0. git checkout -b audit-pyeron-88d24b9 88d24b9bcd5c83b4a0afd3d5baa47f224f901653

1. review all changes since e0b39ef434fdb0a225f2e9dd71bdd677c73e3231:

1.1. differing files:

1.1.1. src/Makefile

1.2. new Binary files:

1.2.1. GnuWin32/dd.exe
1.2.2. GnuWin32/gzip.exe
1.2.3. OriginalSources/TrueCrypt 7.1a Source.tar.gz
1.2.4. OriginalSources/TrueCrypt 7.1a Source.zip
1.2.5. doc/trust/contributors/p/y/pyeron,jason/cla-v2.0.1.pdf
1.2.6. nasm-2.08/nasm.exe

1.3. new files:

1.3.1. OriginalSources/Source.Verification.txt
1.3.2. OriginalSources/truecrypt-hashes.asc
1.3.3. Pkcs11/pkcs11.h
1.3.4. Pkcs11/pkcs11f.h
1.3.5. Pkcs11/pkcs11t.h
1.3.6. README.md
1.3.7. doc/trust/id/g/u/guglielmo,stephen_r/0xDD3766FF.txt
1.3.8. doc/trust/id/p/y/pyeron,jason/0xDA0848AD-smime-signed.msg
1.3.9. doc/trust/id/p/y/pyeron,jason/0xDA0848AD.txt
1.3.10. doc/trust/id/p/y/pyeron,jason/Pyeron.Jason.J.ORC1000040009.Encrypt.crt
1.3.11. doc/trust/id/p/y/pyeron,jason/Pyeron.Jason.J.ORC1000040009.ID.crt
1.3.12. nasm-2.08/LICENSE
1.3.13. src/.gitignore

2. Files

2.1. Makefile

The Makefile was updated [1.1.1] to include “ -I$(BASE_DIR)/Pkcs11” as shown when using a character level [A] diff. The pkcs11 files [1.3.3, 1.3.4, 1.3.5] are downloaded from ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/ using the same file names. These files are header files defining the function, method and constants shared between the various compilation units. These files do not contain cryptographic constants or algorithms.

2.2. OriginalSources

The files in OriginalSources [1.2.3, 1.2.4, 1.3.1, 1.3.2] are based on trust originating from Taylor Hornby[B], associated with Defuse Security, “a one-person security research and development group”. The file truecrypt-hashes.asc gpg verifies to his ID.

```
jpyeron@black /projects/cipherShed
$ gpg --verify < OriginalSources/truecrypt-hashes.asc
gpg: Signature made Sat, May 31, 2014 16:59:44 EDT using RSA key ID E9678D5D
gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: next trustdb check due at 2014-10-22
gpg: Good signature from "Taylor Hornby <havoc@defuse.ca>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: BFAE 45EB D356 1D91 E3E2  56C2 DFA8 209C E967 8D5D
```

That file then lists the two (TrueCrypt 7.1a Source.tar.gz, TrueCrypt 7.1a Source.zip) source archives’ hashes which verify. The files needed to be trusted against the well know TrueCrypt releases and the well known TrueCrypt Foundation gpg public key (0xF0D6B1E0).

```
jpyeron@black /projects/cipherShed/OriginalSources
$ wget https://github.com/DrWhax/truecrypt-archive/raw/master/TrueCrypt%207.1a%20Source.tar.gz.sig
```

```
jpyeron@black /projects/cipherShed/OriginalSources
$ gpg --verify TrueCrypt\ 7.1a\ Source.tar.gz.sig TrueCrypt\ 7.1a\ Source.tar.gz
gpg: Signature made Tue, Feb 07, 2012 15:45:26 EST using DSA key ID F0D6B1E0
gpg: Good signature from "TrueCrypt Foundation <info@truecrypt-foundation.org>"
```

```
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: C5F4 BAC4 A7B2 2DB8 B8F8  5538 E3BA 73CA F0D6 B1E0

jpyeron@black /projects/cipherShed/OriginalSources
$ wget https://github.com/DrWhax/truecrypt-archive/raw/master/TrueCrypt%207.1a%20Source.zip.sig

jpyeron@black /projects/cipherShed/OriginalSources
$ gpg --verify TrueCrypt\ 7.1a\ Source.zip.sig TrueCrypt\ 7.1a\ Source.zip
gpg: Signature made Tue, Feb 07, 2012 15:45:26 EST using DSA key ID F0D6B1E0
gpg: Good signature from "TrueCrypt Foundation <info@truecrypt-foundation.org>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: C5F4 BAC4 A7B2 2DB8 B8F8  5538 E3BA 73CA F0D6 B1E0
```

