Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas

Death By Suicide?

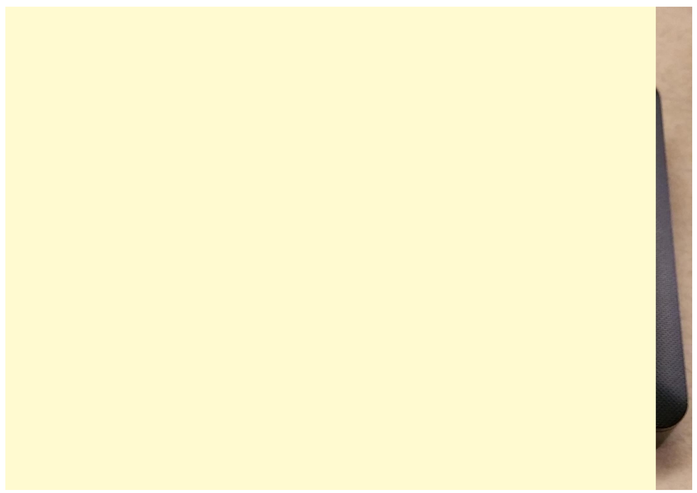
	Expectations
Research	• Looking for a road map on how to proceed. • Look for vulnerabilities(examine encryption process)
DS - View	• Attempt to communicate with Flash Controller Chip
Static Analysis	• Hypothesis: does it use a static key?

Acquisition

Analysis

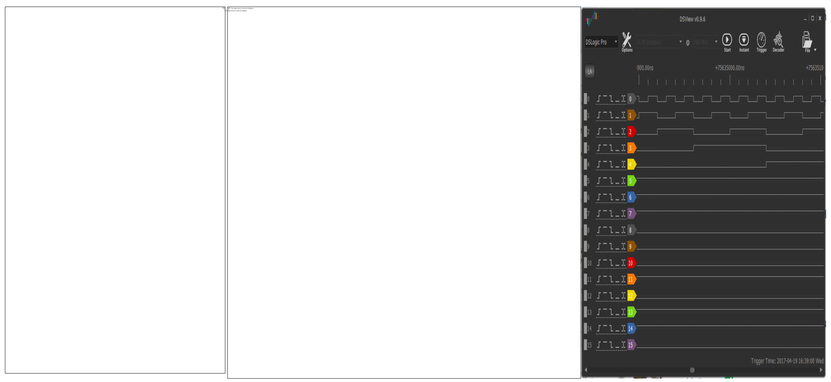
Extraction

More Analysis



Tools

Tools provided(left to right CW): Connection pins, FTDI Friend , write-blocker, Logic Analyzer, Digital Microscope, USB HD Docking Station “Toaster” and DS-View software



Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas
Death By Suicide?

Introduction

- Case Statement
- Using Logic Analyzer with SED
- Potential Attacks against SED
- Searching for commonality

Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas

Death By Suicide?

Case Statement

- Mysterious Death

- Laptop left at the scene, self-encrypting hard drive found disposed of in garbage

- What can we find out?

Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas
Death By Suicide?

Extraction

Logic Analyzer

- Device that captures and displays digital signals from a digital circuit
- Dslogic Pro
  - Connected probes to different pins on flash chip
  - Ground Clock, Input/output
  - No results

Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

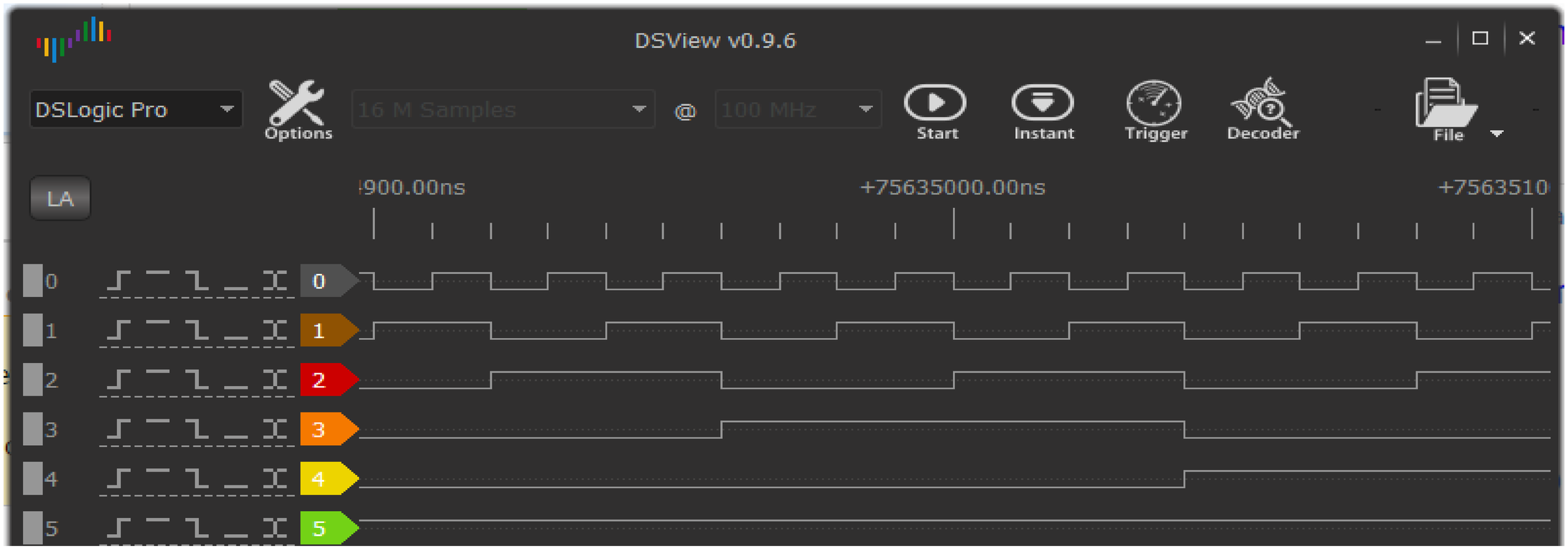
Alex Andrews, Deshun Coomer and Michael Thomas

Death By Suicide?

Logic Analyzer

Extraction

- This is similar to what it should have looked like



Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas
Death By Suicide?

Analysis

Potential Attacks

- Side Channel Attack
- Brute Force Attack (ex: dust for fingerprints)
- Hot Plug Attack
- Forced Restart
- Desoldering Electrically Erasable Programmable Read-Only Memory (EEPROM)

Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas
Death By Suicide?

Analysis

Looking for commonality

Theory: There is a static key used for access on the control chip

BsidesIndy Hacker Convention
bsidesindy.com
Reid Wightman
(twitter: @ReverseICS)

Target: SYBA S.E.D.

