

Gitty RSA 解答

题目：

■ *We find some suspicious activities in our organization's network...*

找到流量中的目标

题目给了一个名叫 `out.pcapng` 的文件，可以看出它是一个流量截获文件：

找到约 87,500 条结果 (用时 0.33 秒)

<https://github.com> > pcapng > pcapng ▾ 翻译此页

PCAP Next Generation (pcapng) Capture File Format - GitHub

The pcap and **pcapng** specifications are written using the kramdown superset of Markdown and the kramdown-rfc2629 extensions to kramdown. This allows ...

<https://wiki.wireshark.org> > Development > Pc... ▾ 翻译此页

Development/PcapNg - The Wireshark Wiki

2018年9月28日 — **PcapNg**. The PCAP Next Generation Dump File Format (or **pcapng** for short) is an attempt to overcome the limitations of the currently widely used ...

[Malformed pcapng Files](#) · [Options working](#) · [Wishlist](#)

<https://pcapng.github.io> > pcapng ▾ 翻译此页

pcapng/pcapng master preview

Editor's drafts for master branch of **pcapng/pcapng**. View saved issues, or the latest GitHub issues and pull requests. [draft-gharris-opsawg-pcap.html](#) · [plain text](#) ...

<https://blog.csdn.net> > article > details ▾

wireshark的pcapng的文件格式_yang_chen_shi_wo的博客 ...

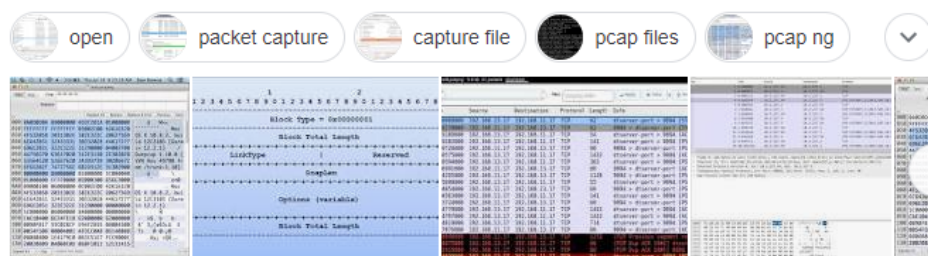
2015年7月1日 — 在linux平台下, 用wireshark-1.12.2进行抓包并保存, 文件格式是**pcapng**格式。由于项目需求, 需要搞清楚其文件格式。通过将保存的**pcapng** ...

<https://m33.wiki> > extension > pcapng ▾

PCAPNG文件扩展名-什么是.pcapng文件, 如何打开它?

什么是**PCAPNG**文件? 包含数据“转储”的数据包捕获格式包 通过网络捕获; 以PCAP下一代文件格式 (用于存储捕获的数据的标准格式) 保存。更多信息。

pcapng的图片搜索结果



举报图片






查看全部






<https://www.qacafe.com> > resources > 5-reaso... ▾ 翻译此页

Five Reasons to Move to the Pcapng Capture Format | qa | cafe

Where did **Pcapng** come from? The original “.pcap” file format is part of an API for performing captures on a network interface. In Unix/Linux, this is ...

怎么打开这个文件

how to open pcapng×



全部视频图片新闻更多设置工具

找到约 131,000 条结果 (用时 0.44 秒)


You need a suitable software like Wireshark from Gerald Combs to **open** a **PCAPNG** file. Without proper software you will receive a Windows message "How do you want to **open** this file?" or "Windows cannot **open** this file" or a similar Mac/iPhone/Android alert.


<https://filext.com> › file-extension › PCAPNG


[PCAPNG File Extension - What is it? How to open a PCAPNG ...](#)


 關於精選摘要 •  意見回饋

其他用户还问了以下问题

What is a Pcapng file?

How do I open PCAP files in Windows?

How do I open a Wireshark file?

How do I open a .CAP file in Windows 10?

反馈

<https://www.wireshark.org> › ChlOOOpenSection ▾ [翻译此页](#)

5.2. Open Capture Files - Wireshark

In addition to its native file format (**pcapng**), Wireshark can read and write capture files from a large number of other packet capture programs as well.

