DIGITAL FORENSICS CERTIFICATION BOARD
Excellence - Integrity - Objectivity

DFCP/DFCA – KSA Domains

The following outline of Knowledge, Skills, and Abilities (KSA's) comprises a listing of KSA domain topics to be mastered in order to achieve the Digital Forensics Certified Practitioner (DFCP) or Digital Forensics Certified Associate (DFCA). Due to the nature of digital forensics, the associated body of knowledge for this profession is extensive. Candidates are not required to have an expert knowledge in all KSA topics but should have a general exposure to all of these areas.

1.0 Legal

1.1 Concepts

1.1.1 Explain the difference between criminal and civil matters
1.1.2 Describe the difference between misdemeanor and felony crimes
1.1.3 The concepts of the *actus reus* (or the guilty act) and the *mens rea* (the guilty mind) in criminal matters
1.1.4 Demonstrate knowledge of the privacy issues that are involved in investigations
1.1.5 Demonstrate knowledge of how the Fourth Amendment impacts digital forensics:
    1.1.5.1 Government agent v. private citizen
1.1.6 Knowledge of Fourth Amendment exceptions (warrantless searches):
    1.1.6.1 Consent
    1.1.6.2 Plain view
    1.1.6.3 Exigent circumstances
    1.1.6.4 Incident to an arrest
    1.1.6.5 Inventory search
1.1.7 Define digital evidence
1.1.8 Explain the concept of Reasonable Expectation of Privacy
1.1.9 Explain the importance of the Chain of Custody
1.1.10 Understand issues related to admissibility of evidence
    1.1.10.1 Business Records exception
    1.1.10.2 Best evidence
1.1.11 Be familiar with:
    1.1.11.1 Federal Rules of Civil Procedure related to electronically stored information
    1.1.11.2 Sedona principles
    1.1.11.3 Civil Discovery
    1.1.11.4 8 Factor Rowe Test for discovery costs
    1.1.11.5 Data preservation orders
    1.1.11.6 Federal Rules of Evidence
    1.1.11.7 Various regulatory acts
        1.1.11.7.1 SOX
        1.1.11.7.2 GLBA
        1.1.11.7.3 HIPAA

1.1.11.7.4 FERPA

1.1.12 Demonstrate knowledge of Internet Laws and Statutes (and exceptions):

1.1.12.1 The USA Patriot Act of 2001

1.1.12.2 Electronic Communications Privacy Act

1.1.12.2.1 Wiretap

1.1.12.2.2 Stored Communications Act

1.1.12.3 Computer Fraud & Abuse Act

1.1.12.4 Economic Espionage Act

1.1.12.5 18 USC §1030 etc.

1.1.12.6 CAN-SPAM Act

1.1.12.7 Child Pornography Protection Act (CPPA)

1.1.12.8 Mail & Wire Fraud Act

1.1.12.9 DMCA

1.1.13 Demonstrate knowledge of Intellectual Property Rights:

1.1.13.1 Patent

1.1.13.2 Trademark

1.1.13.3 Copyright

1.1.13.4 Trade Secret

1.1.13.5 Licensing

1.1.14 Demonstrate knowledge of relevant case laws

1.1.14.1 Criminal

1.1.14.1.1 Arizona v. Hicks, 480 U.S. 321, 325 (1987).

1.1.14.1.2 United States v. Jacobsen, 466 U.S. 109, 113–14 (1984).

1.1.14.1.3 Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (1994).

1.1.14.1.4 Kyllo v. United States, 533 U.S. 27, 32–33 (2001)

1.1.14.1.5 United States v. Runyan 275 F.3d 449 (5th Cir. 2001)

1.1.14.2 Civil

1.1.14.2.1 Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 312 (S.D.N.Y. 2003/04) (I-V)

1.1.15 Demonstrate knowledge of the laws concerning Cyber Stalking

1.1.16 Understand what steps to follow when encountering evidence of criminal activity or violations of corporate policy outside the original scope of authority to capture digital evidence.

