BUUCTF Misc杂项前十二道题的思路和感悟





CTF杂项MISC新手 专栏收录该内容

5 篇文章 1 订阅 订阅专栏

title: BUUCTF Misc date: 2021年8月18日 17点27分 tags: MISC categories: MISC

1、BUUCTF 签到题

直接告诉了flag。



1

签到题 flag{buu_ctf}.ttps://blog.csdn.net/afanzof

2、BUUCTF 第二道题(Stegsolve)

下载附件之后,得到一个gif动图。

使用Stegsolve打开。

使用gif动图工具,

然后一张一张的向后翻,

<u></u>		\times
rame : 21 of 89		aif5.net
flag{		Jucine
<	>	Save
*		\times
Frame : 51 of 89		gif5.net
he12	10	
<	>	Save
<u></u>		×
Frame : 79 of 89		gif5.net
hongl	ke}	
<		Save

得到flag{he11ohongke}

3、BUUCTF二维码(QR Research、Ziperrllo、winhex)

下载附件之后是一个zip压缩包。

解压之后得到了一个png的二维码图片。

利用QR Research工具,扫描得到了一个不是flag的信息。

QR Research			- 🗆	\times
文件(F) 工具(T) 帮助(H)				
	۵ 😯			
		纠错等级 H(30%) 版本 	推码 Auto 尺寸- 4	•
				~
				~
已解码数据 1:				^
	.3,268.4)-(268.7,	268.7)		~
解码完成		htt	ps://blog.csdn	.net/afanzci/

