



安焦峰会讲稿

傅念东



“中华人民共和国公安系统未来必备的强大网络电子组合式武器库”

基于FIPA(The Foundation for Intelligent Physical Agents)引擎的**取证流程智能决策系统**



- 调查取证简介
- 证据保存与分析
- 取证工具介绍
- 详细证据



计算机调查取证的定义

计算机调查取证可以简单说是一门有关计算机操作系统和文件结构的应用科学和分析技术，用来寻找潜在法庭证据的过程。



为什么证据很重要？

- 在互联网世界，证据是一切。
- 证据可以推断事实。
- 法庭调查是基于证据的。



谁需要计算机调查取证？

- 受害者！
- 法律执行者
- 保险公司
- 最终法律系统



谁可能是受害者？

- 私有公司
- 政府
- 个人
- 其它



法庭调查取证分析的目的

- 确定肇事者的身份
- 识别肇事者犯罪轨迹
- 引导受害者实现损失评估
- 保护证据以便法庭上使用



计算机调查取证的类型

- 磁盘调查取证
- 网络调查取证
- 电子邮件调查取证
- 互联网调查取证
- 源代码调查取证



磁盘调查取证

- 磁盘调查取证是指获得和分析储存在物理介质上数据的过程。
- 包括对隐藏和已删除数据的恢复
- 包括识别谁是文件和消息的创建者
 - *梅利莎病毒*: 该病毒首先感染通用模板: Normal.DOT文件, 并修改Windows注册表项:
HKEY_CURRENTUSER\Software\Microsoft\Office,
将其增加表项: Melis_sa?, 并给其赋值为: ...by
Kwyjibo



网络调查取证

- 网络调查取证是检查网络通讯的过程。它包括：
- 案发相关的通讯记录分析
- 网络监控的实时分析
 - SNIFFER
 - 实时跟踪



电子邮件调查取证

- 电子邮件调查取证是通过研究电子邮件来源及其内容，查找证据的过程。
 - 它包括识别实际邮件、消息的实际发送者和接收者，及其内容、时间和地点。有时，有关性别歧视、种族和宗教偏见内容及其它非法活动常常和电子邮件捆绑在一起。



互联网调查取证

- 互联网调查取证是查明特定用户使用因特网资源的地点和时间的过程。



源代码调查取证

- 源代码调查取证可以用来判断软件所有者和软件责任人。
 - 它不是仅仅检查实际的源代码。
 - 它检查软件完整的开发过程，包括开发程序，检查开发时间表，文档检查，和源代码修改。



技术进展

- 计算机专业人员倍增
- 世界网络化程度已经大大加强了，虽然绝大多数的用户仍然是匿名的
- 使用加密手段的现象已经很普遍
- 网络带宽已经加大，而成本正逐渐下降
- 磁盘价格正下降，而容量却越来越大
 - 网络上的数据越来越多



技术进展

爱因斯坦曾经说过：

“技术进展就像是病态犯罪者手中的一把斧头。”



技术进展

- 计算机既是工具也是目标
 - 手段
 - 数据仓库
 - 一些计算机罪犯使用计算机时和通常情况下使用方法是一样的。
- 今日计算机犯罪特点
 - 可以逃避惩罚
 - 追求轰动效果
 - 公众态度冷漠
 - 犯罪很容易



什么是计算机犯罪？

- 计算机犯罪中技术扮演着重要的、通常是必须的角色。
 - 计算机是：
 - 攻击的目标
 - 攻击中使用的工具
 - 用来储存犯罪活动相关的数据



计算机犯罪类型

- 未授权访问
- 拒绝服务
- 勒索
- 偷窃
- 破坏
- 侦察
- 计算机骗子
- 盗用
- 侵犯版权
- 伪造
- 网络骗子—“欺骗性的站点”
- SEC骗子和STOCK操控
- 儿童色情文学
- 围捕和折磨
- 信用卡骗子和盗用者



当前计算机调查取证的议题

- 国内司法鉴定系统还没有做好处理高技术犯罪的准备
 - 缺乏训练有素的调查人员和分析人员
 - 缺乏调查取证标准
- 太多的数据！
 - 大磁盘和磁盘队列
 - 高速网络连接
- 高时间相关性



当前计算机调查取证的议题

- 证据收集和检查不能和下列政策法规相冲突：：
 - 宪法
 - 国家安全法
 - 行政诉讼法



调查取证过程

- 准备
- 保护
- 映像
- 检查
- 文档化



准备

- 对介质分析/检查的授权进行确认。
- 确认分析的目的并且清楚的定义所期望的结果
- 保证有足够的干净介质用来镜像（比如，在使用前确定没有病毒，没有重要的文件等。）
- 保证用来分析的所有软件工具都已经过检验，并且被广泛用来实施调查取证工作。



法律综述



保护

- 保护证据的完整性。
- 要保密到最后一刻。
- HASH保护
- 多人证明



映像

- 使用磁盘镜像软件来镜像目标介质，并确认它。
- 当对目标介质进行分析时，务必使用已制作的介质镜像；决不可以用实际的目标介质。



检查

- 操作系统
- 服务
- 应用程序/处理过程
- 硬件
- 记录文件/日志文件
- 文件系统



检查 (续)

- 已删除的文件/隐藏文件/NTFS流
- 软件
- 加密软件
- 共享/许可
- 密码文件
- SIDS
- 网络结构体系/信任关系



文档

- 文档是一切
- 证据标签
- 保管链
- 证据管理



证据

REALSOI



四个步骤,

- 记住这四个步骤：识别，保护，分析和提交。
 - 我们目的是在于提交证据
 - 分析是个很大的主题,不能全部把它包括进来
 - （司法鉴定实验室还有很多工作）
 - 我们集中于识别和保护
- 一切从保护开始...



证据保护

- 记住我们的“最优证据”和“保管链”原则
- 这里描述的程序和步骤是用来遵循这些原则和对证据提供保护
- 不要完全照搬这些原则
- 除非你确定你具备不需要的理由，否则你都应该遵循这些原则



程序1

- 现场记录
 - 什么样的计算机，在什么地方
 - 给计算机，磁盘，和软盘贴上标签
 - 通常这些工作都要由同一个人完成，所有的记录都要记在同一地方
 - 简要的原则
- 对每一计算机
 - 拆开它 (已取得内部部件)
 - 记录对内部部件, 并贴上标签



程序2

- 对每一磁盘，软盘，CD...
 - 制作md5 hash, 并记录下来
 - 制作司法鉴定映像（如使用/safeback/dd命令 /Encase）到磁带，或到专用文件系统等。
 - `dd if=/dev/had of=/dev/rst0`
 - `dd if=/dev/had | nc 192.168.5.11 7000`
 - `netcat -L -p 7000 >/mnt/evidence/fund.dd`
 - 制作上述映像的 md5 hash, 并记录下来
 - 比较 hashes



程序3

- 回到实验室
 - 把原件/映像放在安全的地方
 - 使用如Encase创建证据文件，利用该工具创建证据介质上数据的准确描述
 - 证据管理人要控制对证据的接触，并把一切文档化
 - 谁提取了证据，原因，日期
 - 谁拷贝了证据，原因，日期
 - 越少的管理者越好 – 可以减少证明



文档

- 文档化必须了解：
 - 是谁，在什么地方，什么地点，如何，基于什么理由和规则（如搜查令）收集证据的
 - 原件和拷贝的Hashes
 - 实时和计算机时间的时钟偏移量 (使用精确的参考时钟!)
- 多人证明



程序

- 建议：
 - 在包中放置一个拷贝 (比如拷贝到磁盘，把原件打包，拷贝到磁带机)
 - 在包上贴上封条，并在上面说明未经许可不能打开
 - 在封条上签名并且签署日期
 - 锁起来
- 直到我们展开调查，我们都不能遗失它们



Checksums and Hashes

- Checksum: 目的是用来错误探测。
 - CRC 16, 32
 - 很容易改变保存的checksum;
- Hash: 目的是用来抵抗恶意的破坏
 - MD5, SHA
 - 很“难”造成hash冲突
 - 很“少”可以发现两份具有同样hash的文本文件



数字时间戳

- 基本思想: 创建hash并公开它
- 显示数据和签署日期hash匹配商业免费服务
 - <http://www.itconsult.co.uk/stamper.htm> - 免费服务
 - <http://www.surety.com> - 商业服务
 - Hashkeeper服务



