2008

Draft Forensic Common Body of Knowledge

SANS INSTITUTE

Rob Lee – rlee@sans.org

11/2008

SANS Forensic Common Body of Knowledge

Who Can Investigate and Investigative Process Laws

The candidate will demonstrate an understanding of the key parties involved in an investigation and the investigative process.

Fairway Markers

- Understanding the difference between internal and external investigations and how different rules apply.
- Discuss items that should be in place to protect you and your organization during an investigation (job description, approval of case by manager, approval of data examination by manager, get everything in writing)
- Discuss the ramifications of involving law enforcement in an investigation
- Discuss the ramifications of an incident that multiple countries
- Discuss following agency/employer policy and procedures
- Understand and discuss digital forensic ethical standards
- Discuss lines of communication between the requestor, examiner and analyst by which information is gathered, processed, disseminated.

Evidence Acquisition/Analysis/Preservation Laws and Guidelines

The candidate will demonstrate an understanding of how to collect and preserve the state of the data by maintaining chain of custody and following evidence acquisition/analysis/preservation guidelines.

Fairway Markers

- Discuss the major goals associated with acquiring data
- Discuss legal authority to allow for data acquisition
- Discuss the differences between stored and real time data
- Discuss evidence/information you can share with third parties and law enforcement
- Demonstrate clear understanding of legal authority necessary to collect data
- Discuss tool validation and process
- Discuss secure evidence storage procedures and guidelines

U.S. Laws Investigators Should Know

The candidate will demonstrate an understanding of U.S. civil and criminal laws related to forensic investigations.

Fairway Markers

- Criminal and Civil Law Procedures –Understanding of the laws and procedures related to evidence, search authority and scope.
- Discuss U.S. Computer Fraud and Abuse Act
- Civil Privacy Laws - A basic understanding of laws, policies, and procedures governing information classification such as proprietary, personal, and private information and government classified data as specified in federal laws such as HIPAA, GLB, FERPA, Government Classified info, ECPA, Tax Return Info, etc.
- Discuss Wiretap Act and Pen Register Trap and Trace Laws
- Discuss U.S. Electronic Communication Privacy Act

E.U. Laws Investigators Should Know

The candidate will demonstrate an understanding of E.U. civil and criminal laws related to forensic investigations.

Fairway Markers

- Criminal and Civil Law Procedures –Understanding of the laws and procedures related to evidence, search authority and scope.
- Discuss several legal entities involved in international and E.U. crime investigations
- Discuss E.U. Data Protection Directive
- Discuss E.U. Data Retention Law
- Discuss E.U. Information System Attacks Decision

Presenting Data

The candidate will demonstrate an understanding of the guidelines associated with presenting acquired evidence and analysis in court.

Fairway Markers

- Discuss evidence admissibility (Authenticity and Relevancy)
- Discuss probative value vs. prejudicial effect of evidence
- Understanding the basic rules of evidence
- Importance of proving the integrity of the data
- Discuss what is defined as “Best Evidence”
- Discuss the difference between lay and expert witnesses
- Discuss the importance of the Daubert and Frye tests in court

Forensic Reports and Testimony

The candidate will demonstrate an understanding of the guidelines associated with the fundamentals of testimony and report writing including a description the scientific process utilized and the legal utility of forensic investigative reports

Fairway Markers

- Discuss the fundamentals of report writing
- Discuss the fundamentals of legal testimony
- Discuss need for report to address scientific process, audience, and legal utility
- Write in a manner in which technical information is presented to a non-technical audience
- Understand how to document work so it is repeatable
- Discuss scientific methods that show clear conclusions based in factual evidence

Computer Forensics Core

The candidate will demonstrate a fundamental understanding of the procedures and core concepts utilized in the investigative process, the scientific process, crime scene/incident examination, and the importance of documentation, reporting, and presentation.