1.1.17 Understand the distinctions that occurs where evidential material is:

1.1.17.1 Highly offensive but not unlawful

1.1.17.2 A breach of procedure, policy etc

1.1.17.3 Inappropriate only,

1.1.17.4 Criminally prohibited and restricted.

1.1.18 Understand the processes involved with investigating sexual harassment incidents.

1.1.19 Understand the legal issues and requirements when investigating Child Pornography.

1.1.20 Demonstrate knowledge of the basic concepts that are associated with Computer Facilitated Crimes:

1.1.20.1 Modes of Attacks

1.1.20.2 Examples of Cyber Crime

1.1.20.2.1 Hacking

1.1.20.2.2 Phishing

1.1.20.2.3 Cyber Stalking

1.1.20.2.4 Identity Theft

1.1.20.2.5 Denial of Service

1.1.20.2.6 Child Pornography

1.1.21 Discuss the importance and judicial considerations for scientific Expert Witness Testimony

1.1.21.1 Frye

1.1.21.2 FRE 702

1.1.21.3 Daubert

1.1.21.4 Kuhmo

1.1.21.5 Joiner

1.2 Process

1.2.1 Understand Search and Seizure

1.2.1.1 What is the planning for search and seizing?

1.2.1.2 How to start initial search of the scene?

1.2.2 Explain the appropriate use of :

1.2.2.1 Subpoenas

1.2.2.2 Court Orders

1.2.2.3 Warrants

1.2.2.4 2703 Orders

2.0 Ethics

2.1 The digital forensic examiner needs to demonstrate an understanding of the fundamentals of Professional Ethics. This includes a knowledge and understanding of:

2.1.1 The Mission, Vision and Values Statements

2.1.1.1 The Mission Statement

2.1.1.2 The Vision Statements

2.1.1.3 A Statement of Values

2.1.2 Demonstrate a fundamental understanding of the major legal requirements and ethical standards related to the practice of digital forensics:

2.1.2.1 Legal Authority

2.1.2.2 Ethics

2.1.2.3 Professional Development

2.1.3 Understanding the need for Ethical Policy as a Professional

2.1.4 Human Resource (HR) Issues

2.1.5 Compliance with legal requirements

2.1.6 Familiarity with the AAFS code of ethics

2.1.7 Roles and duties of expert witnesses

3.0 Storage Media

3.1 Acquisition

3.1.1 Conduct digital evidence captures in accordance with digital evidence community standards.

3.1.2 Techniques

3.1.2.1 Demonstrate knowledge of various evidence file formats and how hashing functions are used to compare and verify data.

3.1.2.2 Gather information about the digital evidence to be captured and prepare a plan and assemble the necessary equipment, storage media and personnel needed to complete the capture.

3.1.2.3 Execute safe handling to preserve other physical evidence located near, on or inside items being examined for recovery of digital evidence.

3.1.2.4 Execute appropriate “chain of custody” documentation and storage procedures for evidence coming into your possession.

3.1.3 Process

3.1.3.1 Decide appropriate acquisition method for digital evidence encountered in the field, including when to seize equipment for off-site imaging. Recognize factors, which affect likelihood to successfully complete acquisition, including on-site dangers, available time, required equipment, storage media and personnel.

3.1.3.2 Take notes and photographs to document activities performed to capture digital evidence, identify the evidence, and document the state of the evidence including necessary or accidental changes to data and details, such as system date and time, operating status (on/off), configuration details, capacity of storage devices, serial numbers and existing damage.

3.1.3.3 Ensure unobtrusive method of marking physical media is used to identify examiner and date of examination.

3.1.4 Concepts

3.1.4.1 Understand the difference between a physical disk and a partition.

3.1.4.2 Understand the reasons for the sterilization (wiping) of digital media for storage.

3.1.4.3 Understand the difference between a “bit for bit” image and logical copy.

3.1.4.4 Understand a logical image.

3.1.4.5 Understand network topology and network operating systems sufficient to acquire data from computers and storage devices on the network while minimizing or eliminating changes to the data.

3.1.4.6 Understand computer assembly and repair techniques sufficient to add and remove system components as needed to acquire data and prevent damage from electrostatic discharge.

3.1.4.7 Understand the consequences to data in volatile memory systems when power is removed from devices or systems.

3.1.4.8 Understand the boot process and interaction of computer hardware components of a standalone computer system sufficient to acquire data from the systems’ storage devices without changing the data.

