# 网站/服务器取证实践与挑战

陆道宏

上海弘连网络科技有限公司

2016年7月14日

# 自我介绍



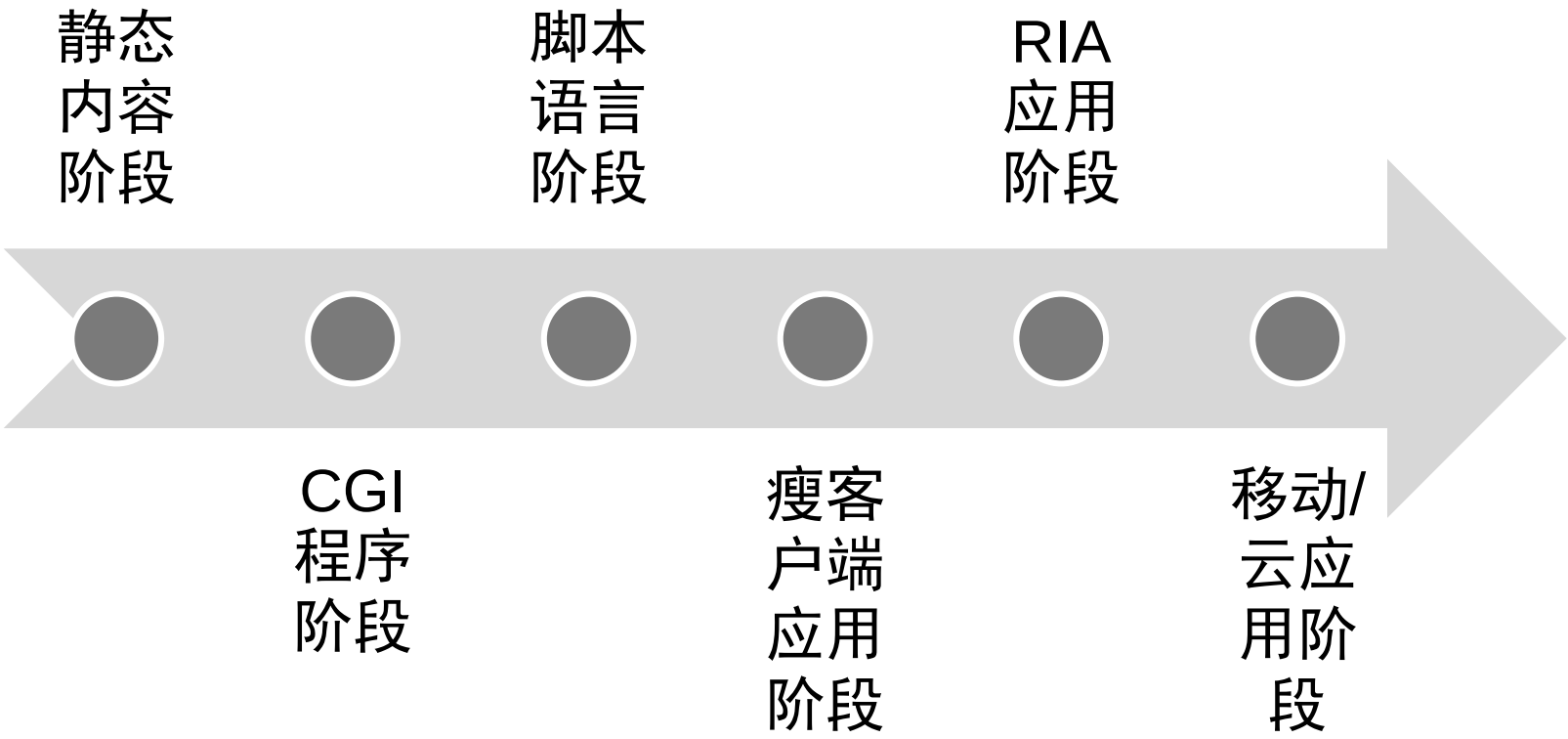


- **电子数据取证领域 15 年工作经验**
- **参与设计/开发过一系列的工具产品**
- **ldh@forensix.cn**


应用/网页取证

数据/主机取证

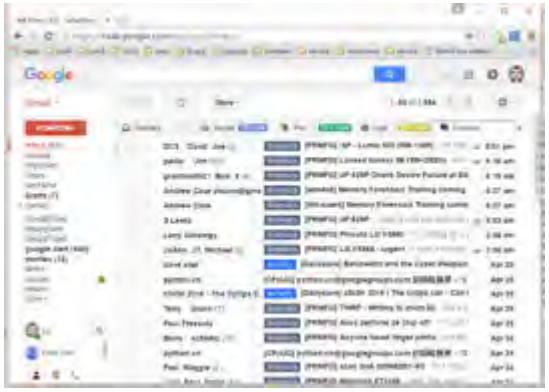
