**Jaypee Institute Of InformationTechnology, Noida**

# Information Security Lab Project
# 5th semester

**Topic: Ramsomware**

**Team members:**

| | |
|---|---|
| Kaushal Bhansali | 17103299 (B-8) |
| Ankit Bathla | 17103302 (B-8) |
| Gyan Ranjan | 17103306 (B-8) |
| Harshit Bajpai | 17103293 (B-8) |
| Harsh Tyagi | 17103322 (B-8) |

**Submitted to:**

Dr. P. Raghu Vamsi

## Introduction:

There is a severe lack of open source ransomware, and for good reason! But by having so few examples, and those examples being inaccurate (intentionally bad code with flaws), or just too complicated, it doesn't leave much to analyze and learn from. People seem to think that ransomware is hard to write. That it's this complex, hard to develop, hard to RE, and hard to prevent beast. A quick read through of this codebase will prove that's not true. Im hoping this can lead to better signatures, a better understanding of how ransomware works and what can be done to stop it, and an overall safer internet.

## Overview:

This project is fully python ransom ware PoC. It's main purpose is not to be run like most software projects, but to be read for educational purposes.

Aside from very minor testing to ensure there are no syntax errors, no testing has been done. This may occur at a later time to ensure it performs in all expected environments,but that is not the point. The point is to be a simple to read PoC that makes for an easy example of what ransomware is and how it works. And hopefully, this can lead to a better understanding of ransomware in the network defense and sysadmin communities.

This project will encrypt and decrypt files. That's about it. No key generation, no sending the key back over a secure channel, no dropping new files or wallpapers or whatever.

## Concepts Used:

## Advance Encryption Standard (AES):

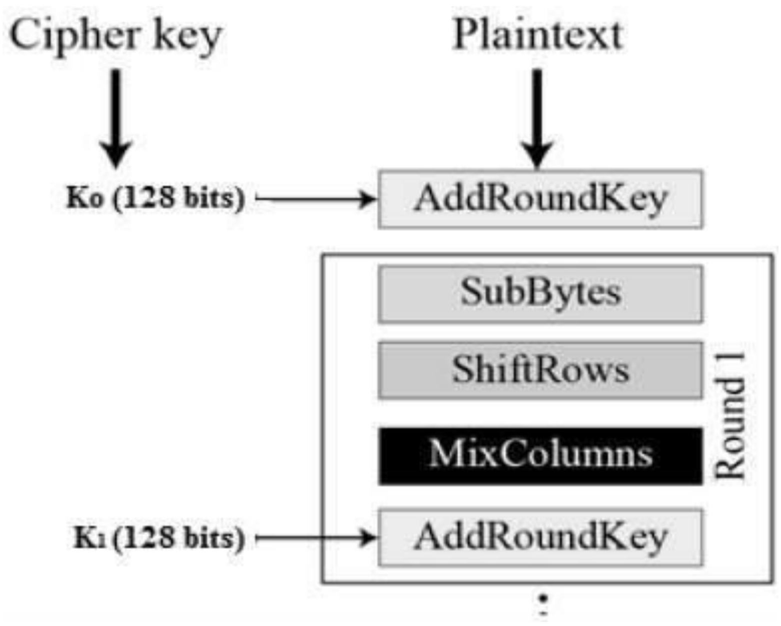
The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

## Encryption Process:

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below −

**Byte Substitution (SubBytes)**

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.



