



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Digital Forensics Analysis (ACCA7031_LON)

Lecture 4

Advanced Digital Forensics Practice

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Content covered

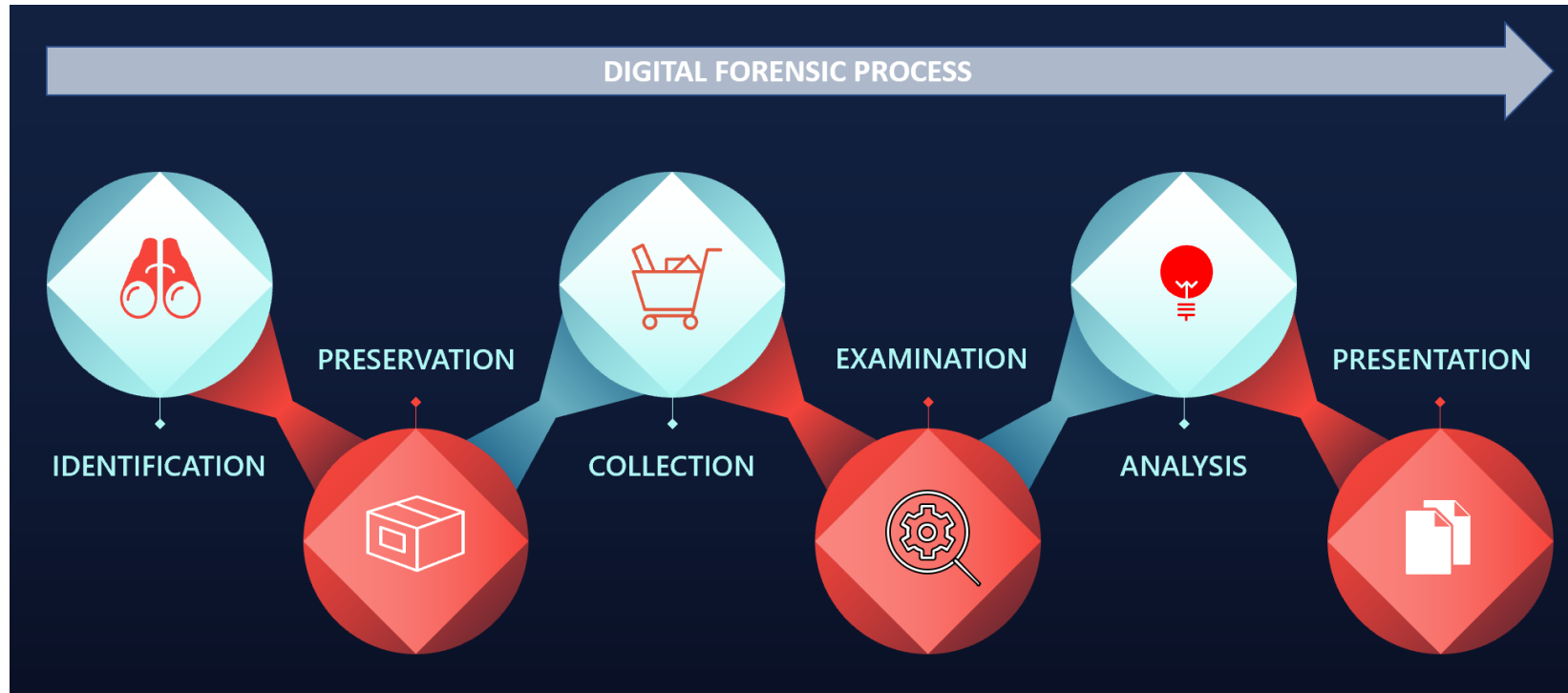
- Determine Timeline in crime or incident investigation
- Data extraction, recovery, and carving
- Find hidden or deleted files in unallocated clusters and slack space
- Reconstruct fragments and partial recovery in context of graphics
- Identify anti-forensics traces and tackle obfuscation
- Identify components of program execution

Objectives

- Understand the utility of timeline analysis in cyber incident investigation
- Understand data carving mechanism and how data recovery software operate
- Familiarise with unallocated memory investigation including clusters and slack space
- Analyse malware multi-stage execution in memory.
- Tackle code obfuscation techniques that hinder static code analysis, including the use of steganography

Basic Forensic Work

Reminder of the Digital Forensics process:



Basic Forensic Work (cont.)

