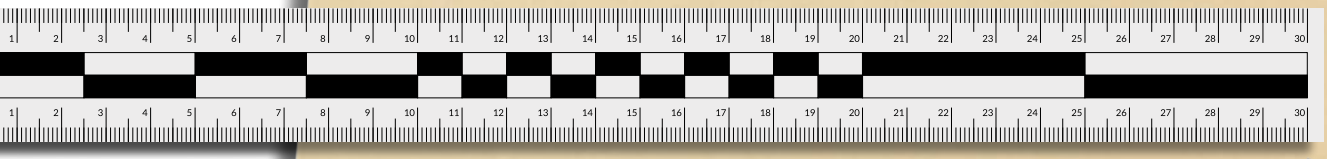
Lesson 1
What is Forensic Science?



Great are the works of the Lord, *studied by all who delight in them* (Psalm 111:2).

CASE STUDY

A period of unrest in a culture can often result in violent, and often unjust, measures to pacify disorderly mobs. Disturbances like these have occurred multiple times throughout criminal justice history. The following case is not only the most famous in history, but the effect of the unjust conviction brought upon necessary consequences that are still felt today.

An innocent man was convicted and executed in an attempt to prevent possible rioting. The populace at the time was supportive of the execution, and hundreds observed his death. Guards assigned to the execution verified the man was deceased. The burial site of the executed man was public knowledge. Once the body was laid to rest, it was officially sealed by the government. If anyone were to break the seal, the punishment would be immediate death. Due to the man's notoriety and the controversy surrounding his execution, the government was concerned the man's supporters would attempt to extract his body. A group of armed guards were assigned to secure the location of burial. The armed guards were a well-trained "military machine" with extensive combat training and loyal allegiance to the government.[1]

Within three days of the burial, the guards would flee for their lives and the body would disappear. According to historian Tacitus, the disappearance of the executed man's body was a "most mischievous superstition."[2]

Three basic theories exist for the disappearance of the body:

1. The man was not really dead and escaped.
2. The body was stolen by his supporters.
3. The man resurrected from the dead.

Sir Arthur Conan Doyle, the author of the Sherlock Holmes mysteries, stated in one of his short stories, "Once you eliminate the impossible, whatever remains, no matter how improbable, must be the truth."[3]

Therefore, consider these facts:

1. The death was verified by the guards assigned to the execution.
2. The burial site was sealed by government professionals.
3. Due to the skilled military machine guarding the burial site, it is improbable the man's supporters would have been physically able to overcome the guards and steal the body.
4. Multiple independent sources attested to the fact that the burial site was empty.
5. The guards disappeared during the night, fearing the repercussions of their failure to secure the burial site.
6. Over 500 eyewitnesses verified through oral and written documents that the executed man was, in fact, alive.

Though a mystery to many individuals during this time period, for others it is a fulfillment of prophecy. Have you determined what famous case this is referring to?

Each case study in this book will correlate to the lesson material. It is important to learn about how the information learned applies to real case work. This case study is referring to the most horrific murder in history, the death of the Creator of Universe, the Lamb of God, the I Am, Jesus Christ. Jesus Christ is the author of knowledge and the study of science. Enjoy this lesson as you learn more about the Savior and how He relates to forensic science.

The discipline of forensic science produces iconic images in the minds of students: investigators probing with flashlights in the night, heroic discoveries of key evidence, and the opportunity to be an adventurous participant in the investigation of a famous crime scene mystery. These images are largely fueled by fictional crime scene television shows, which have popularized the profession of forensic investigation. Fundamentally, forensic science is the application of scientific investigation to the judicial system. There are over twenty forensic disciplines that exist in the field today, and crime scene personnel specialize within this realm of expertise. Regardless of the area of focus for an investigator, there is the opportunity to delight in the works of the Lord (Psalm 111:2). God is the Creator, Designer, and Author of science.

Forensic science experts, or criminalists, require extensive training and must be willing to use a multidisciplinary approach, meaning a forensic investigator works closely with police officers, detectives, coroners, and lab personnel toward a resolution. The American Academy of Forensic Sciences (AAFS) outlines the roles of a forensic scientist as having the ability to distinguish relevant facts from random ones, conduct appropriate testing measures, develop hypotheses, and interpret these results in an attempt to "reach a conclusion or opinion" regarding the evidence's relationship to the crime.[4] This approach will utilize the expertise of several individuals and departments within an agency for the sole purpose of finding evidence that directly links a suspect to a crime or absolves a suspect of a crime.

WHAT IS FORENSIC SCIENCE?

Merriam-Webster defines forensic science as "the application of scientific principles and techniques to matters of criminal justice especially as relating to the collection, examination, and analysis of physical evidence."[5] The Latin root for forensic is *forensis*, which means "of or before the forum," and the root of the word *science* means knowledge. Therefore, the term "forensic science" refers to the acquisition of knowledge gained from the evidence, analysis, and investigator interpretations, with the goal of presenting this knowledge before individuals in the judicial system (the forum).

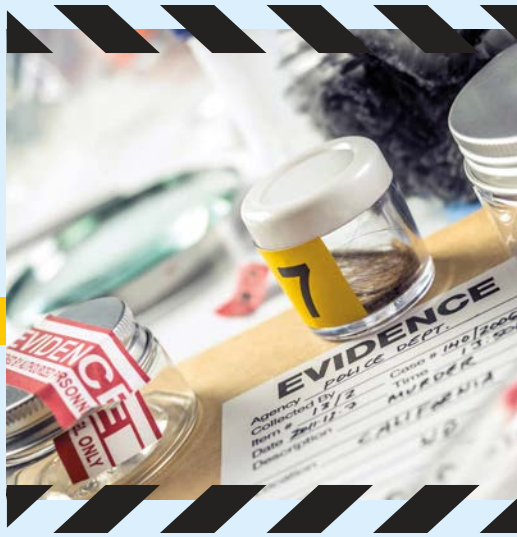
Psalm 111:2:

"Great are the works of the Lord, studied by all who delight in them."

Forensic investigation includes:

- Preservation of the crime scene
- Collection and examination of physical evidence
- Selection and administration of appropriate testing
- Interpretation of data
- Drawing conclusions
- Clear and concise reporting
- Cooperation amongst the investigative team
- Truthful articulation of the facts through the testimony of forensic scientists

The requirements to be a forensic science expert often include hundreds of hours of training, keen observational techniques, rigorous certification testing, the ability to engage in the tedious examination of evidence, and the clear articulation of the facts in courtroom testimony. Once a scientist has prepared themselves with these tools, they are ready for the challenges waiting in forensic field work.



