# 加密解密

## 1.1常见加密场景

各种编码方式，把数据进行加密，对某些敏感信息进行加密传输，可以增强安全性。

加密方式：AES、URL、MD5、DES、DSA

加密解密工具：网页、超级加密解密工具

### 1.1.1URL加密特征和应用场景

应用在域名加密

# 2.CDN绕过

## 2.1检测CDN

原理：从全国各地的ip地址去ping这个目标主机

### 2.1.1超级ping



多地ping目标网址，发现访问的是不同的节点，说明存在CDN

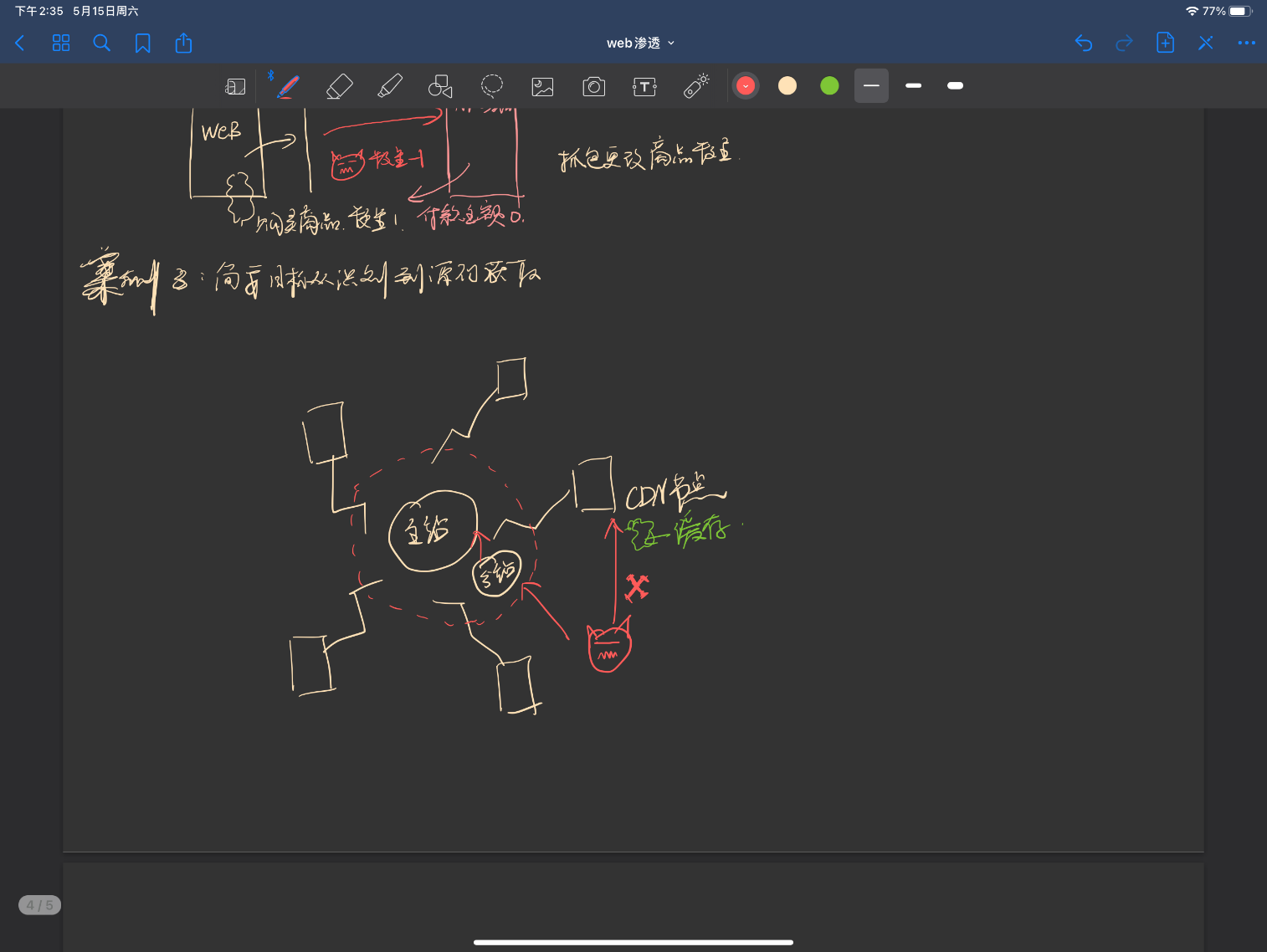
如果访问CDN节点，访问的是网站的缓存，并不是目标主机

## 2.2常见CDN绕过技术

### 2.2.1子域名查询

原理：查询主域名的子域名[[1]](#footnote-1)，通过对子域名进行ip地址查询，通常情况下，主域名服务器和子域名服务器在同一台服务器上面，是同一个ip或者是同一个网段。也有可能两者之间没有任何关系，如果没有关系，即便知道子域名的ip也没有办法知道主网站。这种情况下进行子域名查询就没有意义了嘛？

