GJØVIK UNIVERSITY COLLEGE

The persistence of memory: Forensic identification and extraction of cryptographic keys

Written by:

Carsten Maartmann-Moe

Steffen E. Thorkildsen

André Årnes

Presented by Group 7:

Abalenkovs Dmitrijs, Nordbø André, Ruthven Pieter Bloemerus, Pathapati Vijay Kumar Raju, Bondarenko Petro, Piatkivskyi Dmytro, Rekdal John Erik

What is the paper about

Discusses how to locate keys of encrypted environments in volatile memory structures

Analyzed ciphers:

- *AES*
- *Serpent*
- *Twofish*

Created their own tool for analysis: Interrogate

Known search strategies

- Brute-force with the memory image as dictionary (not used)
- Search for structural properties of the RSA encoding
- Search for high-entropy regions
- Search for the code structures (e.g, C structs) that contain the key
- Search for the key schedule

Identifying the key

- **AES (128bit) and Serpent :**
  - Generate key schedules for all 16 byte windows in memory
  - Check whether the next 112 byte matches the generated schedule (ECC)

- **Twofish:**
  - Searching for byte runs → look for entropy patterns
  - Try 5 different C Structs

Classes of cryptographic software

Whole-Disk Encryption

- Systems that keep keys in memory while a system is powered (full disk encryption)
- TrueCrypt, Bitlocker, FileVault, ProtectDrive, PGP

Virtual Disk Encryption

- Systems that keep keys in memory while mounted (file based encryption)
- TrueCrypt, PGP, FileVault, ProtectDrive, Best Vault

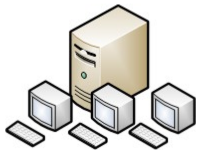
Session-Based Encryption

- Use short-lived keys
- Skype, WinZip, WinRAR and SimpLite-MSN

System states

- Live state (running crypto systems)
  - Screensaver State
  - Dismounted State (Virtual Disk)
  - Hibernation State
  - Logged out State
- Terminated State (terminated crypto systems)
- Reboot State
- Cold Boot State (powered off for a while)

Case setup



Virtual machines:

- Base: Windows XP SP2 on VMware
- One master snapshot of OS (controlled with hash)
- Copies of machines with different software and states
- Raw data extracted from the VM memory file

Physical machines:

- Windows XP SP3
- OSX
- Memory dump taken by cold-booting using PXE

Results

State	Whole disk	Virtual disk	Session based
Live	100%	83%	0%
Screensaver	100%	83%	0%
Dismounted	NA	11%	NA
Hibernation	NA	44%	0%
Terminated	NA	11%	0%
Logged out	100%	11%	0%
Reboot	29%	11%	0%
Boot	0%	0%	0%

Conclusions from paper

For adversary:

•Never leave a computing device powered on unless it is in use or physically protected (full disk) and unmount drives not in use

•Restrict boot options and enable BIOS-protection

•Disable busses like FireWire (DMA memory dumps)

For investigator:

•Securing memory dumps is paramount

•State of system is critical to success → live memory acquisition

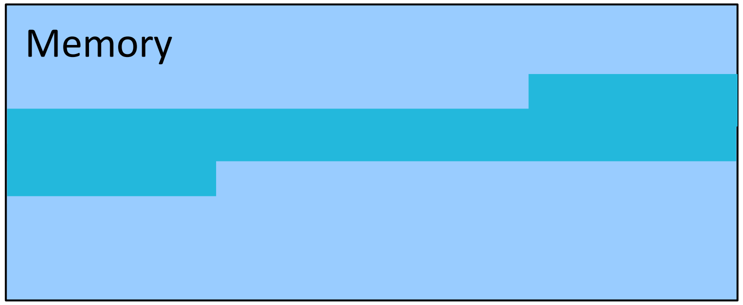
Interrogate - DEMO

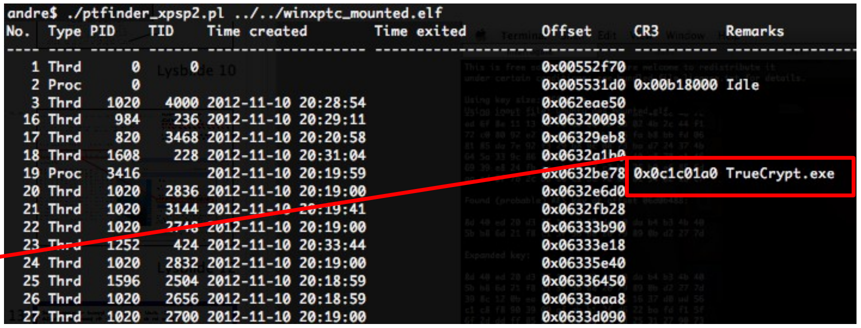
- Command line tool, file input can be anything like RAM dump, paging file or hibernation file.
- Encryption standards
  - AES (128,192,256)
  - RSA (independent of length) (DER encoded)
  - Win-RSA (Private key BLOB-encoded)
  - Serpent (256)
  - (tc) Twofish (256)
- Memory reconstruction

```
Usage: interrogate [OPTION]... [FILE]...
Search for cryptographic keys in the FILEs (memory dumps).

 -a algorithm   search for keys of a certain type (algorithm).
                  Valid parameters: aes, rsa, win-rsa, serpent,
                  [tc-]twofish. Use the -k switch to specify AES
                  key lengths (128, 198, or 256 bits). RSA keys are
                  found independent of their length, while SERPENT
                  and TWOFISH keys are required to be 256 bits.
                  The rsa parameter specifies DER-encoded rsa keys,
                  while win-rsa requires Private Key BLOB (Windows)
                  structure.
 -h               prints usage and help information (this message).
 -i interval    only search within interval. Format of interval is
                  from_offset:to_offset where the offset values
                  are interpreted as hexadecimal values. Omitting
                  one of the offsets will indicate the start or
                  the end of the FILEs, respectively. Used with
                  the -r switch, the interval will be interpreted
                  as the virtual address space that are to be
                  reconstructed.
 -k keylength   length of key to be searched for (NB: in BITS)
 -n               naive mode, calculates true entropy instead of
                  counting unique bytes (which is the normal
                  mode). This may be useful if you get bad quality
                  results, but may yield some performance
                  degradation.
 -p filename    print entropy values for each window separated
                  by newlines to file specified by filename. This
                  may be used as input to plotting tools (gnuplot)
                  WARNING: Slow and generates large files, one
                  input byte maps to potentially six output bytes.
 -q             quick mode, does not use overlapping windows. The
                  larger the window size, the quicker. Use -w to
                  specify window size.
 -r CR3         reconstructs the virtual address space for the
                  process at offset PDB. The PDB is the location of
                  the page directory base, and can be found by
                  scanning for EPROCESSes using PTfinder,
                  Volatility or other similar tools. The
                  regonstructed memory is written to file
                  'pages', and are searched subsequently for
                  keys. The -i option may be used to specify a
                  virtual address space interval.
 -t threshold   sets the entropy threshold (default = 7.0).
 -w windowsize  sets the window size. Not compatible with the -a
                  option.
```