- Identification
 - Trace evidence in forensics left when two objects come into contact. In digital world, similar trace evidence left when two systems come into contact.
 - E.g individual browses a website, the web server or web application firewall may record the individual's IP address
- Preservation
 - Once evidence identified, it is important to safeguard it from any type of modification or deletion.
 - E.g Evidence such as log files, it may become necessary to enable controls that protect log files from removal or modification or host systems such as desktops, it may become necessary to isolate the system from the rest of the network
 - Also critical that any users are not allowed to access a suspect system. This ensures that users do not deliberately or inadvertently taint the evidence

Basic Forensic Work (cont.)

- Collection
 - Imperative that digital forensics examiners take order of volatility into account when starting the process of evidence collection
 - Mistakes in how evidence is acquired can lead to that evidence being tainted and, subsequently, not forensically sound
 - The chain of custody is maintained throughout the life of the piece of evidence. Even when the evidence is destroyed or returned, an entry is made in the chain of custody form, and it is crucial this is maintained
- Examination
 - Details the specific tools and forensic techniques that are utilized, to discover and extract data from the evidence that is seized
 - E.g case where malware is suspected of infecting a desktop system as part of a larger attack, the extraction of specific information from an acquired memory image would take part at this stage

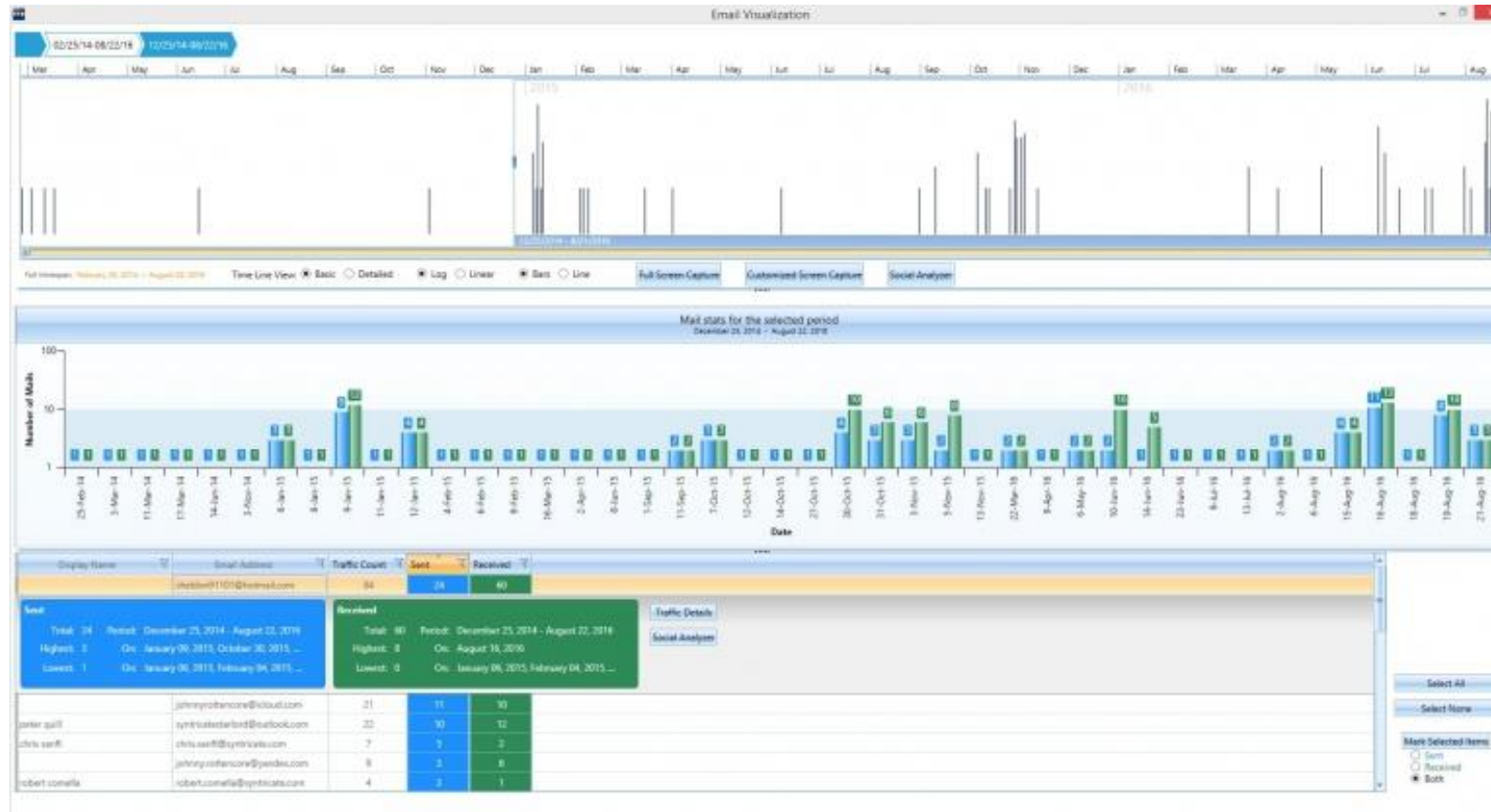
Basic Forensic Work (cont.)

