King Abdulaziz University Faculty of Computing and Information Technology Diploma in Cybersecurity CYB 260_Digital Forensics Learning Objectives: At the end of this chapter, you will be able to: o Determine what data to analyze in a digital forensics investigation o Explain tools used to validate data o Explain common data-hiding techniques CYB -260 2 Chapter 6: Evidence analysis Topics o Fundamentals of Forensic Data Acquisition o Understanding Storage Formats for Digital Evidence - Raw Format - Proprietary Formats o Advanced Forensic Format o Determining the Best Acquisition Method o Contingency Planning for Image Acquisitions o Strategies for Preparing Digital Evidence Image Files in Various Forensic Scenarios o Validating Data Acquisitions CYB -260 3 Determining What Data to Collect and Analyze Determining what data to collect and analyze in digital forensics varies based on the investigation type and data volume.CYB -260 10 Determining What Data to Collect and Analyze: Using Sleuth Kit to examine file system The Sleuth Kit(R) (TSK) (Fig.2) is a sophisticated toolkit consisting of both a library and command-line utilities aimed at assisting in the analysis of disk images for forensic purposes.This emphasizes the need for thorough evidence analysis by prosecution teams before trials, a principle applicable only in criminal cases in the United States CYB -260 4 Determining What Data to Collect and Analyze: Approaching Digital Forensics Cases Approaching digital forensics cases requires a customized plan based on the specific nature of each case.Autopsy Welcome Screen Determining What Data to Collect and Analyze: Using Autopsy to examine file system (cont..) Essential Features of Autopsy: o Event Timeline Visualization: Provides a sophisticated interface for chronological event analysis, complete with instructional videos.CYB -260 5 Determining What Data to Collect and Analyze: Approaching Digital Forensics Cases (cont..) For conducting digital forensics investigations, adhering to a set of standard practices is crucial for ensuring the integrity and reliability of the findings.Following these steps meticulously is vital for the successful and credible completion of a digital forensics investigation CYB -260 7 Determining What Data to Collect and Analyze: Refining and Modifying the Investigation Plan In digital forensics, specifically in civil, criminal, and private-sector investigations, the scope of data recovery varies.Determining What Data to Collect and Analyze: Using Sleuth Kit to examine file system (cont..) Essential Attributes of The Sleuth Kit (TSK): o In-depth Volume and File System Examination: At its core, TSK excels in detailed scrutiny of volume and file system structures.CYB -260 19 Addressing Data-Hiding Techniques Hiding Files by Using the OS - Hiding Partitions CYB -260 20 Data-Hiding Technique Method Detection and Analysis Changing File Extensions Altering the file extension (e.g., from .xlsx to .jpg) to mask the true nature of the file.o Broad System Support: TSK is compatible with a range of partition types and file systems, including but not limited to DOS, BSD, and Mac partitions, Sun slices, GPT disks, and file systems like NTFS, FAT, ExFAT, UFS 1/2, and ext2/3/4.With its adaptable plug-in framework, TSK offers the flexibility to add extra modules for in-depth analysis of file contents and to facilitate the creation of automated forensic systems.This tool's capabilities are critical for precise and efficient forensic analysis CYB -260 14 Validating Forensic Data: Using Hash Values to Discriminate Data In the realm of digital forensics, using hash values to discriminate data is a critical method for identifying specific types of files within evidence drives or image files.CYB -260 8 Determining What Data to Collect and Analyze: Using Autopsy to examine file system As mentioned in chapter 4, autopsy (Fig.1) is a comprehensive digital forensics

platform used for investigating activities on computers and other digital devices.CYB –260 13 Validating Forensic Data: Validating with Hexadecimal Editors In digital forensics, validating forensic data is a crucial process, especially when dealing with files that may have been altered or renamed to appear innocuous.Application in Forensics: These tools and databases are crucial in forensic investigations for efficiently discriminating between irrelevant data and potential evidence, especially in cases involving large volumes of digital data.Built-in Validation Features: Commercial digital forensics tools come equipped with features that validate image acquisitions by generating hash values, particularly MD5 and SHA-2.Methods may include setting up surveillance cameras, using