http://sourceforge.net/projects/interrogate/

Extract **source** and run "**make**"
(requires C-compiler: aptitude install build-essential)





```
andre$ ./ptfinder_xpsp2.pl ../../winxptc_mounted.elf
No.  Type PID    TID    Time created        Time exited         Offset     CR3        Remarks
---- ---- ------ ------ ------------------- ------------------- ---------- ---------- ----------------
   1 Thrd      0      0                                         0x00552f70
   2 Proc      0                                                0x005531d0 0x00b18000 Idle
   3 Thrd   1020   4000 2012-11-10 20:28:54                     0x062eae50
  16 Thrd    984    236 2012-11-10 20:29:11                     0x06320098
  17 Thrd    820   3468 2012-11-10 20:20:58                     0x06329eb8
  18 Thrd   1608    228 2012-11-10 20:31:04                     0x0632a1b0
  19 Proc   3416        2012-11-10 20:19:59                     0x0632be78 0x0c1c01a0 TrueCrypt.exe
  20 Thrd   1020   2836 2012-11-10 20:19:00                     0x0632e6d0
  21 Thrd   1020   3144 2012-11-10 20:19:41                     0x0632fb28
  22 Thrd   1020   2748 2012-11-10 20:19:00                     0x06333b90
  23 Thrd   1252    424 2012-11-10 20:33:44                     0x06333e18
  24 Thrd   1020   2832 2012-11-10 20:19:00                     0x06335e40
  25 Thrd   1596   2504 2012-11-10 20:18:59                     0x06336450
  26 Thrd   1020   2656 2012-11-10 20:18:59                     0x0633aaa8
  27 Thrd   1020   2700 2012-11-10 20:19:00                     0x0633d090
```

Twofish

Testbed

- Oracle VirtualBox (version 4.1.12)
- Windows XP SP3
  - Updated to current state
  - Google Chrome
  - MS Security Essentials
- TrueCrypt (version 7.1a)
  - Encrypted container with pass phrase “test”

Memory extraction

- While VM is live, running from console:

