# Table of Contents

## Introduction

- Example 1

## Overview

- Example 2
- Example 3

## Product Information and Description

## Special Features

## Target Customers

## Law Enforcement Applications

## Evaluation and Testing of TrueCrypt

- Example 4
- Example 5

## Installation of TrueCrypt

## Configuration of TrueCrypt

- Example 6
- Example 7

## Conclusion

- Example 8
Introduction

The National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTCoE) has been assigned the responsibility of conducting electronic crime and digital evidence tool, technology and training testing and evaluations in support of the NIJ research, development, testing and evaluation (RDT&E) process.

The NIJ RDT&E process helps ensure that NIJ's research portfolios are aligned to best address the technology needs of the criminal justice community. This rigorous process has five phases:

- **Phase I: Determine technology needs, principally in partnership with the Law Enforcement and Corrections Technology Advisory Council (LECTAC) and the appropriate Technology Working Group (TWG).** NIJ identifies criminal justice practitioners’ functional requirements for new tools and technologies. (For more information on LECTAC and the TWGs, visit http://www.justnet.org/.)

- **Phase II: Develop technology program plans to address those needs.** NIJ creates a multi-year research program to address the needs identified in Phase I. One of the first steps is to determine whether products that meet those needs currently exist or whether they must be developed. If a solution is already available, Phases II and III are not necessary and NIJ moves directly to demonstration, testing and evaluation in Phase IV. If solutions do not currently exist, they are solicited through annual, competitively awarded science and technology solicitations and TWG members help review the applications.

- **Phase III: Develop solutions.** Appropriate solicitations are developed and grantees are selected through an open, competitive, peer-reviewed process. After grants are awarded, the grantee and the NIJ program manager then work collaboratively to develop solutions.

- **Phase IV: Demonstrate, test, evaluate and adopt potential solutions into practice.** A potential solution is tested to determine how well it addresses the intended functional requirement. NIJ then works with first-adopting agencies to facilitate the introduction of the solution into practice. During the testing and evaluation process, performance standards and guides are developed (as appropriate) to ensure safety and effectiveness; not all new solutions will require the publication of new standards or guides. After adoption, the solution’s impact on practice is evaluated.

- **Phase V: Build capacity and conduct outreach to ensure that the new tool or technology benefits practitioners.** NIJ publishes guides and standards and provides technology assistance to second adopters.¹

NIJ's High-Priority Criminal Justice Technology Needs are organized into five functional areas:

- Protecting the Public.
- Ensuring Officer Safety.
- Confirming the Guilty and Protecting the Innocent.
- Improving the Efficiency of Justice.
- Enabling Informed Decision-Making

These NIJ ECTCoE tool, technology and training evaluation and testing reports support the NIJ RDT&E process, which addresses high-priority needs for criminal justice technology.

Overview

Encryption is the practice of concealing information using a protective algorithm and a key. This enables only those entities with knowledge of the algorithm and the key to read protected information. In law enforcement settings, encryption can be used to secure information such as electronic evidence. Encryption can also enable law enforcement to transmit evidence by means that may not be secure, such as the Internet.

Encryption can also be used to conceal potential evidence from law enforcement. An understanding of how encryption software behaves will benefit law enforcement by enabling an agent to identify when encryption is being used and how to circumvent encryption protection schemes to successfully obtain evidence for processing cases.

There are many tools for performing encryption on a computer. One popular tool for performing encryption is TrueCrypt.

Product Information and Description

The following is taken from TrueCrypt’s documentation, located on its website:

“TrueCrypt is free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X and Linux.

TrueCrypt is a software system for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted or decrypted right before it is loaded or saved, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. Entire file system is encrypted (e.g., file names, folder names, contents of every file, free space, meta data, etc).

