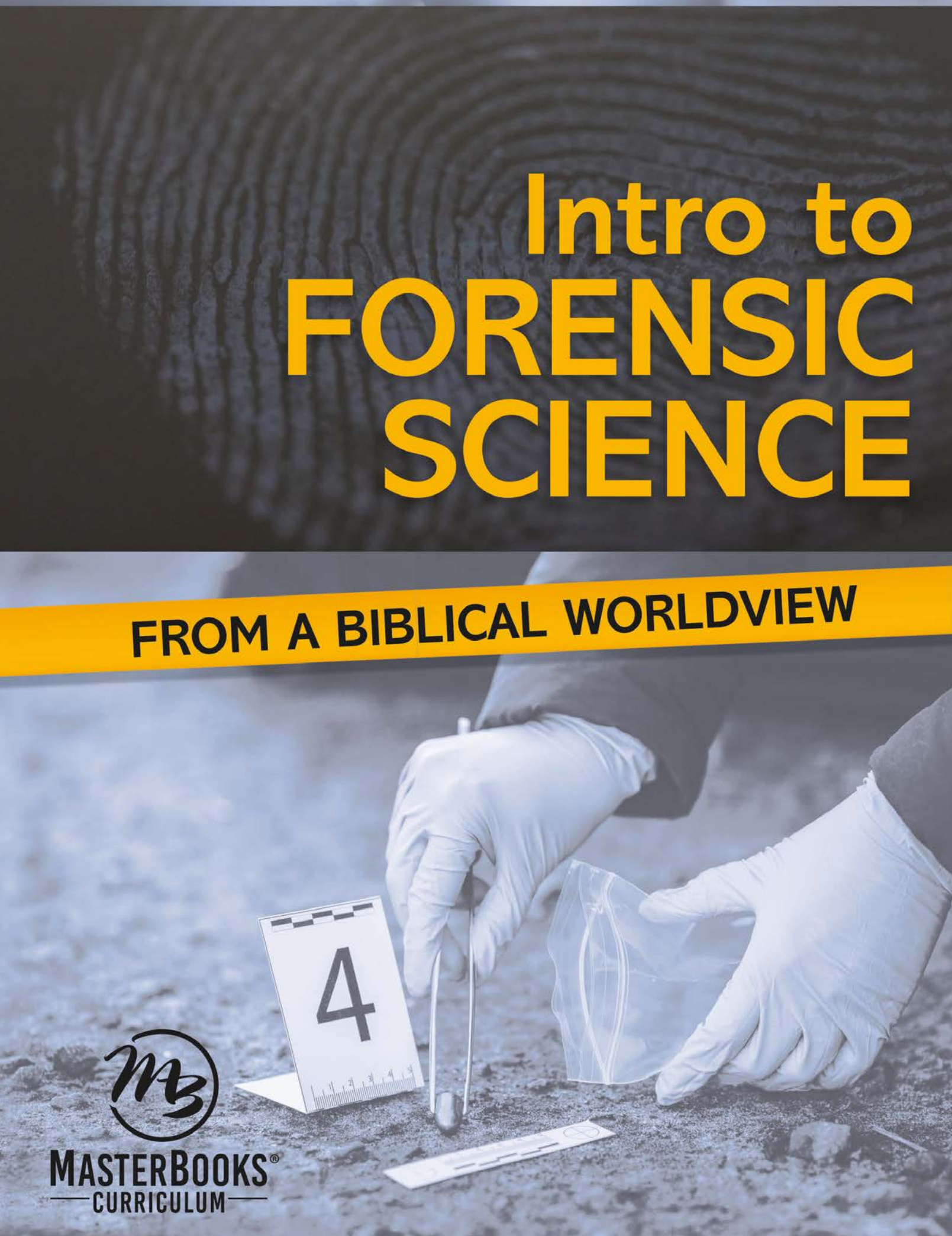
Intro to FORENSIC SCIENCE

FROM A BIBLICAL WORLDVIEW



MASTERBOOKS®
CURRICULUM

MASTERBOOKS®
CURRICULUM

Curriculum Development:
Kristen Pratt

Editor-in-Chief:
Laura Welch

Editorial Team:
Craig Froman
Willow Meek
Judy Lewis

Art Director:
Diana Bogardus

Design Team:
Diana Bogardus
Terry White
Jennifer Bauer

Content Review:
Ron Smith and Associates, Inc.

First printing: May 2023

Master Books, P.O. Box 726, Green Forest, AR 72638
Master Books® is a division of the New Leaf Publishing Group, LLC.

ISBN: 978-1-68344-241-7
ISBN: 978-1-61458-802-3 (digital)
LOC: 2023933564

Printed in the United States of America.

Please visit our website for other great titles:
www.masterbooks.com

For information regarding promotional opportunities, please contact the publicity department at pr@nlpg.com.

About the Author

Jennifer Hall Rivera EdD is the Director of Educational Programs for Answers in Genesis, where she oversees and presents in daily workshops and is involved in educational outreach and the high school lab programs. Her interest in the forensic sciences started at an early age and is credited to the godly instruction of her father, a renowned fingerprint expert. Her experience in the field of forensic science includes employment in a crime scene unit, over a decade of teaching, journal publications, and numerous speaking events.

TABLE OF CONTENTS

DEDICATION AND THANK YOU

This book is dedicated to my hundreds of students who, over the years, have wished there was a forensic science textbook from a biblical worldview; and to all future students who are interested in pursuing this fascinating career. Science confirms the Bible, and this is clearly seen in the study of forensic science (Romans 1:20).

Thank you to my husband Michael, Dr. Dana Sneed, Dr. Georgia Purdom, Mr. P (Roger Patterson), and Ron Smith and Associates, Inc., who assisted in reviewing content, capturing images, editing, and so much more. Your support and prayers are greatly appreciated.

FOREWORD

Forensics is a scientific discipline that captures the attention of many young people. It's been made popular by a plethora of TV shows (some more based in reality than others!). My own daughter, while not very interested in science, enjoyed taking forensic science in high school. I homeschooled her and I remember the frustration of choosing a textbook because at that time one didn't exist that taught forensics from a biblical worldview. I was thankful she was able to attend the forensic science high school labs taught by Dr. Jennifer Rivera at the Creation Museum in Petersburg, Kentucky. Dr. Rivera has drawn on her extensive knowledge and experience as both a forensic scientist and educator to develop and write a forensic science textbook that is both factual and practical.

One of the things that makes forensic science unique is its very observable application to real life. Students don't have to wonder how this science would ever be something that's important because it's used every day by police officers and investigators to solve crimes. As God's image bearers, we desire justice and for wrongs to be made right, and forensic science helps accomplish that. I also appreciate that forensic science encompasses many sub-disciplines like chemistry, entomology, botany, genetics, etc., and students can see how all the sciences work together and build on each other.

I'm thrilled that students and teachers alike will now have this tremendous resource to learn forensic science from a biblical worldview. It's filled with not only the facts of forensic science but also real-life case studies and labs that help students apply what they've learned. It's a great opportunity to get students engaged in science!

Georgia Purdom, PhD

Vice President of Educational Content

Answers in Genesis

IMAGE CREDITS

L = left, T= top, TL = top left, B=bottom, BL = bottom left, C = center, CR = center right, CL = center left, R = right, TR = top right, BR = bottom right, BC = bottom center

Getty.com: p 7, p 26 (2), p 28, p 29 B, p 30 (2), p 31 T, p 32 B, p 33 (5), p 34, p 54