子域名查询对于主站信息收集的意义：通常主站流量比分站大，出于成本考虑，只对主站做CDN，而分站没有，所以可以进行ip地址扫描，在经过上述原理可以知道通过分站ip地址很有可能推算出主站ip地址。



### 2.2.2邮件服务查询

很多企业内部会有邮件服务器，而邮件服务器大部分都没有做CDN节点，道理很简单，本来就是公司内部员工访问，外面的人瞎访问啥？？

如果对方有CDN，我访问你，是通过你的CDN节点，但是你给我回复邮件是用自己的邮件服务器给我回，我没有CDN，可以直接看到是谁（源ip地址）发给我的。怎么看到？有这样一种技术可以通过邮件判定发送者的ip地址[[2]](#footnote-2)。

原理同子域名ip地址扫描，邮件服务器可能和主站在同一个主机，使用相同的ip地址或者是同一个网段。

### 2.2.3国外地址请求

出于经济原因，国外如果没有太多的客户和访问量，一般不使用CDN，所以有可能直接访问国外的网站就直接扫描到主站ip地址。

问题：如果国外的网站是主站，可以直接扫描到，怎么判定国外的是主站，在超级ping检测的时候，如果在国外只有一个ip，能判定他就是主站ip吗，或者国外只有一个CDN节点

