Specify the files in the timeline or use Spotlight to search the files or folders.

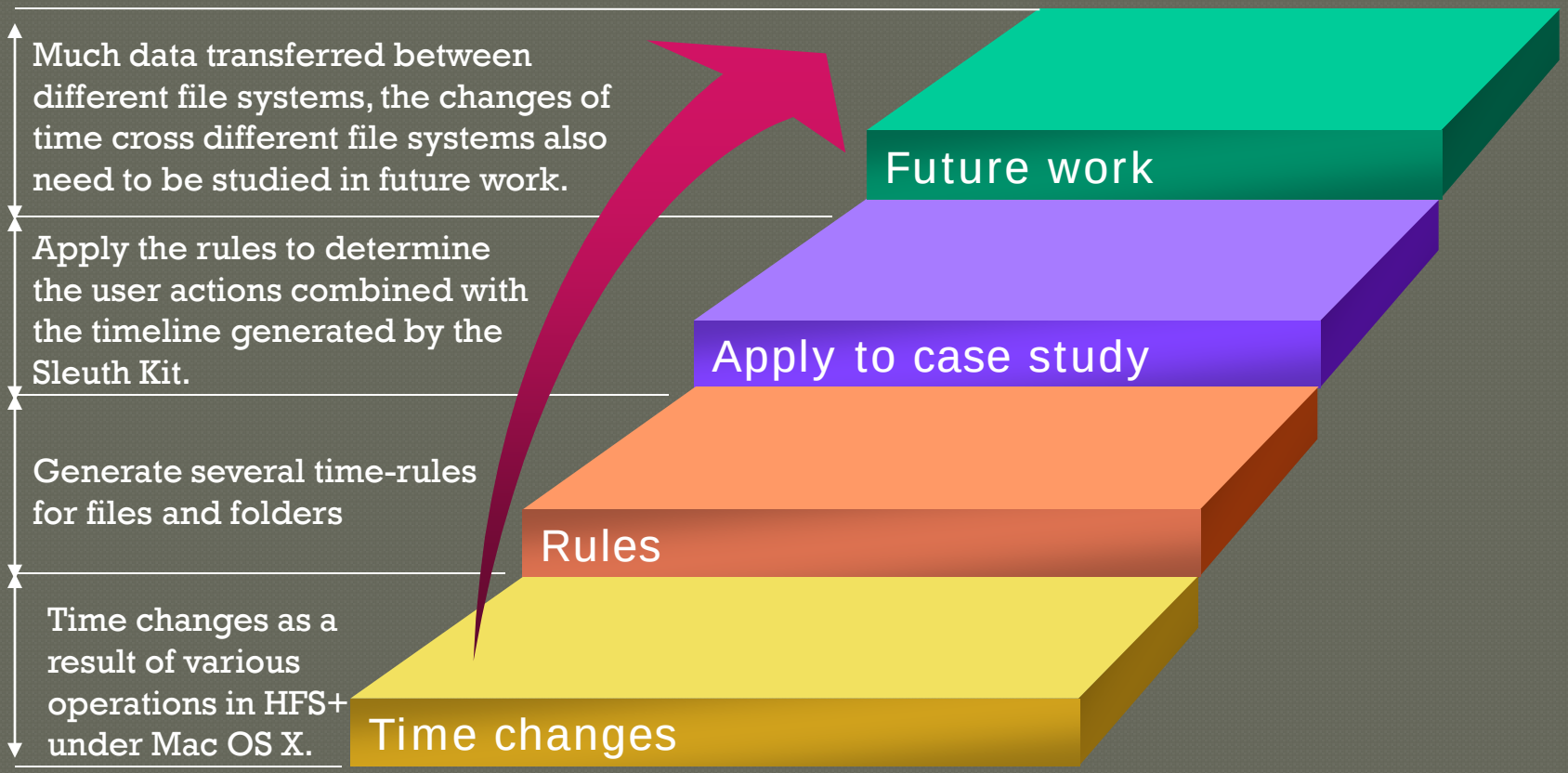
Step 3

• Use the Rules to find out what has been done on the files or folders.

• Maybe the suspect modified some important data or accessed confidential info or copied some sensitive files out.

Contents

Conclusion


Much data transferred between different file systems, the changes of time cross different file systems also need to be studied in future work.
Apply the rules to determine the user actions combined with the timeline generated by the Sleuth Kit.
Generate several time-rules for files and folders
Time changes as a result of various operations in HFS+ under Mac OS X.
Future work
Apply to case study
Rules
Time changes

Q&A

Thank you!

Questions?