- Analysis
 - After examination phase has extracted potentially relevant pieces of data, the digital forensics examiner then analyzes the data in light of any other relevant data obtained
 - E.g If digital forensics analyst has discovered that a compromised host has an open connection to an external IP address, they would then correlate that information with an analysis of a packet capture taken from the network
- Presentation
 - Reporting of facts related to digital forensics needs to be clear, concise, and unbiased
 - Forensic examiners will often be required to prepare a detailed written report that addresses every action and captures the critical data required
 - Aids in determining the root cause of an incident
 - Testifying in court may be required if the incident under investigation has yielded a suspect or other responsible party

Timelining

- Human beings are creatures that primarily learn visually
- As an investigation moves forward, the amount of evidence needing to be correlated will grow
- A seemingly monotonous event or bit of data could turn out to be a massive piece of evidence when placed in conjunction with others
- For a digital forensic analysis or investigation, building a timeline could take place over a day, a week, or months.
- Categorises all the evidence by date and helps visualise the results of investigation

Timeline example



Forensic Data Carving

- Identifying and recovering files based on analysis of file formats
- Carving is a helpful technique in finding hidden or deleted files from digital media
- A file can be hidden in areas like lost clusters, unallocated clusters and slack space of the disk or digital media
- Files should have a standard file signature called a file header (start of the file)
- A search is performed to locate the file header and continued until the file footer (end of the file) is reached