3.1.4.9 Understand write blocking hardware and software, and how these items accomplish the protection of original digital objects.

3.1.4.10 Understand the computer bus sufficiently enough to identify the various types of connectors (e.g., SATA, PCI, ISA).

3.1.4.11 Understand factors that may require the technician to alter his/her acquisition plan (e.g., using TDM to acquire an iMac or having to acquire a live machine due to the presence of a fingerprint reader on the computer).

3.1.4.12 Understand the limitations associated with long-term storage of evidence on various types of storage media.

3.2 Examination/Analysis

3.2.1 Techniques

3.2.1.1 Examine common program and application default storage locations to determine whether data was stored in a default or alternate location.

3.2.1.2 Extract file system information to reveal characteristics such as directory structure, file attributes, file names, date and time stamps, file size, and file location.

3.2.1.3 Examine digital evidence for presence of common programs used to hide, encrypt, protect with passwords, corrupt, eliminate or restrict access to relevant information.

3.2.1.4 Correlate file headers to the corresponding file extensions to identify mismatches.

3.2.1.5 Examine artifacts related to use of Internet browsers such as Internet Explorer, Firefox/Mozilla/Netscape , and America Online to locate browser history, typed URLs, Internet cookies, auto-complete data, stored usernames and passwords, download activity, user profiles, temporary internet files (Internet cache), and web based mail.

3.2.1.6 Examine artifacts related to use of peer to peer file sharing technologies such as Kazaa, Limewire, Gnutella and BitTorrent for transaction information and shared directories.

3.2.1.7 Examine relationships between files for evidence of source or ownership (data provenance). Examples include correlating Internet history to cache files and e-mail files to e-mail attachments.

3.2.1.8 Examine operating system configuration, file contents and metadata for ownership information.

3.2.1.9 Use timeframe analysis to determine when events occurred on a computer system, by reviewing time and date stamps contained in the file system or by reviewing system and application logs to link files of interest to the timeframes relevant to the investigation. Consider differences in the individual’s computer date and time as reported in the BIOS.

3.2.2 Process

3.2.2.1 Maintain a case file in accordance with agency or corporate policies which documents the details of the request, authority to perform examination, associated correspondence, irregularities encountered and chain of custody.

3.2.2.2 Take notes and photographs of the examination process according to agency or corporate guidelines including date, times and descriptions of actions taken detailed enough to allow complete duplication of actions.

3.2.2.3 Provide adequate communications between requestor, examiner and appropriate third parties to refine or revise details of the requested examination, and address priority matters, due to investigative priorities or unanticipated findings.

3.2.2.4 Review system and application logs that may be present, such as error logs, installation logs, connection logs, security logs, etc.

3.2.2.5 Report results of forensic examination according to agency or corporate guidelines including identification of the reporting agency, case identifier or submission number, case investigator, identity of the submitter, date of receipt, date of report, descriptive list of items submitted for examination, including serial number, make, and model; identity and signature of the examiner, description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files, and results/conclusions.

3.2.3 <u>Concepts</u>

3.2.3.1 Understand how files are deleted and location and format of deleted data sufficient to locate and recover deleted files.

3.2.3.2 Understand potential for hidden data in locations such as Host Protected Area (HPA) of hard drives, Alternate Data Streams (ADS) in files on NTFS partitions, encrypted volumes and hidden partitions.

3.2.3.3 Understand how the presence of malware like viruses, Trojans, worms, bots, keystroke loggers can affect interpretation of examination results.

3.2.3.4 Understand hardware conventions such as MAC address, serial numbers, and jumper settings that would uniquely identify a piece of hardware.

3.2.3.5 Understand data reduction methods used to focus the examination by means of key word, date time, file type, file signatures and other criterion searches.

3.2.3.6 Understand common communication applications, such as email and chat programs, including methods of storage, metadata, and relevant protocols and transactions sufficient to locate communications and related information or identify service providers and account details for those programs that do not store information on the user’s computer.

3.2.3.7 Understand methods of transferring data securely between parties (e.g., FTP, encrypting data on drive being shipped via FedEx).