发现问题并不简单,根据之前攻防世界misc几道题的经验,应该是有东西藏在图片里面,直接拖到winhex打开。

Offset 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ANSI ASCII 000000016 09 50 4E 47 00 01 10 00	HEX QR_code	QR_code.png																
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	Offset	0	1	2	3	4	5	6	- 7	8	9	10	11	12	13	14	15	ANSI ASCII
00000016 00 00 01 18 00 00 01 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00000000	89	50	4E	47	OD	ΟA	1A	0A	00	00	00	OD	49	48	44	52	IPNG IHDR
000000032 CF 00 00 00 00 65 04 C 54 45 FF FF FF 00 00 00 55 Ĩ PITEY,YY U 00000064 C2 D3 7E 00 00 10 8C 49 44 41 54 68 81 E D 99 3B ÅO* IDATh 11; 00000064 22 03 30 10 44 22 02 0A 6D CF 47 02 CA 1B 19 59 DE AD Ep B mĨG É YÞ 00000066 A3 70 04 42 02 0A 6D CF 47 02 CA 1B 19 59 DE AD Ep B mĨG É YÞ 00000128 65 D2 12 DD DC ED 66 7E 92 69 C9 3C 6D DE CO 84 eÒ ŶÚIF*1É <fài< td=""> 00000140 32 D8 E6 PD 86 6D 85 57 AB E2 25 8E CA 289 8F I,0#id83 IW+I 00000160 32 D8 E6 PD 86 6D 85 57 CA 54 EC 23 58 25 8E CA 200001144 TP 9E 2G 30 23 EC 64 EA 33 IA 8B 80 57 2B 99 8F I,0#id83 IW+I 00000160 32 D8 E6 PD 86 6D 85 57 CA 54 EC 24 5E 62 CB SC 80 200001144 TP 9E 2B 80 367 FO A54 52 24 5E 62 CB SC 84840ÅI g ĨE 2 00000122 AB 10 93 C5 EA 38 5B ED 86 20 53 89 09 9A 01 98 IA681(IT SI I IPEČA*#AS IPEČA*#AS IPEČA*#AS 00000224 AB 10 93 C5 EA 38 5B ED 86 2C 7B 92 4C 08 C6 14 11 É I#411f(IL Æ IA81(IT SI I) IPEČA*#AS IPEČA*#AS IPEČA*#AS IPEČA*#A</fài<>	00000016	00	00	01	18	00	00	01	18	01	03	00	00	00	BD	40	7B	1⁄2@{
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	00000032	CF	00	00	00	06	50	4C	54	45	FF	FF	FF	00	00	00	55	Ï PLTEÿÿÿ U
00000064 92 83 00 14 ES 2 40 CR 11 7C 14 8E 06 47 DB AN CB MIG Ê YP 000000096 BB BA 23 BC YD CA BS F4 10 B3 CB YD P SÅ SÅ F4 10 B3 CB YD SÅ	00000048	C2	DЗ	7E	00	00	01	8C	49	44	41	54	68	81	ED	99	ЗB	ÂÓ~ IDATh i ;
00000000 A3 70 04 42 02 0A 60 CF 47 02 CA 1B 19 59 DE A0 \$p B mIG £ YÞ 000000006 B8 0A B2 35 BC 49 3C 9A 8F E4 10 A8 36 1A 92 EB \$*15MI<1 a "6 "a	00000064	92	83	30	10	44	E5	52	40	C8	11	7C	14	8E	06	47	DB	′∎O DåR@È ∎ GÛ
00000096 BB 8A B2 35 BC 49 3C 9A 8F E4 10 A8 36 1A 92 EB >>1*5\Lambda1(1 a "6 '6 00000112 A7 C3 D3 E3 CB 2C E6 2E 9B 57 32 75 98 C5 7E 6F SÃÓAË,æ.IW2uIÅ~o 00000144 07 9E 2C 30 23 EC 64 EA 33 1A 8B 80 57 2B 99 8F I,0#idé3 IIW+I 00000160 32 D8 E6 FD 86 6D 8E 57 64 BE C3 58 22 58 BC A0 20@ytmlwd&ÄX"X4 00000192 78 E9 CB 64 DE 64 AE C2 92 1F 67 09 CC CB 1B 32 xedEd+d&AI g IE 2 00000192 78 E9 CB 64 DE 64 AE C2 92 1F 67 09 CC CB 1B 32 xedEd+d&AI g IE 2 00000192 A3 D 23 CB 7E D 23 FC 66 5E 92 2D 53 4F A6 2D A3 clc`+&#ufr`-S0'+E 00000224 A3 D 23 CB 7E D 23 FC 66 5E 92 2D 53 4F A6 2D A3 clc`+&#ufr`-S0'+E 00000272 C9 14 93 8F A5 B9 CE 8B CE 7B 9E 4C 0B C6 141 11 É I +#11[t[t.# 00000272 C9 14 93 8F A5 B9 CE 8B C2 7B 92 4D 73 97 B1 79 32 ''X¬V È'd*EjKegô 00000274 A9 10 86 X5 57 7A 01 E0 39 0F 9C A7 B 20 73 97 B1 79 34 ''X¬V È'd*EjKegô 00000272 C9 14 93 8F A5 B9 CC 21 BD 7B DF B4 E7 EA A0 Ik1 I211k[K'G'é 00000272 S9 14 93 0F 95 AC C2 14 D7 7B 7B P4 C2 A3 73 B ''X¬V È'd*EjKegô 00000376 9E 68 9 81 05 99 5A CC 21 BD 7B DF B4 E7 EA A0 Ik1 I I211k[K'G'é </t</td><td>00000080</td><td>AЗ</td><td>70</td><td>04</td><td>42</td><td>02</td><td>ΟA</td><td>6D</td><td>CF</td><td>47</td><td>02</td><td>CA</td><td>$1\mathrm{B}$</td><td>19</td><td>59</td><td>DE</td><td>AO</td><td>£p B mÏG Ê Y⊧</td></tr><tr><td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td><td>00000096</td><td>BB</td><td>8A</td><td>В2</td><td>35</td><td>BC</td><td>49</td><td>ЗC</td><td>9A</td><td>8F</td><td>E 4</td><td>10</td><td>Α8</td><td>36</td><td>1A</td><td>92</td><td>EΒ</td><td>» ²5¼I< ä "6 ′ë</td></tr><tr><td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td><td>00000112</td><td>A7</td><td>CЗ</td><td>DЗ</td><td>EЗ</td><td>CB</td><td>2C</td><td>E6</td><td>2E</td><td>9B</td><td>57</td><td>32</td><td>75</td><td>98</td><td>C5</td><td>7E</td><td>6F</td><td>§ÃÓãË,æ.∥W2u∥Å~o</td></tr><tr><td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td><td>00000128</td><td>65</td><td>D2</td><td>12</td><td>DD</td><td>DC</td><td>ED</td><td>66</td><td>7E</td><td>92</td><td>69</td><td>C9</td><td>3C</td><td>60</td><td>DE</td><td>CO</td><td>84</td><td>eÒ ÝÜíf~′iÉ<`ÞÀ∣</td></tr><tr><td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td><td>00000144</td><td>07</td><td>9E</td><td>2C</td><td>30</td><td>23</td><td>EC</td><td>64</td><td>ΕA</td><td>33</td><td>1A</td><td>8B</td><td>80</td><td>57</td><td>2B</td><td>99</td><td>8F</td><td> ,O#ìdê3 ₩+ </td></tr><tr><td>00000176 09 8C 39 8E CB 14 62 9E 1F 67 09 CC CB 12 xxétdad@Ål g IÉ 2 00000192 78 E9 CB 64 DE 64 AE C2 9E 1F 67 09 CC CB 18 2 xxétdad@Ål g IÉ 2 00000224 A3 D2 3C B7 E0 23 FC 65 12 25 53 89 09 9A 19 8 ALé8[i¶ SI I I 00000226 AE 19 38 AS BS CE 18 07 32 F7 92 15 10 10 15 11 10 00000288 AF 57 AO 12 12 14 93 8F AS B9 C2 73 77 17 17 12 19 154 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14<</td><td>00000160</td><td>32</td><td>D8</td><td>E6</td><td>FD</td><td>86</td><td>6D</td><td>8E</td><td>57</td><td>64</td><td>ΒE</td><td>CЗ</td><td>58</td><td>22</td><td>58</td><td>BC</td><td>AO</td><td>20æý∎m∎Wd¾ÃX″X¼</td></tr><tr><td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td><td>00000176</td><td>09</td><td>8C</td><td>39</td><td>88</td><td>С8</td><td>D4</td><td>62</td><td>92</td><td>4B</td><td>CC</td><td>03</td><td>ΕA</td><td>FC</td><td>04</td><td>73</td><td>71</td><td>∣9∣ÈÔb′KÌ êü sq</td></tr><tr><td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td><td>00000192</td><td>78</td><td>Ε9</td><td>CB</td><td>64</td><td>DE</td><td>64</td><td>AE</td><td>C2</td><td>9E</td><td>1F</td><td>67</td><td>09</td><td>CC</td><td>CB</td><td>1B</td><td>32</td><td>xéËdÞd®Â∣ g ÌË 2</td></tr><tr><td>$\begin{array}{c c c c c c c c c c c c c c c c c c c$</td><td>00000208</td><td>6D</td><td>18</td><td>37</td><td>Ε7</td><td>9E</td><td>2B</td><td>03</td><td>67</td><td>FO</td><td>AA</td><td>54</td><td>E2</td><td>45</td><td>E6</td><td>26</td><td>DЗ</td><td>m 7ç∎+ gðªTâEæ&Ó</td></tr><tr><td>$\begin{array}{ c c c c c c c c c c c c c c c c c c c$</td><td>00000224</td><td>AЗ</td><td>D2</td><td>ЗC</td><td>Β7</td><td>ΕO</td><td>23</td><td>FC</td><td>66</td><td>5E</td><td>92</td><td>2D</td><td>53</td><td>4F</td><td>Α6</td><td>2D</td><td>AЗ</td><td>£Ò<•à#üf^″-SO¦-£</td></tr><tr><td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td><td>00000240</td><td>AB</td><td>10</td><td>93</td><td>C5</td><td>ΕA</td><td>38</td><td>5B</td><td>ED</td><td>B6</td><td>20</td><td>53</td><td>89</td><td>09</td><td>9A</td><td>01</td><td>98</td><td>≪ Åê8[í¶ S </td></tr><tr><td>$\begin{array}{c c c c c c c c c c c c c c c c c c c$</td><td>00000256</td><td>62</td><td>Β4</td><td>29</td><td>E8</td><td>9C</td><td>29</td><td>BЗ</td><td>8D</td><td>58</td><td>Β1</td><td>30</td><td>07</td><td>32</td><td>F7</td><td>99</td><td>21</td><td>b´)è∣)³ X±0 2÷∣!</td></tr><tr><td>$\begin{array}{c c c c c c c c c c c c c c c c c c c$</td><td>00000272</td><td>C9</td><td>14</td><td>93</td><td>8F</td><td>A5</td><td>Β9</td><td>CE</td><td>8B</td><td>CE</td><td>7B</td><td>9E</td><td>4C</td><td>ΟB</td><td>C6</td><td>14</td><td>11</td><td>É ∣ ¥¹Î∣Î{∣L Æ</td></tr><tr><td>00000304 9E 3C 64 84 17 87 29 2F C8 54 60 A4 9A EB 6A 28 I<dII</td> / L I<dII</td> <tdI</td> I<dII</td> I<dII</</td><td>00000288</td><td>AF</td><td>55</td><td>7A</td><td>01</td><td>ΕO</td><td>39</td><td>OF</td><td>9C</td><td>Α7</td><td>BC</td><td>20</td><td>73</td><td>97</td><td>B1</td><td>79</td><td>ЗE</td><td>¯Uz à9 ∎§¼ s∎±y></td></tr><tr><td>00000320 91 91 58 AC 56 7F C8 B4 64 A4 FE 58 C9 51 73 D4 ''X¬V È'd*pXÉQsÔ 00000336 9E 68 89 81 05 99 5A CC 21 BD 7B DF B4 E7 EA A0 IkI IZ1!