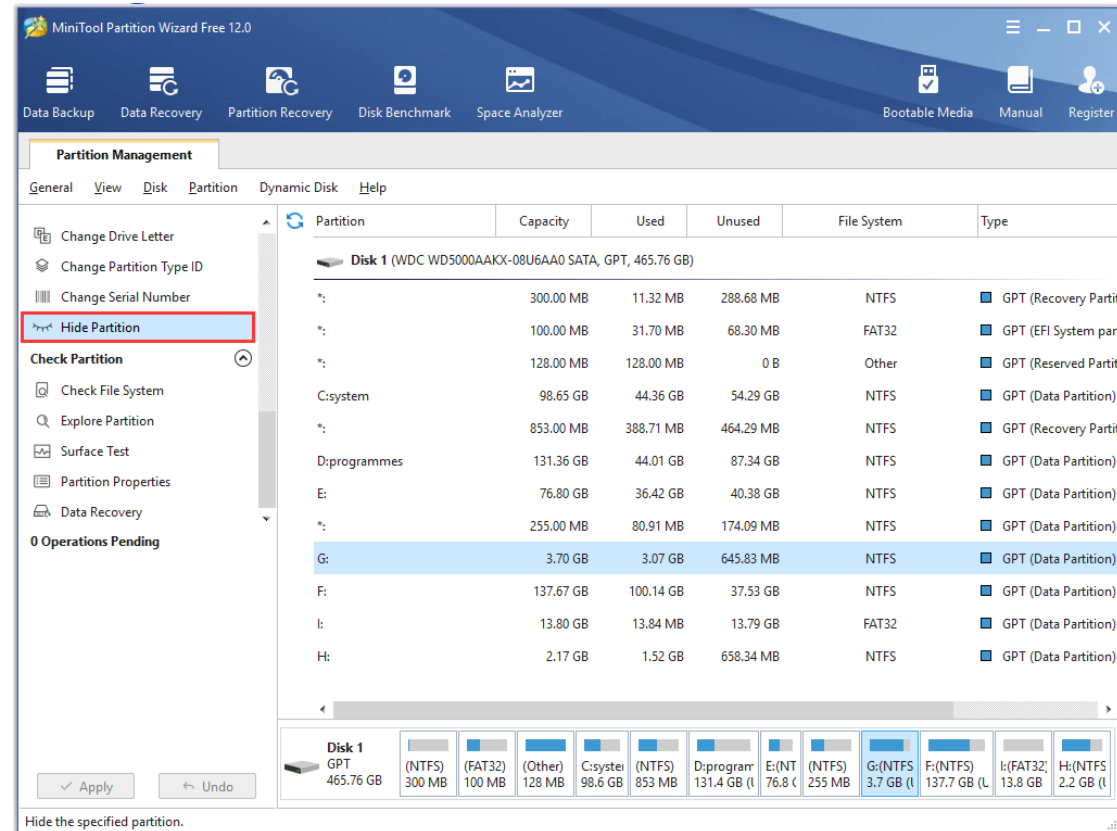
Addressing Data-hiding Techniques

- File manipulation
 - File names and extensions
 - Hidden property
- Disk manipulation
 - Hidden partitions
 - Bad clusters
- Encryption
 - Bit shifting
 - Steganography

Hiding Partitions

- Delete references to a partition
 - Re-create links for accessing it
- Use disk-partitioning utilities
 - PartitionMagic
 - System Commander
 - LILO
- Account for all disk space when analyzing a disk