3.2.3.8 Understand the difference between volatile and non-volatile memory.

3.2.3.9 Understand the difference between low-level and high-level disk formatting.

4.0 Mobile and Embedded Devices

4.1 <u>Acquisition</u>

4.1.1 ***Techniques***

4.1.1.1 Demonstrate knowledge of different types of mobile devices (e.g., mobile phones, PDAs, cameras, GPS devices)
4.1.1.2 Present a standard step-by-step procedure for acquiring mobile devices in a forensically proper manner, including proper handling of the devices
4.1.1.3 Execute proper chain-of-custody mechanisms over mobile devices
4.1.1.4 Explain the different types of information that one would expect to find on a given mobile device

4.1.2 ***Process***

4.1.2.1 Describe mechanisms with which to isolate a mobile device from the wireless network
4.1.2.2 Describe means with which a mobile phone can be acquired physically and/or logically
4.1.2.3 Describe the ways in which a SIM card can be acquired
4.1.2.4 Describe the ways in which a memory expansion can be imaged
4.1.2.5 Describe hardware, software, and other means of acquiring mobile device information
4.1.2.6 Ensure that acquisition is within the scope of any court order, permission, or other authority to act

4.1.3 ***Concepts***

4.1.3.1 Differentiate between different mobile phone technologies (e.g., TDMA, CDMA, GSM, iDEN)
4.1.3.2 Explain the process of a mobile telephone call setup
4.1.3.3 Describe the elements of different types of mobile devices (e.g., memory expansion cards, SIM cards, onboard memory)
4.1.3.4 Describe the various protocols used for mobile phone voice calls, text messaging, and Internet data transfer
4.1.3.5 Describe some fundamental differences between forensic acquisition of computer memory and storage devices (including memory expansion cards) and that of mobile devices
4.1.3.6 Explain the role of PINs and PUKs and how they might affect the ability to acquire a mobile device

4.2 ***Examination/Analysis***

4.2.1 ***Techniques***

4.2.1.1 Examine common default storage locations of information within a given device's file system, RAM location, or common field
4.2.1.2 Describe how a photograph found on a mobile device can be potentially linked to that device
4.2.1.3 Describe what information would be expected on a given mobile device and how that information might be viewed and/or extracted
4.2.1.4 Explain how mobile device history information can be linked to mobile service provider records

4.2.2 ***Process***

4.2.2.1 Ensure that the examination is within the scope of any court order, permission, or other authority to act

4.2.2.2 Maintain a case file (including notes and photographs) consistent with the procedures of your organization

4.2.2.3 Ensure appropriate communication between the investigator/requestor and the examiner to provide a proper analysis, appropriate reporting, and to address unforeseen circumstances.

4.2.2.4 Provide a report of the examination in a fashion consistent with the organization's policies and procedures

4.2.3 __Concepts__

4.2.3.1 Describe the function of call histories and call timers in mobile phones

4.2.3.2 Explain why deleted files (e.g., SMS messages and photographs) are sometimes recoverable and sometimes not

4.2.3.3 Explain why some information (e.g., contact lists) will sometimes appear on the phone and other times appear on a SIM card or memory expansion card

4.2.3.4 Describe how malware can affect certain types of mobile devices

4.2.3.5 Describe the various numbers associated with mobile phones (e.g., IMEI, IMSI, ICCID) and how they might uniquely identify a piece of hardware

4.2.3.6 Explain the role of PINs and passwords and how they might affect the ability to examine a mobile device

5.0 Network Forensics

5.1 __Acquisition__

5.1.1 __Techniques__

5.1.1.1 Image network drives, shares, and other virtual network devices

5.1.1.2 Demonstrate knowledge of various methods used to identify and acquire digital evidence:

5.1.1.2.1 Network information reporting tools

5.1.1.2.2 Packet sniffers

5.1.1.2.3 Traffic analysis tools

5.1.1.2.4 Penetration testing tools

5.1.1.2.5 Network reconnaissance tools

5.1.2 __Process__

5.1.2.1 Describe the various court orders required to obtain information from an Internet service provider or other third-party in a criminal and/or civil case