<https://fileinfo.com> › extension › pcapng ▾ [翻译此页](#)

PCAPNG File Extension - What is a .pcapng file and how do I ...

pcapng suffix is and **how to open** it. The Pcap-NG Packet Capture file type, file format description, and Mac, Windows, and Linux programs listed on this page have ...

Format: Binary

<https://www.file-extension.org> › extensions ▾ [翻译此页](#)

File extension PCAPNG - Simple tips how to open the ...

PCAPNG you have two ways to do it. The first and the easiest one is to right-click on the selected **PCAPNG** file. From the drop-down menu select "Choose default ...

<https://file.org> › File Help Guides ▾ [翻译此页](#)

PCAPNG File - What is it and how do I open it? - File.org

How to open PCAPNG files. Did your computer fail to open a PCAPNG file? We explain what PCAPNG files are and recommend software that we know can open ...

稍微浏览一下文件.....

在 Wireshark 顶部有可以筛选所截获的包。

out.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol
64	135.842887581	42.194.203.61	10.0.2.15	TCP
65	135.842934809	10.0.2.15	42.194.203.61	TCP
66	135.843092428	10.0.2.15	42.194.203.61	HTTP
67	135.843192691	42.194.203.61	10.0.2.15	TCP
68	135.929312265	42.194.203.61	10.0.2.15	HTTP
69	135.929336884	10.0.2.15	42.194.203.61	TCP
70	140.949302175	PcsCompu_67:33:6c	RealtekU_12:35:02	ARP
71	140.949463043	RealtekU_12:35:02	PcsCompu_67:33:6c	ARP
72	142.038606535	10.0.2.15	42.194.203.61	HTTP

