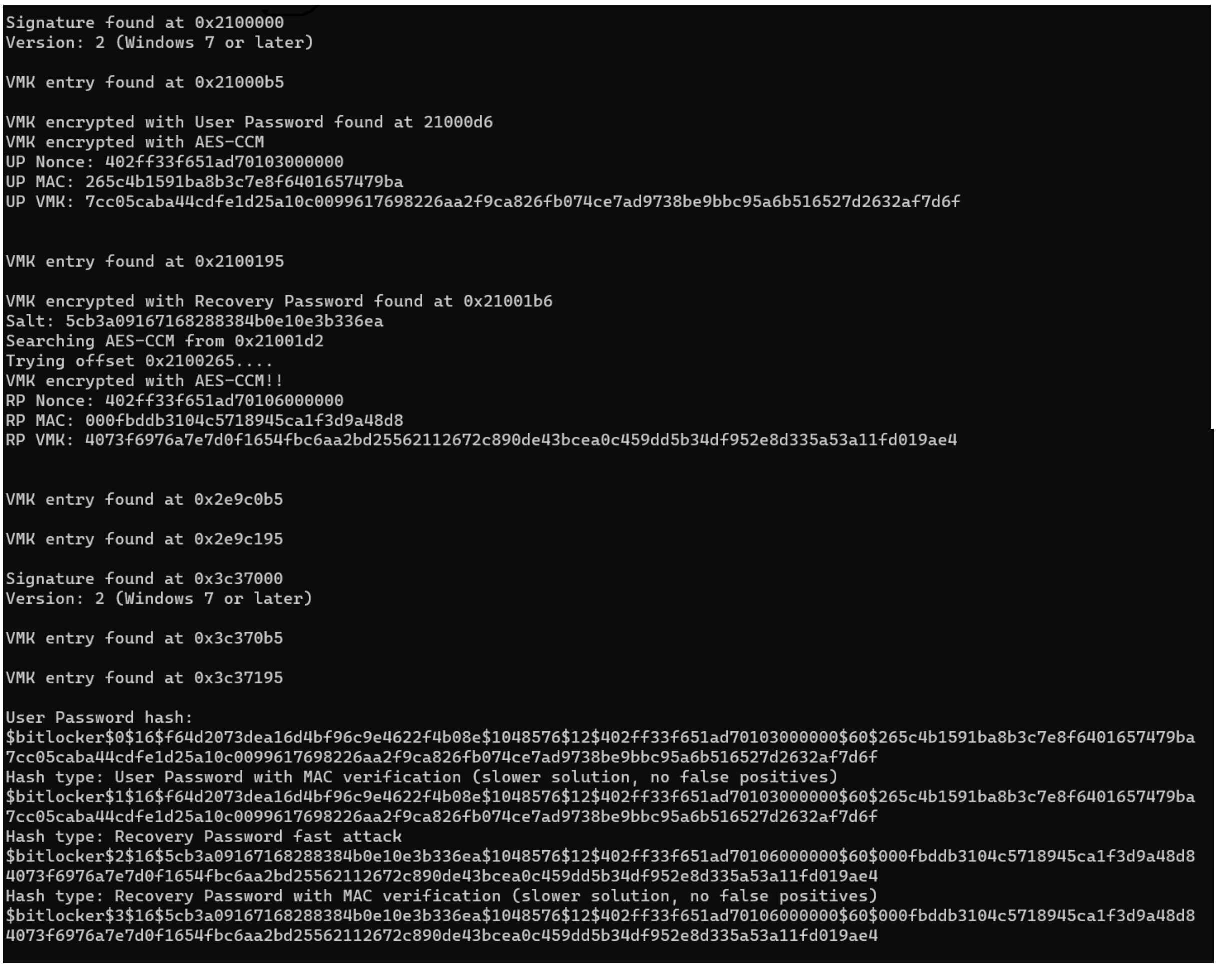
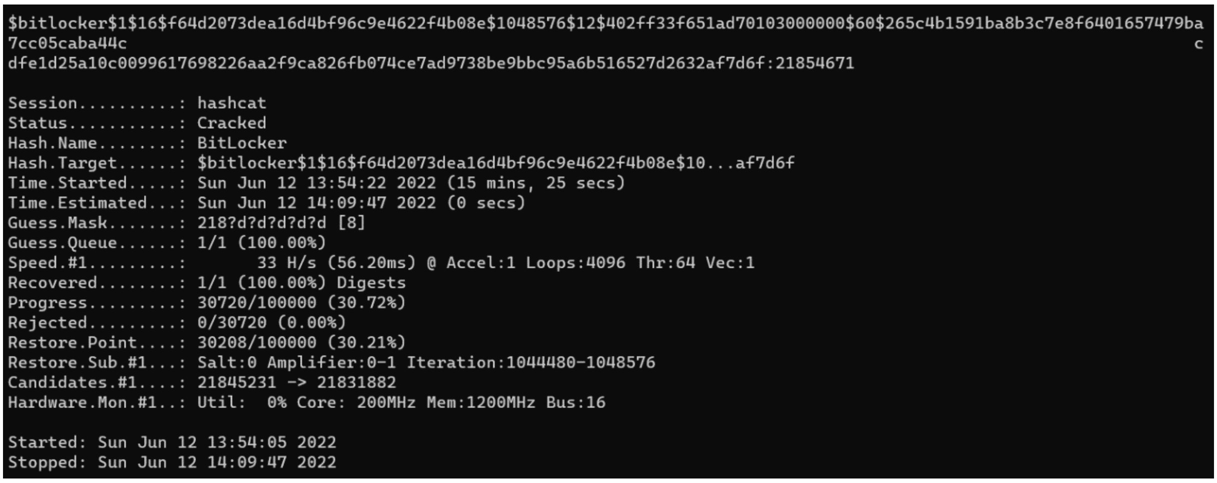
LABORATORIJSKA VJEŽBA 1

Jakov Melvan



```
Signature found at 0x2100000
Version: 2 (Windows 7 or later)

VMK entry found at 0x21000b5

VMK encrypted with User Password found at 21000d6
VMK encrypted with AES-CCM
UP Nonce: 402ff33f651ad70103000000
UP MAC: 265c4b1591ba8b3c7e8f6401657479ba
UP VMK: 7cc05caba44cdfe1d25a10c0099617698226aa2f9ca826fb074ce7ad9738be9bbc95a6b516527d2632af7d6f


VMK entry found at 0x2100195

VMK encrypted with Recovery Password found at 0x21001b6
Salt: 5cb3a09167168288384b0e10e3b336ea
Searching AES-CCM from 0x21001d2
Trying offset 0x2100265....
VMK encrypted with AES-CCM!!
RP Nonce: 402ff33f651ad70106000000
RP MAC: 000fbddb3104c5718945ca1f3d9a48d8
RP VMK: 4073f6976a7e7d0f1654fbc6aa2bd25562112672c890de43bcea0c459dd5b34df952e8d335a53a11fd019ae4


VMK entry found at 0x2e9c0b5

VMK entry found at 0x2e9c195

Signature found at 0x3c37000
Version: 2 (Windows 7 or later)

VMK entry found at 0x3c370b5

VMK entry found at 0x3c37195

User Password hash:
$bitlocker$0$16$f64d2073dea16d4bf96c9e4622f4b08e$1048576$12$402ff33f651ad70103000000$60$265c4b1591ba8b3c7e8f6401657479ba
7cc05caba44cdfe1d25a10c0099617698226aa2f9ca826fb074ce7ad9738be9bbc95a6b516527d2632af7d6f
Hash type: User Password with MAC verification (slower solution, no false positives)
$bitlocker$1$16$f64d2073dea16d4bf96c9e4622f4b08e$1048576$12$402ff33f651ad70103000000$60$265c4b1591ba8b3c7e8f6401657479ba
7cc05caba44cdfe1d25a10c0099617698226aa2f9ca826fb074ce7ad9738be9bbc95a6b516527d2632af7d6f
Hash type: Recovery Password fast attack