### 2.2.4遗留文件，扫描全网

①遗留文件

没搞懂

②扫描全网

利用类似于超级ping的工具从全世界各地对该网站进行访问，把所有的ip地址都进行搜集，真正的主站ip地址很可能在这些ip里面，然后再进行整理分析。

### 2.2.5黑暗引擎搜索特定文件

①Shodan

②Zoomeye

③FOFA

搜索特定文件的hash值，使用黑暗殷勤进行搜索，类似于全网扫描，找到所有可能出现过这个文件的网站主站或者节点

### 2.2.6Dns历史记录，以量打量

在这个网站有钱做CDN之前，会有一个原来唯一的ip地址，查看DNS解析记录有可能查到这个网站在做CDN之前的真实ip地址记录。

以量打量：CDN流量是付费的，如果使用DDos攻击，把某一个节点的流量消耗完，再访问的就是他本身主站的ip。

## 2.3案例实践

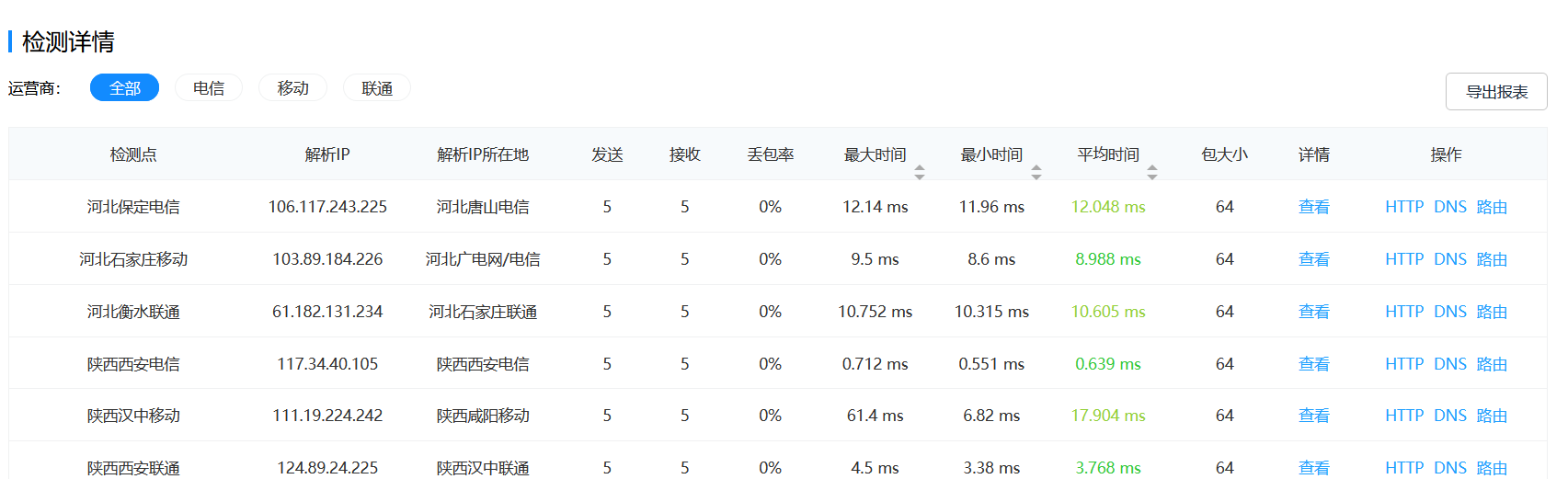
### 2.3.1网站域名解析和CDN节点的关系

本案例的对象以[www.xueersi.com](http://www.xueersi.com)网站为例：

上面提到，子域名可能会不做CDN，在本案例当中，首先访问[www.xueersi.com](http://www.xueersi.com)，然后访问xueersi.com，发现都可以访问到官网，说明该网站的域名管理中包含了www，和\*两条解析记录。