*vboxmanage debugvm <**vmname**> dumpguestcore –filename <**filename**>*

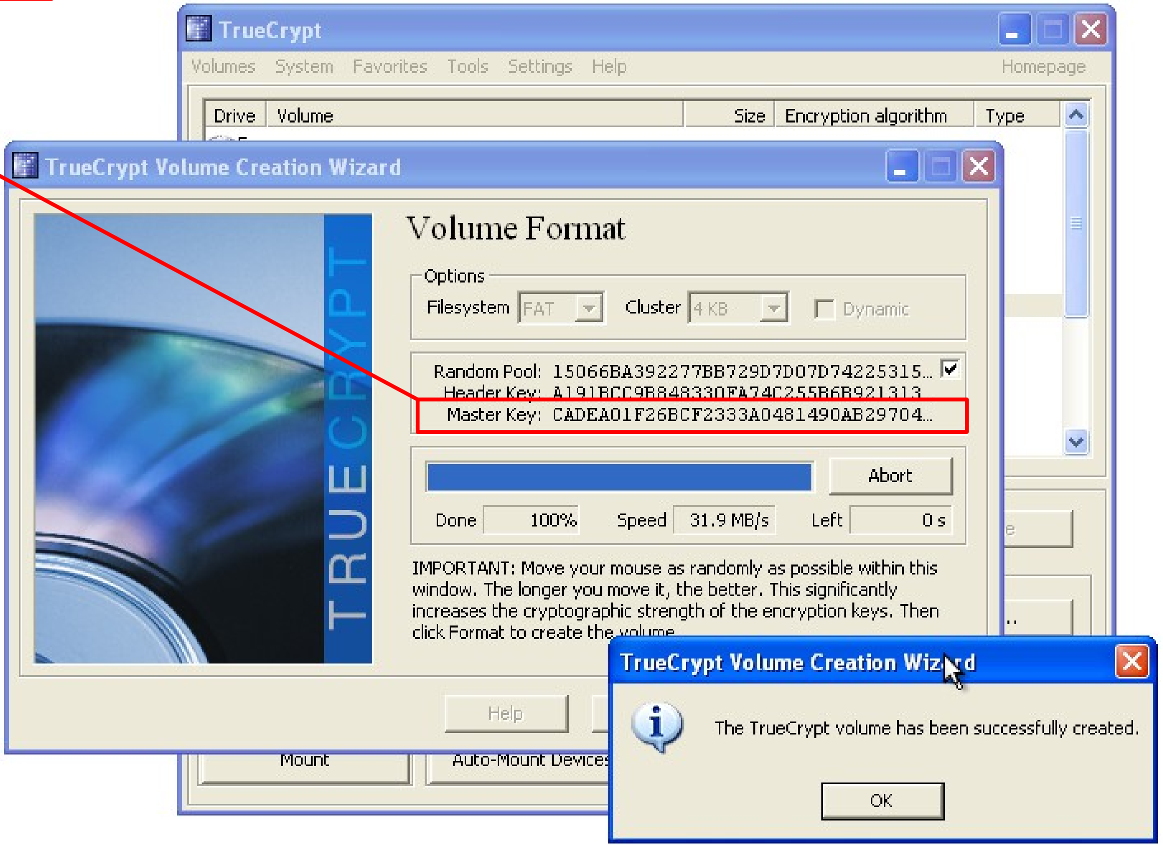
(ELF format with some additional meta data)

```
$ ./interrogate -a aes -k 256 ~/Desktop/winxptc_mounted.elf
Interrogate  Copyright (C) 2008  Carsten Maartmann-Moe <carmaa@gmail.com>
This program comes with ABSOLUTELY NO WARRANTY; for details use `-h'.
This is free software, and you are welcome to redistribute it
under certain conditions; see bundled file licence.txt for details.

Using key size: 256 bits.
Using input file: /home/andynor/Desktop/winxptc_mounted.elf.
Attempting to load entire file into memory, please stand by...
Success, starting search.

---------------------------------------------------------------------------
Found (probable) AES key at offset 062ee6b8:

ca de a0 1f 26 bc f2 33 3a 04 81 49 0a b2 97 04
e6 d5 71 f5 b7 8b 30 59 1d 02 f4 c8 4a 6e 7f f7

Expanded key:

ca de a0 1f 26 bc f2 33 3a 04 81 49 0a b2 97
e6 d5 71 f5 b7 8b 30 59 1d 02 f4 c8 4a 6e 7f
54 0c c8 c9 72 b0 3a fa 48 b4 bb b3 42 06 2c
ca ba 00 5c 7d 31 30 05 60 33 c4 cd 2a 5d bb
1a e6 48 2c 68 56 72 d6 20 e2 c9 65 62 e4 e5
60 d3 d9 e9 1d e2 e9 ec 7d d1 2d 21 57 8c 96
7a 76 e7 77 12 20 95 a1 32 c2 5c c4 50 26 b9
33 24 8f ae 2e c6 66 42 53 17 4b 63 04 9b dd
66 b7 5b 85 74 97 ce 24 46 55 92 e0 16 73 2b
74 ab 7e ec 5a 6d 18 ae 09 7a 53 cd 0d e1 8e
8e ae 8e 52 fa 39 40 76 bc 6c d2 96 aa 1f f9
d8 6b e7 3c 82 06 ff 92 8b 7c ac 5f 86 9d 22
f0 3d 09 16 0a 04 49 60 b6 68 9b f6 1c 77 62
44 9e 4d ac c6 98 b2 3e 4d e4 1e 61 cb 79 3c
06 d6 34 09 0c d2 7d 69 ba ba e6 9f a6 cd 84
```

Runtime: 70-71 min
(Got two more keys:

00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f

a4 17 88 14 5c 06 fb 3f 7d 77 02 55 b5 1f a6 cc
e7 f9 df ff 33 aa cc ac 87 df 90 57 04 44 bc 83


TrueCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption algorithm Type
TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Format
Options
Filesystem FAT
Cluster 4 KB
Dynamic
Abort
Help
Mount
Auto-Mount Devices
OK

Random Pool: 15066BA392277BB729D7D07D74225315...
Header Key: A191BCC9B848330FA74C255B6B921313
Master Key: CADEA01F26BCF2333A0481490AB29704...