Shutterstock.com: p 5, p 8 (2), p 9, p 11, p 14 (2), p 15 B, p 16 (3), p 17, p 20 T, p 21 (2), p 22 (2), p 23 T, p 24 (2), p 29 T, p 30 C, p 35, p 36 (2), p 38 (2), p 39, p 40 (2), p 41, p 42 (2), p 43 B, p 44 (3), p 46 T, p 49 (2), p 50 B, p 51, p 53 (2), p 55 (2), p 56 (2), p 57, p 59, p 60, p 61, p 62 (3), p 63, p 65, p 67 (5), p 72 (2), p 73 (2), p 77, p 78 (2), p 79 (3), p 80 (3), p 81 (2), p 82 T, p 83, p 89 B, p 92 (2), p 93 (2), p 94 B, p 95, p 96, p 98, p 99 T, p 100 T, p 101, p 102 (2), p 103, p 104, p 105, p 106 (2), p 107 (2), p 108, p 109, p 110, p 112 (2), p 113, p 114, p 115 B, p 117 C, p 118 (2), p 119 C, p 120 B, p 121 (2), p 122 (3), p 123 (2), p 124 (2), p 125 (2), p 126 (2), p 127, p 129 (2), p 130 T, p 132, p 133 (3), p 134 (2), p 135 T, p 136 (2), p 137 B, p 138 (2), p 140 B, p 141, p 143 (2), p 144 (2), p 145, p 146 (2), p 147, p 148 (2), p 149 T, p 150, p 151 (2), p 152, p 153, p 154, p 155,p 157 (2), p 158, p 159 (2), p 160 (6), p 161 (4), p 162 (2), p 163 (4), p 164, p 166 R, p 168, p 169 (2), p 170 (4), p 171 (5), p 173, p 174, p 175, p 176, p 179, p 180, p 181 B, p 182, p 186 (2), p 187, p 188, p 189 (2), p 190 (2), p 192 T, p 193 (3), p 194 T, p 196, p 200 L, p 201 L, p 202 T,p 203, p 204, p 205, p 206 (2), p 207 BR, p 208, p 209 B, p 210 C, p 213, p 214, p 215, p 216, p 218 (2), p 219 (3), p 220, p 221 (2), p 222, p 223 (2), p 224, p 225 T, p 226, p 228, p 229, p 231, p 233 (2), p 234 (5), p 235 (6), p 236 (4), p 237 (3), p 238, p 239 (4), p 240, p 241, p 243, p 244 (2), p 245 (2), p 246 B, p 247 (2), p 249 (2), p 254 (2),p 255, p 257 (2), 259 (2), p 262 (3), p 263 (2), p 264 (2), p 265 (2), p 266 T, p 267 B, p 268, p 269, p 270 BL, p 271 B, p 272, p 273 (3), p 274 (7), p 275 (2), p 276 T, p 277 B, p 279 (2), p 280 (2), p 281 (T), p 282 (2), p 283, p 285, p 286 (9), p 287, p 288 (2), p 290 (2), p 291 (2), p 292 T, p 293 (5), p 294 (2), p 295 B, p 296, p 297, p 298, p 299 B, p 300, p 301, p 302 (2), p 303 (5), p 304 (2), p 305 B, p 306 (2), p 307, p 309, p 312, p 313 C, p 314 (3), p 315 (4), p 316 (4), p 317 (2), p 318 (2), p320 R, p 321, p 324, p 325, p 328 T, p 330 (2), p 331 (2), p 333 B, p 334 (2), p 335, p 337, p 338 B, p 343, p 344, p 345, p 347, p 348 (2), p 349 B, p 351, p 354, p 355 (2), p 357 (4), p 358 T, p 359, p 360 L, p 361 (2), p 362, p 365, p 367 B, p 368, p 369 T, p 371, p 372, p 373 (2), p 374 (2), p 375, p 376, p 377, p 378, p 379, p 381, p 382 (2), p 383, p 384, p 386, p 388, p 390, p 392, p 393 (2), p 395, p 397, p 398 T, p 399, p 401, p 402, p 405, p 406, p 407, p 409, p 410, p 411, p 412, p 413, p 415, p 416, p 417, p 418, p 420, p 421, p 422, p 424 (2), p 425

FBI Multimedia: p 192 (2), p 225 (2), p 227, p 241, p 340 C, p 341, p 358 B, p 360 R, p 364 T

iStock.com: p 262 CR, p 268, p 291 (2), p 326

Colourbox.com: p 131 B

Science Photo Library: p 117 B, p 183, p. 267 T, p 278 T

NLPG Staff: p 20 B, p 44 T, p 107 T, p 123 TR, p 246 (2), p 261 (2), p 273 (6), p 292 B, p 313 B, p 317 (3), p 419

J. Rivera: p 19, p 23 B, p 31 (2), p 32 (2), p 50 T, p 66 (2), p 67 TL, p 68 (2), p 69, p 76 R, p 80 (2), p 82 (3), p 87, p 91 (3), p 92 B, p 94 T, p 119 B, p 120 T, p 124 C, p 137 T, p 149 B, p 161 B, p 165, p 170 (4), p 171 (3), p 172 (2), p 181 T, p 184, p 193 T, p 194 B, p 195 (2), p 196 (4), p 197, p 198 (6), p 199, p 200, p 201, p 202 (2), p 207 (3), p 209, p 210 (3), p 211 (2), p 212 (5), p 215 (2), 232 (4), p 237 (3), p 248 (8), p 271 T, p 295 (2), p 312, p 369 (2), p 396, p 398 B, p 404, p 412

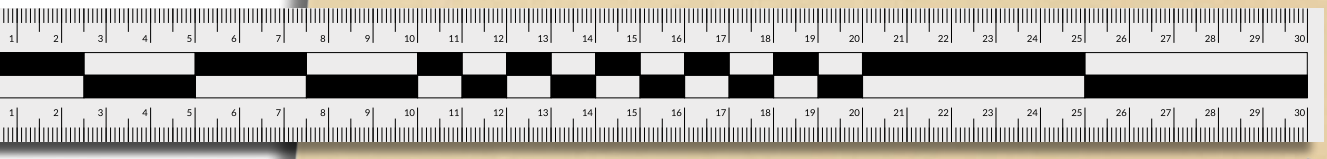
Answers in Genesis: p 20 B, p 74 (2), p 89 T, p 299 T, p 367 T

Library of Congress: p 340 T

Wikimedia Commons: p 12, p 13, p 15 T, p 26 T, p 27, p 36 C, p 37, p 43 T, p 46 B, p 47, p 52, p 67 TR, p 70 (2), p 71, p 75 (3), p 76 L, p 84 (2), p 85, p 88 (2), p 96 T, p 97, p 99 B, p 100 B, p 115 T, p 116 (3), p 117 T, p 118 (2), p 119 T, p 130 (2), p 131 T, p 135 B, p 139, p 140 T, p 154 (2), p 166 L, p 167, p 170, p 176 (2), p 177, p 190 C, p 191 (2), p 195 T, p 196 B, p 207 (4), p 209 T, p 210 (3), p 217, p 232 B, p 255, p 258 (3), p 264 TR, p 266 B, p 270 (2), p 273 C, p 276 B, p 277 (2), p 278 B, p 281 (B), p 288 B, p 289, p 290 T, p 291 B, p 294 B. p 299 T, p 305 T, p 308, p 313 T, p 316 BR, p 320 L, p 322, p 323, p 327, p 328 B, p 329 (2), p 332 (2), p 333 T, p 334, p 335, p 338 T, p 339, p 340 (2), p 342, p 346 (3), p 349 T, p 352, p 353, p 356 (3), p 360 TR, p 361 T (Karen T. Taylor, KTT), p 364, p 365, p 369 (2), p 370 (2), p 391, p 396, p 398 B, p 404

Images from Wikimedia Commons are used under the (PD-US), CC0 1.0, CC BY-SA 2.0, CC BY-SA 2.5, CC BY-SA 2.0 DE, CC-BY-SA-3.0, CC By SA 4.0, CC By SA 4.0 International, CC By SA Spain, license or the GNU Free Documentation License, Version 1.3.

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).

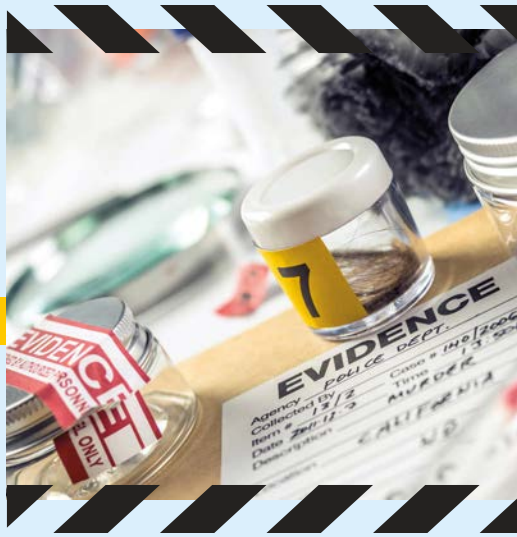
Psalm 111:2:

"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**).

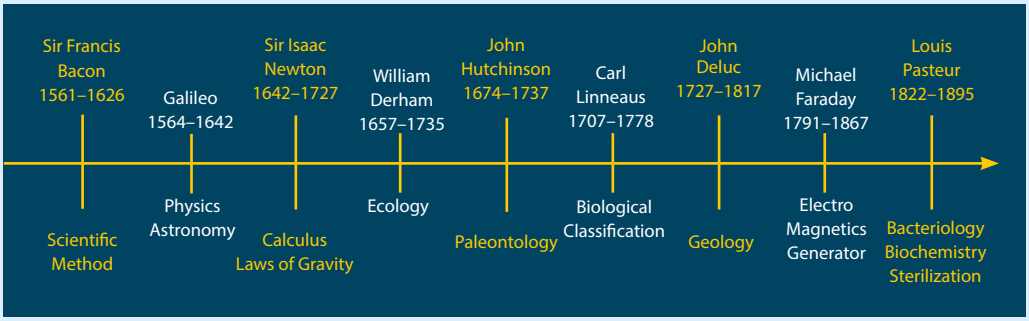
Table 1

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."

