ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Amir Alsbih and Christian Schindelhauer

Distributed Storage and

Computer Forensic

MAC Times

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

		Modification	Access	Change	Blocks
[1]	touch test	X 1171373610	X 1171373610	X 1171373610	(None)
[2]	echo "hello" > test	X 1171373739	1171373610	X 1171373739	X 2160644
[3]	ls -l test	1171373739	1171373610	1171373739	2160644
[4]	more test	1171373739	X 1171373932	1171373739	2160644
[5]	echo "olleh" > test	X 1171373952	1171373932	X 1171373952	X 2168699
[6]	echo "hello" >> test	X 1171373961	1171373932	X 1171373961	2168699
[7]	chown jess test	1171373961	1171373932	X 1171374156	2168699

	1	2	3	4	5	6	7
1171373610	mac	.a.	.a.				
1171373739		m.c	m.c	m.c			
1171373932				.a.	.a.	.a.	.a.
1171373952					m.c		
1171373961						m.c	m..
1171374156							..c

Source: Jess Garcia

3 Searching

Search for Unicode Strings

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- *#srch_strings [OPTIONS] filename*
  - *-a: all strings*
  - *-t: output offset in bytes {o=octal, x=hex, d=decimal}*
  - *-e l: little endian (unicode)*
  - *-e b: big endian (unicode)*
  - *-NUM: strings of at least NUM lenght (default 4)*

GREP

- *# grep [OPTIONS] pattern filename*
  - *-i: ignore case*
  - *-A NUM: print NUM lines AFTER pattern*
  - *-B NUM: print NUM lines BEFORE pattern*
  - *-f filename: file with list of words*

6

Lets do it practical

Marijuana case

- Joe Jacobs, 28, was arrested yesterday on charges of selling illegal drugs to high school students.
- The police are interested in finding Joe Jacob's supplier/producer of marijuana.
- Jacobs has denied selling drugs at any other school besides Smith Hill and refuses to provide the police with the name of his drug supplier/producer.
- They would like you to examine the floppy disk and provide answers to the following questions.

Marijuana case

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
2. What crucial data is available within the coverpage.jpg file and why is this data crucial?
3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
4. For each file, what processes were taken by the suspect to mask them from others?
5. What processes did you (the investigator) use to successfully examine the entire contents of each file?
6. What Microsoft program was used to create the Cover Page file. What is your proof (Proof is the key to getting this question right, not just making a guess).

Use a tool from now

- http://www.caine-live.net/
- http://www.deftlinux.net/
- Helix 2.0
- …

Tools used

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

- file: determine file type
- fsstat: Display general details of a file system
  - Sectorsize
  - Clustersize
  - Clusterchains(fromFAT)
- fls: List file and directory names in a disk image
- istat: Display details of a meta-data structure
- icat: Output the contents of a file based on its inode number
- blkcat: Display the contents of file system data unit in a disk image