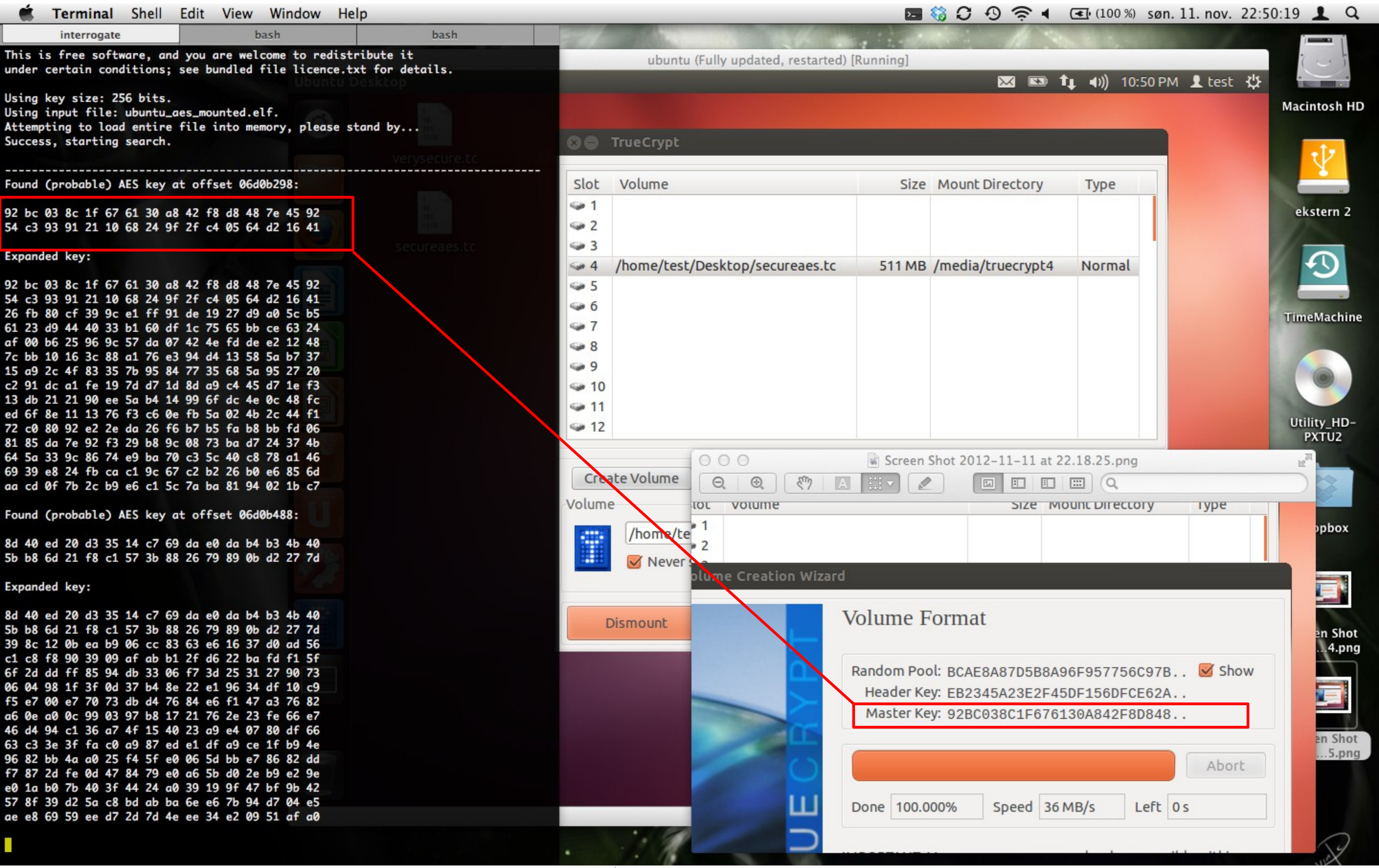
Done 100% Speed 31.9 MB/s Left 0 s

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

TrueCrypt Volume Creation Wizard

The TrueCrypt volume has been successfully created.