然后进行超级ping检测CDN节点是否开启

1. 检测[www.xueersi.com](http://www.xueersi.com)，结果如下



明显存在CDN节点

1. 检测xueersi.com，结果如下



发现只有124.250.113.71，124.250.113.72两个ip地址，说明主站就在这两个ip地址上。

### 2.3.2通过注册邮箱来获取ip地址

以huawei网站为例



①先通过邮箱注册，收到注册的邮件



②查看邮件源码，可以看到发送者的ip地址，这是发送者的邮箱地址，很有可能是网页服务器的ip地址。

2.3.3使用黑暗引擎来进行全网检索—以shodan为例

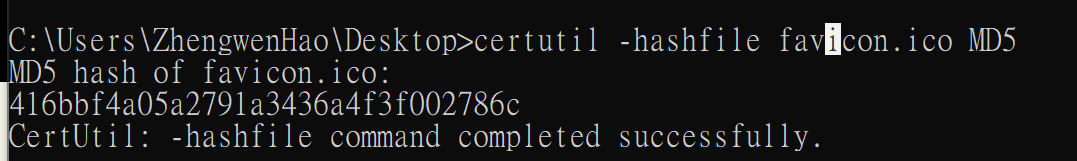
①查看网页源代码



②找到.ico文件并下载下来



③通过命令行来得到md5值



④利用shodan黑暗引擎来进行检索

# 3.信息搜集

## 3.1架构、搭建、WAF等

### 3.1.1安装git（监控源代码和最新的漏洞利用）

Redhat：**yum -y install git**

**Rpm -qi git**

Debian/ubuntu：**apt-get install git**

**Rpm -qi git**

Windows：从git官方网站下载并安装<https://git-scm.com/downloads>

1）在windows下进行配置

①配置

**git config --global user.name "xxx"**

**git config --global user.email** [**xx@xxx.com**](mailto:xx@xxx.com)

**mkdir ggiitt**

**cd ggiitt**

**git init**

**ls -a**

只能对文本文档进行跟踪，二进制文件不可以，所以建议使用notepad++进行编辑，编码方式都选择UTF-8

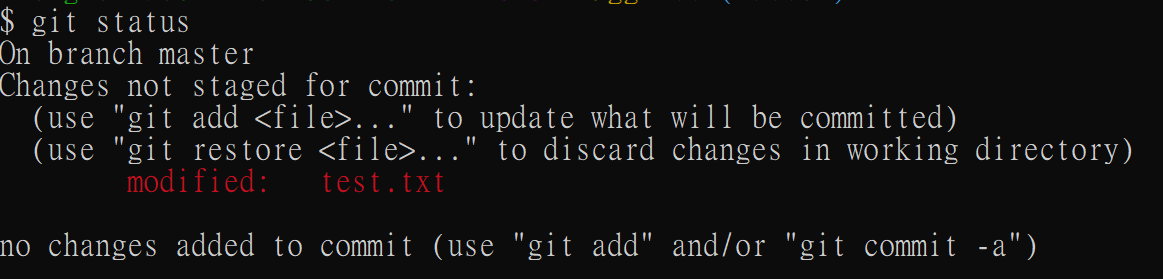
把文件添加到仓库当中去：创建一个文本文件test.txt，然后放到仓库一级目录或者是子目录中，然后执行命令