## Shiftrows:

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

## MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

## Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

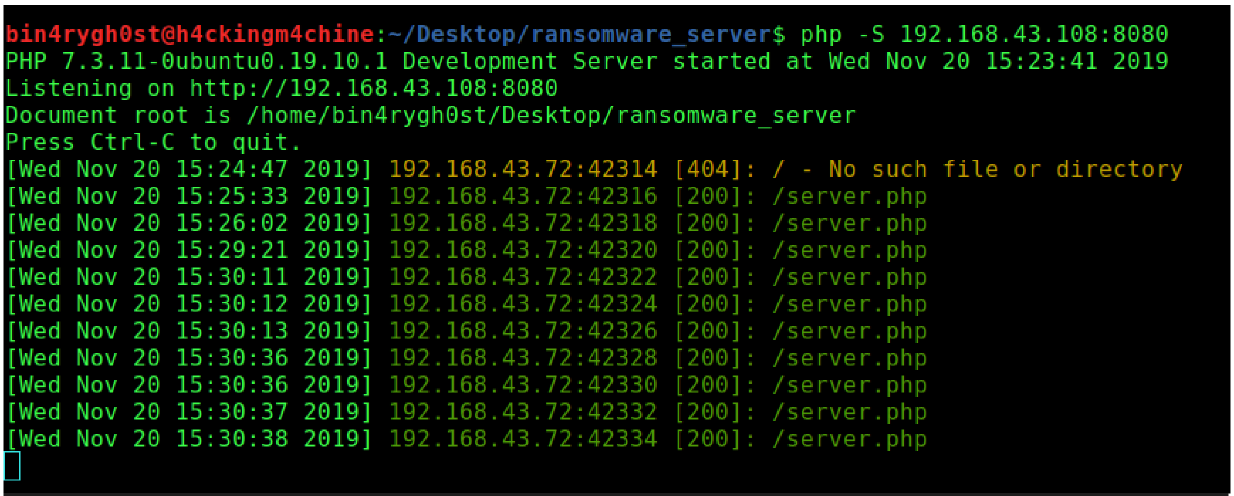
## **Decryption Process:**

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

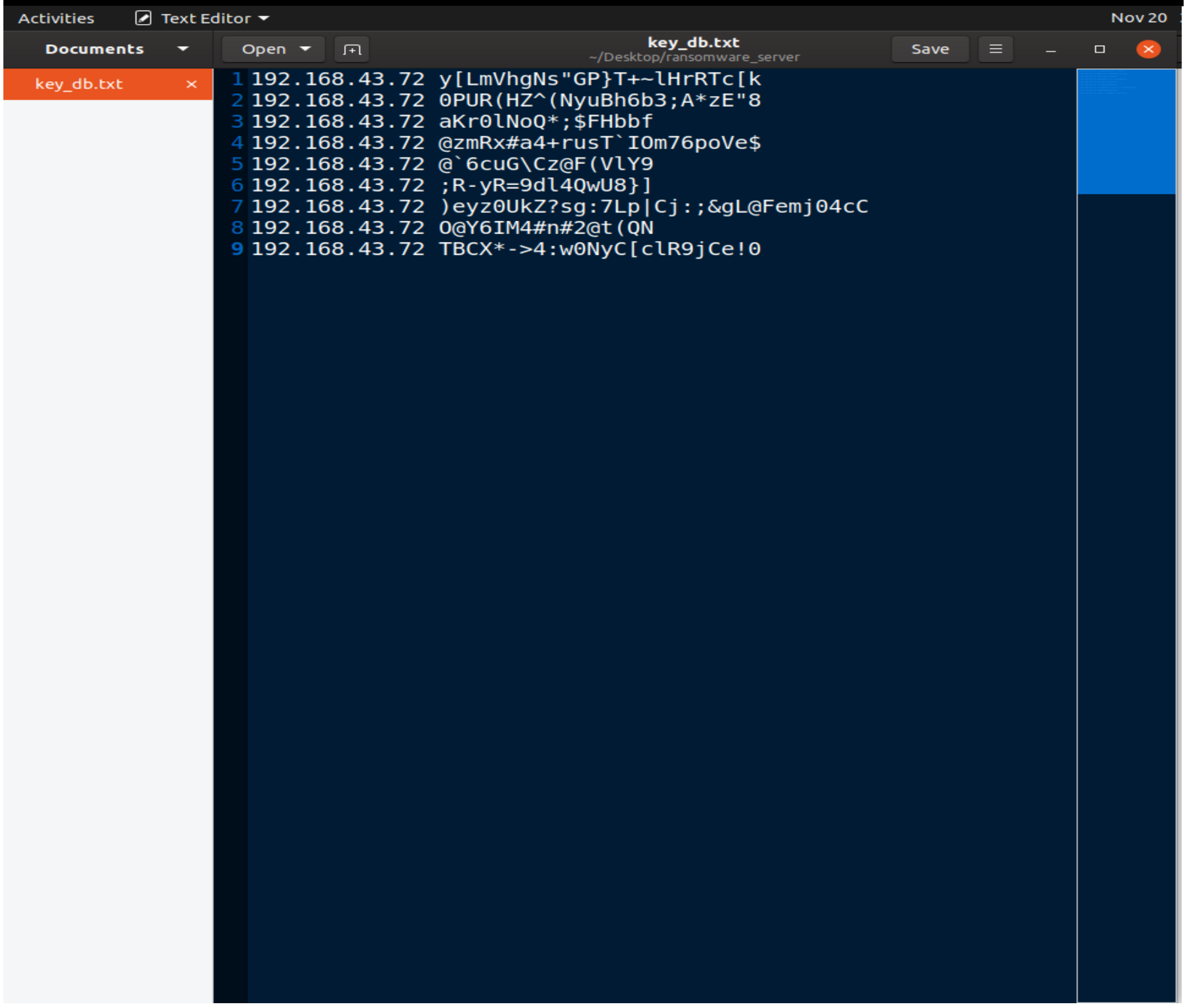
- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

