EC521 HW3

Problem 0. Basics. [40 points]

I first started my disk forensic analysis by copying the disk image to my kali VM and searching the image with debugfs and sleuthkit / ingesting it into autopsy and starting a case. In autopsy I was able to see the directory structure of the image, see the image file system, metadata, content, block group, and inode information. As well as the exsisting deleted files in the image.

I was also able to mount the image in read only mode and use df to find the amount of disk space, number of blocks used / available, etc.

i. How much free space is available on the disk?

Out of the 200MB dsik image file:

**Free Block x Block size: 190214 x 1024 = 194,779,136B**

*df -T /dev/loop0*  
Filesystem Type 1K-blocks Used Available Use% Mounted on  
/dev/loop0 ext3 194641 4427 179982 3% /root/Desktop/hw3

210 MB — **195 MB free** (7.1% full)  
210 MB (209,715,200 bytes)  
Ext3 (version 1.0) — Mounted at /root/Desktop/hw3

METADATA INFORMATION

Inode Range: 1 - 48001  
Root Directory: 2  
**Free Inodes: 47969**

CONTENT INFORMATION

Block Range: 0 - 204799  
Block Size: 1024  
Reserved Blocks Before Block Groups: 1  
**Free Blocks: 190214**

BLOCK GROUP INFORMATION

Number of Block Groups: 25  
Inodes per group: 1920  
Blocks per group: 8192

ii. How many times may the image be mounted before a filesystem check is required?

Using debugfs and searching the file: debugfs -R "stats" /root/Desktop/hw3.img > /root/Desktop/debugfs\_stats.txt

.....

Mount count: 11  
**Maximum mount count: 23**  
Last checked: Thu Nov 8 00:11:12 2012  
Check interval: 15552000 (6 months)  
Next check after: Tue May 7 01:11:12 2013  
Lifetime writes: 16 MB

...

iii. What type of filesystem does the disk contain?

**Ext3 (version 1.0)**

FILE SYSTEM INFORMATION

**File System Type: Ext3**  
Volume Name:  
Volume ID: d2acbaf1c281ba999b4a72e3c614bf49

Last Written at: 2016-10-23 00:49:52 (EDT)  
Last Checked at: 2012-11-08 00:11:12 (EST)

**Last Mounted at: 2016-10-23 00:49:36 (EDT)**  
Unmounted properly  
Last mounted on: /root/Desktop/hw3

**Source OS: Linux**  
Dynamic Structure  
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index  
InCompat Features: Filetype,  
Read Only Compat Features: Sparse Super,

Journal ID: 00  
Journal Inode: 8

iv. To what host did the person using this disk try to connect securely?

After finding the m.pcap in the hidden .Trash directory, which I found by searching for pcaps since I knew they would contain info about remotely connecting. I was then able to copy the pcap to my VM and view to view the packets in Wireshark and seached for ssl and https connections and found that the host that the disk was trying to connect to with **ssl was 173.194.75.84 (accounts.l.google.com), 173.194.43.22 (googlemail.l.google.com), 173.194.43.47 (ssl.gstatic.com), 173.194.43.32 (ww3.l.google.com), 82.103.140.40 (secure.information.com)**

v. Name one file that contain a *block* in block group 0 (or state that no such file exists).

*Name one file that contain a block in block group 0 (or state that no such file exists).*

I was able to find the inodes in the Group 0 through debugfs stats and autopsy (**Inode Range: 1 - 1920 and Block Range: 1 - 8192**).

*debugfs /root/Desktop/hw3.img -R "testb 1 8192" | grep -v not | less*

This gave me a list of all blocks in use. I was also able to mount the image and use ils -i to see the directories and files transvering the file system and the associated inodes. I was able to find the following:

***/main/working/484.txt: inode 499***

**/main/.htpasswd: Inode 21**

**/words: Inode: 13**

vi. How many directories are in block group 2?

Using autopsy, istat and debugfs I was able to find

**Group: 2:**  
Inode Range: 3841 - 5760  
Block Range: 16385 - 24576  
Layout:  
Data bitmap: 16385 - 16385  
Inode bitmap: 16386 - 16386  
Inode Table: 16387 - 16626  
Data Blocks: 16387 - 16386, 16627 - 24576  
Free Inodes: 1910 (99%)  
Free Blocks: 6943 (84%)  
**Total Directories: 6**

*How many directories are in block group 2?*

Problem 0 grade: (**GRADER ONLY**)

Comments:

Problem 1. Investigation. [30 points]

i. What is the secret stored on the disk?

*What is the secret stored on the disk?*

I was able to find the secret stored on the disk by analyzing the exsisting and deleted files using autopsy and debugfs. In the main/etc directory I found the README~ file that contained the password for secret. I was also able to see multiple secret\* deleted files and a secret-aes-256-cdc exsisting file. After researching this file type and viewing it to see it was encrypted I determined I need to decrypt the aes-256 encryption using openssl. Once doing so I was able to put in secret's password and find the secret. See below:

*cat README~*  
The password for the secret is orangutan

*openssl aes-256-cbc -d -in secret.aes-256-cbc -out secret\_decrpt.txt*  
enter aes-256-cbc decryption password:

*cat secret\_decrpt.txt*   
**The secret is that there is no secret.**

ii. Where is the an ece letterhead file?

Found by searching the sleuth kit / autopsy:

**~/main/Downloads/ece\_letterhead.doc (It was deleted but is recoverable.)**

Also by using the fls tool, fls -rd path/to/image, and greping the output for **letterhead** to find the delete file. THen I was able to follow the path up to determine my answer.

*Where is the an ece letterhead file?*

iii. *Find a file with password hashes, and crack as many of them as you can.*

Using autopsy I was able to locate the hidden file **.htpasswd**. After mounting the image (or using debugfs) I was copy the file to my desktop and run john the ripper to get the passwords:

ng:82120692: [qil@secret.net](mailto:qil@secret.net):0:8107051632

yune:iloveyou: [wa@secret.org](mailto:wa@secret.org):0:8106443161

oiiu:flyheart: [liut@secret.org](mailto:liut@secret.org):0:8106860097

xuhen:15930380: [xxs@secret.net](mailto:xxs@secret.net):0:8106445209

Ahuga:apl12345: [apel@secret.net](mailto:apel@secret.net):0:8106859832

uong:unseenon: [bdu@secret.net](mailto:bdu@secret.net):0:8106518392

Baerk:flatso: [bb@secret.net](mailto:bb@secret.net):0:8106440541

ELi:leo0715: [l@secret.org](mailto:l@secret.org):0:8108345828

klin:Chunwah8: [wo@secret.net](mailto:wo@secret.net):0:8106860047

gshu:19900214: [kz@secret.net](mailto:kz@secret.net):0:8107251681

Du:hengdude: [he@secret.net](mailto:he@secret.net):0:8106821553

yNg:kelly711: [jng@secret.net](mailto:jng@secret.net):0:8106784090

io:123qwe: [m@secret.net](mailto:m@secret.net):0:8106594647

arda:IDontkno: [rich@secret.net](mailto:rich@secret.net):0:8106859786

rAhdd:password: [samah@secret.net](mailto:samah@secret.net):0:8107909018

Thr:goshdont: [khur@secret.net](mailto:khur@secret.net):0:8106860294

eabb:Wooleys: [mcn@secret.net](mailto:mcn@secret.net):0:8107402267

utkami:xionxion: [kkawa@secret.net](mailto:kkawa@secret.net):0:8108014323

Aam:SuperSku: [mrca@secret.net](mailto:mrca@secret.net):0:8107327530

olas:423535: [nip@secret.net](mailto:nip@secret.net):0:8106860062

Vse:dn7fg88t: [vp@secret.net](mailto:vp@secret.net):0:8107304025

iv. Who on earth uses such *\_\_*? Fill in the blank.

*Fill in the blank.*

Using autopsy and icat, I was able to find to the answer to this fill in the blank. After following the question to examine inode 11, I viewed the inodes contents and saw it contained a direct pointer to a direct data block 6657. After viewing the data in this block i was able to find "**Who on earth uses such file names?**" This was visable not only using autopsy and the slueth toolkit but it was also visable when viewing inode 11 stats using icat. Both are displayed below.

*icat /root/Desktop/hw3.img 11*  
**Who on earth uses such file names?**

*Autopsy:*

ASCII Contents of F**ragment 6657** in hw3\_copy.img-0-0

**Who on earth uses such file names?**

Problem 1 grade: (**GRADER ONLY**)

Comments:

Problem 2. Digging deeper. [30 points]

i. Look at the words file on the disk, which appears to be a common word list found on linux machines at /usr/share/words/dict, but at least one word is missing ... what words are missing?

Using vimdiff and diff I was able to find what word is missing:

*vimdiff*

**diff /root/Desktop/words /root/Desktop/hw3\_drive\_find/words**  
48814d48813 (<-- line number difference)  
**< gullible**

ii. Use regular expressions to find a word with at least 3 consonants in a row. [(1)](https://algorithmics.bu.edu/fw/EC521/HomeworkThree" \l "FootNote1note) Include the regular expressions you used to get this result.

Use regular expressions to find a word with at least 3 consonants in a row. Include the regular expressions you used to get this result.

**grep -r "[bcdfghjlmnpqrstvwxz]\{3,\}"**

The regex found all the words containing 3 consonants in a row in the disk image. The regex above looks for 3 or more consonants (considering y as a vowel). There were over 1000 results with the first few being listed below:

words:Accra  
words:Accra's  
words:Acts  
words:Adolph  
words:Adolph's  
words:Advents  
words:Aelfric  
...

iii. Find a large file that was deleted from the volume, and answer the following questions about it:

I was able to recover all deleted recovered files using entundelete. I was also able to see all deleted files and thier sizes in debugfs with lsdel and autopsy. After recovering the files that were recoverable I was able to view them in the REOVERED\_FILES directory created and found the largaest file that was deleted, recovered: **1.txt**

*extundelete /root/Desktop/hw3\_copy.img --restore-all*  
NOTICE: Extended attributes are not restored.  
Loading filesystem metadata ... 25 groups loaded.  
Loading journal descriptors ... 4003 descriptors loaded.  
Searching for recoverable inodes in directory / ...   
5 recoverable inodes found.  
Looking through the directory structure for deleted files ...   
Block 825899312 is out of range.  
3 recoverable inodes still lost.  
Unable to restore inode 11 (file.11): Space has been reallocated.  
Unable to restore inode 12 (file.12): Space has been reallocated.  
Unable to restore inode 13 (file.13): Space has been reallocated.

1. What service likely created the data in this file?
   1. The file contains HTTP POST and GET requests, **web server logs**, made by a web sever.
2. Write a regular expression that matches **exactly** IPs in our target subnet for class (i.e. 10.241.13.x). Are any of these IPs in the file?
   1. ***grep -Ea '10\.241\.13\.[0-9]{1,3}' 1.txt OR grep -Ea '10\.241\.13\.[0-255]{1}' 1.txt***  
      10.241.13.29 [29:23:59:31] "GET / HTTP/1.0" 200 4889  
      10.241.13.29 [29:23:59:33] "GET /icons/circle\_logo\_small.gif HTTP/1.0" 200 2624  
      10.241.13.29 [30:00:00:05] "GET /icons/book.gif HTTP/1.0" 200 156  
      10.241.13.29 [30:00:00:05] "GET /logos/small\_gopher.gif HTTP/1.0" 200 935  
      10.241.13.29 [30:00:00:06] "GET /logos/small\_ftp.gif HTTP/1.0" 200 124  
      10.241.13.29 [30:00:00:09] "GET /logos/us-flag.gif HTTP/1.0" 200 2788  
      10.241.13.29 [30:00:00:17] "GET /icons/ok2-0.gif HTTP/1.0" 200 231  
      10.241.13.29 [30:00:00:31] "GET /information.html HTTP/1.0" 200 617  
      10.241.13.29 [30:00:00:33] "GET /icons/people.gif HTTP/1.0" 200 224
3. How many unique IP addresses are there in the file (and how did you determine this)?
   1. *grep -oa '[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}' 1.txt | sort | uniq ==>* **5**  
      10.215.67.47  
      10.241.13.29  
      134.67.99.11  
      140.112.68.241  
      141.243.1.241
   2. Or you can also use: *grep -E -o -a '(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)' 1.txt | sort | uniq*

iv. What is wrong with inode 11? What information is this "problem" hiding?

Using sutopsy, istat, icat and debugfs I was able to find what group inode 11 was a part of, what direct block it was pointing to and what file and data that direct block contained. When I viewed the files and directories in the home directory of the image I found inode 11 to be associated with a file or directory that is blank. Running istat on this inode shows it has a link to a direct block 6657. It does show the inode is allocated but points to the block/fragment 6657, which is in range of the file system, but it also **points to blocks outside of the file system (see below)**. This is what's wrong with the inode. Using extundelete, bless , and debugfs: imap <11> to see that the inode info is stored in block 95, then using autopsy to see the Hex of block 95 and see that**Password:FOO** is stored in slack space.

*extundelete --inode 11 /root/Desktop/hw3\_copy.img*   
NOTICE: Extended attributes are not restored.  
Loading filesystem metadata ... 25 groups loaded.  
Group: 0  
Contents of inode 11:  
0000 | a4 81 00 00 23 00 00 00 06 8f 35 54 01 8f 35 54 | ....#.....5T..5T  
0010 | 01 8f 35 54 00 00 00 00 00 00 01 00 02 00 00 00 | ..5T............  
0020 | 00 00 00 00 00 00 00 00 01 1a 00 00 50 61 73 73 | ...........**.Pass**  
0030 | 77 6f 72 64 3a 46 4f 4f 00 00 00 00 00 00 00 00 | **word:FOO**........  
0040 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................  
0050 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................  
0060 | 00 00 00 00 63 87 a4 17 00 00 00 00 00 00 00 00 | ....c...........  
0070 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................  
  
Inode is Allocated  
File mode: 33188  
Low 16 bits of Owner Uid: 0  
Size in bytes: 35  
Access time: 1412796166  
Creation time: 1412796161  
Modification time: 1412796161  
Deletion Time: 0  
Low 16 bits of Group Id: 0  
Links count: 1  
Blocks count: 2  
File flags: 0  
File version (for NFS): 396658531  
File ACL: 0  
Directory ACL: 0  
Fragment address: 0  
**Direct blocks: 6657,** **1936941392, 1685221239, 1330595386**, 0, 0, 0, 0, 0, 0, 0, 0  
Indirect block: 0  
Double indirect block: 0  
Triple indirect block: 0

FS Error count: 8  
First error time: Sat Oct 22 23:04:29 2016  
First error function: ext4\_iget  
First error line #: 4219  
**First error inode #: 11**  
First error block #: 1936941392  
Last error time: Sun Oct 23 00:49:36 2016  
**Last error function: ext4\_iget**  
Last error line #: 4219  
**Last error inode #: 11**  
**Last error block #: 1936941392**  
Directories: 10

Viewing the contents of the 6657 block and using icat to see the data that inode 11 leads to I was able to find the following:

*debugfs: ls -l (in the home directory)*

* 1. 40755 (2) 0 0 1024 8-Oct-2014 15:22 .  
     2 40755 (2) 0 0 1024 8-Oct-2014 15:22 ..  
     3847 40755 (2) 0 0 1024 8-Nov-2012 00:20 .Trash  
     18 40700 (2) 0 0 102422-Oct-2016 23:31 main  
     13 100644 (1) 0 0 938839 8-Oct-2014 11:15 words  
     **11 100644 (1) 0 0 35 8-Oct-2014 15:22**

*istat /root/Desktop/hw3.img 11*   
**inode: 11**  
Allocated  
Group: 0  
Generation Id: 396658531  
uid / gid: 0 / 0  
mode: rrw-r--r--  
size: 35  
num of links: 1

Inode Times:  
Accessed: 2014-10-08 15:22:46 (EDT)  
File Modified: 2014-10-08 15:22:41 (EDT)  
Inode Modified: 2014-10-08 15:22:41 (EDT)

**Direct Blocks:**  
**6657**

*icat /root/Desktop/hw3.img 11*  
**Who on earth uses such file names?**

*Autopsy:*

ASCII Contents of F**ragment 6657** in hw3\_copy.img-0-0

**Who on earth uses such file names?**