WHAT IS SCIENCE?

The Latin root for the word science is *scientia*, which means knowledge. The word knowledge originated from the Greek word *gnosis* and means to have the capacity to know or understand through observation.[6] But where did knowledge come from? The Bible provides clear answers to this question and tells us that science (knowledge) cannot exist apart from God. Since the Bible is the perfect Word of God, we can trust the authenticity and reliability of this historical record from the very first verse (see **Table 1**).

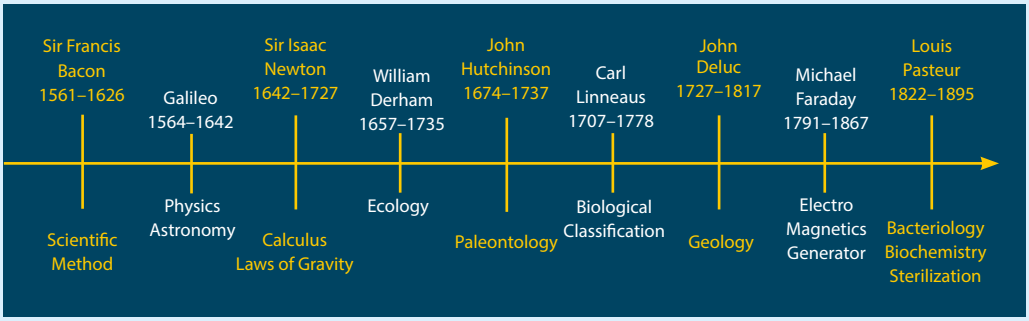
Table 1

The Beginning of Knowledge	**Reference**
In the beginning, God created everything from nothing.	Genesis 1
God created man in His image with an inborn knowledge of Him.	Genesis 1:26–27 Romans 1:21 Romans 2:15
At the end of the creation week, knowledge was perfect and "very good."	Genesis 1:31
Man's sin against God corrupted knowledge.	Genesis 3:6
Humans sinfully desire knowledge for self-glorification.	Genesis 11:4
Jesus Christ is the only source of knowledge.	Colossians 2:2–3 Luke 24:25
Salvation through the Cross is the only path to true knowledge.	1 Corinthians 1:18
One day, God will restore the perfect knowledge of Him.	1 John 3:2

The Knowledge of God[7]	**Reference**
He is the God of knowledge.	Psalm 139:1–6
He has infinite knowledge.	Psalm 147:5
His knowledge is separate from human knowledge.	Isaiah 55:8
His knowledge is perfect.	Job 37:16
His knowledge is denied by the wicked.	Psalm 73:11–12
The believer is secure in this knowledge.	1 John 3:20

Based on the Bible's explanation of knowledge, it is clear that science cannot exist without God as the foundation upon which creation is studied (Proverbs 2:6). And, for centuries, scientific study was attributed to the pursuit of learning about God's creation. The majority of pioneers in science were Bible-believing Christians (see **Table 2**).

Table 2: Timeline of Christian Scientists



After the publication of Charles Darwin's *Origin of Species* in 1859, there was a significant abandonment of scientific endeavors dedicated to the glory of God. The entrance of naturalism (origins without the need for a Creator God) into science academia started a snowball effect away from biblical authority that continues to this day. On the most fundamental level, we can see this change in the very definition of science. Observe how *Webster's Dictionary* has modified the definition of science over time (see **Table 3**). The Webster's 2023 definition of science states it is "knowledge … tested through scientific method."

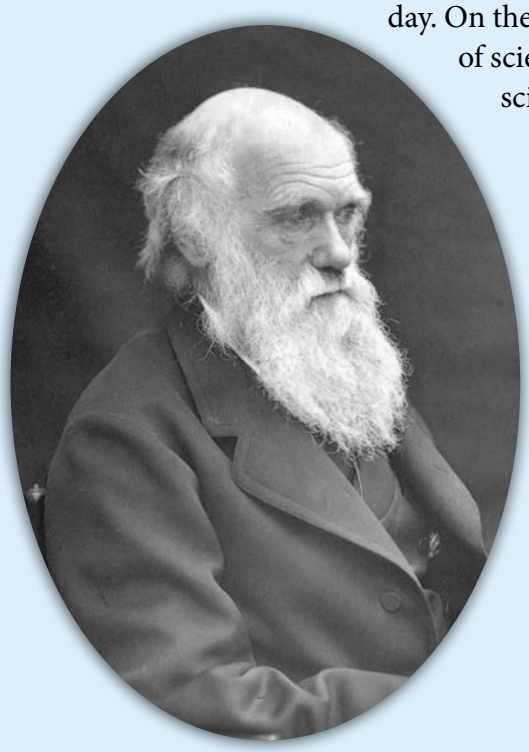
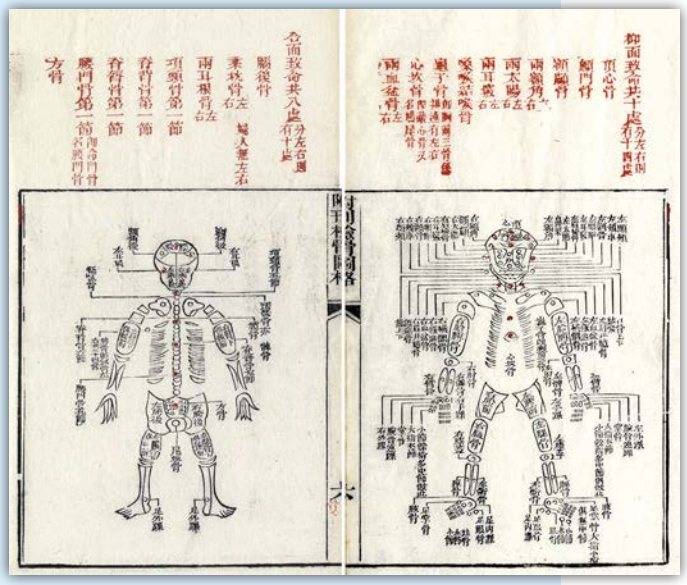


Table 3: Webster's Chronological Definitions of Science

1828	Science: "knowledge; the comprehension or understanding of truth or facts by the mind. **The science of God must be perfect** [emphasis added]."[8]
1913	Science: "knowledge as it relates to the physical world, the nature, constitution, and forces of matter, **called also natural science** [emphasis added]."[9]
2020	Science: "knowledge or system of knowledge covering general truths or the operation of general laws especially as obtained and tested through scientific method."[10]

THE HISTORY OF FORENSIC SCIENCE

When we start with God's Word, we can see evidence of investigation and judgment for criminal behavior as early as 6,000 years ago with the very first murder involving Cain and his brother Abel. God, the all-knowing, all-powerful, and final Judge, punished Cain for his crime. The Bible tells us in Genesis 4:11–12, "And now you are cursed from the ground, which has opened its mouth to receive your brother's blood from your hand. When you work the ground, it shall no longer yield to you its strength. You shall be a fugitive and a wanderer on the earth."

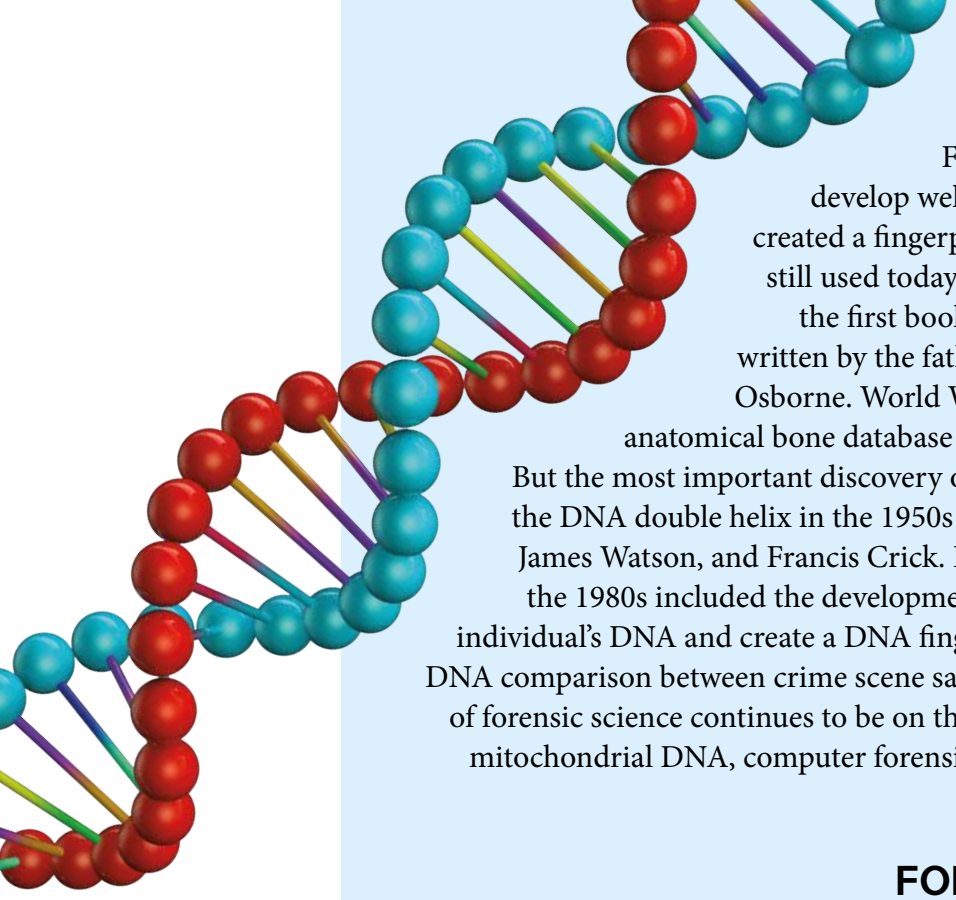


Xǐ-yuān lù jí-zhèng, 1843 edition

All throughout history, there are traces of investigative techniques used in disappearances, deaths, thefts, and related crimes, but the earliest beginnings of the techniques we associate with forensic science can be traced to approximately 300 B.C. Archaeology has provided evidence that the Chinese used fingerprints and handprints as a form of identification.[11] In the early 1200s, forensic entomology (study of bugs) was used to solve a murder case,[12] and the 1600s revealed observations and writings on the unique characteristics in friction ridge skin, but it was not until the late 1800s that we see the beginnings of early crime scene analysis. This was largely due to a book published in 1887 titled *A Study in Scarlet*, written by Sir Arthur Conan Doyle. This fictional book introduced a new character to the world, Sherlock Holmes. Holmes utilized reason, innovative techniques, and investigation to solve crimes.[13] Many of the techniques Sherlock Holmes used were not even practiced or implemented in police work. Interestingly, this is a case where a fictional character sparked innovation in the physical world.

Edmond Locard, a French criminologist known as the Sherlock Holmes of France, started the very first crime lab in 1910. As a pioneer in early investigative practices, Locard initiated many practices still used today. He also worked closely with Alphonse Bertillon on one of the first systems of classification based on body measurements, called anthropometry.[14] He is also considered the father of poroscopy, or the study of pore patterns on friction ridge skin.

Locard's best known contribution to forensic science is Locard's Exchange Principle, which states that when two items come into contact with one another, there is an exchange of material between them. Locard's Exchange Principle is the foundation for forensic science.



Forensic science techniques continued to develop well into the mid-1900s. Sir Edward Henry created a fingerprint classification system in 1896 that is still used today in English-speaking countries. In 1910, the first book examining questioned documents was written by the father of document examination, Sherman Osborne. World War II and the Korean War provided the anatomical bone database for forensic anthropology investigation. But the most important discovery of the last 100 years was the discovery of the DNA double helix in the 1950s by Rosalind Franklin, Maurice Wilkins, James Watson, and Francis Crick. Further advancement by Alec Jeffreys in the 1980s included the development of the testing necessary to process an individual's DNA and create a DNA fingerprint. This technique was integral for DNA comparison between crime scene samples, victims, and suspects. The future of forensic science continues to be on the cusp of innovation within the fields of mitochondrial DNA, computer forensics, and evidence processing techniques.

FORENSIC SCIENCE CAREERS

As stated earlier, there are over twenty disciplines, or specialties, in the field of forensic science. Employment within this field ranges from civilian personnel and sworn deputies to Ph.D. scientists working in laboratories and medical doctors performing autopsies. The American Academy of Forensic Scientists (AAFS) is the largest governing body in the field of forensic science and is composed of over 7,000 scientists. Though the AAFS only distinguishes eleven forensic distinctions on their official list, there are many more areas where experts are needed. According to the AAFS, forensic science career choices include:[15]

- Anthropology
- Criminalistics
- Digital & Multimedia Sciences
- Engineering & Applied Sciences
- General
- Jurisprudence
- Odontology
- Pathology/Biology
- Psychiatry & Behavioral Science
- Questioned Documents
- Toxicology

Early forensic scientists (left) who assisted in solving the Lindberg kidnapping case and began the FBI crime laboratory. The numbers indicate the area the employee worked in.

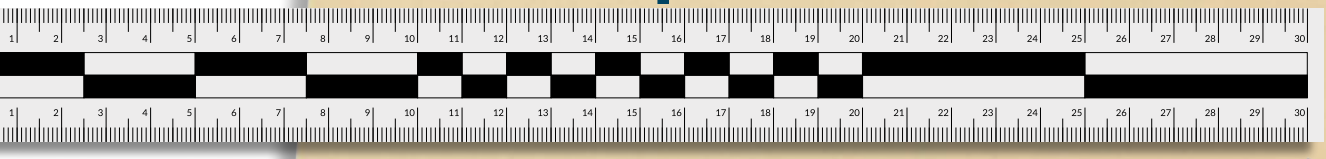
The FBI crime laboratory started in 1932 is one of the largest in the world and employs a variety of forensic experts. In addition to the fields already mentioned, the FBI employs:[16]

- Chemists
- Cryptanalyst-Forensic Examiner
- Forensics Operation Specialist
- Geologist-Forensic Examiner
- Management & Programs Analyst
- Metallurgist Forensic Examiner
- Photographer
- Physical Scientist
- Forensic Accountant
- Fingerprints & Biometric Examiners

Qualifications for employment vary between local, state, and national agencies, but a minimum of a bachelor's or master's degree is required for most forensic fields. Prior to career selection or college coursework, it is recommended that you research the requirements in your field of interest. Many of the specializations mentioned above will require training and additional certifications after employment. Regardless of the forensic field, each one provides the opportunity to give honor to the Creator and Designer of all scientific disciplines, our Lord and Savior Jesus Christ.

Lesson 9

Computer Forensics



All things were made through him, and without him was not any thing made that was made (John 1:3).

CASE STUDY

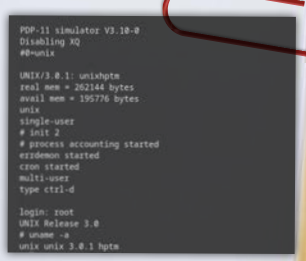
Case Study: The Morris Worm

In 1989, the World Wide Web was invented. A year prior, on November 2, 1988, Robert Tappan Morris, a student working on his master's degree at Cornell, released the first "recognized" computer worm by hacking a terminal at Massachusetts Institute of Technology (MIT) from his location at Cornell University in New York. Morris was known for his technological expertise in the Unix® operating system. Morris' father was one of the computer scientists who helped develop the Unix® system, a system still used in iPhones® today. Morris had designed a worm that would slowly spread through computers using the Unix operation system. A computer worm is different from a computer virus since a worm does not need a software hosting platform but is simply a self-replicating computer program. Robert Morris claimed he did not intentionally design an attack on computers but wanted to see how big the internet was in 1988. He thought he had created an experiment with a slow, stealthily moving program. This program would be passed through the internet to determine the size of it. Unfortunately, the program moved through the internet much faster than expected, wreaking havoc online. The first computer attack had been implemented.

Facts about the case:[118]

- Though the Morris Worm has received notoriety for being the first major computer attack, computer viruses had been detected for five years prior to 1988.
- Within the first 24 hours of the released computer worm, 6,000 of the 60,000 computers connected to the internet received a "denial of service" (DoS) attack.
- The worm was able to decipher weak passwords.
- The worm was programmed to reinfect a computer 1 in 7 times, causing machines to malfunction.[119]
- The worm did not destroy files or attempt to retrieve sensitive information, but it did cause damage, slow down processing times, and cause widespread outages.
- It is estimated the Morris Worm resulted in millions of dollars in damages in 1988.
- The Morris Worm infiltrated Berkeley, Harvard, Princeton, Stanford, John Hopkins, NASA, the Lawrence Livermore National Library, and more.
- As a result of this attack, the Department of Defense launched the first computer emergency response team.

A flaw in the program caused it to multiply much faster than anticipated and revealed its presence in computer systems. When Morris realized the worm was out of control, he contacted two friends. One friend sent out an "anonymous" apology across the internet on behalf of Morris. The other friend called *The New York Times*, stating the initials of the person who wrote the program was RTM. It did not take long for *The New York Times* to figure out the culprit was 23-year-old Robert Morris. The FBI launched an investigation into Morris and his friends.



In 1991, Robert Morris received the first conviction in history under the 1986 Computer Fraud and Abuse Act. His sentences were three years in prison, 400 hours of community service, and a $10,000 fine. He never served prison time and was only given parole. Morris went on to earn a Ph.D. and is now a professor at MIT, the very institution where he initiated the attack.

- A special exhibit in the Computer History Museum in Mountain View, California, contains the original floppy disks of the Morris Worm. This case was not only the beginning of thousands of computer hacks, but it also marked the launch of the cybersecurity industry. Next time you leave your tablet, laptop, or phone on, consider this quote from Spafford, "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards and even then I have my doubts."[120]

Every email, text, digital photograph, social media post, etc., leaves behind trace computer signatures — signatures containing unique identifiers that point to the author and user.

"I am somewhat exhausted; I wonder how a battery feels when it pours electricity into a non-conductor?"— Sherlock Holmes[121]

Computer forensics (cybercrime) is a field dedicated to the search, preservation, and analysis of information computer systems with the goal of presenting evidence to the court. In the forensics discipline, this is one of the fastest growing fields of investigation. A survey conducted in 2018 found that almost 33% of adults in the U.S. had experienced a hack of their social media and/or email account, with an over 362.5-million-dollar loss in scams.[122] Computer forensics includes the investigation of computer hard drives, CDs, DVDs, thumb drives, deleted files, encrypted files, email, chats, social media, cache, bookmarks, and more. Analysts use Computer Forensic Tools (CFT) to collect data from computers, copy the information, and locate hidden data.

COMPUTER FORENSICS FROM A BIBLICAL WORLDVIEW

Though there is no direct computer-related terminology in the Bible, God's Word clearly states multiple times that all things were created by Him. "All things" include the raw materials needed to build computer systems, the intelligent minds that develop computer software and hardware, and the complex, orderly mathematical processes necessary for computer operation.