5.1.2.2 Identify methods for collecting volatile data from network systems

5.1.2.3 Identify methods for collecting non-volatile data from network systems

5.1.2.4 Identify methods for collecting live data from network systems

5.1.3 __Concepts__

5.1.3.1 Demonstrate a basic knowledge of network topologies, and protocols

5.1.3.2 Explain the concept of network shares

5.1.3.3 Demonstrate an understanding of network area storage devices (NAS)

5.1.3.4 Demonstrate knowledge of the appropriate steps and responses to incidents:

5.1.3.4.1 Identification

5.1.3.4.2 Physical and Logical layout

5.1.3.4.3 Identify types of access (Internal/External)

5.1.3.4.4 Isolation

5.1.3.4.5 Stop the attack

5.1.3.4.6 Volatile and Non-Volatile Data Collection

5.1.3.4.7 Live acquisitions

5.1.3.4.8 Internal log files

5.1.3.4.9 Access provider logs

5.1.3.5 Demonstrate a basic knowledge of the various types of methods used for compromise/attacks

5.2 <u>Examination/Analysis</u>

5.2.1 <u>Techniques</u>

5.2.1.1 Demonstrate knowledge of various methods used to examine and analyze digital evidence:

5.2.1.1.1 Log file correlation and analysis

5.2.1.1.2 Network information reporting tools

5.2.1.1.3 Packet sniffers

5.2.1.1.4 Traffic analysis tools

5.2.1.1.5 Penetration testing tools

5.2.1.1.6 Network reconnaissance tools

5.2.1.2 Conduct a detailed log analysis from network devices (e.g., firewalls, intrusion detection system, web server, mail server, routers, switches)

5.2.1.3 Conduct a net flow or packet analysis

5.2.2 <u>Process</u>

5.2.2.1 Identify methods for analyzing data collected from networks

5.2.2.2 Describe where records of Internet activity can be found and describe tools to assist in the examination of that information

5.2.2.3 Describe sources of information to track IP addresses and Internet domain names

5.2.2.4 Discuss mechanisms of obtaining information from ISPs and other service providers

5.2.2.5 Discuss the operation of client-server e-mail and Web-based e-mail

5.2.3 <u>Concepts</u>

5.2.3.1 Demonstrate a fundamental understanding of networks, network systems and information security concepts:

5.2.3.1.1 Network components/devices

5.2.3.1.2 Network structures

5.2.3.1.3 Network protocols

5.2.3.1.4 Network protection

5.2.3.1.5 Internet and Internet Protocols

5.2.3.2 Demonstrate knowledge of basic networking hardware:
- 5.2.3.2.1 Network Interface Card (NIC)
- 5.2.3.2.2 Routers
- 5.2.3.2.3 Switches
- 5.2.3.2.4 Hubs
- 5.2.3.2.5 Repeaters
- 5.2.3.2.6 Wireless Devices
- 5.2.3.2.7 Firewalls

5.2.3.3 Demonstrate an understanding of the various types of methods used to compromise/attack systems and networks:
- 5.2.3.3.1 Social Engineering
- 5.2.3.3.2 Malware
- 5.2.3.3.3 Eavesdropping
- 5.2.3.3.4 Software-based attacks
- 5.2.3.3.5 Exploitation of known weaknesses
- 5.2.3.3.6 System disruptions and Denial of Service (DoS) attacks
- 5.2.3.3.7 Packet floods and DDoS
- 5.2.3.3.8 Exploitation of known weaknesses
- 5.2.3.3.9 Session hijacking
- 5.2.3.3.10 Man-in-the-Middle (MITM) attacks
- 5.2.3.3.11 IP/MAC addressing spoofing
- 5.2.3.3.12 Identity Spoofing

5.2.3.4 Demonstrate and understanding of the role of anonymizers

6.0 Program and Software Forensics

6.1 __Techniques__

6.1.1 Demonstrate a basic knowledge of different types software programming languages, scripting, and techniques.

6.1.2 Execute proper chain-of-custody.

6.1.3 Demonstrate a basic knowledge of decompiling and reverse engineering.

6.1.4 Demonstrate a basic knowledge of binary auditing.

6.2 __Process__

6.2.1 Understand standard step-by-step procedure for reviewing software in a forensically sound manner.

6.2.2 Explain the process required for author attribution:
- 6.2.2.1 Content analysis
- 6.2.2.2 Error analysis
- 6.2.2.3 Non-content analysis

