DFCA STUDY GUIDE

Contents

EXAMINATION OVERVIEW

The Digital Forensics Certified Associate (DFCA) examination provides an entry-level certification with potential progression to the Digital Forensic Certified Practitioner (DFCP) certification after the candidate accumulates five years of experience. It also serves those who no longer perform the requisite hours of "hands-on" forensics to renew their DFCP. The goal of the DFCA certification is to enhance the professionalism and body of knowledge within the digital forensics industry and distinguish individuals who have a broad knowledge of digital forensics. As a DFCA, you become a member of the Digital Forensics Certification Board whose sole purpose is to provide certifications that focus on benefiting the profession and promoting professional collaboration. Your certification status connects you with other members whose mission is to help the maturation of digital forensics as a science and encourage the sharing of information, methods and processes among members of the profession. DFCB Associates are held accountable to a high standard of excellence which provides assurance to employers that certified associates meet objective and independent standards.

This study guide was developed to provide a DFCA candidate with an outline and reference material that may be covered on the DFCA examination. If reviewed and studied while preparing for the DFCA examination, one will increase their chances by focusing on a specific knowledge base useful to a DFCA candidate. Each section of this study guide includes domains that are testable on the DFCA exam, along with concepts, terminology, technical data, and references to material that may be testable.

As stated on the DFCB website, the DFCA exam policy is open book, open notes only. No electronic devices such as computers, flash drives, calculators, phones, etc. We recommend you print all study guide material (like this study guide) and bring as hard paper copies. The DFCA exam must be proctored, and if a fee is involved, the candidate must pay it. Options for proctoring are to use the candidate's college testing center, or our professional proctoring service. The service charges $25 and requires 72 hours' notice; earlier appointments are available for additional fees. If you do not pass the exam, you will be notified by the testing committee and given 45 days from the original exam date to retake the exam at no cost. Candidate will be responsible for proctoring fees. Certification is valid for three years from the date you were certified.

So, what should you expect on the DFCA exam? The following is a summary of the test layout and expectations:

- There are 200 questions,
- The questions are multiple choice,
- The test is timed, and
- The Test Methodology includes
    a. Terminology,
    b. Technical concepts, and
    c. Analyzing a situation based on a scenario

DIGITAL FORENSIC METHODOLOGY

The following concepts and terminologies should be studied:

1) Image File
    a. What is an image file?
        ○ Know the difference between a raw image file AND an embedded image format.
2) Hashing
    a. Also known as cryptographic hashing
    b. What is hashing used for during digital forensic examinations?
    c. What are common reasons for using hash values?
    d. What are the most common types of hashing algorithms?
    e. What is a hash set, and why are they important?
    f. What parts of a file ARE NOT included when generating a hash value?
    g. Are there known vulnerabilities with the MD5 hash algorithm? Is it still a valid hash algorithm for use in Forensic Image validation? Explain.
3) Understand the concept of physical data extraction.
4) Understand what IS NOT captured in a physical data extraction?
5) Understand what happens when restoring an acquisition image.
6) Understand the three methods for live acquisitions.
7) Understand the difference between physically copying a file AND logically copying a file.
8) Understand the limitation of data carving tools.
9) Know the hex value for common file types/signatures.
10) Know common locations for finding index.dat files.
11) Understand difference between physical and logical file sizes.
12) Understand Cylinder-Head-Sector (CHS) and its value to forensic investigations.
13) Understand the OSI Model, its layers, and which layer may glean the most during forensic investigations.
14) Terminology
    a. Target Media
    b. Live Acquisition
    c. Dead/cold Acquisition
    d. File Signature
    e. Data Carving
    f. File Header
    g. File Signature
    h. MIME Encoding
    i. File Slack
    j. EO1 Files
    k. Index.dat
    l. CODEC

m. DCO

REFERENCES

1. https://stackoverflow.com/questions/5055143/will-changing-a-file-name-affect-the-md5-hash-of-a-file

