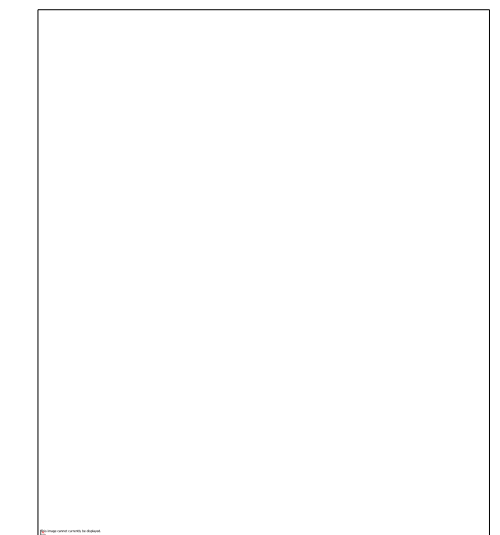
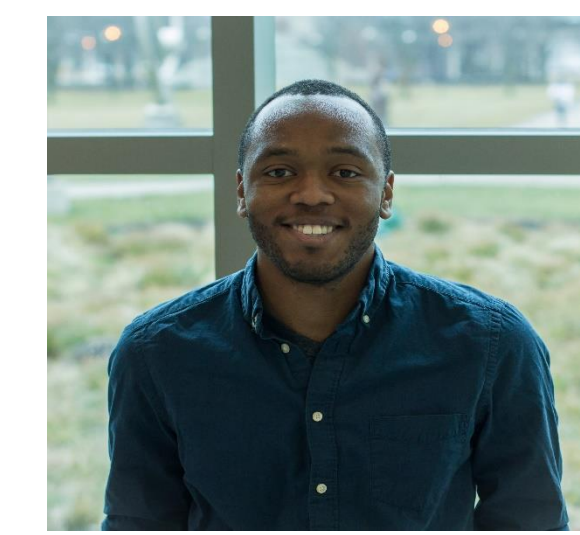
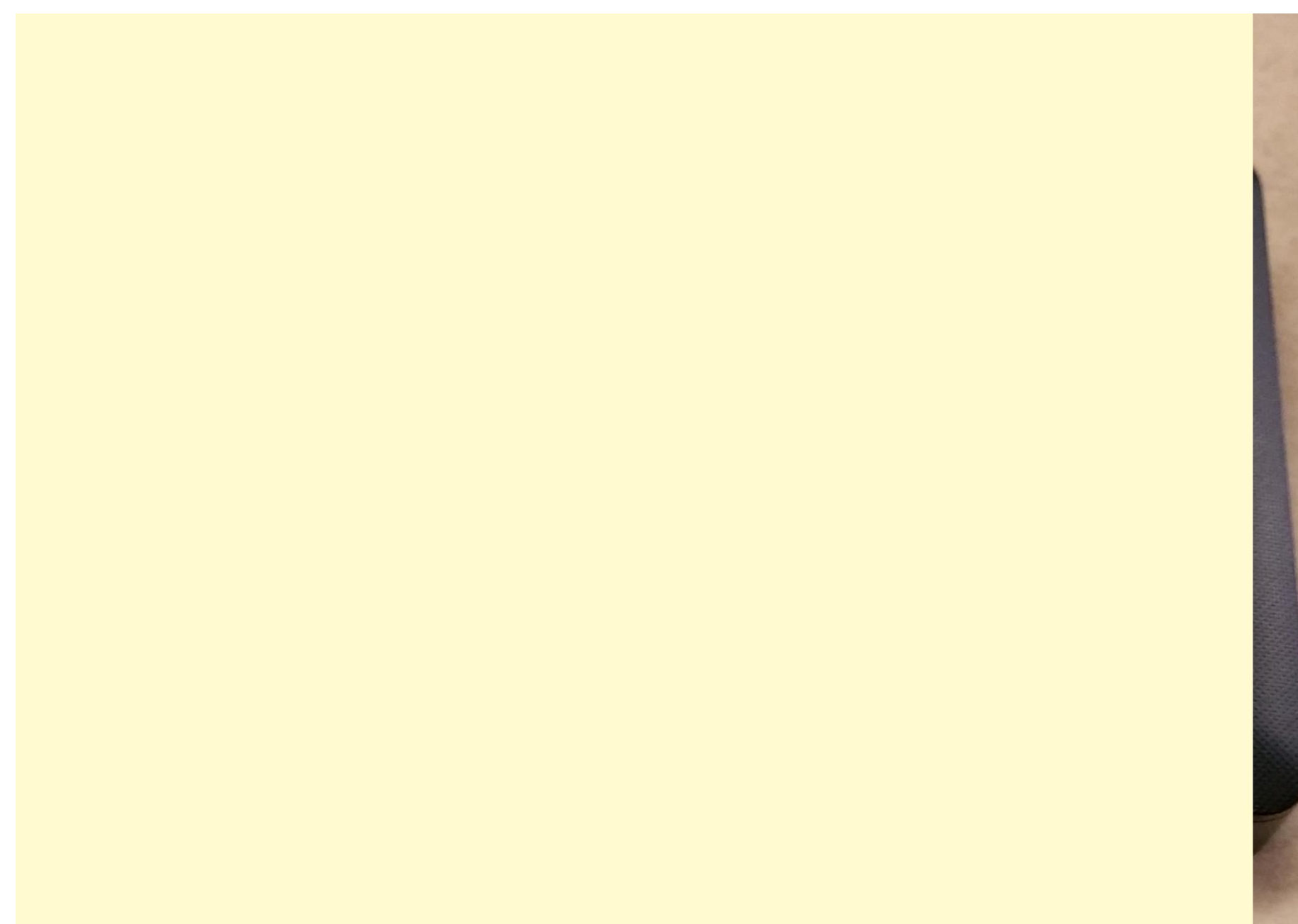
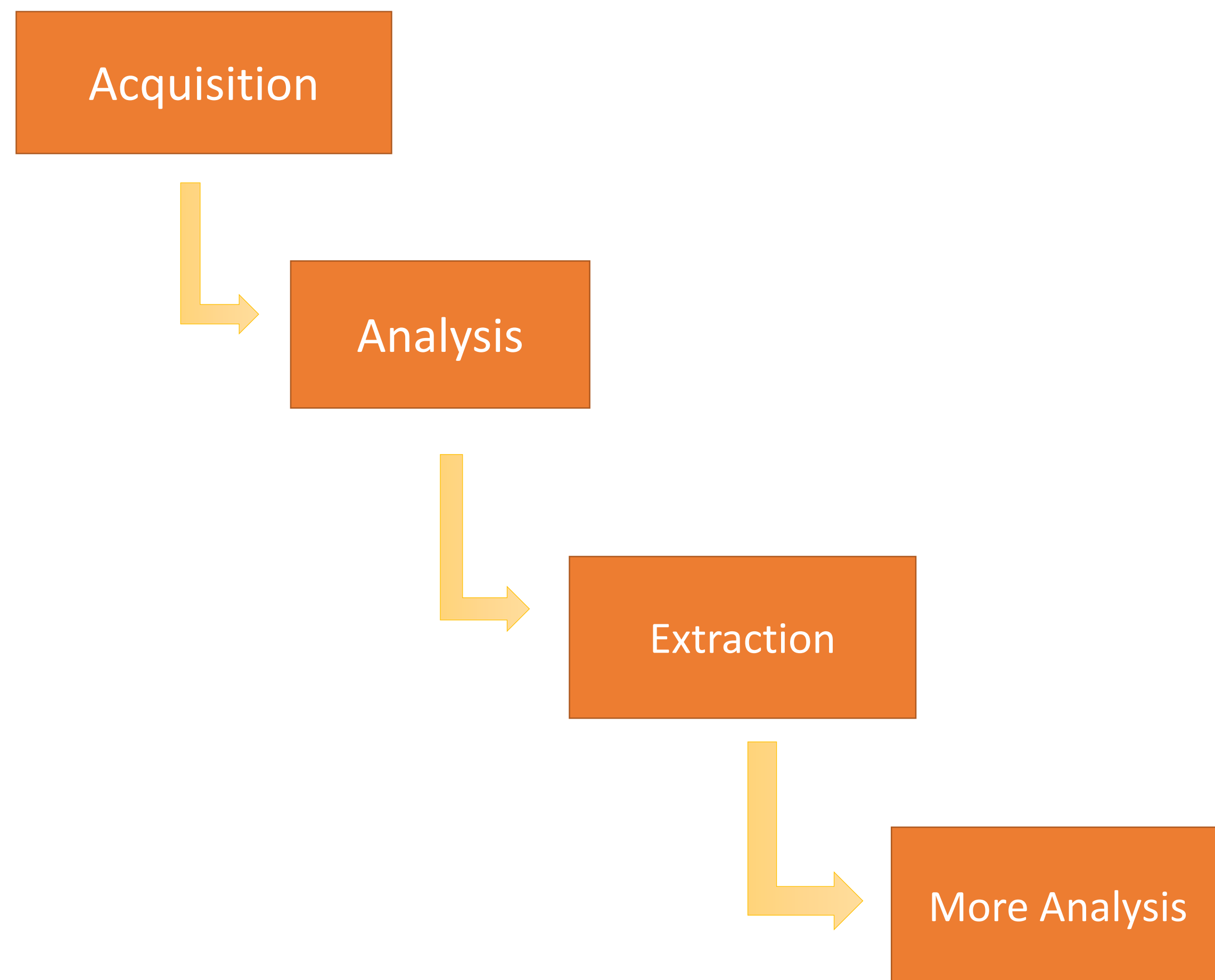


