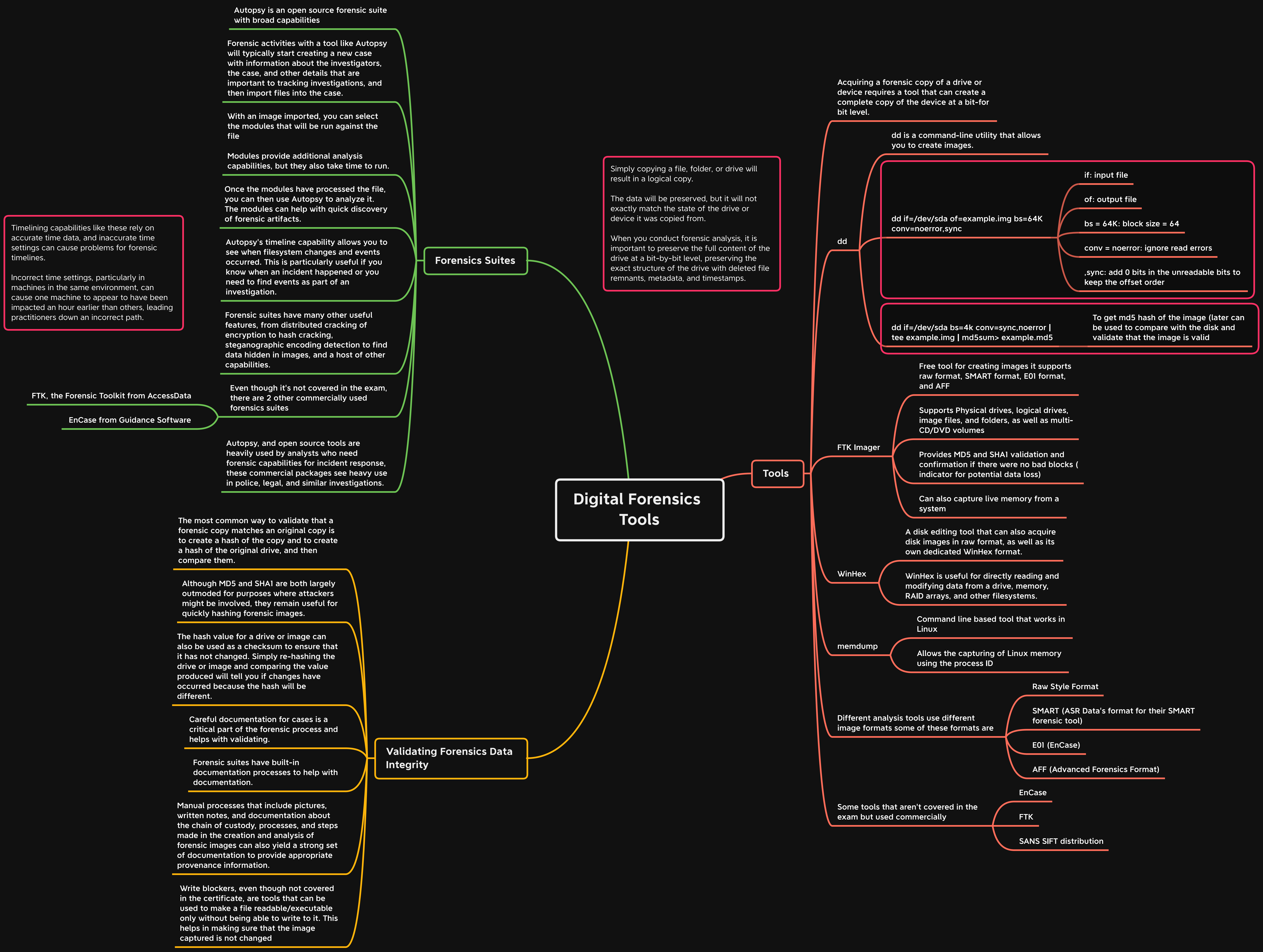

Digital Forensics Tools

Forensics Suites

- Autopsy is an open source forensic suite with broad capabilities
- Forensic activities with a tool like Autopsy will typically start creating a new case with information about the investigators, the case, and other details that are important to tracking investigations, and then import files into the case.
- With an image imported, you can select the modules that will be run against the file