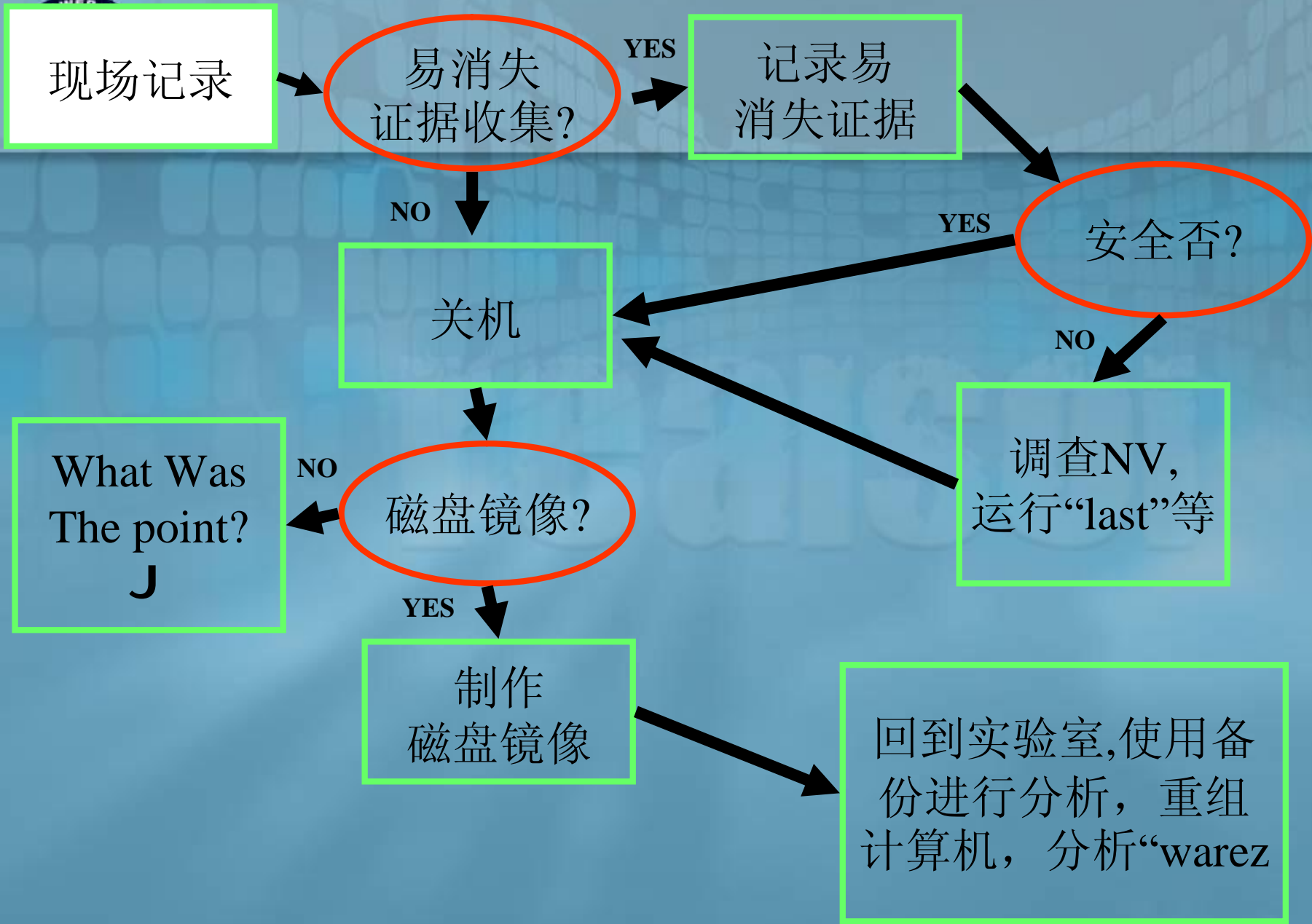
优先响应事务

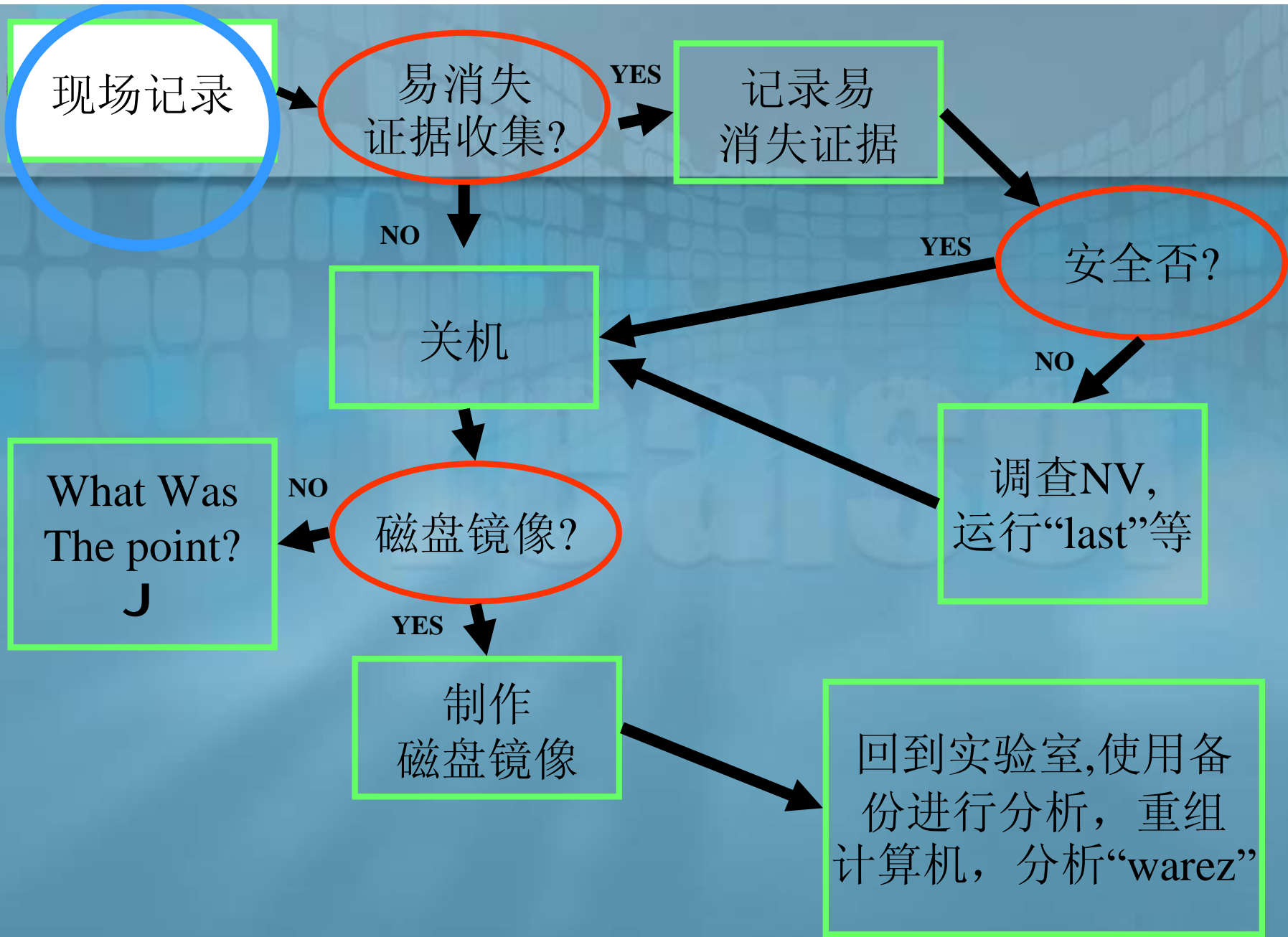
- 保存系统上易消失的证据
- 继续在系统上保留入侵者?
- 系统持续运作可能产生的影响（正面的和负面的）
- 司法的介入以扩大力度，这一步通常都具备



优先响应事务

- 保护
 - 目标系统和资源
 - 牵制入侵
- 保护
 - 证据 (记录, 文件系统, 遗迹文件)
 - 用一种法律接受的方式
- 通报
 - IRT, LE, 管理员, 其它站点...

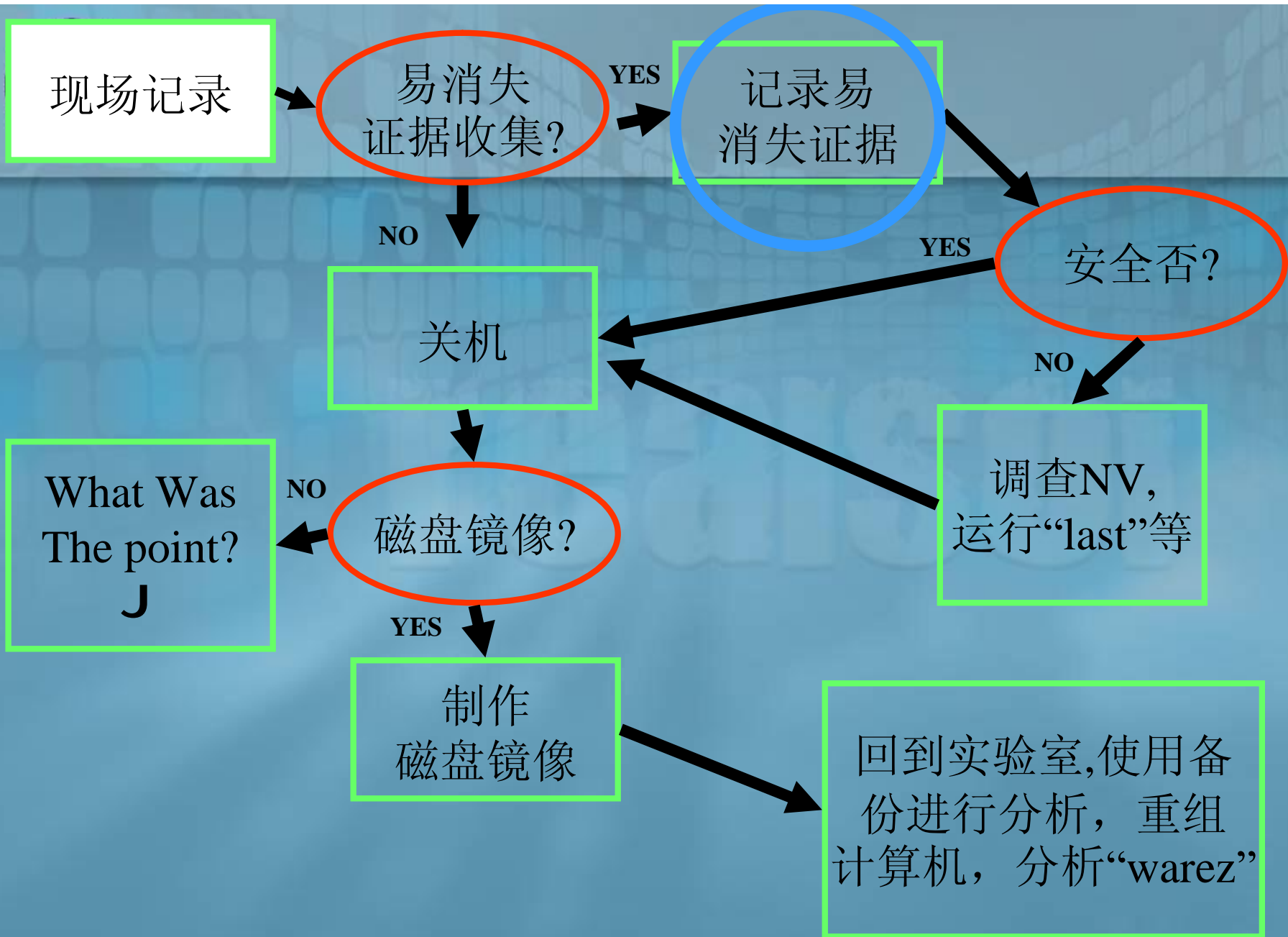






现场记录

- 环境地图
- 拍照
- 对所有物品贴上标签
 - 永久的, 或者可移除的粘性标签 (别粘贴反了)
 - 它们会掉的)
 - 统一“标签” 如– 315-1-2 (room 315, computer 1, disk 2)
- 分类





收集易消失的证据

- “易消失的证据”是那些很快就会消失的证据,比如网络连接信息, 或者当前内存的信息
- 把这些信息和磁盘或者磁带上的信息相比较



收集易消失的证据

- 从 Farmer & Venema –
<http://www.porcupine.org>
 - 注册, 外围存储设备, 高速存储器...
 - 内存 (虚拟的, 物理的)
 - 网络状态
 - 运行过程
 - 磁盘, 软盘, 磁带
 - CD-ROM, 打印输出