Examination of Syba Self-Encrypting Hard Drive

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



	Expectations
Research	<ul style="list-style-type: none"> Looking for a road map on how to proceed. Look for vulnerabilities(examine encryption process)
DS - View	<ul style="list-style-type: none"> Attempt to communicate with Flash Controller Chip
Static Analysis	<ul style="list-style-type: none"> Hypothesis: does it use a static key?



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

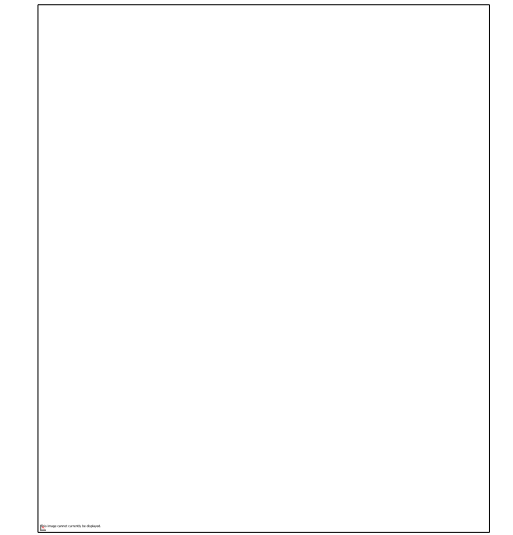
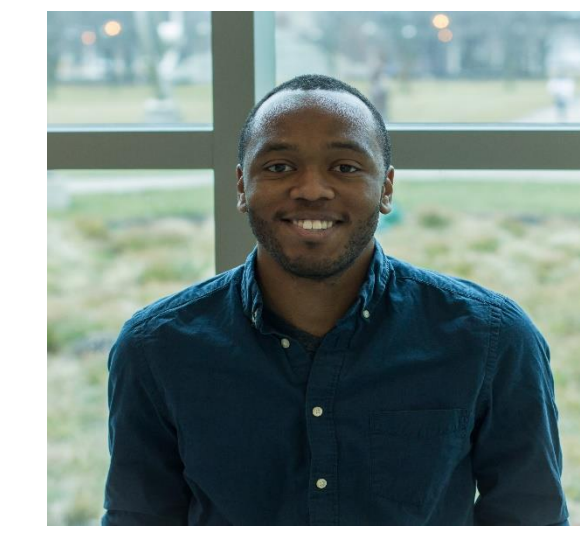


Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas

Death By Suicide?



Introduction

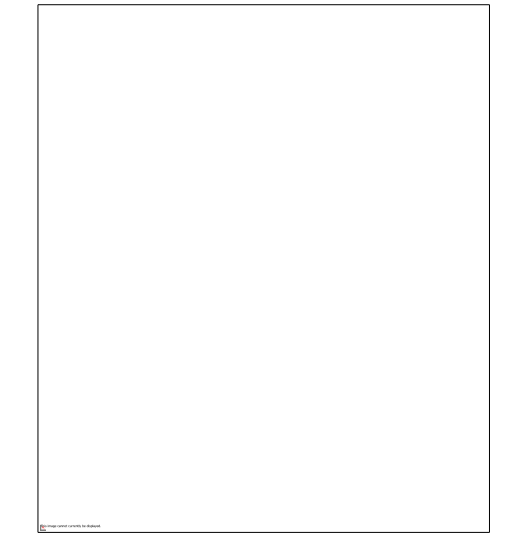
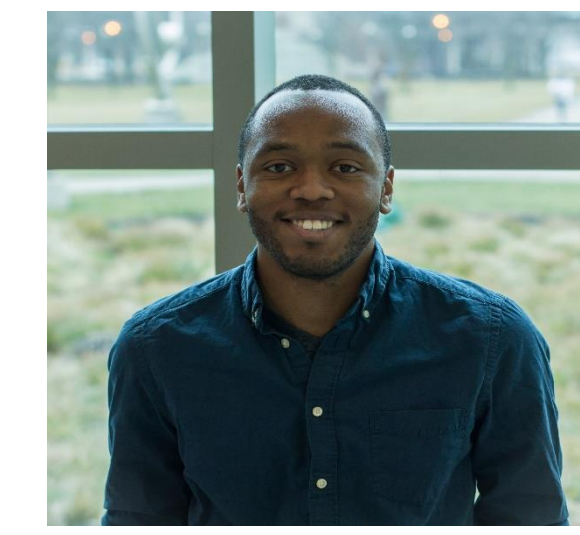
- Case Statement
- Using Logic Analyzer with SED
- Potential Attacks against SED
- Searching for commonality

Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas

Death By Suicide?