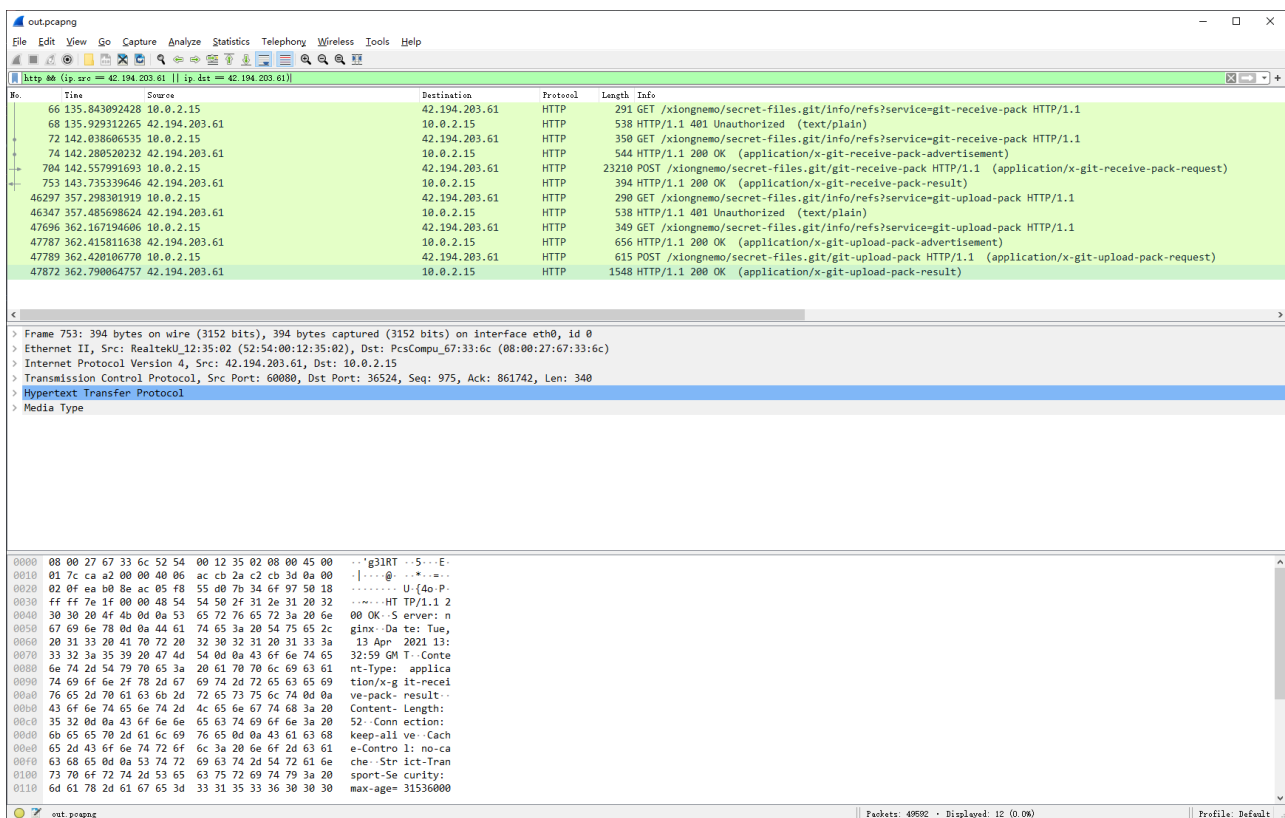
> Frame 68: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface eth0.
 > Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_67:33:6c (08:00:27:
 > Internet Protocol Version 4, Src: 42.194.203.61, Dst: 10.0.2.15
 > Transmission Control Protocol, Src Port: 60080, Dst Port: 36524, Seq: 1, Ack: 238, Len: 48
 > Hypertext Transfer Protocol
 > Line-based text data: text/plain (1 lines)

```

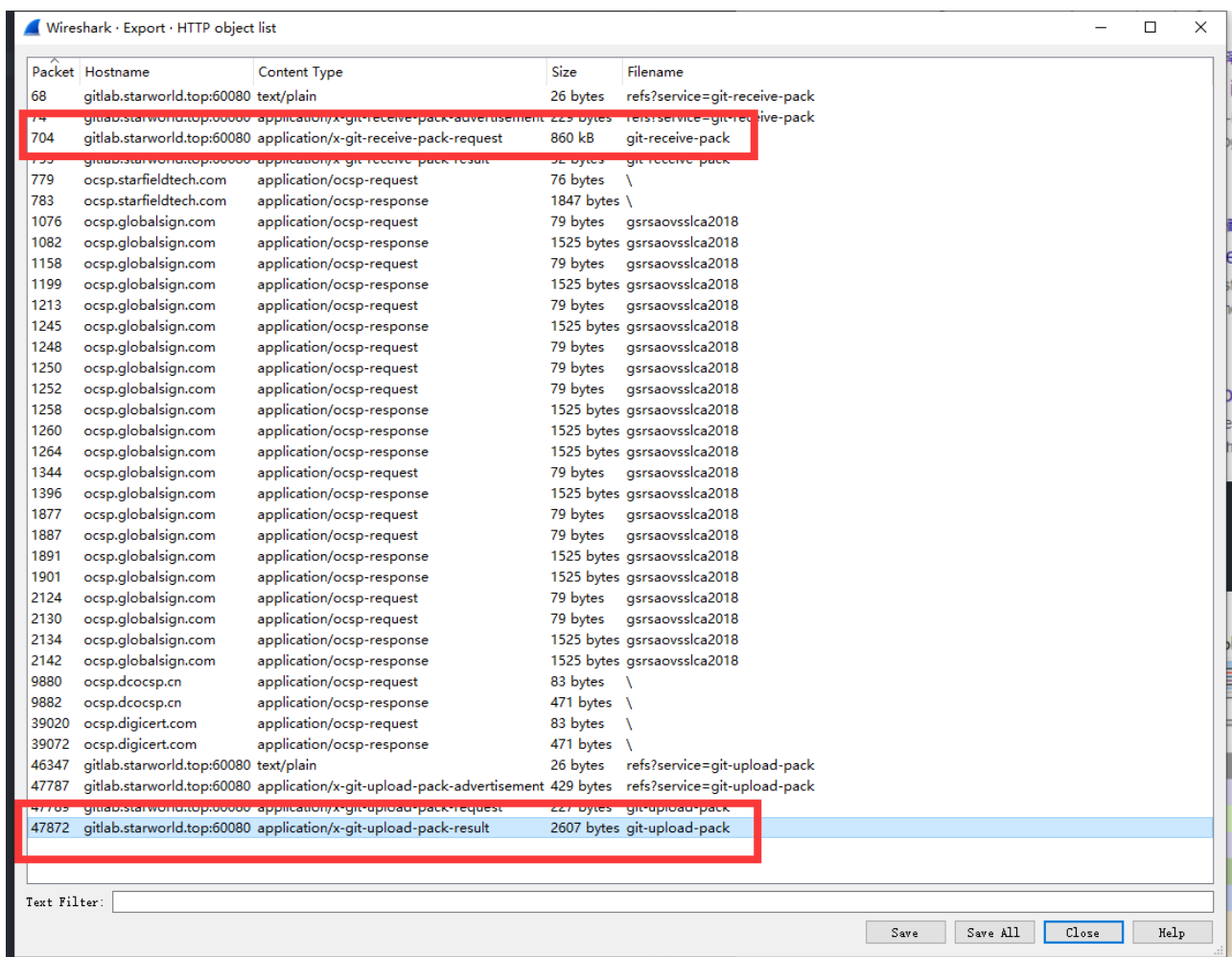
0000  08 00 27 67 33 6c 52 54 00 12 35 02 08 00 45 00  ..'g3lRT ..5...E.
0010  02 0c c8 3b 00 00 40 06 ae a2 2a c2 cb 3d 0a 00  ...;..@. ...*...=..
0020  02 0f ea b0 8e ac 05 f8 52 02 7b 27 4a 57 50 18  .... R-{'JWP.
0030  ff ff 7f 3d 00 00 48 54 54 50 2f 31 2e 31 20 34  ...=..HT TP/1.1 4
0040  30 31 20 55 6e 61 75 74 68 6f 72 69 7a 65 64 0d  01 Unaut horized.
0050  0a 53 65 72 76 65 72 3a 20 6e 67 69 6e 78 0d 0a  -Server:  nginx..
0060  44 61 74 65 3a 20 54 75 65 2c 20 31 33 20 41 70  Date: Tu e, 13 Ap
0070  72 20 32 30 32 31 20 31 33 3a 33 32 3a 35 32 20  r 2021 1 3:32:52
0080  47 4d 54 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70  GMT..Con tent-Typ
0090  65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 3b 20 63  e: text/ plain; c
00a0  68 61 72 73 65 74 3d 75 74 66 2d 38 0d 0a 43 6f  harset=utf-8..Co
00b0  6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 32 36  ntent-Le ngth: 26