收集易消失的证据

- 你在系统上的所作所为对遗留证据的影响
 - 运行 'ps' 将会覆盖部分的内存
 - 你的shell或许会覆盖历史文件
 - 你可能影响文件的访问时间
 - 总是要冒产生木马的风险! (例如 gcore)



收集易消失的证据

- 超级用户工具
 - 守旧派: 用带有木马的程序代替系统程序 (ls, find, login, netstat, ps...)
 - 替换动态库
 - 新潮派: 可承载的内核模块, 造成内核对某些事件不进行报告
 - 其它



收集易消失的证据

- 你需要是已知的，安全的工具来检查磁头
 - 静态链接
 - 或者包括进来你自己的库
 - 从软盘或者CD上，或者通过网络，或者从网络下载来安装
- 这部分不会对内核超级用户工具有帮助



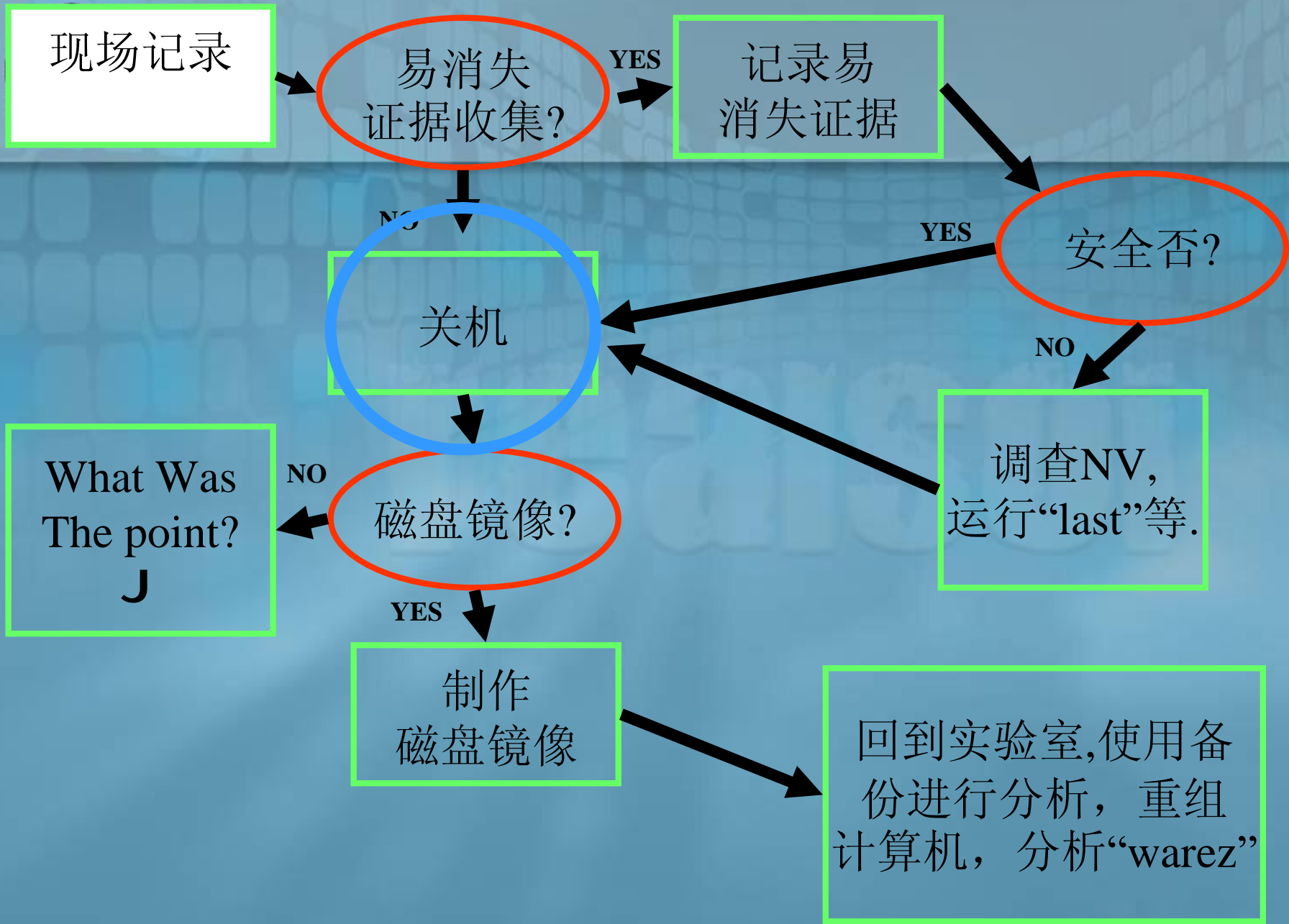
收集易消失的证据

- 工具箱可能包括:
 - UNIX: sh, ls, find, tar/cpio, ps, netstat, ifconfig, cat, less/more, grep, lsmod, The Coroner's Toolkit (grave-robber), emt, lsof, script
 - NT: GNU file utils, handleex, filemon, netmon, dumpevt, dumpreg, dumpacl
 - 站点: foundstone / sysinternals / nti等



收集易消失的证据

- 如果你正在收集易消失的证据：
 - 登录方式 console?
 - 下载安全工具 (通过网络, 软盘, 或者CD)
 - 内存, 交换分区, /tmp, /proc 目录
 - 全部拷贝, 或者运行strings?
 - 网络状态
 - 连接, 混杂接口
 - 进程





你还应该...

- 当你检查计算机的时候，你还应该：
 - 关机？
 - CTRL-ALT-DELETE, L1-A？
 - Reboot？
 - 要不要和网络断开？
 - 要不要在路由器上过滤？
 - 要让它继续运行还是快速进行检查？



关机

- 关机/中止/sync 可以让文件系统变得干净
 - 但是这些程序可能被非法破坏，导致文件破坏
- 不要重启！
 - 这会比关机带来更多的破坏！
 - 重启时删除/tmp目录 (如果它不是动态存储器)
 - 它是否非法重启，带有“bad stuff” (后门, 破坏性的东西)? 或者通过cron重启?



和网络连接断开

- 如果你从网络连接断开并过滤掉它...
 - 有什么样的“dead man switches”记录，它说明它断开的时间和擦除了什么证据？
 - Marcus Ranum wrote about this in the CSI Alert, September 1999, #198



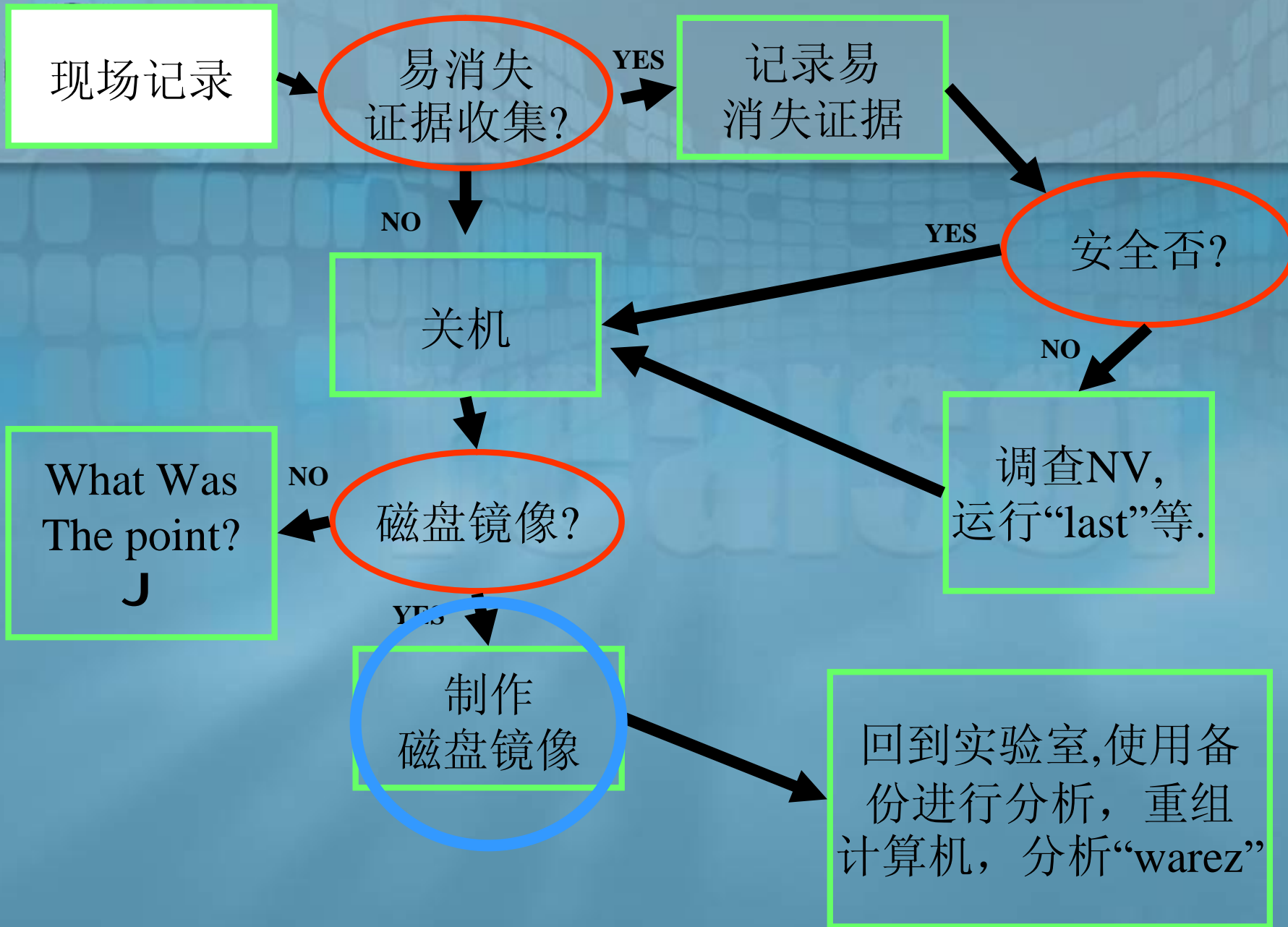
让它继续运行

- 不把它和网络断开
 - 直到你断电关机
- 在短期内它可能是安全的
 - 然而，随着时间的推移，风险是逐步增加的
 - 它们可能被用来做非法的事情 – 责任问题？
 - 它们也可能擦除证据，特别是在它们发现你在探测的时候(聪明的木马)