**git add test.txt**

**git commit -m “creat a file, name :test”**

如果对文件进行了更改，但是并没有提交，而且长时间没有使用，可以使用

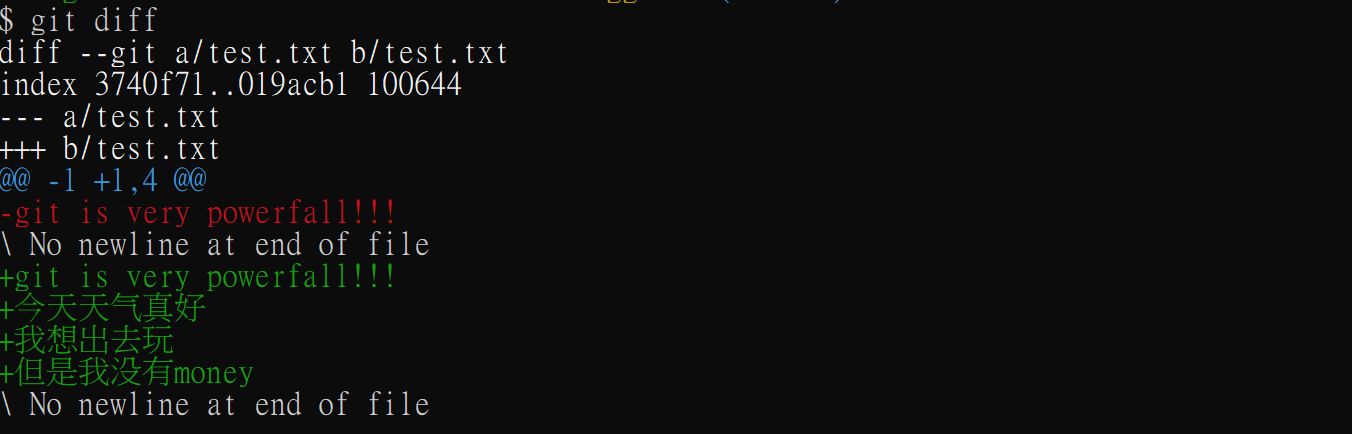
**git status**



查看状态，如果没有提交，他会给出提示说明已经做出了更改，但是没有提交到仓库中。那么如何知道到底做了哪些更改呢？

**git diff（difference）**

可以看到哪里做出了改动

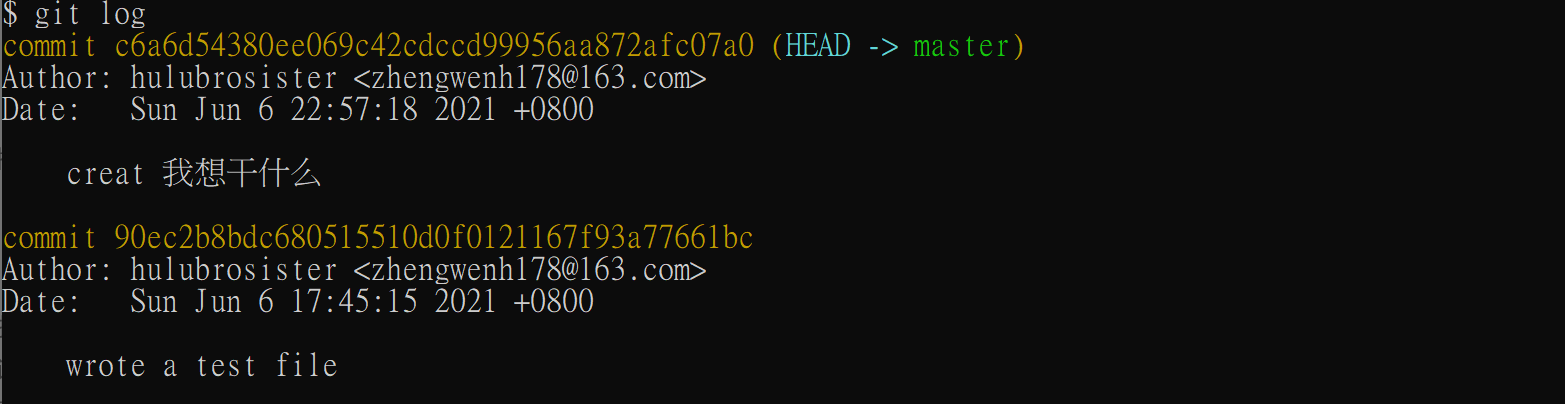


确认无误之后就可以按照git add 和git commit -m “”进行提交。

我操作失误了，想要回退到上一次提交的版本怎么办？使用

**git log**

可以查看到之前每次提交的记录