Case Statement

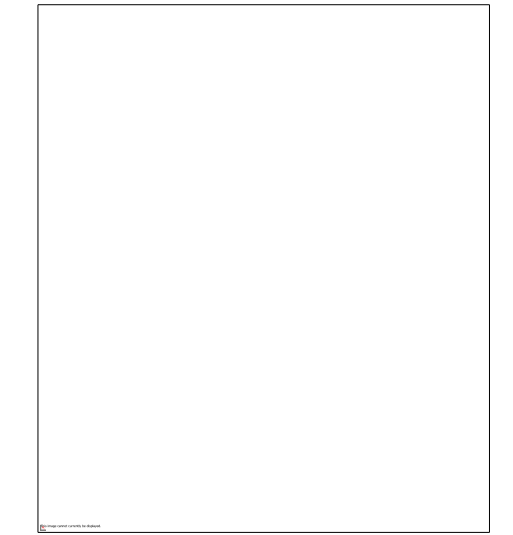
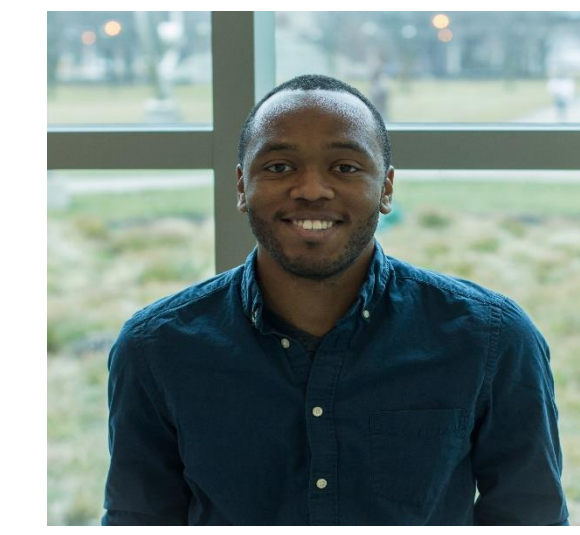
- Mysterious Death
- Laptop left at the scene, self-encrypting hard drive found disposed of in garbage
- What can we find out?

Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas

Death By Suicide?