关机

- 在你关机的時候...
 - 你丢失了易消失的证据: 进程, 网络连接, 网络文件连接, 内存内容...
 - 在很多时候下面的内容是很重要的证据: 黑客增加存储工具, 在远程文件系统上的记录
 - 另一方面, 如果你在一运行的系统上调查, 你就有可能改变了文件系统(特别是对磁盘)





磁盘镜像

- 分区特点
- 整盘镜像最保险
 - `dd if=/dev/wd0s2a of=/incident/1999-10-11-001/hosta/wd0s2a.dd`
- 镜像部分分区有时是很便利的
 - 很容易通过loopback安装
 - 小心：分区可能不能包括整个磁盘



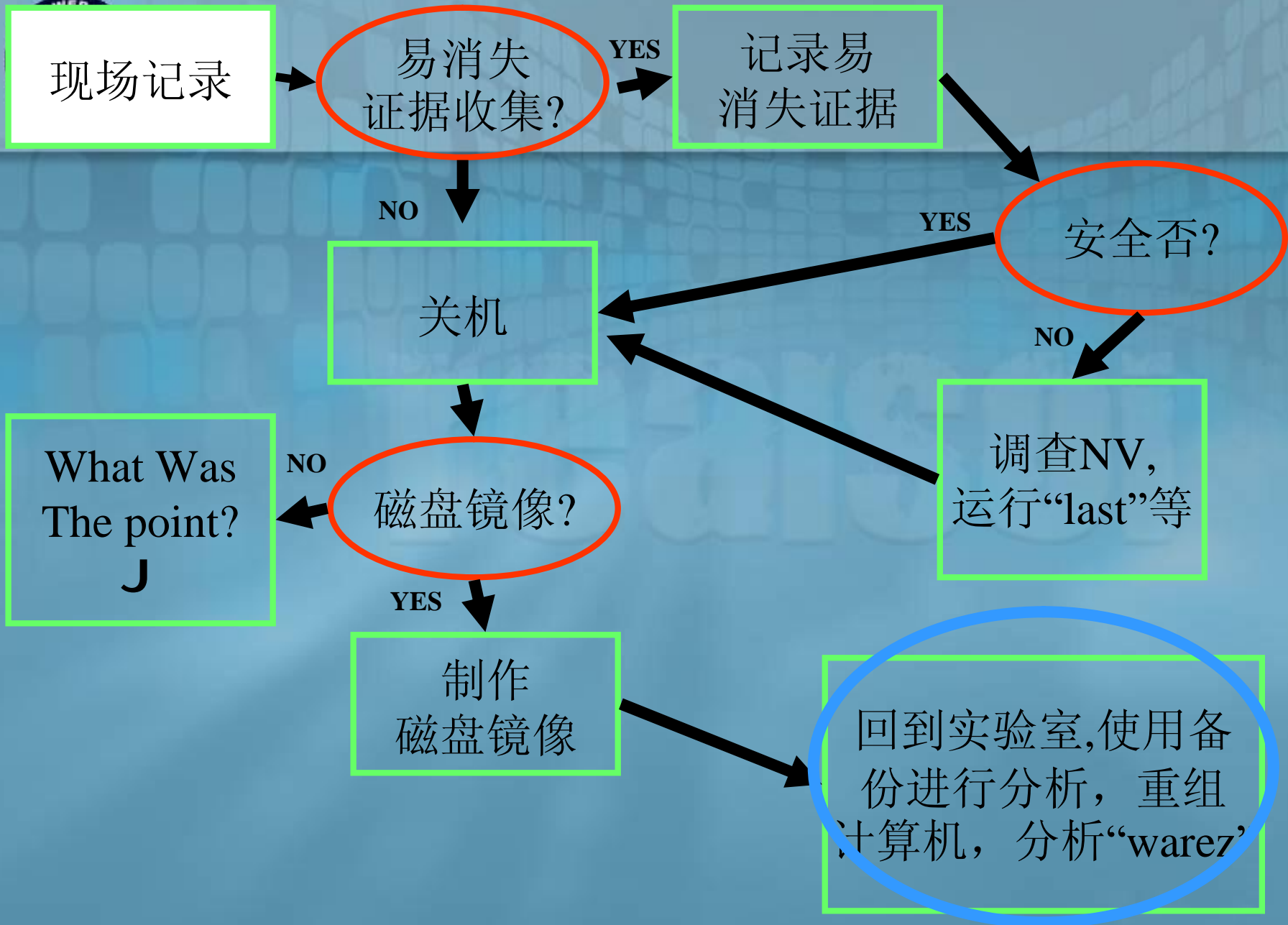
磁盘镜像

- 存储分区信息，特别是当你没有作整盘镜像的时候
 - `fdisk -l /dev/wd0 > /incidents/1999-10-11-001/hosta/wd0.fdisk`



利用镜像的磁盘工作

- 可以在实验室使用镜像来恢复
- UNIX 文件系统使用UNIX 工具
 - The Coroner's Toolkit, Farmer & Venema
 - Tctutils and Autopsy, Brian Carrier
- DOS, Windows 工具
 - NTI tools: getslack, getfree, filter-i, textsearch plus
 - Sydex: safeback to image drive
- 包装 – Windows 系统使用 Windows工具, UNIX 文件系统使用UNIX工具





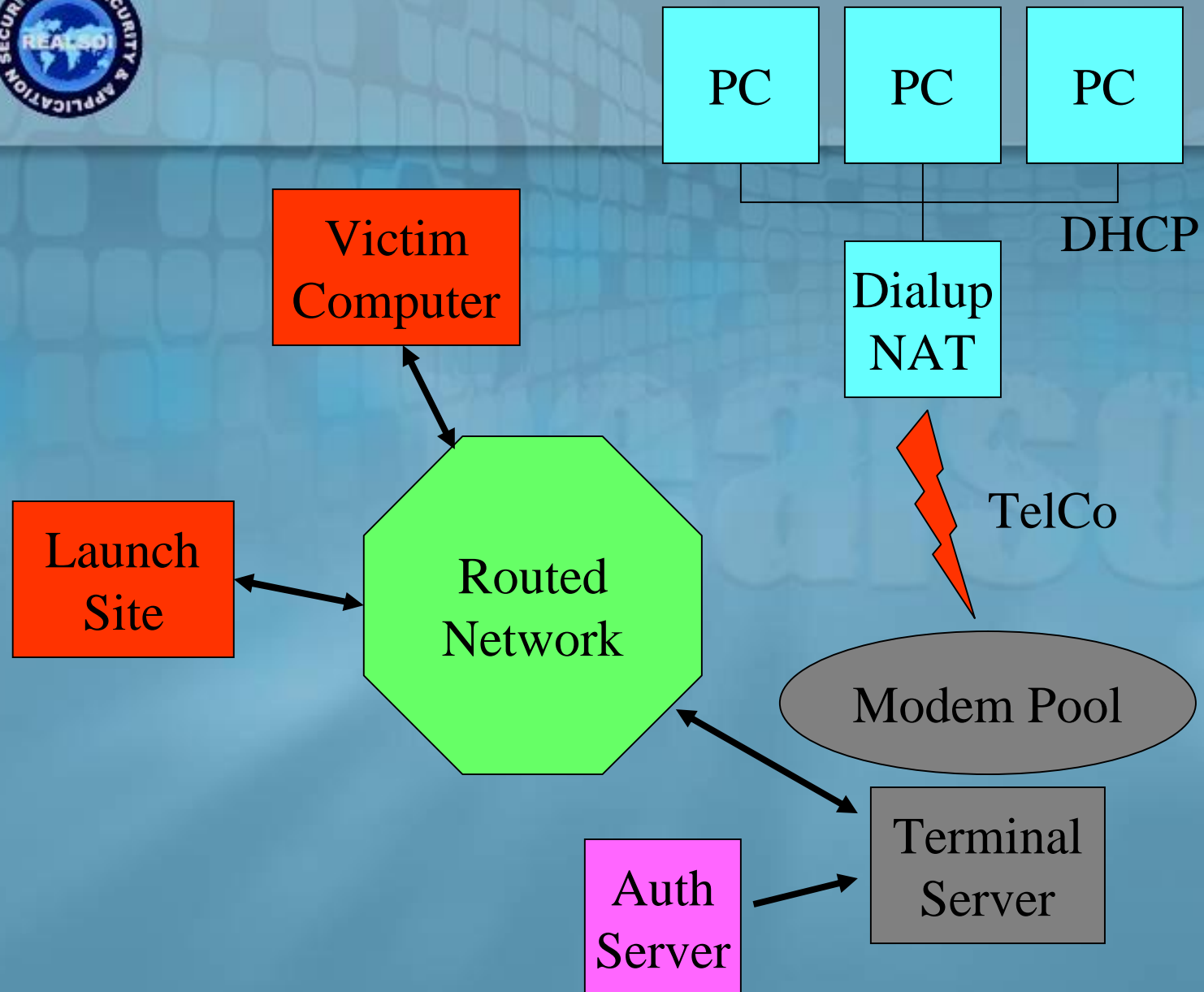
识别和分析证据

REALSOI



我们需要知道:

- 证据在什么地方
- 证据说明了什么
- 怎么把它们整合起来





证据在什么地方

- 家庭系统
- 电话系统
- Modem池
- 网络
- 受害计算机
- 考虑组件
- 提出问题，向专家请教



证据说明了什么

- 需要深层次的理解证据
 - 证据是怎么建立的
 - 它可能在什么地方消失
 - 或者有错误
- 请教专家，提出问题
- 当前不能掩盖证据...