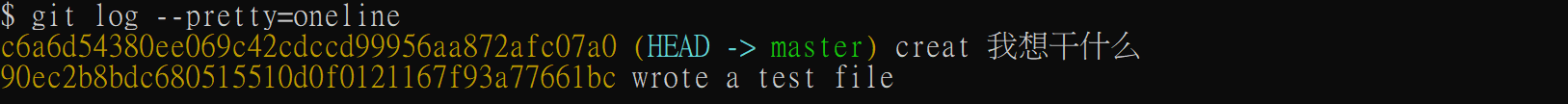


这样就非常方便我们回退了

如果觉得信息繁琐，还可以加上

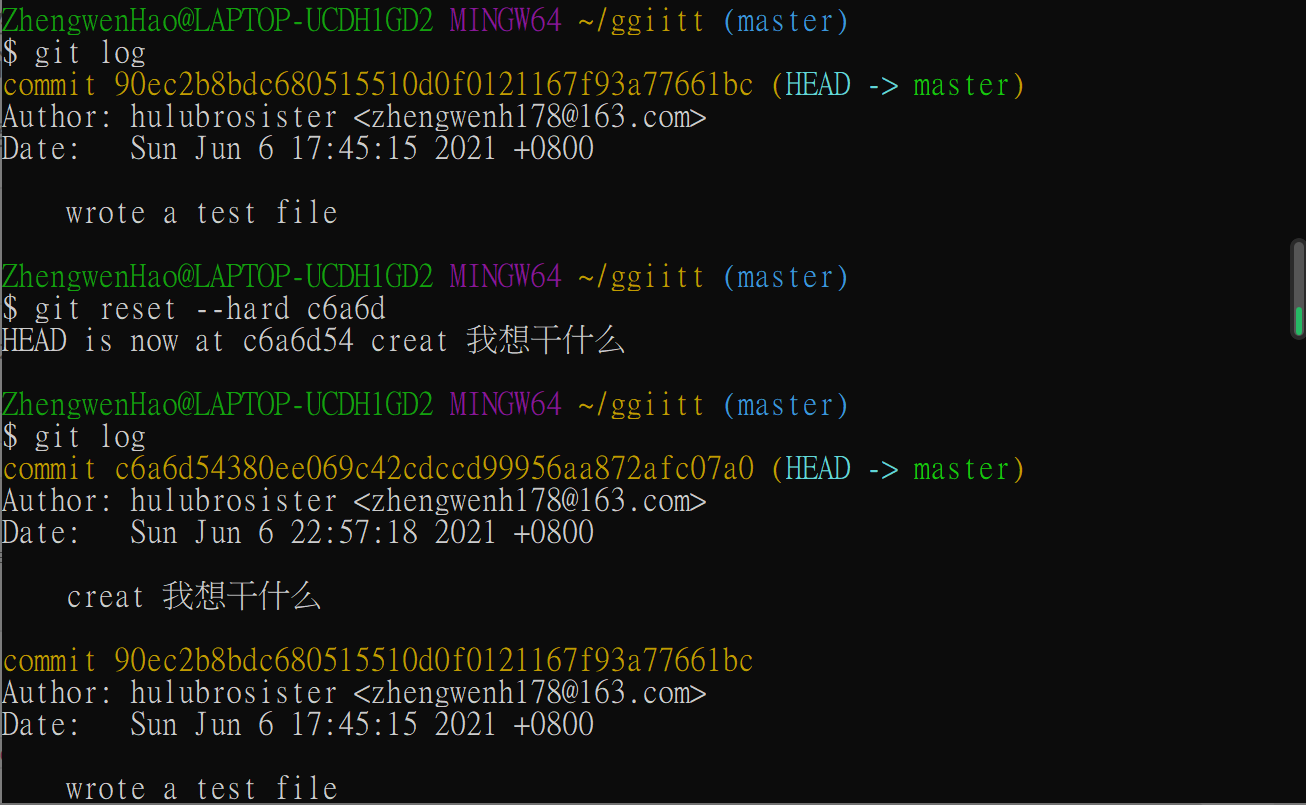
**git log –pretty=oneline**

这样就可以单行输出信息，没有作者和时间



**Git reset --hard 版本号**

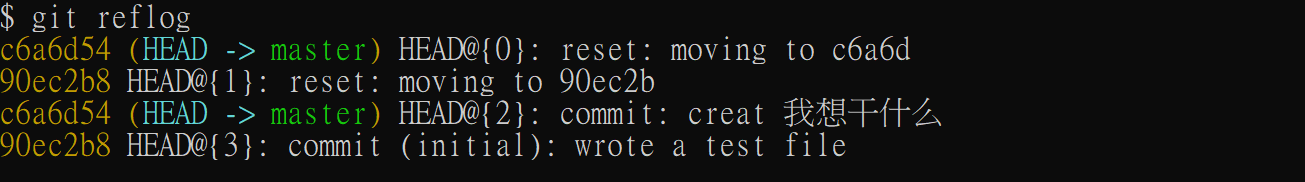
只要知道版本号就可以去到任何一个修改的节点（前提是知道版本号）



如果回退之后，我关闭了界面，第二天又后悔了怎么办？

**Get reflog**

可以查看历史文件变更



②工作区和版本库

工作区就是文件存放地点，版本库就是自动生成的隐藏文件。工作区进行操作之后，通过add添加到版本库中的stage，作为更改的缓存，然后可以统一通过commit一起提交到master分支当中，Stage清空。