%{6'çê 00000352 33 2E E1 52 E7 C9 7C 9A 19 92 4B CF 56 DA 73 3B 3.4RçÉ I 'KIVÚs; 00000368 BB 5C 50 98 4C DC 8F 99 FC B0 4A A6 39 E3 d*2å?IpÜ Iů°J'93 00000400 77 05 96 17 D7 B3 15 99 8A 4C AE 3F B9 FC 8F C7 w I*3'IL@?1w`J'P`U`U`J'y`I`P`U`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'Y`U`J'J'Y`U`J'U`J'J'Y`U`J'J'Y`U`J'Y`U`J'Y`U`J'J'Y`U`J'J'Y`U`J'J'Y`U`J'J'</td><td>00000304</td><td>9E</td><td>ЗC</td><td>64</td><td>84</td><td>17</td><td>87</td><td>29</td><td>2F</td><td>C8</td><td>54</td><td>60</td><td>Α4</td><td>9A</td><td>EΒ</td><td>6A</td><td>28</td><td> <d)∕ÈT`¤lëj(</td></tr><tr><td>00000336 9E 6B 89 81 05 99 5A CC 21 BD 7B DF B4 E7 EA A0 IkI IZÌ!½{B'çê 00000352 33 2E E1 52 E7 C9 7C 9A 19 92 4B CF 56 DA 73 3B 3.áRçÉ I 'KÏVÚs; 00000368 BB 5C 50 98 4C 2D A6 DC 8F E9 47 D4 62 E4 B1 88 >>PIL-¦Ü édÓbä±I 00000384 64 2A 32 E5 3F 8E 70 DC 8F 99 FC B0 4A A6 39 E3 d*2á?IpÜ Iů°J¦9ã 00000400 77 05 96 17 D7 B3 15 99 8A 4C AE 3F B9 FC 8F C7 w I ׳ IL0?'ü Ç 00000416 6C 43 A6 02 63 96 72 27 33 85 3C E8 9C F6 3C 99 1C¦ cIr'3I<èIč(I</td> 00000432 26 8C D7 9A 13 A3 09 B2 FF 3D DB 90 79 93 A1 FE &I×I £ ²ÿ=Û yI i p 00000448 8B 7E 01 B2 1B 8D D5 E6 69 67 86 00 00 00 00 49 I~² 2 ÕæigI I 00000444 45 4E 44 AE 42 60 82 50 4B 03 04 14 00 09 00 08 END®B`IPK 00000496 00 8B 50 2F 48 46 34 4C AE 1D 00 00 00 0F 00 00 IP/HF4L® 00000512 6E 0D DA 0B 3F 5A 17 7A 31 0D 51 6A 78 75 C6 03 n Ú ?Z 1 QjxuÆ 00000544 08 46 34 4C AE 1D 00 00 00 00 00 50 48 01 F4E® FK 00000544 08 46 34 4C AE 1D 00 00 00 00 50 48 01 F4E® FK 00000540 02 1F 00 14 00 99 00 88 00 8B 50 2F 48 46 34 4C IP/HF4L</td><td>00000320</td><td>91</td><td>91</td><td>58</td><td>AC</td><td>56</td><td>7F</td><td>C8</td><td>Β4</td><td>64</td><td>Α4</td><td>FΕ</td><td>58</td><td>С9</td><td>51</td><td>73</td><td>D4</td><td>''X¬V Èíd¤þXÉQsÔ</td></tr><tr><td>00000352332EE152E7C97C9A19924BCF56DA733B$3.4Rc\dot{P}$'KľVÚs;00000368BB5C50984C2DA6DC8FE947D462E4B188>>PIL-;U éGÔbä±100000384642A32E53F8E70DC8F99FCB04AA639E3$d*2\dot{a}$; PU iu°J; 9ã0000040077059617D7B315998A4CAE3FB9FC8FC7w i ׳ILC®?'iu Ç000004166C43A6026396722733853CE89CF63C99IC; clr'3I<<tl>i<elo<</td>i<</td>i<</td>*`ILC®?'iu Ç00000432268CD79A13A309B2FF3DDB907993A1FE<math>\&IL®?'iu Ç000004448B7E01B21B8DD5E66967860000008END@B`IPK00000444454E44AE2668254B030414009008END@B`IPK00000444454E44AE2668756D6267727478744number.txi</t</math></td><td>00000336</td><td>9E</td><td>6B</td><td>89</td><td>81</td><td>05</td><td>99</td><td>5A</td><td>CC</td><td>21</td><td>BD</td><td>7B</td><td>DF</td><td>Β4</td><td>Ε7</td><td>ΕA</td><td>AO</td><td>lkI IZÌ!½{Bíçê</td></tr><tr><td>00000368BB 5C 50 98 4C 2D A6 DC8F E9 47 D4 62 E4 B1 88$\gg PIL - \hat{U} \notin G\hat{O}b\ddot{a}\pm I$0000038464 2A 32 E5 3F 8E 70 DC8F 99 FC B0 4A A6 39 E3$d \star 2\dot{a}?Ip\ddot{U} I\ddot{u}°J 9\ddot{a}$0000040077 05 96 17 D7 B3 15 998A 4C AE 3F B9 FC 8F C7w I ׳ IIL@?¹ü Ç000004166C 43 A6 02 63 96 72 2733 85 3C E8 9C F6 3C 99IC! cIr'3I<<math>\dot{e}I\ddot{o}<I</math>000004488B 7E 01 B2 1B 8D D5 E669 67 86 00 00 00 00 49IC' cIr'3I<<math>\dot{e}I\ddot{o}<I</math>0000044445 4E 44 AE 42 60 82 504B 03 04 14 00 09 00 08END®E`IPK0000045000 8B 50 2F 48 46 34 4CAE 1D 00 00 00 0F 00 00IP/HF4L@000005126E 0D DA 0B 3F 5A 17 7A31 0D 51 6A 78 75 C6 03n Ú ?Z z1 QjxuÆ0000054408 46 34 4C AE 1D 00 0000 0F 00 00IP/HF4L@000005284A 9D 97 A9 B7 5B FC EA01 CB 7F A5 4F 50 4B 07J I@·[üê Ė ¥OPK0000056002 1F 00 14 00 09 00 0800 8B 50 2F 48 46 34 4CE00000576AE 1D 00 00 00 0F 00 0000 00 00 00 00 00 0050 4B 010000054408 46 34 4C AE 1D 00 0000 00 00 00 00 000000576AE 1D 00 00 00 0F 00 0000 00 00 00 0000000576AE 1D 00 00 00 0F 00 0000 00 00 00 000000059200 00 00 00 00 00 00 0000 00 00 00 0000 00006865 72 2E 74 78 74 0A 0020 00 00 00 00 0000000640D1 01 65 7A 68 64 F3 4CD1 01 65 7A 68 64 F3 4C00000664D1 01 65 7A 68 64 F3 4CD1 01 50 4B 05 06 00 000000065600 00 01 00 01 00 5D 0000 00 05 60 00 00 00 00</</td><td>00000352</td><td>33</td><td>2E</td><td>E 1</td><td>52</td><td>Ε7</td><td>С9</td><td>7C</td><td>9A</td><td>19</td><td>92</td><td>4B</td><td>CF</td><td>56</td><td>DA</td><td>73</td><td>ЗB</td><td>3.áRçÉ∣∣ ′KÏVÚs;</td></tr><tr><td>00000384 64 2A 32 E5 3F 8E 70 DC 8F 99 FC B0 4A A6 39 E3 d*2å?lpÜ lü°J¦9ã 00000400 77 05 96 17 D7 B3 15 99 8A 4C AE 3F B9 FC 8F C7 w l ×° llL@?'ü Ç 00000416 6C 43 A6 02 63 96 72 27 33 85 3C E8 9C F6 3C 99 1C' clr'3l<èlö<!</td> 00000422 26 8C D7 9A 13 A3 09 B2 FF 3D DB 90 79 93 A1 FE &lxl £ ²ÿ=Û ylip 00000448 8B 7E 01 B2 1B 8D D5 E6 69 67 86 00 00 00 00 49 I~ 2 Õæig! I 00000444 45 4E 44 AE 42 60 82 50 4B 03 04 14 00 09 00 08 END®B'PK 00000460 00 8B 50 2F 48 46 34 4C AE 1D 00 00 0F 00 00 IP/HF4L@ 00000512 6E 0D DA 0B 3F 5A 17 7A 31 0D 51 6A 78 75 C6 03 n Ú ?Z z1 QjxuÆ 00000544 08 46 34 4C AE 1D 00 00 00 05 04 B01 F4L@ PK 00000544 08 46 34 4C AE 1D 00 00 00 05 04 B01 F4L@ PK 00000544 08 46 34 4C AE 1D 00 00 00 05 04 B01 F4L@ PK 00000540 02 1F 00 14 00 09 00 08 00 8B 50 2F 48 46 34 4C IP/HF4L 00000540 02 1F 00 14 00 09 00 08 00 8B 50 2F 48 46 34 4C IP/HF4L 00000540 02 1F 00 14 00 09 00 00 00 08 00 24 00 00 00 IP/HF4L <t</td><td>00000368</td><td>BB</td><td>5C</td><td>50</td><td>98</td><td>4C</td><td>2D</td><td>Α6</td><td>DC</td><td>8F</td><td>Ε9</td><td>47</td><td>D4</td><td>62</td><td>E 4</td><td>Β1</td><td>88</td><td>»∖P∥L-¦Ü éGÔbä±∥</td></tr><tr><td>00000400 77 05 96 17 D7 B3 15 99 8A 4C AE 3F B9 FC 8F C7 w I ׳ IIL®?¹ü Ç 00000416 6C 43 A6 02 63 96 72 27 33 85 3C E8 9C F6 3C 99 1C¦ cIr'3I<èIč</td> 00000432 26 8C D7 9A 13 A3 09 B2 FF 3D DB 90 79 93 A1 FE &I×I £ ²ÿ=Û yIip 00000448 8B 7E 01 B2 1B 8D D5 E6 69 67 86 00 00 00 00 49 I~ ² ÕæigI I 00000464 45 4E 44 AE 42 60 82 50 4B 03 04 14 00 09 00 88 END®B`IPK 00000460 00 8B 50 2F 48 46 34 4C AE 1D 00 00 00 F 00 00 IP/HF4L® 00000512 6E 0D DA 0B 3F 5A 17 7A 31 0D 51 6A 78 75 C6 03 n Ú ?Z z1 QjxuÆ 00000528 4A 9D 97 A9 B7 5B FC EA 01 CB 7F A5 4F 50 4B 07 J I©·[üė Ě ¥OPK 00000540 02 1F 00 14 00 09 00 08 00 8B 50 2F 48 46 34 4C IP/HF4L 00000576 AE 1D 00 00 00 0F 00 00 00 08 00 8B 50 2F 48 46 34 4C IP/HF4L 00000576 AE 1D 00 00 00 0F 00 00 00 00 00 00 00 00 00 0F 00 00 00 00 9 00000592 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9 9 \$ 00000624 18 00 80 65 27 0E 39 4F 10 1 150 4B 05 06 00 00 0 Ie' 90Ñ ezhdóL </tr</td><td>00000384</td><td>64</td><td>2A</td><td>32</td><td>E5</td><td>ЗF</td><td>8E</td><td>70</td><td>DC</td><td>8F</td><td>99</td><td>FC</td><td>ΒO</td><td>4A</td><td>Α6</td><td>39</td><td>EЗ</td><td>d*2å?∎pÜ ∎ü°J¦9ã</td></tr><tr><td>00000416 6C 43 A6 02 63 96 72 27 33 85 3C E8 9C F6 3C 99 1C¦ clr'3l<èlis<i</td> 00000432 26 8C D7 9A 13 A3 09 B2 FF 3D DB 90 79 93 A1 FE &l×l £ 2ÿ=Û ylip 00000448 8B 7E 01 B2 1B 8D D5 E6 69 67 86 00 00 04 49 I~ 2 Õæigl I 00000444 45 4E 4A AE 2 60 82 50 4B 03 04 14 00 09 00 88 IP/MF4L® 00000440 00 8B 50 2F 48 46 34 4C AE 1D 00 00 00 08 IP/HF4L® 90 97 A9 B7 58 FC EA 01 CB 7F A5 4F 50 4B 01</td><td>00000400</td><td>77</td><td>05</td><td>96</td><td>17</td><td>D7</td><td>BЗ</td><td>15</td><td>99</td><td>8A</td><td>4C</td><td>AE</td><td>ЗF</td><td>Β9</td><td>FC</td><td>8F</td><td>C7</td><td>w∣׳∥L®?