keyloggers for capturing keystrokes, engaging network administrators for monitoring internet activities, and remotely acquiring the employee's drive data.Data Acquisition Record: Document the method used for data acquisition from the suspect drive, including the creation of a bit-stream image and the tool used, ensuring it creates an MD5 or SHA-3 hash for validation.o Forensic Image Requirement: For analysis, TSK necessitates a forensic image, usually in formats like .dd or .E01, which can be created with tools such as AccessData FTK Imager.o Use of Hashing in Forensics Tools: Forensic tools commonly incorporate hashing functions to create unique digital signatures for image files, facilitating the validation of data integrity.These editors offer specific features like hashing individual files or sectors, which is essential for identifying and validating particular files, such as known contraband images.Key Points: o Advanced Features of Hexadecimal Editors: Unlike standard forensic tools, advanced hexadecimal editors can hash specific files or sectors, providing a more targeted approach to data validation.NIST National Software Reference Library (NSRL): Maintained by the National Institute of Standards and Technology, NSRL provides a comprehensive database of file hash values.The following table (Table 1) categorizes these data-hiding techniques, describes the methods used to hide the data, and outlines the forensic approaches employed for their detection and analysis.This creep occurs when investigations expand unexpectedly, necessitating documentation of additional investigative requests.For criminal cases, coordination with ISPs and email services is necessary, noting that many organizations don't retain emails for extended periods.File and Folder Listing: Use forensic tools like Autopsy to generate lists of all files and folders on the suspect's drive in various formats.Password-Protected Files: Attempt to recover contents from all relevant password-protected files using tools like OSForensics Password Recovery and Decryption, AccessData PRTK, or Passware Kit Enterprise.It functions as a graphical interface to The Sleuth Kit(R) (TSK) and incorporates various other digital forensics tools.Utilized by professionals in law enforcement, military, and corporate sectors, Autopsy is versatile, supporting tasks from computer investigations to photo recovery from camera memory cards.This toolkit is not only integral to larger digital forensics applications but is also efficient for direct evidence retrieval in its standalone form.o Expandable Design: The tool's architecture allows for the integration of additional modules, enhancing its analytical capabilities.o Versatile Disk Image Analysis: It is equipped to handle various disk image formats, such as raw (dd), Expert Witness (EnCase), and AFF.o Role of Hexadecimal Editors: Advanced hexadecimal editors are often employed to overcome the limitations of standard forensic tools, offering a more thorough means of ensuring data integrity.o Efficiency of Hexadecimal Editors: Acquiring hash values using a full-featured hexadecimal editor can be faster and more efficient compared to traditional digital

forensics tools.Tools like AccessData's Known File Filter (KFF) and databases like the NIST National Software Reference Library (NSRL) are instrumental in this process.AccessData's Known File Filter (KFF): This is a hashing database exclusive to the Forensic Toolkit (FTK) by AccessData.It serves two primary functions: o Filtering Known Program Files: KFF filters out common program files (e.g., winword.exe) to focus on more relevant data.Integration with Other Forensic Tools: Digital forensic tools like X-Ways Forensics, OSForensics, and Forensic Explorer can import the NSRL database.Handling Raw Data Acquisitions: For raw data acquisitions like dd images, which can't store the original image hash, forensic tools often generate a separate text file detailing the acquisition and its hash value.These techniques range from altering file extensions and utilizing hidden file attributes to more complex methods like bit-shifting, encryption, and password protection.o Analysis of Multimedia Metadata: Retrieves detailed metadata from images and video files, offering insights into multimedia content.o Clear Licensing Details: The toolkit provides explicit licensing information, guiding users on the legalities of its usage.The validation process typically includes the use of hashing techniques to verify that the data collected remains unchanged from its original state.o Limitations of Forensics Tools: Despite their utility, these tools may have limitations in their hashing capabilities, necessitating the use