Hiding Partitions



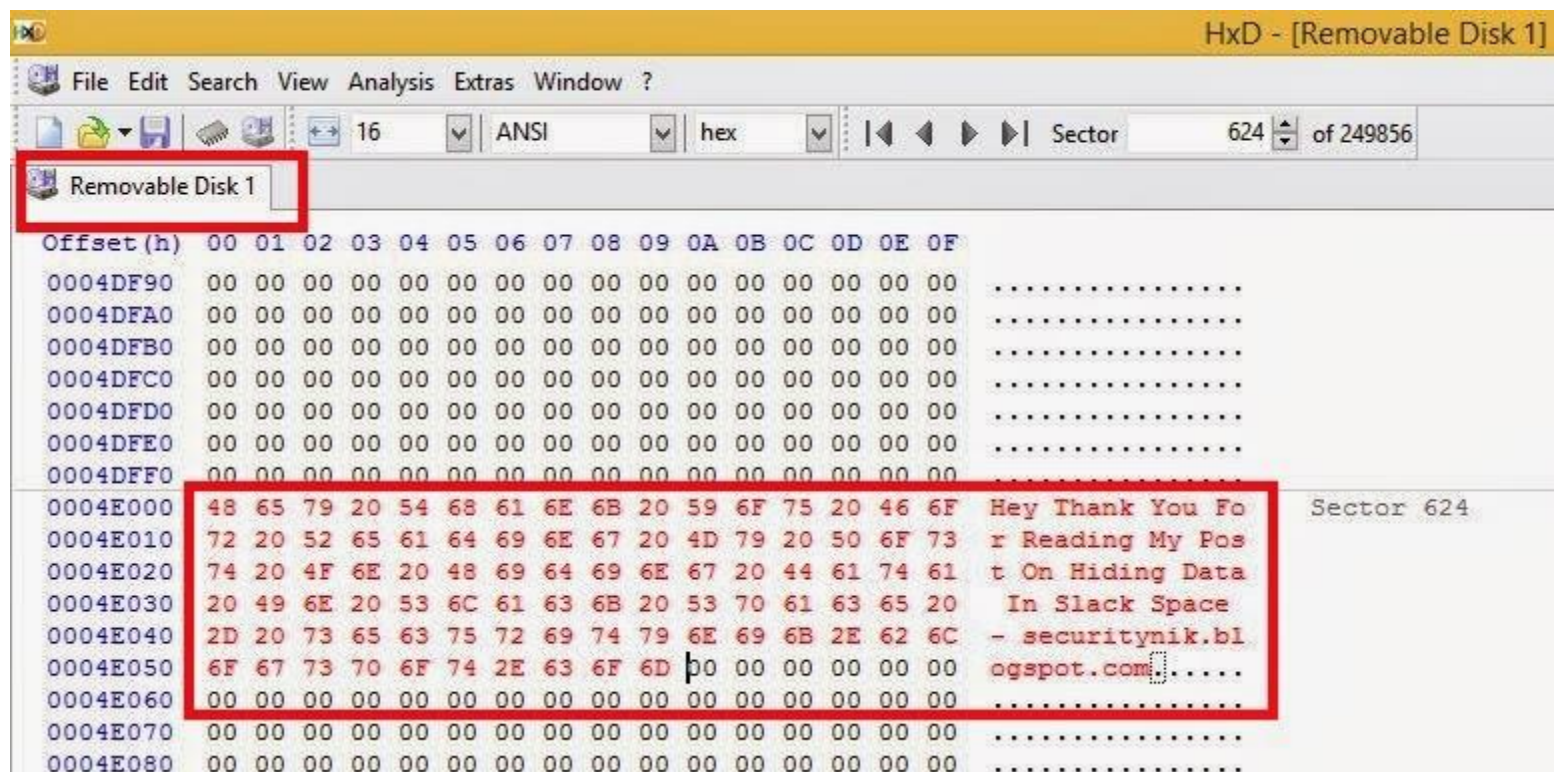
Marking Bad Clusters

- Place sensitive information on free space
- Use a disk editor to mark that space as a bad cluster
- Common with FAT systems

Slack Space

- Leftover storage that exists on a computer's hard disk drive when a computer file does not need all the space it has been allocated
- Technically, a file's slack space is the difference between its logical and physical size
- The logical size of a file is determined by the file's actual size and is measured in bytes
- The physical size of a file is determined by the number of sectors that are allocated to the file
- Sectors are commonly clustered in groups of four by default which means that each cluster has 2,048 bytes

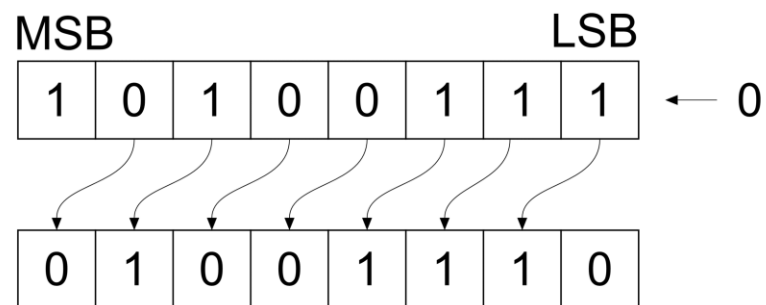
Slack Space (cont.)