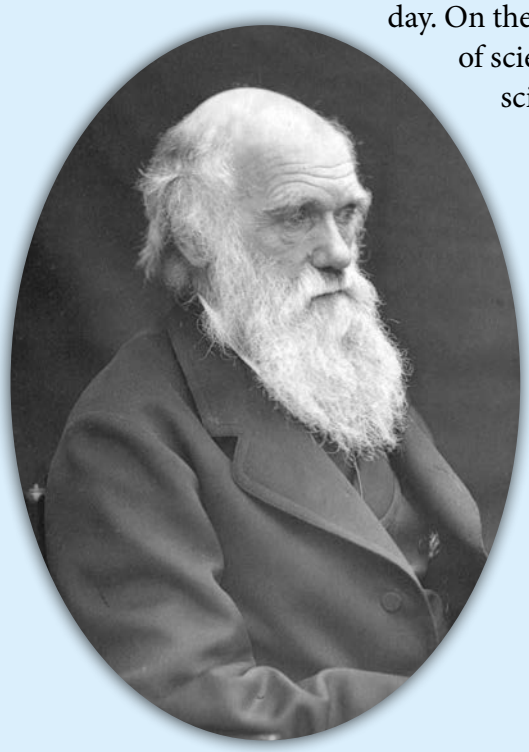
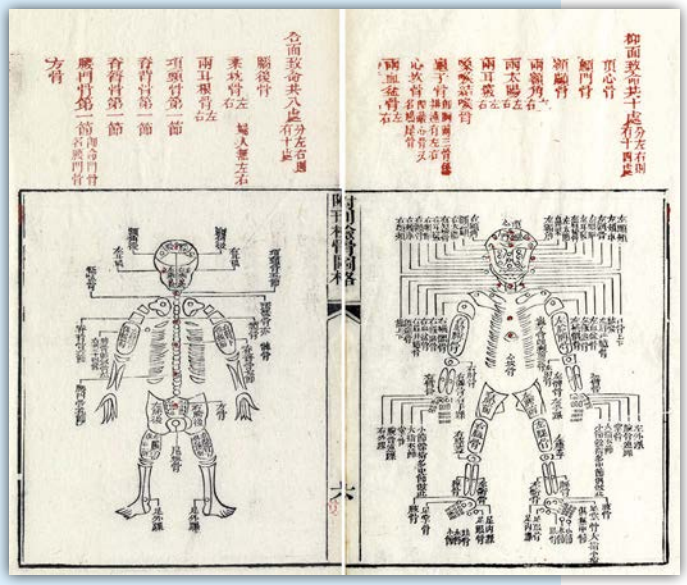


Table 3: Webster's Chronological Definitions of Science

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."

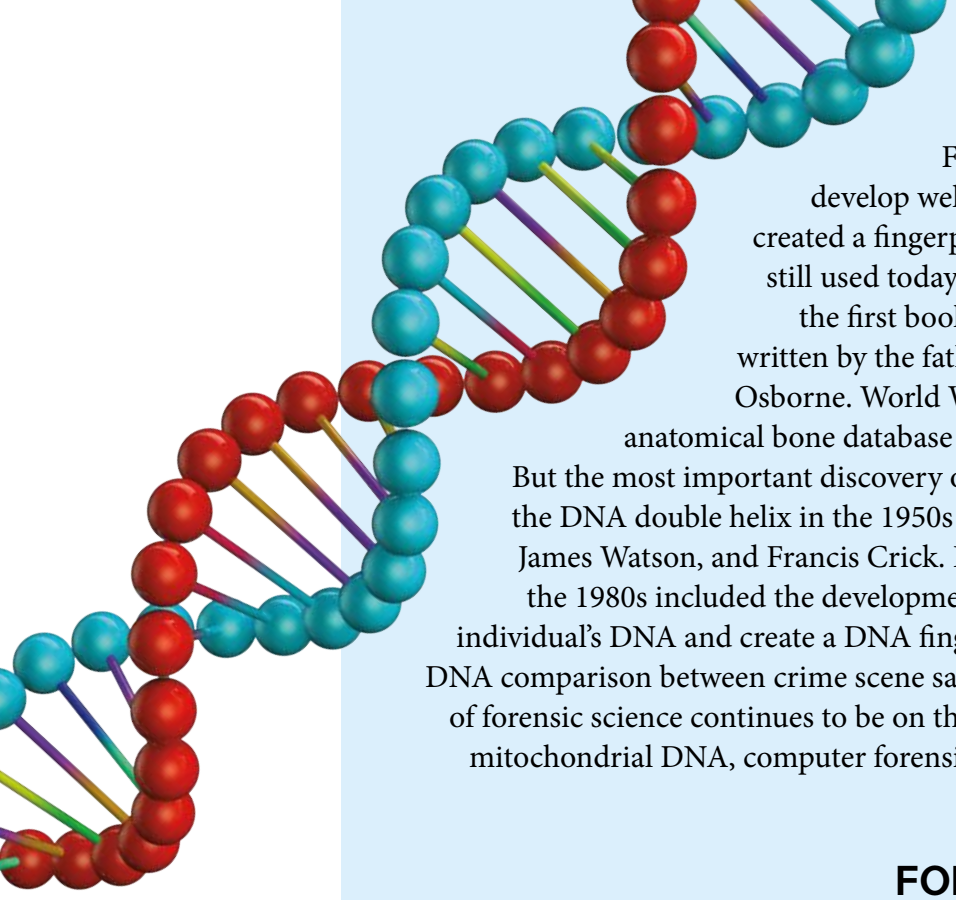


Xǐ-yuān lù jí-zhèng, 1843 edition

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.

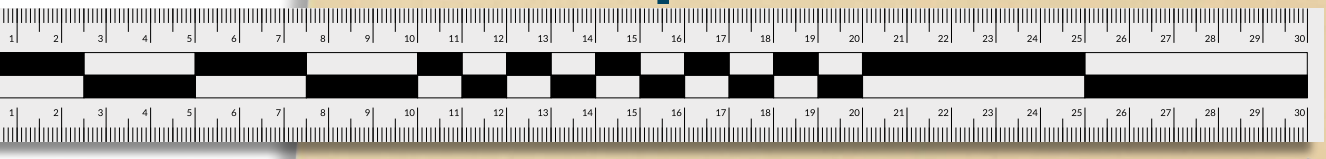
The FBI crime laboratory started in 1932 is one of the largest in the world and employs a variety of forensic experts. In addition to the fields already mentioned, the FBI employs:[16]

- 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

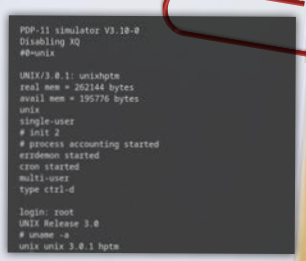
Case Study: The Morris Worm

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.

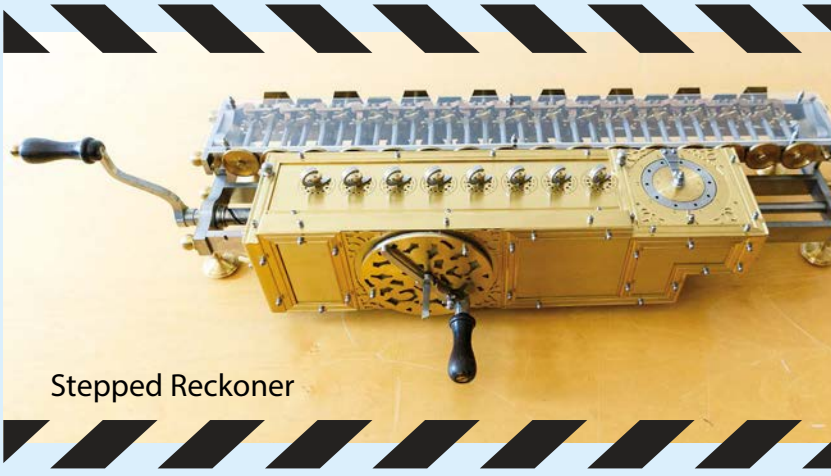
Data structure:

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]



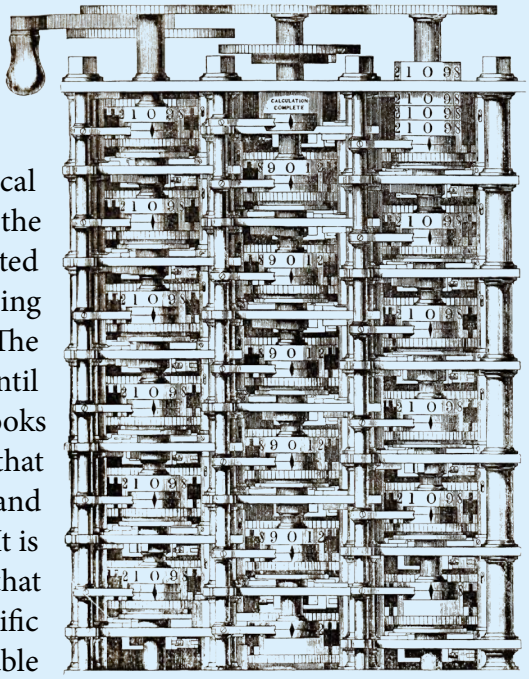
Stepped Reckoner

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.

