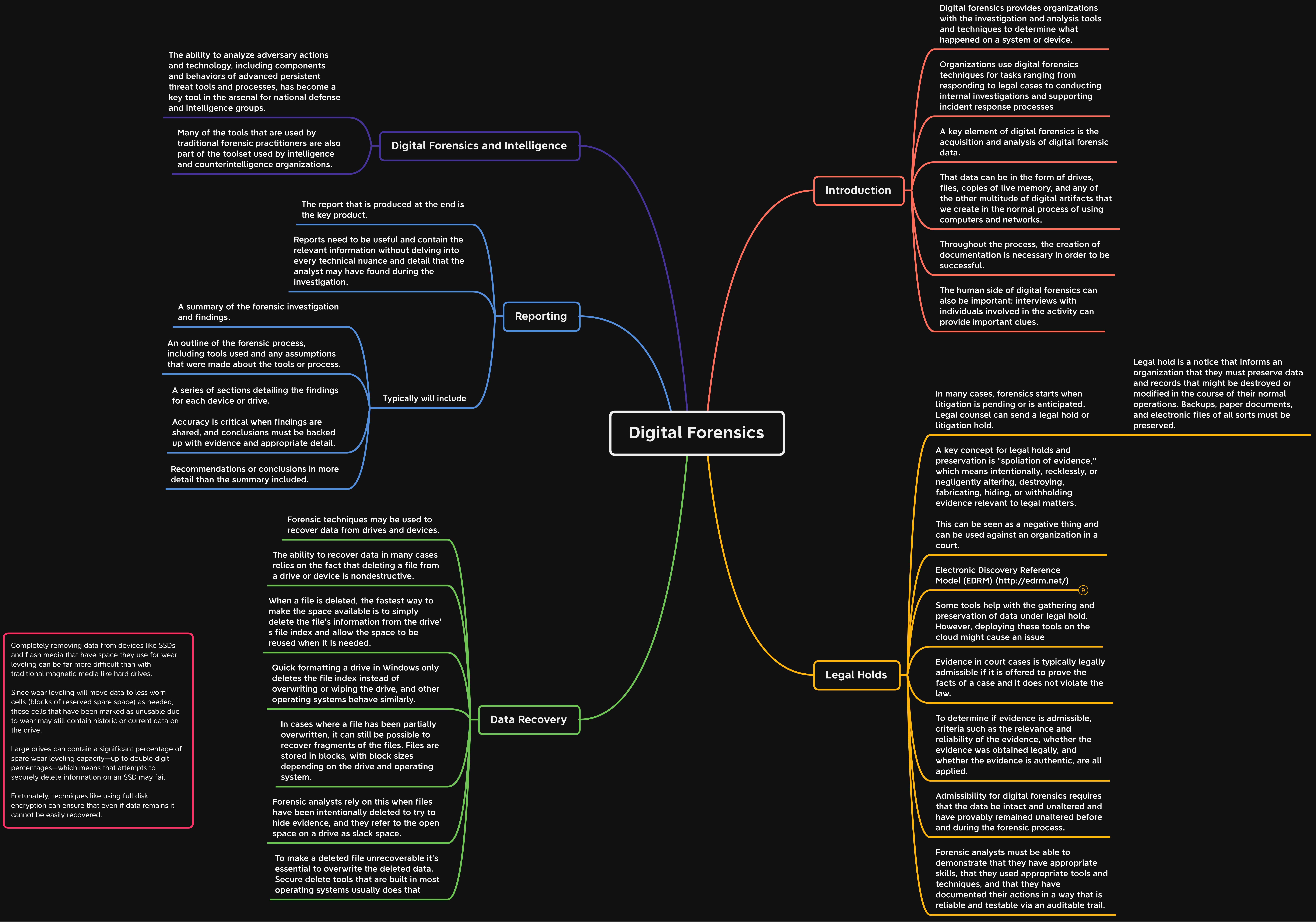

Digital Forensics

Introduction

- Digital forensics provides organizations with the investigation and analysis tools and techniques to determine what happened on a system or device.
- Organizations use digital forensics techniques for tasks ranging from responding to legal cases to conducting internal investigations and supporting incident response processes
- A key element of digital forensics is the acquisition and analysis of digital forensic data.
- That data can be in the form of drives, files, copies of live memory, and any of the other multitude of digital artifacts that we create in the normal process of using computers and networks.
- Throughout the process, the creation of documentation is necessary in order to be successful.
- The human side of digital forensics can also be important; interviews with individuals involved in the activity can provide important clues.