```

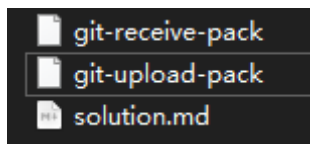
题目中提到了 `git`，那么让我们先来看看 `http` 对象：



导出对象：



导出为以下两个文件：



解包 git pack

直接进行一个 walk 的 bin

```
.tty_rsa/solve
+ solve git:(master) x binwalk -e ./git-upload-pack

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
481          0x1E1          Zlib compressed data, default compression
637          0x27D          Zlib compressed data, default compression
719          0x2CF          Zlib compressed data, default compression

+ solve git:(master) x binwalk -e ./git-receive-pack

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
186          0xBA          Zlib compressed data, default compression
313          0x139          Zlib compressed data, default compression
365          0x16D          Zlib compressed data, default compression

+ solve git:(master) x file ./_git-upload-pack.extracted/*
./_git-upload-pack.extracted/1E1:      ASCII text
./_git-upload-pack.extracted/1E1.zlib:  zlib compressed data
./_git-upload-pack.extracted/27D:      data
./_git-upload-pack.extracted/27D.zlib:  zlib compressed data
./_git-upload-pack.extracted/2CF:      ASCII text
./_git-upload-pack.extracted/2CF.zlib:  zlib compressed data
+ solve git:(master) x file ./_git-receive-pack.extracted/*
./_git-receive-pack.extracted/139:      data
./_git-receive-pack.extracted/139.zlib:  zlib compressed data
./_git-receive-pack.extracted/16D:      PNG image data, 2048 x 2048, 8-bit/color RGBA, non-interlaced
./_git-receive-pack.extracted/16D.zlib:  zlib compressed data
./_git-receive-pack.extracted/BA:      ASCII text
./_git-receive-pack.extracted/BA.zlib:  zlib compressed data
+ solve git:(master) x _
```