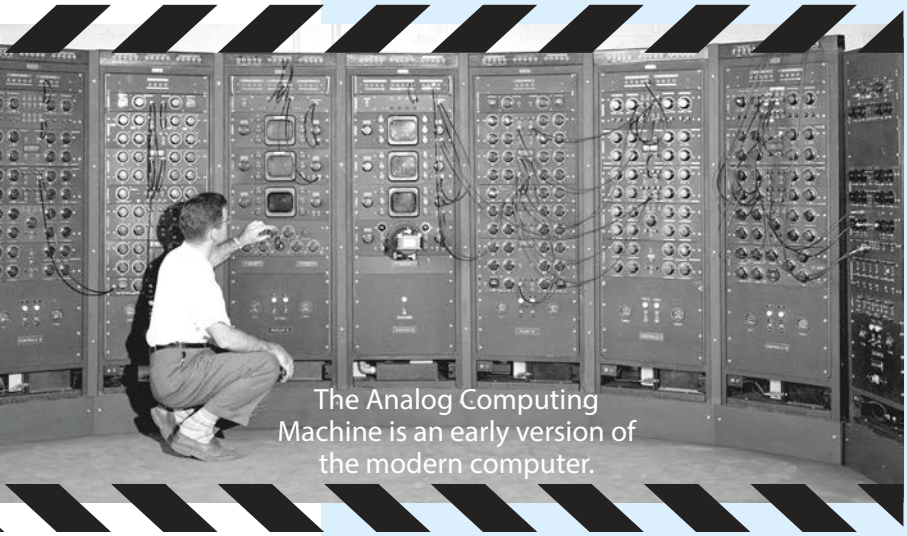
Computers. Charles Babbage invented the Difference Engine in 1823, which performed computations up to eight decimals. In the 1830s, Babbage outlined plans for the Analytical Engine, considered to be the forerunner to the modern computer.[125] Though Babbage worked on the Analytical Engine for the rest 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]

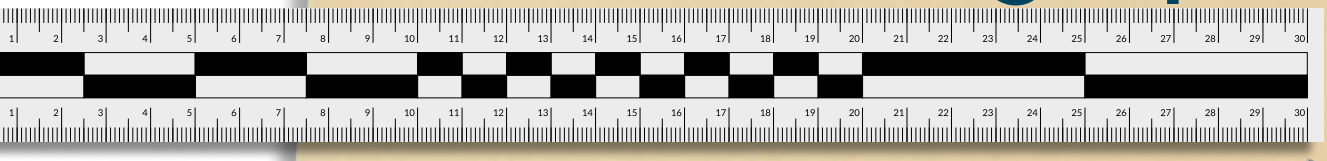
The resolution of a civil court case results in some form of monetary payments, a service, or property.

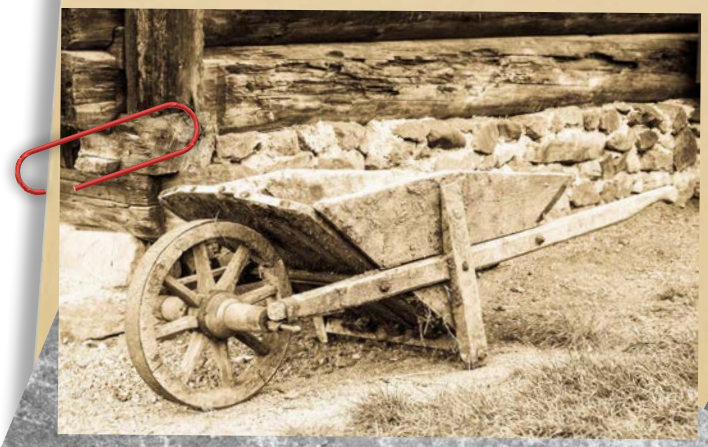
CONCLUSION

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.

Lesson 16

Human Fingerprints





I praise you, for I am fearfully and wonderfully made. Wonderful are your works; my soul knows it very well (Psalm 139:14).

CASE STUDY

Case Study: The Patent Fingerprints

Prior to 1900, fingerprints had never been used to convict a criminal in court in the United States. This changed in 1910, when the very first criminal case to use fingerprints as evidence resulted in a conviction using said evidence. Around 2:00 a.m. on September 19, 1910,[236] Thomas Jennings rolled a wheelbarrow under a window at 1839 West One Hundred and Fourth Street. Standing on the wheelbarrow and using a crowbar, Jennings pried open the window and entered the home of Clarence Hiller and his family in South Chicago. Jennings entered the bedroom of Hiller's daughters. The two daughters were alerted to the intruder and began screaming, which woke up Clarence. Clarence confronted the intruder, Thomas Jennings, and during the scuffle, both men fell down the staircase. Hiller's daughter Clarice told police she heard gunshots before Jennings fled through the front door. Hiller collapsed lifeless from two gunshot wounds at the foot of the stairs.[237] Sherlock Holmes so famously said, "To a great mind nothing is little."[238] In a case, the smallest detail is important.

Neighbors notified the police, who apprehended Jennings a few blocks from the Hiller home. Jennings gave the police a false name of William Jones. During the crime scene examination, Captain William F. Evans observed "fingermarks," an early term for fingerprints, on the front porch rail. The porch rail had been freshly painted. Clear, visible fingerprints were impressed into the wet paint. Impressed fingerprints in a soft surface that result in a three-dimensional impression are called plastic prints. Investigators cut the wood away from the rail and delivered it to the police station. Black powder was sprinkled over the impressed prints to make them more visible for examination. It was quickly discovered that William Jones was really Thomas Jennings, a convict and recent parolee.

Facts about the case:

- When police apprehended Jennings, his coat was covered in blood, and he was carrying a loaded revolver.
- Captain Evans was a fingerprint operator in the Bertillon identification system (also known as anthropometry). This case occurred during the period between Bertillon identification (identification based on body measurements) and the change to fingerprint identification.
- Captain Evans had a son named Emmett, who was also a police investigator. In 1904, Evans sent his son to the World's Fair in St. Louis to learn about the new technique of fingerprinting. He told his son, "I don't think it is any good but look and see."[239] Emmett returned with positive remarks for the new system of identification, and Chicago began collecting fingerprints from criminals in 1905.
- Captain Evans compared the fingerprints to those on file for the suspect and found 33 points of minutiae to be a perfect match.[240]

- Other than the three fingerprints (index, middle, and ring fingers of the left hand) left behind on the front porch rail, all other evidence linking Jennings to the case was circumstantial.
- Captain Evans was one of the first fingerprint examiners in the United States.

During the trial, Jennings' defense attorney, W.G. Anderson, questioned the veracity of fingerprint identification. In forensic science, it is difficult to enter new evidence into the courtroom proceeding if it does not have precedence in the system. In an attempt to disprove the uniqueness of fingerprints, the defense team acquired random fingerprints from the public to show that two people could have the same fingerprint patterns, only to discover that it backfired. It was quickly discovered in the courtroom that their sample did not have matching fingerprints.

Jennings was convicted of the murder of Hiller and sentenced to be hanged. He appealed the conviction on the basis that fingerprints were not infallible. But in 1911, in *People v. Jennings*, the Illinois Supreme Court made a ruling that stands as the landmark case for the use of fingerprints as a form of unique identification. The court upheld the conviction due to "Standard authorities on scientific subjects discuss the use of fingerprints as a system of identification, concluding that experience has shown it to be reliable."[241] Thomas Jennings was hung for his crimes in 1912.

The unique characteristics that make up the friction ridge skin on every individual (and some animals) point to the ingenuity of the Creator God. Job 37:7 tells us, "He seals up the hand of every man, that all men whom he made may know it."

Fingerprint patterns are the primary tool used for criminal identification. Fingerprints are the patterns created by the friction ridge skin located on the entire surface of the hands and feet. Due to the design of friction ridge skin, an uneven surface is created that provides a nonslip surface and firmer grip. Fingerprints develop in the mother's womb between 10 and 16 weeks of fetal development and remain with an individual until the dermal and epidermal skin fully decomposes after death. The value in fingerprint identification lies in three qualities: individuality, identifiable characteristics, and unchanging structure. The beauty, design, and complexity behind the structure of friction ridge skin testifies to a Master Artist and Creator God who loved every single person so much He gave them 20 unique friction ridge skin patterns (ten on the fingers and ten on the toes) unlike anyone else who will ever live on the face of the earth . . . past, present, or future.