¹üÇ</td></tr><tr><td>00000432 26 8C D7 9A 13 A3 09 B2 FF 3D DB 90 79 93 A1 FE & × £ 2ÿ=Û y ip 00000448 8B 7E 01 B2 1B 8D D5 E6 69 67 86 00 00 04 49 × £ 2ÿ=Û y ip 00000444 45 4E 44 AE 42 60 82 50 4B 03 04 14 00 09 00 88 END®B`IPK 00000440 00 8B 50 2F 48 46 34 4C AE 1D 00 00 00 08 1P/HF4L® 00000512 6E 0D DA 0B 3F 5A 17 7A 31 0D 50 4B 07 J I®·[üé É ¥OPK 00000528 4A 9D 97 A9 B7 5B FC EA 01 CB 7F A5 4F 50 4B</td><td>00000416</td><td>6C</td><td>43</td><td>Α6</td><td>02</td><td>63</td><td>96</td><td>72</td><td>27</td><td>33</td><td>85</td><td>ЗC</td><td>E8</td><td>9C</td><td>F6</td><td>ЗC</td><td>99</td><td>1C¦ clr'3KèlöKl</td></tr><tr><td>00000448 8B 7E 01 B2 1B 8D D5 E6 69 67 86 00 00 00 00 49 1^{~ 2} Õæigl I 00000464 45 4E 44 AE 42 60 82 50 4B 03 04 14 00 09 00 08 END®B`IPK 00000480 00 8B 50 2F 48 46 34 4C AE 1D 00 00 00 0F 00 00 0F 00 00 0F 00 00 00000512 6E 0D DA 0B 3F 5A 17 7A 31 0D 51 6A 78 75 C6 03 n Ú ?Z z1 QjxuÆ 00000528 4A 9D 97 A9 B7 5B FC EA 01 CB 7F A5 4F 50 4B 07 J I©·[üė Ë ¥OPK 00000560 02 1F 00 14 00 09 00 08 00 8B 50 2F 00 00 00 07 00 00 00 00 08 00 00 00 0F 00 00 00000560 02 1F 00 14 00 09 00 08 00 8B 50 2F 48 46 34 4C 00 00 00 00 00 00 00 00 00 00 00000576 AE 1D 00 00 00 07 00 08 00 8B 50 2F 48 46 34 4C 1P/HF4L 00000576 AE 1D 00 00 00 07 00 08 00 8B 50 2F 48 46 34 4C 1P/HF4L 00000576 AE 1D 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00000592 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e' 90Ñ ezhdóL 00000624 18 00 80 65 27 0E 39 4F 10 1 15 4B 05 06 00 00 N ezhdóLÑ PK Ie' 90Ñ ezhdóL 000006640</td><td>00000432</td><td>26</td><td>8C</td><td>D7</td><td>9A</td><td>13</td><td>AЗ</td><td>09</td><td>В2</td><td>FF</td><td>ЗD</td><td>DB</td><td>90</td><td>79</td><td>93</td><td>Α1</td><td>FΕ</td><td>&l×l £_²ÿ=Ü yliþ</td></tr><tr><td>00000464 45 4E 44 AE 42 60 82 50 4B 03 04 14 00 09 00 08 END®B' PK 00000480 00 8B 50 2F 48 46 34 4C AE 1D 00 00 0F 00</td><td>00000448</td><td>8B</td><td>7E</td><td>01</td><td>В2</td><td>1B</td><td>8D</td><td>D5</td><td>E6</td><td>69</td><td>67</td><td>86</td><td>00</td><td>00</td><td>00</td><td>00</td><td>49</td><td>I~ ² Öæig∣ I</td></tr><tr><td>00000480 00 8B 50 2F 48 46 34 4C AE 1D 00 00 0F 00</td><td>00000464</td><td>45</td><td>4E</td><td>44</td><td>AE</td><td>42</td><td>60</td><td>82</td><td>50</td><td>4B</td><td>03</td><td>04</td><td>14</td><td>00</td><td>09</td><td>00</td><td>08</td><td>END®B`∎PK</td></tr><tr><td>00000496 00 00 00 34 6E 75 6D 62 65 72 2E 74 78 74 4number.txi 00000512 6E 0D DA 0B 3F 5A 17 7A 31 0D 51 6A 78 75 C6 03 n Ú ?Z 21 QjxuÆ 00000528 4A 9D 97 A9 B7 5B FC EA 01 CB 7F A5 4F 50 4B 07 J I© [üë Ë ¥OPK 00000544 08 46 34 4C AE 1D 00 00 0F 00 00 50 4B 01 F4L® FK 00000560 02 1F 00 14 00 09 00 08 00 24 00 00 00 9 \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$</td><td>00000480</td><td>00</td><td>8B</td><td>50</td><td>2F</td><td>48</td><td>46</td><td>34</td><td>4C</td><td>AE</td><td>1D</td><td>00</td><td>00</td><td>00</td><td>OF</td><td>00</td><td>00</td><td>IP∕HF4L®</td></tr><tr><td>00000512 6E 0D DA 0B 3F 5A 17 7A 31 0D 51 6A 78 75 C6 03 n U ?Z 21 QjxuÆ 00000528 4A 9D 97 A9 B7 5B FC EA 01 CB 7F A5 4F 50 4B 07 J I© [üê E 4OPK 00000564 08 46 34 4C AE 1D 00 00 0F 00 00 50 4B 01 F4L® PK 00000560 02 1F 00 14 00 09 00 80 8B 50 2F 48 46 34 4C IP/HF4L 00000576 AE 1D 00 00 0F 00</td><td>00000496</td><td>00</td><td>ΟB</td><td>00</td><td>00</td><td>00</td><td>34</td><td>6E</td><td>75</td><td>6D</td><td>62</td><td>65</td><td>72</td><td>2E</td><td>74</td><td>78</td><td>74</td><td>4number.tx<mark>t</mark></td></tr><tr><td>00000528 4A 9D 97 A9 B7 5B FC EA 01 CB 7F A5 4F 50 4B 07 J 10:[üê E ¥OPK 00000544 08 46 34 4C AE 1D 00 00 00 0F 00 00 50 4B 01 F4L® PK 00000560 02 1F 00 14 00 09 00 08 00 8B 50 2F 48 46 34 4C IP/HF4L P/HF4L 00000576 AE 1D 00 00 00 0F 00 00 00 0B 00 24 00 00 00 00 00 00 % 00000592 00 00 00 20 00 00 00 00 00 00 00 34 6E 75 6D 62 4numb 00000608 65 72 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00 er.txt 00000624 18 00 80 65 27 0E 39 4F D1 01 65 7A 68 64 F3 4C 1e' 90Ñ ezhdóL 00000640 D1 01 65 7A 68 64 F3 4C D1 01 150 4B 05 06 00 00 Ñ ezhdóLÑ PK 00000656 00 00 01 00 01 00 5D 00 00 00 56 00 00 00 00 00 00 Ie' 90Ñ</td><td>00000512</td><td>6E</td><td>OD</td><td>DA</td><td>ΟB</td><td>ЗF</td><td>5A</td><td>17</td><td>7A</td><td>31</td><td>OD</td><td>51</td><td>6A</td><td>78</td><td>75</td><td>C6</td><td>03</td><td>n U ?Z z1 QjxuÆ</td></tr><tr><td>00000544 08 46 34 4C AE 1D 00 00 0F 00 00 50 4B 01 F4L® PK 00000560 02 1F 00 14 00 09 00 08 85 2F 48 46 34 4C IP/HF4L 00000576 AE 1D 00 00 0F 00 00 08 50 2F 48 46 34 4C IP/HF4L 00000576 AE 1D 00 00 0F 00 00 00 24 00 00 00 08 5 00000592 00</td><td>00000528</td><td>4A</td><td>9D</td><td>97</td><td>Α9</td><td>B7</td><td>5B</td><td>FC</td><td>ΕA</td><td>01</td><td>СВ</td><td>7F</td><td>A5</td><td>4F</td><td>50</td><td>4B</td><td>07</td><td>J ∎©∙[üê E ¥OPK</td></tr><tr><td>00000560 02 1F 00 14 00 09 00 08 00 8B 50 2F 48 46 34 4C IP/HF4L 00000576 AE 1D 00 00 00 0F 00 00 00 0B 00 24 00 00 00 00 00 00 05 00000592 00 00 00 20 00 00 00 00 00 00 00 34 6E 75 6D 62 4numb 00000608 65 72 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00 er.txt 00000624 18 00 80 65 27 0E 39 4F D1 01 65 7A 68 64 F3 4C Ie' 90Ñ ezhdóL 00000640 D1 01 65 7A 68 64 F3 4C D1 01 50 4B 05 06 00 00 Ñ ezhdóLÑ PK 00000656 00 00 01 00 01 00 5D 00 00 00 56 00 00 00 00 00 00 J</td><td>00000544</td><td>08</td><td>46</td><td>34</td><td>4C</td><td>AE</td><td>1D</td><td>00</td><td>00</td><td>00</td><td>OF</td><td>00</td><td>00</td><td>00</td><td>50</td><td>4B</td><td>01</td><td>F4L® PK</td></tr><tr><td>00000576 AE 1D 00 00 00 00 00 00 00 02 00 <</td><td>00000560</td><td>02</td><td>1F</td><td>00</td><td>14</td><td>00</td><td>09</td><td>00</td><td>08</td><td>00</td><td>8B</td><td>50</td><td>2F</td><td>48</td><td>46</td><td>34</td><td>4C</td><td>∎P⁄HF4L</td></tr><tr><td>00000592 00 00 00 00 00 00 00 00 03 4 E 75 6D 62 4numb 00000608 65 72 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00 er.txt 00000624 18 00 80 65 27 0E 39 4F D1 01 65 7A 68 64 F3 4C Ie' 90Ñ ezhdóL 00000640 D1 01 65 7A 68 64 F3 4C Ie' 90Ñ ezhdóL 00000656 00 00 01 00 5D 00</td><td>00000576</td><td>AE</td><td>1D</td><td>00</td><td>00</td><td>00</td><td>OF</td><td>00</td><td>00</td><td>00</td><td>OB</td><td>00</td><td>24</td><td>00</td><td>00</td><td>00</td><td>00</td><td>® \$</td></tr><tr><td>00000608 65 72 2E 74 78 74 0A 00 20 00 00 00 01 00 er.txt 00000624 18 00 80 65 27 0E 39 4F D1 01 65 7A 68 64 F3 4C 1e' 90Ñ ezhdóL 00000640 D1 01 65 7A 68 64 F3 4C D1 01 50 4B 05 06 00 00 N ezhdóL 00000656 00 00 01 00 5D 00</td><td>00000592</td><td>00</td><td>00</td><td>00</td><td>20</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>34</td><td>6E</td><td>75</td><td>6D</td><td>62</td><td>4numb</td></tr><tr><td>00000624 18 00 80 65 27 0E 39 4F D1 01 65 7A 68 64 F3 4C 1e' 90N ezhdóL 00000640 D1 01 65 7A 68 64 F3 4C D1 01 50 4B 05 06 00 0 N ezhdóL 00000656 00 00 01 00 5D 00 00 00 00 00 00 0</td><td>00000608</td><td>65</td><td>72</td><td>2E</td><td>74</td><td>78</td><td>74</td><td>ΟA</td><td>00</td><td>20</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>01</td><td>00</td><td>er.txt</td></tr><tr><td>00000640 D1 01 65 7A 68 64 F3 4C D1 01 50 4B 05 06 00 00 N ezhdóLN PK 00000656 00 00 01 00 01 00 5D 00 00 00 56 00 00 00 00 00] V</td><td>00000624</td><td>18</td><td>00</td><td>80</td><td>65</td><td>27</td><td>ΟE</td><td>39</td><td>4F</td><td>D1</td><td>01</td><td>65</td><td>7A</td><td>68</td><td>64</td><td>FЗ</td><td>4C</td><td>_ le' 90Ñ ezhdóL</td></tr><tr><td>00000656 00 00 01 00 01 00 5D 00 00 00 56 00 00 00 00 00] V</td><td>00000640</td><td>D1</td><td>01</td><td>65</td><td>7A</td><td>68</td><td>64</td><td>F3</td><td>4C</td><td>D1</td><td>01</td><td>50</td><td>4B</td><td>05</td><td>06</td><td>00</td><td>00</td><td>N ezhdóLN PK</td></tr><tr><td>ntrost/nood.csdn.net/atanza</td><td>00000656</td><td>00</td><td>00</td><td>01</td><td>00</td><td>01</td><td>00</td><td>5D</td><td>00</td><td>00</td><td>00</td><td>56</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>] V s://blog.csdn.net/afanzo</td></tr></tbody></table>																		