$bitlocker$2$16$5cb3a09167168288384b0e10e3b336ea$1048576$12$402ff33f651ad70106000000$60$000fbddb3104c5718945ca1f3d9a48d8
4073f6976a7e7d0f1654fbc6aa2bd25562112672c890de43bcea0c459dd5b34df952e8d335a53a11fd019ae4
Hash type: Recovery Password with MAC verification (slower solution, no false positives)
$bitlocker$3$16$5cb3a09167168288384b0e10e3b336ea$1048576$12$402ff33f651ad70106000000$60$000fbddb3104c5718945ca1f3d9a48d8
4073f6976a7e7d0f1654fbc6aa2bd25562112672c890de43bcea0c459dd5b34df952e8d335a53a11fd019ae4
```

Probijanje lozinke:



```
$bitlocker$1$16$f64d2073dea16d4bf96c9e4622f4b08e$1048576$12$402ff33f651ad70103000000$60$265c4b1591ba8b3c7e8f6401657479ba
7cc05caba44c                                                                                                           c
dfe1d25a10c0099617698226aa2f9ca826fb074ce7ad9738be9bbc95a6b516527d2632af7d6f:21854671

Session..........: hashcat
Status...........: Cracked
Hash.Name........: BitLocker
Hash.Target......: $bitlocker$1$16$f64d2073dea16d4bf96c9e4622f4b08e$10...af7d6f
Time.Started.....: Sun Jun 12 13:54:22 2022 (15 mins, 25 secs)
Time.Estimated...: Sun Jun 12 14:09:47 2022 (0 secs)
Guess.Mask.......: 218?d?d?d?d?d [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       33 H/s (56.20ms) @ Accel:1 Loops:4096 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 30720/100000 (30.72%)
Rejected.........: 0/30720 (0.00%)
Restore.Point....: 30208/100000 (30.21%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1044480-1048576
Candidates.#1....: 21845231 -> 21831882
Hardware.Mon.#1..: Util:  0% Core: 200MHz Mem:1200MHz Bus:16

Started: Sun Jun 12 13:54:05 2022
Stopped: Sun Jun 12 14:09:47 2022
```