自由软件使用简易手册

第四版 2024 年 2 月

目录

一、什么是自由软件？为什么要使用自由软件？

自由软件（英语：**free software**），是一类可以不受限制地自由使用、复制、研究、修改和分发的，尊重用户自由的软件。这意味着自由软件一定是对其用户公开源代码的，也就是开源软件。但是开源软件不意味着自由软件，因为有的软件公司选择开源，只是为了想找用户帮它调试、吸收社区贡献的功能，这样子会破坏了自由软件的原意。值得注意的是，自由软件不意味着免费（虽然大部分自由软件是免费的），自由软件也不拒绝提供商业服务。具体来说，自由软件的用户拥有四项基本自由：

(0)自由运行软件、(1)自由学习和修改软件源代码、(2)自由再发布软件拷贝以及(3)自由发布修改后的软件版本。

软件不同于生活中的事物 — 它不同于椅子、三明治或是汽油 — 软件可以更容易地被复制或修改。恰恰是这一特性，使得软件更为有用。我们由此坚信，软件的这一天然属性应该被用户利用。

与**自由软件**相对的是**私有软件**（英语：proprietary software），也被称为专有软件、封闭软件，这些软件出于盈利目的限制人们对其自由使用的权力，典型的如 Windows 、Photoshop 等。

在新技术革命对现代精神带来冲击与新工人群体——程序开发者试图掌握自身劳动的背景下，旷日持久的自由软件运动应运而生，它高举自由、理性的古典旗帜，以先进的技术理念——共建、共享和不断发展的技术手段，对抗着资本主义在信息技术领域的独裁。
这是又一资本主义历史的辩证过程，在最根本的意义上，它将生产从僵化而封闭的资本组织中解放，从而为更广大新劳动者的联合创造条件。而在其他层面，它反对现代新自由主义隐性地剥削人权的做法，倡导使用者的主体权，亦是科学精神——服务于全人类在技术层面的生动实践。
可以说，这是共产主义理念在现代技术领域的自发实践，我们应当以斗争者的自觉与明见将其转化为斗争的工具，而这首先需要我们带着谦逊与热情去积极学习与使用自由软件，并抵制私有软件，以此逐步实现对自身权利的捍卫与对更先进社会的追求。

更多相关信息参考：
https://www.gnu.org/
https://lemmy.tedomum.net/post/60360
https://lemmy.tedomum.net/post/38015

二、安全问题（重点）

即便使用上了自由系统和自由软件，也是远远不够的。第一，现阶段我们难以完全和私有软件脱离联系；第二，在自由的通信系统内，也潜伏着大量的警察，并不是完全安全的。所以就算解决了设备安全的问题但如果使用者没有高度的保密意识和警惕心理，那么也很可能会陷入危险之中。下面将列出一些需着重注意的条目。

1.在家庭、公司、学校、非革命话题为主导的私有网络群聊等环境中，不要轻易向政治立场不明或反动的人暴露自己的政治立场，更不能在公共摄像头下暴露自己的手机屏幕，要学会伪装自己，以免带来不必要的麻烦。如果在私有平台和人辩论过程当中一定慎重，因为不排除对方会使用举报。
2.严禁在不同的平台使用相似甚至有关联的用户名和密码。在私有平台需要单独设置和我们生活相关的账号，不要把它们用作政治用途。有必要的话，要定期更换账号。关闭一切设备登录。
3.不要使用公共 WiFi，除非它不需要实名认证，且自己的设备支持伪造 mac 地址，在私有平台上注意避开敏感词，减少搜索敏感信息的次数。发布图片时注意图片本身所带的文件信息和内容信息，更不能将私有平台和自由平台上的消息不加掩盖就相互转发，这是极其危险的行为！
4.手机必须设置锁屏，不能设置较容易解开的锁屏密码，以防被不相干的人拿去窥探信息。一切消息不得设置锁屏状态下直接显示。消息通知不要设置为屏幕上方直接显示内容。如果手机有指纹解锁功能可以设置，用于在公共场合代替锁屏密码解锁手机，但最好配合使用 F-droid 中的 Private lock 来在必要时禁用指纹解锁，以免被人利用来攻击自己。
5.如是未刷自由软件系统的手机，应将手机的 app 安装安全检测关闭。（刷系统请见第四章）并关闭国内 app 读取手机储存的权限。必须关闭一切应用的云服务功能。
6.输入法应换为 fcitx（小企鹅输入法）、rime 输入法等无联网无后台无监视的自由软件输入法，切勿使用国产私有输入法。剪贴板需定期清理。

7.在与生活和经济依赖父母，父母平常管理较严的学生接触时，容易引发对方父母的干涉导致暴露，因此需要格外小心谨慎，应当尽可能用匿名的帐号与对方线上接触。
8.时常清理聊天记录以及手机上有关我们事业的截图或文件，最好是有两台手机，一台完全不参与我们的事业。（有条件的可以一台日常生活用另一台事业上用）
9.一定做好应急处理设备的思想准备，被人抢夺或要求上交通讯设备时，应立即重置系统（比如 F-droid 中的 Locker，可在输错指定次数的密码后自动重置系统）或彻底删除所有敏感的软件和信息。
10.尽量使用 F-droid 下载软件，如遇特殊情况需要不经过 F-droid 客户端下载安装包时应验证安装包的数字签名。
11.如果你在风险较高的环境中，需要时刻注意自己的计算机硬件安全，以保证他们不会被篡改，例如可以给有螺丝的地方涂指甲油，这是一种很好的廉价方法，但它也可能会引起怀疑，因为这种保护比较明显。因此，你还可以选择隐蔽性更好但操作较麻烦一些的方法，例如，可以对笔记本电脑的背面螺丝进行特写微距摄影，或者在其中一个看起来像普通污垢的螺丝内滴入少量蜡。然后，您可以通过将螺钉的照片与新螺钉的照片进行比较以检查设备的硬件是否被篡改。

三、一些小贴士

1.校验安装包
从 GNU/Linux 发行版 和 f-droid 下载的包都是被软件包管理系统和 f-droid 客户端校验过的。从 github 上下载的包只要 tls 证书没出问题就基本上可以相信。只是不要轻信别人发给你的包。因此我们也尽量不要直接给对方发软件包，而应引导对方用正规手续添加带有公钥指纹的软件仓库，再从软件仓库里安装软件包。

2.浏览器选择
在 PC 上安装 GNU/Linux 发行版提供的主流自由浏览器，如 firefox、chromium 即可，也可以安装和 tor 整合在一起的 tor browser，它还有与 tor 无直接关系的额外反跟踪功能。在 Android 上浏览器分为两种：独立浏览器和依赖于 webview 的浏览器。前者包括所有基于 firefox 和 chromium 的浏览器。后者依赖于作为操作系统一部分的 webview，可能功能不全（比如不支持 firefox send），但常常提供一些有用的次要功能，因此仅建议在 webview 可以经常更新的自由 android 发行版上使用这样的浏览器。

不同浏览器可以互补使用。

3.密码管理
可以用专门的软件（如 GNU/Linux 上的 apg）生成容易记忆但随机性仍然很高的密码，生成后用一个统一的密钥加密保存，必要时解密查看，这样避免了记忆大量密码，而只需要记住一个加密其他密码的主密码。密码管理器常常合并实现这两项功能，可以到 GNU/Linux 发行版和 f-droid 的软件仓库中寻找。

四、操作系统（重点）

GNU/Linux 发行版

自由的 GNU/Linux 系统发行版（或“发行版”）只包含和发行自由软件。他们拒绝各种非自由的应用程序、非自由的编程平台、非自由的驱动、非自由的固件“blobs”，以及其他各种非自由的软件和文档。如果他们发现错误地包含了这些非自由的成分，他们会主动去除它。

自由的 GNU/Linux 发行版

我们推荐您使用自由的 GNU/Linux 系统发行版，那些不包含任何专有软件的发行版。这样，您就能确定自己没有运行任何非自由的程序。这张列表列出了这样的发行版：
自由的 GNU/Linux 发行版。

这些现有的发行版全部都在开发方面需要更多的帮助。因此，如果您希望有效地帮助自由的 GNU/Linux 发行版，那么我们建议您加入这些现有发行版的开发队伍，而不是再自己从头做一个新的发行版。

自由的非 GNU 发行版

这些发行版是自由的，但它们和 GNU 大不相同。它们的用法也和使用 GNU/Linux 不同。但是，它们和自由的 GNU/Linux 发行版一样满足自由软件的道德标准。
自由的非 GNU 发行版。

这些现有的发行版全部都在开发方面需要更多的帮助。因此，如果您希望有效地帮助自由的 GNU/Linux 发行版，那么我们建议您加入这些现有发行版的开发队伍，而不是再自己从头做一个新的发行版。

自由发行版指南

这里列出一些可能会使得一个发行版无法成为自由发行版的一些原因：
自由发行版指南。

常见发行版

大多数常见的和知名的 GNU/Linux 发行版并不能满足我们关于自由的要求。这篇文章为您列举了它们的一些问题：
为什么我们不能支持众多知名的 GNU/Linux 发行版。

我们呼吁这些发行版的开发人员把其中非自由的部分移除，还用户一个完全自由的系统。

自由作为可选项是不够的

有些 GNU/Linux 发行版给用户一个选项，用来安装仅包含自由软件的系统。您请看：
为什么自由作为可选项是不够的。

这为什么重要?