证据说明了什么

- UNIX wtmp文件上的一个romig登录入口指的是...
 - 某人使用romig帐号登录过
 - 或者是攻击者插入的虚假信息?
 - Romig登录不是必须的
- 一条DHCP租借意味着...
 - 有一台计算机是承租方
 - 在租借期间，那台计算机是唯一使用那个IP的计算机



重要知识

- 在什么地方记录可能会发生错误？
 - Syslog, 通过UDP输出的NetFlow (cisco产品)
 - 并行鉴别服务器的鉴别记录
 - 非对称路由和NetFlow记录
 - 欺骗IP地址
 - 可写的记录 (旧UNIX系统上的wtmp, utmp)
 - 被黑客修改的记录



整理记录的相关性

- 如果你可以的得到多重来源的记录，你就可以建造健壮的案例
- 整理接入记录的相关性
 - 通过特定的准确值来匹配记录- 如IP地址
 - 通过时间来匹配接入



时间相关事件

- 我们经常使用时间戳来建立不同系统上的不同记录间的相关连接
- 问题包括:
 - 时间同步
 - 时区
 - 时间记录
 - 时间的历史顺序
 - 事件发展



时间的同步性

- 我们有时可以使用记录的时间戳来推断
 - 计算机A上的Shell的历史记录显示在T1时刻的telnet B纪录
 - 计算机B上的tcp wrapper显示T2时刻
 - 时间偏移量 (可能值 $T2-T1$)
 - 假设是同一时区
- 但是，我们不能永远这么认为
 - 如果我们没有足够的其它信息来做这工作的话
 - 事件记录



时区

- 你不能把苹果和桔子相比较
- 对所有记录发送并请求时区记录
- 我喜欢GMT偏移量
- 大量的这种处理是非常让人头痛的
- 确保你的数学运算是正确的



事件时滞

- 事件时滞是指在不同类型的记录中相关事件记录的时间的差别
 - 使用telnet 和login从一台计算机连接到另一台计算机
 - NetFlow记录显示telnet连接是从13:05:12开始的
 - 计算机B上的TCP wrapper显示telnet连接是在13:05:12发起的
 - wtmp 显示的实际时间是13:05:58
- 时滞变化是非常大的



事件时滞

- 我们还可以使用会话开始时间及持续时间
 - 在电话痕迹中寻找和modem池从2:03:22开始，持续00:10:05相匹配的拨号会话时间
 - 2:03:22 前后开始的wayyyy或许并不和会话相匹配
 - 会话短于 00:10:05的不匹配
 - 会话比 00:10:05 大得多的可能也不匹配



事件时滞

- 会话的终止时间有时可以比开始时间更匹配
 - 把 modem挂起,中止服务, 中止你登录会话
 - 减少时滞
 - 从UNIX退出, telnet会话中止 –时滞很短



事件发生先后顺序

- 某些记录是按会话的中止时间先后顺序来记录的
 - 在Unix上的过程记录
 - Cisco NetFlow 记录
 - TACACS+ 会话摘要记录



事件发生先后顺序

- 这是非常容易混淆的
 - 浏览记录流，查看计算机通信， – 可能直到30分钟以后才产生的
 - 浏览进程统计记录，查看子进程
- 我们经常需要记录会话的开始时间



进程统计记录

ttyp1 romig	12:32:28	00:00:07	ls
ttyp1 romig	12:33:02	00:00:05	cat
ttyp1 romig	12:33:45	00:00:03	egrep
ttyp1 romig	12:33:45	00:00:04	awk
ttyp1 romig	12:33:45	00:00:04	sh
...			
ttyp1 romig	12:30:12	00:10:02	sh



事件边界

- 我们可以使用会话的开始和结束时间来定义会话记录的边界，用它来在其它记录中搜索有用的信息
 - 举个例子， modem审计记录显示 T1到 T2之间的会话
 - 这是很显然的， 时间段说明了一切



事件边界

- 下列事件通常是我们所很难觉察到的
 - 在你登录到UNIX后，很容易运行系统进程
 - 然后是 at, cron, procmail等进程
 - 在modem会话结束后很长时间内仍然会留下痕迹



合并记录

- 某些记录入口会在系统上扩散
 - 多个并行的鉴别服务器
 - 多个 SMTP 前端
 - 不对称路由的多路由记录
- 需要合并记录
- 按照时间发生顺序来编排记录



可靠性

- 用可靠性衡量记录的变化
- 怎么保护记录?
 - 一些 wtmp, utmp 是可写的
 - Shell命令历史记录是他们的所有者可写的
- 取决于产生记录的软件的完整性
 - 黑客可能会用不产生记录或者无法产生登录事件记录版本软件来代替正常的软件- rootkit



可靠性

- 可靠性受到网络传输安全性的影响
 - 使用UDP传输的syslog, NetFlow 记录
 - 遭受数据损失
 - 遭受欺骗
- 利用在不同源上建立相关性来尽可能预防可能发生的问题



可靠性

- 我们需要根据收集到的异常情况来调整理论
 - 查看连接到计算机的telnet会话，但是没有登录会话
 - 这种情形说明可能被安装了个rootkit
 - 不要因为有人入侵了系统，就对理论采取怀疑态度– 要采取支持的态度和行动



IP地址和主机问题

- IP 地址可能会被欺骗
 - 需要去识别它是真的还是假的地址
 - common in flooding
 - 异常的telnet连接
- 域名窃取, cache中毒, 等
 - IP 地址比名字更容易解析
 - 做好两个都要做记录
 - 如果你不得不在其中作个选择, 那么请选择 ip address



找出遗漏了什么

- 有时恰恰是感兴趣的证据原料遗失了
 - 查看NetFlow中telnet到目标的通信记录
 - 但是没有登录会话
 - 在有rootkit的地方提高警惕
- 我们找到一个 ... 目录但是它里面没有内容
 - 可能就是空的
 - 也可能是个rootkit



遗漏了什么

- Flow logs shows traffic to TCP/31337
 - 但是你不能发现一个在那个端口监听的进程
 - 那可能是个rootkit



证据: 细节

REALSOI



证据: 细节

- 我们将列出可获得的一系列证据细节清单
- 计算机细节
 - 易消失的: 需要在关机前取得
 - 非易消失的:
- 用户细节
 - 如果你是对特定用户进行调查的话
- 网络/其他



计算机

REALSOI



数据和时间

- 记录和实际时间的偏移量
- 不要改变计算机时钟
- 你可以在关机和镜像磁盘后得到CMOS时间
 - 你可能不想在关机后再去查看BIOS时间



内存

- 易消失性
- `dd if=/dev/mem | somewhere` (CryptNetcat?)
 - 不要写到文件系统!
 - 不要写到 /tmp!
 - 可以写到软盘, 或者通过 netcat 导出到司法鉴定工作站
 - 我有时通过“strings”过滤它
- 其它工具



内存

- strings /dev/mem > file

- 可以查看是否有我们感兴趣的东西

- 但是，什么是我们感兴趣的呢？

```
03/15/97 00:55:28 sleep s12345 <notty>
```

```
03/15/97 0
```

```
florb&78
```



交换分区

- 易消失性
- UNIX
 - 使用 `/etc/fstab` 来判断交换分区的磁盘物理位置
 - `strings /dev/wd0s2b | less`
 - 试图把它变大
- NT:
 - 通过 ‘control panel>performance’ 并点击 ‘change’ 来得到清单
 - 内存分页可能会有如下的文件名： `c:pagefile.sys`
- 在内存和交换分区上使用 `lazarus (TCT)`



网络状态

- 易消失性
- UNIX
 - ifconfig -a
 - netstat -an
 - 看看附加的“netstat”，什么是 4th tcp?
 - arp -an
 - Lsof -I xxx



网络状态

- 易消失性
- NT
 - ipconfig /all, winipcfg “advanced” tab
 - netstat -an
 - arp -an
 - Tcpview, tdimon from www.sysinternals.com



文件系统

- 易消失性
- UNIX
 - Mounted: mount, df
 - 输出: /etc/exports
 - 检查 samba 输出!
- NT
 - 网络使用, 网络共享
 - Filemon, www.sysinternals.com
- 增加对感兴趣的事件的调查-远程的计算机是谁的?



UNIX /tmp 目录

- 易消失性
- 在某些系统上, /tmp 目录是放在随机存储器上的
 - 该目录中被删除文件的碎片很可能还在内存或者交换分区中
 - 你或许还可以在该目录中发现其它还没有删除的好东西



进程清单

- 易消失性
- UNIX系统
 - ps
 - 可能不会显示所有的进程 – rootkit. 使用安全的 toolkit.
 - “ps -axuwww”, 或者其他你喜欢的方式
 - lsof
 - 查看后缀 “lsof”, 记下最后一次的登录时间
 - 正常的进程, txt通常会是可执行文件
 - 这时候, 仅仅节点被列出来, 没有路径名?
 - ./bar & rm bar



进程清单

- 易消失性
- NT
 - pview, pviewer
 - handleex, pstools (sysinternals)
 - inzider (like lsof)
 - CTRL-ALT-DEL “task manager”
 - Filemon
 - Lservers, nplist (NT Objectives)



Other Process/Kernel Items

- 模块, 磁盘驱动器
 - Unix: lsmod (Linux)
 - NT: winobj
 - 了解自己的基线!
 - 小心 rootkits!



程序内存

- 易消失性
- UNIX
 - “gcore bar 2003”
 - 产生转储镜像 - core.2003
 - strings core.2003
 - 如果二进制程序已经被删除了，它就不会工作
- NT
 - Beats me!



追踪进程

- truss, trace, **strace**, ktrace
 - Creates ktrace.out
 - kdump ktrace.out
 - 跟踪重要和关键的系统调用, 查看读/写操作
 - 查看附录 - kdump
- good trick: “kill -STOP 1234”
 - 挂起进程, 然后检查它
 - 不会被抓到
 - 如果你让它继续运行, 可以在运行后再删掉



进程

- 追溯来源
 - 在系统上可以查到它吗?
 - 可能在 /tmp 目录中
 - 查找磁盘的空闲空间，在内核内存中扫描
 - 从二进制镜像中得到独特的串，在网络上可以搜索到它么?
 - 网页搜索, www.deja.com, packetstorm, bugtraq archives, etc.
 - 对遗留物进行检查，是很有作用的



进程

- 你可以很轻松地分析破解者的工具
 - 模糊不清的来源
- 在受试系统上恢复软件，并运行它
 - 调试
 - 编译
 - 追踪
 - Lsof
 - 观察网络通信 – tcpdump?