The above shows the source files provenance as authentic. The remaining file (Source.Verification.txt), is factually correct in each of the details, but did not provide the information necessary to establish a provenance of the files. The websites [C] consulted were well known sites regarding TrueCrypt.

2.3. Documentation.

2.3.1. The readme file [1.3.6] contains simple details, such as website information. It does not contain any development related instructions, such as compile instructions.

2.3.2. The Contributor License Agreement (CLA) [1.2.5] for Jason Pyeron (I am Jason Pyeron) and the identity files under doc/trust/id/ [1.3.7, 1.3.8, 1.3.9, 1.3.10, 1.3.11] were committed by myself, and should be verified by another auditor.
2.3.2.1. The CLA is a signed PDF, verifiable to my identity.
2.3.2.2. The Pyeron.Jason.J.ORC1000040009* files are my x509 identity certificates, verified by Operational Research Consultants, Inc.
2.3.2.3. The 0xDA0848AD.txt file is my gpg public key, which has been signed with my x509 ID certificate in the S/MIME message contained in the 0xDA0848AD-smime-signed.msg file.
2.3.2.4. This is the gpg public key extracted from the signed git commits.

2.4. Build utilities.

2.4.1. Intel CPU assembler, the Netwide Assembler (NASM), see http://nasm.us/. The TrueCrypt build instructions indicate that nasm 2.08 is needed to build the software. I have fetched the software from www.nasm.us.

```
wget http://www.nasm.us/pub/nasm/releasebuilds/2.08/win32/nasm-2.08-installer.exe

wget http://www.nasm.us/pub/nasm/releasebuilds/2.08/win32/nasm-2.08-win32.zip
```

I have verified the files against the currently downloaded files and from the hashes and signatures reported on a respected website [D] about TrueCrypt.

SHA1 and MD5 sums of each file:

```
86380574b0a199fc83414c5f986fa257e5f2ceff *./nasm-2.08-installer/LICENSE
d89d124974e487e5d64da6f1cd8acfbb         *./nasm-2.08-installer/LICENSE
0173f96b1c0f7725b8c355a7352d179a212bbd2b *./nasm-2.08-win32/LICENSE
0173f96b1c0f7725b8c355a7352d179a212bbd2b *nasm-2.08/LICENSE
8b1e1fd4260a88c3da85ee367ea866a3         *./nasm-2.08-win32/LICENSE
8b1e1fd4260a88c3da85ee367ea866a3         *nasm-2.08/LICENSE
ff09185dd731cc41f878e13da9f5f579d7368e81 *./nasm-2.08-installer/nasm.exe
ff09185dd731cc41f878e13da9f5f579d7368e81 *./nasm-2.08-win32/nasm.exe
ff09185dd731cc41f878e13da9f5f579d7368e81 *nasm-2.08/nasm.exe
71fd096f5b1d97cc8b93dfd22d23c84d         *./nasm-2.08-installer/nasm.exe
71fd096f5b1d97cc8b93dfd22d23c84d         *./nasm-2.08-win32/nasm.exe
71fd096f5b1d97cc8b93dfd22d23c84d         *nasm-2.08/nasm.exe
5efb0265c6d2a9da1eda5dd3ca3abbffc1a625f4 *./nasm-2.08-installer.exe
6ca37399edf93ddf862df87e087f3b90         *./nasm-2.08-installer.exe
78127607125d0105053753c55d87f9c40e74e498 *./nasm-2.08-win32.zip
33703d40d7a00cfa91efa32fdb3364f8         *./nasm-2.08-win32.zip
```

The license files differ in whitespace only and the files from nasm-2.08-installer.exe were extracted using 7zip [E]. The license file for nasm.exe v2.08 in CipherShed came from the win32.zip file.

2.4.2. The dd.exe [1.2.1] utility [F] found in GnuWin32 appears to come from http://gnuwin32.sourceforge.net/packages/coreutils.htm v5.3.0.

SHA1 and MD5 sums of each file:

```
519d153016c75061b99e55e3dd8efdd387b1266a *coreutils-5.3.0-bin.zip
aa7ce7f1f2befb930fb156bddea41bc4         *coreutils-5.3.0-bin.zip
97a97a62664b71f49df745063bce9d613d3b3cb4 *coreutils-5.3.0-bin/bin/dd.exe
97a97a62664b71f49df745063bce9d613d3b3cb4 *GnuWin32/dd.exe
9c36fdfdca4551c377c0fe97c5d64aef         *coreutils-5.3.0-bin/bin/dd.exe
9c36fdfdca4551c377c0fe97c5d64aef         *GnuWin32/dd.exe
```

2.4.3. The gzip.exe [1.2.2] utility found in GnuWin32 appears to come from http://gnuwin32.sourceforge.net/packages/gzip.htm v1.3.12.

SHA1 and MD5 sums of each file:

```
5108786e02247c7df6906625a2873ddac5f125be *gzip-1.3.12-1-bin/bin/gzip.exe
5108786e02247c7df6906625a2873ddac5f125be *GnuWin32/gzip.exe
bf2aaf579a213e86903031a3f95050e2         *gzip-1.3.12-1-bin/bin/gzip.exe
bf2aaf579a213e86903031a3f95050e2         *GnuWin32/gzip.exe
69901b7a58e324e39653d4282deaf5ab5bb5c07f *gzip-1.3.12-1-bin.zip
b24802293f74ab11aaa5786f36c59819         *gzip-1.3.12-1-bin.zip
```

2.5. Ignore files

The src/.gitignore [1.3.13] file tells the SCM system (git) to ignore files created under the src/ directory which match the patterns listed in the file.

2.5.1. *.o – These are object files, created prior to linking, but after compilation.
2.5.2. *.d – These are dependency files created as part of the Make process.
2.5.3. *.a – These are (static) libraries, collections of object code.
2.5.4. The remaining entries are targeted at specific files. But they are not prefixed with a “/” and as such will exclude the improbable existence of src/**/pattern. The .gitignore file should be corrected to prefix the “/”.
2.5.5. Common/Language.xml.h -
2.5.6. Common/Textual_logo_96dpi.bmp.h, Format/TrueCrypt_Wizard.bmp.h, Mount/Drive_icon_96dpi.bmp.h, Mount/Drive_icon_mask_96dpi.bmp.h, and Mount/Logo_96dpi.bmp.h – These are header files generated for the images included in the GUI and console.
2.5.7. Main/SystemPrecompiled.h.gch – a precompiled header. It is likely that the pattern *.h.gch should be used instead.
2.5.8. License.txt.h – file while appears to be only used on non-windows #IFNDEF TC_WINDOWS, I have been unable to find how or where this file is generated.
2.5.9. Main/truecrypt – this appears to be the Linux/non-windows main executable artifact. There are likely to be many more variants of this to be listed in the ignore file.

3. Provenance.

3.1. HEAD Commit.

The 88d24b9bcd5c83b4a0afd3d5baa47f224f901653 commit was a merge between 4281c4d2e38383ce9327aa63f86fdea7188669e1 and ef66ace6bbb66d5f7a18337f96a2df697648e73f. This commit was created by myself and needs to be verified by another auditor.

3.1.1. Selected critical commit log entries.

3.1.1.1.

```
commit 88d24b9bcd5c83b4a0afd3d5baa47f224f901653
gpg: Signature made Thu, Jun 26, 2014 15:39:27 EDT using RSA key ID DA0848AD
gpg: Good signature from "Jason Pyeron <jpyeron@pdinc.us>"
Merge: 4281c4d ef66ace
Author: Jason Pyeron <jpyeron@pdinc.us>
Date:   Thu Jun 26 15:39:12 2014 -0400

    Migration back to master branch - Merge remote-tracking branch 'origin/master' into master-with-history
```

3.1.1.2.

```
commit 4281c4d2e38383ce9327aa63f86fdea7188669e1
gpg: Signature made Thu, Jun 26, 2014 15:36:02 EDT using RSA key ID DA0848AD
gpg: Good signature from "Jason Pyeron <jpyeron@pdinc.us>"
Author: Jason Pyeron <jpyeron@pdinc.us>
Date:   Thu Jun 26 15:35:55 2014 -0400

     * Remove pkcs11 reference in .gitignore
     * Add include on pkcs11 source file in Makefile
```

```
3.1.1.3.
commit ef66ace6bbb66d5f7a18337f96a2df697648e73f
Merge: a03e565 3b350b9
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date:   Thu Jun 26 11:40:26 2014 -0400

    Merge pull request #12 from plcstpierre/master

    Added .gitignore for building on linux and modified the Makefile to include the pkcs headers in Pkcs11/

3.1.1.4.
commit 3b505ca0c338fd2132778a1877e3878705e5769d
gpg: Signature made Wed, Jun 11, 2014 13:11:06 EDT using RSA key ID DD3766FF
gpg: Good signature from "Stephen Robert Guglielmo <srg@guglielmo.us>"
gpg:                 aka "Stephen Robert Guglielmo <srguglielmo@gmail.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 0D54 BE6A B832 8701 AA94  9036 2D15 C7B0 DD37 66FF
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date:   Wed Jun 11 12:26:56 2014 -0400

    Hard reset due to some ambiguity in gpg signing, our workflow method, and the source archives. Signed this
commit. Included unix sources (tar.gz) and windows sources (zip)

3.1.1.5.
commit a03e565835e3ff66774a2a50946dc2290bcbc7d4
Merge: ac812aa b5adb3e
Author: PID0 <p1dz3r0@gmail.com>
Date:   Sat Jun 14 13:32:42 2014 +0100

    Merge pull request #8 from srguglielmo/master

    Reviewed 14/06/2014

3.1.1.6.
commit ac812aa395583b37dfca3f921c36385e744eb121
gpg: Signature made Wed, Jun 11, 2014 13:33:41 EDT using RSA key ID DD3766FF
gpg: Good signature from "Stephen Robert Guglielmo <srg@guglielmo.us>"
gpg:                 aka "Stephen Robert Guglielmo <srguglielmo@gmail.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 0D54 BE6A B832 8701 AA94  9036 2D15 C7B0 DD37 66FF
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date:   Wed Jun 11 13:33:33 2014 -0400

    Extracted archives without any EOL conversion. Removed verification and hash files as they're no longer
needed.

3.1.1.7.
commit b5adb3ed5787eeb767e51200a857f5e104bb2983
gpg: Signature made Thu, Jun 12, 2014 18:36:47 EDT using RSA key ID DD3766FF
gpg: Good signature from "Stephen Robert Guglielmo <srg@guglielmo.us>"
gpg:                 aka "Stephen Robert Guglielmo <srguglielmo@gmail.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 0D54 BE6A B832 8701 AA94  9036 2D15 C7B0 DD37 66FF
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date:   Thu Jun 12 18:36:40 2014 -0400

    Added a few dependencies to compile on Windows. Update README.md to reference the website to avoid creating
differences between the two.

3.1.1.8.
commit e0b39ef434fdb0a225f2e9dd71bdd677c73e3231
Author: TrueCrypt Foundation <info@truecrypt-foundation.org>
Date:   Tue Feb 7 11:37:10 2012 +0100

    TrueCrypt v7.1a - TrueCrypt 7.1a Source.zip

    extracted to src/
```

```
gpg verify TrueCrypt 7.1a Source.zip.sig
gpg: Signature made Tue, Feb 07, 2012 15:45:26 EST using DSA key ID F0D6B1E0
gpg: Good signature from "TrueCrypt Foundation <info@truecrypt-foundation.org>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: C5F4 BAC4 A7B2 2DB8 B8F8  5538 E3BA 73CA F0D6 B1E0

import script note: step 49 formula 20 common 16
```

3.2. Commit analysis.

The commits [3.1.1.1, 3.1.1.2] are signed, but the commit from Mr. Guglielmo [3.1.1.3] is not signed. Tracing the lineage on [3.1.1.3] brings us back to an audited commit [3.1.1.6], but introduces several authors along the way.