当一个 GNU/Linux 发行版包含了私有软件，它就有两个问题：

- 如果你安装了它，你就可能安装和使用了私有软件。
- 它为人们指引了错误的方向。

第一个问题是直接的：它影响了在该发行版上安装了私有软件的用户。然而，第二个问题尤为严重，因为它影响了整个开发社区。 私有发行版的开发者并不会说：“很抱歉，我们的发行版包含了私有软件。我们并不想包含它们。希望下个版本是完全自由的。”如果他们做到了，影响还不会太坏。

然而，他们一般会说非自由软件是其系统的一个有益的功能；他们的目的是“给用户最好的体验”等等，而私有的。换句话说，他们引导用户更关注舒适而不是自由——这恰恰和自由软件运动的主要目标背道而驰，是一种对自由软件运动的修正主义。

这就是我们不支持这些不抵制私有软件的发行版的原因。它们不教育人们重视私有制的危害，因此我们强烈关注这一点。

因此我们推荐您安装 GNU/Linux 操作系统到自己的计算机设备上

这里我们以安装 Debian 发行版为例

安装前的准备工作

在开始之前，确保你满足下列条件:

- 一个 Debian 的可引导 USB 或 DVD；
- 一个快速且稳定的网络（为了安装更新以及第三方软件）；

提示：USB 推荐使用闪迪、金士顿正版 u 盘，不推荐使用盗版水货，也可以使用读卡器 + sd 卡的组合来代替 USB 设备。

提示：如果手边没有其他安装了 GNU/Linux 系统的设备可用，可以使用在 windows 上运行的创建 USB 启动盘的自由软件 rufus 或 ventoy 完成启动盘创建工作。

进行 Debian GNU/Linux 安装过程

插入引导介质（USB 或 DVD）并选择从该介质启动（具体方法请查阅您所用的主板或笔记本电脑的说明书）。

提示：进行此步骤前，请先更改 BIOS 设置，在启动时按住功能键（通常，根据品牌不同，是 F9、F10 或 F12 中的某一个），进入 BIOS，然后选择你系统的引导策略（UEFI 或 Legacy）。另外需要注意如果你的 BIOS 不是自由的，那很可能默认开启了 TPM（信赖平台模组），私有 BIOS 中默认启用这类选项的目的在于只允许用户使用该厂商想让用户使用的软件，并且私有 BIOS 大概率隐藏着后门，这类风险都会

对电脑的安全造成威胁很显然这是私有软件的一种独裁和剥削，你可以将私有 BIOS 替换为自由的 BIOS（例如 coreboot）来解决此类问题，总之在安装系统之前如果你使用的是私有 BIOS 那么需要注意这类选项是否开启，如果开启请禁用他们。这一步骤，对系统是否能进入安装媒体来说，至关重要。保存 BIOS 设置，并重启电脑。

界面会显示一个新的引导菜单：点击 “Graphical install”。

下一步，选择你的偏好语言，然后点击 “继续”。

接着，选择你的地区，点击“继续”。根据地区，系统会自动选择当地对应的时区。如果你无法找到你所对应的地区，将界面往下拉， 点击“其他”后，选择相对应位置。

而后，选择你的键盘布局。

接下来，设置系统的主机名，点击 “继续”。

下一步，确定域名。如果你的电脑不在域中，直接点击 “继续”按钮。

然后，设置 root 密码，点击 “继续”。

下一步骤，设置账户的用户全名，点击 “继续”。

接着，设置与此账户相关联的用户名。

下一步，设置用户密码，点击“继续”。

然后，设置时区。

这时，你要为 debian 安装创建分区。

提示：如果你打算安装 LUKS on LVM，可参考这篇。

如果你是新手用户，点击菜单中的第一个选项，“使用最大的连续空余空间”，点击“继续”。

不过，如果你对创建分区有所了解的话，选择“手动” 选项，点击 “继续”。

接着，选择被标记为 “空余空间” 的磁盘，点击 “继续” 。接下来，点击“创建新分区”。

下一界面，首先确定交换空间大小，一般和电脑的内存大小一致。我的交换空间大小为 2GB，点击 “继续”。

点击下一界面的 “主分区”，点击“继续”。

选择在磁盘 “初始位置” 创建新分区后，点击继续。

选择 “Ext 4 日志文件系统”，点击 “继续”。

下个界面选择“交换空间” ，点击 “继续”。

选中 “完成此分区设置”，点击 “继续”。

返回磁盘分区界面，点击 “空余空间”，点击 “继续”。

可以先创建根目录分区。根目录是 GNU/Linux 系统目录树最根本的目录，其他任何目录都包含在根目录内。

“用于”选择“ext4 日志文件系统”，挂载点选择“/”，然后“完成分区设置”。

返回磁盘分区界面，点击 “空余空间”，点击 “继续”，创建 /home 分区，下个界面确认需要创建的空间大小 /home 是用户的家分区，用户可以自由编辑其中的所有文件，一般要设置得最大，点击 “继续”。

“用于”选择“ext4 日志文件系统”，挂载点选择“/home”，然后“完成分区设置”。

> 提示：挂载到 /home 的分区放在最后有助于在当迁移到更大的磁盘时，可以只调整这个分区而不影响其他分区。

最后， 点击 “完成分区设置，并将改动写入磁盘” ，点击 “继续”。

完成分区设置，并将改动写入磁盘

确定你要将改动写入磁盘，点击 “是”。

而后，安装程序会开始安装所有必要的软件包。

当系统询问是否要扫描其他 CD 时，选择 “否” ，并点击 “继续”。

接着，选择离你最近的镜像站点地区，点击 “继续”。

然后，选择最适合你的镜像站点，可以选择国内的镜像，但不要选择阿里巴巴、腾讯的镜像，请选择中国科学技术大学(ustc)、兰州大学（lzu）、清华大学（tsinghua）等大学的官方镜像站。点击“继续”。

如果你打算使用代理服务器，在下面输入具体信息，没有的话就留空，点击 “继续”。

随着安装进程的继续， 你会被问到，是否想参加一个软件包用途调查。你可以选择任意一个选项，之后点击“继续”，我选择了“否”。

在软件选择窗口选中你想安装的软件包，点击“继续”。

安装程序会将选中的软件一一安装，在这期间，你可以去喝杯咖啡休息一下。

系统将会询问你，是否要将 grub 的引导装载程序安装到主引导记录表（MBR）上。点击 “是”，而后点击 “继续”。

接着，选中你想安装 grub 的硬盘，点击“继续”。

最后，安装完成，直接点击 “继续”。在重启系统前请拔掉安装介质。

你现在应该会有一个列出 Debian 的 grub 菜单。进入 Debian。之后，你就能看见登录界面。

输入用户密码之后，按回车键。

这就完成了！这样，你就拥有了一个全新的 Debian 系统。

修复 GNU/Linux 的引导程序

在一些情况下你可能会不小心损坏 GNU/Linux 操作系统的 GNU GRUB 启动引导程序，这时会导致操作系统无法正常启动停留在 grub 引导界面，这时你可以按以下步骤来修复它。

1.列出硬盘分区 首先，使用 *ls* 命令列出所有分区：

系统会显示出硬盘的所有分区，例如：

(hd0),(hd0,gpt0),(hd0,gpt1),(hd0,gpt2),(hd0,gpt3),(hd0,gpt4)

2.找到 grub 文件夹所在分区 如果系统的「/boot」文件夹没有单独分区（大多数人应该是如此），那么使用 `ls (X,Y)/boot/grub` 命令浏览所有分区，其中 X 代表硬盘号，Y 代表分区号，如：

`ls (hd0,gpt3)/boot/grub` 如果系统没有报错，显示出了文件夹下面的文件，那么该分区就是我们要找的分区，记下硬盘号和分区号。

同样的，如果系统的「/boot」文件夹单独为一个分区或者上一条指令没有找到需要的分区，则使用 `ls (X,Y)/grub` 命令，其中 X 代表硬盘号，Y 代表分区号。

3. 设置 grub 启动位置 输入 `set` 就会出现 *set root=(hd0,gpt3) set prefix=(hd0,gpt3)/boot/grub* 其它的笔记本可能会出现三行或者更多，只要使用 `ls (X,Y)/boot/grub` 没有出现 `error unknown filesystem` 那就把这个没报错的分区（假设是 hd1,gpt8）之前是 *root=(hd0,gpt3) prefix=(hd0,gpt3)/boot/grub* 修改用 *set root=(hd1,gpt8) set prefix=(hd1,gpt8)/boot/grub*

其中的硬盘号和分区号需要自行确定；grub 安装位置也需要自行确定，即第二行中，/boot/grub 根据需求替换为 /grub。

4.设置 grub 进入正常模式 通过以下命令，进入正常模式：

insmod normal normal 至此，grub 由恢复模式进入了正常模式，丢失的启动菜单应该能正常显示了，可以通过 grub 引导至系统。

5.更新 grub 引导 如果此时重启，问题依旧存在。所以我们进入 GNU/Linux 操作系统后，需要马上更新 grub 引导，对 grub 进行修复。在进入 GNU/Linux 操作系统后，在终端执行：

sudo update-grub sudo grub-install /dev/sda 至此，你可以重新启动，进入正常的引导界面了，丢失的引导就修复回来了。

智能手机“引起”个人信息泄漏的实质

一使用智能手机，各路骗子、推销商就会找上门来，网络骚扰也会持续不断，甚至“科学上网”稍有不慎某天还有可能被警方叫去“喝茶”……我们如今对这些甚至有些习以为常并且也很清楚这些问题背后的原因——个人信息被出卖给了商家、政府以及按照前两者的定义来说也属于“不法分子”的家伙。我们知道原因，却又仿佛难以避免这些糟糕情况的发生，以至于仿佛“一使用智能手机，个人信息就没法保护”，甚至在一些人看来“没有隐私”本身就是使用智能手机获得便利，所要必须付出的代价。可事实到底是什么呢？一块小小的智慧屏是如何带来大大的社会问题的呢？个人信息从用户输入手机，再由网络传给商家，传给“第三方”——那些用户所完全不知道的存在，中间经历了怎么样的过程呢我们的智能手机真的是“我们的”——真的忠诚于我们吗？不回答这些问题，我们就不能理解使用智能手机带来的个人信息泄漏风险到底从何而来。

在回答以上问题前，我们先指出一个很多人都没有充分意识到的事实——智能手机泄漏用户个人信息并不是天然存在的问题，任何**硬件**本身都是死的，它们不会对用户做任何事情一块放置在角落里，连电都不通的主板也确实只是一块废铁。

能对用户做出一些什么的只有**软件**，或者说**程序**。它们都是由程序员事先写好的“流程”，手机、电脑等一切计算机都能按照流程来自动处理信息。计算机能按照提前设定好的**“流程”，也就是**程序**，或者说**软件**处理信息，这一点的确大大加速了信息处理速度，但也埋下了隐患——如果某一台设备上存在一个应用程序在用户不知道的情况下自动运行，那么它就能背着用户收集用户的个人信息，如果还能保证网络通畅，它就能将这些个人信息上传至网络，幕后的操控者就等于在用户身边按了一个窃听器，而且这一窃听器足够先进，不仅能记录用户说出的话，发出的文字，甚至还能记录用户的行程轨迹，用户留下的个人影像。

于是，我们都知道的，应用程序背着用户偷偷搜集用户信息的事情每天每时每刻都在发生着，仿佛用的所有软件都具有如此糟糕的性质。这些瞒着用户监视用户行为的软件就必然属于源代码不向用户公开的**私有软件**，它们是操控权完全属于商家、政府、“不法分子”，而完全不属于用户个人的软件，用户也没法查看它们的源代码，调查研究它们到底是什么货色。私有软件泛滥而引发的赛博监控问题才是所谓“智能手机引发个人信息泄漏”的实质。

经过以上的分析，我们能看到，是私有软件的泛滥而不是智能设备本身导致了个人信息泄漏泛滥成灾。但有些人可能就会反驳“我们用的软件都是大公司开发的，分析这些软件是不是私有软件没有用”甚至觉得“按照我们的分析，所有软件都是私有软件”。但是，既然我们已分析出软件本身只是用来给计算设备自动运行的流程，具体要怎么编写和使用流程就是不一定的。大公司能开发软件来监视用户，用户是否可以也开发一些软件为用户自己所掌控，不受大公司控制呢?