本地日志

- 运行本地日志处理命令并保存它的输出
 - who, w, last, lastcomm
 - 进程审计
 - sa (frees), acctcom (sunos)
 - c2 审计日志



进程审计

- “名字”是二进制文件的名称,而不是脚本的
 - 你有时可以比较该进程和运行系统上的脚本来识别脚本
 - 很难得出有结论性的东西



文件

- 使用先前复制的司法鉴定镜像文件进行工作
 - 把它拷到其它地方，并按通常方式安装它
 - 不要使用它来启动系统
 - 使用专用系统对待它，我们惯用linux系统



文件

- Linux 支持几乎所有早期文件系统格式
- 警告: 对应于你所使用的UNIX文件系统, 其它非UNIX文件系统的查看方式
 - ACLs, Alternate 数据流是不可见的
- `mount -t ufs -o ro,ufstype=sun /dev/foo /mnt`



文件

- 可能会找不到你所想找的文件
 - Rootkits 通常隐藏某些文件，不能被ls, du, find等命令查到
- 使用安全的工具 (如果是调查当前活跃的系统) 或者在其它系统安装复制的镜像系统



文件

- UNIX – 寻找:
 - 有坏许可的文件
 - 新的setuid, setgid 文件
 - 在奇怪地方的文件 (/dev中的空白文件, 任何其它地方的dev文件)
 - 有着奇怪名字的文件
 - 空间 – 虽然通常在某固定地方
 - `find / -name * * -print`
 - 太多的点, 并包含空格
 - `find / -name .* * -print`
 - `find / -name ...* -print`



文件

- UNIX (续):
 - 查找最近修改的文件
 - `find / -mtime -14 -ls`
 - 要注意的是，入侵者可以很容易捏造一个时间戳
 - 他们中的大多数人是懒惰的，即使使用rootkits很容易就可以实现
 - 小心别轻易自己改变时间戳!
 - The Coroner's Toolkit - mactimes!
 - 半-文件访问/修改事件的时间顺序
 - 仅仅显示最近的活动
 - 不要显示谁/什么改变了它
 - 很容易被欺骗



文件

- UNIX (续)
 - Core files
 - 缓冲区攻击后留下的?
 - 使用字符串查找 – 任何有疑点的东西比如, `/bin/sh`?
 - 使用`mount`, `df`命令来查看存在那儿的是什么类型的网络文件系统
 - 要小心的查找他们!
 - I usually don't if there's a lot
 - 但是有时那里放的是会让人疯狂的东西



文件

- UNIX, NT
 - 查找可能会对你的查找有所帮助的工作
 - 查找 steganography工具和 jpeg文件捆绑工具?
 - 查找 PGP和奇怪的文件



文件

- 文件完整性分析
 - 文件有什么改变?
- 和干净的系统进行比较
 - UNIX: “`cd /mnt ; find . -type f -print0 | xargs -0 md5 > /tmp/files.md5`”, then compare to same list from a good system.
 - 或者在本地安装一个干净的文件系统，然后使用命令“`diff -r /bad /good`”进行比较
- 和备份文件进行比较



文件

- Tripwire （案发前使用过么？）
 - 和旧有的数据库文件进行比较
 - 什么是旧的数据库？需要首先使用 tripwire
 - 你可以从备份中创建一个数据库文件，但是你必须输入路径



Shell命令历史文件

- 超级用户的，其他普通用户的
- 它们不是总是在HOME目录中的，要查找它们！
- 一些是有时间戳的
- 它们可能会被所有者所修改！
- 历史文件的最后一个命令是exit命令，而且是在退出时写到磁盘上



系统配置 - UNIX

- 对所有的用户检查他的 crontab 设置
- 检查系统配置文件 (rc files, inetd.conf)
- Root .rhosts, /etc/hosts.equiv, ssh config files
- /etc/hosts.allow, hosts.deny



系统配置 - NT

- 注册表
- 交换分区文件
- 临时文件
- 浏览器历史记录文件, cache, cookies, bookmarks, URL memory
- 用户配置用户
- 注册流
- 应用程序记录
- 会话记录



系统配置 - NT

- 运行和查找历史记录
- 开始菜单顺序,历史,最近访问文档
- 我的文档



帐号

- 如果该系统是NIS域的一部分，你可能想去枚举用户/用户组数据库



Palm Pilot

- pilot-link!
- Image of ram - 'pi-getram /dev/ttyd1' (for instance).
- Private records?
- 加密缓冲区 - check for pass phrase in ram image
- 确保把数据等级设得高点 :-)



用户

REALSOI



用户 - UNIX

- Shell 命令历史记录。别忘了ROOT用户的!
- Cron, at 记录
- Netscape cache, history, cookies, bookmarks
- 在所有地方查找该用户拥有的文件
- .rhosts, .ssh*/authorized_keys
 - 可能会导致要调查相关的其它关联主机
- 邮件,文件,等等.



用户 - NT

- 检查系统配置 - NT
- 邮件, 文件 QQ? .



用户

- 检查浏览器代理服务器，记录等
- 你可能可以从其它POP服务器中提取出电子邮件



网络/其他

REALSOI



电话记录

- 拨号记录跟踪
 - 通过法律强制手段进行
- modem pool, single number
 - 不能通过环路来分割它
 - 利用相似的开始时间和会话时间来把相关记录关联起来
 - 他们的时钟总不正确
 - 时滞



电话记录

- 在每天有 60,000 多的电话记录里查找不是很有趣的事情
- 要求要指定时间段内的电子拷贝



电话记录

- 例子
- 入侵者登录Unix 信箱 的记录(最近的一次):

```
user      tty      src ip      date, time, duration
romig     tty5     10.0.0.100  Fri Oct 15 13:16 - 13:25
          (00:09)
```

- 10.0.0.100 属于modem pool 中的一个终端, 登录会话 (from TACACS+) 显示:

```
Fri Oct 15 13:16:05 1999 romig async9 stop addr=10.0.0.100
elapsed_time=576
```



电话记录

- 电话跟踪那一天的整个modem pool (六百多条电话线)，显示:

date	start	end	caller	target
10/15	13:15:23	13:25:42	614-263-7663	614-555-1212
10/15	13:15:32	13:15:33	614-555-1000	614-555-1212

- 要知道从电话开始拨号到确认有着45秒的时滞



电话记录

- Modem pool中的鉴别会话的开始和Unix box之间的通信也有时滞
- 会话的终止时间的时滞是很短的 – 差不多我一挂机就中止了
 - 使用它，有几分把握可以发现时钟的差异
- 越长的通话时间通常比短的越有特征



Pen register

- 通过法律强制手段
- After trace identifies callers
- 记录特定线路上的所有通话记录
- 通常这样做需要正当的理由



呼叫者的身份

- 我对这部分内容没有很多实际经验
- 显然，如果你有办法记录呼叫者的身份，并把它和modem pool 中的会话相关联，那么它将是有益的
- Unlisted numbers, caller-id blocking
- 它是否对 jump-start pen register有帮助？



Cable modems

- 我的提供商并没有要求鉴别
- 使用 DHCP 来配置 IP
- 它是那些有着鉴别或网络通信记录的设施之一，但是我不应该过多依赖它



KBAuth, TACACS, TACACS+

- 见附录中的例子
- KBAuth, TACACS are event logs – login, logout are separate
 - 需要重新登录来得到会话
 - 它很困难的
- TACACS+ is session oriented
- 包括起始时间，用户，显示的IP，终端服务，端口



DHCP

- 计算机引导时, 查询 DHCP服务器, 得到他的IP地址, 并使用它
- 当该线路过期的时候, 另一计算机可以使用它的地址
- 我所见过的服务器, 没有记录历史的通信记录, 只是仅仅记录当前的通信记录
- 见附件
- A lease is just a lease – not proof of use
- Take snapshots



Network Address Translators (NAT)

- 它越来越普通
- 每一 NAT 客户使用私有地址, 特别是通过 DHCP 分配的
- 它们的 IP 通信被解释成 NAT 服务的某一外网 IP 地址, 并使用唯一的端口
- 但是, 没有东西来记录它
- 很遗憾!



POP (IMAP)

- Unix POP, IMAP服务通常通过syslog来记录
- 记录会话，包括被识别的用户
- 或许也可能记录所发生的行为 – 上传下载
- Can be useful as pseudo-authentication for computers that are otherwise unauthenticated!



UNIX: Wtmp, wtmpx, utmp, utmpx

- Readable via who, last, lastlog, w
- Easy for intruder to “zap”
 - 使用带有木马版本的登录命令，其记录工作通常都是失效的
 - 频繁编辑
 - 文件有时是任何人任何地点都可以写的
- chkwtmp: 检查0字节的文件



UNIX: wtmp and friends

- 主机名
 - 有时它是缩写的 (fixed in wtmpx, utmpx) (last truncates)
 - 你可能通过其他记录来解析它
 - Tcp-wrappers, Cisco NetFlow, argus, etc.
 - 主机名可以被欺骗



Login Logs

- UNIX: lastlog
 - 每一帐户最近的登录时间
 - chklastlog – 检查lastlog记录的最近修改时间
- NT last:
 - usrstat (sort of, from resource kit)
 - NTLast (from NT Objectives) – freeware, matches log in/out records



UNIX syslog

- 设施, 级别
- 通常的位置是 /var/log, /var/adm, /var/spool/mqueue
 - I like to crank up levels and split by facility to different files
 - I also like to log to a separate log server
- 对远程访问的使用UDP来记录
 - 要知道入侵者很容易通过网络来插入错误的消息
 - 要知道客户和服务器的某些消息可能会丢失



UNIX Syslog

- Syslog中的时间戳指的是syslog服务收到消息的时间
 - 当从源主机来关联证据的时候要当心！ – 时钟不是同步的
 - 这可能更好用点, syslog服务器或许可以有更精确的时间



NT Eventlog

- `dumpevt /logfile=sec /altfile=foo /computer=bar`
- `eventslog`
- Caution: NT event logs are “funky”
 - <http://www.heysoft.de/nt/eventlog/faq.htm>



Sendmail

- 见附录
- 分割记录来接受消息
- 把相关记录相关联起来是很痛苦的一件事



PMDF

- Run screaming



Web, 包括代理

- 没有什么可说的,除了某些情况下你必须检查web服务日志
- 特别是透明非自愿的代理



FTP servers

- Xferlog
- 会话, 包括受到确认得用户
- 上传下载的文件
- Stock FTP daemons 没有提供足够记录
- Wu-FTPD does



Tcp_wrappers

- 日志工作如何，有用吗？可能通过 `syslogd` 来记录拒绝的连接
- 让它工作是非常有用的，即使你没有用它来拒绝连接企图



Karlbridge TCP Logs

- Wireless KarlBridge/Firewall
- 见附录



Firewall

- Karlbridge, CISCO, ipfw...
- 不是要告诉你具体发生了什么，而是要告诉你实施者试图做什么



Cisco NetFlow

- Flows 显示在单一方向上收集相似的包
 - 源, 目的地自治系统号, IP, TCP/UDP 端口
 - 起始时间
 - TCP 标志
 - IP 协议类型
 - # 包, 八位组



Cisco NetFlow

- 会话的多流通路 Multiple flows for a “session”
 - 覆盖整个生命周期, 超时设定等
 - 至少每个方向必须有一个
- 问题:
 - 根据终止时间进行分类
 - 欺骗IP
 - 不对称路由



Tcpdump

- `tcpdump -i eth0 -s 1600 -w 021229.bin host attacker.com`
- 保证你的 `snaplen` 时间是足够长的
- 确信你的行为已经得到批准 - ECPA?
- 整体回顾