“Files can be copied to and from a mounted TrueCrypt volume just like they are copied to/from any normal disk (for example, by simple drag-and-drop operations). Files are automatically being decrypted on the fly (in memory/Random Access Memory, or RAM) while they are being read or copied from an encrypted TrueCrypt volume. Similarly, files that are being written or copied to the TrueCrypt volume are automatically being encrypted on the fly (right before they are written to the disk) in RAM. Note that this does not mean that the whole file that is to be encrypted/decrypted must be stored in RAM before it can be encrypted/decrypted. There are no extra memory (RAM) requirements for TrueCrypt. For an illustration of how this is accomplished, see the following paragraph.

“Let’s suppose that there is an .avi video file stored on a TrueCrypt volume (therefore, the video file is entirely encrypted). The user provides the correct password (and/or keyfile) and mounts (opens) the TrueCrypt volume. When the user double clicks the icon of the video file, the operating system launches the application associated with the file type – typically a media player. The media player then begins loading a small initial portion of the video file from the TrueCrypt-encrypted volume to RAM (memory) in order to play it. While the portion is being loaded, TrueCrypt is automatically decrypting it (in RAM). The decrypted portion of the video (stored in RAM) is then played by the media player. While this portion is being played, the media player begins loading the next small portion of the video file from

2http://www.TrueCrypt.org/
the TrueCrypt-encrypted volume to RAM (memory) and the process repeats. This process is called on-the-fly encryption/decryption and it works for all file types, not only for video files.

“Note that TrueCrypt never saves any decrypted data to a disk – it only stores them temporarily in RAM (memory). Even when the volume is mounted, data stored in the volume is still encrypted. When you restart Windows or turn off your computer, the volume will be dismounted and files stored in it will be inaccessible (and encrypted). Even when power supply is suddenly interrupted (without proper system shut down), files stored in the volume are inaccessible (and encrypted). To make them accessible again, you have to mount the volume (and provide the correct password and/or keyfile).”

Special Features
The following is a partial list of features from TrueCrypt’s website:

- Creates a virtual encrypted disk within a file and mounts it as a real disk.
- Encrypts an entire partition or storage device such as USB flash drive or hard drive.
- Encrypts a partition or drive where Windows is installed (pre-boot authentication).

Note the TrueCrypt program has many other features in addition to those mentioned. These three features are the most likely to be used by state and local law enforcement officers and agencies and are the focus of this test and evaluation.

Target Customers
The target customers for the TrueCrypt software can be any computer user, including state and local law enforcement organizations, who desires to have data safeguarded by encryption.

Law Enforcement Applications
TrueCrypt can be used by state and local law enforcement in order to protect data’s confidentiality. Information for cases can be encrypted and shipped in a secure manner. Furthermore, it is important for state and local law enforcement with an interest in digital forensics to understand the nature of encryption, including steps that may be taken to ease processing of cases that may involve encryption.
Evaluation and Testing of TrueCrypt

The use of the TrueCrypt program falls into two basic categories. One is the encrypting of data and the second is hiding the presence of encrypted data (encrypted data with encrypted data). The testing and evaluation in this document focuses on data encryption and not on the hiding of encrypted data.

Installation of TrueCrypt

The TrueCrypt program can be run by installing the program on a computer or in stand-alone mode from a folder or removable media. The testing and evaluation process in this document was performed after installing the program on the test computer. Below is the TrueCrypt option menu presented at the beginning of the setup routine.

Configuration of TrueCrypt

The computer used for testing is a computer that is used on a daily basis and has several programs installed. Using this system for testing the TrueCrypt program will mimic an expectant environment for the use of the TrueCrypt program. Below are the details about the computer used for testing.

1. Test Computer Details:
   1.1. Dell Inspiron laptop PC.
   1.2. Model number: E1405.

2. Test Hard Drive Details
   2.1. Hitachi Travelstar 80GB hard drive.
   2.2. Model number: HTS541080G9SA00.
   2.3. Serial number: TH-0PC939-12567-69M-G0WH.
   2.4. Manufacture Date: SEPT 2006.