FINGERPRINTS FROM A BIBLICAL WORLDVIEW

When studying friction ridge skin, the book of Psalms most closely manifests the unique design reflected in fingerprint patterns. Psalm 139:13–14 says, "For you formed my inward parts. . . . I am fearfully and wonderfully made." Job 10:8 describes the hands of God as having "fashioned and made me." Genesis 1 clearly describes the creation of humans as supreme to all other created things because they are formed in the image of God. God designed fingerprints to develop early in the womb. This is a testament to the value of a human life. At ten weeks of fetal development, humans have unique fingerprint patterns that remain with them for their entire lifetime. There is no question this person is fully human and entitled to the life God has planned for them. Also, at the moment of fertilization, a human has six feet of DNA that contains all the genetic instructions to form their fingerprints, as well as the information needed to fully develop. At the moment of fertilization, that tiny single-celled person is fully human. The abortion of a child in the womb at any point in a pregnancy is nothing short of the murder of a human life.

Fingerprints not only provide identifiable features, but the surface of friction skin is extremely sensory and can relay information directly to your brain. Imagine if you were blindfolded and someone placed a feather in your hand. Would your sense of touch allow you to distinguish the object? Absolutely! The intricate design of the hands (and feet) provides humans with the ability to pick up a heavy gallon of milk and an air-filled marshmallow at the same time while discerning the difference.

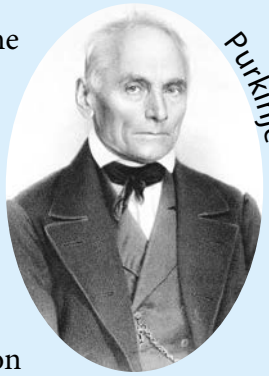
Also, the Creator God recognized the benefit of providing humans with a nonslip surface on their hands and feet. Therefore, the hands can grasp a cup without dropping it, and the feet walk barefoot without slipping. The uneven surface created by friction skin provides grip. Think about it — what is on the bottom of sneakers? Ridges and an uneven surface. Shoe manufacturers simply copied God's brilliant design when they developed nonslip footwear. And what is even more amazing is that God could simply have created friction skin to aid in gripping, but He went one step further and gave humans a special identity through their friction skin patterns in the form of over 10,000 unique details. In the estimated 108 billion humans that have lived in the last 6,000 years, there are not two people who even had one identical fingerprint, much less even ten points of minutiae that are identical. And imagine what the fingerprints of Jesus, who was born as a perfect human, must look like. Those who are believers know they will be able to look at the fingerprints on the nailed-scarred hands of the Savior when they get to heaven.

HISTORY OF FINGERPRINTS

The history of fingerprints dates back over 4,000 years. There is evidence on early stone artifacts, clay seals, pottery, and documents that demonstrates early civilizations recognized that fingerprints held value in someone's identity. Though there is no evidence to suggest these civilizations recognized every person has a unique set of prints, it does demonstrate recognition of a personal mark of identification.

Other historical documents have identified fingerprints as having patterns and include descriptions of spirals and loops, as well as descriptions of the thickness of the skin. In a petroglyph from the early 1700s, the Mi'kmaq peoples carved the ridge detail from a person's hand into slate.[242] There is clear recognition of patterns on the tips of the fingers and a whorl on the thumb, as well as ridge detail (lines) on the palmar area.

Chinese fortune tellers used fingerprint patterns and the number of whorls for their predictions. Though this is a form of witchcraft and holds no validity, it does demonstrate an awareness of friction ridge skin patterns.


Purkinje

But it was not until 1788 that Dr. Johann Mayer published the first information about the uniqueness of friction ridge skin. Mayer stated, "Although the arrangement of skin ridges is never duplicated in two persons, nevertheless the similarities are closer among some individuals. In others the differences are marked, yet despite their peculiarities of arrangement all have a certain likeness."[243] The first person to organize the patterns into a form of classification system was J.E. Purkinje in 1823. Purkinje was also one of the first to publish observations on primate friction ridge patterns as well as the fingerprint-like pattern on the prehensile tail of spider monkeys. Animal fingerprints will be discussed in Lesson 17.


Faulds

In 1879, an important advancement was made in identification by Alphonse Bertillon. Bertillon was a French criminologist who recognized everyone has unique body measurements. He devised the first system of classification based on a series of nine core body measurements. This system came to be known as anthropometry and was so successful that it spread to North America and was used in the United States as a means of filing criminals according to measurement. In 1903, the system was found to have fallibility and was discontinued. This occurred during the West case, the importance of which in relation to the science of fingerprints will be discussed later in the lesson.

Though various publications continued to surface over the next few decades, it was not until 1880 that the first article was published suggesting that fingerprints left at a crime scene could be used for identification. Dr. Henry Faulds is given credit for first publishing this practice, but it is Sir William Herschel, in response to Faulds' article, who stated he had been practicing this method for over twenty years in India. Therefore, Herschel is credited as the first European to implement the methodology of fingerprint identification.

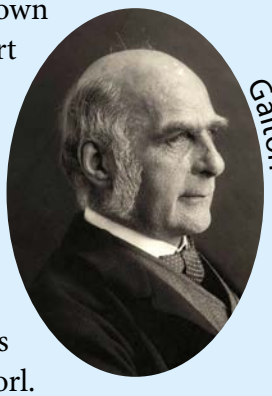
First fingerprints taken by Herschel, 1859

Now that fingerprints were recognized for their value in identification, it became necessary to develop a way to organize fingerprint files aside from someone's name. During this period, scientists also began toying with the idea of creating a superior human race. This initiative was called eugenics. Eugenics is defined as the study of how to force reproduction within a human population to increase the occurrence of heritable characteristics regarded as desirable. The scientist who coined the term eugenics and is considered the father of the eugenics movement, Sir Francis Galton, collected one of the largest repositories of fingerprint files for this period in history. As part of his eugenics research, he spent ten years studying over 8,000 ten-print fingerprint cards and classified each print according to pattern type and ethnicity for the sole purpose of determining what pattern type was special to a particular "race" of people. He published a book titled *Finger Prints* in 1892 that included an important conclusion:

> It may emphatically be said that there is no peculiar pattern which characterizes persons of any of the above races (English, Welsh, Hebrew, Black). There is no particular pattern that is special to any one of them, which when met with enables us to assert, or even to suspect, the nationality of the person.[244]

Once again, observational science confirms the truth of God's Word. The Bible states in Genesis 1 that God created Adam and Eve. Therefore, everyone in the human population is descended from them. In Acts 17:26a, the Bible emphasizes this again by saying, "And he made from one man every nation of mankind to live on all the face of the earth." Galton's own research confirmed that there is no particular fingerprint pattern that can be attributed to one particular people group but that patterns are randomly distributed across the whole of humankind, one human race made in the image of God.

It is important to note that the eugenics movement influenced the Nazi agenda and the extermination of millions of humans they considered less desirable, including those of Jewish descent, the disabled, and other minority groups. But the eugenics movement did not end with the defeat of the Nazi agenda. Eugenics still occurs today. Some countries like Iceland pride themselves on eliminating Down Syndrome,[245] but this is nothing short of eugenics. These countries have made it legal for parents to participate in selective abortions for the sole purpose of eliminating those babies that society deems less desirable.



Galton

In his book *Finger Prints*, Galton, who is also considered the father of fingerprint classification, developed the first system of organized fingerprint classification based on pattern type. In his book, he described the three types of fingerprint patterns still used today: arch, loop, and whorl. Expanding on Galton's research, Sir Edward Henry, a British official in India, developed a systematic method to classify fingerprints by assigning numerical values to fingers with the presence of the whorl pattern. The Henry system was so successful that it was brought to the United States in 1903, though it was used secondarily to the Bertillon method of anthropometry, which remained the primary means of identification until the historic West case.

William West

Will West

In May of 1903, a man was arrested and taken to Leavenworth Penitentiary in Kansas for processing. The clerk recognized the arrestee named Will West. When searching his anthropometry measurements, they found they were very close to another prisoner's — William West — measurements. Upon closer examination, they discovered these two men were identical twins who were unaware they had a twin brother. This case brought to light a discrepancy, or fallibility, in the method of anthropometry. When the fingerprints of Will and William West were analyzed, the technicians discovered they were uniquely different. Identical twins do not have the same fingerprints. The West case forever changed the use of fingerprints, and fingerprints remain the primary means of identification today.

ANATOMY OF FRICTION SKIN

Skin is the largest organ on the human body and covers an average of 22 feet on an adult. The ridged skin found on the hands and feet is distinctly different than the skin found on most of the body. Not only are the palms of the hands and bottoms of the feet two of three places on the body where there is no hair, but this is the location of unique pattern formation. Ridges develop in the womb and create identifiable characteristics. These ridges aid in gripping, and the creases in the ridges allow the skin to flex and bend. Friction skin is composed of two distinct layers: the epidermis and dermal layers. The epidermis is the thinner, outer layer of skin. This layer serves as a barrier against contagions and contains the sensory receptors. Damage to the epidermis in the form of cuts, burns, warts, etc., will undergo cellular repair, and often, no damage is visible in the friction skin patterns after healing.