调查取证工具

- 调查取证工具箱
- 调查取证计算机系统
- 调查取证软件



调查取证工具箱





系统硬件调查取证

- 主系统
 - Pentium系列计算机
 - 多操作系统
 - UNIX, Windows, MAC
- 介质选择
- 可拆除介质 (REM-KIT)
- 磁盘镜像硬件
 - Image MASter 500 & 1000
- Static-Dissipative Grounding Kit w/Wrist Strap
- UPS





介质选择

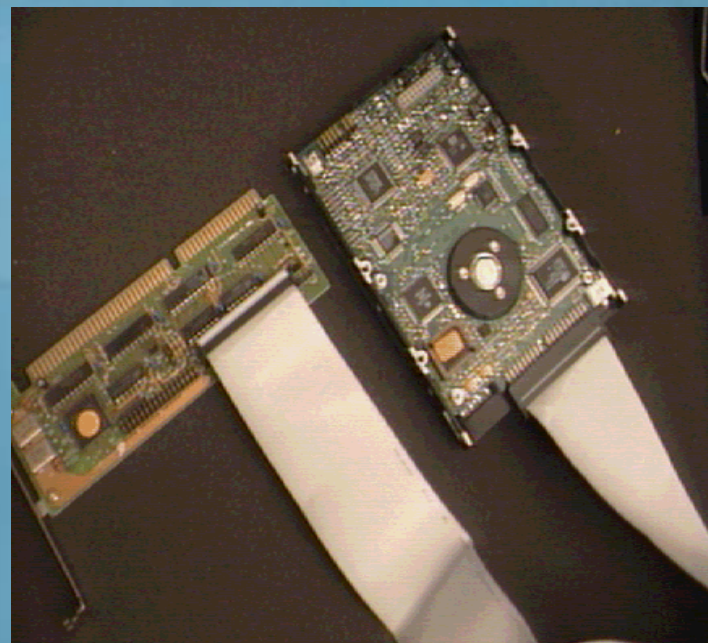
- 调查取证系统应该有大量空间用来扩展和外部设备介质。
- 最好的是用SCSI介质





介质选择

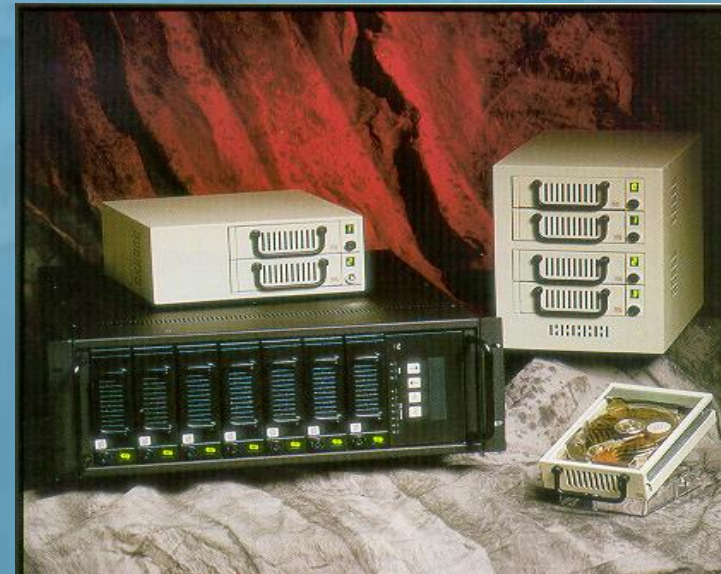
- 内部磁盘
- 磁带
 - QIC磁带机
 - Travan磁带机
 - DAT
- 光学介质
 - CD-ROM
 - CD-Writer
 - DVD





可拆除介质

- 硬盘
- ZIP Drives
- Jazz Drives
- PCMCIA Flash
Disks





磁盘镜像硬件

- 支持 IDE & SCSI
- 扇区拷贝
 - DOS, Windows 3.1,
 - Windows 95, NT, SCO,
 - UNIX, OS/2 & Mac O/S
- 全部读写确认和报告
- 记录能力
- 对主盘不可写





调查取证软件

- 洁净操作系统
- 磁盘镜像备份软件
- 检查和恢复工具
- 文件查看工具
- 破解软件
- 打包和压缩工具



验证软件

- 决定功能
 - 确定操作
 - 确定限制
 - 确定漏洞
- 法庭陈述
 - 用自己的体验来阐述证据
 - 肯定是专家级别阐述



磁盘镜像软件

- 在比特流水平上复制磁盘，而不是文件流水平上
- 非操作系统依赖
- 必须有记录和错误报告
- 必须有删除文件的备份
- 工具
 - EnCase
 - SafeBack
 - SnapBack
 - DD



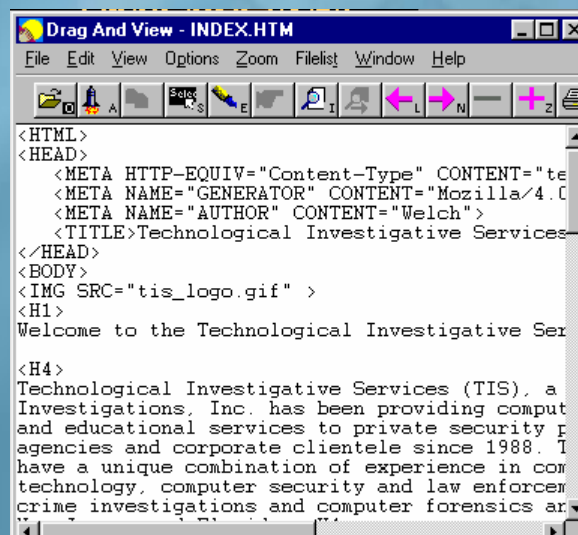
研究工具

- 调查取证工具
 - EnCase
 - 调查取证工具箱
- 文件系统工具
 - DOS, Windows, NT, UNIX
- Norton Utilities



文件查看工具

- 快速查看插件
- 拖拉和查看
- 翻页插件





调查取证分析

- 计算机调查取证
 - 磁盘锁定
 - 创建磁盘镜像
 - 鉴别文件系统
 - 列出磁盘目录和文件系统清单
 - 定位隐藏和模糊数据
 - 簇分析



鉴别文件系统

- 保证和查封数据相关的数据的完整性是很重要的
- 信息摘要——单向hash 算法
 - CRC32 (32 bits)
 - MD5 (128 bits)
 - SHA (160 bits)
- 创建系统目录和文件的MD



鉴别文件系统

Password Recovery Toolkit

File Edit View Actions License Settings Help

Ghosting

All Folders

- Digital Signatur
- Forms
- Ghosting
- Hacker
 - Joauc
 - Lod
 - Phun
 - Uxu
 - Worm
- Htc_book

Contents of 'Ghosting'

- Evidence Log
- Ghosting Letter 2
- Ghosting Letter

Files to recover

Name	In Folder	MD5	SHA
LEGION.TXT	C:\SECURITY\...	5D0142879D8E5E340924740D67A3C81F	01710989ADE0DC47D
LOD01-02.TXT	C:\SECURITY\...	89872C2F4D8823A3EF6DF3B0987FC58F	869FA161DAEF929EC
LOD01-08.TXT	C:\SECURITY\...	1C298E442E3661A448E28A8FA26AABE1	0190A291CB8E0CEF9
LOD01-09.TXT	C:\SECURITY\...	5BE68B5DF25BB8F952EEA1AD2C5E18D6	32D81775625BB858A
LOD01-10.TXT	C:\SECURITY\...	34C7D80E6A43D35504363E6F2E2B05E8	F02F133CF31A852F32
LOD01-11.TXT	C:\SECURITY\...	642E7ED55C8DD527BD03D25C7AAD9740	335A86C4E8B19854B



目录和文件清单

- 创建树状目录清单
- 确定可疑文件
- 清查磁盘上所有的文件
- 检查通信程序
- 注册文件
- 文件最后访问时间
- 相关文件



识别可疑文件

- 利用案例特征进行文件搜索
- 利益案例特征进行关键字搜索
- 改变不适合的文件扩展名
- 隐藏或删除文件



隐藏的和模糊的数据

- 隐藏文件属性
- 隐藏目录
- 临时目录
- 已删除文件
- 松弛空间
- 未分配空间
- 交换空间
- 信息图象隐藏



信息隐藏学

- 信息隐藏学是一门隐藏通信内容的科学。
- 用它来加密数据后，就可以否认数据的存在
- 文件可以藏在图像内
- 把数据伪装为无罪的文档



信息隐藏工具

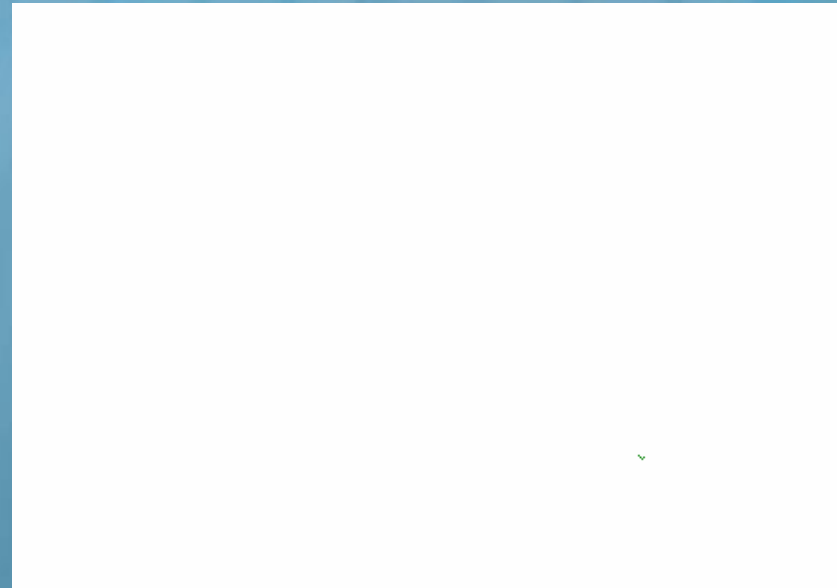
- 把数据隐藏在图象里，图象文件和
松弛空间里





重像

- 白信写在白色的背景上，或者黑信写在黑色背景上





重像

- 白信写在白色的背景上，或者黑信写在黑色背景上

April 15, 1997

Hit Men 'R' Us
935 Highway 47
Fairfield, New Jersey 07741

To Whom It May Concern:

I would like for you to kill my ex-wife. She lives at 1313 Mockingbird Lane, Anywhere, USA. I will pay you \$50,000.00 (Fifty thousand dollars), ½ up front; the rest upon delivery of her head.