3.2.1. Authors:

3.2.1.1. Mr. Guglielmo - ac812aa395583b37dfca3f921c36385e744eb121
3.2.1.2. Mr. Horrocks - a03e565835e3ff66774a2a50946dc2290bcbc7d4
3.2.1.3. Mr. Caron St-Pierre - 6f47efca1a4070e0745f8fb8b80cf3c405a8f4dc
3.2.1.4. Mr. Pyeron - b188dc60742eaa1c23e455b1eb64361e23d855fc

3.2.2. Status.

Given the woven signed and unsigned commits of at least two well known participants it is clear that the source’s history can be trusted as valid. The SCM system provides cryptographic validation as to the accuracy of the changes made, but not the authorship of a given unsigned commit.

4. Conflict of Interest.

4.1. Organizational Conflict of Interest.

At this time, I have no organizational conflicts of interest. I am an employee of PD Inc and a member of the CipherShed PMC.

4.2. Developer Conflict of Interest.

The following commits [G] were either authored or committed by me and are covered by this audit, these commits should be verified by a different auditor.

4.2.1. 88d24b9bcd5c83b4a0afd3d5baa47f224f901653 - Migration back to master branch - Merge …
4.2.2. 4281c4d2e38383ce9327aa63f86fdea7188669e1 - * Remove pkcs11 reference in .gitignore …
4.2.3. 382b08a62dc9babe0c4a27150cfca7a545dfdc65 - Stephen Guglielmo's identification
4.2.4. 65efd37fd5a0513d7fb675028c7a911a5340948c - Merge branch 'master-with-history' into …
4.2.5. cf7b33db41230b77ea8096c23e604dbc62ce7227 - move source files to src directory
4.2.6. b188dc60742eaa1c23e455b1eb64361e23d855fc - Jason Pyeron's Contributor License Agreement & identification
4.2.7. e0b39ef434fdb0a225f2e9dd71bdd677c73e3231 - TrueCrypt v7.1a - TrueCrypt 7.1a Source.zip
4.2.8. d0a9dfa8c3974f149fa06ccd2a3e47affc65c51b - TrueCrypt v7.1a - TrueCrypt 7.1a Source.tar.gz
4.2.9. 12c94add198a5c7416d56fa224af6429c9b83bac - TrueCrypt v7.1 - TrueCrypt 7.1 Source.tar.gz
4.2.10. 7180d32a0aa0d7b97eba02daa3d6c236336e234c - TrueCrypt v7.1 - TrueCrypt 7.1 Source.zip
4.2.11. a264c411bc5b77d192181bb66c10bb9ebe096580 - TrueCrypt v7.0a - TrueCrypt 7.0a Source.zip
4.2.12. e6b1437a2e6e774b5d46e221ca491011fad5ed48 - TrueCrypt v7.0a - TrueCrypt 7.0a Source.tar.gz
4.2.13. 71345ee0d3d264326c04223b8d848a03b26d2e51 - TrueCrypt v7.0 - TrueCrypt 7.0 Source.zip
4.2.14. f1bb489ce96cc469d881a5f089dca2c30a56f0e4 - TrueCrypt v7.0 - TrueCrypt 7.0 Source.tar.gz
4.2.15. cac6cd14b155a775c11f29e65d2bd183c36df2d4 - TrueCrypt v6.3a - TrueCrypt 6.3a Source.tar.gz
4.2.16. 2fbb82aa4794cdb8db364dddb80857c5fea4c7db - TrueCrypt v6.3a - TrueCrypt 6.3a Source.zip
4.2.17. 375d02ae15e2be60e1c5fad2b9272c8144ef0923 - TrueCrypt v6.3 - TrueCrypt 6.3 Source.zip
4.2.18. ca2ea9fd5e239faa9cc7b9c06f2e916a8878305f - TrueCrypt v6.3 - TrueCrypt 6.3 Source.tar.gz
4.2.19. 60b79bde4bd8e597eeb450dc83f8b11be1d4f9dc - TrueCrypt v6.2a - TrueCrypt 6.2a Source.zip
4.2.20. bb6f6d4c31b805b32eb6abce006a5ea6ea68425e - TrueCrypt v6.2a - TrueCrypt 6.2a Source.tar.gz
4.2.21. 46ce567f8998a62c80bbdd01bcb4fbbc86457760 - TrueCrypt v6.2 - TrueCrypt 6.2 Source.zip
4.2.22. d94128a96ae336b71f15c95ceb8aee3c7ec76531 - TrueCrypt v6.2 - TrueCrypt 6.2 Source.tar.gz
4.2.23. 17c6e90b2b8dd57022e219eef80c3dae1986d3e8 - TrueCrypt v6.1a - TrueCrypt 6.1a Source.zip
4.2.24. a757b4d44532b7492033d8868244e2658ada797e - TrueCrypt v6.1a - TrueCrypt 6.1a Source.tar.gz
4.2.25. a3f71f0a419b7acae40ef4255eb8181271569c56 - TrueCrypt v6.1 - TrueCrypt 6.1 Source.zip
4.2.26. 0eb8b4fa18fecdd82dc4e2af820c9aa85f1cef79 - TrueCrypt v6.1 - TrueCrypt 6.1 Source.tar.gz
4.2.27. 893ebe6abb0fa4ea674469fea81aa1612fe307b3 - TrueCrypt v6.0a - TrueCrypt 6.0a Source.zip
4.2.28. 2c69456688c7d4ba2264ff3038c280f554185c93 - TrueCrypt v6.0a - TrueCrypt 6.0a Source.tar.gz
4.2.29. 07b2176f41ce6905a4e11b8f7afe333c0da13fa3 - TrueCrypt v6.0 - TrueCrypt 6.0 Source.tar.gz
4.2.30. 0ff8f78e2f963db6ce5db2f80db8afd0ca6181a7 - TrueCrypt v6.0 - TrueCrypt 6.0 Source.zip
4.2.31. 1b769d91b3fca0cf6fa6a0311484a6755b2bb474 - TrueCrypt v5.1a - TrueCrypt 5.1a Source.zip
4.2.32. 229e9eccd3cdd49fae6c75ab2bfddf465cb7578f - TrueCrypt v5.1a - TrueCrypt 5.1a Source.tar.gz