COMPUTERS, NETWORKING, AND SYSTEM OVERVIEW

1) Understand how many bytes are in a cluster AND how this can be used to calculate last byte of a file stored on a disk.
2) Understand the difference between HPA and DCO.
3) Understand the difference between volatile and nonvolatile data.
4) Understand the types of attacks on computers, applications, and networks.
5) Understand the types of wireless networking encryptions and the level of strength/security they provide.
6) Know the number possible TCP/IP ports available.
7) Understand what CMOS provides AND what is NOT included in the CMOS.
8) Understand what the BIOS is and how it's useful to a forensic investigation.
9) Know the amount of bytes in a standard sector.
10) Know the smallest area data can be written to on a disk.
11) Know the three reparse point types and what they provide.
12) Know the common types of file systems for Windows, Linux, and Macintosh systems.
13) Know the type of file system and its features commonly found on thumb drives.
14) Understand the three things that occur when creating a file in FAT32 systems.
15) Understand the type of time stored by different file systems?
16) Know the maximum cluster size different file systems can produce.
17) Know the file system used by optical media devices like CDs and DVDs and how data is read from these devices.
18) Understand the concepts of file creation, copying and moving, and be able to explain why a file can show a "modified" date and time that is before its "created" date and time.
19) Understand common Linux OS paths and files.
20) Know the different types of RAID configurations and what value they provide.
21) Know the difference between bits and bytes. Understand their size and relationships.
22) Understand what happens in a file system when a file is deleted.

TERMINOLOGY

Understand the following terms, what they stand for, and how what they describe, works in practice:

1) Host Protected Area (HPA)
2) Order of Volatility
3) Pagefile.sys
4) Rootkit
5) Signature-sporadic
6) Endomorphic
7) Polymorphic
8) Worm
9) Virus
10) POST
11) CMOS

12) IP Address
13) NAT Address
14) DNS Servers
15) Memory Address
16) MAC Address
17) ROM
18) CPU
19) RAM
20) Motherboard
21) Partition vs Partition Table
22) Master Boot Record
23) Volume Boot Sector
24) File system
25) Small Computer System Interface (SCSI)
26) Host Protected Area (HPA)
27) Volume
28) Cluster
29) Sector
30) Network protocols
31) ARP
32) TCP
33) TCP Handshake
34) UDP
35) ICMP
36) Sniffer
37) Metadata
38) UDF
39) MAC values
40) Volume Boot Record
41) Master File Table (MFT)
42) Alternate Data Streams
43) Master Boot Record (MBR)
44) DDOS
45) Trojan Horse
46) Port Scan
47) Denial of Service (DOS)
48) Social Engineering
49) Logic Bomb
50) Brute Force
51) Phishing
52) Intrusion

53) .M4V
54) .MOV

REFERENCES

1. https://tools.ietf.org/html/rfc3227#section-2.1
2. RFC 3227: https://www.ietf.org/rfc/rfc3227.txt
3. https://www.techadvisor.co.uk/how-to/windows/what-is-pagefilesys-3608749/
4. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_arp/configuration/15-s/arp-15-sbook/Configuring-Address-Resolution-Protocol.pdf
   http://www.tcpipguide.com/free/t_TCPConnectionEstablishmentProcessTheThreeWayHandsh-3.htm
5. https://www.usna.edu/CyberDept/sy110/lec/netTrans/lec.html
6. https://askubuntu.com/questions/62492/how-can-i-change-the-date-modified-created-of-a-file/62496#62496

LEGAL, SEARCH AND SEIZURE, AND EVIDENCE PRESERVATION

Understand the concept of what our Constitution is, and whose conduct it seeks to restrict or prohibit.

Understand the implications of the 4th Amendment on digital forensic examinations and investigations.

Understand the implication of the 5th Amendment on digital forensic examinations and investigations.

Understand the various rules and procedures for searching and seizing digital evidence.

Understand the DFCB Ethics Rules.

Understand Federal Rules of Evidence and how they apply to digital evidence.

Understand how the Federal Rules of Evidence relate to state rules of evidence.

Understand when a search warrant is needed when performing a digital forensic examination.

Understand the difference between the "Daubert" and "Frye" cases, and the standards they created.

Understand the "Plain View" principle and its application to law enforcement and digital forensics.

Understand different industry standards about digital evidence examinations.

The following concepts should be understood:

1. EVIDENCE PRESERVATION
2. Wiping Media
    a. Why is wiping important?
    b. When should it occur?
3. Forensic Image
    a. Types of forensic image technologies.
4. Write Blocking
    a. Primary purpose of write blocking.
    b. Types of write blockers.
5. Ways an examiner can protect and ensure evidence integrity.
6. Best practices for securing a computer as evidence
7. HEALTH INSURANCE PORTABILITY ACT (HIPAA)
    a. Major terms/components of HIPAA, cybersecurity, and digital evidence.
8. PHI
    a. When can a healthcare provider disclose information to law enforcement?
9. Electronic Communications Privacy Act (ECPA)
    a. What is this law?
    b. What does this law restrict?
10. Spoliation
    a. What does this term mean, and when is it applicable to digital forensic examinations?
11. Discovery
    a. What is this concept, and what does it obligate parties of a digital forensic examination to do?