I will get back to you with all the details.

TW



簇分析

- 簇分析标准
 - 内容，定位和情形
- 识别系统使用和历史
 - 系统的引导区
 - 碎片
 - 重新打包数据文件 w/o 改变数据/时间
 - 系统擦除和重引导
 - 所有的松弛空间和未分配空间置为0
 - 所有数据/时间属性同时关闭



分析问题

- 检查访问控制系统
- 病毒传染
- 格式化磁盘
- 磁盘损坏
- 磁盘擦除和消磁介质
- 碎片磁盘
- 簇边界
- 证据清除器

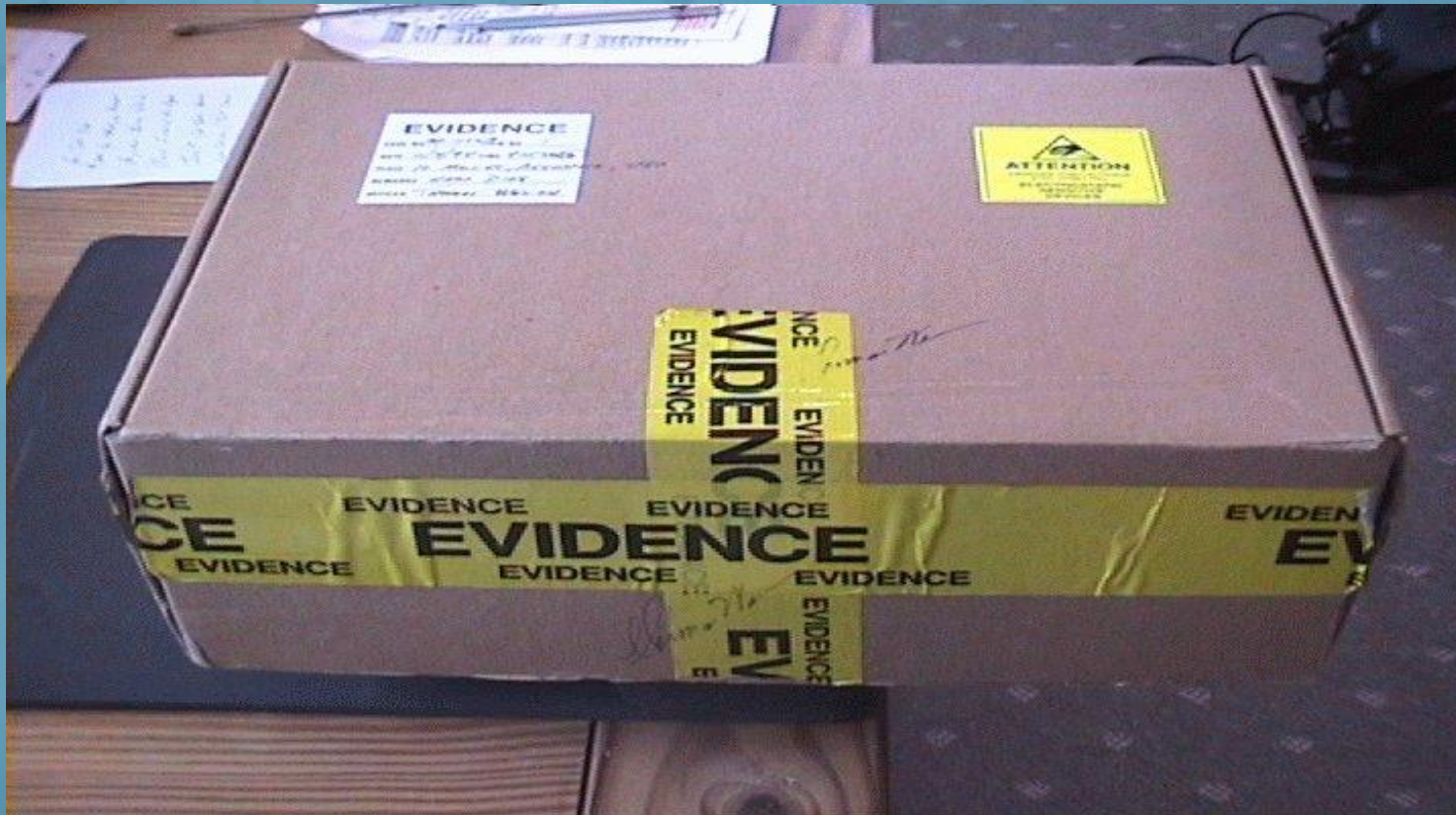


证据保护

- 透明静态保护袋
 - 通过安全封装静电敏感设备来提供静电屏蔽保护。The nickel shielding layer creates a Faraday type shield.
Meets MIL-B-81705 and DoD-STD-1686A
- 泡沫添加磁盘运输箱
- EMF警告标签



证据保护





网络调查取证

- 分析包痕迹
 - 建立事件发展顺序过程
 - 目标是确定入侵者
- 工具
 - 网络 Sniffer
 - 系统记录
 - NTSC Adapter

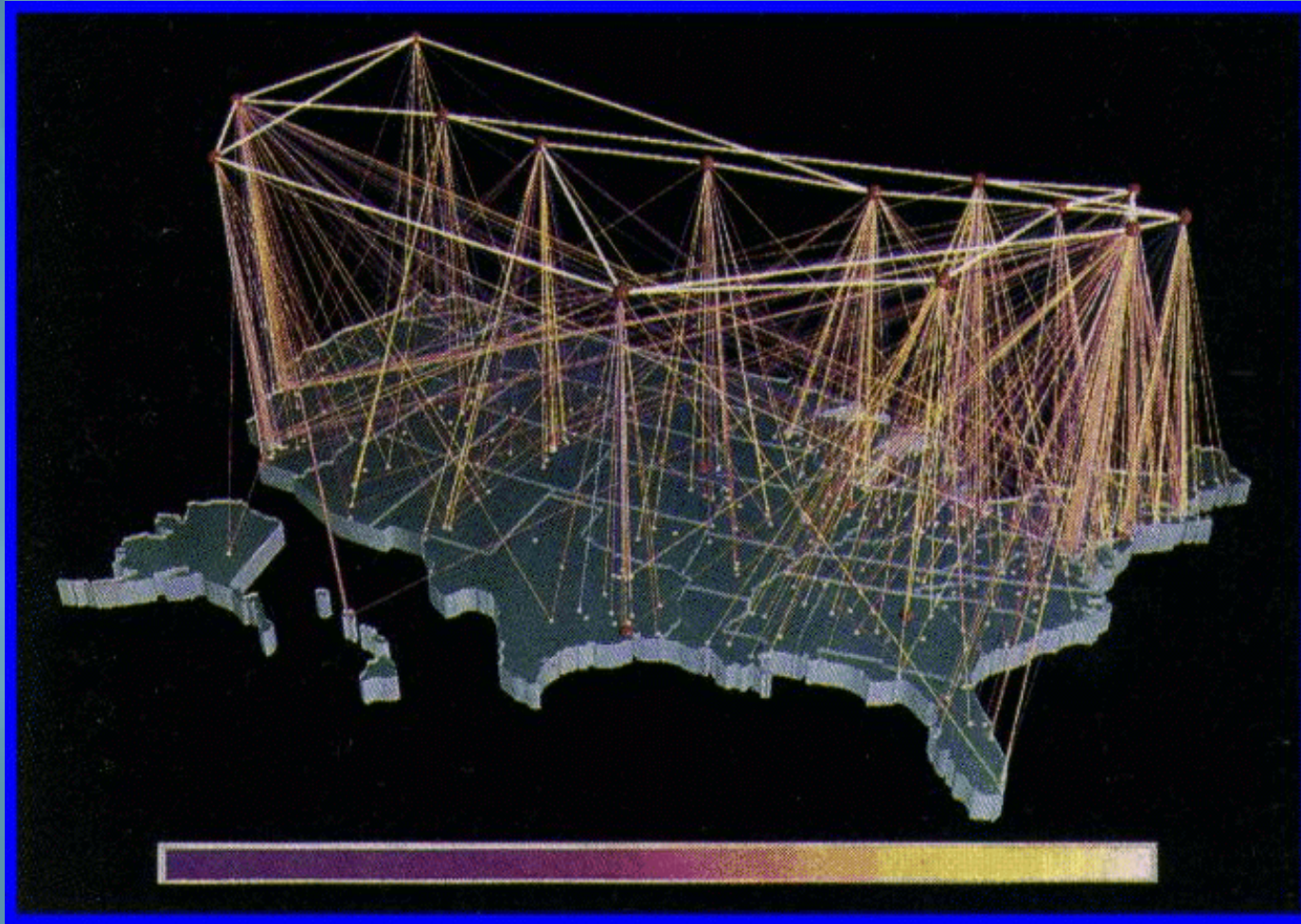


网络调查取证

- IP 欺骗
- Hijacking
- 密码攻击
 - 社会工程
 - 密码破解
 - Sniffers
- 分布式-等价式攻击
- 身份隐藏



Connection Laundering





电子邮件调查取证

- 2000年电子邮件使用情况
 - 108亿电子邮件用户
 - 每天252亿封电子邮件
- 电子邮件使用的是不同步的允许通风的通信机制。
- 人们越来越把更多的信息通过电子邮件来传送，而不是通过电话。
- 电子邮件欺骗。



电子邮件欺骗

- 只要求：
 - 电子邮件中继服务
 - 邮件命令知识
 - telnet <relay server>
 - helo
 - mail from: gwbush@whitehouse.com
 - rcpt to: twelch@sendsecure.com
 - Data <message>



调查取证的展望

- 因为用来隐藏犯罪的方法越来越巧妙，因此调查人员和分析人员应该掌握更多的技术
 - 需要专家
 - 还是需要专家，是在座的各位？
- 加密仍然是重要的关注点—时间能说明一切



调查取证的展望

- 调查取证工具
 - 必须自动化
 - 调查取证工程必须包括 Fuzzy Logic and Intelligence来处理簇边界
 - 必须开发出UNIX 下使用的工具
 - 需要开发出更好的网络分析工具
 - 开发分析分布式应用程序，例如 Java, COM, and DCOM的工具。



总结

- 计算机调查取证是突发事件响应范畴内一项完整的功能
- 处理方法和步骤是计算机调查取证中最重要的方面
- 未来的计算机犯罪要求提升计算机调查取证的能力
- 基于取证方法论的取证决策和指导系统呼之欲出！

• 谢 谢！

• 祝安焦峰会圆满成功！