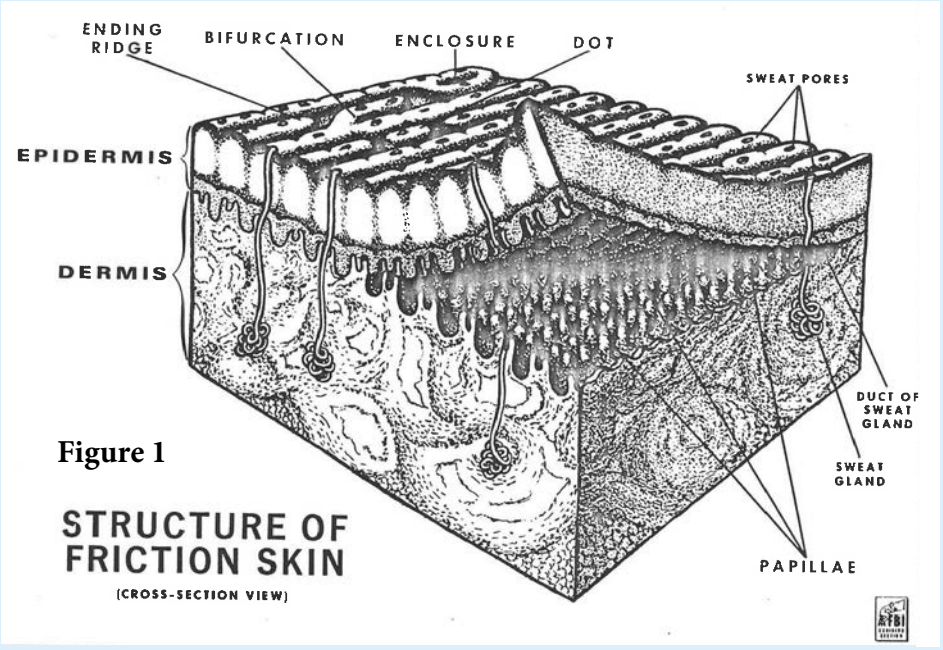


Figure 1

The dermal layer is the connective tissue that nourishes the epidermis. **Figure 1** shows that the fingerprint ridges and furrows are anchored deep within the dermal layer. A deep wound into the dermal layer will result in a permanent scar on the surface of the friction ridge skin. Permanent scars have the potential to become an identifiable feature as unique as minutiae characteristics. Sweat ducts from the dermal layer make their way to the surface of friction skin, secreting perspiration in the form of water (99%), fatty acids, amino acids, sugars, and other chemicals through the eccrine sweat glands. These eccrine sweat glands are the only appendage of friction ridge skin.

THE INDIVIDUALITY OF FINGERPRINTS

Analysis of fingerprints for over a century has confirmed the randomness of minutiae in friction ridge skin as a unique form of identification. In theory, it is a 100% certainty that no two people will have identical fingerprint patterns. God's design is truly amazing to study when you consider that all ten fingers will vary from those of the ten toes on one person. The 20 unique pattern arrangements on each finger (though some people may have more or less than twenty) will be unlike anyone else who will ever be conceived. All fingerprint patterns can be grouped into three basic categories: loops, whorls, and arches. Loops are the most common fingerprint in humans, consisting of 65% of all patterns, whorls are the second most frequent at 30%, and arches are the rarest at 5%.

loops	whorls	arches
65%	30%	5%

Considering there are an estimated 108 billion people who have been conceived in human history and there are only three general fingerprint patterns, what makes a person's fingerprints unique? Friction skin is made of thousands of little characteristics. The unique, comparable characteristics are called minutiae.

IDENTIFIABLE CHARACTERISTICS

The word minutiae basically means "details," and fingerprint patterns are made of thousands of details. It is estimated there are over 10,000 minutiae characteristics covering the entire surface of the hands and feet. Common examples of minutiae are listed below (though deltas and cores are not technically minutiae but common locations in a print).

Figure 1

- *Ridge ending:* the location where a ridge abruptly ends and does not continue.
- *Bifurcation:* the location where a single ridge splits into two separate ridges.
- *Island:* the location of a single spot of friction skin.
- *Crossover:* the location where two ridges cross and form an "X."
- *Delta:* the location where two ridges diverge and a point of reference or friction skin is visible at the center of the divergence. The term comes from the geographical term for a river delta.
- *Core:* the location of the center of the pattern area.

What makes minutiae characteristics so useful is the location of each point in relation to each other. The orientation of minutiae and how they make up the patterns of fingerprints are what is unique to everyone. The minutiae can be compared, counted, and analyzed against other known prints. Biometric software on phones, tablets, and computers are searching minutiae characteristics, not overall pattern type. When two points of minutiae on two different prints occur in the same location, it is considered one matching point. The examiner now begins the process of establishing additional concurring points (see **Figure 2**).

Figure 2

With over 10,000 characteristics on the surfaces of the hands and feet, it only takes between seven and ten minutiae on average to confirm a unique match. There is no official number of minutiae required for an identification, and each comparison is evaluated on its own merit. The greater the number of matching points, the greater the confidence level. If there is even one characteristic that does not match or cannot be explained, the examiner should begin leaning toward an inconclusive opinion. It is fascinating to think that ten minutiae only make up a surface area of about 1 cm^2 of one fingerprint, and this is enough information to confirm someone's identity. God created every single human with identifiable precision in friction ridge skin, made up of tiny details that form recognizable patterns unlike anyone else in His creation.

Biometrics:

A system of body measurements and calculations related to human characteristics for identification. (This topic is discussed further in Lesson 18.)

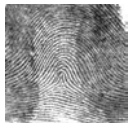
Unchanging Structure. The structure of friction skin remains unaltered during an individual's lifetime. There may be a wearing down of the ridges due to a person's profession or permanent scarring from injuries, but the identity found in the structure of the patterns is unchanging. The patterns that develop in the mother's womb between 10–16 weeks remain with a person until they decompose beyond the dermal layer of the skin. There have been cases when a body's epidermis is gone due to decomposition, but their identity has been verified by using the dermal layer of skin.[246]

FINGERPRINT CLASSIFICATION

Fingerprints are classified into three pattern groups: arch, loop, and whorl. These three basic patterns are further subdivided into eight total patterns, described in the following sections.

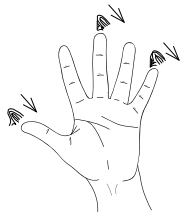
The Arch. Arches are characterized by not having a delta or core. The ridges in an arch enter one side and flow out the other side.

Plain arch: The ridges of a plain arch flow, or tend to flow, from the left side of the print to the right side of the print and create a gentle hill within the pattern area. A plain arch has no upthrust in the core of the fingerprint as seen in the tented arch.



Tented arch: The tented arch has a distinct upthrust in the shape of a camping tent or tepee in the core of the print. A tented arch may also be classified as such when it resembles a loop but lacks one of the three requirements to be classified as a loop.

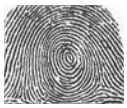
The Loop. The type of loop is determined by the flow of ridges in relation to the ulna and radial bones of the arm. A loop must meet three essential points: sufficient recurve, presence of a delta, and a ridge count of at least one. A ridge count is the number of ridges between the core and the delta.



Ulnar loop: Of the total eight pattern types, ulnar loops are the most common. In an ulnar loop, the ridges flow or tend to flow toward the pinky finger or ulna bone of the arm. The flow of ridges resembles a slide, as the ridges start at the base (delta) and flow upward over the core and then slope down off to the other side of the print.

Radial loop: Radial loops are less common and are characterized by ridges that flow or tend to flow toward the thumb or radius of the arm.

The Whorl. Whorls are characterized by the presence of two deltas and a core. There are four types of whorls:



plain whorl

central pocket loop whorl

double loop whorl

accidental whorl

When looking at all eight subclassifications of fingerprints and their frequency by pattern types, the following percentages reflect their commonality or rarity.

Loops		Arches	
Ulnar	Radial	Tented	Plain
60%	4%	1%	4%

Whorls			
Plain	Central pocket loop	Double loop	Accidental
21%	4%	4%	1%

HENRY CLASSIFICATION

Henry

Sir Edward Henry is given credit for the fingerprint classification system used in the United States. The system is based on the presence of whorls in fingers or thumbs. A point value is only given if a whorl is present. If no whorl is present, no value is given for that finger or thumb. The fingerprint classification is written in fraction form. To avoid a value of "0" when no whorls are present, an arbitrary "1" is always added to both the numerator and denominator. Therefore, an individual who has no whorls present on any of their fingers or thumbs has a primary classification of 1/1. Someone who has whorls on all ten of their fingers, after applying the Henry system, will have a classification of 32/32. Therefore, all primary fingerprint classifications fall within the range of 1/1 to 32/32.

A complete fingerprint classification includes the components below in the format of a large fraction.

