Internet Artifacts:

COMP3731 Computer Forensics Finals Study Guide

• Artifacts of importance and what information can they provide (no need to memorize location paths)

• Formats used by different browsers to store the artifacts

互联网文物：

COMP3731计算机取证决赛学习指南

•重要的工件以及它们可以提供哪些信息（无需记住位置路径）

•不同浏览器用于存储工件的格式

Analysis & Validation:

• Basic steps for all computer forensics investigations

• Data hiding techniques: file manipulation (methods and detection), hiding partitions and clusters, bit shifting, steganography, rootkits (what they do and how to detect them)

• How to recover encrypted files and passwords

分析和验证：

•所有计算机取证调查的基本步骤

•数据隐藏技术：文件操作（方法和检测），隐藏分区和群集，位移，隐写术，rootkit（他们做什么以及如何检测它们）

•如何恢复加密的文件和密码

Data Carving/Steganography/Image Forensics:

• Data carving

- impact of file fragmentation, what are false positives, magic numbers

- types of data carving: basic and advanced

- header-footer, header-maximum length and header-embedded length

carving

- file structure types, what is file structure based carving, performing it on

jpeg and zip files

- how to carve file fragments, carving bi-fragmented files, carving using

matching metrics

数据雕刻/隐写术/图像取证：

•数据雕刻

- 文件碎片的影响，什么是误报，魔术数字

- 数据雕刻类型：基础和高级

-页眉 - 页脚，页眉 - 最大长度和页眉 - 嵌入长度

雕刻

- 文件结构类型，什么是基于文件结构的雕刻，执行它

jpeg和zip文件

- 如何雕刻文件碎片，雕刻双碎片文件，雕刻使用

匹配指标

• Steganography

- what is it and general idea of how its done using data insertion and data substitution

- what is LSB substitution and how can it be done on images and audio files

- steganalysis on images: basic idea behind enhanced LSB and chi-square

method

• Image format types (no need to memorize offsets), lossy and lossless

compression, idea of how Huffman codes work

•隐写术

- 它是什么以及使用数据插入和数据替换完成它的一般概念

什么是LSB替换以及如何在图像和音频文件上完成

- 对图像的隐写分析：增强的LSB和卡方后面的基本思想

方法

•图像格式类型（无需记忆偏移），有损和无损

压缩，关于霍夫曼代码如何工作的想法