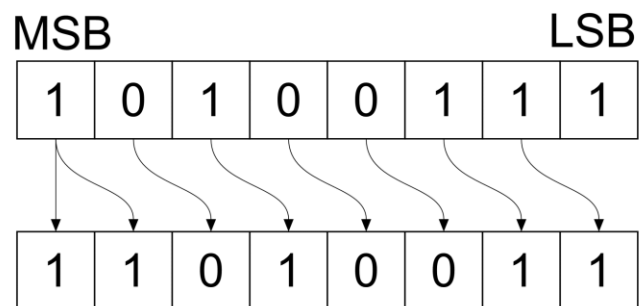
Bit-shifting

- Old technique
- Shift bit patterns to alter byte values of data
- Make files look like binary executable code
- Tool
 - Hex Workshop

Bit-shifting



Left Arithmetic Shift



Right Arithmetic Shift

Using Steganography

- Greek “hidden writing”
- Suspect can hide information on image or text document files
- Very hard to spot without prior knowledge
- Tools
 - S-Tools
 - DPEnvelope
 - jpgx
 - tte

Steganography

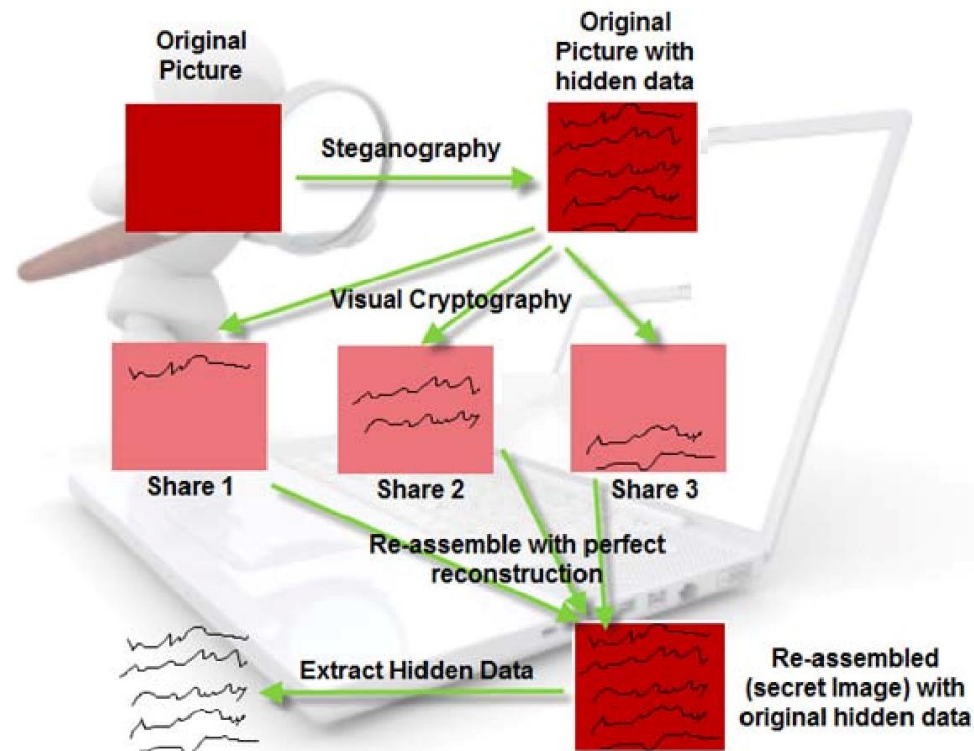


Figure 1: Proposed algorithm using both steganography and visual cryptography with perfect reconstruction