研究内容

先看看 upload pack

👉 ..ack.extracted

```
→ _git-upload-pack.extracted git:(master) x cat 1E1
tree 8ca09ca64b7efe211cbb1f868cada5e48fb857a1
parent 2d6a1ec4b89250c4bfc5976840812219b59853d6
author Nemo Xiong <xiongnemo@126.com> 1618320982 +0000
committer Nemo Xiong <xiongnemo@126.com> 1618320982 +0000
```

super secret rsa key%

```
→ _git-upload-pack.extracted git:(master) x cat ./27D
100644 UbFoPBmQ.png %nS5|B*dgn{.j100644 id_rsa []J[]7[]=B%
```

```
→ _git-upload-pack.extracted git:(master) x cat ./2CF
```

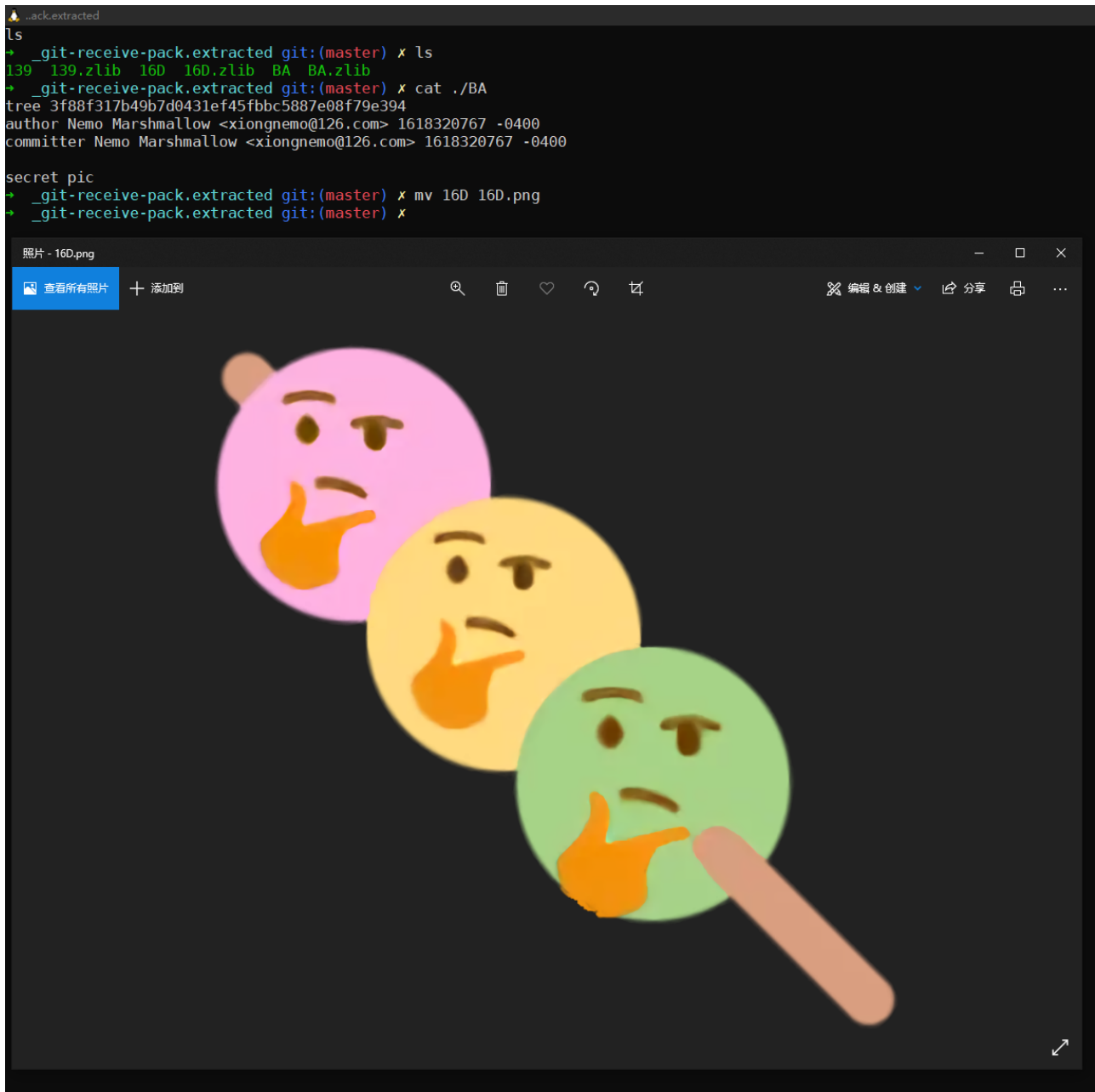
-----BEGIN RSA PRIVATE KEY-----

MIIJKAIBAACKAgEA3129Yyk+TVso9qwdQ3Ri7mijhvM1gc2+CAeSJpkk4TanIo0z
aYyWT6UAj9RuVdWAoSeAqseufBAVLxJIHDlDnne/y7mBPsfTitvpGAK5CT4wkq06
iLeHyDAMUXLIIOjmIZswXk03ejVSdZXyy1M5x8VYyhNkMuR4FAGhfqX00txS9Hkp
L/KrobKh0wq33Uan7WwZjXHgt+JE1Ekj6BAf/oGgbjsUfvIJtV13gmKMuiQqaLAT
YIE7Kop0Rwz06+URgNjXZV+B52h+8adN5DDiwdSPWSlzHEGC4uY3KcWjA1jjdGgK
RLQCqHwo1BUDlhHIkbWgWB/Q6qn7RA5EDp2TAo0SCYDdHTND081y0FR/r1mKijhJ
MfCeggEp8qQqBF100ctrAFIp/u/2wxmx8Cq3+SJ6SQYuruUN4B6ZFY/x9wiAak/a
rfzn+r+yZ3gegZjoCE077UiULypa2VZkRkw1KYuEHS8jLBAByKs0WuwS7hBW9+ffz
of2PyHoQ6WPFzLsqddDfQb1+c+ymr7W0b7Pz2fNrIsh8bgN9CVC0/fsU7TXVPdZ2
EGYQv/Xtz3AkufaXtgo9zW7o/PLw9LTBVGD1N8Y/81he/cf/cWdmRH/s4PFWi2Ua
P/20X2i3uCvIgJc6/+5XeMbMjAWKM30+PIHEKS8JiV0epwJkAqKxaMiYoKkCAwEA
AQKCAgEA11KdRF844Qd06L4og6NJz3vt0CTa0uRkQYdS24ScKcMwTXmmWRebi6o
6P4m0vW7Rx82i0tvh8dVmMmV3CdTyQq1SKXuMtnySH8QKAYUABYEawgMxMjvywq0
hwf+I42d012v9d8fm16VvCat5FW5iJv0qPCikfDu1JJx5Q3fTZyhF21JSCC0VZVG
mg00C/CV52ljBJhesVsdC0uFAquwu/6n8jtf2bRnqX+NupJYCQTeIphI5ao0qEal
iRa0zpaHFgdzNRUpihK89SWMD+MUZT5QgGpVvjJLA2hcWxdbutlQgyHcbDh/q3ep
JbGQQHWqPNSy2uDo2567SvLZpqE+WdScDk0mnM/b8i+TGozxwc6DfGLMhAALGbX6
cqPvkkEtSAM4GNaFk3qqDhhozH1tykdwRfhBzfFwBlCF4dVuG+bu0ZEktc0EoVJL
Po3DjGFYsXIh+vjjt80K0oDM6RTr+UfYr7y5IrRx5zaIy00zXt5z6pfsGEh2a9cY
q5oUo7HFydIf1Fp9R4n9uv+S6UMJmWlgnMyQTDdF6+X10Rr5/A6TRWFMaJpbMw4
LTnxBIy+oiNqKs8+Rnu6Rfqz3NCT1X73lcRu4+YYcmJMHJyyHmPtnvj4InvahVmW
3IsU4ZaC1AMAetPlph35FCzZupa2uc/my5Ap8i1HKWD76DlL04ECggEBAPs+Uizr
g0YtdqgNvGs8D+vRnwX459MZ5iPmPhGC6Yk6LDN8JE3ZNSpXHJn3jgPBUTkFiHuT
-
-
-
-