3. Test Operating System Details
   3.2. Service Pack 3 installed with all current updates.

4. Test Computer Installed Programs
   4.2. AT&T Communication Manager (air card services).
   4.3. Avast Free Anti Virus (current virus definitions installed).
   4.4. Canon iP100 Printer.
   4.5. Cell Phone Analyzer.
   4.6. CPA SIM Analyzer.
   4.7. Cryptomax CleanUSB.
   4.8. Datalifter v2.0.
   4.10. Google Earth.
   4.11. HelpScribble.
   4.12. HTML Workshop.
   4.15. Norton Ghost.
4.18. Ring Central.
4.22. TrueCrypt.
4.24. US-LATT.
4.25. WinRAR.
4.26. WinZIP.
4.27. WS_FTP.

5. Netgear ReadyNAS NV+
5.5. The computer has access to this network storage system.

Test 1 – Virtual Encrypted Disk

The purpose of this test was to evaluate the advertised feature that TrueCrypt creates a virtual encrypted disk within a file and mounts it as a real disk. It also tested whether a password for a TrueCrypt volume can be recovered from the RAM of a running system. Once TrueCrypt was installed and executed, the following steps were performed:

1. Chose the “Create an encrypted file container” option from the Wizard menu.

![TrueCrypt Volume Creation Wizard](image)

2. Chose path and filename for the file container to be “C:\TestOne”.

3. Chose the default encryption scheme, AES. The image below shows other available encryption schemes. AES was chosen for this test due to its acceptance by the U.S. government.

![Encryption Algorithm](image)

4. Chose to create a 5 MB file container for encryption. Note: There was 7.32 GB of free space on the hard drive in the test computer so a much larger file container could have been created.

![Volume Size](image)

5. Chose the password “OneAdam12” (without the quotation marks). TrueCrypt noted this was not a strong password; however, for testing purposes it was acceptable. Note that this is a character string that had not been used on this computer previously.

![Volume Password](image)

6. Chose NTFS as the file system for the file container.
7. After completion, created a 5MB file named “TestOne” in the root of “C:\”.

8. Inspection of the data in the file named “TestOne” revealed what appeared to be random data. The first 512 bytes are shown below using WinHex v13.5 SR-3.

9. Using TrueCrypt to open the file container allowed for the selection of drive letters for the decrypted volume. Volume “R:” was chosen in this test. Clicking “Select File” allowed navigation to the file named “C:\TestOne.” Once the “TestOne” file was selected, the “Mount” button was clicked.

10. The mount process requested the password for the file container.

11. Note that prior to mounting the TrueCrypt file container, the computer folder tree is shown below.

12. After mounting the TrueCrypt file container, the computer folder tree is shown below; now with the newly added “Local Disk (R:)”. From this point on data (files and/or folders) could be added to “Local Disk (R:)”. 
13. “Local Disk (R:)” was available until dismounted using the TrueCrypt Program or by shutting down the computer.

At this point testing of the TrueCrypt virtual disk encryption was completed. Additional steps were performed to determine if the TrueCrypt password could be located in volatile memory (RAM) before the computer was shut down.

Prior to the computer’s being turned off, the RAM memory was acquired (memory dump) using the USLATT tool and examined to determine if it contained the character string “OneAdam12”. The character string “oneadam12” (all lowercase) was found multiple times in the memory dump data. Note that the TrueCrypt documentation discusses the issue of passwords being stored in volatile memory, an issue that can exist with all programs. The following is from the TrueCrypt documentation discussing memory dump files:

“Most operating systems, including Windows, can be configured to write debugging information and contents of the system memory to so-called memory dump files (also called crash dump files) when an error occurs (system crash, “blue screen,” bug check). Therefore, memory dump files may contain sensitive data. TrueCrypt cannot prevent cached passwords, encryption keys, and the contents of sensitive files opened in RAM from being saved unencrypted to memory dump files. Note that when you open a file stored on a TrueCrypt volume, for example, in a text editor, then the content of the file is stored unencrypted in RAM (and it may remain unencrypted in RAM until the computer is turned off). Also note that when a TrueCrypt volume is mounted, its master key is stored unencrypted in RAM. Therefore, you must disable memory dump file generation on your computer at least for each session during which you work with any sensitive data and during which you mount a TrueCrypt volume. To do so in Windows XP or later, right-click the ‘Computer’ (or ‘My Computer’) icon on the desktop or in the Start Menu, and then select Properties > (on Windows Vista or later: > Advanced System Settings >) Advanced tab > section Startup and Recovery >Settings > section Write debugging information > select (none) > OK.

“TrueCrypt cannot and does not ensure that RAM contains no sensitive data (e.g. passwords, master keys, or decrypted data). Therefore, after each session in which you work with a TrueCrypt volume or in which an encrypted operating system is running, you must shut down (or, if the hibernation file is encrypted, hibernate) the computer and then leave it powered off for at least several minutes (the longer, the better) before turning it on again. This is required to clear the RAM.”

14. The Windows Explorer program was used to cut and paste the file container to a folder on the connected network attached storage (NAS) device. TrueCrypt was then configured to use Volume “N:” for mounting the file container (now located on the NAS). The result was the creation of local “Local Disk (N:)”.

15. The file container was dismounted and a USB stick was attached to the computer, at which time it was assigned local volume “F:” and had the volume label “M-DRIVE.” Windows Explorer program was used to “cut and paste” the file container from the NAS to the USB stick. TrueCrypt was then configured to use drive letter “L:” for mounting the file container (now located on the USB stick). The result was the creation of “Local Disk (L:)”.

4http://www.TrueCrypt.org/docs/
This feature performed as advertised. In order to gain access to the encrypted file container regardless of its location (local, on a network or on removable media), the assigned password is required to decrypt the data within the file container. As it is with all password protected systems, security is determined by the strength of the password (length and type of characters) and the secrecy of the password (unknown to unauthorized personal and not easily discernable).

Certainly the presence of the TrueCrypt program on a computer can indicate a likeliness of the presence of a TrueCrypt file container; however, determining the location of a TrueCrypt container can depend on the file name assigned to file container and its location within the folder system. Note that assigning the filename extension ".tc" automatically associates a file container with the TrueCrypt program, which could be used to discover TrueCrypt file containers.

According to the program documentation, there is no back door into an encrypted file container. There is a process outlined in the documentation that allows for the backing up of the initial (master) password and then allowing a change of password. If the changed-to password is forgotten, the volume password can be reset to the initial (master) password. However, that initial password must be remembered, otherwise no access is gained.

Test 2 – Entire Partition or Storage Device Encryption

The purpose of this test was to evaluate the advertised feature that TrueCrypt encrypts an entire partition or storage device such as a USB flash drive or hard drive. It also tested whether a password for a TrueCrypt volume can be recovered from the RAM of a running system. Once TrueCrypt was installed and executed, the following steps were performed:

1. WinHex version 13.5 SR-3 was used to write “00h” to every byte on the USB stick to ensure that no previous data was contained thereon.
2. WinHex was then used to calculate a 64-bit checksum after wipe. The result is shown below.

![Checksum](image)

3. Chose the Wizard menu option to encrypt a non-system partition/drive.

![Volume Type](image)

4. Chose to create a standard TrueCrypt volume. As mentioned at the beginning of this document, the focus of testing covered in this document is on data encryption rather than hiding encrypted data.

![Volume Creation Mode](image)
5. Chose the device “\Device\Hardisk\Partition1.” Note that the USB stick had been assigned the drive letter “F:” automatically by the computer on insertion.

6. Chose to create an encrypted volume.

7. Chose the default encryption scheme, AES. The image below shows other available encryption schemes. AES was chosen for this test due to its acceptance by the U.S. government.

8. The volume size was non-changeable because there was only one partition on the USB stick.

9. Chose the password “TwoXBOX14” (without the quotation marks). TrueCrypt noted this was not a strong password; however, for testing purposes it was acceptable. Note that this is a character string that had not been used on this computer previously.

10. Chose NTFS as the file system for the file container.

11. After completion, the computer displayed the following message. This message indicates that when the USB stick is inserted into the computer and assigned a drive letter, then TrueCrypt will assign a different drive letter to the mounted file container.
12. The USB stick was removed from the computer and re-inserted, at which time it was assigned the drive letter “F:”.

![My Computer with USB stick](image)

13. Attempting to use Windows Explorer to open the USB stick (F:) resulted in the message shown below. As a side note, choosing ‘Yes’ to format the USB stick at this point removes the TrueCrypt partition.

![Disk is not formatted](image)

14. Before mounting the file container with TrueCrypt, WinHex was used to open the physical media of the USB stick to view the data on the USB stick. Noted was the absence of a valid partition table and all of the data on the USB stick appeared to contain random hex values. (Recall that all of the bytes on the USB stick were written “00h” prior to the TrueCrypt creating the encrypted partition.

15. TrueCrypt was used to open the partition it identified as “Drive F:” and the drive letter “L:” was chosen as the drive letter to use when mounting the encrypted partition.

![Disk encryption status](image)

16. The mount process requested the password for the partition.

![Password request](image)

17. The computer drive structure then reported both drives “Removable Disk (F:)” and “Local Disk (L:)”.

![My Computer with drives](image)

18. After the partition was mounted with TrueCrypt, WinHex was used to open the physical media (drive “F:”) and the result was the same as encountered above: the absence of a valid partition table and all of the data on the USB stick appeared to contain random hex values.

19. WinHex was then used to open the logical volume that TrueCrypt created when mounting the partition “L:” and that volume contained the expected characteristics of a valid volume. It was noted that
1. The free space of “Local Disk (L:)” contained what appeared to be random hex values rather than the “00h” that was written to the USB stick prior to the TrueCrypt program’s being used to create the encrypted partition.

20. A command prompt was opened and the MS-DOS internal command “COPY CON” was used to create and save a text file in the root of “Local Disk (L:)”. The text file contained the character string “This_is_test_data” (without the quotation marks) and saved to a file named “TESTDATA.TXT.”

21. The TrueCrypt program was then used to dismount volume “L:” at which time the logical mapping was removed, leaving only drive “Removable Disk (F:)”.

22. WinHex was used to open the physical media (USB stick) that displayed all of the data on the USB stick, which appeared to be random hex values. A sector-level search was conducted for the character string “This_is_test_data.” The character string was not found.

23. The TrueCrypt program was then used to mount the partition on the USB stick to volume “L:”. WinHex was then used to conduct a search for the character string “This_is_test_data”. The character string was found in the data.

24. After the previous step and prior to the computer’s being turned off, the RAM memory was acquired (memory dump) using the USLATT tool and then examined to determine if it contained the character string “TwoXBOX14.” The character string “TwoXBOX14” was found multiple times in the memory dump data. This is the same issue pointed out in the above-mentioned Test One.

25. TrueCrypt was used to dismount the partition and the USB stick was removed from the computer. Note that the encrypted partition on the USB stick still contained the file TESTDATA.TXT located in the root folder.

The USB stick was then re-inserted into the computer. Before allowing TrueCrypt to mount the encrypted partition, the USB stick was “quick formatted” (write a new partition table and File Allocation Table but not overwrite the data area) in order for the operating system (Windows Explorer) to read the USB stick.

WinHex was then used to open the physical media (USB stick) and a search (without capitalization sensitive) for the character string “This_is_test_data” was conducted. The character string was not found. An additional search for just the character string “This_” produced the same negative result.

The partition and storage device encryption performed as advertised. In order to gain access to the encrypted partition on the USB stick, the assigned password is required.

In this case, if only the USB stick was examined, then it reports itself as an unformatted USB stick and no partition table or boot record are present. Further examination of the physical data reveals the USB stick...
filled with what appears to be random hex values. No specific data was present to indicate the use of the TrueCrypt program.

Without any pre-knowledge that the TrueCrypt program was used for this USB stick and attempting to use TrueCrypt without an incorrect password resulted in the message shown below. The same message appears when attempting to use TrueCrypt to mount a partition that has not been encrypted by TrueCrypt.

These two conditions, without prior knowledge of the use of the TrueCrypt program, make it quite difficult to determine what program wrote the data to the disk and any encrypted data within.

As mentioned in Test One, if it is known that the TrueCrypt program was used but the password is not known, then the access to the data will depend on the complexity and security of the password.

**Test 3 – TrueCrypt’s Pre-Boot Authentication**

The purpose of this test was to evaluate the advertised feature that TrueCrypt encrypts a partition or drive where Windows is installed (pre-boot authentication). It also tested whether a password for a TrueCrypt volume can be recovered from the RAM of a running system and the difficulty of removing the encryption from a boot device.

Note that the laptop computer on which this test is being performed contains a single hard drive (described at the beginning of this document) and that hard drive contains extended partitions (see below).

The operating system on this computer is Windows XP. TrueCrypt reported that it cannot encrypt the extended partitions, but only the partition from which Windows boots. Note: This reportedly is not the case with Windows 7. Therefore, in this test only volume “C:” was encrypted.

Once TrueCrypt was installed and executed the following steps were performed:

1. Run TrueCrypt from the Start menu and chose to create a new volume.
2. Chose to Encrypt an entire system drive.
3. Chose to create a normal type of encryption.
4. Chose the device "\Device\Hardisk\Partition1."

Area to Encrypt

- **Encrypt the Windows system partition**
  Select this option to encrypt the partition where the currently running Windows operating system is installed.

- **Encrypt the whole drive**
  Select this option if you want to encrypt the entire drive on which the currently running Windows system is installed. The whole drive, including all its partitions, will be encrypted except the first track where the TrueCrypt Boot Loader will reside. Anyone who wants to access a system installed on the drive, or files stored on the drive, will need to enter the correct password each time before the system starts. This option cannot be used to encrypt a secondary or external drive if Windows is not installed on it and does not boot from it.

5. Chose the single-boot option because it pertains to this particular computer.

Number of Operating Systems

- **Single-boot**
  Select this option if there is only one operating system installed on this computer (even if it has multiple users).

- **Multi-boot**
  Select this option if there are two or more operating systems installed on this computer.

  - Windows XP and Windows XP
  - Windows XP and Windows Vista
  - Windows and Mac OS X
  - Windows and Linux
  - Windows, Linux and Mac OS X

6. Chose the default encryption scheme, AES. The image below shows other available encryption schemes. AES was chosen for this test due to its acceptance by the U.S. government.

<table>
<thead>
<tr>
<th>Encryption Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
</tr>
<tr>
<td>AES</td>
</tr>
<tr>
<td>Serpent</td>
</tr>
<tr>
<td>Twofish</td>
</tr>
<tr>
<td>AES-Twofish</td>
</tr>
<tr>
<td>AES-Twofish-Serpent</td>
</tr>
<tr>
<td>Serpent-AES</td>
</tr>
<tr>
<td>Serpent-Twofish-AES</td>
</tr>
<tr>
<td>Twofish-Serpent</td>
</tr>
</tbody>
</table>

7. Chose the password “ThreeBY16” (without the quotation marks). TrueCrypt noted this was not a strong password; however, for testing purposes it was acceptable. Note that this is a character string that has not been used on this computer in the past.

8. A rescue disk in the form of a ISO file was created during this process. The ISO file was sent to a USB stick and the ISO file was then burned to a CD. The CD was then required to be placed into the computer's CD drive to confirm the creation of the rescue disk before the user’s being allowed to proceed.

<table>
<thead>
<tr>
<th>Rescue Disk Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>The TrueCrypt Rescue Disk has been successfully verified. Please remove it from the drive now and store it in a safe place.</td>
</tr>
<tr>
<td>Click Next to continue.</td>
</tr>
</tbody>
</table>

9. After the disk in the CD drive was examined, the following message appeared. The “Encrypt” button was pressed and the process of encrypting the drive started. On this particular computer it took approximately 65 minutes to complete the process.
10. After the encryption process finished, the computer was rebooted and the following message appeared. Note that an incorrect password was intentionally entered and that resulted in a message that the password was incorrect. Entering the correct password allowed the Windows operating system to boot as normal.

At this point, testing of the TrueCrypt pre-boot authentication was completed. Additional steps were performed to determine if the TrueCrypt password could be located in volatile memory (RAM) before the computer was shut down.

11. After the computer was booted and prior to shutting the computer down, the RAM memory was acquired (memory dump) using USLATT and examined to determine if it contained the character string “ThreeBY16”. The character string “ThreeBY16” was not found in this test. Although the password was not located in memory during this test, caution should be urged since previous tests found the password in memory.

Even though the USLATT tool did not locate the pre-boot password, it did report the following programs as running:

1. The process “C:\Program Files\TrueCrypt\TrueCrypt.exe”.
2. The service “\SystemRoot\System32\drivers\TrueCrypt.sys”.
3. Installed application “TrueCrypt 7.0a”.

12. A command prompt was opened and the MS-DOS internal command “COPY CON” was used to create and save a text file to the root of “C:\.” The text file contained the character string “This_is_test_data.” (without the quotation marks) and saved to a file named TESTDATA.TXT.

13. A computer was shut down and the hard drive removed. With a Tableau write blocker, EnCase 4.22a was used to acquire a forensic image of the physical hard drive.

14. Using EnCase to examine the first sector (512 bytes) of the hard drive did not reveal a normally expected boot record; however, the first 521 bytes of the hard drive indicated the presence of a TrueCrypt boot loader.
15. The EnCase program was then used to examine the data associated with encrypted partition and it was reported as all Unallocated Clusters.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Logical Size</th>
<th>Physical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unallocated Clusters</td>
<td>File, Unallocated Clusters</td>
<td>55,013,172,640</td>
<td>55,013,172,640</td>
</tr>
</tbody>
</table>

16. Used EnCase to search (without capitalization sensitive) the entire image of the hard drive for the character string “This_is_test_data” (without the quotation marks). The character string was not found.

17. EnCase was then used to search (without capitalization sensitive) for a smaller portion of the character string by searching only for “This_is_” (without the quotation marks). The character string was not found.

18. The EnCase program was used to search (without capitalization sensitive) the entire image of the hard drive for the character string “ThreeBY16” (without the quotation marks). The character string was not found.

The following additional steps were performed to determine the ease of removal of TrueCrypt encryption from the boot partition.

19. Followed the instructions shown below provided in the TrueCrypt documentation.

After the “permanent decryption” process was finished, the computer was back to its normal boot processing; no boot password was requested. The computer simply booted as though encryption had not been previously installed.

This feature performed as advertised. In order to gain access to the encrypted boot partition on the hard drive, the assigned password is required. If the password is not known or forgotten the only way to access the data on the hard drive is to locate the TrueCrypt Rescue Disk created when the data was initially encrypted.

Attempting to look at the data post mortem (meaning the system not booted with the TrueCrypt boot loader) resulted in no user files or data being readable.
Conclusion

The tested features of the TrueCrypt software performed as advertised. TrueCrypt would enable law enforcement to protect sensitive data that may be exposed to eavesdropping. There is extensive documentation for the TrueCrypt program that is easily understandable and Wizards that enable easy configuration of desired features. Once TrueCrypt encrypts the data, access is all but impossible provided that a strong password is chosen. There are methods for circumventing some of the encryption, as demonstrated in discovering the password in RAM of a live running system. In a law enforcement application, the cost of this program ($0) is quite inviting given that it provides similar results to competing programs that are commercially sold.

For digital forensics examination, to determine the presence of a TrueCrypt program the following methods may be useful:

- If the computer has been booted with the TrueCrypt boot loader then a memory dump can identify the active TrueCrypt services and processes and possibly the TrueCrypt password.
- If the computer is not booted, then examination of physical sector 0 indicates the presence of the TrueCrypt boot loader.