取消修改

**Git checkout -- test.txt**  #把工作区的所有操作都取消，其实是把版本库的文件替换掉工作区的文件

**Git restore test.txt**  #可以实现相同的效果

如果已经添加到stage当中，则无法清空

那么stage当中的应该怎么清空？

**Git reset HEAD test.txt** #HEAD表示最新的版本

这个时候stage是空的，回到了工作区中还没有add的时候

③远程仓库

Github就是一个免费的远程仓库，通过ssh和仓库进行加密传输，首先需要建立ssh密钥

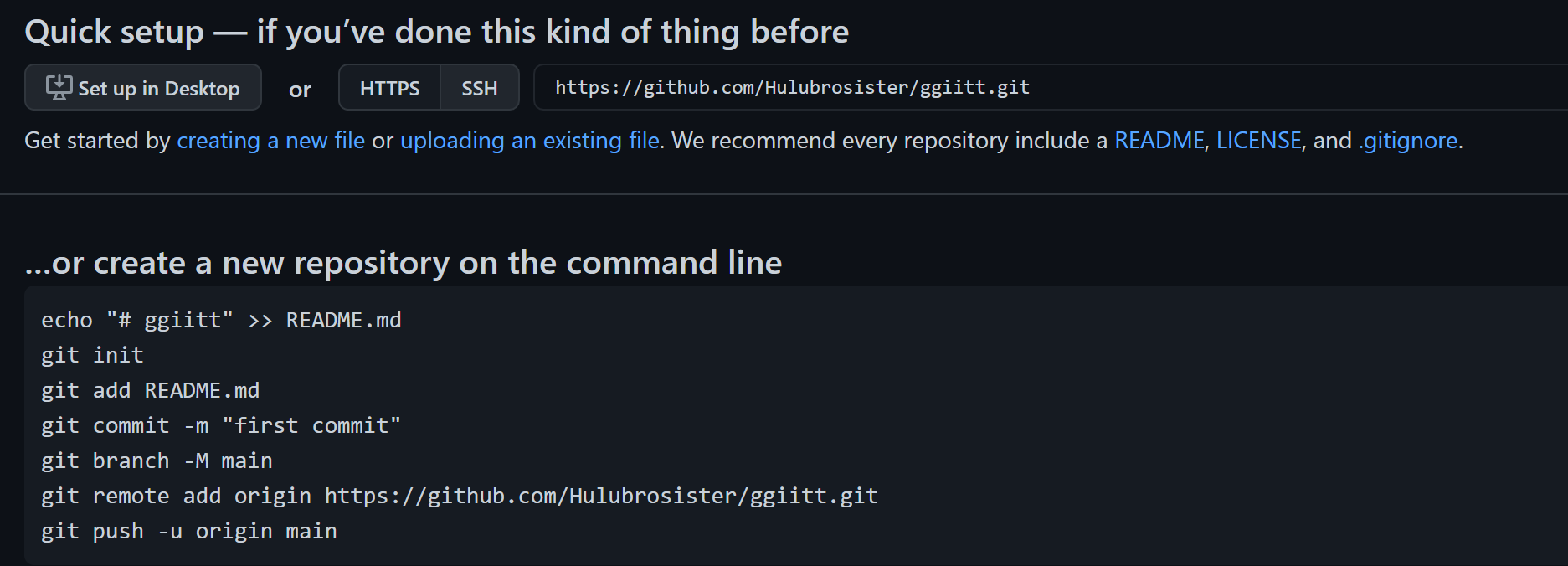
**ssh-keygen -t rsa -C "youremail@example.com"**

这个时候会在用户主目录下添加一个.ssh的文件，把其中的pub公钥复制出来

注册github账号，登陆之后来到account setting，add sshkey，添加公钥之后，就可以上传来自你主机的文件。

然后建一个远程库，通过new repository新建

根据提示操作



创建成功之后，之后怎么通过这个去提交到远程库中呢？

**git push origin main**（注意刚开始关联第一次推送需要加-u参数）

1. 子域名：[www.netsun.com](http://www.netsun.com)是主域名，[www.new.netsun.com](http://www.new.netsun.com)就是他的一个子域名，子域名也叫多级域名，主域名是一级（顶级）域名 [↑](#footnote-ref-1)
2. 通过邮件查询发送方ip地址：例如qq邮箱，可以通过‘显示邮件原文’看到‘X-originating-IP:’；Foxmail可以通过‘查看邮件源码’中的‘Received:From’查看发送者IP [↑](#footnote-ref-2)