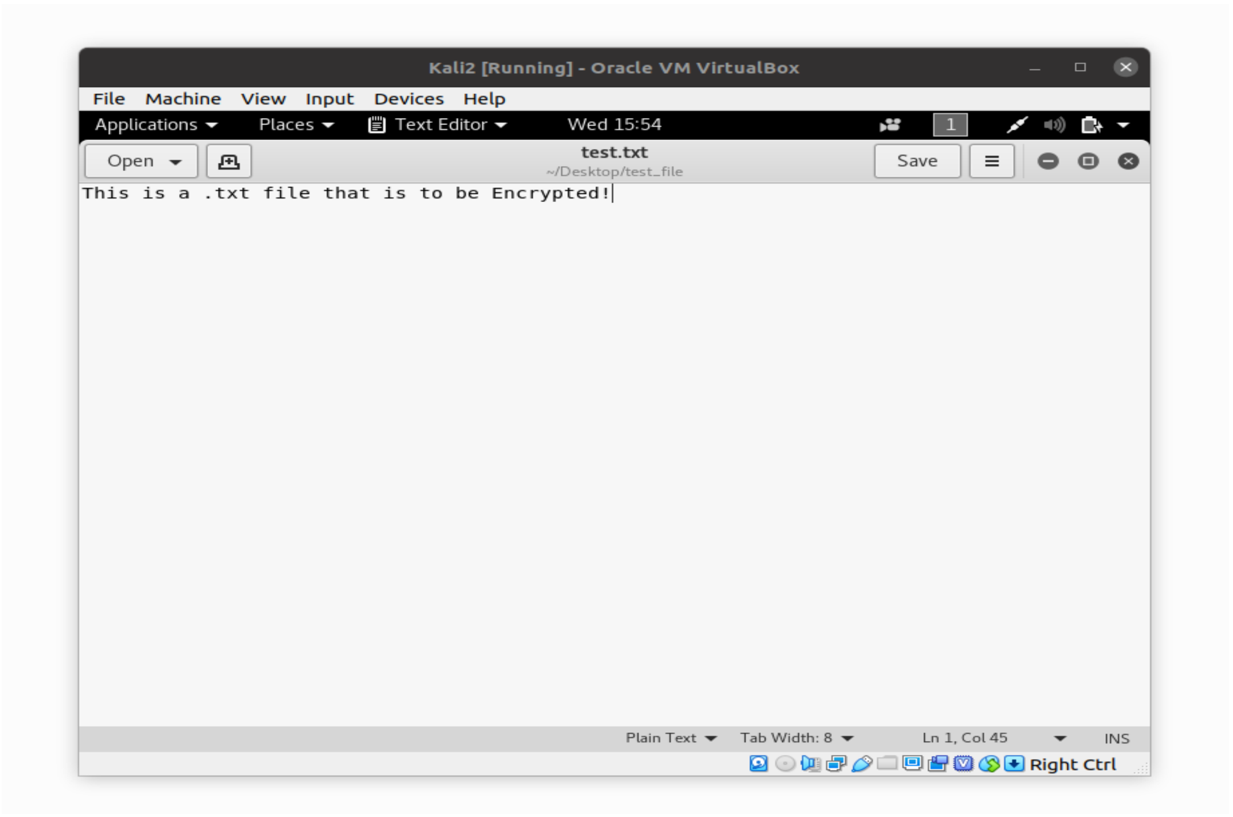
## Code Output:



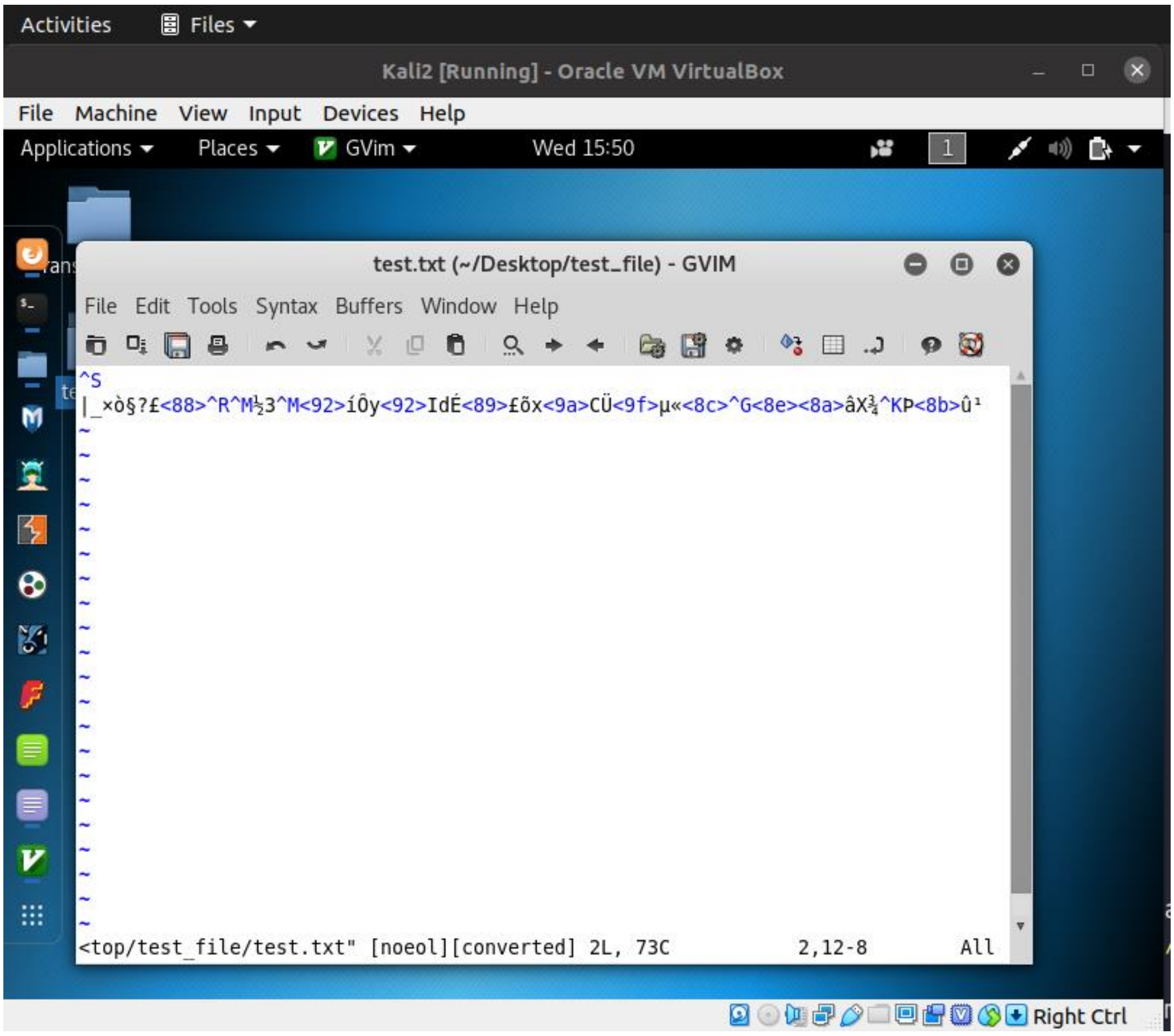
```
bin4rygh0st@h4ckingm4chine:~/Desktop/ransomware_server$ php -S 192.168.43.108:8080
PHP 7.3.11-0ubuntu0.19.10.1 Development Server started at Wed Nov 20 15:23:41 2019
Listening on http://192.168.43.108:8080
Document root is /home/bin4rygh0st/Desktop/ransomware_server
Press Ctrl-C to quit.
[Wed Nov 20 15:24:47 2019] 192.168.43.72:42314 [404]: / - No such file or directory
[Wed Nov 20 15:25:33 2019] 192.168.43.72:42316 [200]: /server.php
[Wed Nov 20 15:26:02 2019] 192.168.43.72:42318 [200]: /server.php
[Wed Nov 20 15:29:21 2019] 192.168.43.72:42320 [200]: /server.php
[Wed Nov 20 15:30:11 2019] 192.168.43.72:42322 [200]: /server.php
[Wed Nov 20 15:30:12 2019] 192.168.43.72:42324 [200]: /server.php
[Wed Nov 20 15:30:13 2019] 192.168.43.72:42326 [200]: /server.php
[Wed Nov 20 15:30:36 2019] 192.168.43.72:42328 [200]: /server.php
[Wed Nov 20 15:30:36 2019] 192.168.43.72:42330 [200]: /server.php
[Wed Nov 20 15:30:37 2019] 192.168.43.72:42332 [200]: /server.php
[Wed Nov 20 15:30:38 2019] 192.168.43.72:42334 [200]: /server.php
```



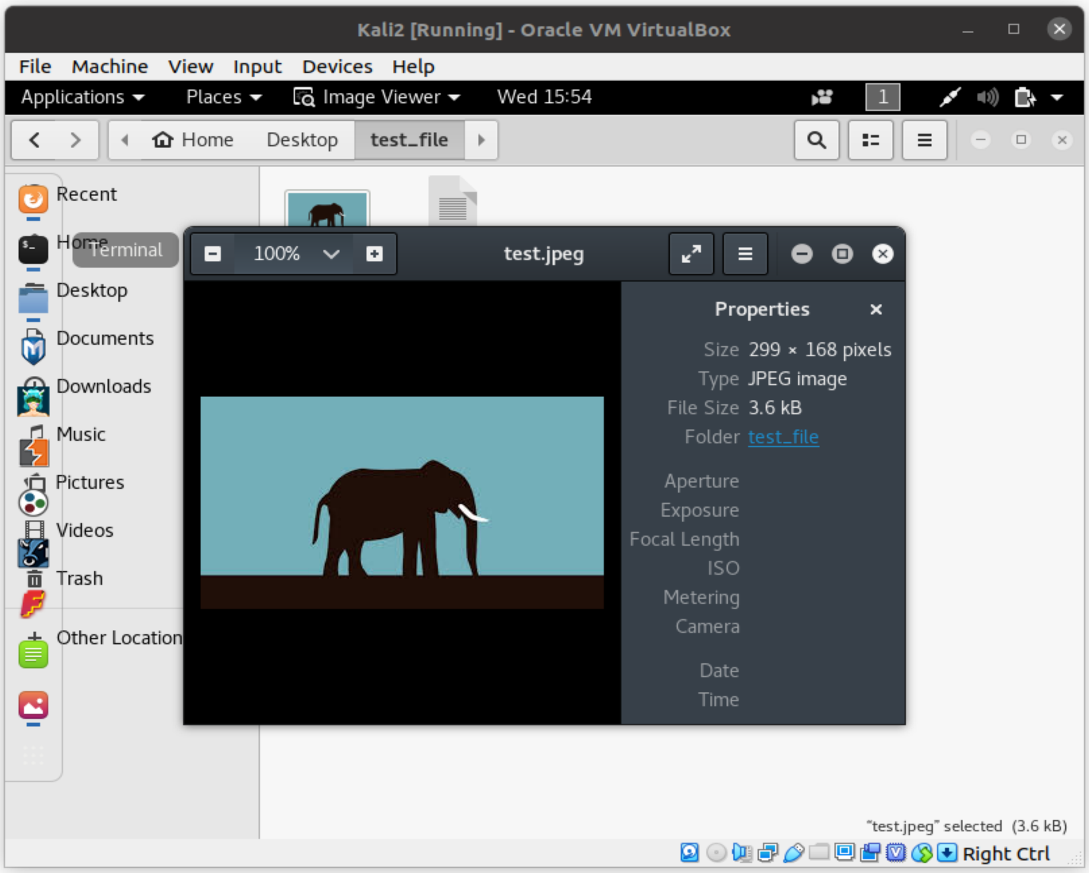
```
192.168.43.72 y[LmVhgNs"GP}T+~lHrRTc[k
192.168.43.72 0PUR(HZ^(NyuBh6b3;A*zE"8
192.168.43.72 aKr0lNoQ*;$FHbbf
192.168.43.72 @zmRx#a4+rusT`IOm76poVe$
192.168.43.72 @`6cuG\Cz@F(VlY9
192.168.43.72 ;R-yR=9dl4QwU8}]
192.168.43.72 )eyz0UkZ?sg:7Lp|Cj:;&gL@Femj04cC
192.168.43.72 O@Y6IM4#n#2@t(QN
192.168.43.72 TBCX*->4:w0NyC[clR9jCe!0
```



```
This is a .txt file that is to be Encrypted!
```



```
^S
|_×ò§?£<88>^R^M½3^M<92>íÔy<92>IdÉ<89>£õx<9a>CÜ<9f>µ«<8c>^G<8e><8a>âX¾^KÞ<8b>û¹
~
<top/test_file/test.txt" [noeol][converted] 2L, 73C          2,12-8        All
```



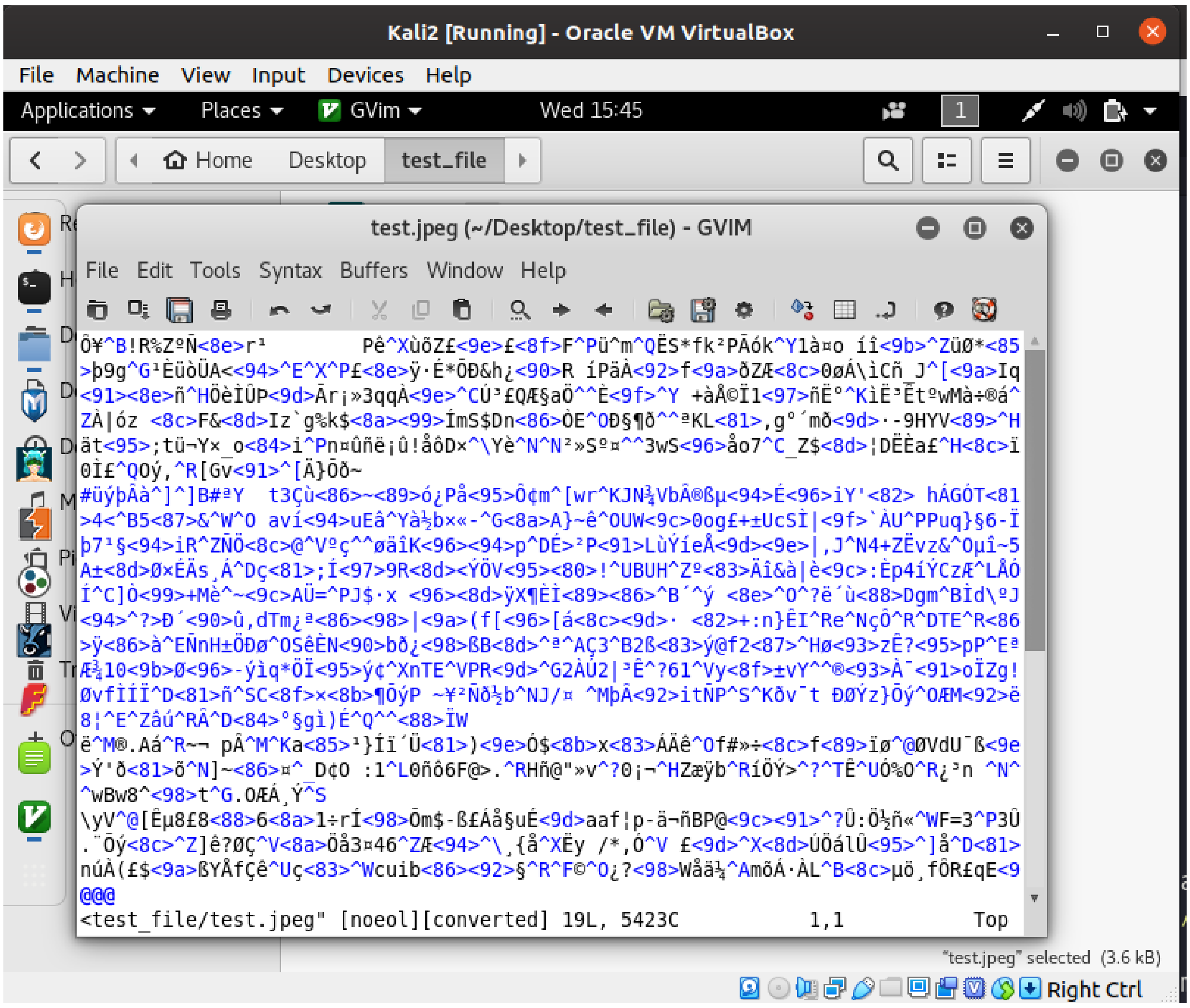
Properties

Size 299 × 168 pixels
Type JPEG image
File Size 3.6 kB
Folder test_file

Aperture
Exposure
Focal Length
ISO
Metering
Camera

Date
Time

"test.jpeg" selected (3.6 kB)