发现里面有一个txt文件。

猜想应该是涉及到了分离工具foremost。

但是电脑没装kali,于是把后缀改为zip试试。

🧱 QR_code.zip - WinRAR (非商业个人版)

文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)



https://blog.csdn.net/afanzcf

居然打开了,但是可以看到这个txt需要密码,根据它文件名的提示,我们知道这是一个4位数的密码,于是用Ziperrllo暴力破解密码。

7 Ziperello				—	
ziperello zip password	l recovery tool		帮助	关于	退出
当 当 逝去时间: 00:00:01	前密码长度 前密码 前速度 7% 开如	4 7639 3113938密码/秒 剩余时间: 00:00:28 台 停止	准备就绪,请点击[开 注意:搜索进度条 (% 前的密码效验长度相关 耗时较长。	步骤 4 始] 按钮) 及剩余时间字段(5。破解 AES 算法;	显示的信息与当 加密的密码可能
11:11:31:密码 : "7639" .时间: 2 s					
Ziperello ver. 2.1 得到密码7639,然后打开txt,行	版权所有 (C) 2008 FDF 得到flag。	步骤 4 / 4: 破解密码.Go RLab		https://bio	NEXT



flag{vjpw_wnoei}

4、BUUCTF N种方法解决(base64转图片、直接网址打开)

下载题目附件之后,得到了一个exe文件,准备打开这个exe,却发现打不开。用PE查一下。

File : KE	Y.exe				🔑 н	
Entry Point :	?	00 <	EP Section :	?	-	_
File Offset :	?]	First Bytes :	64.61.74.61.3A		
Linker Info :	?]	SubSystem :	?		
File Size 🦕	00000F1Eh	< N	Overlay :	?		
Diagnose:						

发现并不是exe文件,用winhex打开。

KEY.exe																		
KEY.exe																		
Offset	0	1	2	3	4	- 5	6	- 7	8	- 9	10	11	12	13	14	15	ANSI ASCII	_
00000000	64	61	74	61	ЗA	69	6D	61	67	65	2F	6A	70	67	ЗB	62	data:image/jpg;b	
00000016	61	73	65	36	34	2C	69	56	42	4F	52	77	30	4B	47	67	ase64,iVBORwOKGg	
00000032	6F	41	41	41	41	4E	53	55	68	45	55	67	41	41	41	49	oAAAANSUhEUgAAAI	
00000048	55	41	41	41	43	46	43	41	59	41	41	41	42	31	32	6A	UAAACFCAYAAAB12j	
00000064	73	38	41	41	41	41	41	58	4E	53	52	30	49	41	72	73	s8AAAAAXNSR0IArs	
00000080	34	63	36	51	41	41	41	41	52	6E	51	55	31	42	41	41	4c6QAAAARnQU1BAA	
00000096	43	78	6A	77	76	38	59	51	55	41	41	41	41	4A	63	45	Cxjwv8YQUAAAAJcE	
00000112	68	5A	63	77	41	41	44	73	4D	41	41	41	37	44	41	63	hZcwAADsMAAA7DAc	
00000128	64	76	71	47	51	41	41	41	72	5A	53	55	52	42	56	48	dvqGQAAArZSURBVH	
00000144	68	65	37	5A	4B	42	69	74	78	49	46	67	54	76	2F	33	he7ZKBitxIFgTv/3	
00000160	39	36	54	78	35	36	34	47	31	55	6F	75	69	63	4B	67	96Tx564G1UouicKg	
00000176	31	39	68	77	50	43	44	63	72	4D	4A	39	6D	37	2F	37	19hwPCDcrMJ9m7/7	
00000192	6E	34	35	7A	66	64	78	65	35	5A	33	73	4A	37	70	72	n45zfdxe5Z3sJ7pr	
00000208	48	62	66	39	72	58	4F	33	50	34	6C	4C	76	59	50	63	Hbf9rX03P41LvYPc	
00000224	74	62	65	4D	38	30	64	76	74	50	2B	33	70	6E	44	70	tbeM80dvtP+3pnDp	
00000240	39	79	46	37	74	6E	65	51	76	76	6D	63	5A	75	2F	32	9yF7tneQvvmcZu/2	
00000256	6C	66	37	38	7A	68	55	2B	35	69	39	79	78	76	34	54	lf78zhU+5i9yxv4T	
00000272	33	54	32	4F	30	2F	37	65	75	64	36	38	4F	54	32	48	3T200/7eud680T2H	
00000288	33	4C	43	66	74	30	6C	2F	61	65	39	5A	6C	54	6F	2B	3LCft01/ae9Z1To+	
00000304	32	33	70	50	76	58	37	2F	72	77	4A	48	62	66	63	73	23pPvX7/rw.THbfcs	