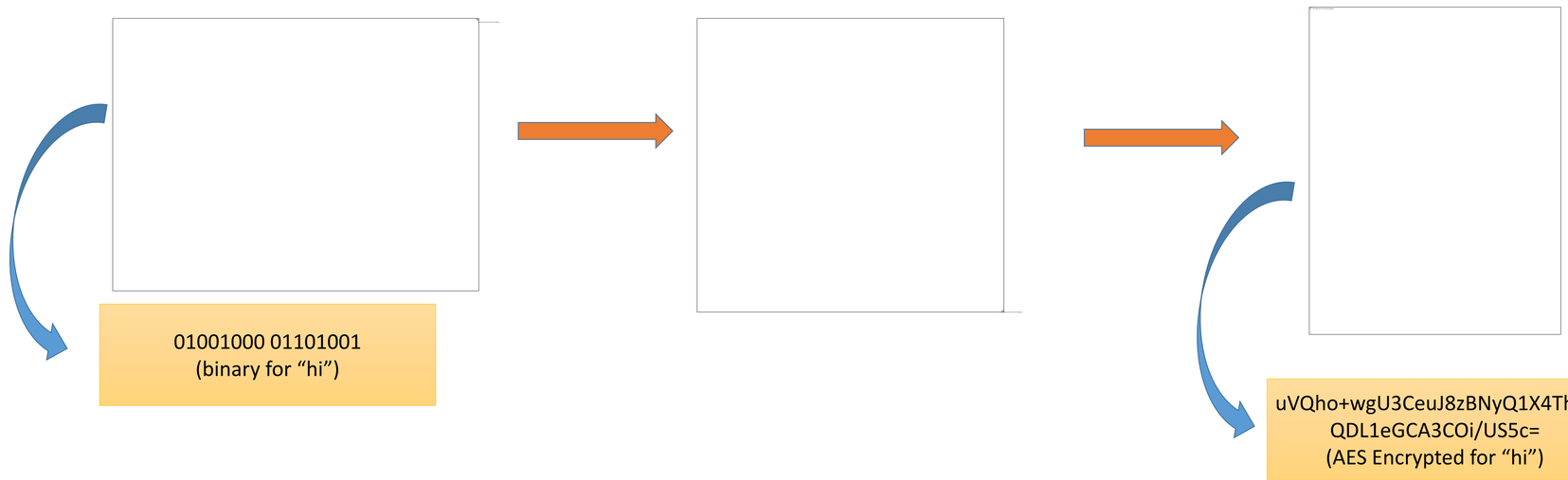
Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas

Death By Suicide?

Looking for commonality

Analysis



Target: SYBA S.E.D.

Sources:
http://aesencryption.net/
and **http://www.unit-conversion.info/texttools/convert-text-to-binary/**

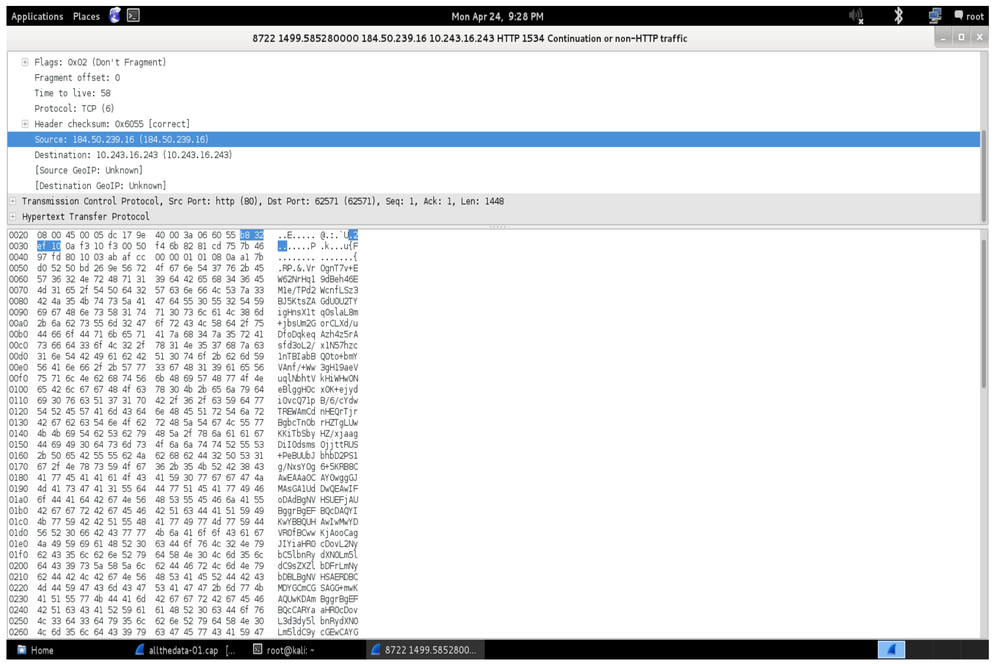
Examination of Syba Self-Encrypting Hard Drive