这听起来似乎有点不可思议，好像不符合某些人对软件用户就该对软件工程一窍不通的刻

板印象，但别忘了最早的软件用户也是最先编写软件的人——程序员。并非所有程序员都甘受大公司的淫威，拿着貌似很高的工资，在 996 和狼性文化中“卷到死”，也并非所有程序员都觉得写一个自己不能掌控的软件来反对自己是“无所谓的”“自己只是个打工仔”。

早在信息技术刚刚开始在美国普及到民间的上个世纪 80 年代，就有一群不满于大公司淫威的程序员，面对大公司欺压用户，剥削程序员，还让程序员写他们控制不了的程序的现状发起了自由软件运动。他们曾以编写了 GNU 系统的理查德·斯托曼以及事实上为 GNU 系统编写了 Linux 内核的林纳斯·托瓦兹为代表，并已发展了 40 余年，积累成果颇丰。自由软件运动发起以来，这些自由软件早已走入生活的方方面面，只是还不为用户所熟知罢了关于自由软件的详细介绍可以参看这篇，这里不再赘述。

小结一下，个人信息泄漏问题是私有软件带来的，和硬件无直接关系，使用能保护用户隐私权的自由软件是能避免个人信息泄漏的。

在手机上实现软件自由保障信息安全

结合之前对自由软件的认识，我们可以问一个问题：在手机上使用自由软件就能保证信息安全了吗?

实际上并没有这么简单。那些使用了国产安卓的手机基本只有其 Linux 内核算是自由软件，而其操作系统的用户态部分则完全是私有软件——因为安卓虽然是自由软件，但其用户态部分使用的是允许私有化的版权许可证，而这些国产安卓的源代码又在哪里？它们一般都不会去实现手机存储区加密功能，甚至自行集成侵犯用户隐私的恶意功能者都不在少数，这就会导致，只要警方愿意彻底检查我们的手机，我们存储在手机上的任何信息都能被他们获知。我们自己设定的解锁手势和口令根本毫无用处——它们仅仅作为登录用户界面的鉴权令牌。只有那些使用了相对自由的安卓版本的手机才会去实现存储区加密，进而将解锁手势和口令用于解密存储区。

正如那篇《自由操作系统的重要性》中说的那样，操作系统作为最底层的程序，对其上的所有应用程序具有统治力，只有在自由的操作系统里，才谈得上实现软件自由。就如同只有在社会主义国家才谈得上无产阶级当家作主。

不幸的是，手机操作系统的自由实现得很不彻底，手机硬件所受的限制远大于电脑硬件，不仅仅是操作系统构架如此，甚至连硬件本身对软件的支持上来说都是如此[1]。因此，现阶段手机能达到的自由度不如电脑。

硬件自然是死的，但硬件的运行又离不开软件，这种直接和硬件发生作用，需要在特定硬件设备内部存储或运行，且一般不能由用户轻易替换的软件，被称为**固件**。存储在个人电脑主板的 rom 芯片中、负责初始化必要板载硬件并加载操作系统的 BIOS 也属于固件，目前其自由替代品已被开发出来，比较有名的有 coreboot。

在手机端，操作系统基本为苹果开发的 ios 和谷歌开发的 Android 所垄断，前者干脆搞封

闭，尽管用户可以通过“越狱”获得很大的权限，但仍不能完全掌控设备，不能停用一些和 ios 深度绑定，且旨在侵犯用户隐私的系统服务，并且它完全不给用户留一点自主选择第三方发行版的机会，其软件商店之中更是毫无自由软件的生存空间——哪怕其中的确有部分软件有公开的源代码，但因为用户无法在 ios 中安装自行编译的软件（违反了自由软件定义的第零、一基本自由），故仍然毫无自由可言；后者倒是大谈“开源”，可是又狡猾地绕开了左版（copyleft）的限制，搞出一套可以被全盘私有化的用户态框架，成为一个对用户限制重重的操作系统，尽管它是基于 Linux 内核开发的。

那么手机端的 GNU/Linux 操作系统呢？手机端的 GNU/Linux 系统确实存在（例如 sailfishos、postmarketos），但是配适的应用软件非常少，可用性不足。而想要在 Android 中把 Linux 内核解放出来，也不是一个轻轻松松的事情。

不过 Android 用户为了隐私安全还是建议各位刷入相对自由的第三方 Android，如 lineageos，rros 等。这些第三方 Android 操作系统架构仍然是 google 设定的，但少了谷歌框架等侵犯用户隐私的东西，其用户态框架属于尚未被私有化的非左版自由软件，还允许用户加密设备，在软件自由方面虽依然不足，但在保护隐私方面却也够用了。但这并非每一种型号的 Android 手机都能刷第三方 Android，只有那些可以“解锁”，且有专门适配该型号的第三方 Android 安装包的手机才能。至于 IThing 用户，我们只能建议您卖掉自己的烂苹果设备——非也，那是你交钱允许烂苹果派遣到你身边的电子狱卒。

在现阶段我们虽然不能在手机端实现彻底的用户自由，却能通过给 android 手机刷相对自由的第三方 Androuid 来保障用户隐私权。

那么该如何给我们的设备刷入第三方 Android 呢?

1.为设备解除 Bootloader 锁

为了限制用户更换 android 发行版本，各个手机厂家纷纷给设备上了 Bootloader 锁，简称“BL 锁”。我们为了给设备刷入第三方 Android，首先需要解开设备的 BL 锁。不同的厂家的不同型号手机有着不同的解锁方法。Bootloader （引导程序）负责加载操作系统的内核，所谓的锁，指的是引导程序仅会加载被厂商的私钥签名的内核，而解锁后引导程序方可加载任意内核。

Google pixel 的引导器还允许用户自行导入公钥，允许引导程序仅加载能被承认的公钥验签的内核。从这个意义上讲，只要 BL 锁能为用户掌控，也会成为用户数据安全的一道保障。

第一类设备是无法解锁的。代表是华为的设备。华为标榜着自己是“爱国企业”，却处处学习美国企业苹果，在烂苹果身后亦步亦趋，解锁它的设备早已变成不可能。对于这样的设备，我们仍然建议您赶快将它们卖掉（华为早期型号中有一部分可以解锁，这一部分尚可以尝试）。

第二类是解锁相对复杂，需要使用私有软件和解锁码的。代表有小米。小米的较新型号都需要通过向小米公司发送解锁申请，并凭借专用的私有软件将解锁码上传到手机中才能解锁而用户为了获得解锁码不仅需要等待，还需要向小米公司再次出卖自己的个人信息。

第三类是解锁比较简单，用户可以自行解锁的。代表是谷歌 nexus/pixel 系列的手机以及国产的 oneplus （一加）系列手机，用户可以使用 adb 和 fastboot 工具自行解锁。

第四类是没有 BL 锁的。这类设备包括了小米和三星的一些早期型号（比如小米的 redmi 1s），它们虽然没有锁，但型号本身过旧，设备性能不够用。

nexus/pixel 系列手机和 oneplus 系列手机，除了最新型号一时可能无可用安装包外，全系列均有安装包可用，且大多数型号的安装包至今仍在稳定维护中。刷相对自由的第三方安卓可优先考虑。

为了解锁，我们需要首先准备好 adb 工具和 fastboot 工具，并确保它们能够与手机建立连接。接下来以一部能用户自主能使用 adb 工具解锁的手机为例，说明用户如何自主解锁。

首先我们需要在手机上调出开发者模式。点开“设置”，在其中点开“关于手机”，找到“版本号”，并点击五到十次即可令开发者模式处于显示状态。之后我们返回上一级，选择“系统”，就可在其中找到开发者模式（在不同的安卓发行版中其位置会有些许不同）。进入“开发者模式”后找到并开启“ USB 调试”。之后在电脑上的终端模拟器里输入`$ adb devices`，然后在手机上确认连接。

之后我们就可以进入设备的 bootloader 页面，具体的进入方法有：

(1)通过手机按键进入

各种型号略有区别，但大都为同时长按音量键和电源键，音量键只需按住上键或下键中的一个，但不能同时按，同时按音量上下箭和电源键的作用是强制关机。

(2)通过 adb 工具进入

如果通过 adb 工具进入，则需要在电脑上输入`$ adb reboot bootloader`，等待片刻便能进入 bootloader 模式。

在手机上出现 bootloader 模式的页面后，我们在电脑上需要通过 fastboot 工具为手机解锁。解锁往往会清空用户数据，在解锁前应当备份好个人数据。

输入`$ fastboot oem unlock`，手机会提示是否解锁，选择确认即可。

2.下载设备所需的第三方 recovery 和 第三方 Android 安装包

我们需要先使用 adb 工具为手机刷入第三方 recovery 工具，然后再用第三方 recovery 工具为手机刷入第三方 Android。

第三方 recovery，我们推荐的有 twrp 和 lineageos 自带的 recovery（可在对应的安装包的下载页面下载到，比如 onelous5 的 lineageos 安装包下载页面同时提供 r 安装包和 recovery 的 .img 文件）。前者功能更强大，后者更能适应较新型号的安卓设备。

为了取得所需的第三方 Android 安装包，我们可以打开第三方 Android 之一的 lineageos 的 wiki 页面，看看您手中的设备型号是否能在这里找到。如果您没有找到，也可以选中“Show discontinued devices”，然后会将现在已经不更新维护的设备也展示出来。这些

不再维护更新安装包的设备也能刷 lineageos，但它们的安装包长期无法更新，安全性不如那些稳定更新的强。

如果您还是没有找到您的设备型号，那么大概率您的设备无法刷第三方 Android，我们建议您使用其他能刷第三方 Android 的设备，而现有设备先留下来，也许未来可能推出安装包，特别是对于一些新型号，安装包往往需要间隔几个月到一年多才会推出。

同时 lienageos 官方的下载页也提供安装包，但只提供仍在滚动更新中的。

3.为设备刷入第三方 recovery 和 第三方 Android 安装包

刷入第三方 recovery 同样需要在 bootloader 页面下操作，输入`$ fastboot flash recovery <对应的 .img 文件>`，等过程结束报“succeed”即说明刷入成功。

接下来进入第三方 recovery，进入方法有：

(1)通过 bootloader 页面进入。 google 的 nexus/pixel 系统手机和 oneplus 出的系列手机的 bootloader 页面允许用户使用音量键调整选项，并通过电源键选择，找到所需的“recovery”项选中即可进入 recovery 页面。

(2)通过手机按键进入。同样是长按电源键和音量键。一般情况下，如果手机进入 bootloader 页面时需长按音量下键和电源键，那么进入 recovery 页面则需要同时按住电源键和音量上键。反之亦然。

(3)通过 fastboot 工具进入。在手机处于 bootloader 页面时，在电脑上输入`$ fastboot reboot recovery` 即可进入。

twrp 的功能远比 lineageos 自身的 recovery 强大，支持备份、恢复主要分区的内容，一定程度上可用于将用户数据迁移到使用同一发行版的另一手机上，且 lineageos 自身的 recovery 仅能用于 lineageos，不能用于其他第三方 Android，比如 rros。第一次解锁刷机的手机最好使用 twrp 进行刷机。以下说明都以使用 twrp 为背景。