4.2.33. 8e221a243adb18c8e789f31101b0a583b321462e - TrueCrypt v5.1 - TrueCrypt 5.1 Source.tar.gz
4.2.34. 0f01a1bcd339158667d0bbc3658fc92f0afc4572 - TrueCrypt v5.1 - TrueCrypt 5.1 source.zip
4.2.35. c409c65b151e3c094779ae591cb08335a19ad005 - TrueCrypt v5.0 - TrueCrypt 5.0 Source.tar.gz
4.2.36. a17c95a3cf1d590a6e620839ded4d672f5fb338c - TrueCrypt v5.0 - TrueCrypt 5.0 Source.zip
4.2.37. 1fd5ff4fe5193f4fae3996815d39e669421176d0 - TrueCrypt v4.3 - truecrypt-4.3-source-code.zip
4.2.38. a33dc7e9dc5f5d886ea3d61b1e257c8dc885cdc4 - TrueCrypt v4.3 - truecrypt-4.3-source-code.tar.gz
4.2.39. 380b308c1060029c72efe213745476729a074466 - TrueCrypt v4.2a - truecrypt-4.2a-source-code.zip
4.2.40. 1ff4930a30b9903780d8875426ded1ae2aaddcbb - TrueCrypt v4.2a - truecrypt-4.2a-source-code.tar.gz
4.2.41. 5baff8a18699c25f7d215fe2cb0590c901aec254 - TrueCrypt v4.2 - truecrypt-4.2-source-code.zip
4.2.42. fe3d44a25be4d5789bc8808b283c6b302f25877d - TrueCrypt v4.2 - truecrypt-4.2-source-code.tar.gz
4.2.43. 02ec14954088e6dc3717f4142f4285eda3ccad3d - TrueCrypt v4.1 - truecrypt-4.1-source-code.zip
4.2.44. 53b9e897e9437f902819bd3f45c573c1b0decacb - TrueCrypt v4.1 - truecrypt-4.1-source-code.tar.gz
4.2.45. 55fe3189f75db92e759cda4172ff1bb4fbfd8b3b - TrueCrypt v4.0 - truecrypt-4.0-source-code.zip
4.2.46. 859f8eec4e1745df38210f816418ab5750febdb4 - TrueCrypt v4.0 - truecrypt-4.0-source-code.tar.gz
4.2.47. 4dc11fa5414331d7d504751f1ff8b4549e69ac49 - TrueCrypt v3.1a - truecrypt-3.1a-source-code.zip
4.2.48. 589151147d47b12039f4810d9c931a36fbdc26d6 - TrueCrypt v3.1 - truecrypt-3.1-source-code.zip
4.2.49. 9ef9b6d699f1dfaecc63c63f0ed78f0049a50db0 - TrueCrypt v3.0a - truecrypt-3.0a-source-code.zip
4.2.50. eced519edc5f02643b57ebe4bb1c83498da700ff - TrueCrypt v3.0 - truecrypt-3.0-source-code.zip
4.2.51. 2810da8c095f36c9b43312c93a871df5637f3924 - TrueCrypt v2.1a - truecrypt-2.1a-source-code.zip
4.2.52. 25a5d23abc434d8fcf99c3f11ea52c7c4dc8428a - TrueCrypt v2.1 - truecrypt-2.1-source-code.zip
4.2.53. 18ad9b18f9832f6316c33cc7089c2f557ed1d78e - TrueCrypt v2.0 - truecrypt-2.0-source-code.zip
4.2.54. 09754806c463d3765a723cf578e434b8d2074b54 - TrueCrypt v1.0a - truecrypt-1.0a-source-code.zip
4.2.55. 8294aa4ee6207be4103af0212e91f09c2ecfbb8e - TrueCrypt v1.0 - truecrypt-1.0-source-code.zip
4.2.56. d8da7787a770975c80a338aacd140a27cb183208 - Initial workspace for history extraction