ss+XxUdDq1/IG9ECggEBA00YTvw8fEy5squfr9xDhLczCGAP7b2+/AhcryEbmBGL
HNvydqvP02chYCLh7rDGSHScflgTmH5K4n40x/vEywUd0FNeWzAmLeHhITK9JuPe
2Du4LHfC6I9ReD1t2A9hpnt2ECpYi/inFugKbfbq80/lpACLJ0F2/0z2I60Ik1Qf
EcpPJgsZ0lvFnIXz1dRR6kr4MGtN5vIlLRL6qak7NFwa7fnCQKyGI8QCNdayD0o4
YFMVek9yVy2/N85p3J/ivZMJX9/Rf7BWLkqkccetSujly+mspnDdrPQj70AJ2tq00
+obNKVMnVM9+8aeSSzBRhcZZEBwXVgT6sLx7zMMV5VkCggEAQimxtql4ER++sJaN
Fx2Eg3Iz1dqkDCoxLxoZFLsFhx5NLHBTjiCzoiW0Xc0RGuP04bHXL9C9n5IFzUd9
PBRj5hzMsBT0dYocSYCjyDBQqbozoCD16ujevqCLygQgYRzeZkXm/2RXN0/as9BG
3Q6ZUWoEnT4yNUTxmDfVVSgyh/bTEU8CbyR8PHBpUtsMLoHlh9V7ftZrbL5iYC+F
qA3xyDylhz4laebvS4TYqP0r30TCWe0NuSPvoQHWina70HmICf35G1Gyq8I/FezW
kdVR9XPAdiRuTQEFdHg2XAHGJxdAa1ttTt9F0VP0/nL10qi4jHye6Vf95i/puszR
fDFNQQKCAQAePMcJpf0Rs415QJVTjccq9AKCz03yN7tMXsm9+aNNiFAa4curm7U
-
-
-

```
-  
-  
-  
-  
-  
-  
-----END RSA PRIVATE KEY-----%  
→ _git-upload-pack.extracted git:(master) x
```

再看看 receive pack



从 upload pack 中，我们看到了一个不完整的 RSA 私钥。

从 receive pack 中，我们看到了一个图片。

找到 **flag**

```
-bash-5.1$ ls  
welcome.txt  
-bash-5.1$ cat welcome.txt  
find super SECRET flag  
-bash-5.1$
```

你知道该干什么：

```
-bash-5.1$ find / | grep SECRET
find: /proc/tty/driver: Permission denied
find: /proc/1/task/1/fd: Permission denied
find: /proc/1/task/1/fdinfo: Permission denied
find: /proc/1/task/1/ns: Permission denied
find: /proc/1/fd: Permission denied
find: /proc/1/map_files: Permission denied
find: /proc/1/fdinfo: Permission denied
find: /proc/1/ns: Permission denied
find: /proc/8/task/8/fd: Permission denied
find: /proc/8/task/8/fdinfo: Permission denied
find: /proc/8/task/8/ns: Permission denied
find: /proc/8/fd: Permission denied
find: /proc/8/map_files: Permission denied
find: /proc/8/fdinfo: Permission denied
find: /proc/8/ns: Permission denied
find: /proc/33/task/33/fd: Permission denied
find: /proc/33/task/33/fdinfo: Permission denied
find: /proc/33/task/33/ns: Permission denied
find: /proc/33/fd: Permission denied
find: /proc/33/map_files: Permission denied
find: /proc/33/fdinfo: Permission denied
find: /proc/33/ns: Permission denied
find: /proc/35/task/35/fd: Permission denied
find: /proc/35/task/35/fdinfo: Permission denied
find: /proc/35/task/35/ns: Permission denied
find: /proc/35/fd: Permission denied
find: /proc/35/map_files: Permission denied
find: /proc/35/fdinfo: Permission denied
find: /proc/35/ns: Permission denied
find: /proc/37/task/37/fd: Permission denied
find: /proc/37/task/37/fdinfo: Permission denied
find: /proc/37/task/37/ns: Permission denied
find: /proc/37/fd: Permission denied
find: /proc/37/map_files: Permission denied
find: /proc/37/fdinfo: Permission denied
find: /proc/37/ns: Permission denied
find: /proc/39/task/39/fd: Permission denied
find: /proc/39/task/39/fdinfo: Permission denied
find: /proc/39/task/39/ns: Permission denied
find: /proc/39/fd: Permission denied
find: /proc/39/map_files: Permission denied
find: /proc/39/fdinfo: Permission denied
find: /proc/39/ns: Permission denied
find: /root: Permission denied
/lib/SECRET.txt
-bash-5.1$ cat /lib/SECRET.txt
tjctf{mo5@IC_M#Ans_noThiNG}
-bash-5.1$
```