进入 twrp 后，我们不能立刻开始刷入第三方 rom，而是要将残存的数据清理（wipe）掉，选择“wipe”，选择“Advanced Wipe”，第一次刷机最好将 Cache、System、Data、Internal Storage 全部选中，然后滑动“Swipe to Wipe”，注意不要清理 vendor。清理（Wipe）后建议立即重启设备到 recovery，避免残留数据。

接下来可以选择两种方式刷机：

(1)将安装包本体传至设备上。我们可以通过 USB 传输将安装包包从电脑直接复制粘帖到设备上，然后在 twrp 里选择“Install”找到对应的 安装包。安装包是一个 .zip 文件。

(2)使用 adb sideload 不将安装包上传到设备上，而是通过 usb 传输的方式刷第三方 Android。在 twrp 里选择“Advanced”，选择其中的“ADB Sideload”，滑动“Swipe to Start Sideload”，等设备上准备就绪后。在电脑上输入`adb sideload <rom 包名称>`。

等过程结束后如果报 Succeed，则说明安装成功，可以重启设备进入相对自由的安卓系统。

如果报 failed，则建议再次清理（Wipe），并核对安装包的 sha256 值，或者以报错信息为关键词寻求搜索引擎的帮助。

刷机过程中会遇到各种意想不到的问题，欢迎大家详细向我们提出问题，本手册会根据大家的反馈意见更新。

五、网络安全和翻墙（重点）

方法 1 v2ray/mihomo（原 clashmeta）
优点：全平台，节点随便换，一般不限速，比较安全
缺点：可能需要每日换订阅/付费订阅不用（一般几块钱一个月）

V2RAY/MIHOMO/
mihomo 源代码仓库地址
https://github.com/MetaCubeX/mihomo
v2ray 源代码仓库地址
https://github.com/v2ray/v2ray-core

v2ray 安卓版直接地址（存在 GFW 限制）
https://github.com/2dust/v2rayNG/releases
mihomo 安卓版 （存在 GFW 限制）
https://github.com/MetaCubeX/ClashMetaForAndroid

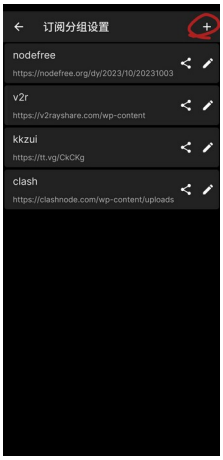
补充：GNU/Linux 端可用 mihomo/ v2ray （带图形化）
v2ray： https://v2raya.org/docs/prologue/introduction/
（系统激活进程以后 打开浏览器输入设置网址 http://127.0.0.1:2017/ 即可使用）
mihomo (需从源代码仓库下载发行版压缩包后手动安装)

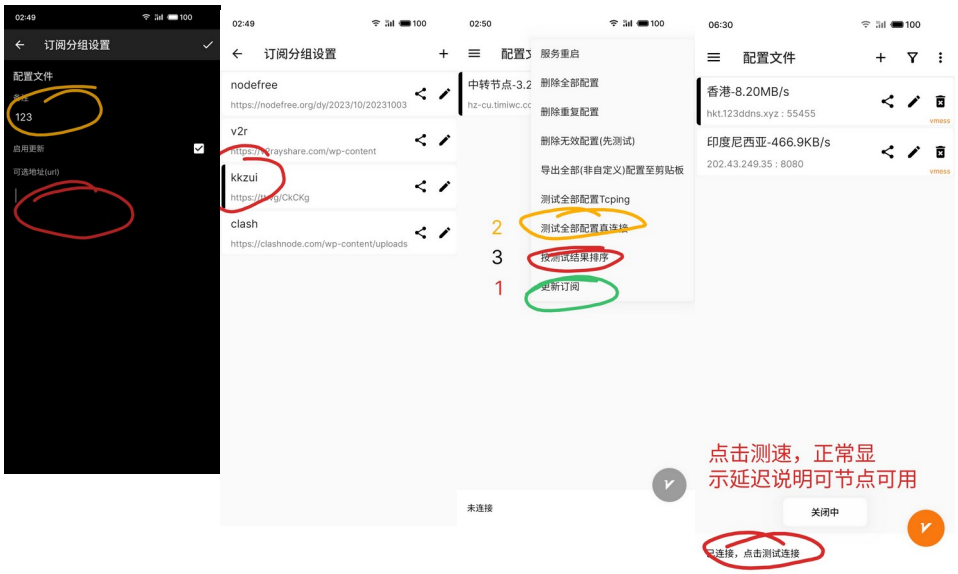
免费节点订阅地址：（需要每日手动更新，旧节点失效较快）
注：以下为私有平台建议使用 tor 网络匿名访问
https://clashnode.com/
https://v2rayshare.com/
https://nodefree.org
https://kkzui.com/

通过 Gitub 搜索节点：
https://github.com/ （存在 GFW 限制）
搜索 mihomo 订阅 v2ray 订阅

(mihomo 节点如果没有网址，就下载 yaml 文件， clash 里用文件导入)
尽量选择更新时间最近，点击量较高的。

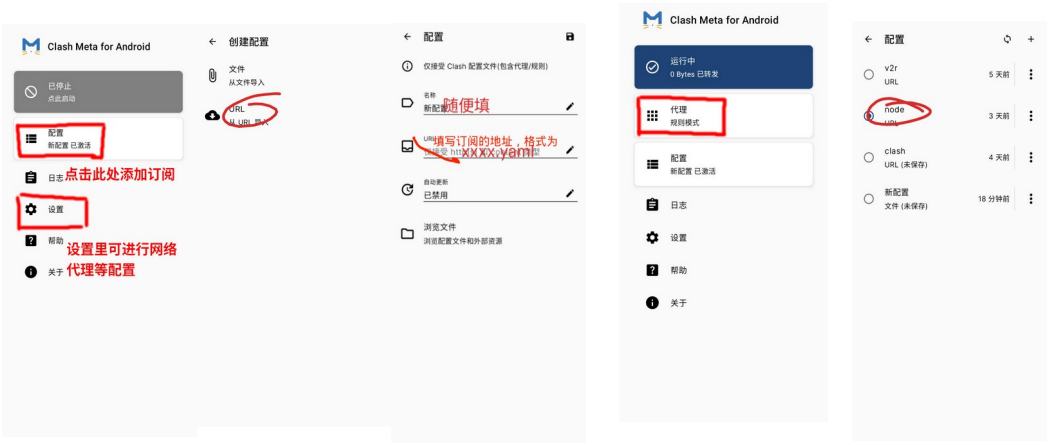
v2ray 的节点后缀为 txt;mihomo 的节点后缀为 yaml ,两者不能混用。打开软件 导入订阅 ，点击订阅选择订阅 ， 更新节点 ， 测速， 排序 连接， 连接测速使用,连不上换节点， 可以选择自定义哪些应用走 mihomo 提供的 vpn 。

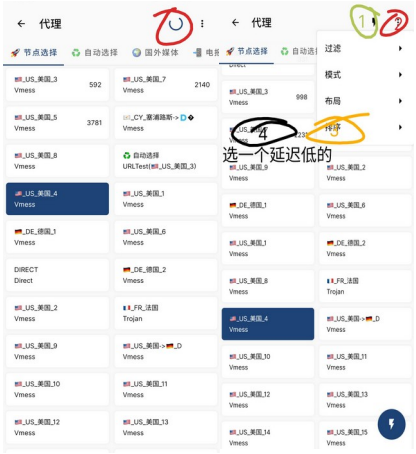




mihomo 点击配置添加订阅保存 点击勾选订阅 返回主界面 点击（已停止）来启动，点击代理选择节点

测速 排序 选节点 点击连接





（注意：GNU/Linux 的 mihomo 需要 系统设置手动代理 127.0.0.1 端口 7890，火狐浏览器需要在网络设置里配置代理服务器，或用插件 foxyproxy 代理管理代理服务器，设置 地址 127.0.0.1 端口 7890，然后切换到此代理）

好的时候可以高清视频无压力，差的时候就完全连不上。不同地区、时间段、网络运营商的实际测试效果都不太一样。

也有商人卖节点，小机场容易跑路、大机场稳定但收费高。基本上10G/ 元的价格。

结论：**安全性相对高**，节点的质量决定了上网的质量。节点获取途径较多，**建议大家掌握。**

1. Clash 软件教程

下载地址：

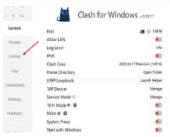
安卓端下载：github.com/Kr328/ClashForAndroid/releases

Windows 下载：github.com/Fndroid/clash_for_windows_pkg/releases

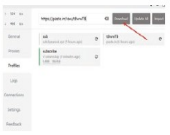
汉化：github.com/ender-zhao/Clash-for-Windows_Chinese/releases

使用教程：

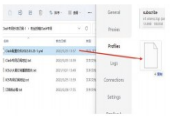
1.Clash 订阅有一键导入订阅和手动复制订阅两种选择。进入界面，先进入箭头所示 Profile(代理）选项。输入订阅地址（已失效，举例用），将其复制，点击粘贴。



再点击箭头所示 Download(下载），Clash 会自动拉取配置文件进行更新，如果一切顺利，你应当可以看到绿色提示信息「Success!」，并且可以看到一个新增的配置文件。



另外，如果有配置文件，直接按箭头方向拖进来也可以用。



回到初始界面常规项：开启系统代理，完成！（不开启就等于没翻墙）

说明：如果 Clash 用户看见很多节点失效不可用，建议换 V2ray 或者 winxray 进行使用！而且很多订阅地址下载是需要科学上网的，这点很不友好。

目前就电脑端 Clash 而言给我的使用感受越来越差，手机端还可以，主要是配置不方便。

但 Clash 的 **TUN** 模式可以实现**虚拟网关**，例如能看奈飞视频；**LAN** 模式可以设置其他设备的代理，实现局域性的**全设备翻墙**。这是它的**优势。**

很多机房被政府停机造成很多白嫖节点见光死！这也就是目前白嫖节点不耐用的原因，我想应该全网都是这样子！

2. V2ray 软件教程

下载地址：

V2rayN: github.com/2dust/v2rayN/releases

Xray: github.com/XTLS

V2rayNG: github.com/2dust/v2rayNG/releases

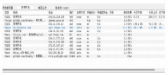
winXay: github.com/TheMRLL/WinXray/releases/tag/V4.3

电脑端：

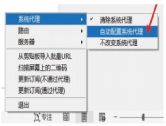
打开软件会出现在任务栏，点击进入。

此软件操作较为简便，先介绍手动导入。以图示节点为例：

选中全文→复制→打开 V2ray 软件→粘贴（Ctrl+V）



理论上来说导入的节点只要质量高，那就可以直接用了，比如上图的节点都可用。选中一个，回车，然后在任务栏中选择自动配置系统代理。（和 Clash 开启系统代理一样）



图标变成红色的就可以了。

之后订阅就更方便了。将准备好的链接，例如：https://v1.vmess.top/api/v1/client/subscribe?token=5a969759f72565a5f10c9f3b7af7eb2b，复制，进入软件 Ctrl+V 粘贴。或者进订阅设置里添加，之后更新订阅就可以了。