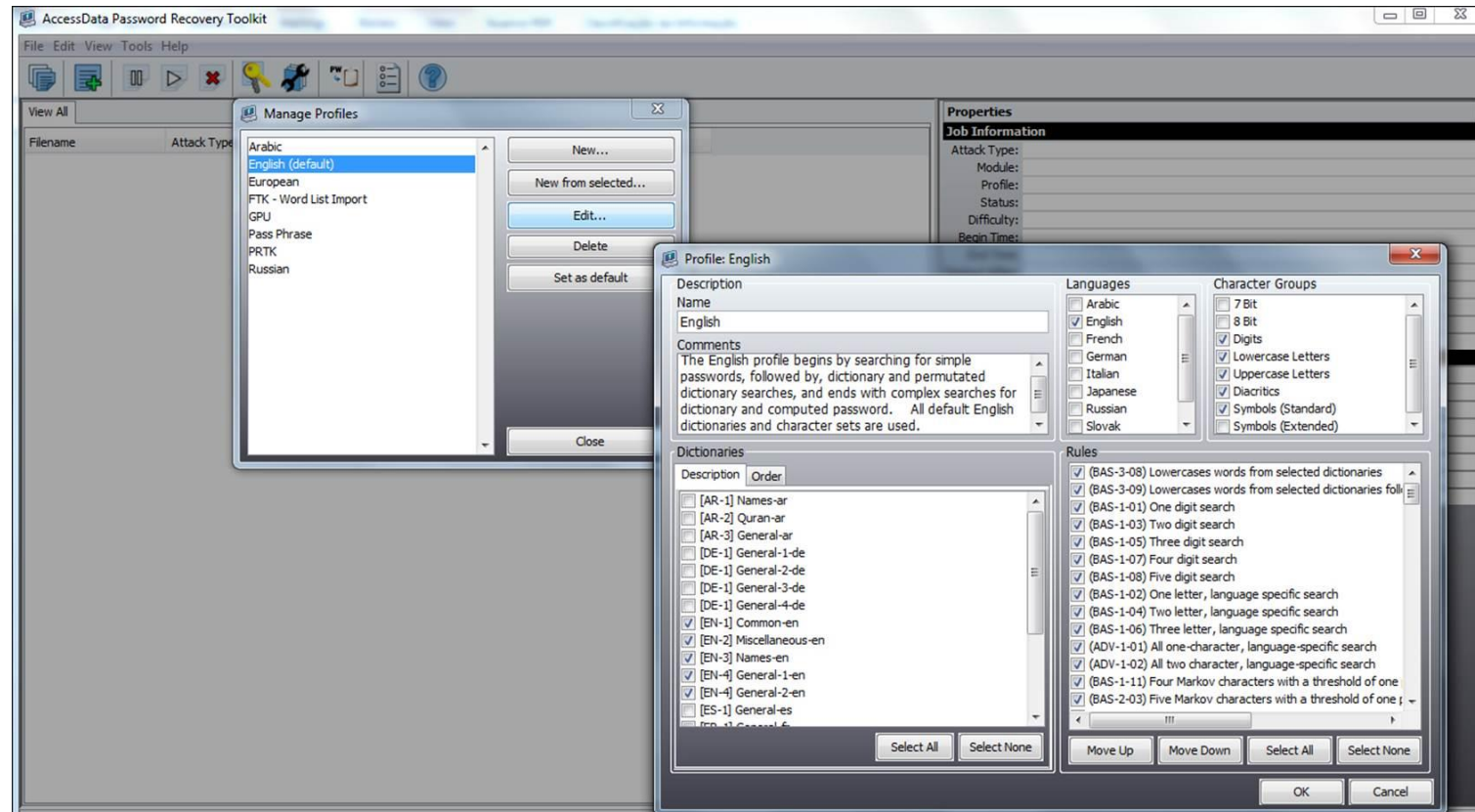
Examining Encrypted Files

- Prevent unauthorized access
 - Password or passphrase
- Recovering data is difficult without password
 - Key escrow
 - Cracking password
 - Expert and powerful computers
 - Persuade suspect to reveal password

Recovering Passwords

- Dictionary attack
- Brute-force attack
- Password guessing based on suspect's profile
- Tools
 - PRTK
 - Advanced Password Recovery Software Toolkit
 - @stake's LC5 (L0phtCrack)

Recovering Passwords



Recognizing a Graphics File

- Contains digital photographs, line art, three-dimensional images, and scanned replicas of printed pictures
 - Bitmap images: collection of dots
 - Vector graphics: based on mathematical instructions
 - Metafile graphics: combination of bitmap and vector
- Types of programs
 - Graphics editors
 - image viewers

Understanding Graphics File Formats

- Standard bitmap file formats
 - Graphic Interchange Format (.gif)
 - Joint Photographic Experts Group (.jpeg, .jpg)
 - Tagged Image File Format (.tiff, .tif)
 - Window Bitmap (.bmp)
- Standard vector file formats
 - Hewlett Packard Graphics Language (.hpgl)
 - Autocad (.dxf)

Understanding Graphics File Formats (cont.)