Fairway Markers

- The major forensic principles and be able to apply them
- The importance of evidence integrity and how to ensure it
- Discuss the idea of minimizing data loss and how to avoid data spoliation
- Discuss the concept of evidence volatility and how it affects an investigation
- What a disk image is and its relevance to an investigation
- Forensic Methodology/Incident Response process and why each step is important.
- Documentation, reporting and presentation

Forensic Investigation

The candidate will demonstrate an understanding of the computer forensics investigation methodology and investigative mindset.

Fairway Markers

- Identify the major phases of the forensic methodology
- Discuss the importance of the investigative mindset
- Discuss the importance of proper evidence collection
- Discuss the importance of case and file system timelines and how they are used
- Discuss the importance of string/byte searching and how they can be used to identify existing and deleted data
- What media analysis and artifact analysis is and how data from them is useful
- Discuss the steps that are required to find and recover deleted or unallocated data
- The purpose and importance of reporting

File System Essentials

The candidate will be able to demonstrate an understanding of the fundamental concepts associated with hard drives and file systems including partitioning, file clusters/blocks, metadata, and files.

Fairway Markers

- Understand and describe the file system layers
- Understand the difference between a physical and logical disks, and why partitioning is important
- Understand the components of the master boot record and partition tables
- Understand the difference between the MBR Partition Table and GUID Partition Tables
- Understand the elements of a partition entry and their significance
- Understand the key elements of the data layer (variable size, addressable, allocation status)
- Discuss the difference between data layer allocated, unallocated, and slack space
- Discuss the key elements of the metadata layer (metadata address, pointer to data layer, timestamps, file attributes, metadata allocation status)
- Discuss the difference between metadata layer allocation and data layer allocation
- Discuss the key elements of the file name layer (directory files/hierarchy, filenames)

Linux/Unix File System Basics

The candidate will demonstrate an understanding of the basics of Linux/Unix file systems including

Fairway Markers

- What is the superblock and why is it important
- What are block groups and how are they organized
- What blocks are and how they are used
- What are the timestamps in Linux/Unix metadata and what do they mean
- Discuss the key elements of Linux/Unix inode (no filename, 12 direct blocks, mactimes, link count, file type, indirect block pointers)
- Discuss when indirect blocks are utilized and how they work
- Discuss different types and uses of Linux/Unix file types
- Describe what happens when data is “deleted” from a Linux/Unix File system

Windows FAT File System Basics

The candidate will demonstrate an understanding of the basics of Windows FAT file systems.

Fairway Markers

- Discuss the major characteristics, sector/cluster layout, and the limitations of the various types of FAT file systems (FAT12/16/32 and exFAT/FAT64)
- What a cluster is and how it is used in a FAT file system
- What is the FAT boot sector and what key data is stored in it
- Discuss structure and function of the File Allocation Table
- What is the root directory area in FAT12/16 file systems and why is it used
- Discuss the key elements of a FAT Directory short and long entries
- What are the timestamps in FAT metadata and what do they mean
- Discuss the function and importance of cluster chains
- Describe what happens when data is “deleted” from the FAT file system

Windows NTFS File System Basics

The candidate will demonstrate an understanding of the basics of Windows NTFS file systems.

Fairway Markers

- Discuss major characteristics of the NTFS file system
- What is the NTFS boot sector and what key data is stored in it
- What a cluster is and how it is used in an NTFS file system
- Discuss structure and function of the Master File Table
- Discuss MFT the core and optional NTFA metadata attributes (e.g. $Std_Info, $Filename, $Data)
- What are the timestamps in NTFS metadata and what do they mean
- Discuss purpose of the NTFS volume metafiles
- Describe what happens when data is “deleted” from the NTFS file system

Key Forensic Acquisition/Analysis Concepts

The candidate will demonstrate an understanding of the methods and techniques utilized to acquire/analyze evidence, maintain integrity, and conduct a forensics investigation.