And the Bible does mention technology. A variety of tools and technology would have been necessary for humans to achieve the architectural wonders described in the historical record in the Bible. Genesis 4:17 states that Cain built a city, and verse 22 says that Tubal-Cain was a user of bronze and iron. Genesis 6 describes the dimensions of the Ark, and Genesis 11 tells of man's self-glorification through a collective effort to build a tower. The book of Nehemiah describes how Nehemiah rebuilt the great wall in Jerusalem. Jesus Himself was a carpenter and would have used tools and technology in His trade. The Bible was written by the hands of men inspired by the very Word of God. In the Bible lies truth, and just as a computer requires a programmer, creation requires a Creator.

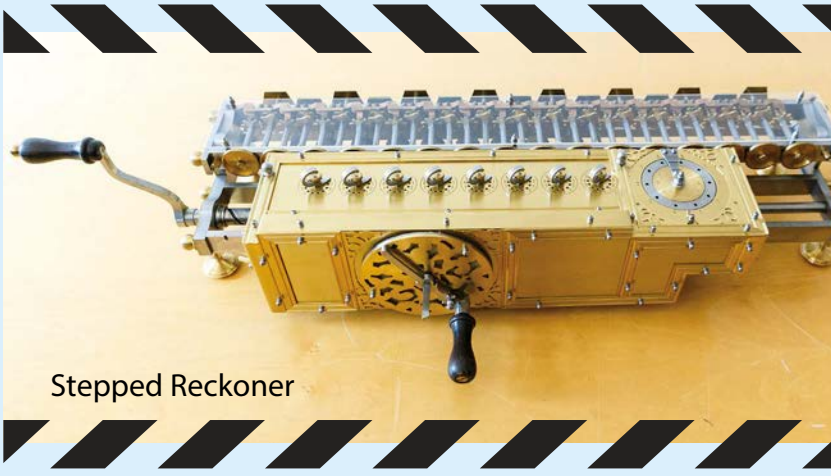
Data structure:

A method of organizing information (data) in the virtual system of a computer. Data structures and algorithms work hand-in-hand to build computer programs.

HISTORY

Computer history includes the development of computer language, hardware, software, and network connections. Each one of these components is necessary for a computer system to connect, collaborate, and process information.

Binary Language. The precursor to the binary code used in computers today originated between the 2nd and 3rd centuries B.C. Pingala, a mathematician from India, developed a binary numeral system. Though he did not use "0" and "1" like the modern system, he used light (*laghu*) and heavy (*guru*). The systematic process he used is very similar to the binary code used today.[123] In the 1700s, binary logic was formalized by German mathematician Gottfried Leibniz. He used 0 and 1 to represent commands. Leibniz also invented a calculating machine called a Stepped Reckoner that could add, subtract, multiply, and divide.[124]



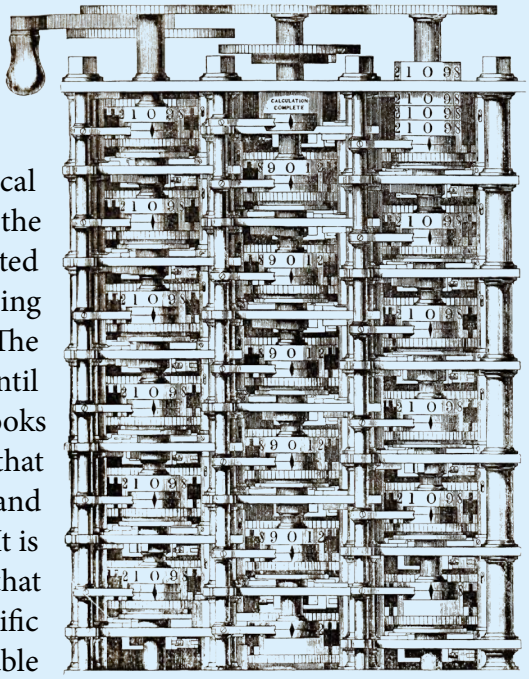
Stepped Reckoner

Algorithms. Algorithms are the step-by-step instructions that define a set of procedures that must be carried out in specific order to obtain a desired result. Algorithms serve as the underpinnings that operate computer programs and are organized by a data structure. Algorithms are derived from algebra, which was first introduced in the 7th century by Brahmagupta, an Indian mathematician. "Algorithm" is a term derived from *Algoritmi de numero Indorum*, the Latin translation of a work by the 9th-century mathematician al-Khwarizmi.

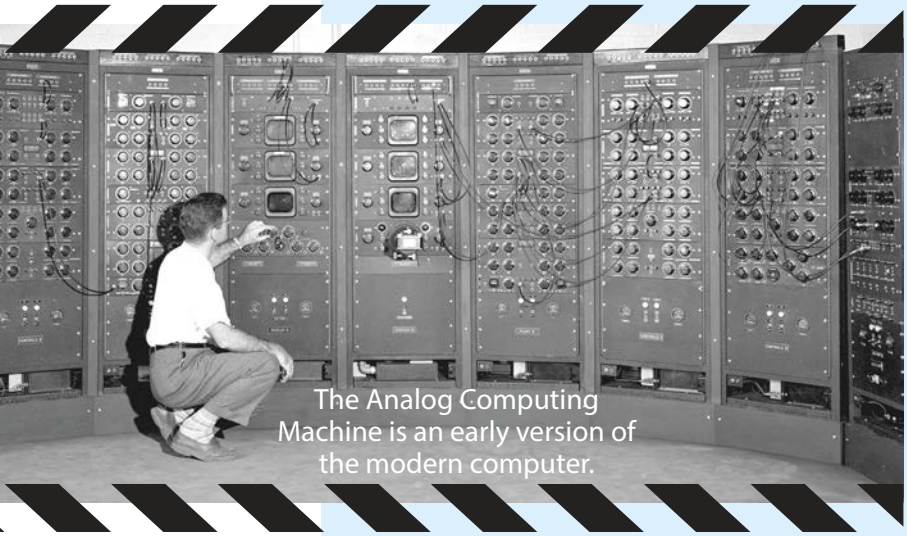
Computers. Charles Babbage invented the Difference Engine in 1823, which performed computations up to eight decimals. In the 1830s, Babbage outlined plans for the Analytical Engine, considered to be the forerunner to the modern computer.[125] Though Babbage worked on the Analytical Engine for the rest of his life, the machine was never completed due to the cost of producing new hardware components. The machine was forgotten until 1937, when Babbage's notebooks were discovered. It is important to note that Charles Babbage was a devoted Christian and attributed his study to the Creator God. It is said of Charles Babbage, "[He] believed that the study of the works of nature with scientific precision, was a necessary and indispensable preparation to the understanding and interpreting their testimony of the wisdom and goodness of their Divine Author."[126]

Analog computer:

A non-digital computer that analyzes data directly without converting into numerals or codes.