- Nonstandard graphics file formats
 - Targa (.tga)
 - Raster Transfer Language (.rtl)
 - Adobe Photoshop (.psd) and Illustrator (.ai)
 - Freehand (.fh9)
 - Scalable Vector Graphics (.svg)
 - Paintbrush (.pcx)
- Search the Web for software to manipulate unknown image formats

Understanding Data Compression

- Some image formats compress their data
 - GIF, JPEG, PNG
- Others, like BMP, do not compress their data
 - Use data compression tools for those formats
- Data compression
 - Coding of data from a larger to a smaller form
 - Types
 - Lossless compression and lossy compression

Lossless and Lossy Compression

- Lossless compression
 - Reduces file size without removing data
 - Based on Huffman or Lempel-Ziv-Welch coding
 - For redundant bits of data
 - Utilities: WinZip, PKZip, StuffIt, and FreeZip
- Lossy compression
 - Permanently discards bits of information
 - Vector quantization (VQ)
 - Determines what data to discard based on vectors in the graphics file
 - Utility: Lzip

Lossless and Lossy Compression



Lossless



Lossy



Locating and Recovering Graphics Files

- Operating system tools
 - Time consuming
 - Results are difficult to verify
- Computer forensics tools
 - Image headers
 - Compare them with good header samples
 - Use header information to create a baseline analysis
 - Reconstruct fragmented image files
 - Identify data patterns and modified headers

Identifying Graphics File Fragments

- Carving or salvaging
 - Recovering all file fragments
- Computer forensics tools
 - Carve from slack and free space
 - Help identify image files fragments and put them together

Repairing Damage Headers

- Use good header samples
- Each image file has a unique file header
 - JPEG: FF D8 FF E0 00 10
 - Most JPEG files also include JFIF string

Reconstructing File Fragments

- Locate the starting and ending clusters
 - For each fragmented group of clusters in the file
- Steps
 - Locate and export all clusters of the fragmented file
 - Determine the starting and ending cluster numbers for each fragmented group of clusters
 - Copy each fragmented group of clusters in their proper sequence to a recovery file
 - Rebuild the corrupted file's header to make it readable in a graphics viewer

Analysing Graphics File Headers

- Necessary when you find files your tools do not recognize
- Use hex editor such as WinHex
 - Record hexadecimal values on header
- Use good header samples

Tools for Viewing Images

- Use several viewers
 - ThumbsPlus
 - ACDSee
 - QuickView
 - IrfanView
- GUI forensics tools include image viewers
 - ProDiscover
 - EnCase
 - FTK
 - X-Ways Forensics
 - iLook

Understanding Steganography in Graphics Files

- Steganography hides information inside image files
 - Ancient technique
 - Can hide only certain amount of information
- Insertion
 - Hidden data is not displayed when viewing host file in its associated program
 - You need to analyze the data structure carefully
 - Example: Web page

Understanding Steganography in Graphics Files



No Message



Attack at midnight

Using Steganalysis Tools

- Detect variations of the graphic image
 - When applied correctly you cannot detect hidden data in most cases
- Methods
 - Compare suspect file to good or bad image versions
 - Mathematical calculations verify size and palette color
 - Compare hash values

Program Execution Artifact Investigations

- Identify when certain programs or applications were executed, how often were they used, and who accessed them
- Can help determine information about deleted and uninstalled programs
- Additionally proof of existing data in a location that is no longer available as well as the last time a program was launched

Summary

1. Cyber Incident chain of event
2. Timeline in cybercrime investigation
3. Extraction, recovery, and carving
4. hidden files, deleted files and unallocated space
5. Data reconstruction and fragments assembly
6. Anti-forensics techniques and Anti-anti-forensics
7. Program execution artifact investigations



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk