

# Cyber Security Workshop 2015

## "System Hacking"

By

Ashish Belwase

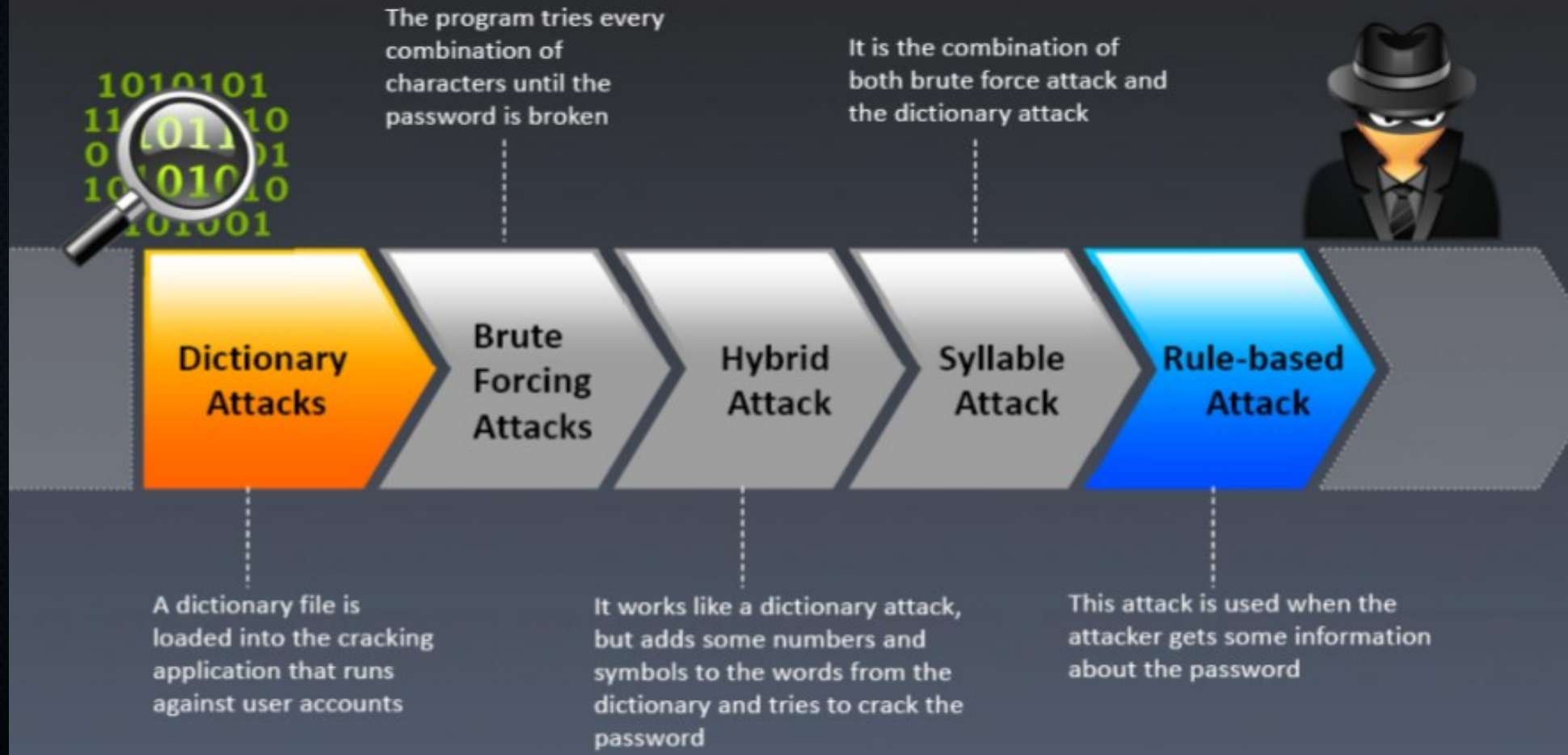
KU Security Researchers

# Password Cracking

- Most commonly used Attacks
- Depends on password complexity

# Password Cracking

## Password Cracking Techniques





# Password Cracking

- Cracking Windows Hash
  - Cd to system32/config
  - Bkhive SYSTEM /home/hash.txt
  - Samdump2 SAM /home/hash.txt > /home/hasfile.txt
  - More /home/hashfile.txt # display users
  - John /home/hashfile.txt --format=nt2 -users=test
- Cain & Abel
- Rainbow Table = ophcrack
  - <https://www.objectif-securite.ch/en/ophcrack.php>

# Password Cracking

- Cracking Linux Passwords
  - /etc/shadow
  - John shadow
- Hashcat
  - Cp /etc/shadow hash.lst
  - Cat /etc/login.DEFS | grep ENCRYPT >> check hashing algo
  - Get password.lst
  - Hashcat -m 1800 -a 0 -o cracked.txt hash.lst password.txt

# Generating wordlist

- Some information about passwords
- Crunch <min length> <max length> <list of strings> <dest>
- Crunch 4 4 012345 pw.txt



# Bruteforcing

- FTP
  - Medusa -h 192.168.5.1 -U username.lst -P pass.lst -M ftp
- Router
  - Medusa -h 192.168.0.1 -U admin -P pass.lst -M http

# Password Sniffing

- FileZilla, Wireshark, ip.addr==<ip>

The image shows a Wireshark packet capture interface. The filter bar at the top is set to `ip.addr==192.168.0.7`. The packet list shows several packets, with packet 179 highlighted in orange. The packet details pane shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and File Transfer Protocol (FTP). The FTP section shows the request command `PASS` with the argument `abcd`. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
170	2.936253	8.8.8.8	192.168.0.7	DNS	85	Standard query response A 116.90.239.10
171	2.936683	192.168.0.7	116.90.239.10	TCP	74	24463 > ftp [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=4788691 TSecr=0 WS=128
172	2.939549	116.90.239.10	192.168.0.7	TCP	74	ftp > 24463 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=613263161 TSecr=0
173	2.939601	192.168.0.7	116.90.239.10	TCP	66	24463 > ftp [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=4788692 TSecr=613263161
174	2.941959	116.90.239.10	192.168.0.7	FTP	86	Response: 220 (vsFTPd 2.2.2)
175	2.941993	192.168.0.7	116.90.239.10	TCP	66	24463 > ftp [ACK] Seq=1 Ack=21 Win=14720 Len=0 TSval=4788692 TSecr=613263163
176	2.942433	192.168.0.7	116.90.239.10	FTP	77	Request: USER test
177	2.943380	116.90.239.10	192.168.0.7	TCP	66	ftp > 24463 [ACK] Seq=21 Ack=12 Win=14592 Len=0 TSval=613263164 TSecr=4788692
178	2.943400	116.90.239.10	192.168.0.7	FTP	100	Response: 331 Please specify the password.
179	2.943543	192.168.0.7	116.90.239.10	FTP	77	Request: PASS abcd
181	2.984307	116.90.239.10	192.168.0.7	TCP	66	ftp > 24463 [ACK] Seq=55 Ack=23 Win=14592 Len=0 TSval=613263206 TSecr=4788693
326	3.440148	192.168.0.7	8.8.8.8	DNS	81	Standard query A lc48.dsr.livefyre.com
327	3.440172	192.168.0.7	8.8.8.8	DNS	81	Standard query A lc48.dsr.livefyre.com

Frame 179: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)  
Ethernet II, Src: Dell\_ad:44:05 (14:fe:b5:ad:44:05), Dst: Netronix\_53:c5:6b (00:08:54:53:c5:6b)  
Internet Protocol Version 4, Src: 192.168.0.7 (192.168.0.7), Dst: 116.90.239.10 (116.90.239.10)  
Transmission Control Protocol, Src Port: 24463 (24463), Dst Port: ftp (21), Seq: 12, Ack: 55, Len: 11  
File Transfer Protocol (FTP)  
PASS abcd\r\n  
Request command: PASS  
Request arg: abcd

0000 00 08 54 53 c5 6b 14 fe b5 ad 44 05 08 00 45 00 ..TS.k.. ..D...E.  
0010 00 3f 98 b4 40 00 40 06 7d f0 c0 a8 00 07 74 5a .?..@.@. }.....tZ  
0020 ef 0a 5f 8f 00 15 b2 4a 89 6f 59 c8 05 fd 80 18 ..\_....J .oY.....  
0030 00 73 e4 af 00 00 01 01 08 0a 00 49 11 d5 24 8d .s..... ...I..\$.  
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 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
01b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
01c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
01d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
01e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
01f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
02a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
02b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
02c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
02d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
02e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
02f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0330 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0340 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0350 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0370 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
03a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
03b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
03c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
03d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
03e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
03f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0410 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0420 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0430 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0450 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0460 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0470 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0490 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
04a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
04b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
04c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
04d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
04e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
04f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0510 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0520 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0530 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0540 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0550 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0560 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0570 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0580 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0590 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
05a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
05b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
05c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
05d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
05e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
05f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0610 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0620 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0630 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0640 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0650 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0660 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0670 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0680 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0690 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
06a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
06b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
06c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
06d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
06e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
06f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0710 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0720 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0730 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0740 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0750 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0760 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0770 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0780 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0790 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
07a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
07b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
07c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
07d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
07e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
07f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0810 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0820 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0830 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0840 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0850 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0860 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0870 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0880 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0890 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
08a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
08b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
08c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
08d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
08e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
08f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0910 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0920 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0930 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0940 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0950 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0960 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0970 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0980 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0990 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
09a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
09b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
09c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
09d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
09e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
09f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0a00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0a10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0a20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0a30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0a40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0a50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0a60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0a70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0a80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0a90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0aa0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0ab0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0ac0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0ad0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0ae0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0af0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0b00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0b10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0b20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0b30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0b40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0b50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0b60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0b70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0b80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0b90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0ba0