# WEB 应用/网站的发展



前端渲染网站

后端渲染网站

静态网站



# 网页取证相关技术

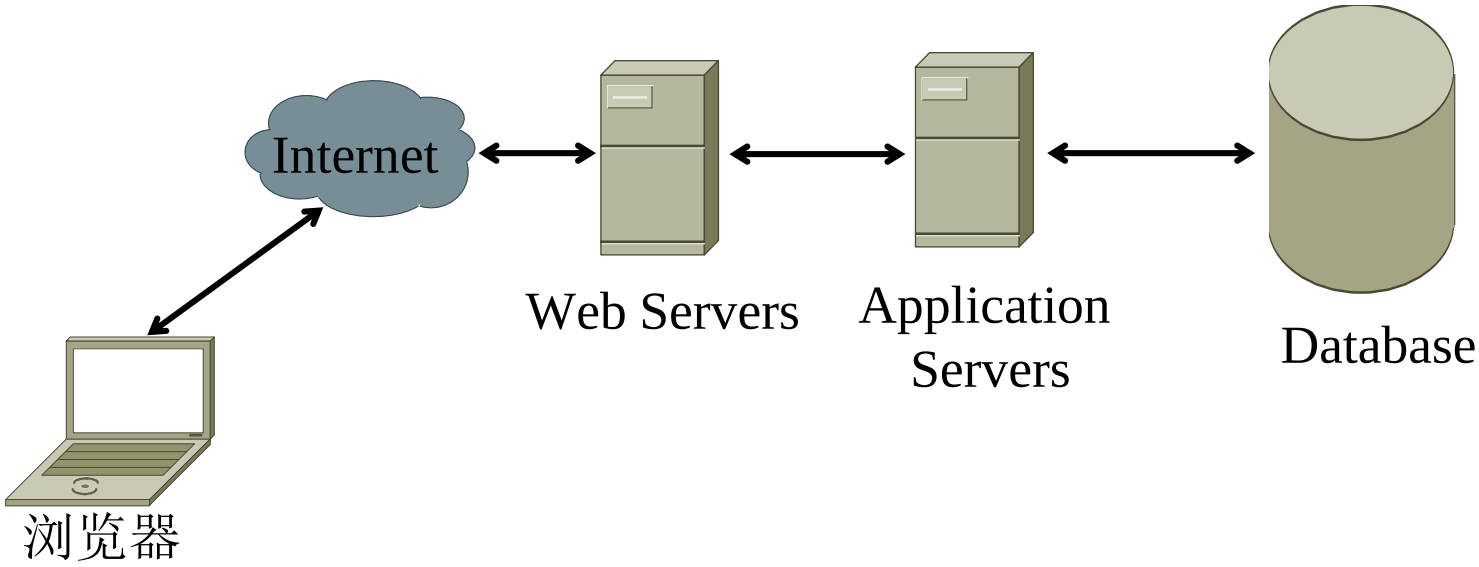
| | | |
|---|---|---|
| URI | HTTP | HTML |
| MIME | Chrome / JavaScript | Fiddler / Charles |
| IP/DNS | Python / Node | … |