Difference Engine



The Analog Computing Machine is an early version of the modern computer.

With the discovery of Babbage's personal notes, the Analytical Engine No. 2 was built and accurate up to 31 digits. The first computer programmer was Ada Lovelace, who worked closely with Babbage and published the first algorithm to be carried out by the Analytical Engine.

The field of computer forensics began in the mid-1940s, when the age of analog computers (left) was going to be replaced by digital computers. The first microprocessor was invented in the 1960s. The first computer crime to be prosecuted was in 1966, but the emergence of what is considered computer crime today resulted from the invention of the home computer in the 1980s. The Morris Worm in 1988 (described in the case study at the beginning of the lesson) brought to the forefront the need for cybersecurity forces. As a result, by the early 1990s, law enforcement agencies across the country had implemented protocols for the investigation of computer-related crimes.

HARDWARE AND SOFTWARE

Hardware is defined as a device that is physically connected to a computer. Software is the computer programs that perform tasks on the operating system. The primary differences between hardware and software can be reviewed in **Table 1** below.

Table 1	Hardware	Software
Types	Input Storage Processing Control Output	System software Programming software Application software
Function	Delivery system Infrequently changed Dependent on software	Perform tasks Easily changed, updated, modified Dependent on hardware
Examples	Hard drives, monitors, printers, CD ROM, video cards	Microsoft® Word, Keynote®, QuickBooks®, Adobe®, internet browser
Nature	Physical	Logical[127]

COMPUTERS

Every computer consists of three main components: the CPU (Central Processing Unit), RAM (Random Access Memory), and the control bus. The CPU is the brain of the computer and controls the processing of any and all information. How fast information moves through the control bus is determined by the CPU. The four basic operations of the CPU include fetch, decode, execute, and store.[128] RAM is short-term memory. When a Microsoft® Word document is open on a computer, it is a visual representation of what is currently stored in RAM that a user is accessing. But as soon as that file is saved permanently, it moves to long-term storage on a physical disk (hard drive, USB, SD card, etc.). The control bus is the communication pathway between the data, the hardware, and the software. The control bus is located in the system board. To understand a control bus, imagine the traffic lane a school bus travels for student pick-ups and the route it takes to arrive at the school, or the central nervous system in the human body as the nerves detect sensory information and carry it back to the brain. These pathways are similar to the control bus, controlling the movement of information throughout the computer. Computers can also be extended with additional hardware like a Network Interface Card (NIC), which is a circuit board. This allows the computer to connect to a network. NICs work in both wired and wireless formats.

OPERATING SYSTEM

The operating system (OS) is the essential software that serves as the interface, or bridge, between the software and the hardware.[129] A computer cannot function without an operating system. The operating system controls the input and output, file management, memory, commands, resources, and security. The OS uses a series of drivers that allow the application software to talk to the hardware. An example would be pulling up a social media app (which is the application software) on your mobile device (which uses a mobile device operating system) and taking a picture with your camera (which is a piece of hardware).

FORMATTING

Format is the instructions for an operation system to read and write to a drive (physical device you put data on). Formatting is the preparation of the drive to receive the set of instructions (or format). Basically, it is a file system or layout to allow data to be written. During the formatting, a set of instructions on how to read and write data to a system, its restrictions and limitations, is provided to the operation system.

For example, one cabinet in a kitchen is usually designated for dishes. The dishes are organized by type and size of dish (big and little plates, big and little bowls, platters, etc.) while being confined to the size of the cabinet. Or a student is assigned a research paper, and the teacher requires a certain format — Times New Roman type, size 12 font, 1-inch margins, 1,000-word length, etc. The text must fit within this required format. Just as you can organize your dishes or prepare a research paper according to a specific size and shape, your computer has to be able to format data in a specific way in a specific place according to the space limitations provided.

When a hard drive is formatted, the platter (flat circular piece of metal), which is coated with iron oxide or chromium dioxide (magnetic substances), spins. While spinning, a read/write device sends small amounts of electricity through the head of the device, magnetizing the platter. Binary code, in the form of 0's and 1's, records the data on the hard drive.[130]


platter

ERASING DATA

There are four different terms that are associated with erasing data on computer systems. Those are reformatting, wiping (deep formatting), shredding, and erasing. Though they are often used interchangeably, they are distinctly different in their overall function. Each one presents a unique set of challenges to a forensic investigator.

Reformatting. When someone reformats their computer, or essentially attempts to erase current data and replace with a new set of instructions and new data, residual data still remains. Residual data is traces of data that remain on a system. Imagine an old-fashioned chalkboard. When you erase a chalkboard, there are usually visible letters, sentences, or numbers remaining. Often with chalkboards, it requires multiple erasure attempts or a wet wash to remove the data. A drive retains residual data in much the same way. A shadow of data still remains on the system. Multiple formatting attempts will continue to reformat or clean the system. Forensic computer analysts will attempt to retrieve this residual or shadow data for information regarding the criminal case using data recovery software.

Wiping (Deep Formatting). Wiping attempts to permanently delete records and makes recovery almost impossible. During this process, data is overwritten with new data. As with formatting (or wiping a chalkboard), multiple wipes are required to ensure the data is irretrievable.

Shredding. When you feed a piece of paper through a shredder, it slices that paper into hundreds of little strips. A similar device is available for computers. A physical shredder can be used to destroy the hard drive and the data remaining on the device. There are also digital shredders. A digital shredder erases portions of a hard drive, but instead of replacing it with structured data, it replaces it with random data.

Erasing. Erasing means to permanently eliminate any attempt to retrieve data. There are three methods to achieve this goal: using a destructive wiping (deep formatting) program described above, degaussing, or physical destruction. Degaussing is to use a magnetic field to neutralize (erase) the data on a device. It does this by removing the magnetic properties existing in the iron oxide or chromium dioxide. Degaussing results in a permanent erasure or randomization of files.


data erasing

THE INTERNET

The birth of the internet began in the 1960s as scientists and military experts, worried about foreign breaches of information, developed a method of communication separate from the telephone. They discovered a way for computers (the size of a small house at the time) to talk to one another by a method called packet switching.[131] By 1970, four computers were now connected to the new ARPAnet (Advanced Research Project Agency Network). Now move forward to the late 1970s, when a computer scientist named Vinton Cerf invented the TCP (transmission control protocol). The TCP/IP is the "handshake" that allows different computers to communicate.[132] Cerf's invention provided the needed mechanism for the worldwide network, which allowed files to be interchanged around the world. The year 1991 was important to the history of the internet. Tim Berners-Lee, a computer programmer, introduced the world to the internet. No longer was it limited to file exchange, but virtual access was now open to everyone. The first search engine was developed in 1992, as well as the ability for companies to create websites. Over 230 nations are now connected to the internet.[133]

Packet switching:

A digital network transmission process in which data is broken into bite-sized pieces or blocks of information for fast, efficient transfer through network devices.

The ability to search topics on the internet is a resource that has opened the door to easy knowledge acquisition. When a topic is searched on the internet, the computer begins to record information (artifacts) about that search, such as browser history, bookmarks, IP addresses, storage in the cache, and permission access to cookies. Each of these terms are described below.

- *Browser history*: a record of the website addresses that the computer has recently visited and any data associated with the websites. Browser history retains information about search queries, logins, passwords, social networks, and financial information.
- *Bookmark*: a shortcut to a particular website. Just as a page in a book can be bookmarked by folding the corner of the page down or using a paper bookmark, an electronic bookmark saves a web address to your profile.
- *IP addresses*: fundamental protocol for communication on the internet. It determines how information is packaged, addressed, transferred, and routed by networked devices. It is an address that points to a location on the internet.
- *Cache*: temporary storage that retains information about browser history, frequently visited sites, and search terms in a file cache. The cache stores downloaded images, videos, documents, and files.
- *Cookies*: a piece of data inside the browser that gives feedback about the user to the server. Cookies mark and track information and are software that lives in the browser. For example, a user will search a certain product or be talking about specific merchandise on or near their computer, only to discover later that afternoon that the exact product is now offered to them in the computer ads popping up on their screen.

A computer forensics investigator will conduct a thorough examination of all related activity mentioned above. Web browsers offer the ease of integration between browser service and synchronization of passwords, and users unknowingly save important information, like their interests, personal life, and future plans. The history in the computer browser is stamped by date and time and provides a timeline for investigators. Even when a user attempts to delete internet history and cache data, it is likely the data remains. Often, no data is actually removed from the hard drive and, even when deleted, is retrievable. Though computer history and frequently visited webpages are only circumstantial evidence, it does provide supporting documentation of intent to commit a crime. For example, in 2009, Krenar Lusha of the U.K. was arrested based solely on his internet searches. Investigators monitored key word searches from Lusha on how to make explosives; investigated his downloads, which contained manuals on building explosives; and reviewed his chat session, which revealed he referred to himself as a terrorist. This evidence helped to convict Lusha, and he received seven years in prison.[134]

Email. The ability to email messages and files from computer to computer transformed the world. There is debate over who invented the email delivery system. Some say it is Ray Tomlinson, who in 1971 created a system of communication for the ARPAnet system discussed earlier. Others give credit to Shiva Ayyadurai, who claims to have written a program in high school called EMAIL in the late 1970s. Regardless of the true inventor, since 1971, email has evolved into over 2.6 billion active users and is the most used form of communication for personal and professional use. Email-related crimes include phishing, spam, harassment (threats, doxing, or other abusive language), illegal (pornographic) images, and sensitive information (e.g., banking information, medical records, etc.).[135] Email investigation is challenging since the majority of email is not encrypted. The primary goal in computer forensics is to verify the sender and receiver of the email by means of the email header. The header contains information regarding the pathway in which the email traveled, but this can be easily manipulated by a knowledgeable user.

Encryption:

The process of encoding information from plaintext to ciphertext.

Instant Messaging. Instant messaging (chat) crimes are similar to those of emails, except whereas email can be delayed by hours or days (dependent upon when the email is opened), instant messaging is in real-time. Difficulty in investigating instant messaging crimes is due to the different platforms' methods of time stamping, the location of system folders, which vary according to operating system, and the storage fluidity of historical information.[136]

Servers. Information is not only stored in the memory of personal or business computers, but on servers as well. Servers are virtual filing cabinets that store information. Whereas in the past, servers simply sent and received messages, their role has drastically changed. Servers now function as collaborative tools that monitor databases and store documents, contacts, etc. When a terrorist searches, "How do I build a bomb?" on the internet, a series of events occurs. As the terrorist types and hits the search button, the computer will begin to store that information, any websites visited, permission access in the form of cookies, etc. Additionally, that information is sent to the offsite server that hosts the internet service. The Communications Assistance for Law Enforcement Act passed in 1992 allows law enforcement to "conduct electronic surveillance while protecting the privacy information outside the scope of investigation." The law goes on to state that communication companies are required to have "all necessary surveillance capabilities to comply with legal request for information."[137] There are hundreds of varying servers monitoring information, such as web servers, email servers, proxy servers, and identity servers.[138]

Media (CD & DVD) and USB Drives. CDs (compact disc) and DVDs (digital versatile disc) are optical discs that read and write information. DVDs have the capability to store significantly more information than a CD and provide information on both sides of the disc. Recovery of information on DVDs and CDs is often challenging due to the variety of file system formats. Professional data recovery software is available that will not only read all system formats, but is also equipped with CD imaging and the ability to report over 50 data items.[139] A USB (universal serial bus) drive (thumb drive or flash drive) is a small, durable device used for data storage that can only operate when plugged into a USB port. Compromised USB drives contain malware that can infect a computer system. God created humans to be curious, but it is never wise to insert a USB drive from an unknown source into a personal computer.

SECURITY

Computer security protects computer systems from theft, unauthorized access, and security breaches. Computer security is a top concern among businesses due to the number of data breaches that continue to occur on a regular basis. Computer hackers have cost consumers and business owners billions of dollars. The Yahoo!® data breach that occurred between 2013 and 2016 resulted in over three billion compromised personal records and billions of dollars in damages.

There are a variety of protections available to guard information stored on a computer hard drive or in virtual locations such as clouds. But it is important to recognize that computer hackers are on the forefront of technology and are continuing to find ways to bypass the latest updates in computer security. The seven layers of cyber security are laid out similar to an arc, with humans providing the ultimate shield of protection.