of more advanced methods.Advanced hexadecimal editors play a vital role in this process due to their capabilities that extend beyond those found in standard digital forensics tools.It's useful for validating specific files or sectors, verifying data integrity, and ensuring accuracy in sparse acquisition scenarios.Regular Updates of KFF: AccessData periodically updates the KFF with new hash values, ensuring the database remains current and effective in identifying known illegal files.CYB -260 16 Validating Forensic Data: Validating with Digital Forensics Tools Validating digital evidence through commercial digital forensics tools is an essential process in ensuring the integrity of image acquisitions.These tools typically generate MD5 and SHA-2 hash values for data within image files, facilitating the verification of data authenticity.A mismatch in hash values indicates potential corruption of digital evidence, prompting the need for reacquisition or careful reporting.CYB -260 18 Addressing Data-Hiding Techniques Hiding Files by Using the OS - Hiding Partitions Data hiding is a technique used to conceal information within a digital environment.Understanding these methods is crucial for digital forensic investigators, as identifying and analyzing hidden data can be pivotal in an investigation.Investigators should check for unexplained gaps in disk space using forensic tools or hex editors to find hidden partitions.Requires advanced analysis with forensic tools capable of interpreting the binary data and recognizing patterns.Forensic analysis may detect encrypted files, but decrypting them requires the encryption key or password.Each case type demands a distinct set of strategies and tools, underscoring the importance of tailoring the investigation approach to the specific circumstances and legal boundaries of each case.CYB -260 6 Determining What Data to Collect and Analyze: Approaching Digital Forensics Cases (cont..) 6.Legal cases are often guided by search warrants or subpoenas, defining the extent of permissible data retrieval.o Internet Usage Extraction: Gathers internet usage details including browsing history and saved web data from major browsers like Firefox and Chrome.o Deleted File Recovery: Uses PhotoRec to salvage files from areas of storage not actively in use, enhancing data recovery efforts.Additional Elements of TSK: o Accessibility for Download: Users

can download TSK for their investigative needs.o Comprehensive Resources: TSK offers detailed documentation and a record of its evolution and updates.CYB –260 12 Validating Forensic Data In digital forensics, the validation of forensic data is a pivotal process.Key Points: o Essentiality of Data Integrity: The core of digital evidence validation lies in ensuring the unaltered state of the data from the point of collection to its presentation in legal settings.o Importance in Forensic Investigations: Mastery of these tools is crucial for forensic analysts, particularly when searching for specific files that might be disguised under different names.o Example of a Hexadecimal Editor – WinHex: WinHex is an example of such a tool, offering multiple hashing algorithms like MD5 and SHA–2.o Identifying Illegal Files: The database contains hash values of known illegal files, such as child pornography, enabling it to compare these values with files in the evidence to identify suspicious content.Autopsy's E01 Verifier: Similar to FTK Imager, Autopsy includes a feature for verifying Expert Witness image files.Image File Verification Process: When an image file is opened in a forensics tool, another hash (MD5 or SHA–2) is computed for the copied data.Forensic tools verify file headers against extensions; discrepancies are flagged for further analysis.While forensic tools can identify password–protected files, accessing the content requires the password or bypass methods.In the private sector, investigations might focus on specific items like emails for company policy violations, streamlining the process.However, in cases involving or anticipating litigation, extensive data recovery might be requested, leading to extensive work and possible scope creep.In criminal cases, detailed evidence examination is crucial to prepare for defense strategies, as defense teams have full discovery rights and might use newly found evidence to their advantage.This planning involves defining the investigation's goals, scope, required materials, and tasks.E–mail Harassment Case: This might involve simple tasks like accessing network logs and e–mail server backups to find specific messages.CYB –260 15 Validating Forensic Data: Using Hash Values to Discriminate Data (cont..) 2.2.2.3.4.5.7.8.9.10.3.4.5.2.3.5.6.