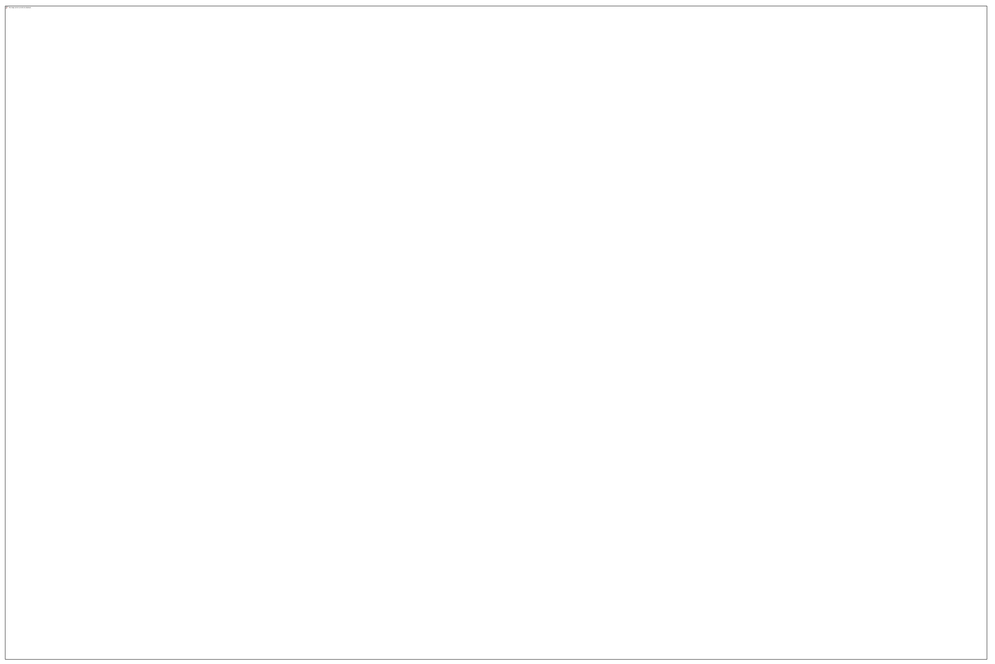
Alex Andrews, Deshun Coomer and Michael Thomas

Death By Suicide?

Looking for commonality

Analysis





➡ Set of command prints multiple “A”s to the device “sdc”

➡ llsbik command to <u>list</u> what devices are available

➡ Head is a command that lists off the top 10 lines in a file.

Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas

Death By Suicide?