发现并不简单,类似于base64,但是又有图片。想到了base64转图片。

用notepad打开文件。



全选复制。

(1) 直接拉到网站打开



扫描二维码,得到flag。

(2) 在线base64转图片

base64图片在线转换工具 - 站长工具 (chinaz.com)

在线调色板	网页常用色彩	中日传统色彩	传图识色	WEB安全色	网页颜色选择器	颜色代码查询、	RGB颜色值	base6	4图片在线转换工具	
					In IJpM IYP/ O1y9PH7KF +zySpMyVt Mv7WD3LS +paTtk9O7 3dc3rw8nzE Omb72pYfz Y3/LT8H301 6DlfvfsTcJLL mxvt3yqWE Jyf61+/68CI eUtvLfrO1y2 nE8hbe2/Uc	K/I8PWI//tJ2Yb3J tttbfhq+zySpMyV br7D1cvjp2yxveV fsU8P6lpO2T07v 1s11/P7EnOTWG i1iucG9SVJnarR9 cn1rf8NHwffXXW VkfTpibpM13Na J50e6tbzlhf1diO /Z3J2YT9uk7XL1 Z3/Kn4ftNYrlhe PH7K05y+z3sm dzv9X+sy/OP/88	vv8Pd/il+WWi /tbr7D1cvjp2y: Vn4ftMkjpT0u WxPXcy/tYPct. Svb5LUmRptr wv2n+/rm9eg //mxPrW34av WGfvsPVux8xh +1GDJX8avti 8vJif71uz48id2 8vJif71uz48id2 svJif32n6uX 1/SqtvcdpBh+	sswb//D3 weWn4ftM bmO1y9ftf h+XTw/gW 3D/6b6+e EuUksN7g 3r7+bE+p o++QuVD 18lubrR761 J8lubrR761 J8lubrR761 J8lubrR761 J3/Gn4fpN x095mtP3 wAAAABJF	V8ptlliucG9+Q5//6f4, AkjpT0ubmO1y9H7K Ag9y0n7FPD+paTtk9 k7ZPTu9bE9dzL+1g9 X04YW4Syw3uTZI6U 3SepMjbZPu990X9+t afhu+jr876cMLcJG2+ CXOT7OZGu7e+5YT9 tO2N+VWE7Yp+9w5 6F+/680T2H3Ln4bvf Ybtjecnkif/3+++HTn ec8klrfw3q7vcPXy+C RU5ErkJggg==	ZYNIBVIM ⟨Fttbfhq Q71sT13 y0n7FPD J6PtE+4/ 8PptwNN g2H93Zx XYnIhH3 9e5HzE2y N4nIhu0t ub0fd4zi IPc/o+75
*请上传小于300	(B的.jpg/.jpeg/.gif/.k	omp/.png/.ico格式图	3片,不建议将大图	转换。			图片转成	Base64	Base64还原图片	清空结果

扫描二维码,得到flag

KEY{dca57f966e4e4e31fd5b15417da63269}

5、你竟然赶我走(winhex、Stegsolve)

(1) 自己靠运气解出(解法一winhex)

下载附件之后,一个压缩包,解压之后,打开一张图片,并没有什么消息。用winhex打开。

	hex biubiu.j	pg																					
	Offset	0	1	2	3	4	- 5	6	- 7	8	- 9	10	11	12	13	14	15			ANS]	ASC	II	1
	00000000	FF	D8	FF	ΕO	00	10	4A	46	49	46	00	01	01	00	00	01	ÿØÿ	żà ,	JFI	7		
	00000016	00	01	00	00	FF	DB	00	43	00	03	02	02	03	02	02	03		ÿU	IС			
	00000032	03	03	03	04	03	03	04	05	08	05	05	04	04	05	ΟA	07						
	00000048	07	06	08	OC	ΟA	OC	OC	ΟB	ΟA	ΟB	ΟB	OD	ΟE	12	10	OD						
	00000064	OE	11	ΟE	OB	OB	10	16	10	11	13	14	15	15	15	OC	OF						
	00000080	17	18	16	14	18	12	14	15	14	FF	DB	00	43	01	03	04			Ś	in c		
	00000096	04	05	04	05	09	05	05	09	14	OD	OB	OD	14	14	14	14						
	00000112	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14						
	00000128	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14						
	00000144	14	14	14	14	14	14	14	14	14	14	14	14	14	14	FF	CO					ÿΑ	
	00000160	00	11	08	01	BC	01	88	03	01	22	00	02	11	01	03	11		. 14	۰ ۱			
	00000176	01	FF	C4	00	115	00	00	01	05	01	01	01	01	01	01	00	y y f	7				
	00000192	00	00	00	00	00	00	00	01	02	03	04	05	06	07	08	09	is://h	lac.				
	00000208	UA	UВ	Γŀ	C4	υu	85	10	υυ	UΖ	UI	UJ	UJ	UΖ	04	UJ	05	2	7A≊µ	l			
看到一个FF	D8,ipg的一个	ト文イ	牛头	, 我	本	を想	找一	下in	oa的	文件	尾,	FFI	09的	1 ,	武直	接お	行到量						
	00025312	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@	00	00	00	0	
	00025328	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	0	Q@	Q@	Q@	ô	
	00025344	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	0	Q@	Q@	Q@	<u>õ</u>	
	00025360	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	0	Q@	Q@	Q@	Q	
	00025376	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	0	Q@	Q@	Q@	Q	
	00025392	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	0	Q@	Q@	Q@	Q	
	00025408	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	0	Q@	Q@	Q@	Q	
	00025424	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	0	Q@	Q@	Q@	Q	
	00025440	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	0	Q@	Q@	Q@	Q	
	00025456	40	05	14	51	40	05	14	51	40	1F	FF	D9	2D	2D	2D	A1	0	Q@	Q@	ÿÙ	– i	
	00025472	Β7	66	6C	61	67	20	49	53	20	66	6C	61	67	7B	73	74	•f1	ag	IS f	lag{	st	
	00025488	65	67	6F	5F	69	73	5F	73	30	5F	62	6F	72	31	69	6E	ego	_is	_s0_	bor1	in	
	00025504	67	7D															g}					
																							of.

发现了flag?复制到,BUUCTF,对了。。。

flag{stego_is_s0_bor1ing}

这里直接winhex里面十六进制搜索FFD9,也能出来

			∎ ••••• N×FF ≫R .	
biubiu.jpg				
HEX biubiu ing				
位署管理哭 (仝部)				2 16日
Offset ▲ 搜索结果		时间		2 项口
25466 FFD9		2021/08/18		
6816909 flag		2021/08/15		
Offset 0 1 2 3 00025344 40 05 14 51	4 5 6 7 8 9 10 40 05 14 51 40 05 14	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	ANSI ASCII	biubiu.jpg
00025360 40 05 14 51 00025376 40 05 14 51	40 05 14 51 40 05 14 40 05 14 51 40 05 14 40 05 14 51 40 05 14 40 05 14 51 40 05 14	51 40 05 14 51 @ Q@ 51 40 05 14 51 @ Q@	Q@ Q@ Q Q@ Q@ Q	C:\Users\86131\De
00025392 40 05 14 51 00025408 40 05 14 51 00025424 40 05 14 51	40 05 14 51 40 05 14 40 05 14 51 40 05 14 40 05 14 51 40 05 14 40 05 14 51 40 05 14	51 40 05 14 51 @ Q@ 51 40 05 14 51 @ Q@ 51 40 05 14 51 @ Q@	Q@ Q@ Q Q@ Q@ Q	25,506 字节
00025440 40 05 14 51	40 05 14 51 40 05 14 40 05 14 51 40 1F FF	51 40 05 14 51 @ Q@ 09 20 20 20 A1 @ 0@	Q@Q@Q 0@ <mark>00</mark> 1i	缺省编辑模式
00025472 B7 66 6C 61	67 20 49 53 20 66 6C	61 67 7B 73 74 •flag	IS flag{st	状态: 原始的
00025488 65 67 6F 5F 00025504 67 7D	69 73 5F 73 30 5F 62	6F 72 31 69 6E ego_is g}	s_s0_borlin	撤消级数: 0反向撤消: 暂无信息
				创建时间21/08/18 15:14:13
				最后写双时间:1/13 16:20:15
			~	属性: A 图标: 0
页 76 / 76	偏移地址: 25,466	= 255 选块:	25,481 - 25,505	5 大小: create net/ai/25

(2) 解法二(Stegsolve)

用Stegsolve打开图片,



然后用这个打开。

🕌 File Format Ana			\times	\times
Humman table				i
Length: b5 (181)				
				_
Start of scan				
Header Length: c (12)				
Detected 24843 bytes in scan				
End of Image				
Additional bytes at end of file = 38				
Dump of additional bytes:				
Hex:				
2d2d2da1b7666c61 6720495320666c	61			
677b737465676f5f 69735f73305f626	f			
7231696e677d				
Ascii:			=	
fla g IS fla				
g{stego is s0 bo				
r1ing}			-	
ОК	itips://blo	g.csdn.nei	i/aifainz	¢Ť.