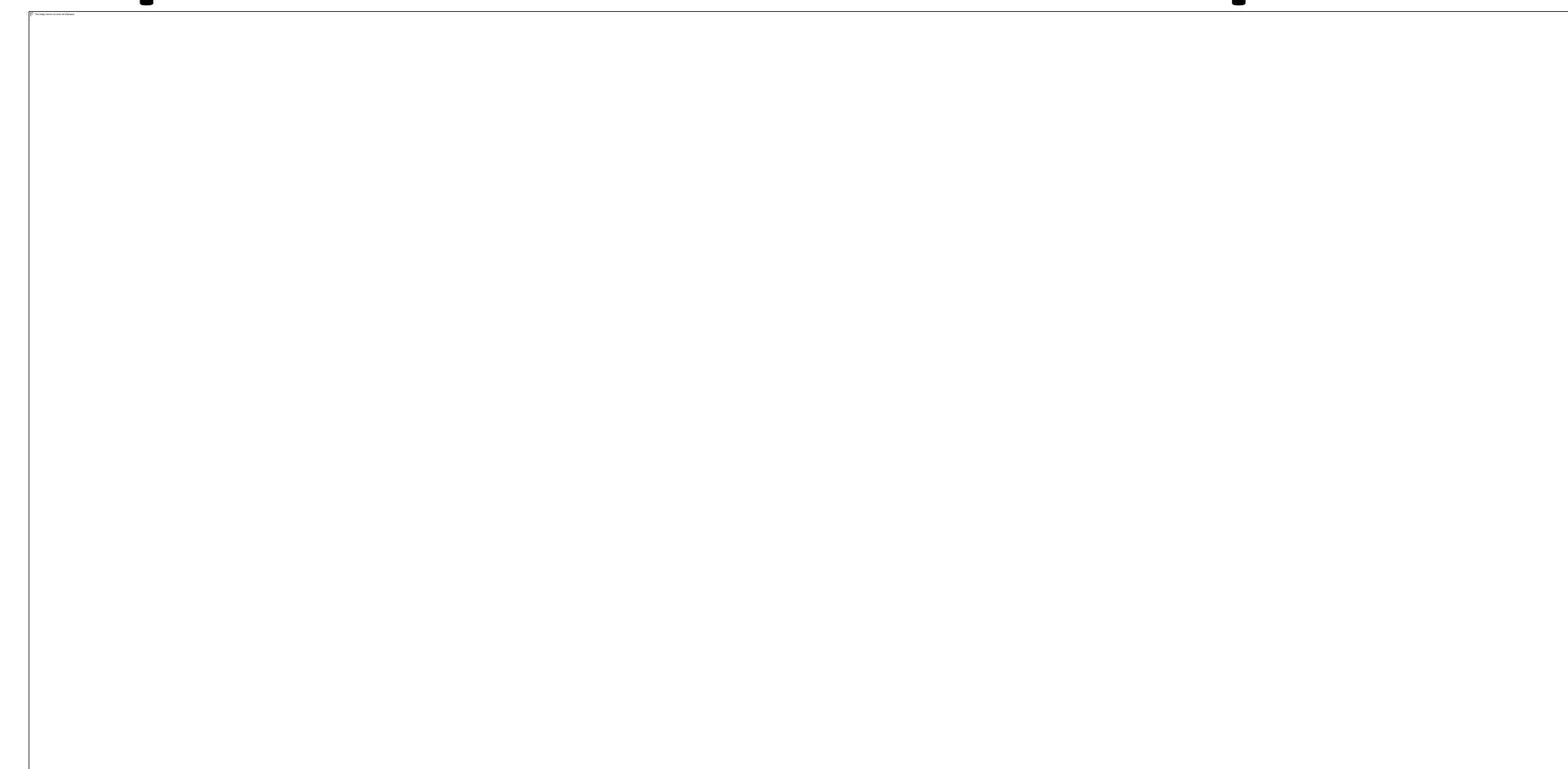


Logic Analyzer

Extraction

- 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

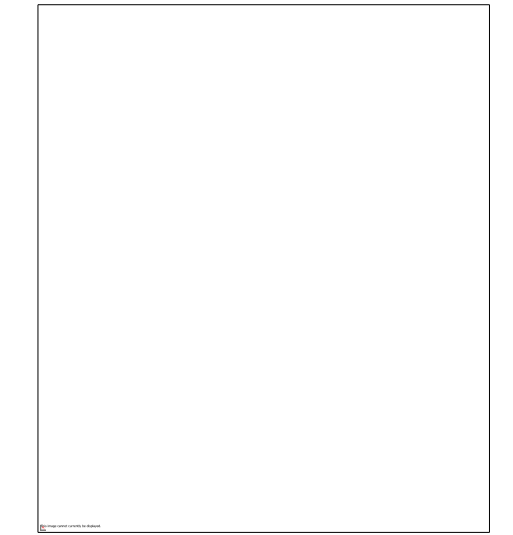
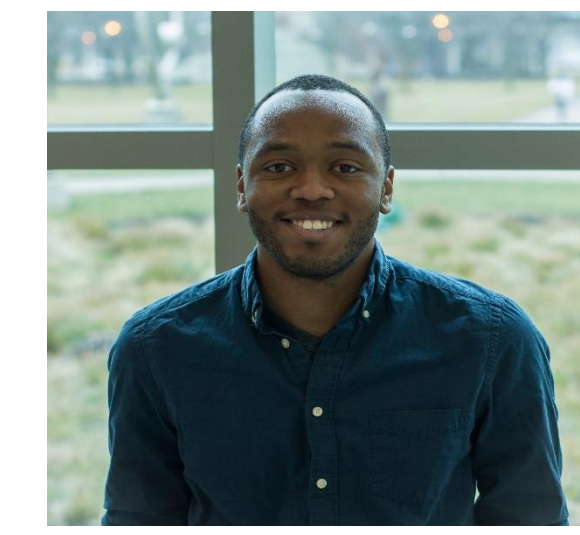
Target: SYBA S.E.D.



Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas

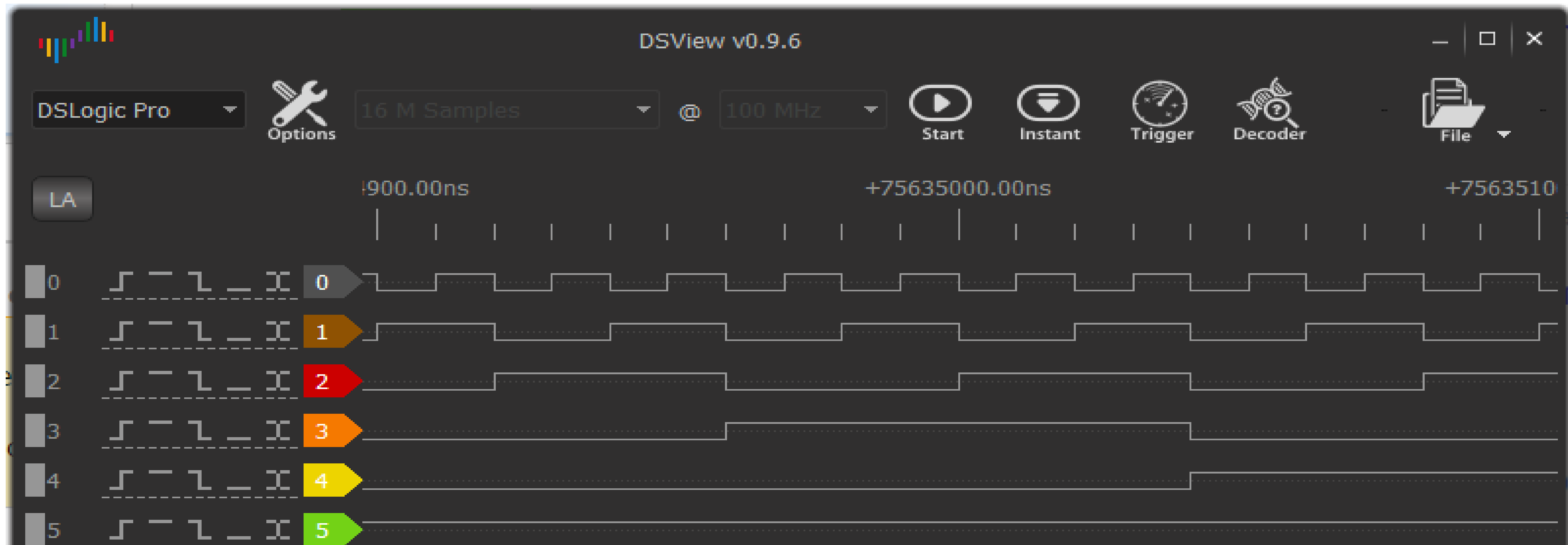
Death By Suicide?



Logic Analyzer

Extraction

- This is similar to what it should have looked like

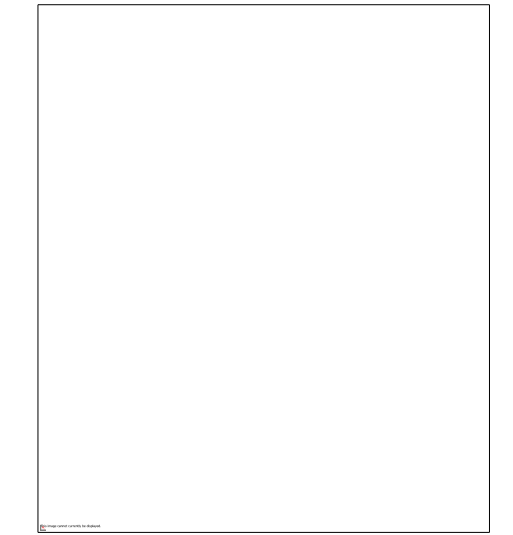
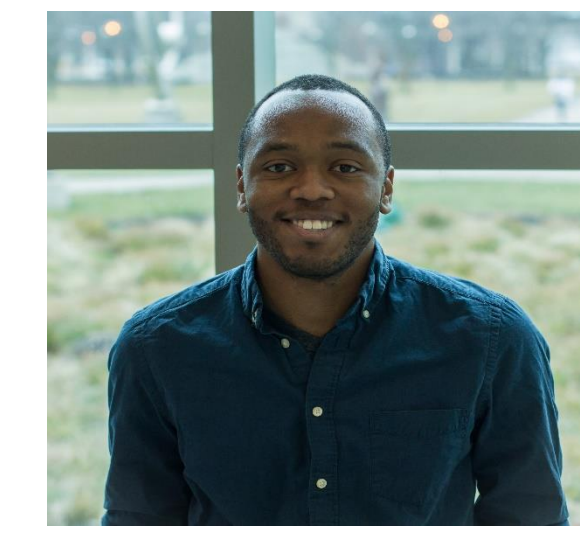


Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas

Death By Suicide?