Fairway Markers

- Why it is important to use the right forensic tools
- Discuss different types of toolkits and when they are used
- Discuss key windows and Linux evidence gathering tools conceptually and why they are needed (Memory, Process/Network data collection, evidence integrity, imaging)
- Why do you need an evidence acquisition kit and what are the components?
- Essential information to collect at the start of an investigation

Volatile Evidence Gathering and Analysis

The candidate will demonstrate an understanding of the tools used to collect volatile evidence and system memory from a computer system

Fairway Markers

- Discuss what type of data is in system memory and why it is useful to an investigation
- Discuss how to obtain system memory for Windows/Linux and when it should be accomplished
- Discuss memory analysis and interpretation techniques and how they could be used to help an investigation
- Discuss how to obtain and interpret process and network information useful to an investigation
- What volatile information should be collected at the start of an investigation
- Discuss the importance of event log collection and analysis

Evidence integrity

The candidate will demonstrate an understanding of the methods and procedures utilized to create and maintain evidence integrity

Fairway Markers

- Discuss why cryptographic hashes are used and why they prove integrity
- Describe the key characteristics of the MD5 algorithm and how it is used to prove evidence integrity
- Describe the key characteristics of the SHA-1 algorithm and how it is used to prove evidence integrity

Forensic Evidence Acquisition and Imaging

The candidate will demonstrate an understanding of the methods to use for collecting computer evidence from a powered-on or powered-off computer system or hard drive.

Fairway Markers

- Key issues surrounding the creation of system images (bit-by-bit, different rules for live vs. dead, etc.)
- The difference between a physical and logical image and when to use each
- Ways and differences between the major ways to acquire an image (Boot disk such as HELIX, Hardware based, Live Acquisition)
- Discuss why write blockers are useful and when they should be utilized
- Discuss what a host protected area of a disk is and why it should be checked for
- Discuss filling out a chain of custody form and what information is required
- How to use dd and its kin to acquire an image
- Discuss how to perform a secure wipe
- How and why you would extract logical partition information
- How to mount images maintaining integrity after you have acquired them

File System Timeline Analysis

The candidate will demonstrate an understanding of creating and analyzing a file system timeline through examining the details of the file system’s time-stamps and how temporal data is useful in an investigation.

Fairway Markers

- Discuss the benefits to analyzing a timeline and how it is useful to a case
- Discuss the sensitivity of data in a timeline and how it could affect the analysis
- Discuss the difference in timeline data between various file systems
- Demonstrate the understanding of reading the context surrounding examining timeline analysis (context, read line by line)
- Discuss how timelines are created and the steps one must follow to generate one
- Discuss the difference and significance between unallocated metadata, deleted files, and allocated files in the analysis of a timeline

Forensic Analysis Key Methods

The candidate will demonstrate an understanding of key evidence analysis methods/concepts and how they are used during a forensics investigation

Fairway Markers

- Discuss the importance of file headers and footers
- What are some tools that can categorize data based on file headers/data (file)
- Discuss the significance of creating an ASCII and UNICODE strings list of an image and how to generate them
- Discuss why the byte offset is needed in a strings output file (location)
- How a "dirty word list" can be used during a forensics investigation
- Discuss how to search for items in the dirty word list in the strings files and how to identify the data structure that contains a "hit"

File System and Data Layer Examination

The candidate will demonstrate an understanding of how to analyze and recover evidence from the file system and data layer on major file systems.

Fairway Markers

- Discuss methods to examine the key details of a file system partition and what critical information is needed by forensic tools
- How to use data layer tools to extract information from data units on an image
- How to work with unallocated or slack space on an image
- How to extract files from an image based on the file headers
- How to determine the location of data in a forensic image

Metadata Layer Examination

The candidate will demonstrate an understanding of how to analyze and recover evidence via metadata on major file systems.

Fairway Markers

- How to locate specific metadata structures of interest in an investigation
- How to obtain and use attributes about a given metadata structure
- How to extract the data associated with a specific metadata structure
- Discuss methods of listing the metadata structures associated with a forensic image
- How to identify specific file names and directories in a forensic image
- How to determine the file name associated with a specific metadata unit

File Name Layer

The candidate will demonstrate an understanding of the tools needed to recover and analyze evidence via the file name layer on major file systems.