12. Three exceptions to the search warrant requirement before law enforcement officers may seize digital evidence
13. The concept of "A Reasonable Expectation of Privacy" and how it relates to search warrants and Digital Forensic Examinations
14. General consideration before performing a forensic examination
15. Chain of Custody
    a. What is it?
    b. What is purpose?
    c. What does it document?
16. Report Writing
    a. Examiners should create a report to document their process and findings
    b. Report Goals
        i. Completed in a timely manner.
        ii. Accurately describe the details of the incident and findings.
        iii. Offer valid conclusions and opinions as to the content discovered.
        iv. Contain all information to explain the examiner's conclusions.

REFERENCES

1. https://www.crime-scene-investigator.net/crime-scene-procedures.htm
2. http://www.forensicsciencesimplified.org/legal/frye.html
3. https://www.law.cornell.edu/wex/plain_view_doctrine
4. https://www.ncjrs.gov/pdffiles1/Digitization/63104NCJRS.pdf
5. Horton v. California, 496 U.S. 128 (1990). https://caselaw.findlaw.com/us-supremecourt/496/128.html
6. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=6992&context=jclc
7. Scientific Working Group on Digital Evidence
    a. https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices% 20for%20Mobile%20Phone%20Forensics
8. The Best Practices for Computer Forensics.
    a. https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices% 20for%20Computer%20Forensics

TECHNICAL ANALYSIS – Forensic Examination of Windows-Based Systems

1. Understand the different types of internet history files.
2. Understand the major components of the NTFS File System.
3. Understand major DOS Commands.
4. Understand the difference between a Registry Root Level Key and a Registry Hive.
5. The following terms, concepts, and references should be reviewed when preparing for the examination:
    a. DOS and DOS Commands
    b. nslookup
    c. What will this command do?
        i. DIR /S *.TXT
    d. DOS Partitioning Scheme
        i. A disk organized using DOS contains what information in the first sector?
    e. Common file extensions and what they generally pertain to. Examples:
        i. .dbx
        ii. .PST
        iii. .SHD
        iv. .SPL
    f. Five registry root level keys in Microsoft XP
        i. HKEY_CLASSES_ROOT
        ii. HKEY_CURRENT_USER
        iii. HKEY_CURRENT_CONFIG
        iv. HKEY_LOCAL_MACHINE
        v. HKEY_USERS
    g. Features of a Virtual Memory Swap File
    h. Windows Swap Files
        i. Significance from a forensics perspective
    i. Common path/location of event log files
        i. Default location.
        ii. What are the three types of event log files.
    j. Prefetch Files.
        i. Locations within different OS types.
    k. Volume Shadow Copy
    l. Windows Registry
        i. What is it?
    m. NTUSER.DAT
        i. Significance to digital forensics?
    n. Where can you find Time Zone Information and Computer Name?
    o. Likely location of:
        i. "…/Software/Yahoo/Pager/profiles/screen name/chat"
    p. RunMRU
    q. INFO2 Files

r. Thumbs.db
s. Location of recycle bin in different OSs.
t. $1
    i. Original file name of a file found in, what?
u. Windows Link Files

REFERENCES

1. https://docs.microsoft.com/en-us/windows/desktop/sysinfo/structure-of-the-registry

TECHNICAL ANALYSIS – Forensic Examination of Unix/Linux-Based Systems

1. Understand how Unix records time within the OS.
2. Understand what Epoch Time is.

TECHNICAL ANALYSIS – Forensic Examination of Macintosh-Based Systems

1. Understand what File Vault is, and what it protects.
2. Understand what happens when File Vault is enabled, and be able to describe how to determine whether it is enabled or not.
3. Study and understand the following terms, concepts, and references:
    a. .DMG
    b. Disk Arbitration:
    c. "secure empty trash" option in the Finder

TECHNICAL ANALYSIS – Forensic Examination of Mobile Devices

1. Understand the different components of a cell phone architecture.
2. Understand the difference between GSM and CDMA.
3. Understand and study the following concepts, terminology, and references:
    a. Subscriber Identity Module (SIM) Card
    b. SIMs
        i. Forensic procedure for examining SIMs
    c. GSM
        i. Steps to best isolate a phone from a GSM carrier
    d. CDMA
        i. Steps to best isolate a phone from a CDMA carrier?
    e. RF SIGNALS
    f. Different Protection Features
        i. Faraday Bags
    g. Types of mobile device examinations
        i. Chip Off Analysis
        ii. JTAG
        iii. Logical Acquisition
        iv. File System Acquisition
        v. Physical Acquisition
        vi. Manual Acquisition/Manual Analysis.
        vii. Least forensically sound b/c it involves utilizing the user's interface to investigate content.
    h. Apple iPhones
        i. Disk layout
        ii. divided into 2 partitions

REFERENCES

1. https://www.forensicmag.com/article/2014/02/need-faraday-bag