5. Conclusion.

While some of the content being verified was produced by me, the properties of the SCM system along with the analysis presented above should be sufficient for a disinterested 3rd party to validate this audit treating my contributions with the highest skepticism.

It is clear that there are no changes made to the source code in the commits reviewed by this audit. But there were changes made to the build process. We reviewed those changes and found them to be needed, and proscribed, actions to properly build the CipherShed source code.

This audit did not attempt to build the software on Windows or any other platform, and as such it did not perform any validation on the generated binaries.

It is the conclusion of this audit that the source code has no newly introduced risks since the last audit on commit ac812aa395583b37dfca3f921c36385e744eb121 [H].

Jason Pyeron
Principal Consultant
PD Inc
10 W 24th St #100
Baltimore, MD 21218
USA

[A] --word-diff --word-diff-regex=.

[B] Public key found at https://keybase.io/defuse & https://defuse.ca/contact.htm and is attached to this report.

[C] https://www.grc.com/misc/truecrypt/truecrypt.htm
https://github.com/DrWhax/truecrypt-archive
http://andryou.com/truecrypt_orig/downloads2/

[D] https://madiba.encs.concordia.ca/~x_decarn/truecrypt-binaries-analysis/

[E] http://downloads.sourceforge.net/sevenzip/7z920-x64.msi

[F] https://en.wikipedia.org/wiki/Dd_(Unix)

[G]
```
git log --pretty=format:"%H%x09%ae%x09%ce%x09%s" |\
  grep jpyeron@pdinc.us |\
  sed 's/\t[-a-z@\.]\+\t[-a-z@\.]\+\t/ - /'
```

[H] https://github.com/CipherShed/CipherShed/blob/master/doc/trust/audits/p/y/pyeron%2Cjason/audit-report.txt