# HGAME 2021 WEEK 4 WRITE UP



# MISC

## Akira之瞳-1

解压下载的压缩包，得到`important_work.raw`。第一反应是相机原片。用`PS`打开是一坨不知道什么东西。搜索之后了解到内存取证这种东西，按照教程使用`Volatility`工具尝试对该文件进行解析。

> volatility -f important_work.raw imageinfo

首先判断系统。输入上述命令提示多个可能的系统，验证后确认操作系统为`Win7SP1x64`

> volatility -f important_work.raw --profile=Win7SP1x64 psscan

查看内存中的进程。发现有名一个为`important_work`的进程，与`.raw`文件名字相同，十分可疑。

> volatility -f important_work.raw --profile=Win7SP1x64 memdump -p 1092 --dump-dir=dump_dir

从内存中通过PID，将该进程dump至dump_dir目录下。获得`1092.dmp`。

使用`binwalk`对`1092.dmp`进行分析，读取到非常多文件头信息。在靠前位置读取到三个ZIP文件信息。

> 1155104 0x11A020 Zip archive data, at least v2.0 to extract, name: Liz to Aoi Bird/
> 1155150 0x11A04E Zip archive data, encrypted at least v2.0 to extract, compressed size: 12061353, uncompressed size: 12686717, name: Liz to Aoi Bird/Blind.png
> 13216558 0xC9AB2E Zip archive data, encrypted at least v2.0 to extract, compressed size: 11383965, uncompressed size: 11408307, name: Liz to Aoi Bird/src.png

发现其中有两个`.png`。结合题目中*原画师*，该压缩包高度可疑。使用`WinHex`提取出该压缩包。

打开压缩包，发现需要密码。压缩包的详细信息中有如下提示

> Password is sha256(login_password)

也就是需要找到当前用户的登录密码。

> volatility -f important_work.raw --profile=Win7SP1x64 printkey -K "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"

使用以上命令查看用户及最后登陆时间等信息。显示有且仅有名为`Genga03`的用户在近日登陆。要找的用户就是他了。

> volatility -f important_work.raw --profile=Win7SP1x64 hivelist

从注册表中获取`SYSTEM`和`SAM`的 Virtual 地址

> volatility -f .\important_work.raw --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a000bc3410

(两个参数依次为SYSTEM和SAM) 得到

> Genga03:1001:aad3b435b51404eeaad3b435b51404ee:84b0d9c9f830238933e7131d60ac6436:::

其中`84b0d9c9f830238933e7131d60ac6436`为`Genga03`登陆密码的哈希值。在https://cmd5.com/查询得到原密码，进行`sha256`加密后，即得到压缩包密码。

解压后得到`Blind.png`和`src.png`。两图片肉眼观察相同；前者占用空间较大。

双图隐写，看到过好多次但从来没有考过。使用`stegsolve`的插件进行尝试，一无所获。

再次注意到文件名`Blind`，查询后发现有名为`盲水印`隐写方式，似乎是什么暗示。使用`BlindWaterMark`工具提取出水印。水印即为Flag，但实在太花难以分辨，问学长要了。