  Modules provide additional analysis capabilities, but they also take time to run.
- Once the modules have processed the file, you can then use Autopsy to analyze it. The modules can help with quick discovery of forensic artifacts.
- Autopsy's timeline capability allows you to see when filesystem changes and events occurred. This is particularly useful if you know when an incident happened or you need to find events as part of an investigation.
- Forensic suites have many other useful features, from distributed cracking of encryption to hash cracking, steganographic encoding detection to find data hidden in images, and a host of other capabilities.
- Even though it's not covered in the exam, there are 2 other commercially used forensics suites
  - FTK, the Forensic Toolkit from AccessData
  - EnCase from Guidance Software
- Autopsy, and open source tools are heavily used by analysts who need forensic capabilities for incident response, these commercial packages see heavy use in police, legal, and similar investigations.

Timelining capabilities like these rely on accurate time data, and inaccurate time settings can cause problems for forensic timelines.

Incorrect time settings, particularly in machines in the same environment, can cause one machine to appear to have been impacted an hour earlier than others, leading practitioners down an incorrect path.

Tools

Simply copying a file, folder, or drive will result in a logical copy.

The data will be preserved, but it will not exactly match the state of the drive or device it was copied from.

When you conduct forensic analysis, it is important to preserve the full content of the drive at a bit-by-bit level, preserving the exact structure of the drive with deleted file remnants, metadata, and timestamps.

- Acquiring a forensic copy of a drive or device requires a tool that can create a complete copy of the device at a bit-for bit level.
- dd
  - dd is a command-line utility that allows you to create images.
  - `dd if=/dev/sda of=example.img bs=64K conv=noerror,sync`
    - if: input file
    - of: output file
    - bs = 64K: block size = 64
    - conv = noerror: ignore read errors
    - ,sync: add 0 bits in the unreadable bits to keep the offset order
  - `dd if=/dev/sda bs=4k conv=sync,noerror | tee example.img | md5sum> example.md5`
    - To get md5 hash of the image (later can be used to compare with the disk and validate that the image is valid
- FTK Imager
  - Free tool for creating images it supports raw format, SMART format, E01 format, and AFF
  - Supports Physical drives, logical drives, image files, and folders, as well as multi-CD/DVD volumes
  - Provides MD5 and SHA1 validation and confirmation if there were no bad blocks (indicator for potential data loss)
  - Can also capture live memory from a system
- WinHex
  - A disk editing tool that can also acquire disk images in raw format, as well as its own dedicated WinHex format.
  - WinHex is useful for directly reading and modifying data from a drive, memory, RAID arrays, and other filesystems.
- memdump
  - Command line based tool that works in Linux
  - Allows the capturing of Linux memory using the process ID
- Different analysis tools use different image formats some of these formats are
  - Raw Style Format
  - SMART (ASR Data's format for their SMART forensic tool)
  - E01 (EnCase)
  - AFF (Advanced Forensics Format)
- Some tools that aren't covered in the exam but used commercially
  - EnCase
  - FTK
  - SANS SIFT distribution

Validating Forensics Data Integrity

- The most common way to validate that a forensic copy matches an original copy is to create a hash of the copy and to create a hash of the original drive, and then compare them.
- Although MD5 and SHA1 are both largely outmoded for purposes where attackers might be involved, they remain useful for quickly hashing forensic images.
- The hash value for a drive or image can also be used as a checksum to ensure that it has not changed. Simply re-hashing the drive or image and comparing the value produced will tell you if changes have occurred because the hash will be different.
- Careful documentation for cases is a critical part of the forensic process and helps with validating.
- Forensic suites have built-in documentation processes to help with documentation.
- Manual processes that include pictures, written notes, and documentation about the chain of custody, processes, and steps made in the creation and analysis of forensic images can also yield a strong set of documentation to provide appropriate provenance information.
- Write blockers, even though not covered in the certificate, are tools that can be used to make a file readable/executable only without being able to write to it. This helps in making sure that the image captured is not changed