	Key	Major	Primary	Secondary	Sub-Secondary	Final
Numerator	The ridge count of the first loop. If there are no loops, there is no key.	The ridge count or whorl tracing of the right thumb. If a small letter group, this will take precedence.	The value of fingers 2, 4, 6, 8, 10 + 1.	The capital letter representation of the right index print pattern (A, T, U, R, W).	The ridge count codes (I, O) or whorl tracings (I, M, O) in fingers 2–4 of the right hand. If a finger has a print in the small letter group, this will take precedence.	The ridge count of the pinky finger in the right hand. If there is no loop in the right pinky, the left-hand pinky is used and placed in the denominator. If there is no loop in either pinky finger, there is no final.
Denominator	If there is no value for the key, this is left blank.	The ridge count or whorl tracing of the left thumb. If a small letter group, this will take precedence.	The value of fingers 1, 3, 5, 7, 9 + 1.	The capital letter representation of the left index print pattern (A, T, U, R, W).	The ridge count codes (I, O) or whorl tracings (I, M, O) in fingers 2–4 of the left hand. If a finger has a print in the small letter group, this will take precedence.	The ridge count of the left-hand pinky finger when there is no loop in the right pinky. If there is a loop in the right hand, this is left blank. If there is no loop in either pinky finger, there is no final.

Step 1: Identify the pattern of each finger with a letter under the finger: whorls (capital W in all fingers), arch (lowercase a in all fingers except the index finger where a capital A is used), tented arch (lowercase t in all fingers except the index finger where a capital T is used), radial loop (lowercase r in all fingers except the index finger where a capital R is used). The only exception is for ulnar loops, which are the most common type of fingerprint. A diagonal line slanting in the direction of the loop is used to signify an ulnar loop — "\" in the right hand and "/" in the left hand. Notice that the diagonal line follows the flow of ridges toward the ulna bone in that hand. See the fingerprint card to the right.

Step 2: Once the patterns have been identified, identify the ridge counts in the loops and the type of tracing in the whorls.

- *Ridge counts in ulnar and radial loops:* Count the number of ridges that cross an imaginary straight line from the delta to the core of the fingerprint. This value is written in the top right corner of the fingerprint block.

- *Whorl tracings:* Trace from the center of the left delta to the center of the right delta. Assign a value of I (inner) for a tracing that flows inside the right delta, M (meet) for a tracing that aligns with the core of the right delta, or an O (outer) for a tracing that flows outside the right delta. The tracing is written in the upper right corner of the fingerprint block along with the type of whorl (plain "P," central pocket "C," double loop "D," accidental "X").

Inner tracing (I)

Meet (M)

Outer (O)

Step 3: Record the Key. The key is the ridge count of the first finger with a loop pattern. The first finger to have a loop is the right index finger, and when counting the number of ridges from the delta to the core, the count is 7. The key is placed in the numerator. If there are no loops in the ten fingers on the fingerprint card, there is no key.

Step 4: Record the Major. The major is either the whorl tracings or ridge count code in the thumbs. If a whorl tracing, only use the capital letter for the trace type, I (inner), M (meet), or O (outer).

For ridge counts, the coding for the thumbs is:

		Grouping Sizes		
	Coding	**Small**	**Medium**	**Large**
Right hand	When the left thumb is 16 ridge counts or less	1–11	12–16	17 and over
Right hand	When the left thumb is 17 ridge counts or over	1–17	18–22	23 and over
Left hand		1–11	12–16	17 and over

The right thumb's information is placed in the numerator and the left thumb's in the denominator.

Step 5: Record the Primary. Calculating the primary is the most important step in the classification process. A point value is given only if a whorl is present in the assigned finger block. The chart below provides the point value given to each finger. The whorl can be any one of the four types of whorl patterns.

Finger 1 Right thumb 16 points	Finger 2 Right index 16 points	Finger 3 Right middle 8 points	Finger 4 Right ring 8 points	Finger 5 Right pinky 4 points
Finger 6 Left thumb 4 points	Finger 7 Left index 2 points	Finger 8 Left middle 2 points	Finger 9 Left ring 1 point	Finger 10 Left pinky 1 point

To formulate the primary or numerical portion of a classification, the whorl value assigned to each finger is added to create a numerator and denominator.

The numerator is the sum of the values of fingers 2, 4, 6, 8, and 10, if a whorl is present, plus arbitrary 1.

Numerator: sum of fingers
2, 4, 6, 8, 10 +1

The denominator is the sum of the values of fingers 1, 3, 5, 7, and 9, plus arbitrary 1, only if a whorl is present.

Denominator: sum of fingers
1, 3, 5, 7, 9 +1

Observe the fingerprint card below. Using the Henry system of classification, the primary is calculated as 1/17.

Numerator: no whorls in fingers
2, 4, 6, 8, 10 + 1 = 1

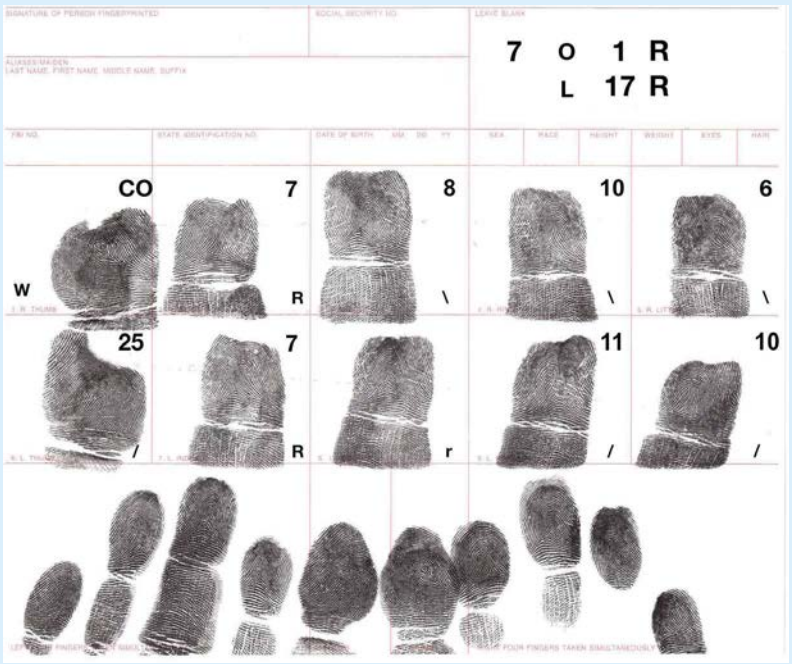
Denominator: 16 points for finger 1, no whorls in
3, 5, 7, 9 + 1 = 17

Step 6: Record the Secondary. Following the primary is the secondary, which is simply the pattern type in the index fingers. This is represented by a capital letter:

Whorl	Plain arch	Tented arch	Ulnar loop	Radial loop
W	**A**	**T**	**U**	**R**

Observe the fingerprint card below. Using the Henry system of classification, the secondary is R/R.

The secondary is written directly next to the primary.



Step 7: Record the Sub-secondary. The secondary is followed by the sub-secondary, which is the pattern types in the index, middle, and ring fingers of both hands, unless there is a member of the "small letter group" such as a radial loop, tented arch, or plain arch in the middle fingers (fingers 3 and 8), ring fingers (fingers 4 and 9), pinky fingers (fingers 5 and 10), or thumbs (fingers 1 and 6) of either hand. Due to the rarity of these pattern types outside of the index fingers, they are given priority in the classification. Small letters are brought up to the classification in their exact position adjacent to the index finger (secondary) in both the numerator and the denominator. If there are multiple small letters, a dash is used in between the letters to indicate an absence. If a small letter is in the thumb, that letter is placed to the left of the index (secondary).

If there are no small letters present in the middle fingers, ring fingers, pinky fingers, or thumbs, then the following process is followed for loops and whorls.

Ulnar loops: In the example below, there is a ridge count of 17. The number of ridges present in each finger determines the code of I or O.

Code	Index	Middle	Ring
I	9 or less ridges	10 or less ridges	13 or less ridges
O	10 or more ridges	11 or more ridges	14 or more ridges

The ridge count is written in the upper right corner of the fingerprint box. The right-hand codes are written in the numerator and left hand in the denominator.

Observe the fingerprint card to the right. Using the Henry system of classification, the sub-secondary is R/Rr.

This is because the radial loop in the middle finger is considered in the small letter group. Since it is in the middle finger of the left hand, it is placed in the denominator directly next to the index finger.

Step 8: Record the Final. The final is the ridge count of the pinky in the right hand. If the pinky of the right hand does not have a ridge count (such as when an arch or whorl is present), then use the ridge count in the left pinky finger and write in the denominator. If no ridge count is present in either pinky, leave this section blank. Observe the fingerprint card below. Using the Henry system of classification, the final is 6.

CONCLUSION

Fingerprints are fascinating to study because every single one is different. There is always something new to discover in the field of dactyloscopy (classification of fingerprints). God's ingenuity and creative design is reflected in the arches, loops, and whorls through the functionality of friction ridge skin. The rippled surface aids in gripping and provides a nonslip surface on the hands and feet. There is no question that fingerprints are just one example of how the human body is fearfully and wonderfully made.

