

TorProject.org

## Tor 使命

作为一家非盈利机构，Tor Project 开发了一系列的自由软件和服务。利用这些工具，任何人，包括记者、人权活动家、外交官以及商务人士，都能够在使用互联网的时候，不再担心政府与企业的监控。

同时，Tor Project 也是一所全球性的机构，致力于言论自由、在线隐私和反抗审查并提供相应的技术、研究、教育以及宣传推广。Tor Project 为成为一个有领导力的 501(c)(3) 非营利组织而自豪。

更多信息，请访问

<https://www.torproject.org/>



## 欢迎加入

言论自由、在线隐私与反抗审查是一项全球性的持续工作，我们需要你的支持和帮助。你可以赞助 Tor Project，或者参与志愿项目，也可以参加 Tor 团队举办的各项活动。

## Tor 优势

- 保护在线隐私
- 反抗审查
- 保护记者
- 保护人权捍卫者
- 保护家庭暴力受害者
- 让每个人都可以访问世界各地的在线信息
- 帮助制订政策
- 帮助学术机构进行研究



# 执法机构与 Tor Project

## Tor 工作原理

### 谁在使用 Tor?

绝大部分 Tor 用户是想要保护自身在线隐私的普通公民，还有一部分是需要突破网络审查的用户。至于那些敢于违法的罪犯，他们已经能够使用比 Tor 更为有效的工具了。

### 不记录，无后门

用户可以依赖 Tor 提供的隐私保护。根据设计意图，Tor 中继搭建者，以及能够实际接触这些节点的人，也无法获取 Tor 用户的真实 IP 地址。学术界和开源社区一直在对 Tor 源码进行审核，确保 Tor 不存在后门。

### 匿名密报

对于证人与消息提供者，确保在线通信渠道安全至关重要，而 Tor 能够为需要完全匿名的在线密报提供最为可靠的基础架构。

### 秘密侦察

执法机构和调查人员用 Tor 匿名监视可疑网页和网络服务。Tor 可以用户的身份和位置，有助于调查人员成功进行在线侦察。



韩梅梅首先将发往李雷的网页请求进行三次加密，然后将其发送到中继节点 1。



中继节点 1 解除第一层加密，但无法获悉网页请求指向李雷。



中继节点 2 解除第二层加密，然后将网页请求转发至下一节点 3。



中继节点 3 解除最后一层加密，然后将网页请求转发给李雷，但无法获悉该请求来自韩梅梅。



如果她不说，李雷也无法知道该请求来自韩梅梅。

### 更多信息

- Tor 一直进行有关 Tor 的培训，对象包括执法机构和决策人士。
- 人人都可以访问 Tor 文档。同时，我们面向所有人提供相关技术支持。
- 可以通过 ExoneraTor 服务判断某个 IP 是否为 Tor 中继。
- 如需了解更多信息，可与我们的专业团队联系。



## 在线匿名益处

### 现实

通信服务商（比如电信和联通）、网站（比如百度和微博）以及政府，可通过 IP 地址跟踪这一常见互联网监控方式，对公共网络通信进行监视。

- 新闻网站可根据你所在地理位置推广相应的内容。
- 购物网站可能根据你所在的国家或来源机构进行价格区分。
- 一般网络用户会受到上百家公司的跟踪。这些公司将获取的用户信息卖给广告客户。
- 坏人也可以利用社交网络获取你的个人信息并对你造成伤害。

### 自由

网络版图一直在变化，来自法律、政策和科技领域的最新趋势将对隐私带来前所未有的威胁：侵害我们的在线言论自由以及获取在线信息的权利。除了监控国内的公民，国家之间也在互相监视：封锁网站，显示网络通信内容，限制重大世界信息。

## Tor 工作原理



韩梅梅首先将发往李雷的网页请求进行三次加密，然后将其发送到中继节点 1。



中继节点 1 解除第一层加密，但无法获悉网页请求指向李雷。



中继节点 2 解除第二层加密，然后将网页请求转发至下一节点 3。



中继节点 3 解除最后一层加密，然后将网页请求转发给李雷，但无法获悉该请求来自韩梅梅。



如果她不说，李雷也无法知道该请求来自韩梅梅。

## 在线隐私的首选工具

- 在过去 10 多年里，Tor 机构下的安全研究人员与软件开发人员，一直在对作为自由开源科技的 Tor 工具进行研究和改善。
- 作为一款最有效的隐私保护工具，Tor 可以确保个人对自身在线安全的控制。



# 自由与在线隐私

## Tor 工作原理

### 审查：

(韦氏字典, 2012年)

以违反公共利益为由修改或压制言论和写作的行为。

### 在线审查

站在互联网这一全球性的平台上来看，审查具有全新的涵义。大多数人并未意识到，信息审查和内容发布监控远比想象的要司空见惯。Tor Project 的研究人员致力于开发对抗审查的工具并能够领先于审查技术与策略，从而为每个人提供开放的在线通信渠道。Tor 团队与一些机构合作，增强用户对于在线隐私的意识，改善大家对于在线安全重要性的认知。



韩梅梅首先将发往李雷的网页请求进行三次加密，然后将其发送到中继节点 1。



中继节点 1 解除第一层加密，但无法获悉网页请求指向李雷。



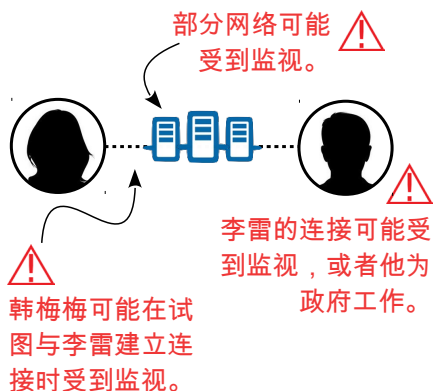
中继节点 2 解除第二层加密，然后将网页请求转发至下一节点 3。



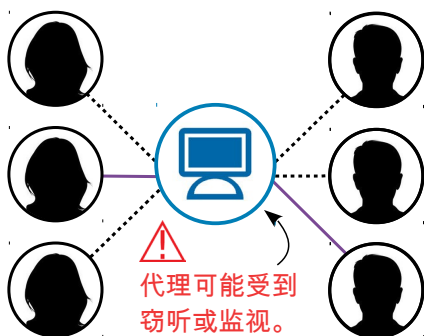
中继节点 3 解除最后一层加密，然后将网页请求转发给李雷，但无法获悉该请求来自韩梅梅。

如果她不说，李雷也无法知道该请求来自韩梅梅。

网络监控易于部署且无处不在。



一些对抗审查的工具，其设计仅利用一层规避方式来隐藏连接。



遗憾的是，一层规避设计（例如代理）很容易失效。