6.2.3 Describe items to ascertain when examining malicious code:
- 6.2.3.1 What is does
- 6.2.3.2 When it was written
- 6.2.3.3 Process flow
- 6.2.3.4 Software pattern
- 6.2.3.5 Programmer patterns

6.3 __Concepts__

- 6.3.1 Demonstrate knowledge of the objectives of author attribution:
  - 6.3.1.1 Individual identification
  - 6.3.1.2 Group identification
- 6.3.2 Demonstrate knowledge of how source code is compiled/decompiled.
- 6.3.3 Demonstrate knowledge of the importance of “debug” versions of software.
- 6.3.4 Describe what knowledge can be gained from reviewing systematic “release” versions of software code.
- 6.3.5 Describe various types of software programming errors (bugs).
- 6.3.6 Describe the importance of consistent bug patterns.
- 6.3.7 Demonstrate knowledge of software metrics.
  - 6.3.7.1 Describe various metrics that can be extracted from source code.
  - 6.3.7.2 Complexity of control flow and the affects of code written over lengthy time in contrast to short time periods
- 6.3.8 Explain knowledge of the “FLEXIBILITY” in structured language programming
- 6.3.9 Explain the different types of information that could be expected to be found from reviewing software and/or source code:
  - 6.3.9.1 Programming skill/level
  - 6.3.9.2 Programming language
  - 6.3.9.3 Compiler information
  - 6.3.9.4 System information
  - 6.3.9.5 Sequencing
  - 6.3.9.6 Formatting
  - 6.3.9.7 Commenting
    - 6.3.9.7.1 Grammar
  - 6.3.9.8 Error similarities
  - 6.3.9.9 Programmer determination
  - 6.3.9.10 Programmer discrimination
  - 6.3.9.11 Programmer characterization/identification
- 6.3.10 Understand the types and quality of commenting
  - 6.3.10.1 Errors
  - 6.3.10.2 Style
  - 6.3.10.3 Grammar
  - 6.3.10.4 Language
  - 6.3.10.5 The quantity of commenting
  - 6.3.10.6 The layout of the code
  - 6.3.10.7 Data structure
  - 6.3.10.8 Variables
  - 6.3.10.9 Borders
- 6.3.11 Demonstrate knowledge of what information is lost in the compiling and decompiling processes.
- 6.3.12 Demonstrate knowledge of various types of malicious code:
  - 6.3.12.1 Malware:
    - 6.3.12.1.1 Backdoors
    - 6.3.12.1.2 Adware

- 6.3.12.1.3 Trojans
- 6.3.12.1.4 Worms
- 6.3.12.1.5 Viruses
- 6.3.12.1.6 Rootkits
- 6.3.12.1.7 Logic Bomb

7.0 Quality Assurance, Control, and Management

7.1 Concepts & Techniques – Understand and explain the theory and application of the following concepts and techniques:

- 7.1.1 Quality Assurance
- 7.1.2 Quality Assurance Officer
- 7.1.3 Quality Control
- 7.1.4 Quality Management
- 7.1.5 Quality Process/System
- 7.1.6 Quality Manual
- 7.1.7 Standard Operating Procedures
- 7.1.8 Validation
- 7.1.9 Verification
- 7.1.10 Calibration
- 7.1.11 Standards and Controls
- 7.1.12 Examiner Notes
- 7.1.13 Forensic Report
- 7.1.14 Peer Review
- 7.1.15 Administrative Review
- 7.1.16 Examiner Qualification/Competency
- 7.1.17 Proficiency/Competency Testing
- 7.1.18 Quality Audit
- 7.1.19 Certification
- 7.1.20 Accreditation
- 7.1.21 Physical Security
- 7.1.22 Laboratory Access Control
- 7.1.23 Laboratory Safety

7.2 Processes

- 7.2.1 Certification
  - 7.2.1.1 Vendor Certifications
  - 7.2.1.2 Employer Certifications
  - 7.2.1.3 Community Certifications
- 7.2.2 Accreditation
  - 7.2.2.1 American Society of Crime Laboratory Directors – Laboratory Accreditation Board
  - 7.2.2.2 International Standards Organization 17025