Digital Forensics Lab
Lab 10
Autopsy

Submitted from:

Abdul Sami Qasim (22i-1725)

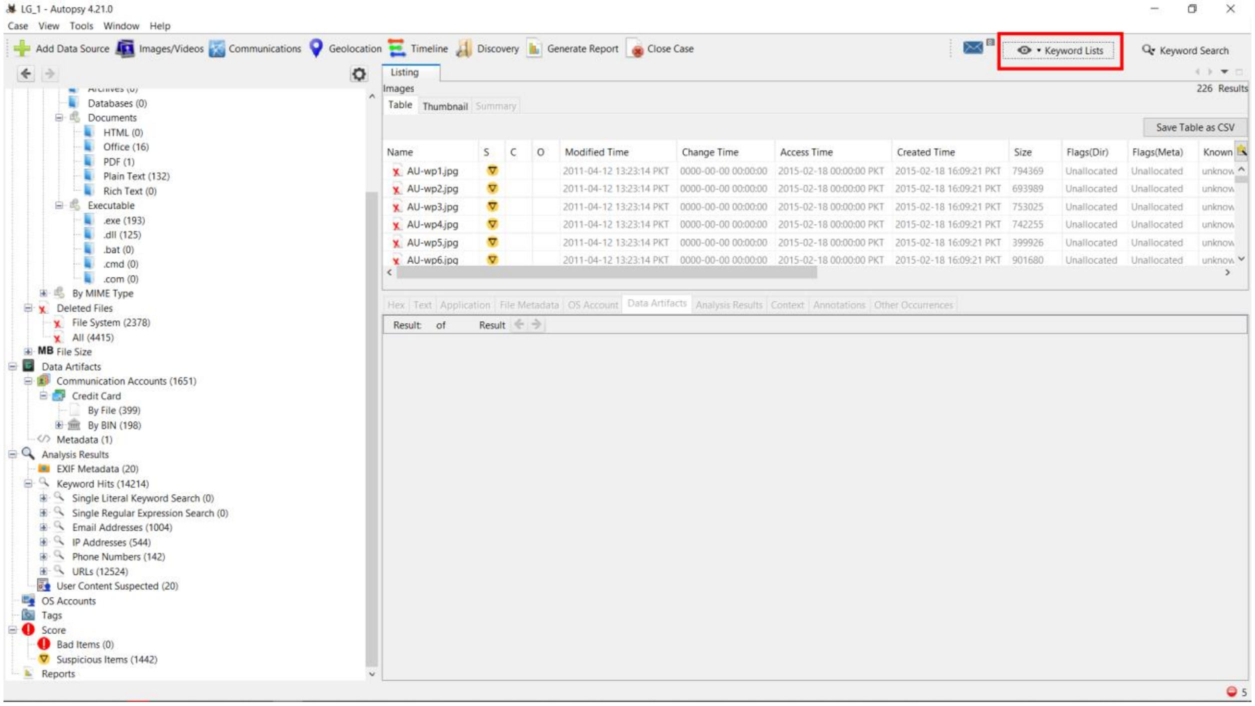
CY-D

Submitted to:

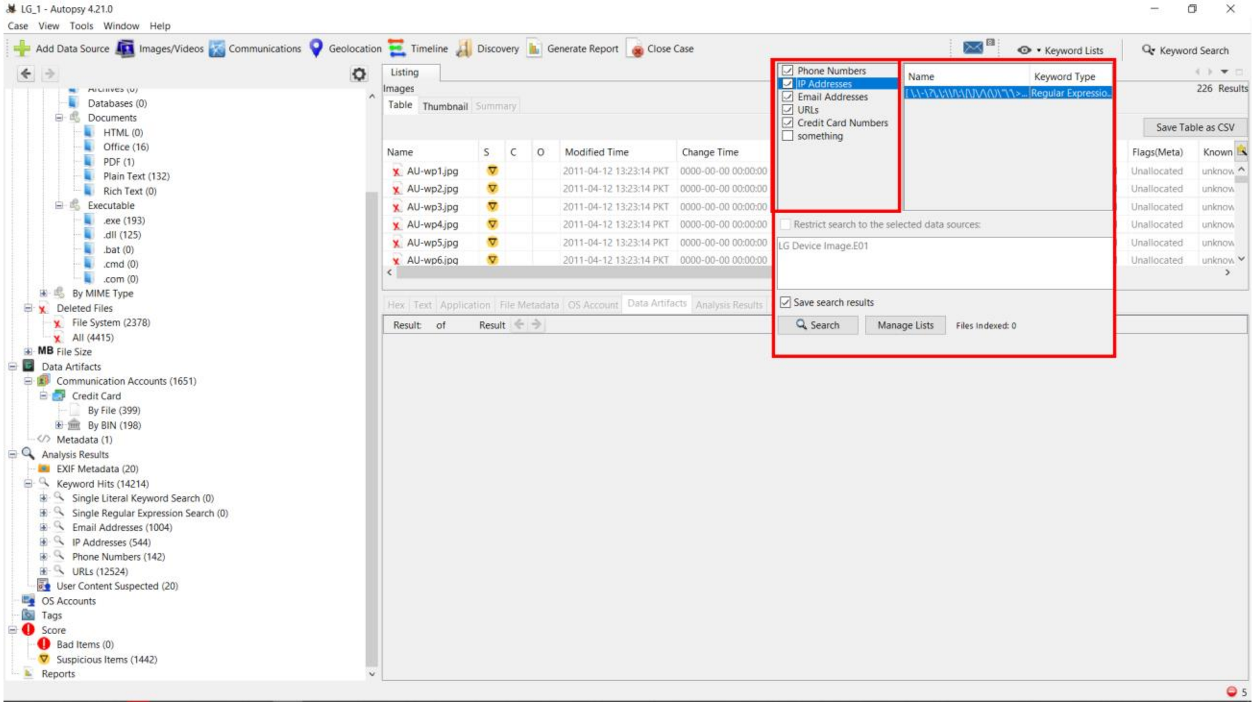
Sir Ubaidullah

Keyword Lists Search:

Using autopsy to search for Ip addresses, emails, phone numbers and URLs



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
AU-wp1.jpg	▽			2011-04-12 13:23:14 PKT	0000-00-00 00:00:00	2015-02-18 00:00:00 PKT	2015-02-18 16:09:21 PKT	794369	Unallocated	Unallocated	unknow
AU-wp2.jpg	▽			2011-04-12 13:23:14 PKT	0000-00-00 00:00:00	2015-02-18 00:00:00 PKT	2015-02-18 16:09:21 PKT	693989	Unallocated	Unallocated	unknow
AU-wp3.jpg	▽			2011-04-12 13:23:14 PKT	0000-00-00 00:00:00	2015-02-18 00:00:00 PKT	2015-02-18 16:09:21 PKT	753025	Unallocated	Unallocated	unknow
AU-wp4.jpg	▽			2011-04-12 13:23:14 PKT	0000-00-00 00:00:00	2015-02-18 00:00:00 PKT	2015-02-18 16:09:21 PKT	742255	Unallocated	Unallocated	unknow
AU-wp5.jpg	▽			2011-04-12 13:23:14 PKT	0000-00-00 00:00:00	2015-02-18 00:00:00 PKT	2015-02-18 16:09:21 PKT	399926	Unallocated	Unallocated	unknow
AU-wp6.jpg	▽			2011-04-12 13:23:14 PKT	0000-00-00 00:00:00	2015-02-18 00:00:00 PKT	2015-02-18 16:09:21 PKT	901680	Unallocated	Unallocated	unknow



☑ Phone Numbers
☑ IP Addresses
☑ Email Addresses
☑ URLs
☑ Credit Card Numbers
☐ something

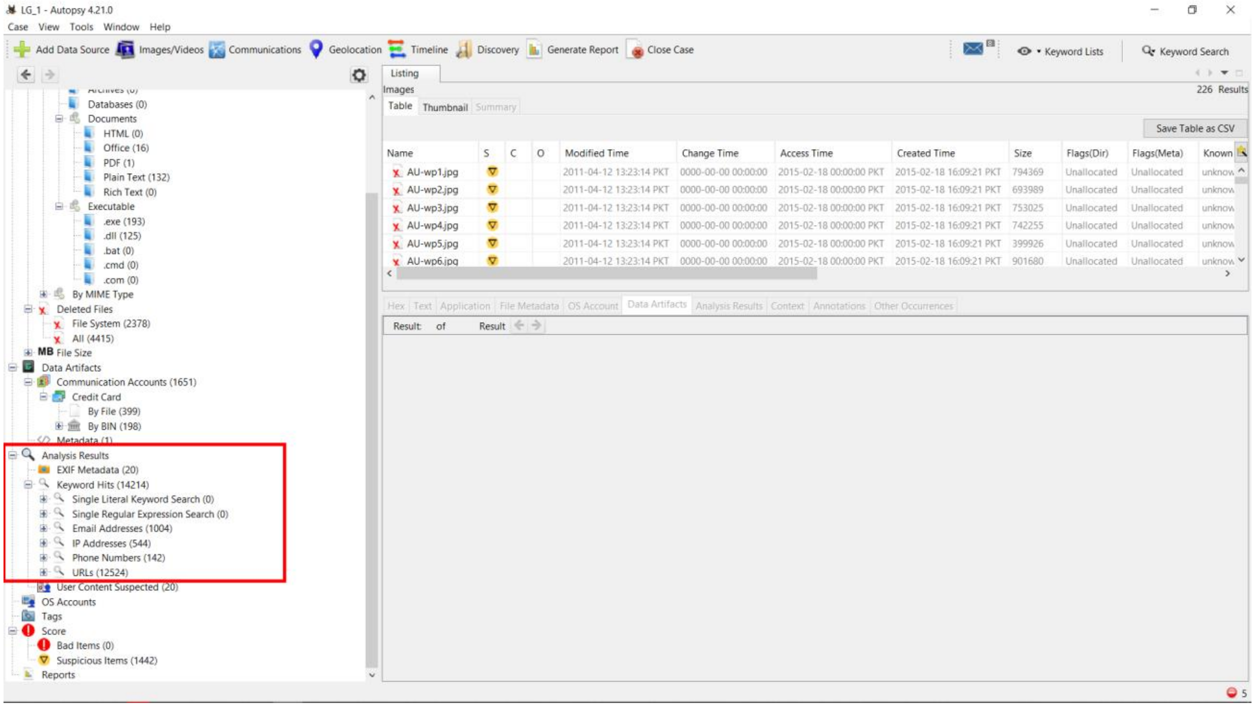
Name	Keyword Type
[\.\-\?\.\:\\\\\:\[\]\/\(\)\"\'\>...	Regular Expressio...

☐ Restrict search to the selected data sources:

LG Device Image.E01

☑ Save search results

Files Indexed: 0



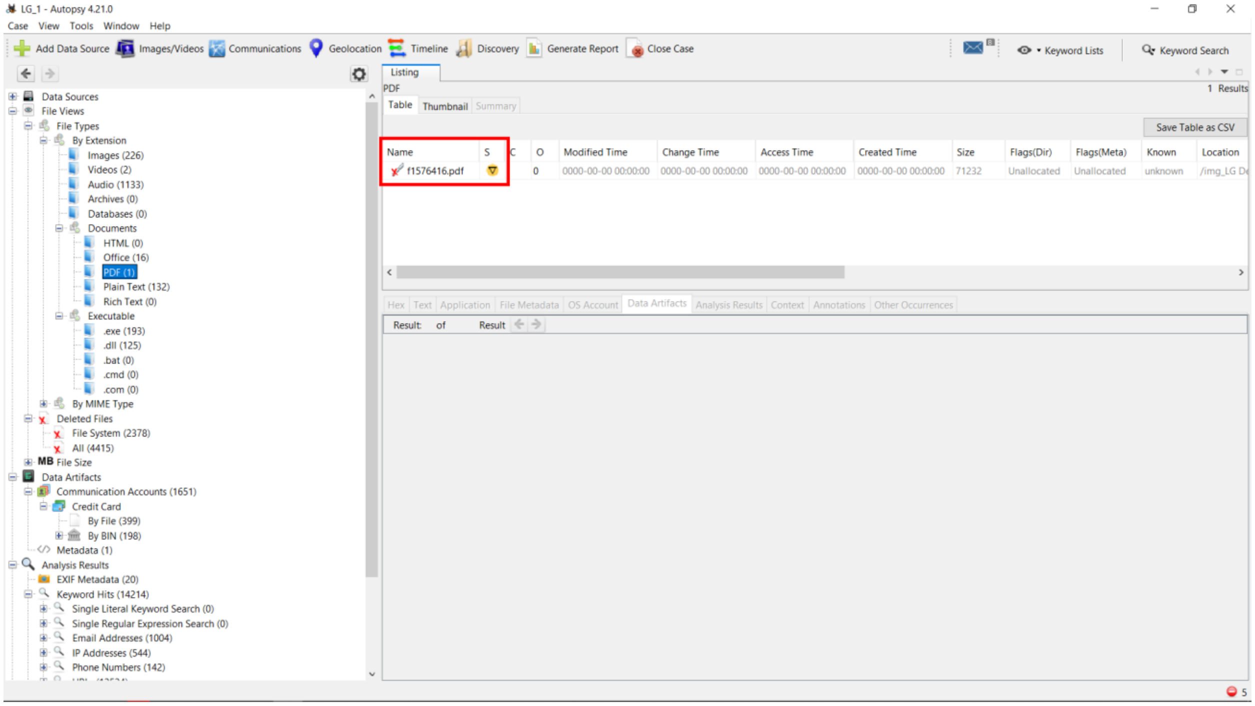
```
        Archives (0)
        Databases (0)
        Documents
            HTML (0)
            Office (16)
            PDF (1)
            Plain Text (132)
            Rich Text (0)
        Executable
            .exe (193)
            .dll (125)
            .bat (0)
            .cmd (0)
            .com (0)
    By MIME Type
  Deleted Files
    File System (2378)
    All (4415)
  MB File Size
Data Artifacts
  Communication Accounts (1651)
    Credit Card
      By File (399)
      By BIN (198)
  Metadata (1)
Analysis Results
  EXIF Metadata (20)
  Keyword Hits (14214)
    Single Literal Keyword Search (0)
    Single Regular Expression Search (0)
    Email Addresses (1004)
    IP Addresses (544)
    Phone Numbers (142)
    URLs (12524)
  User Content Suspected (20)
OS Accounts
Tags
Score
  Bad Items (0)
  Suspicious Items (1442)
Reports
```

Images 226 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
AU-wp1.jpg	▽			2011-04-12 13:23:14 PKT	0000-00-00 00:00:00	2015-02-18 00:00:00 PKT	2015-02-18 16:09:21 PKT	794369	Unallocated	Unallocated	unknow
AU-wp2.jpg	▽			2011-04-12 13:23:14 PKT	0000-00-00 00:00:00	2015-02-18 00:00:00 PKT	2015-02-18 16:09:21 PKT	693989	Unallocated	Unallocated	unknow
AU-wp3.jpg	▽			2011-04-12 13:23:14 PKT	0000-00-00 00:00:00	2015-02-18 00:00:00 PKT	2015-02-18 16:09:21 PKT	753025	Unallocated	Unallocated	unknow
AU-wp4.jpg	▽			2011-04-12 13:23:14 PKT	0000-00-00 00:00:00	2015-02-18 00:00:00 PKT	2015-02-18 16:09:21 PKT	742255	Unallocated	Unallocated	unknow
AU-wp5.jpg	▽			2011-04-12 13:23:14 PKT	0000-00-00 00:00:00	2015-02-18 00:00:00 PKT	2015-02-18 16:09:21 PKT	399926	Unallocated	Unallocated	unknow
AU-wp6.jpg	▽			2011-04-12 13:23:14 PKT	0000-00-00 00:00:00	2015-02-18 00:00:00 PKT	2015-02-18 16:09:21 PKT	901680	Unallocated	Unallocated	unknow

Result: of Result

File Password Cracking:



```
Data Sources
File Views
  File Types
    By Extension
        Images (226)
        Videos (2)
        Audio (1133)
        Archives (0)
        Databases (0)
        Documents
            HTML (0)
            Office (16)
            PDF (1)
            Plain Text (132)
            Rich Text (0)
        Executable
            .exe (193)
            .dll (125)
            .bat (0)
            .cmd (0)
            .com (0)
    By MIME Type
  Deleted Files
    File System (2378)
    All (4415)
  MB File Size
Data Artifacts
  Communication Accounts (1651)
    Credit Card
      By File (399)
      By BIN (198)
  Metadata (1)
Analysis Results
  EXIF Metadata (20)
  Keyword Hits (14214)
    Single Literal Keyword Search (0)
    Single Regular Expression Search (0)
    Email Addresses (1004)
    IP Addresses (544)
    Phone Numbers (142)
```

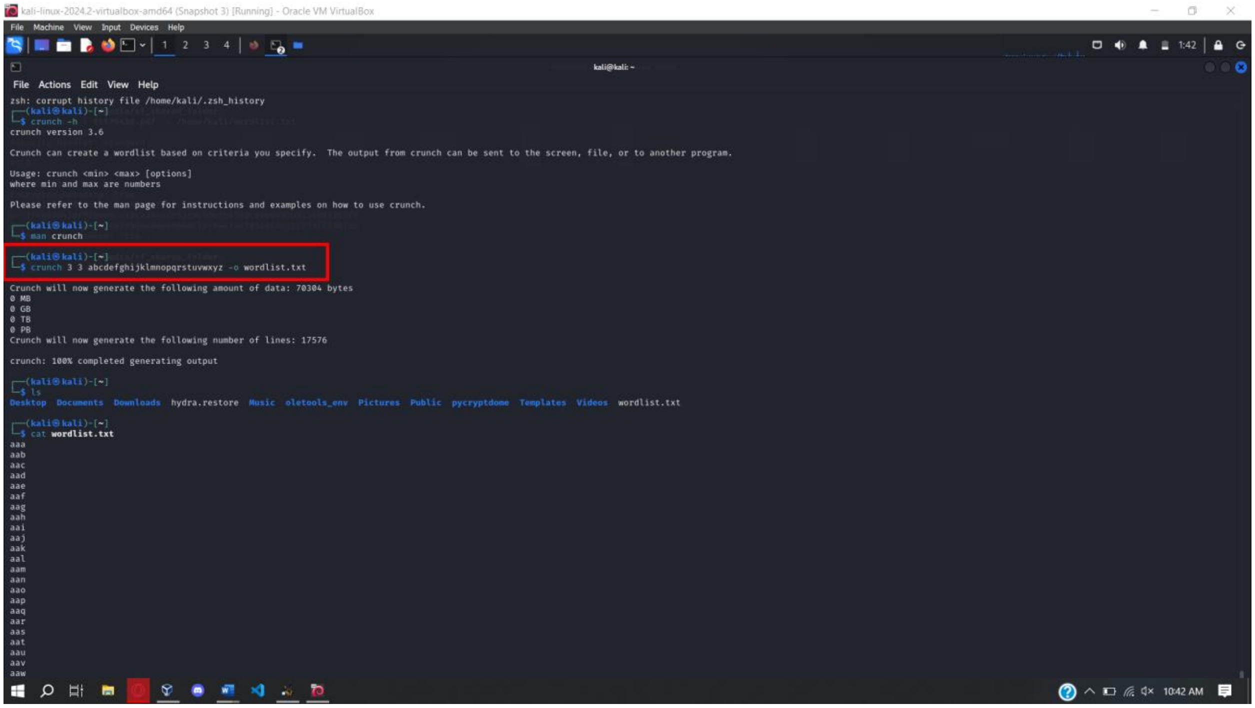
PDF 1 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f1576416.pdf	▽		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	71232	Unallocated	Unallocated	unknown	/img_LG De

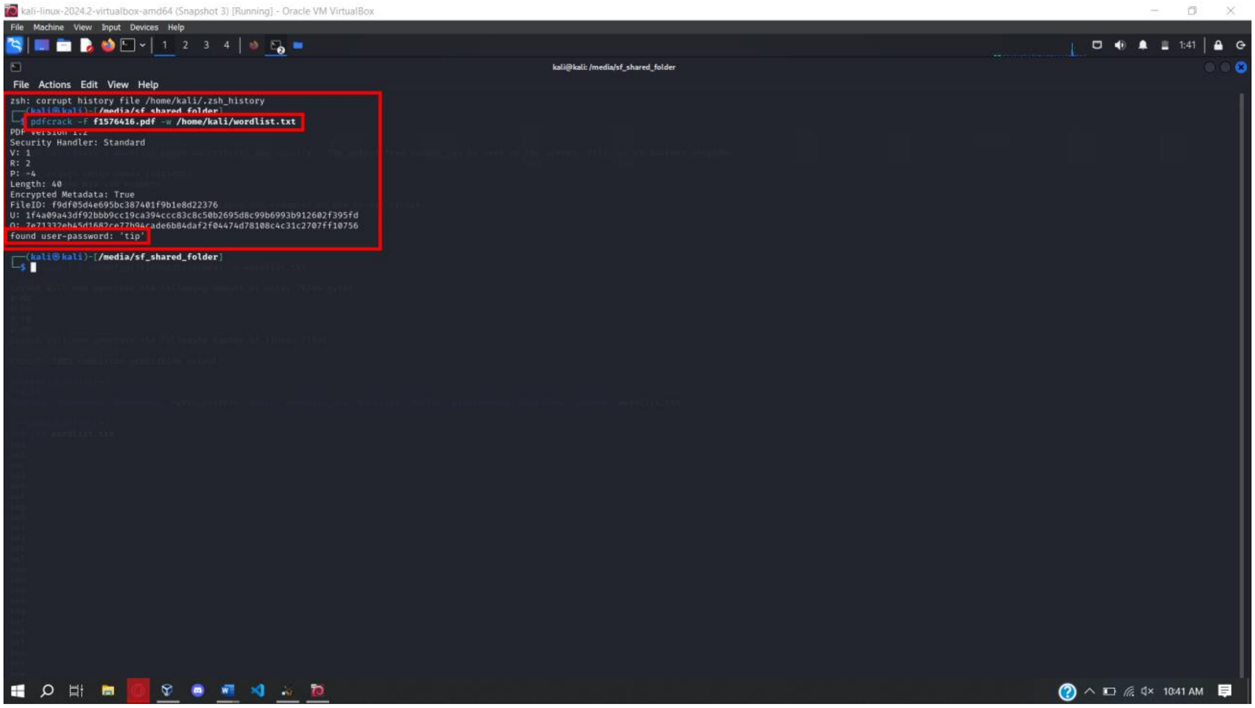
Result: of Result

I found this password protected file and now I'm going to crack it's password. I've exported the file into kali linux and I'm going to use

1. Crunch to make a 3 small alphabet wordlist.
2. Pdfcrack to bruteforce the password.



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ crunch -h
crunch version 3.6

Crunch can create a wordlist based on criteria you specify.  The output from crunch can be sent to the screen, file, or to another program.

Usage: crunch <min> <max> [options]
where min and max are numbers

Please refer to the man page for instructions and examples on how to use crunch.

┌──(kali㉿kali)-[~]
└─$ man crunch

┌──(kali㉿kali)-[~]
└─$ crunch 3 3 abcdefghijklmnopqrstuvwxyz -o wordlist.txt
Crunch will now generate the following amount of data: 70304 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 17576

crunch: 100% completed generating output

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  hydra.restore  Music  oletools_env  Pictures  Public  pycryptdome  Templates  Videos  wordlist.txt

┌──(kali㉿kali)-[~]
└─$ cat wordlist.txt
aaa
aab
aac
aad
aae
aaf
aag
aah
aai
aaj
aak
aal
aam
aan
aao
aap
aaq
aar
aas
aat
aau
aav
aaw
```

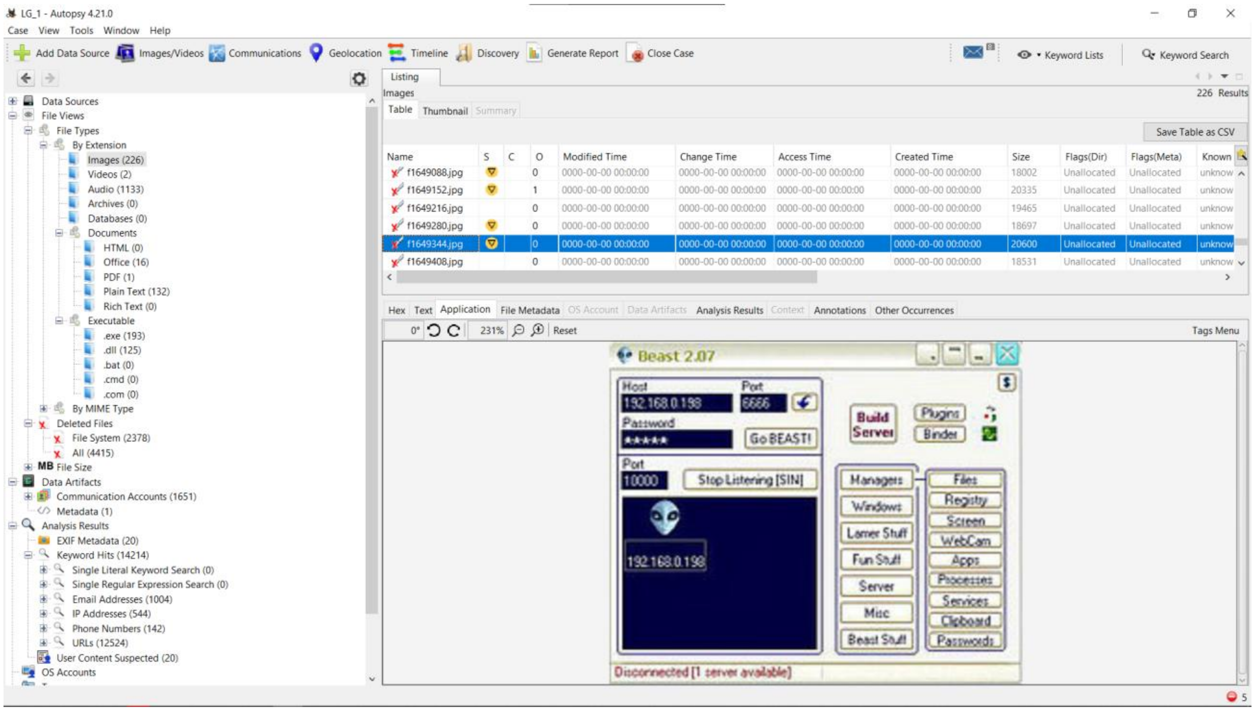


```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[/media/sf_shared_folder]
└─$ pdfcrack -f f1576416.pdf -w /home/kali/wordlist.txt
PDF version 1.2
Security Handler: Standard
V: 1
R: 2
P: -4
Length: 40
Encrypted Metadata: True
FileID: f9df05d4e695bc387401f9b1e8d22376
U: 1f4a09a43df92bbb9cc19ca394ccc83c8c50b2695d8c99b6993b912602f395fd
O: 7e71332eb45d1682ce77b94cade6b84daf2f04474d78108c4c31c2707ff10756
found user-password: 'tip'

┌──(kali㉿kali)-[/media/sf_shared_folder]
└─$ 
```

The password for the file is “tip”.

Interesting find:

While going through the images, I found this image which is pretty interesting:



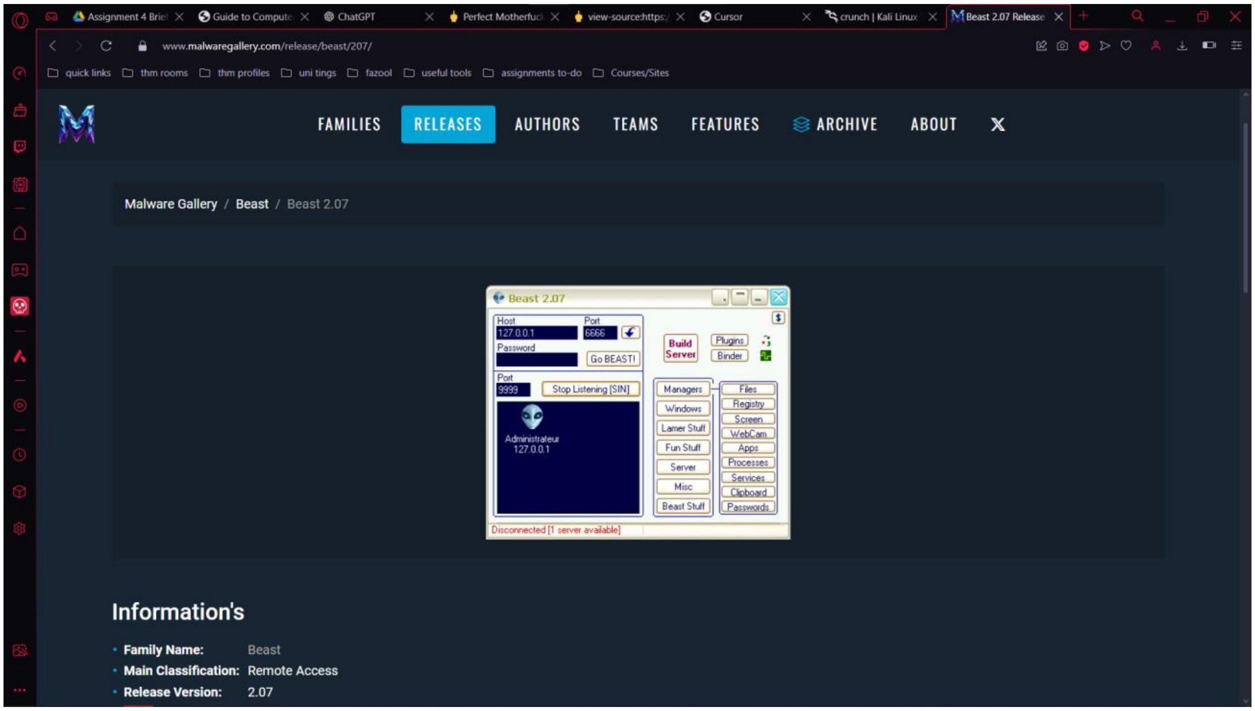
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
f1649088.jpg	▽		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	18002	Unallocated	Unallocated	unknow
f1649152.jpg	▽		1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20335	Unallocated	Unallocated	unknow
f1649216.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	19465	Unallocated	Unallocated	unknow
f1649280.jpg	▽		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	18697	Unallocated	Unallocated	unknow
f1649344.jpg	▽		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20600	Unallocated	Unallocated	unknow
f1649408.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	18531	Unallocated	Unallocated	unknow

Host: 192.168.0.198
Port: 6666
Password: *****
Port: 10000

192.168.0.198

Disconnected [1 server available]

A quick search about beast 2.07 gave me this:



Host: 127.0.0.1
Port: 6666
Password:
Port: 9999

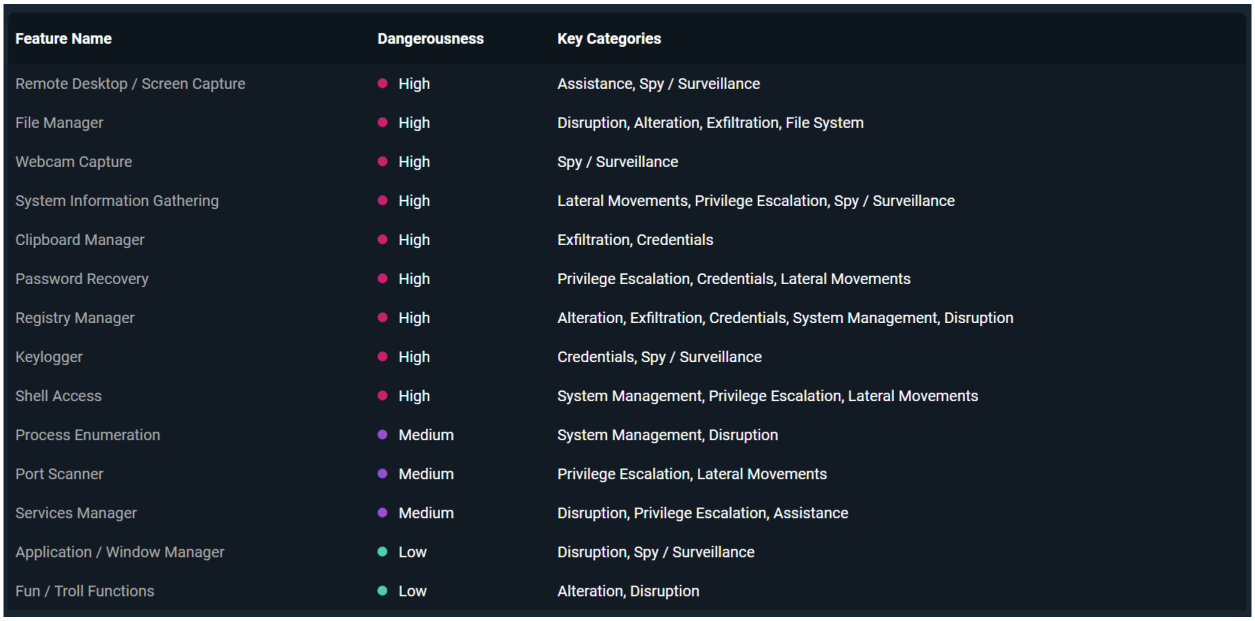
Administrateur
127.0.0.1

Disconnected [1 server available]

Information's

- **Family Name:** Beast
- **Main Classification:** Remote Access
- **Release Version:** 2.07

This is a trojan which has the following “features”:



Feature Name	Dangerousness	Key Categories
Remote Desktop / Screen Capture	● High	Assistance, Spy / Surveillance
File Manager	● High	Disruption, Alteration, Exfiltration, File System
Webcam Capture	● High	Spy / Surveillance
System Information Gathering	● High	Lateral Movements, Privilege Escalation, Spy / Surveillance
Clipboard Manager	● High	Exfiltration, Credentials
Password Recovery	● High	Privilege Escalation, Credentials, Lateral Movements
Registry Manager	● High	Alteration, Exfiltration, Credentials, System Management, Disruption
Keylogger	● High	Credentials, Spy / Surveillance
Shell Access	● High	System Management, Privilege Escalation, Lateral Movements
Process Enumeration	● Medium	System Management, Disruption
Port Scanner	● Medium	Privilege Escalation, Lateral Movements
Services Manager	● Medium	Disruption, Privilege Escalation, Assistance
Application / Window Manager	● Low	Disruption, Spy / Surveillance
Fun / Troll Functions	● Low	Alteration, Disruption