Potential Attacks

Analysis

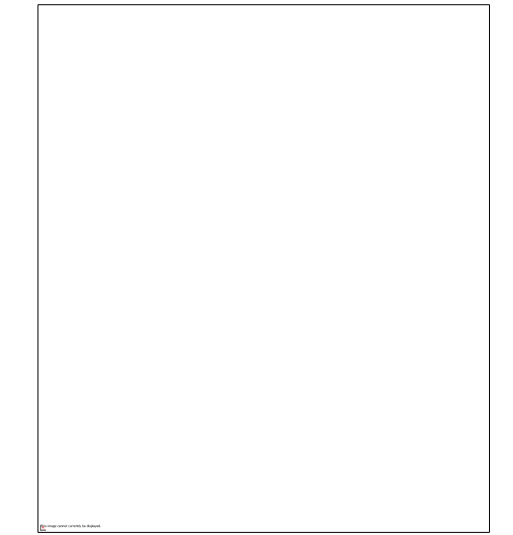
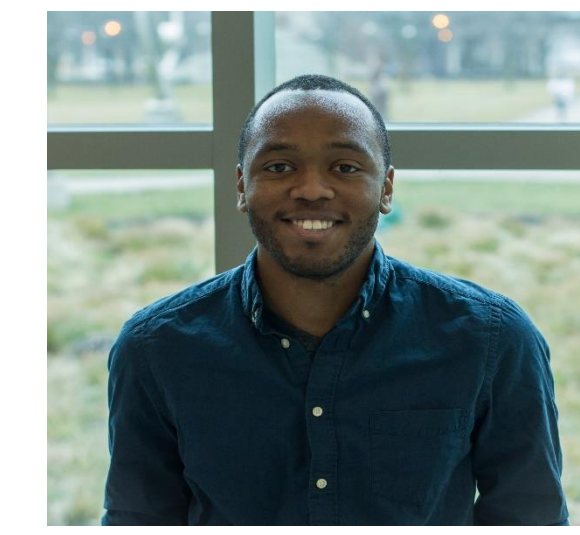
- Side Channel Attack
- Brute Force Attack (ex: dust for fingerprints)
- Hot Plug Attack
- Forced Restart
- Desoldering Electrically Erasable Programmable Read-Only Memory (EEPROM)

Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

Alex Andrews, Deshun Coomer and Michael Thomas

Death By Suicide?



Looking for commonality

Analysis

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

BsidesIndy Hacker Convention

bsidesindy.com

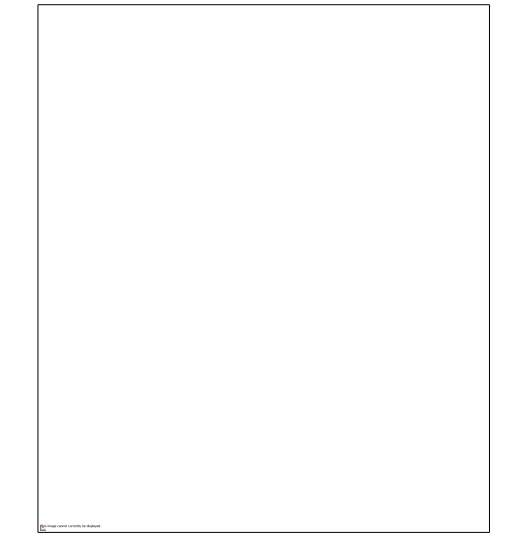
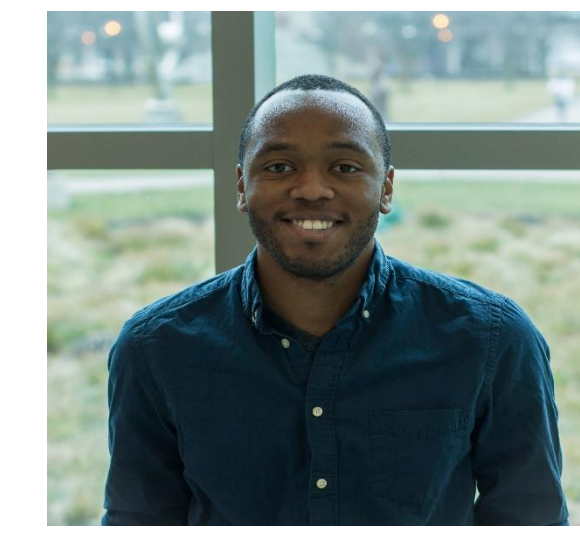
Reid Wightman

(twitter: @ReverseICS)

Target: SYBA S.E.D.

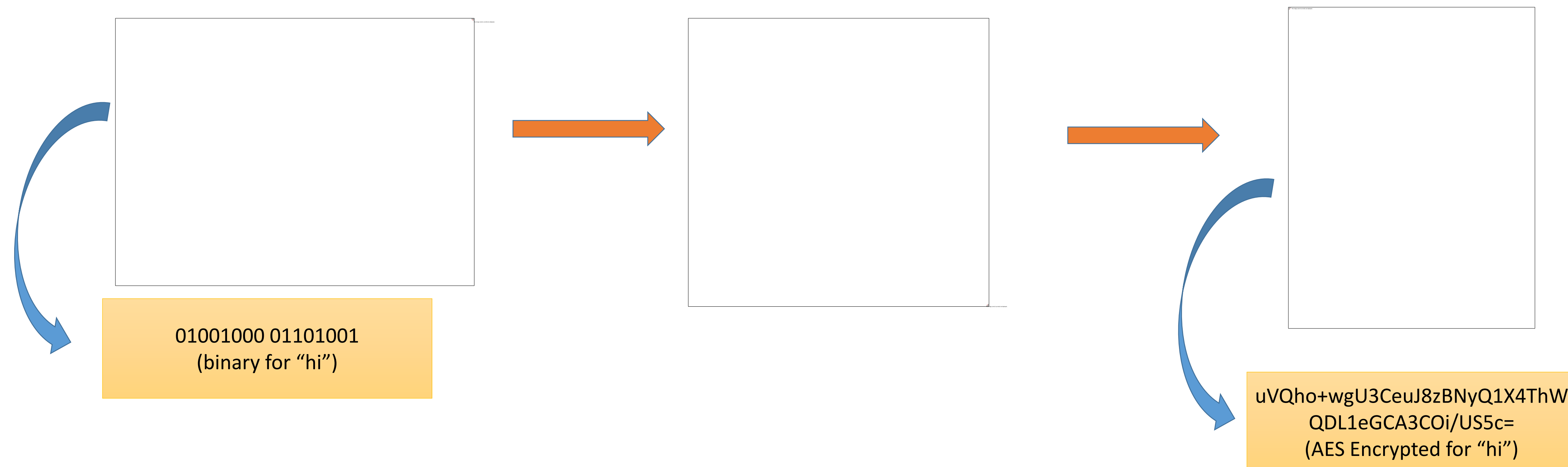
Examination of Syba Self-Encrypting Hard Drive

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



Looking for commonality

Analysis



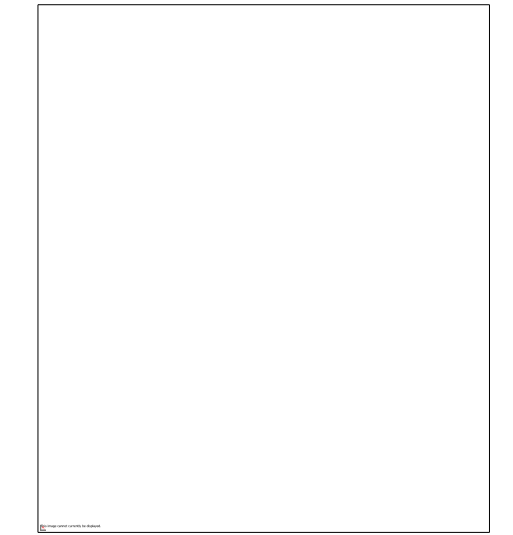
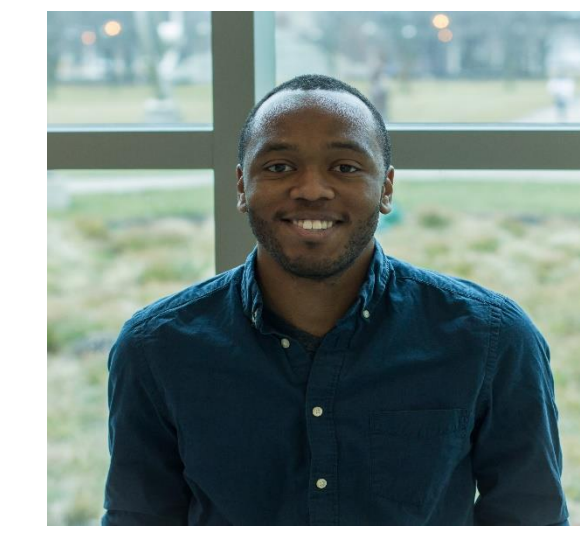
Sources:

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

Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

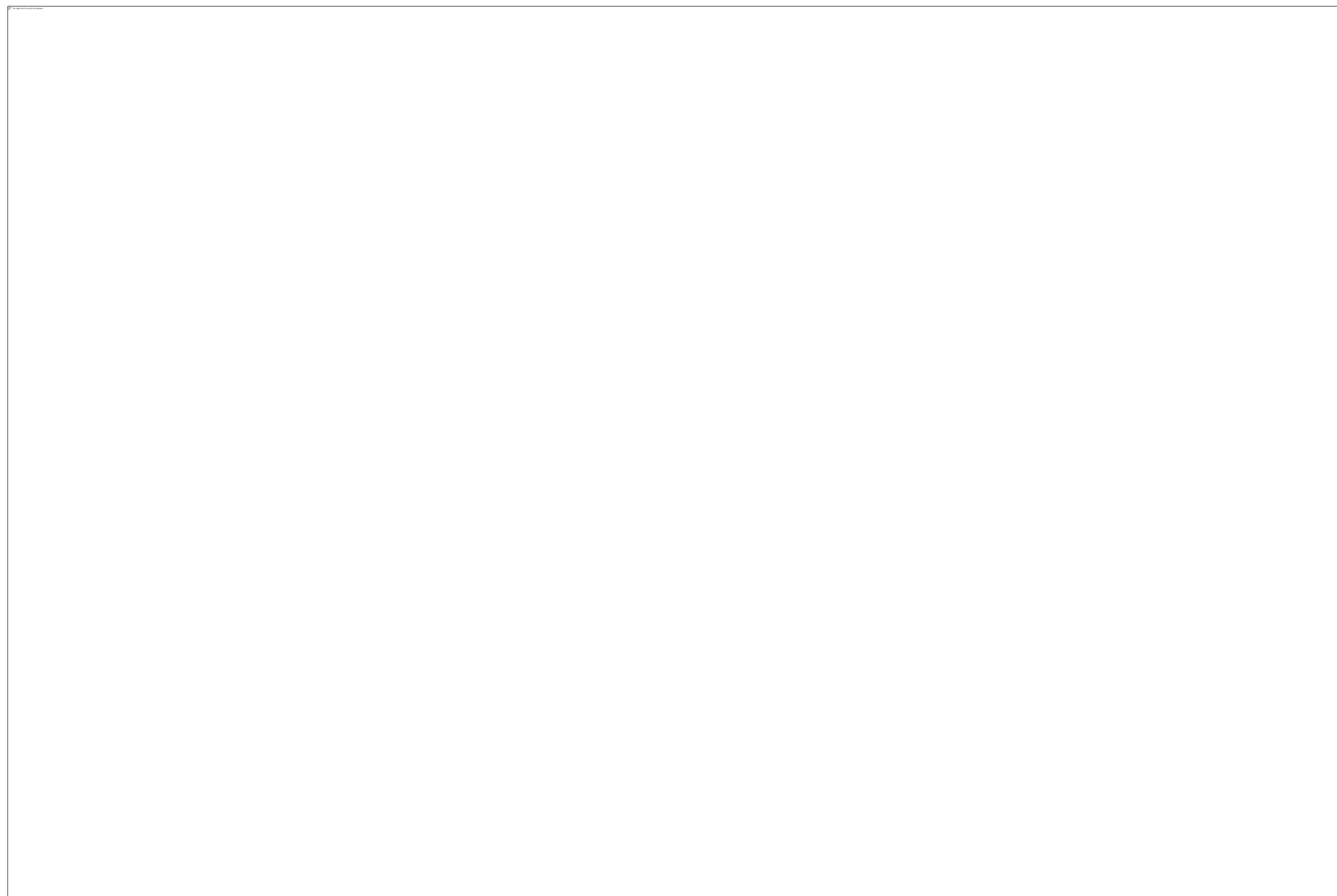
Alex Andrews, Deshun Coomer and Michael Thomas
Death By Suicide?