# 色情网站视频固定案例

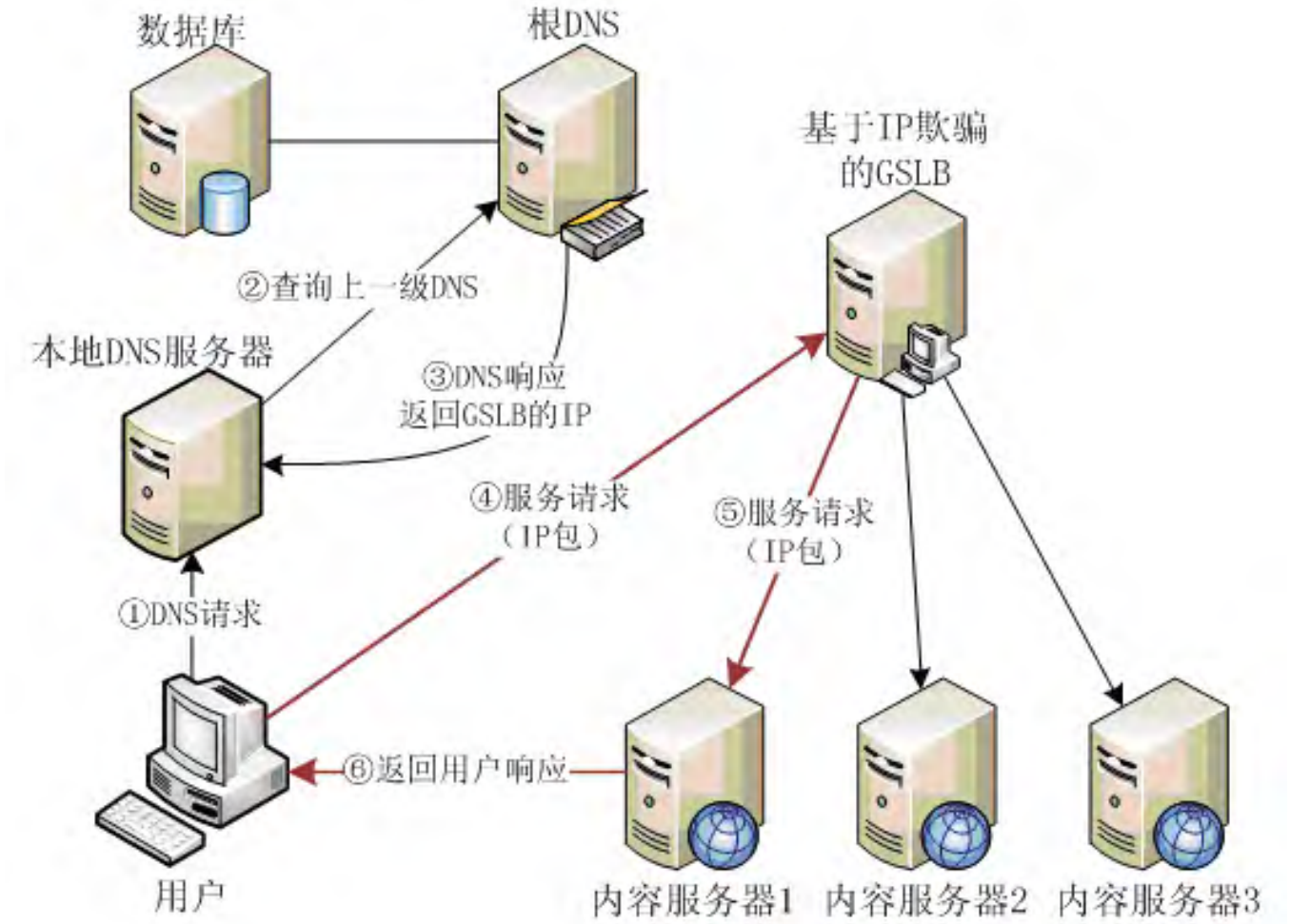
```
for hashstr in furls.readlines():
    try:
        outUrl = str(i)

        uri = 'http://www.demo-site.tv/api.php#!u=' + hashstr
        outUrl = outUrl + ',' + uri
        req = urllib2.Request(uri)
        req.add_header('User-Agent', 'Mozilla/5.0 (Macintosh; Intel Mac OS X 1
        req.add_header('Referer', 'http://www.demo-site.tv/api.php')
        response = urllib2.urlopen(req, timeout=3)

        uri = 'http://www.demo-site.tv/play.php?class=api&key=' + hashstr
        outUrl = outUrl + ',' + uri
        req = urllib2.Request(uri)
        req.add_header('User-Agent', 'Mozilla/5.0 (Macintosh; Intel Mac OS X 1
        req.add_header('Referer', 'http://www.demo-site.tv/api.php')
        response = urllib2.urlopen(req, timeout=3)
        decryptUrl = ''
        html = response.read()
        decryptUrl = re.search("decrypt.php\?key=[^'.]*", html).group()
        title = ''
```