Fairway Markers

- Discuss ways to identify the filename given a metadata address
- Discuss how directory files are utilized to store filenames in a hierarchy
- Show the importance of directory and file name and location is important contextually to a case

File Sorting and Hash Comparisons

The candidate will demonstrate an understanding of how to use MD5, SHA-1, or fuzzy hashes to identify known good and bad files and how to sort files based on content type

- Discuss why file sorting based on content is useful to an investigation
- Demonstrate how the process of sorting files based on content could be accomplished
- What a hash database is and how it can be used during an investigation
- Different hash database resources available to an investigator
- The importance of known good hashes for a system
- Methods for creating known good and known bad hash databases
- What fuzzy hashing is and how it can be used in an investigation
- Methods used to conduct fuzzy hashing

Windows Response and Volatile Evidence Collection

The candidate will demonstrate an understanding of the tools used to collect volatile evidence and system memory from a Windows computer system and some of the core methods used to respond to a Windows based investigation.

Fairway Markers

- Demonstrate methods to collect windows critical data
- Discuss event log collection and analysis
- How to gather and interpret critical system information
- How to recover system passwords

Key Windows File System Analysis Concepts

The candidate will demonstrate an understanding of how to collect evidence and analyze critical Windows concepts for a forensic investigation including, but not limited to, volume metadata files, restore points, and volume shadow copy.

Fairway Markers

- Demonstrate knowledge of how to examine windows images using a way to mount and examine the files of a windows image
- Discuss how to detect known malware once an image is mounted
- The importance of knowing where to look for evidence during an investigation
- Discuss how XP Restoration Point and how to utilize restore point information in an investigation
- Discuss how VISTA Volume Snapshot Service (Shadow Copy) works and how to utilize Shadow Copy information in an investigation

Windows Registry Analysis

The candidate will demonstrate an understanding of how to collect evidence and analyze Windows registry for a forensic investigation.

Fairway Markers

- Discuss what a registry hive is and where the various hives are located on various windows machines
- Discuss how to create a timeline of last write times in the registry
- Collecting evidence of user activity via the registry
- Discuss and analyze evidence of external device evidence in the registry
- Analyzing evidence of application execution
- Discuss and analyze evidence on system configuration (Users, settings, configuration, software)

Windows Internal File Metadata

The candidate will demonstrate an understanding of how to collect evidence and analyze Windows files that contain key metadata or contain evidence for a forensic investigation.

Fairway Markers

- Discuss and analyze from EXIF data from media files (pictures, movies, music)
- Discuss and analyze evidence from link (LNK) files
- Discuss and analyze evidence from Microsoft Office documents
- Discuss and analyze evidence from thumbnail files
- Analyzing email evidence
- Analyzing evidence from the XP and VISTA Recycle Bin

Application Footprinting and Software Forensics

The candidate will demonstrate and understanding of the tools and methods used to identify the location and critical evidence contained in an application or software's key files, configuration files/parameters, and registry keys/settings.

Fairway Markers

- What application foot printing is and how it is useful in an investigation
- Demonstrate understanding to show how both file and configuration residue from applications can be examined using timeline analysis,
- Understand how to perform registry analysis of applications and artifacts
- Demonstrate understanding to show how both file and configuration residue from applications can be examined using memory analysis

Automated GUI Based Forensic Toolkits

The candidate will be able to discuss the Automated GUI Based Forensic Toolkits such as (Autopsy, Encase, or FTK) and their capabilities and drawbacks during a forensic investigation.

Fairway Markers

- What Automated GUI Based Forensic Toolkits are used for; what makes them so useful
- How are different images imported into a GUI tool
- Utilize GUI Toolkit to follow forensic methodology to perform timeline analysis, media/artifact analysis, string/byte searching, and file based extraction
- Identifying and recovering deleted information
- Searching for keywords, dates, and other relevant information