THE JOURNAL OF
DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 12 | Number 2 Article 12

6-30-2017

Protecting Digital Evidence Integrity and Preserving Chain of Custody

Makhdoom Syed Muhammad Baqir Shah
National University of Sciences and Technology, 14msismshah@seecs.edu.pk

Shahzad Saleem
National University of Sciences and Technology, shahzad.saleem@seecs.edu.pk

Roha Zulqarnain
National University of Sciences and Technology, 14msisrzulqarnain@seecs.edu.pk

PROTECTING DIGITAL EVIDENCE INTEGRITY AND PRESERVING CHAIN OF CUSTODY

Makhdoom Syed Muhammad Baqir Shah, Shahzad Saleem and Roha Zulqarnain
National University of Sciences and Technology
School of Electrical Engineering and Computer Science
Islamabad, Pakistan
14msismshah@seecs.edu.pk
shahzad.saleem@seecs.edu.pk
14msisrzulqarnain@seecs.edu.pk

ABSTRACT

Evidence is the key to solve any crime. Evidence integrity needs to be protected in order to make it admissible in the court of law. Digital evidence is more revealing, but it is fragile; it can easily be tampered with or modified. There are different techniques available to protect the integrity of digital evidence. Different automated digital evidence acquisition tools are available in the market. In this paper, we have analyzed two automated tools (EnCase and FTK Imager) that are used for disk imaging. These tools claim to protect the integrity of digital evidence. The techniques used by these tools are analyzed in this paper. Problems with their approaches are discussed and a solution is proposed to address the problems. A prototype of an automated tool is developed with an implementation of the proposed solution.

Keywords: Digital evidence, integrity, chain of custody, digital hash, digital signature, disk imaging

1. INTRODUCTION

Generally, when a crime is committed, evidence is collected from the crime scene. The criminal is identified after the examination and analysis of the evidence. In order to prosecute the criminal, a court requires sound evidence. If integrity of the evidence presented in court could not be proved then it becomes inadmissible. If there is even a doubt that the evidence could have been tampered with then its integrity becomes questionable. If there is some period of time when the evidence could have been mishandled or it could have been in the custody of an unauthorized person, its integrity is doubted. From the time of collection of the evidence till the prosecution of the case, evidence integrity must be kept sound and its chain of custody must also be made tamperproof.

A former Xerox engineer, Larry Benedict, 45, was sentenced to four years in prison by a federal judge. He was accused of trafficking in child pornography. All the evidence in this case was electronic. Larry Benedict hired a computer expert who found evidence that pointed towards his innocence. It was found that all the evidence presented in court was

allegedly tampered with or otherwise altered after it was in government custody ("Electronic evidence anchors porn case - CNET," n.d.). In another case, Jodi Arias in Arizona was arrested and found guilty of murder of Travis Alexander. She was sentenced to death. She hired a computer forensics expert to examine the victim computer. It was found that thousands of files were deleted from the computer while it was in the custody of Mesa police department ("Did Mesa Police Botch The Arias Case?," n.d.). The problem of corruption exists worldwide and law enforcement agencies are not an exception to that. The need of protection and preservation of digital evidence during the extraction phase is emphasized in the paper (Saleem, Popov, & Bagilli, 2014). It is also emphasized in the IOEC's guidelines (Enfsi, 2009). In order to minimize human interaction and subjectivity, it is important to automate the system for preservation of digital evidence integrity and its chain of custody.

Digital evidence is fragile in nature and it is handled differently. The process of collection and archiving digital evidence is outlined in RFC3227 (Brezinski & Killalea, 2002). Many tools have been developed to aid forensic examiners in gathering and preserving digital evidence. These tools use message digest to ensure integrity of the digital evidence. Only message digest is not enough to guarantee the integrity of the digital evidence (Lee, Kim, Lee, & Lim, 2005), because it can easily be forged. Authors (Aoki, Guo, Matusiewicz, Sasaki, & Wang, 2009) (Robshaw, 1996) (Xie, Liu, & Feng, 2006) (Wang, Yin, & Yu, 2005) (Wang & Yu, 2005) describe some of the methods to forge integrity.

The PIDESC Model (Saleem & Popov, 2011) provides a solution to deal with the problem in message digests but it ignores the protection of the chain of custody. Not only the evidence, but also the chain of custody needs to be protected and made tamperproof. There is need of a method that can ensure not only protection of the digital evidence integrity, but also preservation of the digital chain of custody.

This paper consists of seven sections, including references. The current section explains the problem that needs to be solved. Second and third sections discuss digital evidence integrity protection techniques currently being used and their shortcomings. Then in the fourth section, our solution is explained. The fifth section is based on the analysis and comparison of our solution with the currently present solutions. Section six gives conclusion and future directions. The last section is composed of references.

2. CURRENT PRACTICES FOR DIGITAL EVIDENCE INTEGRITY PROTECTION

In this section, we will discuss the techniques that are used by FTK Imager ("Product Download," 2014) and Encase (Guidance Software, 2016) to protect digital evidence integrity.

2.1 Integrity Protection by FTK Imager

FTK Imager is a disk imaging tool. It can be used for imaging of logical drives as well as physical drives. It supports four different formats to store the extracted image. These formats are AD1, E01, RAW and SMART. Digital evidence integrity is ensured by calculating MD5 and SHA1 hashes of the extracted content and storing it in a report along with other details related to the drive. It also offers an encryption feature to ensure the confidentiality of the digital evidence. The

digital evidence can be encrypted by using a password or a digital certificate.

The documentation of FTK Imager recommends using "Write Blocking Hardware" so that digital evidence contents are not changed during the data extraction phase.

2.2 Integrity Protection by Encase

Encase is a forensics tool and it is used to extract an image of the whole drive. The extracted image is stored in E01 format. Integrity of the extracted contents is ensured by generating CRC and digital hashes (MD5 and SHA1). It also provides an optional feature of encryption to ensure the confidentiality of the extracted contents.

Just like FTK Imager, Encase recommends using "Write Blocking Hardware."

3. SHORTCOMINGS OF CURRENT PRACTICES

In this section, we will discuss the problems with the practices used by the FTK Imager and Encase.

3.1 Problems with FTK Imager

There are a few points that need to be addressed in the approach used by the FTK Imager. Firstly, there is no functionality present in it that can verify or authenticate the person who is extracting the forensic image. Anyone can enter the name of anyone else as a forensic examiner and extract the image. There is no way of knowing that evidence was, indeed, extracted by an authorized person. So, there is a big question on the soundness of the evidence. Secondly, integrity of the evidence is provided through hashes. Hashes are not enough to guarantee the integrity of the evidence. If contents of the evidence are modified and hashes are recalculated and stored, then the changes in the evidence will go undetected. This again makes the integrity of the evidence questionable. If encryption is used then it becomes difficult for the modifications to go undetected but still possible (Saleem & Popov, 2011).

3.2 Problems with Encase

Just like the FTK Imager, Encase does not provide any functionality to verify or authenticate the person who is extracting the forensic image. So, there is no way of knowing who actually extracted the evidence that makes integrity of the evidence questionable. Encase uses MDCs to provide integrity, but MDCs are not enough to ensure the integrity and can be forged. In (Saleem & Popov, 2011), it is discussed in detail that how can MDCs be forged and even using encryption with MDCs does not guarantee the integrity.

Both the FTK Imager and the Encase claim to ensure the integrity of digital evidence, but the techniques used by these tools leave the evidence integrity questionable. Moreover, these tools do not offer any functionality that can enforce chain of custody preservation.

4. PROPOSED SOLUTION

It is evident from above that digital hash or MDCs alone are not enough to guarantee the integrity of digital evidence. Storing passwords or digital keys on local systems is not a safe approach because if an unauthorized person gets access to the system, then he or she could compromise the passwords or digital keys. Using smart cards to store the digital credentials is one of the best approaches, as it securely stores the digital keys or passwords (Smartcard Alliance & Alliance, 2014). We propose to use smart cards to store private keys of forensics examiners and to generate digital signatures to ensure the integrity of the digital evidence. This approach will make the

contents tamperproof and as private keys are unique, the forensic examiner can be verified as well.

Our proposed solution is the development of an automated tool that can ensure the integrity of digital evidence. It should be able to not only protect the digital evidence but also preserve digital chain of custody. In order to achieve this, we have developed a prototype of a forensic tool with the following functionalities and it works in the order specified below:

1. Authenticate and Authorize the forensic examiner using smart card credentials
2. Extracting a bit by bit image of the whole disk drive containing the evidence (Our prototype tool only supports RAW imaging for now. Other imaging formats like E01, AFF etc. can also be used instead of RAW format)
3. Creating a digital chain of custody and appending it to the extracted image
4. Computing hash (SHA1) over the extracted image and the digital chain of custody
5. Generating digital signature over the computed hash by using private key (RSA-1024 bit) of the forensics examiner stored in the smart card
6. Appending the generated digital signature at the end of chain of custody

This approach will ensure that any of the contents in the evidence or the digital chain of custody does not get tampered. Integrity of both the digital evidence and its chain of custody can be verified. It removes the possibility of even a single bit being changed in the extracted evidence, and its digital chain of custody to go undetected. This can guarantee the digital evidence integrity and digital chain of custody preservation.

We have created a simple template for the digital chain of custody. In our tool, we have stored the extracted image and its digital chain of custody in a structure as shown in Figure 1. The forensic examiner needs to enter the case number and the evidence number manually. The rest of the data is inserted automatically by the tool.

The digital chain of custody consists of two types of rings; first ring and additional ring. When the digital evidence is extracted by the forensic examiner, first ring is added. Whenever the evidence is handed over to an authorized person, additional ring is added to the chain of custody. In the chain of custody there can be only one first ring, whereas the number of additional rings depends upon number of persons to whom the evidence is handed over. Each handover adds an additional ring to the chain of custody. First ring is composed of 1024 bytes, whereas each additional ring is composed of 512 bytes. Structure and composition of the rings are discussed in the subsections.

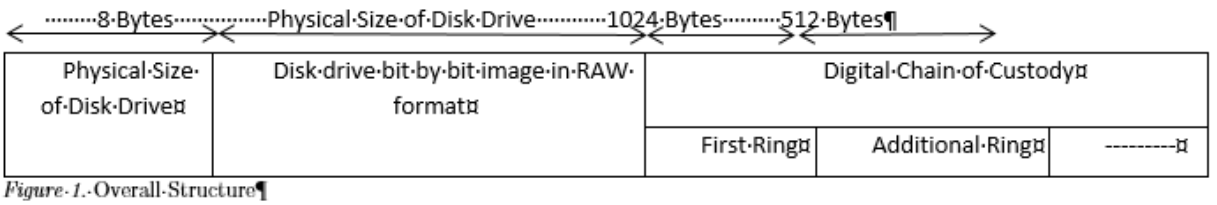

Figure 1. Overall Structure

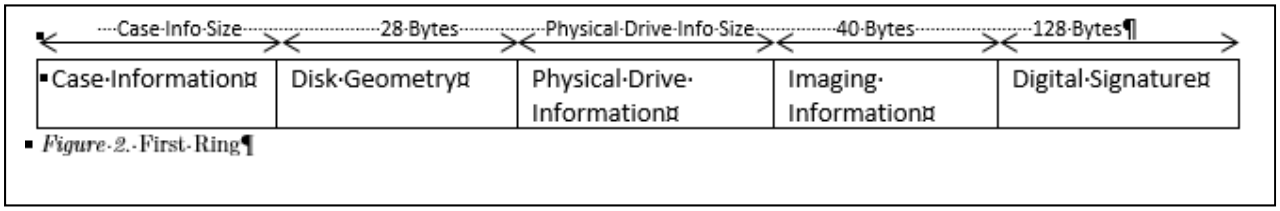

Figure 2. First Ring

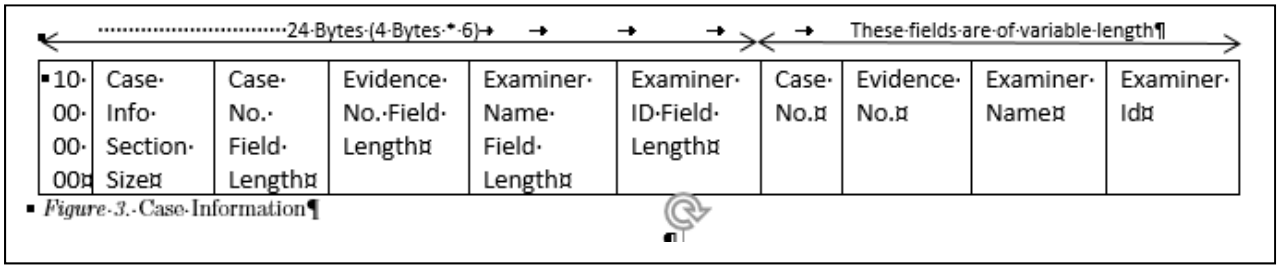

Figure 3. Case Information

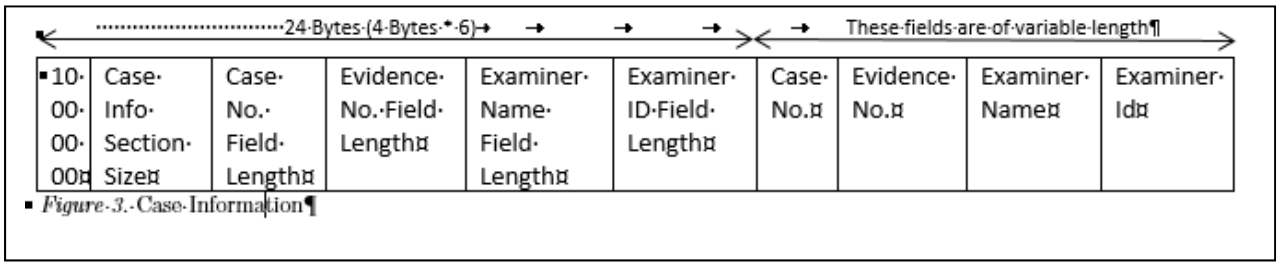

Figure 3. Case Information

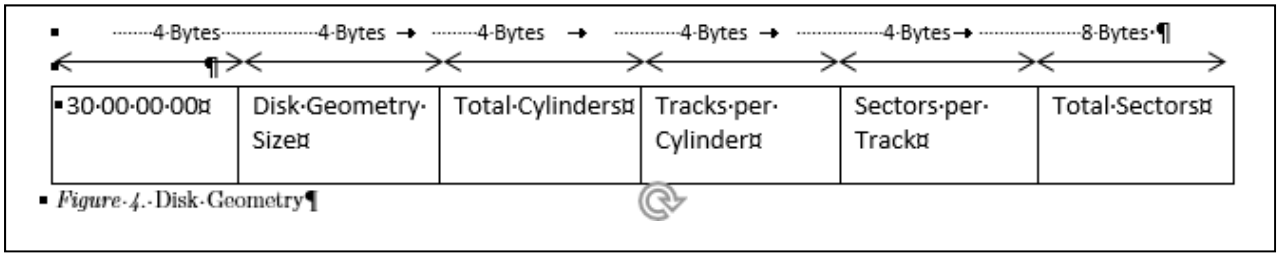

Figure 4. Disk Geometry

4.1 First Ring

First ring of the digital chain of custody is divided into five sections. These sections are of different sizes. The first and third sections are of variable size, whereas the second, fourth and fifth sections are of fixed size as shown in Figure 2. The details of each section are as follows.

4.1.1 Case Information

This section contains information related to the case. It starts with a four bytes tag, which in hex is, "10 00 00 00." The next four bytes (5^{th} -8^{th}) represents the size of this section in bytes, including the tag bytes. The next sixteen bytes (9^{th}- 24^{th}) consist of four sections, each of which consists of four bytes, representing the case number field length, the

evidence number field length, the examiner name field length and the examiner ID field length in bytes, in the same order. Structure of this section is shown in Figure 3.

4.1.2 Disk Geometry

This section contains information about the geometry of the disk drive whose image is extracted. It starts with a four bytes tag, which in hex is, "30 00 00 00." The next four bytes (5th -8th) represent the size of this section in bytes, including the tag bytes. The next four bytes (9th – 12th) represent the total cylinders in the disk drive. The four bytes after that (13th – 16th) represent the tracks per cylinder in the disk drive. The next four bytes (17th – 20th) represent the sectors per track in the disk drive. The next eight bytes (21st – 28th) represent the total number of sectors in the disk drive. Structure of this section is shown in Figure 4.

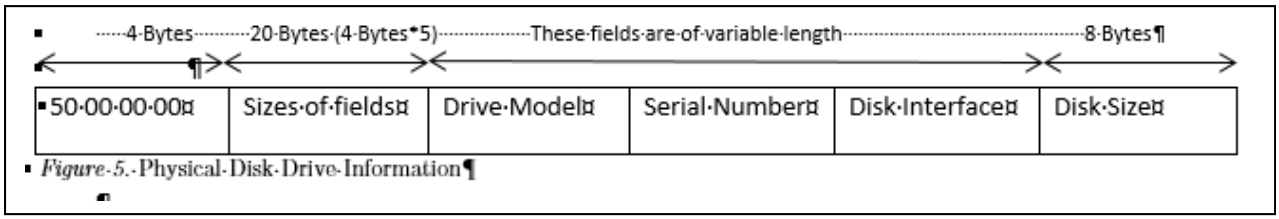

Figure 5. Physical Disk Drive Information

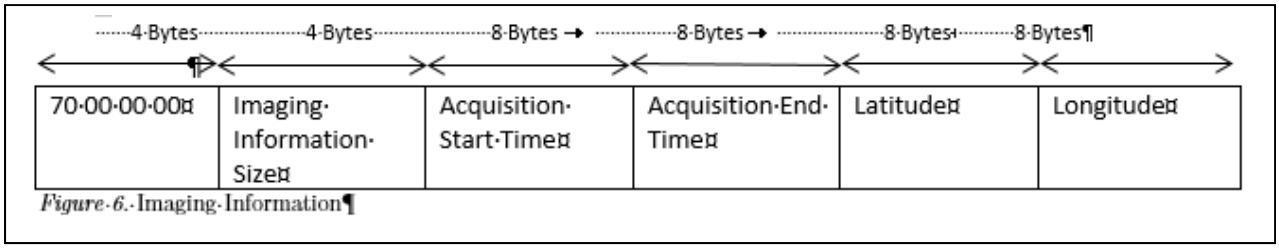

Figure 6. Imaging Information

4.1.3 Physical Drive Information

This section contains information about the physical disk drive whose image is extracted. It starts with a four bytes tag, which in hex is, "50 00 00 00." The next four bytes (5th -8th) represent the size of this section in bytes, including the tag bytes. The next 16 bytes (9th – 24th) consist of four sections, each of which consists of four bytes, representing the drive model field length, the serial number field length, the disk interface field length and the disk size field length in bytes, in the same order. Structure of this section is shown in Figure 5.

4.1.4 Imaging Information

This section contains information that is related to the imaging of the disk drive. It starts with a four bytes tag, which in hex is, "70 00 00 00." The next four bytes (5th -8th) represent the size of this section in bytes, including the tag bytes. The next eight bytes (9th – 16th) represent the time when the image acquisition was started. The next eight bytes (17th – 24th) represent the time when the image acquisition was completed. The next sixteen bytes (25th – 40th) represent the geographical location of the forensic examiner at the time of acquisition, where first eight bytes (25th – 32nd) represent latitude and last eight bytes (33rd –

40th) represent longitude. Structure of this section is shown in Figure 6.

4.1.5 Digital Signature

The last 128 bytes section contains the digital signature which is generated via a smart card using RSA 1024 bit private key of the forensic examiner.

1024 bytes are reserved for the digital chain of custody in which first 896 bytes contain data related to the chain of custody and the last 128 bytes are for the digital signature.

4.2 Additional Ring

This ring is composed of 512 bytes with a 4 bytes starting tag of "90 00 00 00" in hex. This ring includes the authorized person's name, his/her ID (name and ID are stored in his/her smart card), time at which the evidence is handed over, location of the evidence hand over and his/her digital signature via a smart card. This digital signature needs to be calculated over the previous chain of custody rings and the current ring's first 384 bytes. The calculated digital signature is then stored in last 128 bytes of the current ring.