得到flag。

6、大白(winhex修改图片的高度)

大白

看不到图? 是不是屏幕太小了注意:得到的 flag 请包上 flag{} 提交

📥 379140b0-c...

https://blog.csdn.net/afanzcf

首先看到图片,便知道,这可能是一道修改图片高度的题目。

打开文件一看,果然如此。



https://blog.csdn.net/afanzcf

可以看出图片,还有一大截没有露出来。拖入winhex中。

第一行是文件头,第二行的前四个字节是图片的宽度,后面的四个字节是图片的高度。

🔛 dabai.pi	ng																		
Offset	0	1	2	3	4	- 5	6	- 7	8	- 9	10	11	12	13	14	15		ANSI	ASCII
00000000	89	50	4E	47	OD	ΟA	1A	ΟA	00	00	00	OD	49	48	44	52	∎ PNG		IHDR
00000016	00	00	02	A7	00	00	01	00	08	06	00	00	00	6D	7C	71	S		m q

将01改为A7.保存更新之后,得到falg



flag{He1I0_d4_ba1}

7、基础破解(ARCHPR、base64解密)

基础破解

1

给你一个压缩包,你并不能获得什么,因为他是四位数字加密 的哈哈哈哈哈哈哈。。。不对==我说了什么了不得的东 西。。注意:得到的 flag 请包上 flag{}提交

📩 5e46643e-b		
Flag		提交

https://blog.csdn.net/afanzcf

从题目看来,应该是要暴力破解了,且密码是4位数字。

打开ARCHPR,暴力破解。

	_	\times	13								
F) 恢复(R) 帮助(H)											
;. 🔊 🔏 🔇 🥸 🕡											
打开 开始! 停止 基准测试 升级 帮助 关于											
10家的200000000000000000000000000000000000											
sword Recovery 统计	信息:										
3,565											
总计时间 11s 129ms											
平均速度(口令/秒) 320											
这个文件的口令 2563											
十六进制口令 32 35 36 33											
保存 ✔ 确定											
31\Desktop\基础碳解	≩.rar″已打开。	^									
2021/8/18 16:10:50 - 开始暴力攻击 2021/8/18 16:11:01 - 口今已成功恢复!											
2021/8/18 16:11:01 - '2563' 是这个文件的一个有效口令											
当前口令: 2563 平均速度: 320 p/s 已用时间: 11s 剩余时间: 23s 口令长度 = 4, 总计: 10,000, 已处理: 2,565											
25%											
oft Co. Ltd.	https://blog.cs	dn.net/afan:	zof								
	試 升级 帮 Tb ± 346 TUIL Tb ± 346 TUIL SSWORD Recovery 统计 3,565 11s 129ms 320 2563 32 320 2563 323 35 36 33 ✓ 31\Desktop\基础破解 的一个有效口令 平均速度: 剩余时间: 55 25% oft Co. Ltd.	id	→ →								

得到解压密码,2563.

🧾 flag.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

ZmxhZ3s3MDM1NDMwMGE1MTAwYmE30DA20DgwNTY2MWI5M2E1Y30=

https://blog.csdn.net/afanzcf

给的txt,一看就是base64了,直接解密。

Base64 在线编码解码 | Base64 加密解密 - Base64.us

Base64.us Base64 在线编码解码 (最好用的 Base64 在线工具	Ę)
Base64 URLEncode MD5 TimeStamp	
请输入要进行 Base64 编码或解码的字符	
ZmxhZ3s3MDM1NDMwMGE1MTAwYmE3ODA2ODgwNTY2MWI5M2E1Y30=	
编码 (Encode) 解码 (Decode) ↓ 交换 (编码快捷键: Ctrl + Enter)	
Base64 编码或解码的结果:	
flag{70354300a5100ba78068805661b93a5c}	

得到flag。

flag{70354300a5100ba78068805661b93a5c}

8、BUUCTF misc第八题(winhex、Stegsolve)

下载之后,又是一个jpg,同5、你竟然赶我走的解法一样。

(1) winhex直接拖到尾

00020752 |98 1D 69 AA AC BC 97 CO 27 OO 1A 9E 24 12 OD CD | I i≧¬¼IÅ' 1\$ İ C9 A9 36 81 8E FF 00 5A A0 20 F9 FB 50 65 20 E0 |ɩ6 |ÿ Z ùûPe à 00020768 00020784 A9 AB 48 8A D8 24 75 A1 E1 41 CD 02 2A 34 83 A7 ©≪H∣0\$uiáAÍ *4∣§ 00020800 AF 4A 68 5C FC C4 55 B1 04 64 72 29 8D 02 2E 76 ⁻Jh∖üÄU± dr) .v E4 7D 0D 00 45 E5 AB 75 03 F9 51 E5 11 F7 5D C7 ä} Eå≪u ùQå ÷]Ç 00020816 E3 9F E7 48 46 D6 1C E7 9A 90 75 EA 69 01 13 47 00020832 ãlçHFÖ çl uêi G 00020848 29 18 OE BF 5C 73 FF OO EB A5 43 E5 61 42 90 3D) č∖sÿ ë¥CåaB = s**lll**¼k in rL g 00020864 73 9A 94 8E BC 9A 6B A8 A1 6E 04 72 4C 81 09 67 00020880 OA 07 AD 50 03 32 34 99 E5 CF 4C F0 3E 95 66 55 -P 24∎åÏLð>∎fU ∖ I8 ÅÝÓ JÑ I 06 5C 1E 8A 38 15 16 C5 DD D3 1F 4A D1 20 1F 9F 00020896 7A 29 DE 5A FB D1 4F 51 z)ÞZúÑOQ ÿÙ fla 00020912 1F FF D9 OD OA 66 6C 61 00020928 67 7B 39 37 33 31 34 65 37 38 36 34 61 38 66 36 g{97314e7864a8f6 00020944 32 36 32 37 62 32 36 66 33 66 39 39 38 63 33 37 2627b26f3f998c37 00020960 66 <mark>3</mark>1 7D f1}

https://blog.csdn.net/afanzcf_

(2) Stegsolve



flag{97314e7864a8f62627b26f3f998c37f1}

9、BUUCTF 第九题LSB(Stegsolve、QR Research)

下载附件之后,打开是一个png图片,拿到图片之后,打开winhex,发现文件头89504E47,正确,文件尾,AE426082,正确。 而且没有在winhex中直接发现flag。于是用Stegsolve打开,查看文件信息,也没有发现flag。

然后怀疑是不是把图片的宽和高修改了,于是在winhex中,找到第二行,修改宽和高,保存之后,直接图片打不开了。。。

常规的图片题,如今方法都失败了,也没有查到在图片里面有其他文件。

用了Stegsolve的分离图片功能,但是我是一个一个勾选的,且没有注意分离出来的信息。

借鉴了一下wp,发现自己在Stegsolve工具上漏了一个功能。

DATA分离的那个(这里本来有一张图的,但是审核多次不通过,说我政治的问题,想不明白)

\$	- 🗆 X										
Extract Preview											
Bit Planes	Order settings										
Alpha 7 6 5 4 3 2 1 0	Extract By Row Column										
Red 7 6 5 4 3 2 1 0	Bit Order 💿 MSB First 🔾 LSB First										
Green 7 6 5 4 3 2 1 0	Bit Plane Order										
Blue 7 6 5 4 3 2 1 0	 RGB GRB RBG BRG 										
Preview Settings Include Hex Dump In Preview 🔽	⊖ gbr ⊖ bgr										
Preview Save Text Save Bin Cancel https://blog.csdn.nei/afanzdi											