手机端：

点击订阅设置，点击右上角“+”号，在下方粘贴订阅地址，输入一个备注名称，点右上角确定。如图所示，上方的绿色为激活，下方的灰色为未激活。点一下就可激活。

回到软件主界面，点右上角，选择更新订阅。在下方一系列节点中任选一个，点击，然后再点 V 标，如图所示为绿色，并显示已连接，即可科学上网。

下面介绍的机场也会提供软件使用方法，此处不一一示范了。

3．如何寻找节点

接下来是最重要的部分：节点怎么找？有很多节点粘贴过来并不好用，测试超时或不稳定。公益节点大家都测速带宽就被占了，其他用户使用效果就差了。而且有些节点测速很高，实际体验并不好。

机场地址：

freefq.com/v2ray（免费翻墙网，每日更新 v2ray 免费节点）

jjkj5.com

www.paopaoyun.fun

okgg.xyz/auth/register?code=9Zgr

xmrth.com/auth/register?code=SHDO

www.paopao.dog/index.php#/register?code=oQgZ7hBw

teacat.cloud

科技分享


梦歌

破解资源君

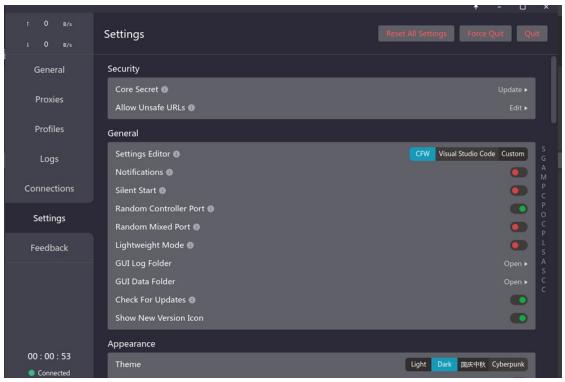

俊佳科技JJ

youtube 博主不良林的 tg 节点机器人（每 30 分钟自动更新 10 个节点）：@freenodeshare_bot

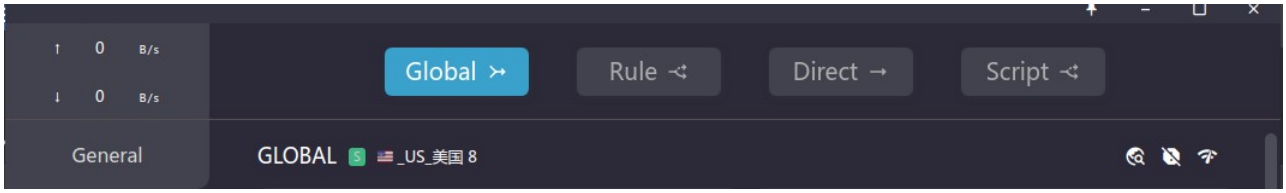
机场、油管、电报各种渠道都有人分享节点，已知几位 youtube 博主会不定时更新节点，梦歌的节点质量较高，更新频率低。以这些博主的分享节点，轻度上网还是可以满足的。各种 TG 频道也会分享节点，质量可能不错，但架不住人多。

进阶的安全科学上网（比如防止 DNS 污染和高危漏洞等）、v2ray 精通、clash 精通和节点搭建等内容，可自学不良林的相关教学视频。

最后附上 V2ray 软件测试节点 ping 值的方法，按图中箭头（或真连接延迟）点击测试即可。



profiles (添加订阅) 添加后点击 download 然后右键 导入成功的订阅 update 刷新节点
（*有些订阅链接可能存在 GFW 限制*）
Proxies 查看和连接节点（*wifi 标志为测速*） 可以测试后 左键点击连接



方法二 tor 洋葱网络

优点：

使用 tor 匿名网络，中间三次节点跳转，每次一跳转一加密，每个服务器自己也不知道流量内容，即使被知道所有服务器地址，因为采取的是众多服务器随行选三个来跳转，因此相对安全，比较可能的是进出口被抓流量，所以尽量使用网桥连接而非直连。

缺点：

速度较慢，因为要跳转节点来确保安全。

软件名：

orbot / InviZible Pro / tor browser
（tor bowser 为内置了 tor 代理的浏览器。）
（ Orbot/InviZible Pro 为移动端 tor 网络代理工具）

只有浏览网页的 tor 浏览器会默认使用集成的 tor，要让其他应用程序走 tor 网络代理 需要根据实际情况手动设置代理 ip 和端口号。

tor 浏览器官网下载地址 https://www.torproject.org/download/（存在 GFW 限制）

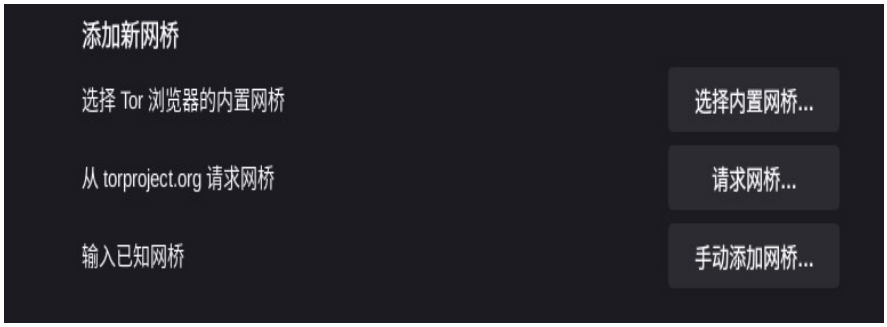
Orbot/InviZible Pro 可在 F-droid 下载

使用 GNU/Linux 下载 tor 可以将软件源替换为国内源后用应用商店或者终端指令下载
比如 GNU/Linux 发行版 manjaor：终端输入 sudo pacman -S yay （安装 yay 商店）
yay tor （通过 yay 安装 tor 浏览器）
选择安装正确版本(如下图)

A 获取网桥

tor 网络目前受 GFW 屏蔽严重，需要用网桥连接（能直连也最好别用，特征太明显），以 tor 浏览器电脑版为例，讲解网桥

1.自动获取网桥
软件内连接
设置—— 连接（定制网桥）-添加网桥-确认后连接-等待连接成功（首次连接较慢）

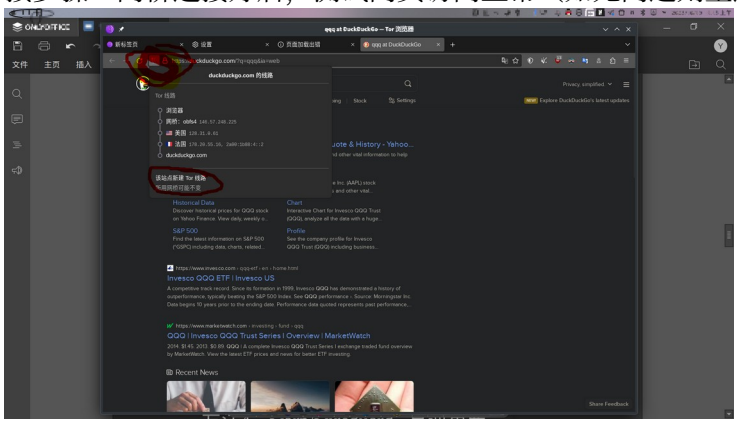


三种网桥模式对比（如上图）

内置网桥 和请求网桥 都连接不上，说明屏蔽当地屏蔽比较严重，需要手动获取网桥

2.手动获取 获取网桥方法：
匿名邮箱发送空白邮件给 bridges@torproject.org ,收到网桥地址格式如：
obfs4 75.134.106.30:42539 90348959527F525394CB9A2BAA8FF1338BC08EE7 cert=ghcbxHarg5xNSk69iy61kMiieEnHdbZadrpaznSvF4VtfNH0CXAidIJ22yyH9v582m39dA iat-mode=0
连接不上换一个桥，再发一次空白邮箱
此 app 可以选择哪些应用使用 tor 网络

如无速度则点新身份/刷新 更换节点
按步骤 A 网桥连接好后，测试网页访问正常（如无网速则重连如网速慢则换节点/换网桥)



B 其他应用走 tor 代理
tor 的默认本地 ip 和端口 为：
127.0. 0.1 9150/或者 9050
代理模式为 socks5
tor 浏览器连接好以后别关浏览器
（1）系统全局：

GNU/Linux 发行版 manjaro
系统设置-网络-代理服务器-手动地址
地址 127.0.0.1 端口：9150
然后所有应用都走 tor 网络

orbot/InviZible Pro

运行软件后点击启动即可,
点击 配置连接方式-定制网桥-下一步- 内置网桥/获取网桥/手动输入网桥地址（看上文如何获取网桥）-点击连接-点击启动
InviZible Pro 设置 快速设置 -网桥（可开启 dns 保护和 i2p）

（orbot 不许截图所以无图片另外新版默认开启 vpn 模式，可启用“高级用户模式”禁用 vpn 功能，而仅保留代理功能。）

连接后无网速点击刷新 更换节点
设置里可以指定 app 走 tor 网络信道 ， 默认是全局

备注：orbot 的代理地址和默认端口为 地址 12.0.0.1 端口：9050
另外如果非要插卡使用蜂窝网络（当然我们非常不推荐在你的自由软件系统设备上这样做）使用 orbot/InviZible Pro 来连接 tor 网络时请务必通过网桥来连接。
(*一般情况下我们都不推荐通过前置代理来连接 tor 网络，因为 tor 的 obfs4、snowflake 等网桥的特征远弱于 shadowsocks、v2ray 等国人一重隧道方案，把 tor 放在这些隧道里不过是欲盖弥彰。*)

VPN 和代理的区别

在绝大多数**场景**下, 我们提到 VPN, 实际上是代指访问外网. 其实, VPN 和我们平时使用的软件有着本质的区别.

能够实现外网访问功能的软件总共有两种类型 : VPN, 代理.

代理软件其实还可以细分为 TUN/TAP 代理和系统代理 两种. 接下来的内容中, 我们会一一详细介绍.

一. 什么是 VPN

VPN 的全称是 Virtual Private Network, 中文名称是 虚拟私域网络. VPN 出现的主要原因是为了将不同局域网连接起来,组成新的局域网.

初次接触这个概念可能会有点懵, 我们来仔细说说.

1. 案例

我们举个例子, 公司有一台服务器, 在局域网中的 IP 地址是 192.168.1.10. 我们连接上公司的网络之后, 通过这个 IP 地址就能访问到这台服务器.

但是一旦我们回到家中, 就没有办法访问这台服务器了. 原因就是电信运营商根本不知道 192.168.1.10 这个地址在哪.

2. 解决方案

想要解决这个问题, 有两种方案.

方案一 : 配置公网 IP

给服务器购买一个公网 IP, 这样, 公司的这台服务器就能在被公司外部的网络访问到了.

这种方式是非常不靠谱的. 公司那么多服务器, 不可能每台都购买一个公网 IP, 有钱也不能这么花. 而且, 将公司的设备直接暴露在公网中, 会增加被攻击的风险.

方案二 : VPN 组网

简单来说, VPN 组网的原理是用一台拥有公网 IP 的服务器作为中间人, 多个局域网都和中间人进行互通. 当一个局域网中的设备访问另外一个局域网中的设备时, 会先将请求转发给中间人, 中间人在分析路由之后, 再将请求转发到真实的目的地.

通过一系列的复杂操作, 我们实现了多个局域网之间的互通. 将广域网中的多个局域网组成了一个更大的局域网. 这个新的局域网内部是互通的, 但是对外屏蔽.

因为 VPN 中的多个局域网之间通信是利用了广域网的线路, 所有, 局域网之间的通信是严格加密的.

这就是所谓的虚拟私域网络. VPN 主要用于大型公司多个子公司之间的保密通信.

3. 总结

当我们拥有一台处于墙外的服务器作为中间人, 将自身所在的局域网和墙外的广域网进行组网之后, 就能够实现访问外网的需求. 但是, 我们也能明显看出来, VPN 并不是为了访问外网而生的. 这只是其衍生功能而已.

VPN 的技术难度非常高, 对于大部分人, 根本不具备这个条件. 而且通信速度较慢.

二. 什么是代理

使用一台新的设备, 帮助当前设备完成所有的网络通信, 这种技术我们称之为代理

1. 解释

正常的生活中, 我们想要购买商品, 就需要自己跑到商店, 提出要求, 然后商店老板会将商品交给我们.

这个过程中, 我们跟商店老板之间是信息公开的, 他是知道是谁买的商品.

如果我们要买的商品比较隐私, 害怕别人知道, 那该怎么办呢?

很简单, 我们可以找一个人, 帮我们去买. 这样商店老板就不知道其实是我们购买的商品. 帮我们跑腿的这个人, 就称之为代理人.

网络访问中也是一样, 个人电脑想要跟目标服务器通信, 就需要先跟目标服务器建立连接, 然后相互传输数据. 这时,目标服务器清楚的知道是个人电脑在跟他通信.

如果我们在中间加了一台服务器作为代理服务器, 当个人电脑想跟目标服务器通信的时候, 先将目标服务器的地址告诉代理服务器, 让他跟目标服务器建立连接. 然后个人电脑再将通信的数据交给代理服务器, 让他转交给目标服务器.

这样也能实现跟目标服务器的沟通. 而且目标服务器并不知道, 其实是个人电脑在跟他通信.

说了这么多, 其实就是想告诉大家, 代理技术就是利用代理人跟外部沟通, 从而隐藏自身信息. 降低暴露的风险.

2. 总结

代理技术的重点在于请求的转发 : 从个人电脑转发到代理服务器, 从代理服务器转发到目标服务器.

其主要目的是为了隐私保护. 整个通信流程其实可以不用加密, 整体的通信效率相较于 VPN 要高很多.

当然, 如果我们有一台位于墙外的服务器作为代理服务器, 也能够实现访问外网的需求. 但为了避开监管, 就必须要对数据进行加密.

市面上的所有 VPN 软件, 虽然名字叫 VPN, 但是使用的都是代理技术.

这里还有一个重要问题, 如何将个人电脑的请求交个代理代理服务器处理呢 ?

主要有两种方案 : TUN/TAP 代理, 系统代理.

我们接下来继续为大家介绍

三. TUN/TAP 代理

TUN : tunnel 隧道

TAP : network tap 桥接

1. 解释

这种技术的重点在于在个人电脑中建立一张虚拟网卡. 我们都知道, 电脑中的数据想要发送出去, 肯定需要依赖网卡, 所有的数据都必须要经过网卡才行. 利用这一点, 就能完成流量的收集转发.

具体实施步骤是 :

我们先在电脑中创建了一张虚拟网卡, 设定路由, 将电脑的流量都指向虚拟网卡. 虚拟网卡再指向物理网卡. 然后启动软件, 对虚拟网卡接收到的数据进行封装, 重新设定目的地为代理服务器. 之后将封装过的数据还给虚拟网卡. 虚拟网卡会继续将数据交给物理网卡. 这时, 物理网卡就会将数据发送到代理服务器上.代理服务器在收到数据之后进行解封, 获取到原始的数据, 从原始数据中我们能够获取到真实的目标服务器地址, 最后将数据发送过去即可.

2. 总结

TUN 和 TAP 的区别在于收集数据的层级不一样, TUN 是在网络层收集数据, TAP 是在数据链路层收集数据. 在实际使用中区别不大. 而且都是依赖虚拟网卡工作. 所以被归为一类.

TUN/TAP 代理几乎可以收集个人电脑中的所有网络请求. 在移动端也能完美支持. 市面上的大部分加速器就是使用的这种技术.

想要读取虚拟网卡的数据, 就必须要调用平台自身的 API, 也就是说, 想要开发一款 TUN/TAP 代理软件, 就必须要使用平台自身的语言. 比如说 MacOS 的 Swift 语言, Windows 的 .Net 语言, 安卓的 Kotlin 语言, 第三方语言无法使用.

所以软件的开发难度较大, 尤其是在跨平台的情况下, 需要程序员会多门语言.

四. 系统代理

每个操作系统有预先设定了代理功能. 一般我们只需要填写上代理服务器的 ip 地址和端口号, 操作系统就能帮我们将个人电脑的请求转发到代理服务器. 省去了创建虚拟网卡, 封装数据的过程.

1. 执行流程

当我们开启了操作系统的代理功能之后, 一旦操作系统发现有请求发出, 就会先阻拦住请求. 操作系统跟代理服务器进行沟通, 先将本次请求的目的地址发送给代理服务器, 然后再将数据发送给代理服务器.代理服务器在收到目的地信息之后, 和目标服务器建立连接. 在收到通信数据之后, 转发给目标服务器即可.

2. 总结

系统代理的操作和开发难度极低. 开发者只需要将注意力放在代理服务器上. 在代理服务器上实现接收数据, 转发数据的功能即可.

而且, 如果想要开发自己的软件, 只需要会一门语言即可. 像 Java, Go, JS 这种第三方语言都能轻松开发自己的代理软件.

当然, 有利就有弊, 这种方案的弊端也很大.

无法收集所有的请求. 只有那些使用系统语言开发的软件, 或者使用第三方语言开发的软件进行了特殊设置, 支持系统代理功能. 才能被系统代理转发.

比如说在 Windows 平台上, 我们可以使用 Java, Go 等其他第三方语言开发桌面应用. 但这些语言开发的软件如果没有特殊设置, 就不支持系统代理. 从这些软件中发出的网络请求就无法被系统代理拦截转发. 部分操作系统支持的代理协议版本较低, 无法代理 udp 协议的请求

比如说 Windows11 就只支持 socks4 代理协议, 这种协议是不支持 UDP 协议的对移动端的支持极差.

这种方案只适用于那些平时访问外网时以浏览器为主(浏览器完美支持系统代理), 或者使用少部分系统自带的软件的用户.

当然, 平台不同, 对系统代理的支持也不同, 比如说 MacOS 系统中, 绝大部分软件都是使用平台语言开发的, 都能使用系统代理. 但是 Windows 中的情况就是反过来的.

五. 区别

我们从开发难度, 网络通信速度, 数据收集率 , 是否可以自定义加密对以上几种方案进行总结.

(这里, 如果软件可以自定义加密方式, 就能极大的提升通信速度)

名称	开发难度	网络通信速度	数据收集率	能否自定义加密
VPN	高	慢	完全	否
TUN/TAP 代理	高	快	完全	是
系统代理	低	快	部分	是

六、F-Droid 应用商店

F-Droid 是一个安卓平台上自由开源软件的应用商店，并提供下载安装支持。使用客户端可以更轻松地浏览、安装及跟进设备上的应用更新。例如**小企鹅输入法**、**简单图库**等自由软件都可以从上面下载到。进入 app 后，请下拉刷新以更新储存库（有时更新比较慢，需要耐心等待，失败时多试几次，实在无法更新可以考虑临时使用代理来完成更新），否则应用商店里边看不到任何内容。

官网：https://f-droid.org/ （存在 GFW 限制）
安卓客户端下载：https://f-droid.org/F-Droid.apk（存在 GFW 限制）
通过镜像源下载：https://mirrors.tuna.tsinghua.edu.cn/fdroid/repo/org.fdroid.fdroid_1018050.apk
应用图标：

七、XMPP 即时通讯（重点）

XMPP 的全称是“Extensible Messaging and PresenceProtocol”，一个说明书给出的参考翻译为“组件式在线通讯协议”。它是一套世界通用的自由通信标准，是一套用于机器程序之间的稳定通信规则，遵守此规则的应用程序们可以顺利地一起对话。XMPP 的公共服务器由世界各地的志愿者们架设，提供免费且没有歧视的服务。它不依赖于中央服务器，所有的公共服务器都可以和其他公共服务器建立通信，也就是说，并不会因为一个服务器无法使用而导致用户根本无法使用公共的 XMPP 服务。所以它更难以被资产阶级政府所控制。

(1)我们为什么要使用 XMPP

简而言之，XMPP（又称为 Jabber）是一种开放的互联网实时通讯协议。很多流行的聊天软件都是 XMPP 的封装应用，比如 Google Hangout、Facebook Message、AOLChat、米聊、人人桌面和陌陌等。很多网络游戏的内部聊天用的也是 XMPP 协议。

与通常我们使用的集中式架构的私有通讯软件（如 QQ、微信）不同，采取邦联式架构的自由 XMPP 客户端与服务器、服务器之间的通信使用的是公开而标准化的协议——这保证了任何人都可以参考这些标准开发出可以和系统中其他组件互操作的组件，甚至可以自己搭建服务器，为自己提供服务。通过 XMPP 所支持的“不留记录即时通讯协议（Off-the-Record Messaging，缩写为 OTR，原理见网址），可以实现端到端通讯的加密，从而保障“私聊”的真正“私密”性质和通讯的安全性。

我们推广 XMPP 是希望推动这种开放的聊天协议和自由软件的使用，用 XMPP 配合 OTR 或 OMEMO 的端对端加密聊天，替代传统封闭的、有隐私泄漏风险的私有软件。

(2)安装客户端

支持 XMPP 的客户端有很多，这里仅选取经过 BLUG 成员测试挑选之后，最适合自由软件社群的。以下所列均为自由软件。

PC 客户端：推荐使用 Pidgin，GNU/Linux 发行版可通过包管理器搜索“pidgin”来安装也可以从 https://pidgin.im 下载源码包编译安装。Windows 可前往 https://pidgin.im 网站下载二进制安装包，但 Windows 作为私有系统存在安全隐患，且 Pidgin 的 otr 插件和消息反馈插件需要额外下载。最好的做法是把它换成 GNU/Linux，并在 GNU/Linux 安装 pidgin。Pidgin 支持通过额外插件拓展功能，实现完整 otr 加密，pidgin 使用的 otr 插件—— pidgin-otr 也可以在通过 GNU/Linux 发行版的包管理器下载安装。

移动客户端：Android 系统强烈推荐 blabber.im，支持 omemo 加密。可以直接访问 https://f-droid.org/en/packages/de.pixart.messenger/ 下载 blabber.im, 这样只能安装到网页提供的 blabber.im 版本，不能及时更新 blabber.im。更推荐的做法是先下载 f-droid 的客户端，并通过 f-droid 客户端下载 blabber.im。首先前往 https://f-droid.org 下载安装 F-Droid 市场，然后更新包缓存，之后就可以搜索并安装 blabber.im 了，这样能及时更新 blabber.im。f-droid 是提供自由软件的自由的应用商店，强烈推荐在手机上安装一个。有余力的可以尝试使用 xabber 2.0.1 版本实现比较完整的 otr 功能。

对于苹果设备来说，iOS 系统上的 chatsecure 的 iOS 版勉强可用，macOS 也可暂且使用 Adium，可以从 https://adium.im 网站下载到。不过它们都不好用，往往会丢消息，只有越狱并设法禁止自动挂起网络才能彻底解决这个问题。烂苹果这个自诩比用户自己还懂用户的需求的暴君，通过一系列恶心的设计，把为 iOS 用户提供邦联化的即时通信服务变得难如登天，而这个工作本应仅仅需要一条持久 TCP 连接和客户端断线时重连。基本上想为 iOS 实现即时通信服务就必须在一定程度上放弃邦联化，开发者还必须接受烂苹果的盘剥才能保证其用户能及时收到消息，这使得 iOS 能用的即时通信服务基本上都是圆形监狱。因此最好的办法是换掉苹果设备。

(3)注册 XMPP 账号

常使用的还是通过客户端直接注册。注册时需要选定一台服务器、填写用户名和密码后，就可以得到形式和电子邮件地址类似——“用户名@服务器”的身份标识——JID 了。

电脑端的 pidgin 使用同一个界面来操作“创建新账号”和“添加现有账号”的功能，仅仅通过类似“在服务器上创建此账号”的选项来区分。

手机端的 blabber.im 可以在初次登录时，在登录界面的右下角点击“创建新帐号”，然后写上用户名，并通过“选择您的 jabber 提供商”来选择服务器。如果 blabber.im 默认提供的注册服务器没有您喜欢的，也可以选中“使用自己的服务器”，然后在填写用户名处以“用户名@服务器”的格式填写您需要的 JID 实现注册。密码需要在下一界面填写。

互联网上有很多开放的 XMPP 服务， 在正式尝试在服务器上注册帐号之前建议用 xmpp 观测站服务（https://xmpp.net/ 和 https://check.messaging.one/ ）检查一下服务器的特性，然后顺着 xmpp 观测站服务提供的 xmpp 服务器官网链接在官网上注册。

不建议在少数几个服务器上扎堆，这样会丧失邦联制的优势，容易被针对封锁服务器，同时信息大规模泄漏的风险也会更大。

(4)基本设置及登录使用

1. blabber.im **的使用**

登录

初次登录时，在登录界面的右下角点击“我已有帐号”，然后输入 JID 和密码后点击下一步，昵称和头像设置可保持默认。登录如果失败，请检查 JID 是否完整，一个完整的 JID 应是 xxx@xxx，例如 suibianjugelizi@dismal.de，检查登录时是否正确输入。

设置

需要在“开始会话”界面（左上角会显示这四个字），点击右上角的三个竖点，找到“设置”。

blabber.im 设置中建议进行的操作有：

I.打开“专家模式”中的“启用多个账户”； II.打开“专家模式”中的“使用 DNSSEC 验证主机名”； III.关闭“安全和数据保护”中的“显示位置预览”； IV.打开“用户界面”里的“彩色名称显示对方状态”（如果不选择“隐藏联系人”）。

如果您已经“启用多个帐号”，那么点击右上角的三个竖点，会出现“管理账户”，在“管理账户”界面，点击右上角带“+”的小人进入一个新界面，以“用户名@服务器”的格式填写您需要的 JID，输入您需要的密码，选中或不选中“在服务器上注册新账户”，可进行注册或者多用户登录。

2. pidgin

pidgin 使用插件架构支持各种协议及其扩展，将插件文件（主体部分为动态链接库）放入插件所在的目录（pidgin 的安装目录下的一个叫 plugins 的子目录），重新启动程序，即可在“工具”菜单下的“插件”对话框中启用并配置。

使用 pidgin 之前，需要先安装两个插件：

OTR 插件

用于实现上文所述的 OTR 加密协议。

GNU/Linux 可以在通过 GNU/Linux 发行版的包管理器下载安装 pidgin-otr。

windows 可下载 https://otr.cypherpunks.ca/index.php#downloads 中的 https://otr.cypherpunks.ca/binaries/windows/pidgin-otr-4.0.2.zip，并将其全部内容放入 pidgin 的插件目录，插件名为 Off-the-Record Messaging，有额外选项。

消息反馈插件

用于得知消息成功送达对方（以及成功解密，在使用 OTR 时），启用后成功送达的消息后面会出现对勾。

遗憾的是 Debian 的软件源中并未收录 pidgin-xmpp-receipts 插件，最好的方法是通过源代码从头编译它。

先通过 GNU/Linux 发行版的包管理器下载安装 git，然后打开终端模拟器，输入`$ git clone https://github.com/noonien-d/pidgin-xmpp-receipts` 获得 pidgin-xmpp-receipts 的源代码。之后输入`$ cd pidgin-xmpp-receipts`，进入源代码所在的目录。然后输入`$cat README.md`，会显示 pidgin-xmpp-recipts 的编译和安装流程：

```
pidgin-xmpp-receipts
====================

This pidgin-plugin implements xmpp message delivery receipts ([XEP-0184
v1.2](https://xmpp.org/extensions/xep-0184.html)).

When no delivering confirmation is displayed, it is also possible that the
receiver doesn't support the extension.

Compiling
---------
To compile the plugin, run
>       $ make
You will need pidgin development packages
(link in ubuntu: libpurple-dev and pidgin-dev).

Installation
------------
To copy the extension to your personal plugin folder (~/.purple/plugins)
run:

>       $ make install
Now you may activate the extension within the pidgin settings.
```

认真阅读 READ.md，严格按照它的提示进行安装操作。

对于 Debian GNU/Linux 用户来说，需要先检查是否安装了 libpurple-dev 和 pidgin-dev，不安装它们后续的编译工作将无法完成。在确认安装了 libpurple-dev 和 pidgin-dev 的情况下，按照 READ.md 的操作，先输入`$ make`，后输入`$ make install` 即可完成 pidgin-xmpp-recipts 插件的安装操作。

当然也可从可信的渠道得到编译过的 pidgin-xmpp-recipts.so 二进制文件，将它放入 ~/.purple/plugins 中，注意 .purple 是隐藏目录。

windows 可下载 https://app.assembla.com/spaces/pidgin-xmpp-receipts/documents 中的 xmpp-receipts.dll 放入 pidgin 的插件目录即可，插件名为 XMPP Receipts，无额外选项。

pidgin 的登录

Pidgin 支持很多协议。如欲添加 xmpp 账号，请在“管理账号”对话框中点“添加”，“协议”选 xmpp、“用户名”填@之前的部分，“域”填@之后的部分，再输入密码。

注册新账号和添加已有账号靠下方的“在服务器上创建此账号”选项区分。

设置

强烈建议将账户配置的“高级”选项卡中的“连接安全性”选项设置为“需要加密”。并启用上述两个插件。

添加好友和聊天

在最基本的情况下，知道对方的 JID 就可以和对方用 XMPP 通信了，当然更方便的做法是将对方添加为自己的联系人。不过对方有可能不在线，因此你往往需要向对方提出申请，让他的客户端主动告知你他的在线状态（虽然大部分客户端都可以在将对方添加为联系人时自动向对方提出申请，同时自动向对方启用告知自身的在线状态，但还是有少数场景需要手动提出申请）。

聊天时，在 pidgin 上，请在开启 OTR 插件后，于聊天页面最上面一栏最右侧点击小人头像启动私密聊天。blabber.im 的 omemo 加密是默认开启的。

注意，pidgin 上的 OTR 启用后，默认的自动聊天记录归档会对该会话禁用（可通过插件的选项配置）。如仍需对该会话归档，请使用“对话”菜单中的“另存为”功能。

加密聊天建立后，还可以通过保密问题或直接验证指纹的方式对对方身份进行验证。

八、Lemmy 自由贴吧

Lemmy 是一大套自由的去中心化的论坛，就像百度贴吧、Reddit 一样，但是 lemmy 与这些网站的根本区别之一就在于，lemmy 是一个自由的视频平台，使用 lemmy 的各个服务器能互联互通，还可以保持独立自主，形成邦联宇宙。用户完全可以选择自己喜欢的浏览器或 APP（主要是 **lemmur** 和 **Jerboa for Lemmy**）来访问这些服务器（实例）。

实例查询：

https://fedidb.org/network（需要在“software”处将要找到的邦联制社交媒体类型由“ALL”改为“Lemmy”，内容更多）

https://join-lemmy.org/instances（适合寻找能快速注册的实例）

注册账号：

虽然大部分 lemmy 服务器都支持注册，但那些用户最多、知名度最高的 lemmy 服务器，比如 lemmy.ml、lemmygrad.ml 往往限制新用户注册，用户不仅需要认真回答管理员设

置的问题，还要等待管理员审核，通过才算注册成功，因此我们首先不去考虑这些服务器。通过上述的实例查询网站，用户可以根据自己的需求进行查找。推荐新手先找适合快速注册的实例进行注册。
需要注意的是，用户在哪个服务器上注册了帐号就只能在哪个服务器上创建社区，不能跨服务器创建社区，如用 lemmy.ml 的帐号在 lemmygrad.ml 上创建社区就是办不到的。
更为重要的是，**不要在一个实例上扎堆注册，也不要为了关注一个社区就在它所在的服务器上注册**！！！这样做容易让单一的服务器不堪重负，也会促成新的私有社交媒体诞生，更难以有效应对资产阶级的攻击。

一些实例不要求强制用邮箱注册，但有一些要求，甚至有些实例要求回答问题并让管理员审核才能注册成功。
验证不同服务器的互联互认：
比如您想知道某服务器是否能关注位于服务器 A 上的 B 社区，您可以输入如下的网址格式：**欲测试的服务器的地址/c/社区 B 名称@社区 B 所在服务器 A**，比如，您可以输入 https://community.hackliberty.org/c/hackerfederation@exploding-heads.com 来看看是否能从服务器 https://community.hackliberty.org/访问到 hackerfederation 社区，如果能访问，便可看到社区的内容，进而可以选择在这个服务器上注册自己的账号；如果不能访问，就会提示“404: couldnt_find_community”。
需要注意的是，当您所在的服务器和社区所在服务器不相同的情况下，想输入社区名称必须加上后缀 **@服务器地址（例：@exploding-heads.com）**，而如果您不加此后缀，查找社区只会在您所在的服务器查找，会出现和您想要进入的社区不相符的情况。
参考：https://exploding-heads.com/post/61705

九、Peertube 自由视频平台

以下内容大体和 Lemmy 相似。
Peertube 是一大套自由的去中心化的视频平台，用户们可以在上面观看视频、写评论、上传自己的视频，就像 YouTube、bilibili 一样，但是 peertube 与这些网站的根本区别之一就在于，peertube 是一个自由的视频平台，且所有人都可以使用 peertube 的源代码去构建自己的 peertube 网站。各个网站运行的软件支持一种或多种遵循开放标准的通信协议（protocol），而其中最主要的通信协议则是 ActivityPub，它们可以以此互联，形成邦联宇宙。
建立的这个新视频网站一般被称为一个 peertube 的**实例**（instance）。在这个新实例当中，管理者可以自己设定各种权限和事项。此外，大多数 peertube 的实例域名并不包含 peertube 字样。目前所有的 peertube 实例接近九千个，而 peertube 的第一个稳定版本则是 2018 年 10 月才发布的。
以 https://peertube.su 为例，如需注册或登录，点击左上角即可看到注册通道。进入"我的设置"页面可以设置对敏感视频的默认策略，偏好语言，是否使用分享系统，是否自动播放，是否自动连播，主题等内容。

实例查询：
https://joinpeertube.org （点击 see the instances list 查看）
https://instances.joinpeertube.org
https://fedidb.org/network?s=peertube

推荐实例：
https://peertube.su
https://wirtube.de/
https://peertube.uno/
https://libre.video （这三个相对比较容易注册）

https://video.ploud.jp（该实例上中文内容较多）
其他有趣的实例还请读者亲自探索。
参考：https://exploding-heads.com/post/87757

十、文件传输

利用专门进行文件传输的 firefox send 服务器进行安全加密的文件传输。直接使用 xmpp 的服务器传输会受到服务器寄存文件大小的限制，不方便传输稍大或很大的文件。
链接：https://github.com/timvisee/send-instances/
此链接里收录了诸多服务器路径和相关属性（URL、文件大小上限、文件保存天数上限、最大下载次数、服务器所在国家、版本等信息）
注意：不推荐用私有浏览器进行下载，容易出现下载失败和保存文件失败的情况，建议使用符合 W3C 标准并支持 Firefox Send 功能的自由软件浏览器，例如 Firefox 浏览器，Fennec 浏览器，Cromite 浏览器，Brave 浏览器，Chromium 浏览器等等。

①选择服务器，上传想要传输的文件

②设置文件最大下载次数和最大寄存时间。超过下载次数和寄存时间，下载链接会自动销毁。还可以设置下载密码。不同的服务器时限和次数都不同，需要根据需求选择合适的服务器进行传输。

③上传完毕后，复制链接或二维码。其他人可以通过链接和二维码下载你想要传输的文件。

以下列出一些常见的 firefox send 非官方实例

https://send.vis.ee (2.5GB, 7 days) (maintainer, contact)

https://send.zcyph.cc (20GB, 365 days) (maintainer, contact)

https://send.turingpoint.de (8GB, 30 days) (contact)

https://send.ephemeral.land (8GB, 28 days)

https://send.mni.li (8GB, 15 days)

https://send.monks.tools (5GB, 7 days)

https://send.boblorange.net/ (5GB, 7 days)

https://send.aurorabilisim.com (2.5GB, 7 days) (contact)

https://nhanh.cloud (2GB, 30 days)

https://send.datahoarder.dev (1GB, 1 day) (maintainer, contact)

https://fileupload.ggc-project.de (2.5GB, 7 days)

https://drop.chapril.org (1GB, 5 days) (contact)

https://send.jeugdhulp.be (50MB, 10 days) (contact)

https://files.psu.ru (16GB, 7 days)

https://send.portailpro.net (10GB, 30 days)

https://bytefile.de (5GB, 7 days)

https://transfer.acted.org (5GB, 7 days)

十一、记事本

安全的记事本，可供多人编辑和查看，适合记录小组内的私密信息。
网址：https://pad.chapril.org/
https://privatebin.support-tools.com/（剪贴板）

十二、加密货币

注意：尽管加密货币通常是自由的，但购买加密货币的平台却大多是私有的，在选择时请注意甄别。

如何选择加密货币

比特币和其他“主流加密货币”不完全是匿名的，不建议从交易平台上购买比特币并直接使用。因为比特币等在区块链上把区块链的数据公开，这意味着每个人都可以看到交易记录。据称利用 BitIodine（一个用来实现大型比特币交易的追踪的工具）就找到了杀手 Dread Pirate Roberts 的一笔交易。

尽量不使用 Crypto Mixers 和 Tumblers 之类的服务。它们不仅对 BTC/ETH/LTC 等加密货币毫无用处，而且它们也很危险，因为他们可能会在你不知情的情况下将你的货币参与进洗钱等非法活动中。

注意：有风险的私有匿名钱包平台，例如 https://we.incognito.org 等不推荐使用。

门罗币

门罗币是所有加密货币中最重视隐私保护的，但是仅靠门罗币所给予的保护仍然是不够的具体可以去看第二部分的安全问题。
另外需要注意的是从非 KYC / AML 交易所获得门罗币并非也都是同样隐私的，让我们先搞明白，我们常说的 KYC / AML 是什么，该缩写代表了解客户信息 KYC 和反洗钱 AML 法律，它们规定交易所和银行收集有关其客户的个人信息。兑换的金额越大，需要的信息就越多。可以肯定的是，实名认证的钱，买门罗币要比买比特币或任何其他透明币之类的东西更好更难追踪，但是仍然需要考虑其它的信息会不会破坏隐私和安全。具体来说，当你从银行提取大笔现金，而银行知道你的详细信息，包括你的家庭住址，电话，出纳员可以查看你的银行帐户中有多少钱，并且可能根据流水跟其它用户行为习惯进行比较. 他们就有可能针对你进行税务调查，冻结账户，如果泄露信息给坏人甚至可能图财害命. 由于钱是在银行里而不是在你的房子里，因此在这种情况下他们可以轻而易举的渗透和窥探。 对于门罗币而言,如同把现金放在家里，并非由第三方担保. 但成为自己的银行并不是看起来那么简单。比特币相当于上面故事里的银行，无论从 BTC 如何转移到 XMR,也就是说无论实名交易所，非实名交易所， DEX 还是原子互换，都会在比特币区块链上留下痕迹. 尽管这确实比 BTC 与 BTC 之间的转账损害要小，因为毕竟门罗币的强制性隐私十分强大，但我们必须考虑比特币透明的那部分留下记录的含义. 如果交易过程中的任何地方涉及 KYC，则这些记录会产生更大的影响。请想象一个应用场景，当你出售商品或服务，收入了一些黑钱的比特币，你不知道这些比特币是犯罪活动获得的，因为你没有时间和大数据去甄别，也没有钱给一家分析公司来为你检查这些币是不是被盗的或者制裁名单上的，但作为一个聪明的用户，

为了安全起见，你决定兑换为门罗币。当你计划将比特币存入交易所，然后将其换成门罗币，然后提现本地钱包. 首先第一步可能就要出问题，因为交易所可能会标记你的比特币并锁定你的帐户，比如币安曾被盗了 7000 个比特币，如果你收到了其中一部分，并且充值回币安，那么肯定会被冻结账户。为了探究其它问题，这里我们假定第一步没有问题，充值成功，交易所没有冻结。但由于比特币交易记录永久保留在区块链上，任何时候政府跟踪罪犯的比特币钱包，他们都可以看到有笔交易到了交易所，通过关联 KYC 信息，看到它们已被兑换成门罗币了，然后警察就会登门拜访你了。这并不是说你应该避免将比特币兑换成门罗币，以免看起来可疑. 造成这个问题的根源是，你接受了肮脏的比特币，如果不进行交换，它们仍然会使用区块链分析，并且还会警察上门。 这个例子是想说比特币这类完全透明币的巨大风险，并且哪怕用门罗币这样的完全匿名的币去兑换仍旧不能消除透明区块链中留下的足迹。对于隐私保护敏感个人，应尽量减少使用透明区块链，从根本上解决麻烦.并且应尽可能避免使用实名交易所，因为此元数据可用于关联你的根本信息，并产生问题，而由于不称职的交易所中泄漏数据的例子，屡见不鲜。即使你只购买了门罗币并将其从交易所提走，这些泄露的信息仍会显示你曾经拥有多少门罗币以及你当时所在的位置我们都知道枪打出头鸟，财不外露，没有人会希望暴露信息，即使是在网络空间中。总而言之，尽管默认情况下使用门罗币确实可以抵消许多攻击，并最大程度地减少元数据泄漏但用户自己在门罗以外的地方犯的错，最终也会破坏自己的隐私。 很多人意识不到的问题之一是使用透明链作为购买门罗币的途径，另一些人低估了使用 KYC 的危害，更不用说有的人同时使用两者了。再次重申本文的目的不是要引起恐惧，而是要鼓励用户批判性地考虑自己的行为，并提醒在某些情况下，即使是最强的隐私也可能是脆弱的。用户必须保持警惕，通过明智地方法购买，隐藏实际的地理位置对于保护隐私也是十分必要的。

如何选择交易所

非 KYC 的交易所:
这是非 KYC 加密交换服务的一小部分列表，请记住它们并非都是自由平台且都需要支付使用费:
https://sideshift.ai
https://bisq.network/（只能用数字货币购买 XMR）
http://mlyusr6htlxsyc7t2f4z53wdxh3win7q3qpxcrbam6jf3dmua7tnzuyd.onion/
coinswap（Tor 网站）

推荐查看 https://kycnot.me/， 这是一个列出非 KYC 交换/交换服务的自由项目（位于 https://codeberg.org/pluja/kycnot.me 的存储库）。

如何将门罗币转化为比特币

不要使用任何交换服务，使用他们的原子交换功能。 这将防止在使用商业交换服务时产生不必要的费用和中间商。该网站一目了然，包含所有操作系统的详细说明。、将您的 Zcash 从一个 VM Zcash 钱包转移到另一个您控制的 VM Zcash 钱包，同时确保您使用的是屏蔽地址（一些交易所直接允许这样做）。
另外请确保两个虚拟机钱包不同并在打开收件人钱包之前更改您的 Tor 身份。再次使用兑换服务将您的 Zcash 兑换成 Monero/BTC/other。