5. ANALYSIS AND COMPARISON

If we compare the proposed approach to the approach being used to ensure the integrity of the digital evidence, then the proposed approach is undoubtedly the better one. It rules out doubts about the unauthorized modification of the evidence; it provides non-repudiation. It does a better job in protecting the integrity than the techniques currently being used. In terms of cost, the proposed approach costs a little more. The additional cost is incurred due to the use of smart cards, which are cheap in price. The added cost is well justified in terms of the level of trust and clarity it provides in integrity of digital evidence and its digital chain of custody. In terms of time, this approach takes hardly a second extra than the techniques currently being used. This added time is for digital signature generation which takes less than one second. So, the difference in terms of time is negligible. In addition to the digital evidence integrity, our proposed approach preserves the chain of custody but the current tools do not offer such functionality. This comparison is based on the results of the tool that we developed as a proof of concept to analyze the proposed approach.

6. CONCLUSION AND FUTURE DIRECTIONS

The proposed solution is effective and feasible. It provides not only digital evidence integrity protection but also the digital chain of custody preservation. We developed a tool as a proof of concept with limited functionality to evaluate our proposed solution. An industrial standard forensic tool can be developed based on the concept that we used to develop our tool. The forensic tool should extract forensic image and store it in multiple formats, contrary to our tool that only stores image in RAW format.

REFERENCES

Aoki, K., Guo, J., Matusiewicz, K., Sasaki, Y., & Wang, L. (2009). Preimages for step-reduced SHA-2. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 5912 LNCS, pp. 578–597). http://doi.org/10.1007/978-3-642-10366-7_34

Brezinski, D., & Killalea, T. (2002). RFC 3227 Guidelines for Evidence Collection and Archiving Status. Rfc, 1–10.

Did Mesa Police Botch The Arias Case? (n.d.). Retrieved December 22, 2016, from http://evidencesolutions.com/web/index.php/Digital-Evidence-Articles/did-mesa-police-botch-the-arias-case-computer-forensics.html

Electronic evidence anchors porn case - CNET. (n.d.). Retrieved December 22, 2016, from https://www.cnet.com/news/electronic-evidence-anchors-porn-case/

Enfsi. (2009). Guidelines for Best Practice in the Forensic - United Kingdon. Science, (April), 1–30.

Guidance Software. (2016). EnCase Forensic Software - Top Digital Investigations Solution. Retrieved from https://www.guidancesoftware.com/encase-forensic

Lee, S., Kim, H., Lee, S., & Lim, J. (2005). Digital evidence collection process in integrity and memory information gathering. In Proceedings - First International Workshop on Systematic Approaches to Digital Forensic Engineering (Vol. 2005, pp. 236–247). http://doi.org/10.1109/SADFE.2005.9

Product Download. (2014). Retrieved from http://accessdata.com/product-download/digital-forensics

Robshaw, M. (1996). On recent results for MD2, MD4 and MD5. RSA Laboratories Bulletin, 4, 2–7. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:On+Recent+Results+for+MD2,+MD4+and+MD5#0%5Cnhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:On+recent+results+for+MD2,+MD4+and+MD5#0

Saleem, S., & Popov, O. (2011). Protecting digital evidence integrity by using smart cards. In Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST (Vol. 53, pp. 110–119). http://doi.org/10.1007/978-3-642-19513-6_9

Saleem, S., Popov, O., & Bagilli, I. (2014). Extended abstract digital forensics model with preservation and protection as umbrella principles. Procedia - Procedia Computer Science, 35, 812–821. http://doi.org/10.1016/j.procs.2014.08.246

Smartcard Alliance, & Alliance, S. (2014). About Smart Cards : Introduction : Primer - Smart Card Alliance. Retrieved from http://www.smartcardalliance.org/smart-cards-intro-primer/

Wang, X., Yin, Y. L., & Yu, H. (2005). Finding Collisions in the Full SHA-1. In Advances in Cryptology – CRYPTO 2005 (pp. 17–36). http://doi.org/10.1007/11535218_2

Wang, X., & Yu, H. (2005). How to Break MD5 and Other Hash Functions. In

Advances in Cryptology – EUROCRYPT 2005 (pp. 19–35). http://doi.org/10.1007/11426639_2

Xie, T., Liu, F., & Feng, D. (2006). Fast collision attack on MD5. IACR ePrint Archive Report, 104, 17. http://doi.org/10.1.1.301.4421

