

0. git checkout

```
# Audit of e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c
git checkout -b audit-pyperon-e8529e9 e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c
```

1. git diff

```
# review all changes since 88d24b9bcd5c83b4a0afd3d5baa47f224f901653
git diff 88d24b9bcd5c83b4a0afd3d5baa47f224f901653 | grep ^diff | sed -e 's/ b\|.*$//; s/diff --git a\|/'
```

1.1. Renamed Files

- 1.1.1. src/Pkcs11/pkcs11.h
- 1.1.2. src/Pkcs11/pkcs11f.h
- 1.1.3. src/Pkcs11/pkcs11t.h
- 1.1.4. src/Common/CipherShed.ico
- 1.1.5. src/Format/CipherShed_Wizard.bmp
- 1.1.6. src/Release/Setup Files/CipherShed User Guide.pdf
- 1.1.7. src/Resources/Icons/CipherShed.icns
- 1.1.8. src/Setup/CipherShed_setup.bmp
- 1.1.9. src/Setup/CipherShed_setup_background.bmp
- 1.1.10. src/CipherShed.sln
- 1.1.11. src/Common/CipherShed_Volume.ico
- 1.1.12. src/Common/CipherShed_mounted.ico

1.2. Added Files

- 1.2.1. doc/trust/audits/p/y/pyeron,jason/audit-report.txt

1.3. Renamed & Changed Files

- 1.3.1. src/Main/Forms/CipherShed.fbp
- 1.3.2. src/Resources/Icons/CipherShed-16x16.xpm
- 1.3.3. src/Resources/Icons/CipherShed-48x48.xpm

1.4. Changed Files

- 1.4.1. README.md
- 1.4.2. src/Boot/Windows/BootMain.cpp
- 1.4.3. src/Boot/Windows/BootSector.asm
- 1.4.4. src/Boot/Windows/Decompressor.c
- 1.4.5. src/Build/Resources/MacOSX/Info.plist.xml
- 1.4.6. src/Common/Apidrvr.h
- 1.4.7. src/Common/BaseCom.cpp
- 1.4.8. src/Common/BaseCom.h
- 1.4.9. src/Common/BootEncryption.cpp
- 1.4.10. src/Common/BootEncryption.h
- 1.4.11. src/Common/Common.rc
- 1.4.12. src/Common/Crypto.c
- 1.4.13. src/Common/Dlgcode.c
- 1.4.14. src/Common/Dlgcode.h
- 1.4.15. src/Common/Exception.h
- 1.4.16. src/Common/GfMul.h
- 1.4.17. src/Common/Inflate.c
- 1.4.18. src/Common/Keyfiles.c
- 1.4.19. src/Common/Language.c
- 1.4.20. src/Common/Language.xml
- 1.4.21. src/Common/Registry.c
- 1.4.22. src/Common/Resource.h
- 1.4.23. src/Common/SecurityToken.cpp
- 1.4.24. src/Common/SecurityToken.h
- 1.4.25. src/Common/Tcdefs.h
- 1.4.26. src/Common/Volumes.c
- 1.4.27. src/Common/Xml.c
- 1.4.28. src/Core/Core.h
- 1.4.29. src/Core/CoreBase.cpp
- 1.4.30. src/Core/CoreBase.h
- 1.4.31. src/Core/CoreException.cpp
- 1.4.32. src/Core/CoreException.h
- 1.4.33. src/Core/FatFormatter.cpp
- 1.4.34. src/Core/FatFormatter.h
- 1.4.35. src/Core/HostDevice.cpp
- 1.4.36. src/Core/HostDevice.h
- 1.4.37. src/Core/MountOptions.cpp
- 1.4.38. src/Core/MountOptions.h
- 1.4.39. src/Core/RandomNumberGenerator.cpp
- 1.4.40. src/Core/RandomNumberGenerator.h
- 1.4.41. src/Core/Unix/CoreService.cpp
- 1.4.42. src/Core/Unix/CoreService.h
- 1.4.43. src/Core/Unix/CoreServiceProxy.h
- 1.4.44. src/Core/Unix/CoreServiceRequest.cpp
- 1.4.45. src/Core/Unix/CoreServiceRequest.h
- 1.4.46. src/Core/Unix/CoreServiceResponse.cpp
- 1.4.47. src/Core/Unix/CoreServiceResponse.h
- 1.4.48. src/Core/Unix/CoreUnix.cpp
- 1.4.49. src/Core/Unix/CoreUnix.h
- 1.4.50. src/Core/Unix/FreeBSD/CoreFreeBSD.cpp
- 1.4.51. src/Core/Unix/FreeBSD/CoreFreeBSD.h
- 1.4.52. src/Core/Unix/Linux/CoreLinux.cpp

1.4.53. src/Core/Unix/Linux/CoreLinux.h
1.4.54. src/Core/Unix/MacOSX/CoreMacOSX.cpp
1.4.55. src/Core/Unix/MacOSX/CoreMacOSX.h
1.4.56. src/Core/Unix/MountedFilesystem.h
1.4.57. src/Core/Unix/Solaris/CoreSolaris.cpp
1.4.58. src/Core/Unix/Solaris/CoreSolaris.h
1.4.59. src/Core/VolumeCreator.cpp
1.4.60. src/Core/VolumeCreator.h
1.4.61. src/Crypto/Aes.h
1.4.62. src/Crypto/Aes_x64.asm
1.4.63. src/Crypto/Aes_x86.asm
1.4.64. src/Crypto/Aesopt.h
1.4.65. src/Crypto/AesSmall.c
1.4.66. src/Crypto/AesSmall_x86.asm
1.4.67. src/Crypto/Aestab.c
1.4.68. src/Crypto/Blowfish.c
1.4.69. src/Crypto/Cast.c
1.4.70. src/Crypto/Des.c
1.4.71. src/Crypto/Rmd160.c
1.4.72. src/Crypto/Serpent.c
1.4.73. src/Crypto/Shal.c
1.4.74. src/Crypto/Twofish.c
1.4.75. src/Crypto/Whirlpool.c
1.4.76. src/Driver/BuildDriver.cmd
1.4.77. src/Driver/Driver.rc
1.4.78. src/Driver/Driver.vcproj
1.4.79. src/Driver/Fuse/FuseService.cpp
1.4.80. src/Driver/Fuse/FuseService.h
1.4.81. src/Driver/Ntdriver.c
1.4.82. src/Driver/Ntvols.c
1.4.83. src/Driver/Sources
1.4.84. src/Driver/VolumeFilter.c
1.4.85. src/Format/Format.rc
1.4.86. src/Format/Format.vcproj
1.4.87. src/Format/FormatCom.cpp
1.4.88. src/Format/FormatCom.h
1.4.89. src/Format/FormatCom.idl
1.4.90. src/Format/InPlace.c
1.4.91. src/Format/Tcformat.c
1.4.92. src/Main/Application.cpp
1.4.93. src/Main/Application.h
1.4.94. src/Main/CommandLineInterface.cpp
1.4.95. src/Main/CommandLineInterface.h
1.4.96. src/Main/FatalErrorHandler.cpp
1.4.97. src/Main/FatalErrorHandler.h
1.4.98. src/Main/FavoriteVolume.cpp
1.4.99. src/Main/FavoriteVolume.h
1.4.100. src/Main/Forms/AboutDialog.cpp
1.4.101. src/Main/Forms/AboutDialog.h
1.4.102. src/Main/Forms/BenchmarkDialog.cpp
1.4.103. src/Main/Forms/BenchmarkDialog.h
1.4.104. src/Main/Forms/ChangePasswordDialog.cpp
1.4.105. src/Main/Forms/ChangePasswordDialog.h
1.4.106. src/Main/Forms/DeviceSelectionDialog.cpp
1.4.107. src/Main/Forms/DeviceSelectionDialog.h
1.4.108. src/Main/Forms/EncryptionOptionsWizardPage.cpp
1.4.109. src/Main/Forms/EncryptionOptionsWizardPage.h
1.4.110. src/Main/Forms/EncryptionTestDialog.cpp
1.4.111. src/Main/Forms/EncryptionTestDialog.h
1.4.112. src/Main/Forms/FavoriteVolumesDialog.cpp
1.4.113. src/Main/Forms/FavoriteVolumesDialog.h
1.4.114. src/Main/Forms/Forms.cpp
1.4.115. src/Main/Forms/Forms.h
1.4.116. src/Main/Forms/InfoWizardPage.cpp
1.4.117. src/Main/Forms/InfoWizardPage.h
1.4.118. src/Main/Forms/KeyfileGeneratorDialog.cpp
1.4.119. src/Main/Forms/KeyfileGeneratorDialog.h
1.4.120. src/Main/Forms/KeyfilesDialog.cpp
1.4.121. src/Main/Forms/KeyfilesDialog.h
1.4.122. src/Main/Forms/KeyfilesPanel.cpp
1.4.123. src/Main/Forms/KeyfilesPanel.h
1.4.124. src/Main/Forms/LegalNoticesDialog.cpp
1.4.125. src/Main/Forms/LegalNoticesDialog.h
1.4.126. src/Main/Forms/MainFrame.cpp
1.4.127. src/Main/Forms/MainFrame.h
1.4.128. src/Main/Forms/MountOptionsDialog.cpp
1.4.129. src/Main/Forms/MountOptionsDialog.h
1.4.130. src/Main/Forms/NewSecurityTokenKeyfileDialog.cpp
1.4.131. src/Main/Forms/NewSecurityTokenKeyfileDialog.h
1.4.132. src/Main/Forms/PreferencesDialog.cpp
1.4.133. src/Main/Forms/PreferencesDialog.h
1.4.134. src/Main/Forms/ProgressWizardPage.cpp
1.4.135. src/Main/Forms/ProgressWizardPage.h

1.4.136. src/Main/Forms/RandomPoolEnrichmentDialog.cpp
1.4.137. src/Main/Forms/RandomPoolEnrichmentDialog.h
1.4.138. src/Main/Forms/SecurityTokenKeyfilesDialog.cpp
1.4.139. src/Main/Forms/SecurityTokenKeyfilesDialog.h
1.4.140. src/Main/Forms/SelectDirectoryWizardPage.cpp
1.4.141. src/Main/Forms/SelectDirectoryWizardPage.h
1.4.142. src/Main/Forms/SingleChoiceWizardPage.h
1.4.143. src/Main/Forms/VolumeCreationProgressWizardPage.cpp
1.4.144. src/Main/Forms/VolumeCreationProgressWizardPage.h
1.4.145. src/Main/Forms/VolumeCreationWizard.cpp
1.4.146. src/Main/Forms/VolumeCreationWizard.h
1.4.147. src/Main/Forms/VolumeFormatOptionsWizardPage.cpp
1.4.148. src/Main/Forms/VolumeFormatOptionsWizardPage.h
1.4.149. src/Main/Forms/VolumeLocationWizardPage.cpp
1.4.150. src/Main/Forms/VolumeLocationWizardPage.h
1.4.151. src/Main/Forms/VolumePasswordPanel.cpp
1.4.152. src/Main/Forms/VolumePasswordPanel.h
1.4.153. src/Main/Forms/VolumePasswordWizardPage.cpp
1.4.154. src/Main/Forms/VolumePasswordWizardPage.h
1.4.155. src/Main/Forms/VolumePropertiesDialog.cpp
1.4.156. src/Main/Forms/VolumePropertiesDialog.h
1.4.157. src/Main/Forms/VolumeSizeWizardPage.cpp
1.4.158. src/Main/Forms/VolumeSizeWizardPage.h
1.4.159. src/Main/Forms/WizardFrame.cpp
1.4.160. src/Main/Forms/WizardFrame.h
1.4.161. src/Main/Forms/WizardPage.h
1.4.162. src/Main/GraphicUserInterface.cpp
1.4.163. src/Main/GraphicUserInterface.h
1.4.164. src/Main/Hotkey.cpp
1.4.165. src/Main/Hotkey.h
1.4.166. src/Main/LanguageStrings.cpp
1.4.167. src/Main/LanguageStrings.h
1.4.168. src/Main/Main.make
1.4.169. src/Main/Resources.cpp
1.4.170. src/Main/Resources.h
1.4.171. src/Main/StringFormatter.cpp
1.4.172. src/Main/StringFormatter.h
1.4.173. src/Main/TextUserInterface.cpp
1.4.174. src/Main/TextUserInterface.h
1.4.175. src/Main/Unix/Main.cpp
1.4.176. src/Main/UserInterface.cpp
1.4.177. src/Main/UserInterface.h
1.4.178. src/Main/UserInterfaceException.h
1.4.179. src/Main/UserInterfaceType.h
1.4.180. src/Main/UserPreferences.cpp
1.4.181. src/Main/UserPreferences.h
1.4.182. src/Main/VolumeHistory.cpp
1.4.183. src/Main/VolumeHistory.h
1.4.184. src/Main/Xml.cpp
1.4.185. src/Main/Xml.h
1.4.186. src/Makefile
1.4.187. src/Mount/Favorites.cpp
1.4.188. src/Mount/Favorites.h
1.4.189. src/Mount/MainCom.cpp
1.4.190. src/Mount/MainCom.h
1.4.191. src/Mount/MainCom.idl
1.4.192. src/Mount/Mount.c
1.4.193. src/Mount/Mount.h
1.4.194. src/Mount/Mount.rc
1.4.195. src/Mount/Mount.vcproj
1.4.196. src/Platform/Buffer.cpp
1.4.197. src/Platform/Buffer.h
1.4.198. src/Platform/Directory.h
1.4.199. src/Platform/Event.cpp
1.4.200. src/Platform/Event.h
1.4.201. src/Platform/Exception.cpp
1.4.202. src/Platform/Exception.h
1.4.203. src/Platform/File.h
1.4.204. src/Platform/FileCommon.cpp
1.4.205. src/Platform/FileStream.h
1.4.206. src/Platform/FilesystemPath.h
1.4.207. src/Platform/ForEach.h
1.4.208. src/Platform/Functor.h
1.4.209. src/Platform/Memory.cpp
1.4.210. src/Platform/Memory.h
1.4.211. src/Platform/MemoryStream.cpp
1.4.212. src/Platform/MemoryStream.h
1.4.213. src/Platform/Mutex.h
1.4.214. src/Platform/PlatformBase.h
1.4.215. src/Platform/PlatformTest.cpp
1.4.216. src/Platform/PlatformTest.h
1.4.217. src/Platform/Serializable.cpp
1.4.218. src/Platform/Serializable.h

1.4.219. src/Platform/Serializer.cpp
1.4.220. src/Platform/Serializer.h
1.4.221. src/Platform/SerializerFactory.cpp
1.4.222. src/Platform/SerializerFactory.h
1.4.223. src/Platform/SharedPtr.h
1.4.224. src/Platform/SharedVal.h
1.4.225. src/Platform/Stream.h
1.4.226. src/Platform/StringConverter.cpp
1.4.227. src/Platform/StringConverter.h
1.4.228. src/Platform/SyncEvent.h
1.4.229. src/Platform/SystemException.h
1.4.230. src/Platform/SystemInfo.h
1.4.231. src/Platform/SystemLog.h
1.4.232. src/Platform/TextReader.cpp
1.4.233. src/Platform/TextReader.h
1.4.234. src/Platform/Thread.h
1.4.235. src/Platform/Time.h
1.4.236. src/Platform/Unix/Directory.cpp
1.4.237. src/Platform/Unix/File.cpp
1.4.238. src/Platform/Unix/FilePath.cpp
1.4.239. src/Platform/Unix/Mutex.cpp
1.4.240. src/Platform/Unix/Pipe.cpp
1.4.241. src/Platform/Unix/Pipe.h
1.4.242. src/Platform/Unix/Poller.cpp
1.4.243. src/Platform/Unix/Poller.h
1.4.244. src/Platform/Unix/Process.cpp
1.4.245. src/Platform/Unix/Process.h
1.4.246. src/Platform/Unix/SyncEvent.cpp
1.4.247. src/Platform/Unix/SystemException.cpp
1.4.248. src/Platform/Unix/SystemInfo.cpp
1.4.249. src/Platform/Unix/SystemLog.cpp
1.4.250. src/Platform/Unix/Thread.cpp
1.4.251. src/Platform/Unix/Time.cpp
1.4.252. src/Platform/User.h
1.4.253. src/Readme.txt
1.4.254. src/Setup/ComSetup.cpp
1.4.255. src/Setup/ComSetup.rgs
1.4.256. src/Setup/SelfExtract.c
1.4.257. src/Setup/Setup.c
1.4.258. src/Setup/Setup.h
1.4.259. src/Setup/Setup.rc
1.4.260. src/Setup/Setup.vcproj
1.4.261. src/Setup/Wizard.c
1.4.262. src/Volume/Cipher.cpp
1.4.263. src/Volume/Cipher.h
1.4.264. src/Volume/Crc32.h
1.4.265. src/Volume/EncryptionAlgorithm.cpp
1.4.266. src/Volume/EncryptionAlgorithm.h
1.4.267. src/Volume/EncryptionMode.cpp
1.4.268. src/Volume/EncryptionMode.h
1.4.269. src/Volume/EncryptionModeCBC.cpp
1.4.270. src/Volume/EncryptionModeCBC.h
1.4.271. src/Volume/EncryptionModeLRW.cpp
1.4.272. src/Volume/EncryptionModeLRW.h
1.4.273. src/Volume/EncryptionModeXTS.cpp
1.4.274. src/Volume/EncryptionModeXTS.h
1.4.275. src/Volume/EncryptionTest.cpp
1.4.276. src/Volume/EncryptionTest.h
1.4.277. src/Volume/EncryptionThreadPool.cpp
1.4.278. src/Volume/EncryptionThreadPool.h
1.4.279. src/Volume/Hash.cpp
1.4.280. src/Volume/Hash.h
1.4.281. src/Volume/Keyfile.cpp
1.4.282. src/Volume/Keyfile.h
1.4.283. src/Volume/Pkcs5Kdf.cpp
1.4.284. src/Volume/Pkcs5Kdf.h
1.4.285. src/Volume/Version.h
1.4.286. src/Volume/Volume.cpp
1.4.287. src/Volume/Volume.h
1.4.288. src/Volume/VolumeException.cpp
1.4.289. src/Volume/VolumeException.h
1.4.290. src/Volume/VolumeHeader.cpp
1.4.291. src/Volume/VolumeHeader.h
1.4.292. src/Volume/VolumeInfo.cpp
1.4.293. src/Volume/VolumeInfo.h
1.4.294. src/Volume/VolumeLayout.cpp
1.4.295. src/Volume/VolumeLayout.h
1.4.296. src/Volume/VolumePassword.cpp
1.4.297. src/Volume/VolumePassword.h
1.4.298. src/Volume/VolumePasswordCache.cpp
1.4.299. src/Volume/VolumePasswordCache.h
1.4.300. src/Volume/VolumeSlot.h

1.5. Deleted Files

- 1.5.1. bin/history-common-steps.sh
- 1.5.2. bin/history-step-00.sh
- 1.5.3. bin/history-step-01.sh
- 1.5.4. bin/history-step-02.sh
- 1.5.5. bin/history-step-03.sh
- 1.5.6. bin/history-step-04.sh
- 1.5.7. bin/history-step-05.sh
- 1.5.8. bin/history-step-06.sh
- 1.5.9. bin/history-step-07.sh
- 1.5.10. bin/history-step-08.sh
- 1.5.11. bin/history-step-09.sh
- 1.5.12. bin/history-step-10.sh
- 1.5.13. bin/history-step-11.sh
- 1.5.14. bin/history-step-12.sh
- 1.5.15. bin/history-step-13.sh
- 1.5.16. bin/history-step-14.sh
- 1.5.17. bin/history-step-15.sh
- 1.5.18. bin/history-step-16.sh
- 1.5.19. bin/history-step-17.sh
- 1.5.20. bin/history-step-18.sh
- 1.5.21. bin/history-step-19.sh
- 1.5.22. bin/history-step-20.sh
- 1.5.23. bin/history-step-21.sh
- 1.5.24. bin/history-step-22.sh
- 1.5.25. bin/history-step-23.sh
- 1.5.26. bin/history-step-24.sh
- 1.5.27. bin/history-step-25.sh
- 1.5.28. bin/history-step-26.sh
- 1.5.29. bin/history-step-27.sh
- 1.5.30. bin/history-step-28.sh
- 1.5.31. bin/history-step-29.sh
- 1.5.32. bin/history-step-30.sh
- 1.5.33. bin/history-step-31.sh
- 1.5.34. bin/history-step-32.sh
- 1.5.35. bin/history-step-33.sh
- 1.5.36. bin/history-step-34.sh
- 1.5.37. bin/history-step-35.sh
- 1.5.38. bin/history-step-36.sh
- 1.5.39. bin/history-step-37.sh
- 1.5.40. bin/history-step-38.sh
- 1.5.41. bin/history-step-39.sh
- 1.5.42. bin/history-step-40.sh
- 1.5.43. bin/history-step-41.sh
- 1.5.44. bin/history-step-42.sh
- 1.5.45. bin/history-step-43.sh
- 1.5.46. bin/history-step-44.sh
- 1.5.47. bin/history-step-45.sh
- 1.5.48. bin/history-step-46.sh
- 1.5.49. bin/history-step-47.sh
- 1.5.50. bin/history-step-48.sh
- 1.5.51. bin/history-step-49.sh
- 1.5.52. bin/history-step-50.sh
- 1.5.53. bin/history-step-51.sh
- 1.5.54. etc/history-conversion-dos2unix-exempt
- 1.5.55. etc/history-conversion-dos2unix-utf
- 1.5.56. etc/history-conversion-unix2dos
- 1.5.57. etc/history-conversion-unix2dos-utf
- 1.5.58. etc/history-step-01.srcmod
- 1.5.59. etc/history-step-02.srcmod
- 1.5.60. etc/history-step-03.srcmod
- 1.5.61. etc/history-step-04.srcmod
- 1.5.62. etc/history-step-05.srcmod
- 1.5.63. etc/history-step-07.srcmod
- 1.5.64. etc/history-step-10.srcmod
- 1.5.65. etc/history-step-18.srcmod
- 1.5.66. etc/history-step-20.srcmod
- 1.5.67. etc/history-step-22.srcmod
- 1.5.68. etc/history-step-26.srcmod
- 1.5.69. etc/history-step-30.srcmod
- 1.5.70. etc/history-step-50.srcmod
- 1.5.71. etc/scripts.xls
- 1.5.72. files/TrueCrypt 7.1a Source.tar.gz
- 1.5.73. files/TrueCrypt 7.1a Source.tar.gz.sig
- 1.5.74. files/TrueCrypt 7.1a Source.zip
- 1.5.75. files/TrueCrypt 7.1a Source.zip.sig
- 1.5.76. src/License.html
- 1.5.77. readme-history.txt

2. Files

2.1. Unneeded Files

2.1.1. Deleted files 1.5.1 ... 1.5.53 are the scripts used to import the TrueCrypt history.

- 2.1.2. Deleted files 1.5.54 ... 1.5.57 are support scripts to fix and manage line endings during the TrueCrypt history import
- 2.1.3. Deleted files 1.5.58 ... 1.5.70 are kludge patches to help git understand the changes in a human fashion.
- 2.1.4. Deleted file 1.5.71 is the Excel file used to create the command sequence for the TrueCrypt history import.
- 2.1.5. Deleted files 1.5.72 ... 1.5.75 are the TrueCrypt 7.1a source files and GPG signatures.
- 2.1.6. Deleted file 1.5.76 is a HTML duplicate of src/License.txt.
- 2.1.7. Deleted file 1.5.77 contains notes on the history import.

2.2. Reorganization

- 2.2.1. Files 1.1.1 ... 1.1.3 were moved into the src directory since they are source files.
- 2.2.2. The team is in the progress of renaming TrueCrypt to CipherShed, as required by the TrueCrypt license. The following files were renamed, but otherwise unmodified, as part of that effort: 1.1.4 ... 1.1.12 .

2.3. Documentation

- 2.3.1. Audit report (#1.2.1)
- 2.3.2. Removed documentation, see 2.1.6 & 2.1.7 .
- 2.3.3. Readme.txt (#1.4.253) was primarily simplified by pointing the reader at <https://ciphershed.org> but also included license compliance clause 'Based on TrueCrypt, freely available at <http://www.truecrypt.org/>' and a bulk renaming of the TrueCrypt name as covered in 2.4.1 .
- 2.3.4. README.md (#1.4.1) is the file used by github.com and other source viewers to present the 'default' documentation. It was modified to point users to the main website [<https://ciphershed.org>] and to the wiki [<https://wiki.ciphershed.org>] .

2.4. License Compliance

2.4.1. Rename TrueCrypt to CipherShed

- 2.4.1.1. A bulk search and replace for 'truecrypt' with 'ciphershed' was performed on the source. The automated replacement took care to ensure case sensitive issues were preserved, but did not take into account the semantics of the usage. It is a naive approach, likely to cause functionality problems. Examples like 1.4.6, 1.4.9 and 1.4.257 are worrisome. The file modified by this technique are as follows:
 - 2.4.1.1.1. Renamed files 1.3.1, 1.3.2 and 1.3.3 .
 - 2.4.1.1.2. Changed files 1.4.2 ... 1.4.25, 1.4.26 ... 1.4.91, 1.4.92 ... 1.4.252, 1.4.254 ... 1.4.260, 1.4.261 and 1.4.262 ... 1.4.300 .

2.4.2. Other changes due license compliance

- 2.4.2.1. src/Build/Resources/MacOSX/Info.plist.xml
 - 2.4.2.1.1. CFBundleIdentifier should be in reverse DNS format per <https://developer.apple.com/library/ios/documentation/General/Reference/InfoPlistKeyReference/Articles/CoreFoundationKeys.html> both the old and new domains need to be managed.
- 2.4.2.2. src/Common/Dlgcode.c
 - 2.4.2.2.1. Removed 'A TrueCrypt Foundation Release'
- 2.4.2.3. src/Driver/Ntdriver.c
 - 2.4.2.3.1. Due to the search and replace described in 2.4.1, the hard coded constant 9 has to be replaced with 10 in several locations. These constants represents the length of 'truecrypt' and 'ciphershed'.
- 2.4.2.4. src/Main/Forms/AboutDialog.cpp
 - 2.4.2.4.1. Removed 'A TrueCrypt Foundation Release'

3. Provenance

3.1. Commits

3.1.1. HEAD commit

The e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c is a merge of a pull request #15 (344df5d), preceded by another pull request #14 (f0ae850), an individual commit (a014f72) and the rebranding branch (1ca13ed / 8d7bf49). The 88d24b9 commit was subject to a previous audit and all commits in this audit have a common parent ac812aa covered by that audit.

3.1.2. Commit graph

```
* e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c
|\
| * 344df5dd9758eb82334cfbbb770f93666d253bb7
|/
* 6bccfd68c6e3dbc1e447626a009c47fccf1440dd
|\
| * f0ae85017fec4f318b84d055685187f06bf71312
* | a014f721c87d870613e9b1cc99d2d2c435cf3054
* | d60fc07272295fc57c2fac7c50911f74177a89c7
|\
| * | 1ca13ed2271d60ba93d40bcc8db17ced8545f172
| * | d8587c43cfdb12343524ce117a4a59726c438925
| * | 49ecd874029ea287d2755f7e0d5188ce49e81a
| * | 4054940be1088f23f968b610fa6a158ff05e2015
| * | b50a2fb10f15e77a96223af07afbe60228c4d520
| * | 5e56915f9f5ff190fb26273071f280b40c7f3d18
| * | 0d0c2129d8eda46d205fa5894efd128a1cf3e8d2
| * | 5fda89e7ed0c19817644cc4c390e67c98b31f5a0
| * | 164eb7ec93e2dbbcb7a804796179abcd4e33e223
| * | c9a2bb77f9942b6edc7fa807d4ab98d54332db85
| * | e362af03fa040dccff361cd3263490082ed99dfc
| * | 9aae7980d8ec60378cb2a07ec36c90f32a9f97f6
| * | 2e3598df96de419897294faced437c04f8e8f5d6
| * | 574dc0e5333d4197a6d3f5150e4f976b819755f1
| * | ca2f5d9c6cadd2f6f94f10434d0ca1274ecf573a
| * | e6db9b8e5decfb9fd1aaa06f84229b178b6d7f9b
| * | 1bd84ec051aac97332e4b983dce31836a3b238a0
| * | a0c84ff28f356bcb8b872a9c65a2e9bff97b3f68
| * | a79e05a24d25835a693bfcfbffe70d06175a54f5
| * | 71d4dc4f609d78f14fd264159d75081fe98d2ec2
* | | 8d7bf49c3adb639358e30a6be794f661655f5929
* | | 131ed5a07fc6ab88bc63db7d8d4088da692a1aa8
* | | 0d4799cba4a28ad4d644e78b7c55d9856b36baab
* | | 1bece0cf497338571d365eb8e7a5dda151237365
* | | 2e975682a98a9a1065521a314c7375e76ce65516
* | | 623f0c1c63a36998be8a483fe9996e2c68a4683d
* | | 91c0cd167dec0bab0a1b3b174ba5f9abac62f5a1
* | | 19de3eeb75bd4244ad542cc3ddbef55c1eb2758d
* | | 702dfef58ef4287500aeaea87c3fb6569cb6b35a
* | | de40b684577c75501617c235aea677921314094e
* | | 61ea96dfd9a305154fffd968e666b269f976eb989
* | | 806630e83cf788221be7e7463f2e781fdd5d9e07
* | | d7eeb3fbd0716db074744cb499a848ebbfde3lcb
* | | c2728a4ff19b5d965a5a7505535a17dea2ae3fb5
* | | 71ff2b0644962ad512ced1c739300211b866181c
* | | ee579eab5cc1df9fa7d1462a6fa6a88e9c8b5039
* | | ef3bfd993d21e933fa4c9fc9b58987e9a080e2a4
* | | c2dc7ffde4e779b7d0cd27ce2cd9c8b659807451
* | | 188850b70fd1a56a018ef581b6502bf6649b6541
* | | bdba05dd344762d2cbc9a9cbc874e82083a42974
* | | d3c8039a50f9ec5a1278459df94d3ccc312050db
* | | b60070f4d0879e277f44d174a163bbb292325fea
* | | 88d24b9bcd5c83b4a0afd3d5baa47f224f901653
|\
| * | ef66ace6bbb66d5f7a18337f96a2df697648e73f
|\
| * | | 3b350b9afb7f1094036ac3f593169b4a91f5eae4
* | | | 4281c4d2e38383ce9327aa63f86fdea7188669e1
* | | | 382b08a62dc9babe0c4a27150cfca7a545dfdc65
* | | | 65efd37fd5a0513d7fb675028c7a911a5340948c
|\
| * | | cf7b33db41230b77ea8096c23e604dbc62ce7227
| * | | b188dc60742eaa1c23e455b1eb64361e23d855fc
|
| | / / / /
| * | | 6f47efcala4070e0745f8fb8b80cf3c405a8f4dc
|
| | / / /
| * | | a03e565835e3ff66774a2a50946dc2290bcbcd7d4
|
| | / / /
|
| * | b5adb3ed5787eeb767e51200a857f5e104bb2983
| * | 756cdddae11a25bbb8e65e2c25bb932cc84ce3cd
| * | 3950ecd50c4dc33eff49529fa59a84ee17b8ad8e
|
| * | ac812aa395583b37dfca3f921c36385e744eb121
```

3.1.3. Selected critical commits' log entries

3.1.3.1. commit e8529e95d89d3f519a31ef7de5bd7f0d0d318e8c

Merge: 6bccfd6 344df5d
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date: Tue Jul 1 12:11:39 2014 -0400

Merge pull request #15 from srguglielmo/master

Update README with new links

3.1.3.2. commit 344df5dd9758eb82334cfbbb770f93666d253bb7

gpg: Signature made Tue, Jul 01, 2014 12:07:11 EDT using RSA key ID DD3766FF
gpg: Good signature from "Stephen Robert Guglielmo <srg@guglielmo.us>"
gpg: aka "Stephen Robert Guglielmo <srguglielmo@gmail.com>"
Primary key fingerprint: 0D54 BE6A B832 8701 AA94 9036 2D15 C7B0 DD37 66FF
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date: Tue Jul 1 12:07:04 2014 -0400

Update README with new links

3.1.3.3. commit 6bccfd68c6e3dbcle447626a009c47fccf1440dd

Merge: a014f72 f0ae850
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date: Tue Jul 1 12:02:25 2014 -0400

Merge pull request #14 from pdinc-oss/audit-pyperon-2014-06-15

Audit info by Jason

3.1.3.4. commit f0ae85017fec4f318b84d055685187f06bf71312

gpg: Signature made Thu, Jun 26, 2014 16:15:15 EDT using RSA key ID DA0848AD
gpg: Good signature from "Jason Pyeron <jpyeron@pdinc.us>"
Author: Jason Pyeron <jpyeron@pdinc.us>
Date: Mon Jun 23 10:06:58 2014 -0400

audit of ac812aa395583b37dfca3f921c36385e744eb121 by Pyeron, Jason

3.1.3.5. commit a014f721c87d870613e9b1cc99d2d2c435cf3054

gpg: Signature made Tue, Jul 01, 2014 11:53:10 EDT using RSA key ID DD3766FF
gpg: Good signature from "Stephen Robert Guglielmo <srg@guglielmo.us>"
gpg: aka "Stephen Robert Guglielmo <srguglielmo@gmail.com>"
Primary key fingerprint: 0D54 BE6A B832 8701 AA94 9036 2D15 C7B0 DD37 66FF
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date: Tue Jul 1 11:53:03 2014 -0400

Fix string length

3.1.3.6. commit d60fc07272295fc57c2fac7c50911f74177a89c7

gpg: Signature made Mon, Jun 30, 2014 10:05:18 EDT using RSA key ID DD3766FF
gpg: Good signature from "Stephen Robert Guglielmo <srg@guglielmo.us>"
gpg: aka "Stephen Robert Guglielmo <srguglielmo@gmail.com>"
Primary key fingerprint: 0D54 BE6A B832 8701 AA94 9036 2D15 C7B0 DD37 66FF
Merge: 8d7bf49 1ca13ed
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date: Mon Jun 30 10:04:58 2014 -0400

Merge of 1ca13ed2271d60ba93d40bcc8db17ced8545f172 branch - rebranding

3.1.3.7. commit 8d7bf49c3adb639358e30a6be794f661655f5929

gpg: Signature made Mon, Jun 30, 2014 10:04:58 EDT using RSA key ID DD3766FF
gpg: Good signature from "Stephen Robert Guglielmo <srg@guglielmo.us>"
gpg: aka "Stephen Robert Guglielmo <srguglielmo@gmail.com>"
Primary key fingerprint: 0D54 BE6A B832 8701 AA94 9036 2D15 C7B0 DD37 66FF
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date: Mon Jun 23 09:45:27 2014 -0400

Minor URL updates

(cherry picked from commit 1ca13ed2271d60ba93d40bcc8db17ced8545f172)

3.1.3.8. commit 1ca13ed2271d60ba93d40bcc8db17ced8545f172

gpg: Signature made Mon, Jun 23, 2014 9:45:47 EDT using RSA key ID DD3766FF
gpg: Good signature from "Stephen Robert Guglielmo <srg@guglielmo.us>"

gpg: aka "Stephen Robert Guglielmo <srguglielmo@gmail.com>"
Primary key fingerprint: 0D54 BE6A B832 8701 AA94 9036 2D15 C7B0 DD37 66FF
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date: Mon Jun 23 09:45:27 2014 -0400

Minor URL updates

3.1.3.9. 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>"
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.

3.1.3.10. commit 71d4dc4f609d78f14fd264159d75081fe98d2ec2

gpg: Signature made Sat, Jun 14, 2014 13:47:42 EDT using RSA key ID DD3766FF
gpg: Good signature from "Stephen Robert Guglielmo <srg@guglielmo.us>"
gpg: aka "Stephen Robert Guglielmo <srguglielmo@gmail.com>"
Primary key fingerprint: 0D54 BE6A B832 8701 AA94 9036 2D15 C7B0 DD37 66FF
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date: Sat Jun 14 13:47:35 2014 -0400

Removed the HTML license. Rebranded a few files. Modified Readme.txt.

3.1.3.11. 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>"
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.

3.1.3.12. commit bdba05dd344762d2cbc9a9cbc874e82083a42974

gpg: Signature made Mon, Jun 30, 2014 10:02:08 EDT using RSA key ID DD3766FF
gpg: Good signature from "Stephen Robert Guglielmo <srg@guglielmo.us>"
gpg: aka "Stephen Robert Guglielmo <srguglielmo@gmail.com>"
Primary key fingerprint: 0D54 BE6A B832 8701 AA94 9036 2D15 C7B0 DD37 66FF
Author: Stephen R Guglielmo <srg@guglielmo.us>
Date: Sat Jun 14 13:47:35 2014 -0400

Removed the HTML license. Rebranded a few files. Modified Readme.txt.

(cherry picked from commit 71d4dc4f609d78f14fd264159d75081fe98d2ec2)

Conflicts:
src/License.html

3.1.3.13. commit d3c8039a50f9ec5a1278459df94d3ccc312050db

gpg: Signature made Sat, Jun 28, 2014 4:45:24 EDT using RSA key ID DA0848AD
gpg: Good signature from "Jason Pyeron <jpyeron@pdinc.us>"
Author: Jason Pyeron <jpyeron@pdinc.us>
Date: Sat Jun 28 04:44:55 2014 -0400

oops, should have moved this with the source (src).

3.1.3.14. 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

3.1.3.15. commit 0aac64ceaa6c606b46af36510fbf507c80b8f708

gpg: Signature made Mon, Dec 08, 2014 23:10:53 EST using RSA key ID DA0848AD
gpg: Good signature from "Jason Pyeron <jpyeron@pdinc.us>"
Author: Jason Pyeron <jpyeron@pdinc.us>
Date: Sun Aug 17 00:10:04 2014 -0400

audit of 88d24b9bcd5c83b4a0afd3d5baa47f224f901653

3.1.3.16. commit ae8fff30f5d9083380c96e550cfe568a7fa22707

gpg: Signature made Tue, Dec 09, 2014 12:08:03 EST using RSA key ID DA0848AD
gpg: Good signature from "Jason Pyeron <jpyeron@pdinc.us>"
Author: Jason Pyeron <jpyeron@pdinc.us>
Date: Tue Dec 9 12:07:34 2014 -0500

replace Microsoft Word format with signed portable document format (PDF)

3.2. Commit analysis

The merge commit [3.1.3.1] is not signed, but [3.1.3.2] is and the diff confirms it is the only change since [3.1.3.3].

The merge commit [3.1.3.3] is not signed, but the two parent commits [3.1.3.4] and [3.1.3.5] are. A git show on [3.1.3.3] confirms that all changes are part of either parent commit and no independent changes were introduced with the merge.

The parent of [3.1.3.4] is the signed commit [3.1.3.9] covered by a previous audit in commit [3.1.3.15].

The parent of [3.1.3.5] is the signed commit [3.1.3.6].

The signed merge commit [3.1.3.6] is a fix using cherry picks [3.1.3.7] to replace [3.1.3.8].

The series, ending with commit [3.1.3.8], of same author commits has an ultimate parent of [3.1.3.10], whose parent is [3.1.3.11].

Commit [3.1.3.11] traces back with same author signed commits, to the same commit [3.1.3.9] covered by a previous audit in commit [3.1.3.15].

The series, ending with commit [3.1.3.7], of same author cherry pick commits has an ultimate parent of [3.1.3.12], whose parent is [3.1.3.13].

The parent of [3.1.3.13] is [3.1.3.14], which is subject of a previous audit in commit [3.1.3.15].

The commit [3.1.3.9] is a parent of [3.1.3.14].

3.2.1. Authors

3.2.1.1. Mr. Caron St-Pierre - 6f47efcala4070e0745f8fb8b80cf3c405a8f4dc
3.2.1.2. Mr. Guglielmo - ac812aa395583b37dfca3f921c36385e744eb121
3.2.1.3. Mr. Horrocks - a03e565835e3ff66774a2a50946dc2290bcbc7d4
3.2.1.4. Mr. Pyeron - b188dc60742eaalc23e455b1eb64361e23d855fc

3.2.2. Status

Given the woven signed and unsigned commits of more than 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. The status of this audit is based on the information included in the previous audit included in commits [3.1.3.15] / [3.1.3.16].

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

4.2.1. d3c8039a50f9ec5a1278459df94d3cccc312050db - oops, should have moved this with the source (src).
4.2.2. b60070f4d0879e277f44d174a163bbb292325fea - removed history branch files.
4.2.3. f0ae85017fec4f318b84d055685187f06bf71312 - audit of ac812aa395583b37dfca3f921c36385e744eb121 by Pyeron, Jason
4.2.4. 88d24b9bcd5c83b4a0afd3d5baa47f224f901653 - Migration back to master branch - Merge remote-tracking branch ...
4.2.5. 4281c4d2e38383ce9327aa63f86fdea7188669e1 - * Remove pkcs11 reference in .gitignore * Add include on pkcs11 ...
4.2.6. 382b08a62dc9babe0c4a27150cfca7a545dfdc65 - Stephen Guglielmo's identification
4.2.7. 65efd37fd5a0513d7fb675028c7a911a5340948c - Merge branch 'master-with-history' into ciphershed-history-merge
4.2.8. cf7b33db41230b77ea8096c23e604dbc62ce7227 - move source files to src directory
4.2.9. b188dc60742eaalc23e455b1eb64361e23d855fc - Jason Pyeron's Contributor License Agreement & identification

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.

As part of the change sets reviewed it was clear that almost every source file was modified in some fashion. 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. If this audit were to perform functional testing, it is reasonable to assume the program would fail to perform for upgrades based on the automated license compliance changes.

It is clear that the changes made were in an effort to comply with the license set forth by the previous maintainers of TrueCrypt. All other changes were of a documentation nature.

It is the conclusion of this audit that the source code has no newly introduced risks since the last audit on commit 88d24b9bcd5c83b4a0afd3d5baa47f224f901653 (see: 3.1.3.16 & 6.1.1).

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

6. Appendix

6.1. References

6.1.1. Audit on 88d24b9: <https://github.com/pdinc-oss/CipherShed/blob/audit-pyeron-88d24b9/doc/trust/audits/p/y/pyeron%2Cjason/audit-report-2014-08-16-88d24b9bcd5c83b4a0afd3d5baa47f224f901653.pdf>

6.2. Colophon

6.2.1. git version 2.1.1 was used on Cygwin.

6.2.2. Microsoft Word 2003 and Adobe Acrobat 8 Professional were used to produce this report.

6.2.3. The commit tree was created by: `git log --pretty=format:"%H" -graph`

6.2.4. The developer conflict of interest was created by:
`git log --pretty=format:"%H%x09%ae%x09%ce%x09%s" |\`
`grep jpyeron@pdinc.us |\`
`sed 's/\t[-a-z@\.]\+\t[-a-z@\.]\+\t/ - /'`

6.2.5. Finding a unique set of authors/committers:
`cat /tmp/commits.txt |\`
`while read line; \`
`do git log -1 --pretty=format:"%H%x09%ae%x09%ce%x0a" $line; \`
`done |\`
`sed 's/^[0-9a-f]\+\t\(.*)\t\(.*)/1\n2/' |\`
`sort -u`

6.3. Commit Index

0d0c212	7	88d24b9	1, 7, 9, 10, 12, 13
0d4799c	7	8d7bf49	7, 8
131ed5a	7	91c0cd1	7
164eb7e	7	9aae798	7
188850b	7	a014f72	6, 7, 8
19de3ee	7	a03e565	7, 10
1b84ec	7	a0c84ff	7
1bece0c	7	a79e05a	7
1ca13ed	7, 8, 9	ac812aa	7, 8, 9, 10
2e3598d	7	b188dc6	7, 10, 11
2e97568	7	b50a2fb	7
344df5d	6, 7, 8	b5adb3e	7, 9
382b08a	7, 11	b60070f	7, 10
3950ecd	8	bdba05d	7, 9
3b350b9	7	c2728a4	7
4054940	7	c2dc7ff	7
4281c4d	7, 9, 10	c9a2bb7	7
49ecdfe	7	ca2f5d9	7
574dc0e	7	cf7b33d	7, 11
5e56915	7	d3c8039	7, 9, 10
5fda89e	7	d60fc07	7, 8
61ea96d	7	d7eeb3f	7
623f0c1	7	d8587c4	7
65efd37	7, 11	de40b68	7
6bccfd6	7, 8	e362af0	7
6f47efc	7, 10	e6db9b8	7
702dfef	7	e8529e9	1, 6, 7, 8
71d4dc4	7, 9	ee579ea	7
71ff2b0	7	ef3bfd9	7
756cddd	8	ef66ace	7, 9
806630e	7	f0ae850	6, 7, 8, 10