THE 7 LAYERS OF CYBERSECURITY

Humans. Humans are the preeminent layer to computer security. Humans ultimately are the number one key to the protection of personal and business information. Human error and failure to follow security protocols are the primary reason for computer crimes. Human cybercrime falls within these categories:

- *Phishing*: an email disguised as professional in which the user is requested to provide passwords, address, telephone number, etc.
- *Ransomware*: hackers access computer files and lock the user out, often demanding ransom to regain access.
- *Webcam managing*: hackers hijack the user's webcam in hopes of watching the user's keystrokes for passwords, conversations, and other data.
- *Screenshot managing*: hackers access the user's screen and take screenshots of passwords, etc.
- *Keylogging*: hackers record the user's keystrokes to decipher passwords, etc.
- *Ad clicking*: hackers display advertisements that may entice the user to click on an ad and open malware.

Perimeter. Authentication methods validate a person's access to the system. When a user logs into their email account, the provider authenticates their permission to access the system. Due to security breaches, many websites and emails have instituted multifactor authentication. Multifactor authentication requires two or more pieces of evidence to receive access to a system. Evidence may include passwords, email codes, text codes, personal information, etc. This verification through authorization validates the authentication. An example of perimeter security is passwords. Passwords are a set of characters, words, numbers, etc., that are used to authenticate user access to a digital system. Passwords ensure the user has permission to view or access information.

Network. A computer network is a group of computers, using similar protocols, that are connected to one another for the purpose of communicating data electronically. A network is capable of instituting a series of security protocols to protect the information of the computers connected to its system. An example of network security is firewalls. Firewalls prevent unauthorized access to specific devices, such as hardware or software, and protect from people trying to get into the computer system. Based upon a set of security rules, a firewall will either allow traffic to access or block information on a computer or network. Another example of network security is a Virtual Private Network (VPN). When an individual uses a VPN to connect to the internet, your request is encrypted and it masks your location.

Endpoint. This is the breaking down of a network into individual systems. An example of endpoint security is Google® allowing the user to access the public tools, such as Google Docs™, Slides™, and Sheets™.

Application. This refers to individual authorization within a single application or service. For example, a college presentation group project has been assigned by a professor, and the group decided to use Google Slides™. Google Slides™ is hosted on the internet. Each user will have to be granted access to use the individual application, Google Slides™ from Google®.

Data. Data is an extension of application security and allows an individual to grant access to files for the purpose of modifying those files. Refer back to the group Google Slide presentation. The creator has full control of the presentation, but the other members of the group need to be granted access to read, write, and update data. Data security permissions allow authorized individuals to change, delete, or copy the individual files.

ANTI-FORENSIC TOOLS

Even with the development of computer security measures to counteract cybercrime, there is a continual and steady increase in breaches of sensitive information. By the year 2024, there is an expected 70% increase in cybercrime, as well as an estimated cost of $5 trillion due to breaches of information.[140] Almost on a daily basis, the FBI website publishes another arrest related to cybercrime. One of the issues facing law enforcement is the use of Anti-Forensic (AF) tools, which have the ability to erase and alter information, create "chaff" that hides information, plant fake evidence, and leave tracer data that prevents computer forensic software from revealing hacker information.

Chaff:

Worthless information designed to lead an investigation awry.

There are four goals for AF tools:

1. Avoid detection.
2. Disrupt the collection of data.
3. Increase the period of time allotted for investigation.
4. Cast doubt on forensic testimony.

The use of AF tools does not completely eliminate the possibility of identifying criminal activity or traceable information, but it does impede investigations and increase the time frame for analysis and resolution.

CYBERCRIME INVESTIGATION

Computer crime investigations fall within both criminal and civil court cases, but the method of investigation varies between the two types. A computer forensic analyst may be utilized for either scenario.

I. Criminal Computer Forensic Investigations
1. Law enforcement obtains a search warrant and secures the computer. The Fourth Amendment to the Constitution provides protection against unreasonable search and seizure. A search warrant is required to seize and search not just the computer, but the files as well. The warrant must specify the exact information (and potential files) the investigators are looking for on the machine. They cannot just randomly search a suspect's computer. Securing the computer by preventing any unauthorized access is the key to evidence integrity and court admissibility. Search and seizure include the correct storage, labeling, and chain of custody as outlined by the law enforcement agency.
2. Identify and copy all files on the system by using Computer Forensic Tools (CFT). This includes deleted, encrypted, protected, and overwritten files. Difficulties occur within this area of computer forensics. Once detectives begin opening computer files, there is no way to verify they did not change anything, and it can be contested in court. Documentation of every single step and every single piece of evidence is essential to maintain integrity.
3. Examine unused or hidden storage space on the computer.
4. Document every step of the investigation and maintain chain of custody.
5. Prepare for courtroom testimony.

Ultimately, a conviction in a criminal investigation will result in incarceration, parole, community service, criminal record, or other form of criminal punishment.

II. Civil Computer Forensic Investigations
1. A private investigator is hired to investigate a dispute or lawsuit claim. Search and seizure do not apply in this situation; instead, the party negotiates a time and place for the investigator to examine the related computer materials. If the private investigator is provided access, then they will follow similar protocols regarding CFT, copying, etc.
2. Interview all involved parties in the investigation.
3. Since the private investigator does not have the rights and privileges of law enforcement, they may need to implement surveillance measures to gain information. Though they are permitted to eavesdrop on conversations, according to privacy laws, they are not permitted to record private conversations through a listening device.[141]

The resolution of a civil court case results in some form of monetary payments, a service, or property.

CONCLUSION

The field of computer forensics is one of the fastest growing divisions in law enforcement. The expected increase in computer-related crime, in addition to the innovative methods of computer hackers, has established the need for knowledgeable computer scientists in law enforcement. A computer forensic scientist is required to have a bachelor's degree in computer science or criminal justice. Once hired within an agency, hundreds of hours of training and mentoring are required to prepare the analyst for independent casework and courtroom testimony. An expert in this field will be expected to understand the overall mechanisms and operations of computers; their relationship with virtual platforms, internet regulations, and networks; as well as enjoy the hunt for hidden, coded information. Considering humans are the weakest link in computer security, a computer forensic investigator must adhere to the strictest protocol and follow all departmental guidelines to ensure their integrity in the field. Integrity, professionalism, and character are all biblical traits that should reflect a follower of Christ. Even within this technical field, a person can give glory to the Creator of knowledge, and the One who is knowledge, Jesus Christ.