- Same procedure on TrueCrypt 7.1a running on Ubuntu 12.04
- AxCrypt (session based) with 128bit AES keys did not succeed



```
This is free software, and you are welcome to redistribute it
under certain conditions; see bundled file licence.txt for details.

Using key size: 256 bits.
Using input file: ubuntu_aes_mounted.elf.
Attempting to load entire file into memory, please stand by...
Success, starting search.

------------------------------------------------------------------------------
Found (probable) AES key at offset 06d0b298:

92 bc 03 8c 1f 67 61 30 a8 42 f8 d8 48 7e 45 92
54 c3 93 91 21 10 68 24 9f 2f c4 05 64 d2 16 41

Expanded key:

92 bc 03 8c 1f 67 61 30 a8 42 f8 d8 48 7e 45 92
54 c3 93 91 21 10 68 24 9f 2f c4 05 64 d2 16 41
26 fb 80 cf 39 9c e1 ff 91 de 19 27 d9 a0 5c b5
61 23 d9 44 40 33 b1 60 df 1c 75 65 bb ce 63 24
af 00 b6 25 96 9c 57 da 07 42 4e fd de e2 12 48
7c bb 10 16 3c 88 a1 76 e3 94 d4 13 58 5a b7 37
15 a9 2c 4f 83 35 7b 95 84 77 35 68 5a 95 27 20
c2 91 dc a1 fe 19 7d d7 1d 8d a9 c4 45 d7 1e f3
13 db 21 21 90 ee 5a b4 14 99 6f dc 4e 0c 48 fc
ed 6f 8e 11 13 76 f3 c6 0e fb 5a 02 4b 2c 44 f1
72 c0 80 92 e2 2e da 26 f6 b7 b5 fa b8 bb fd 06
81 85 da 7e 92 f3 29 b8 9c 08 73 ba d7 24 37 4b
64 5a 33 9c 86 74 e9 ba 70 c3 5c 40 c8 78 a1 46
69 39 e8 24 fb ca c1 9c 67 c2 b2 26 b0 e6 85 6d
aa cd 0f 7b 2c b9 e6 c1 5c 7a ba 81 94 02 1b c7

Found (probable) AES key at offset 06d0b488:

8d 40 ed 20 d3 35 14 c7 69 da e0 da b4 b3 4b 40
5b b8 6d 21 f8 c1 57 3b 88 26 79 89 0b d2 27 7d

Expanded key:

8d 40 ed 20 d3 35 14 c7 69 da e0 da b4 b3 4b 40
5b b8 6d 21 f8 c1 57 3b 88 26 79 89 0b d2 27 7d
39 8c 12 0b ea b9 06 cc 83 63 e6 16 37 d0 ad 56
c1 c8 f8 90 39 09 af ab b1 2f d6 22 ba fd f1 5f
6f 2d dd ff 85 94 db 33 06 f7 3d 25 31 27 90 73
06 04 98 1f 3f 0d 37 b4 8e 22 e1 96 34 df 10 c9
f5 e7 00 e7 70 73 db d4 76 84 e6 f1 47 a3 76 82
a6 0e a0 0c 99 03 97 b8 17 21 76 2e 23 fe 66 e7
46 d4 94 c1 36 a7 4f 15 40 23 a9 e4 07 80 df 66
63 c3 3e 3f fa c0 a9 87 ed e1 df a9 ce 1f b9 4e
96 82 bb 4a a0 25 f4 5f e0 06 5d bb e7 86 82 dd
f7 87 2d fe 0d 47 84 79 e0 a6 5b d0 2e b9 e2 9e
e0 1a b0 7b 40 3f 44 24 a0 39 19 9f 47 bf 9b 42
57 8f 39 d2 5a c8 bd ab ba 6e e6 7b 94 d7 04 e5
ae e8 69 59 ee d7 2d 7d 4e ee 34 e2 09 51 af a0
```

TrueCrypt

Slot	Volume	Size	Mount Directory	Type
1				
2				
3				
4	/home/test/Desktop/secureaes.tc	511 MB	/media/truecrypt4	Normal
5				
6				
7				
8				
9				
10				
11				
12				

Volume Creation Wizard

Volume Format

Random Pool: BCAE8A87D5B8A96F957756C97B.. ✓ Show
Header Key: EB2345A23E2F45DF156DFCE62A..
Master Key: 92BC038C1F676130A842F8D848..

Done 100.000% Speed 36 MB/s Left 0 s