Looking for commonality

Analysis

```
root@research-Latitude-E6220: /home/research
File  Edit  Tabs  Help
==> PASSWORD_1 <==
0000000: 335c 4163 c7a9 00c3 151c e2ce 2480 b737  3\Ac........$..7
0000010: 64be e187 c24c bec1 55a5 92cd 9865 7b64  d....L..U....e{d
0000020: 7194 ed99 29bf 0c4e 18e8 6b0a 0fc1 41b2  q...)..N..k...A.
0000030: 6d49 ed4a 9994 ca36 d27c 27af edb9 a839  mI.J...6.|'....9
0000040: 8ffc d07c e6a9 4067 147e 4a2f 873e c0df  ...|..@g.~J/.>..
0000050: eb1c 45ee 1e48 8fc2 1c28 5587 7f27 477d  ..E..H...(U..'G}
0000060: de93 ed3d 9a9e 46ba 497a ffb1 5a2d 1faa  ...=..F.Iz..Z-..
0000070: 8453 12cd 69aa 6093 a567 893b 30fa 4977  .S..i.`..g.;0.Iw
0000080: a292 1695 e7ec ae9e 81bc ad66 b4e3 0455  ...........f...U
0000090: f85e f794 15ed 177f ddc9 a262 8079 bela  .^.........b.y..

==> PASSWORD_1_AGAIN <==
0000000: 27f0 9257 4962 8755 8e21 d495 eedf 3bc0  '..WIb.U.!....;.
0000010: 7395 a508 c1a7 b5f5 4887 c384 8cfd ec26  s.......H......&
0000020: 0a6c 1330 1cc4 3791 8838 6be9 3b17 4b68  .l.0..7..8k.;.Kh
0000030: 01af 4f98 a3f7 d1d7 8d50 c98c 4c0a 2e7f  ..O......P..L...
0000040: ab19 6f37 061b 137c d2cf cb5f f2a5 ffcc  ..o7...|..._....
0000050: 7db3 e4b2 5eff 611e f857 beaf f3af 46da  }...^.a..W....F.
0000060: c4bf a3fc 7ad3 df9a ab71 6c12 d862 4f7b  ....z....ql..bO{
0000070: 2890 9951 43c0 a094 c25a 044f 81e6 6800  (..QC....Z.O..h.
0000080: 70dd 62d9 e4a6 1a56 8a06 4dcb ca2e 5088  p.b....V..M...P.
0000090: 664d ac9c 85d6 637f 5939 74ba 81a6 eb4a  fM....c.Y9t....J

==> PASSWORD_2 <==
0000000: 9baa dd21 23d0 5215 abd7 bac4 39b5 5b2d  ...!#.R.....9.[-
0000010: 53e8 cb45 52da 3b97 9f29 7370 e75b 48e9  S..ER.;..)sp.[H.
0000020: 09ab b154 6d9e 78f2 bceb 4290 0bfe e7f0  ...Tm.x...B.....
0000030: f9d1 b944 c0e5 7fed c5b9 859d 7761 6a10  ...D........waj.
0000040: e808 913c c1f5 f0f8 e145 2351 461d 057f  ...<.....E#QF...
0000050: e513 20ae 9763 674e 7d8a 6ff2 ccd2 a02d  .. ..cgN}.o.....-
0000060: 4779 5e7c 9dac a17e 5a8d d562 c426 7da3  Gy^|...~Z..b.&}.
0000070: 59db e462 d9de de63 6e98 d124 869f c3f5  Y..b...cn..$....
0000080: c9f0 f8d4 28d2 75fc 6b99 dc17 9f3d f3ed  ....(.u.k....=..
0000090: 763e 811f 1061 df34 541a 4751 b756 9b85  v>...a.4T.GQ.V..
root@research-Latitude-E6220:/home/research#
```

Diff is a command to compare differences between files.

“1,193c1,166” means line file 2 1 -193 have changed versus file 1 line 1 - 166

Target: SYBA S.E.D.

Is there a difference between password 1, password 2 and going back to password 1 again?

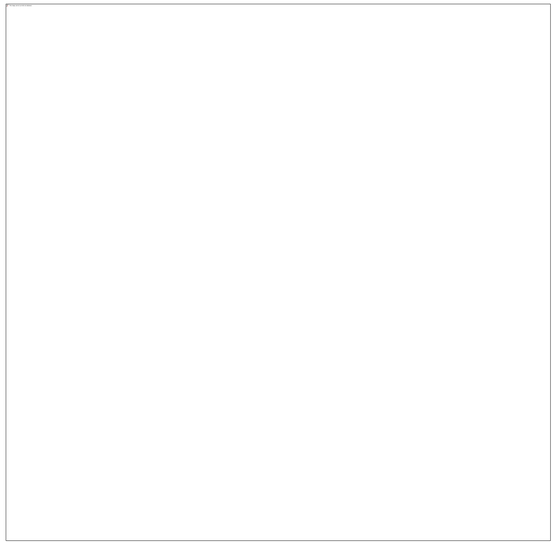
Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas

Death By Suicide?

Looking for commonality

More Analysis



At this time, there is no found commonality for this SED.

"*A great challenge of life – Knowing enough to think you're doing it right, but not enough to know you're doing it wrong*." - **Neil Degrasse Tyson**

Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas
Death By Suicide?

Summary

- The SED was unable to be accessed with tools used
- Checking for commonality ended up inconclusive
- Group 5 recommends further analysis on this case be continued by higher level examiners

Target: SYBA S.E.D.