Legal Holds

- In many cases, forensics starts when litigation is pending or is anticipated. Legal counsel can send a legal hold or litigation hold.
  - Legal hold is a notice that informs an organization that they must preserve data and records that might be destroyed or modified in the course of their normal operations. Backups, paper documents, and electronic files of all sorts must be preserved.
- A key concept for legal holds and preservation is "spoliation of evidence," which means intentionally, recklessly, or negligently altering, destroying, fabricating, hiding, or withholding evidence relevant to legal matters.

  This can be seen as a negative thing and can be used against an organization in a court.
- Electronic Discovery Reference Model (EDRM) (http://edrm.net/)
- Some tools help with the gathering and preservation of data under legal hold. However, deploying these tools on the cloud might cause an issue
- Evidence in court cases is typically legally admissible if it is offered to prove the facts of a case and it does not violate the law.
- To determine if evidence is admissible, criteria such as the relevance and reliability of the evidence, whether the evidence was obtained legally, and whether the evidence is authentic, are all applied.
- Admissibility for digital forensics requires that the data be intact and unaltered and have provably remained unaltered before and during the forensic process.
- Forensic analysts must be able to demonstrate that they have appropriate skills, that they used appropriate tools and techniques, and that they have documented their actions in a way that is reliable and testable via an auditable trail.

Digital Forensics and Intelligence

- The ability to analyze adversary actions and technology, including components and behaviors of advanced persistent threat tools and processes, has become a key tool in the arsenal for national defense and intelligence groups.
- Many of the tools that are used by traditional forensic practitioners are also part of the toolset used by intelligence and counterintelligence organizations.

Reporting

- The report that is produced at the end is the key product.
- Reports need to be useful and contain the relevant information without delving into every technical nuance and detail that the analyst may have found during the investigation.
- Typically will include
  - A summary of the forensic investigation and findings.
  - An outline of the forensic process, including tools used and any assumptions that were made about the tools or process.
  - A series of sections detailing the findings for each device or drive.

    Accuracy is critical when findings are shared, and conclusions must be backed up with evidence and appropriate detail.
  - Recommendations or conclusions in more detail than the summary included.

Data Recovery

- Forensic techniques may be used to recover data from drives and devices.
- The ability to recover data in many cases relies on the fact that deleting a file from a drive or device is nondestructive.
- When a file is deleted, the fastest way to make the space available is to simply delete the file's information from the drive' s file index and allow the space to be reused when it is needed.
- Quick formatting a drive in Windows only deletes the file index instead of overwriting or wiping the drive, and other operating systems behave similarly.
- In cases where a file has been partially overwritten, it can still be possible to recover fragments of the files. Files are stored in blocks, with block sizes depending on the drive and operating system.
- Forensic analysts rely on this when files have been intentionally deleted to try to hide evidence, and they refer to the open space on a drive as slack space.
- To make a deleted file unrecoverable it's essential to overwrite the deleted data. Secure delete tools that are built in most operating systems usually does that

Completely removing data from devices like SSDs and flash media that have space they use for wear leveling can be far more difficult than with traditional magnetic media like hard drives.

Since wear leveling will move data to less worn cells (blocks of reserved spare space) as needed, those cells that have been marked as unusable due to wear may still contain historic or current data on the drive.

Large drives can contain a significant percentage of spare wear leveling capacity—up to double digit percentages—which means that attempts to securely delete information on an SSD may fail.

Fortunately, techniques like using full disk encryption can ensure that even if data remains it cannot be easily recovered.