# 网站 / 数据库 / 日志 / 关联 / ...

配置 | 网站文件 | 日志 | 数据库



# 网站架构的复杂性


数据库
根DNS
基于IP欺骗
的GSLB
②查询上一级DNS
本地DNS服务器
③DNS响应
返回GSLB的IP
④服务请求
（IP包）
⑤服务请求
（IP包）
①DNS请求
⑥返回用户响应
用户
内容服务器1
内容服务器2
内容服务器3

# 云服务模式和挑战


https://www.aliyun.com
欢迎上云，请登录 注册
管理控制台 帮助与文档 备案 论坛 万网 手机APP 阿里邮箱
阿里云 aliyun.com
最新活动 产品 解决方案 云市场 开发者社区 服务与培训 合作与生态 大数据
免费注册
注册享新手礼包
全球规
阿里金融云邀你一
7月17日-18日
查看详情
弹性计算
数据库
存储与 CDN
网络
大规模计算
云盾
管理与监控
应用服务
互联网中间件
移动服务
视频服务
域名与网站(万网)
云服务器 ECS
可弹性扩展、安全稳定、简单易用的计算服务
块存储
可弹性扩展、高性能、高可靠的块级随机存储
专有网络 VPC
帮您轻松构建逻辑隔离的专有网络
负载均衡
对多台云服务器进行流量分发的负载均衡服务
弹性伸缩
自动调整弹性计算资源的管理服务
E-MapReduce
基于 Hadoop/Spark 的大数据处理分析服务
资源编排
批量创建、管理、配置云计算资源
容器服务
应用全生命周期管理的 Docker 服务
高性能计算 HPC
加速深度学习、渲染和科学计算的 GPU 物理机
云市场相关产品
免费预装PHP环境服务器
免费预装JAVA环境服务器
免费预装建站系统服务器
免费预装数据库服务器
免费预装全能环境服务器
最新特性
ECS 高效云盘上线
ECS 美国硅谷第二可用区开放
ECS 等10余款产品开放新加坡地域
ECS 镜像共享功能上线
SSD 云盘和IO优化型实例免费公测
新手学堂
轻松玩转阿里云
新产品发布
不断满足您的需求
阿里云定价
全面了解价格信息
迅速上手OSS
OSS新手学堂全新开启
架构师在线直播
解读电商客户上云架构
安全、稳定的云计算基础服务
数据库
存储与CDN
云盾（安全）

# 网站/服务器取证技术

| | | |
|---|---|---|
| HTTP / HTML/MIME | JavaScript / AJAX | PHP/ASP/… |
| APACHE / IIS | MSSQL / MySQL | 日志分析 |
| Web 安全 | CDN / Cloud | … |

# 最近案例


云数据库 Memcache
云数据库 RDS
微信 · 公众平台
再小的个体，也有自己的品牌
七牛 · 直播云
魅族、龙珠、熊猫 TV、美拍等
千家直播平台的选择。

陆道宏

ldh@forensix.cn