Looking for commonality

Analysis

```
Applications Places Mon Apr 24, 9:28 PM
8722 1499.585280000 184.50.239.16 10.243.16.243 HTTP 1534 Continuation of non-HTTP traffic
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 58
Protocol: TCP (6)
Header checksum: 0x6055 [correct]
Source: 184.50.239.16 (184.50.239.16)
Destination: 10.243.16.243 (10.243.16.243)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: http (80), Dst Port: 62571 (62571), Seq: 1, Ack: 1, Len: 1448
Hypertext Transfer Protocol
0020 08 00 45 00 05 dc 17 9e 40 00 3a 06 60 55 33 32 ..E.....@...U
0030 10 0a f3 10 f3 00 50 f4 0b 82 81 cd 75 7b 46 .....P.k...uIF
0040 97 fd 80 10 03 ab af cc 00 00 01 01 08 0a a1 7b .....{
0050 d0 52 50 bd 26 9e 56 72 4f 67 6e 54 37 76 2b 45 .RP.&.Vr OgnT7v+E
0060 57 36 32 4e 72 48 71 31 39 64 42 65 68 34 36 45 WQ2VrHq1 9dBh48E
0070 4d 31 65 2f 54 50 6a 32 57 63 6e 66 4c 53 7a 33 M4/TP2 WcnfLSc3
0080 42 4a 35 4b 74 73 5a 41 47 64 55 30 55 32 54 59 B3KtsZ4 G4UQUZTY
0090 69 67 48 6e 73 58 31 74 71 30 73 6c 61 4c 38 6d iHhsX1t q0sLaL8m
00a0 2b 6a 62 73 55 6d 32 47 6f 72 43 4c 58 64 2f 75 +jbsUm2G orCLXd/u
00b0 44 66 6f 44 71 6b 65 71 41 7a 68 34 7a 35 72 41 DfoDqkeq Azh425rA
00c0 73 66 64 33 6f 4c 32 2f 78 31 4e 35 37 68 7a 63 sfd3eL2/ x1N57hzc
00d0 31 6e 54 42 49 61 62 42 51 30 74 6f 2b 62 6d 59 InTSElab Q0t+bmV
00e0 56 41 6e 66 2f 2b 57 77 33 67 48 31 39 61 65 56 VAnf+Hw 3gh19aeV
00f0 75 71 6c 4e 62 68 74 56 6b 48 69 57 48 77 4f 4e uqLnhvtV kH1WhwON
0100 65 42 6c 67 67 48 4f 63 78 30 4b 2b 65 6a 79 64 eLggH0c x0K+ejyd
0110 69 30 76 63 51 37 31 70 42 2f 36 2f 63 59 64 77 10vcQ7lp B/6/cYdw
0120 54 52 45 57 41 6d 43 64 6e 48 45 51 72 54 6a 72 TR6WmCd RHEQrTJr
0130 42 67 62 63 54 6e 4f 62 72 48 5a 54 67 4c 55 77 BgbcTr0b RHZTgUw
0140 4b 4b 69 54 62 53 62 79 48 5a 2f 78 6a 61 61 67 Kk1TbSby HZjxaaq
0150 44 69 49 30 64 73 6d 73 4f 6a 6a 74 74 52 55 53 DiI0dsm5 OjttRUS
0160 2b 50 65 42 55 55 62 4a 62 68 62 44 32 50 53 31 +PeBUbJ bnbDZPS1
0170 67 2f 4e 78 73 59 4f 67 36 2b 35 4b 52 42 38 43 g/Nxst0g 6r5KRfB8C
0180 41 77 45 41 41 61 4f 43 41 59 30 77 67 67 47 4a AwEAa0C AY0vqGsl
0190 4d 41 73 47 41 31 55 64 44 77 51 45 41 77 49 46 MAsG1Ud DWQEAWJF
01a0 6f 44 41 64 42 67 4e 56 48 53 55 45 46 6a 41 55 oAdAgNw HSUEFjAU
01b0 42 67 67 72 42 67 45 46 42 51 63 44 41 51 59 49 BggrBg9F BQcDAQYI
01c0 4b 77 59 42 42 51 55 48 41 77 49 77 44 77 59 44 KwY8BQJH AwIwMwYD
01d0 56 52 30 66 42 43 77 77 4b 6a 41 6f 6f 43 61 67 VR9fBQwv KJAp0Cag
01e0 4a 49 59 69 61 48 52 30 63 44 6f 76 4c 32 4e 79 J1Y1aHRO cDovL2WY
01f0 62 43 35 62 6e 52 79 64 58 4a 30 4c 6d 35 6c bcS1bnRy dXNOLmSL
0200 64 43 39 73 5a 58 5a 6c 62 44 46 72 4c 6d 4e 79 dC9eZXZL bDfRLmNy
0210 62 44 42 4c 42 67 4e 56 48 53 41 45 52 44 42 43 bDBLbgNv HSAER0BC
0220 4d 44 59 47 43 6d 43 47 53 41 47 47 2b 6d 77 4b MDYGC0cG5 SAGGmmK
0230 41 51 55 77 4b 44 41 6d 42 67 67 72 42 67 45 46 AQLwK04m BggrBg9F
0240 42 51 63 43 41 52 59 61 61 48 52 30 63 44 6f 76 BQcCARYa aHRQCDov
0250 4c 33 64 33 64 79 35 6c 62 6e 52 79 64 58 4e 30 L3d3dyS1 bnRydxNO
0260 4c 6d 35 6c 64 43 39 79 63 47 45 77 43 41 59 47 Lm5ldc3y cGEwCAYG
```



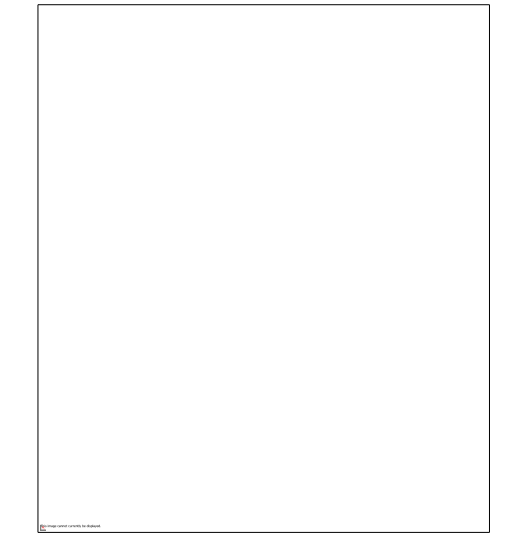
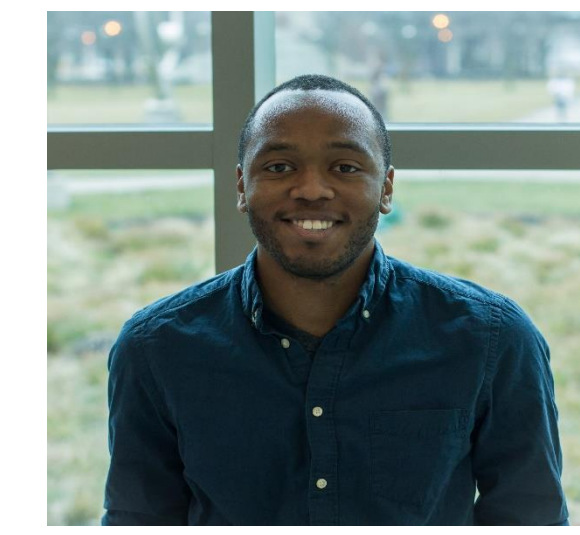
➡ Set of command prints multiple “A”s to the device “sdc” ➡ llsbik command to list what devices are available