打开之后,发现有几个颜色通道。

	Х
Extract Preview	
89504e470d0ala0a 0000000d49484452 .PNGIHDR	
0000011800000118 08020000008ec7e~	=
db00000542494441 54789ceddd416e23BIDA TxAn#	
391000416931ffff b2f707c480932e57 9AilW	
cb1157c3564b5682 8702c9f7d7d7d70bVKV	
183/1111d1403c027 1012048404012141 .7'!A	
f77bac30720383a6 c30775788cbbdfca / 0r	
e5ffe5bbb7bcdff9_9f62458280902020bE	
2408080902428280 9020202408080902 \$B \$	
	•
Bit Planes Order settings	
Alpha 7 6 5 4 3 2 1 0 Extract By Row Column	
Red 7 6 5 4 3 2 1 0 Bit Order MSB First LSB First	
Green 7 6 5 4 3 2 1 1 0 Pit Plane Order	
bit Plaile Older	
Blue 7 6 5 4 3 2 1 0 0 RGB GRB	
Preview Settings	
Include Hex Dump In Preview 🖌	
Preview Save Text Save Bin Cancel https://blog.csdn.net/afa	

三个都选了之后,Preview,拖到最上面,发现了有一个信息是png。也就是说,隐藏着一张图片了。

直接保存为xxx.png。然后打开,发现是一张二维码图片。

🔡 QR Research			_		\times
文件(E) 工具(I) 帮助(H)					
	» 📀				
		→		俺码─ Auto 尺寸─ 4	•
					^
					~
已解码数据 1:					^
位置:(9.0,9.0)-(270.0,9.0)-(9.0,270 颜色正常,正像 版本: 3 纠错等级:H, 掩码:4 内容: <u>cumtctf{1sb_i4_s0_Ea4y}</u>).0)-(270.0,270.0	-)) -			
			https://blo	g.asdn.na	el/alfanzel

flag{1sb_i4_s0_Ea4y}

10、文件中的秘密(Stegsolve、winhex)

(1) 方法一(Stegsolve)

直接打开文件之后,发现是一张jpeg的图片。话不多说,直接用Stegsolve打开图片。



在查看图片具体信息的中间的位置,发现了flag。复制出来之后,将中间的.删去。

得到flag。

flag{870c5a72806115cb5439345d8b014396}

(2) 方法二 (winhex)



直接winhex里面文本搜索flag。得到flag。

11、wireshark (wireshark)

下载附件之后,是一个pcapng文件,用wireshark打开。

由于目前做这种流量包的题,我就一种方法,搜索字符串。

所以直接搜索字符串flag。



直接查找到flag。

>	Tr	ansm:	iss	ion	Со	ntro	51 I	Pro	tocol,	Sro	: Po	rt:	22	494,	Ds	st	Port:	80,	Seq:	1,	Ack:	1,
>	> Hypertext Transfer Protocol																					
~	HTML Form URL Encoded: application/x-www-form-urlencoded																					
	✓ Form item: "email" = "flag"																					
	Key: email																					
	Value: flag																					
	>	Form	it	em:	"p	ass	wor	'd''	= "ff	0756	7a1	d4f4	labo	lffd	b54	e02	22f8fa	cd"				
	>	Form	it	em:	- ۲	ant	cha	" =	BYU	;" ;"												
	·							·														
0	2a0	31	61	37	33	32	64	65	61 3	5 39	37	61	35	65	63	39	1a7	32dea	a 597	a5e	c9	
0	2b0	34	63	3d	31	34	33	35	35 3	9 30	35	37	34	Ød	0a	43	4c=	1435	5 905	74 ·	- C	
0	2c0	6f	6e	6e	65	63	74	69	6f 6	e 3a	20	6b	65	65	70	2d	onn	ecti	o n:	kee	p-	
0	2d0	61	6c	69	76	65	0d	0a	43 6	f 6e	74	65	6e	74	2d	54	ali	ve(C ont	ent	-Т	
0	2e0	79	70	65	3a	20	61	70	70 6	c 69	63	61	74	69	6f	6e	уре	: ap	o lic	ati	on	
02	2 f 0	2f	78	2d	77	77	77	2d	66 6	f 72	6d	2d	75	72	6c	65	/x-	WWW	f orm	ı-ur	le	
03	300	6e	63	6f	64	65	64	0d	0a 4	3 6f	6e	74	65	6e	74	2d	nco	ded -	- Cor	ten	t-	
03	310	4c	65	6e	67	74	68	3a	20 3	6 35	0d	0a	0d	0a	65	6d	Len	gth:	65 ·	•••	em	
03	320	61	69	6c	3d	66	6c	61	67 2	670	61	73	73	77	6f	72	ail	=fla	g &pa	SSW	or	
03	330	64	3d	66	66	62	37	35	36 3	7 61	. 31	64	34	66	34	61	d=f	fb75	5 7a1	.d4f	4a	
03	340	62	64	66	66	64	62	35	34 6	5 30	32	32	66	38	66	61	bdf	fdb54	4 e02	2f8	fa	
03	350	63	64	26	63	61	70	74	63 6	8 61	. 3d	42	59	55	47		cd8	capt	c∍ha=	BYU	Gnet/at	

可以看到, email = flag, password = ffb7567a1d4f4abdffdb54e022f8facd

我们就得到了

flag{ffb7567a1d4f4abdffdb54e022f8facd}

12、rar (ARCHPR)

首先看到提示信息。

题目

解题快手榜

X

rar

1

这个是一个rar文件,里面好像隐藏着什么秘密,但是压缩包 被加密了,毫无保留的告诉你,rar的密码是4位纯数字。注 意:得到的 flag 请包上 flag{}提交



https://blog.csdn.net/afanzcf

提示的太明显了。秘密是四位的纯数字,那么直接暴力破解。

🔏 ARC	HPR 4.54	- 87%			_	_	\times			
文件(F)	恢复(R)	帮助(H)								
R	A		3	1	2					
打开	• <i>•</i> /// 开始!	停止	基准测试	升级	帮助	关于	退出			
				<u></u>	al					
口令日	成功恢复!						×			
		Advanced A	rchive Passw	ord Recover	r <mark>y</mark> 统计信息	(:	_			
总计	口令		9,	797						
总计时间 33s 477ms										
平均	平均速度(口令/秒) 292									
这个:	文件的口令		87	795			<u> </u>			
<u> +</u>	进制口令		38	3 37 39 35			_ 4			
l.		保存			💙 确定	Ē				
1/VOIB	A ALE MICO	T10076 001	50707							
2021/8	3/18 17:12:1	- 10076_201 8 - 开始暴力	.50/0/_rar.n	ar已打开。						
2021/8/18 17:12:51 - 口令已成功恢复! 2021/8/18 17:12:51 - '8795' 是这个文件的一个有效口令										
当前口谷): 8	3795		平均速度	: 29	2 p/s				
口令长月]. 夏 = 4, 总计	: 10,000, 已;	处理: 8,797	潮赤时间	5					
			87	7%						
		/ >		- · · · ·	5.60	and later and	In meddedenerer			

ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

压缩包秘密, 8975得到

解压。直接就是flag.txt。打开就是flag

🥘 flag.txt	- 记事本								
文件(F) 编辑	冒(E) 格式(O)	查看(V)	帮助(H)						
flag	$\{1773c$	c5da	1790ł	od3ca	aff	38e3	decd	180et	$\mathbf{b7}$

https://blog.csdn.net/afanzcf

flag{1773c5da790bd3caff38e3decd180eb7}

总结

花了一个上午和下午的时间,做完了这十二道题,随着在攻防世界新手练习区Misc的经验积累,以及自己对很多工具的了解之后,做这十二道题,倒也是比较轻松了。从这十二道题来说,大部分题目是跟图片有关的,

(1) 跟图片有关,那么两个工具,

一个是winhex,一个是Stegsolve,首先问winhex看看,图片里面有没有被隐写其他的文件,然后如果感觉图片的宽高被改写,那么使用winhex直接改写,还有就是有的题目,直接将flag写在了图片中,在winhex中直接搜索flag即可,或者使用Stegsolve的 查看信息功能,查看也行。

(2) 如果是跟rar, zip有关,

根据题目告诉的密码提示,直接使用工具暴力破解密码即可,虽然现在大部分密码还是四位数的简单密码,但是至少在脑海中, 也是要有这个思路才行。

(3) 还有一个题倒是需要使用wireshark工具,

但是也还算是简单题目,直接搜索字符串flag就行,之前在攻防世界遇到一个wireshark的题目,是在搜索flag之后,查找到了其他几个文件,比如xxx.txt,xxx.jpg,这时候就需要先使用foremost先分离文件之后,再解题了。

这是目前我所遇到的Misc题目的一些思路,随着自己的做题,后面遇到的题目和脑洞也会越来越大,继续加油啊。