Kali2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places GVim Wed 15:45
Home Desktop test_file
test.jpeg (~/Desktop/test_file) - GVIM
File Edit Tools Syntax Buffers Window Help
Right Ctrl

```
Ô¥^B!R%ZºÑ<8e>r¹        Pê^XùõZ£<9e>£<8f>F^Pü^m^QËS*fk²PĀók^Y1à¤o íî<9b>^ZüØ*<85
>þ9g^G¹ÈüòÜA<<94>^E^X^P£<8e>ÿ·É*ŌÐ&h¿<90>R íPäÀ<92>f<9a>ðZÆ<8c>0øÁ\ìCñ_J^[<9a>Iq
<91><8e>ñ^HÖèÌÛP<9d>Ār¡»3qqÀ<9e>^CÚ³£QÆ§aÖ^^È<9f>^Y +àÅ©Ï1<97>ñË°^KìË³Ētº wMà÷®á^
ZÀ|óz <8c>F&<8d>Iz`g%k$<8a><99>ÍmS$Dn<86>ÒE^OÐ§¶ð^^ªKL<81>,g°´mð<9d>·-9HYV<89>^H
ät<95>;tü¬Y×_o<84>i^Pn¤ûñë¡û!åôD×^\Yè^N^N²»Sº¤^^3wS<96>åo7^C_Z$<8d>¦DËÈa£^H<8c>ï
0Ì£^QOý,^R[Gv<91>^[Ä}Ōð~
#üýþÂà^]^]B#ªY  t3Çù<86>~<89>ó¿På<95>Ô¢m^[wr^KJN¾VbÂ®ßµ<94>É<96>iY'<82> hÁGÓT<81
>4<^B5<87>&^W^O aví<94>uEâ^Yà½b×«-^G<8a>A}~ê^OUW<9c>0og£+±UcSÌ|<9f>`ÀU^PPuq}§6-Ï
þ7¹§<94>iR^ZÑÖ<8c>@^Vºç^^øäîK<96><94>p^DÉ>²P<91>LùÝíeÅ<9d><9e>|,J^N4+ZËvz&^Oµî~5
A±<8d>Ø×ÉÄs¸Á^Dç<81>;Í<97>9R<8d><ÝÖV<95><80>!^UBUH^Zº<83>Äî&à|è<9c>:Èp4íÝCzÆ^LÅÓ
Í^C]Ò<99>+Mè^~<9c>AÜ=^PJ$·x <96><8d>ÿX¶ÈÌ<89><86>^B´^ý <8e>^O^?ë´ù<88>Dgm^BÌd\ºJ
<94>^?>Ð´<90>û,dTm¿ª<86><98>|<9a>(f[<96>[á<8c><9d>· <82>+:n}ÊI^Re^NçÔ^R^DTE^R<86
>ÿ<86>à^EÑnH±ÖÐø^OSêÈN<90>bð¿<98>ßB<8d>^ª^AÇ3^B2ß<83>ý@f2<87>^Hø<93>zÊ?<95>pP^Eª
Æ¾10<9b>Ø<96>-ýìq*ÖÏ<95>ý¢^XnTE^VPR<9d>^G2ÀÜ2|³Ê^?61^Vy<8f>±vY^^®<93>À¯<91>oÏZg!
ØvfÌÍÏ^D<81>ñ^SC<8f>×<8b>¶ŌýP ~¥²Ñð½b^NJ/¤ ^MþÂ<92>itÑP^S^Kðv¯t ÐØÝz}Ōý^OÆM<92>ë
8¦^E^Zâú^RÂ^D<84>°§gì)É^Q^^<88>ÏW
ë^M®.Aá^R~¬ pÂ^M^Ka<85>¹}Íï´Ü<81>)<9e>Ó$<8b>x<83>ÁÄê^Of#»÷<8c>f<89>ïø^@ØVdU¯ß<9e
>Ý'ð<81>õ^N]~<86>¤^_D¢O :1^L0ñô6F@>.^RHñ@"»v^?0¡¬^HZæÿb^RíÖÝ>^?^TÊ^UÓ%O^R¿³n ^N^
^wBw8^<98>t^G.OÆÁ¸Ý^S
\yV^@[Êµ8£8<88>6<8a>1÷rÍ<98>Ōm$-ß£Áå§uÉ<9d>aaf¦p-ä¬ñBP@<9c><91>^?Û:Ö½ñ«^WF=3^P3Û
.¨Ōý<8c>^Z]ê?ØÇ^V<8a>Öå3¤46^ZÆ<94>^\¸{å^XËy /*,Ó^V £<9d>^X<8d>ÚÖálÛ<95>^]å^D<81>
núÀ(£$<9a>ßYÅfÇê^Uç<83>^Wcuib<86><92>§^R^F©^O¿?<98>Wåä¼^AmõÁ·ÀL^B<8c>µö¸fÔR£qE<9
@@@
<test_file/test.jpeg" [noeol][converted] 19L, 5423C          1,1          Top
```

"test.jpeg" selected (3.6 kB)