➡ 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 be1a .^.....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 ..0.....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..b0{
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.G0.V..
root@research-Latitude-E6220: /home/research#
```

Diff is a command to compare differences between files.
"1,193c1,166" means line 2 1 -193 have changed versus file
1 line 1 - 166

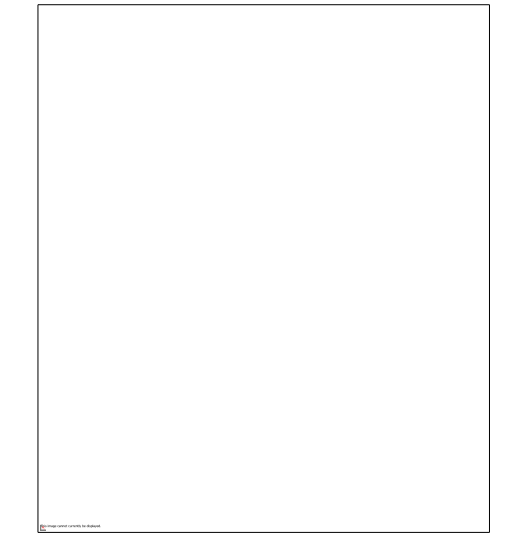
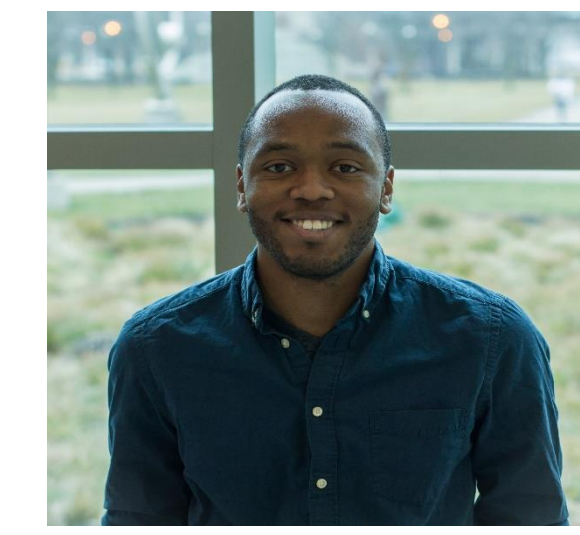
Is there a difference between password 1,
password 2 and going back to password 1
again?

Target: SYBA S.E.D.

Examination of Syba Self-Encrypting Hard Drive

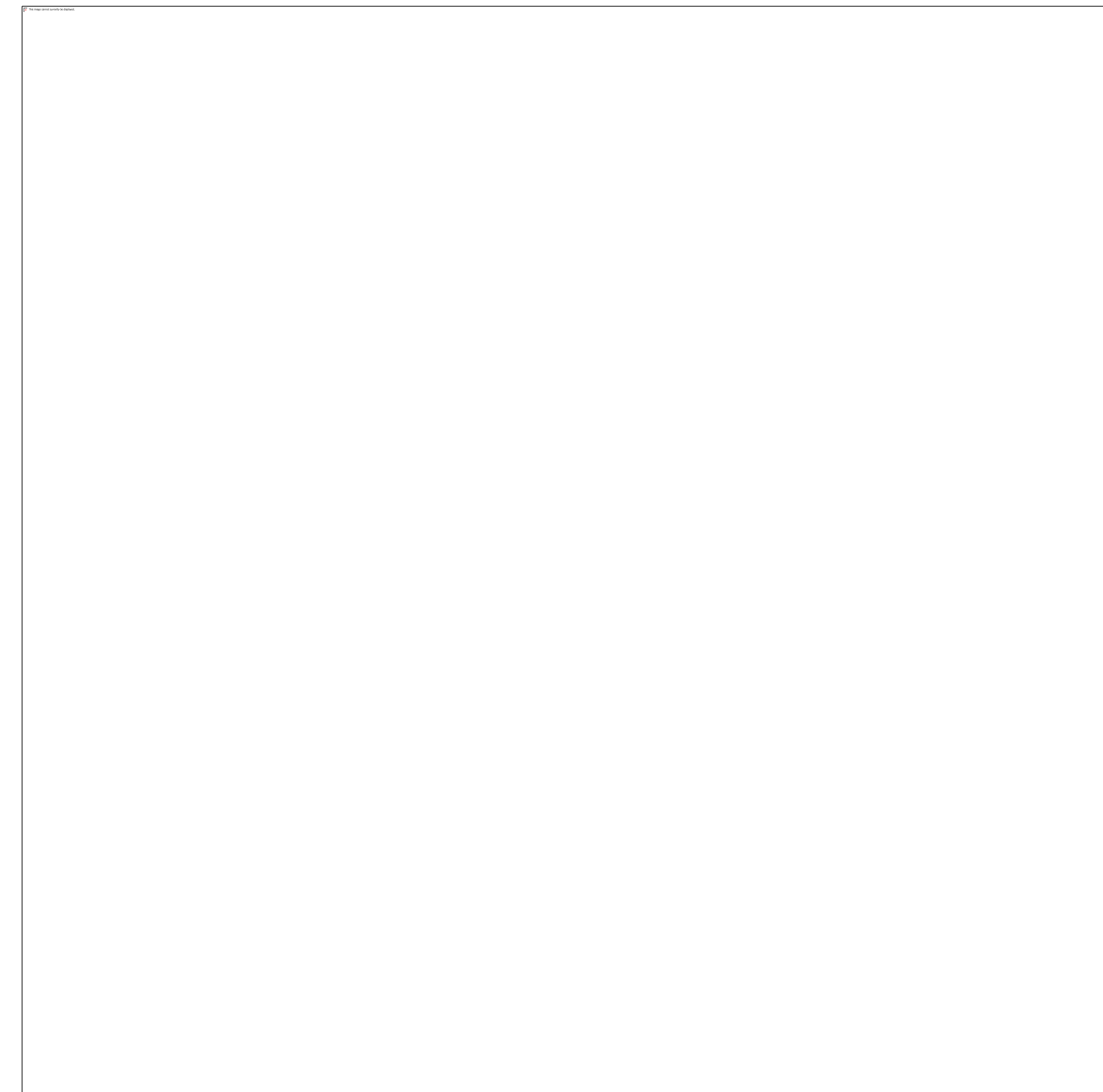
Alex Andrews, Deshun Coomer and Michael Thomas

Death By Suicide?



Looking for commonality

More Analysis



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

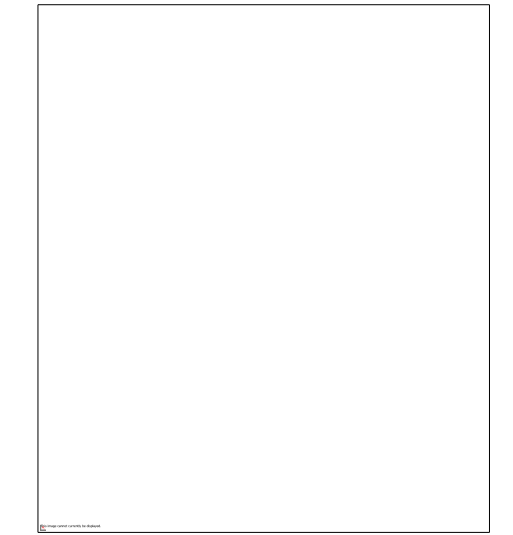
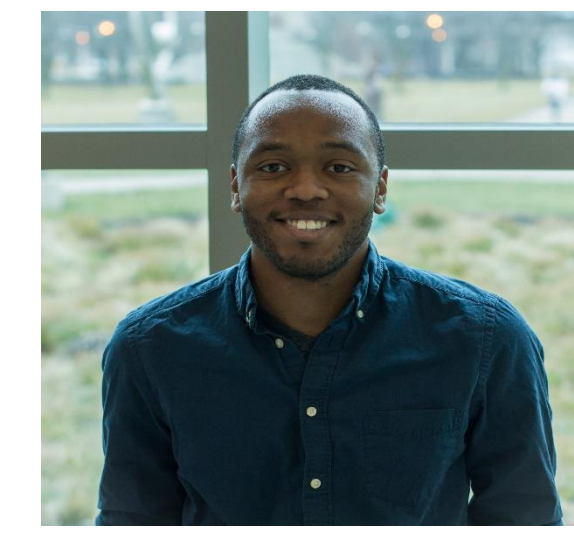
“A great challenge of life – Knowing enough to think you’re doing it right, but not enough to know you’re doing it wrong.” - Neil Degrasse Tyson

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.