Lesson 25

Residues and Patterns

This is he who came by water and blood—Jesus Christ; not by the water only but by the water and the blood. And the Spirit is the one who testifies, because the Spirit is the truth (1 John 5:6).

CASE STUDY

Case Study: Murder of Marilyn Sheppard

On the night of July 4, 1954, Dr. Sam Sheppard had fallen asleep on the couch when he was awakened by a cry of "Sam" from his wife upstairs. When he entered their bedroom, he claimed to have seen a "bushy-haired man" attacking his wife. Sheppard was hit on the head and fell to the floor unconscious. When he regained consciousness, he checked the pulse of his wife and found her to be dead. Their son, Sam Sheppard Jr., was unharmed and asleep in the home. Sheppard heard noises in the lower level of the house, found the back door open, and saw someone running toward the lake. He attacked the man. During the altercation, Sheppard claimed he was rendered unconscious a second time. When he regained consciousness again, he was shirtless, and his watch was missing. Sheppard called a family friend before calling the police.[412]

Dr. Sam Sheppard was a well-known neurosurgeon and the son of a prominent doctor, but investigators did not believe his story. Dr. Sheppard had a history of marital affairs, and there were rumors of friction in the marriage. To the police, it appeared as a simple domestic murder case. The police did not investigate the "bushy-haired man" or any other suspect. Dr. Sheppard was arrested, tried, and convicted of second-degree murder on December 21, 1954. The trial drew lots of attention and not only had a very biased judge ruling over the proceedings but is also recognized "as a mockery of justice" by the federal courts and studied by law students.[413] He was sentenced to life in prison. Maintaining his innocence, Sheppard began the appeal process. F. Lee Bailey took over as Sheppard's chief counsel on July 30, 1961. On July 16, 1964, Sheppard was released on the grounds that during the original trial, there were multiple violations of his constitutional rights. But it was not over. In May of 1965, his conviction was reinstated by a federal appeals court, and Sheppard went through a second trial.

Blood spatter analysis had never been introduced in court as evidence. During the second trial, blood spatter analysis and testimony by Dr. Paul Kirk was entered as evidence. Dr. Kirk pointed to the blood spatter patterns as evidence. He testified that Dr. Sheppard could not possibly be guilty. This was the first case where blood spatter analysis was key to the exoneration of a suspect. Based on this new testimony and other credible facts from the case, Sheppard was found not guilty. Sheppard returned to his surgical practice, but after killing two patients and having a pattern of alcoholism, he was forced to quit practicing medicine. He tried professional wrestling and used the stage name "Killer Sheppard."[414] Since his second trial, Sheppard had become addicted to barbiturates and was an alcoholic. Sheppard died of liver failure in 1970 at the age of 46. He never admitted guilt to friends, family, or even his lawyers and claimed his innocence until his death.

But there's another piece to this mystery — a man named Richard Eberling. But who is he? Richard Eberling owned a window cleaning company at the time of the murders, and the Sheppards were one of his clients. Eberling was arrested for grand larceny in 1959. When police later searched his home, they found nothing of the Sheppards except a cocktail ring belonging to Marilyn Sheppard.[415] The ring is claimed to have been stolen three years after the

murder from the home of a Sheppard family member. Eberling consented to a lie detector test regarding Marilyn's murder, and the results were found to be inconclusive. It did become clear that Eberling found Marilyn attractive and appealing. Eberling was never addressed as a possible suspect in either the first or second trial. Eberling was later convicted of murdering Ethel Durkin in 1989. Kathie Collins, a nurse for Durkin, told police that Eberling confessed to her that he killed Marilyn Sheppard. Eberling denied making this claim. His murder conviction renewed interest in his possible involvement in Marilyn's death.

The question remains to this day: Who really killed Marilyn Sheppard? According to a statement by Eberling, "The Sheppard answer is in front of the entire world. Nobody bothered to look."[416]

Though there are extensive facts surrounding this case, these are a few of the highlights.

Facts about the case regarding the Sheppards:

- At the time of the murder, Marilyn was four months pregnant with a baby boy. The baby was Sam Sheppard's, dispelling the theory that Marilyn was having an affair and Sam killed her in anger.
- No fingerprints were found in the house besides those of the family.
- Prosecutors claimed there were no signs of forced entry into the home. Years later, it was revealed that the Scientific Investigation Unit never told the prosecution they had found evidence of forced entry outside the cellar door, enough to warrant a toolmark casting.[417]
- There were visible signs of a robbery (or staged robbery), such as open drawers and broken items.
- Sheppard claimed to be wearing a t-shirt on the night of the murder. A t-shirt was found a few yards from the Sheppards' property line that was Sam's size. No blood was found on the shirt. There was also no blood found on Sam's pants, belt, socks, or shoes, other than one stain on the knee area of his pants. This was believed to have occurred as he was checking his wife's pulse.
- Marilyn died from 35 blows to the head, and blood spatter covered the room. The act was clearly passion driven and not an arbitrary robber.
- Marilyn had described her husband to a family friend as a "Jekyll and a Hyde."[418]
- The coroner testified in court, "In this bloodstain I could make out the impression of a surgical instrument."[419] No surgical instrument matching the description was ever found.
- Sheppard's bloody watch was found inside a green bag on the bluff above Lake Erie. The watch had stopped at 4:15 a.m.
- Dr. Kirk's blood analysis testimony stated the killer was left-handed; Sheppard was right-handed.

- F. Lee Bailey was Sam Sheppard's second attorney. Bailey would go on to become a famous attorney and would be one of the people on the defense team representing O.J. Simpson in 1995.
- The Sam Sheppard case inspired a popular TV series and movie.

Facts about the case regarding Eberling:

- Richard Eberling had type A blood; no type A blood was identified in the blood evidence.
- When Eberling was arrested for larceny in 1959, he did not have "bushy hair," but he was known to wear toupees.
- During his 1959 arrest, Eberling told police he had cut himself while installing a screen at the Sheppards' home two days before the murder in 1954. He had a scar on his left wrist.
- When Eberling was testifying for the defense in Sheppard's second trial, Sheppard never identified him as the man with the "bushy hair" or the suspect who attacked him the night of Marilyn's death.
- Eberling identified the cellar door on a detailed sketch he drew of the Sheppard home in 1992 during the reinvestigation, a detail not visible on the police sketch in 1954.
- In 1998, a DNA profile developed from a bloodstain near the closet in the bedroom showed that Eberling's profile fit within a rare blood DNA profile.
- On July 25, 1998, Eberling died in prison.
- In August of 1998, an inmate at the same prison with Eberling told police that Eberling had confessed to Marilyn's murder before he died.

Several books have been published on the murder of Marilyn Sheppard, some pointing to Dr. Sheppard and some pointing to Eberling as the killer. Blood spatter analysis has come a long way in validity since the 1960s. This lesson will cover the techniques used in interpreting blood patterns and the value found in a single drop of blood.

"The most common place crime is often the most mysterious, because it presents no new or specific features from which deductions may be drawn." — Sherlock Holmes[420]

Blood spatter analysis is the field of forensic examination that deals with the physical properties of blood and the shapes, locations, and distribution patterns of bloodstains. The goal of blood spatter analysis is to provide a knowledgeable, expert interpretation of the physical events that produced the blood evidence. The first major case that involved blood spatter analysis was the Sam Sheppard case in 1955 discussed above.

Remember from Lesson 11 that the components of blood are 45% formed elements and 55% plasma. The formed elements comprise red blood cells, white blood cells, and platelets. Ninety-one percent of plasma is water. As the Bible says in Leviticus 17:11, life is in the blood. A human would have to lose 40% of their blood volume, either externally or internally, to produce death. A cut vein or artery will result in a loss of half a liter of blood per minute. Investigators understand that dead people do not bleed. The heart must still be circulating blood for bleeding to occur. When a living person is struck with an object, the initial injury does not cause the blood spatter. There must be an open, bleeding wound that is then struck a second, third, or more times to leave a blood spatter pattern.

Blood exhibits a high level of surface tension (0.058 N/m), and this characteristic causes blood to form the spherical shapes visible in blood spatter patterns. Surface tension is the result of the intermolecular forces at work between the liquid and the surface. The liquid molecules adhere together and give the appearance of an elastic membrane in the droplet. Blood is also very viscous. Viscosity is the blood's resistance to flow. The phrase "blood is thicker than water" describes the viscosity. Blood will flow more slowly than water due to its cellular components. The surface tension and viscous nature of blood contribute to the unique shape of the patterns left behind.

BLOOD SPATTER FROM A BIBLICAL WORLDVIEW

Blood spatter analysis requires an understanding of mathematical calculations in the field of geometry and a fundamental understanding of physics. The reliability of mathematical laws used in this discipline demonstrates that there must be a law giver. Someone set into motion the mathematical principles measurable throughout creation. Though blood spatter analysis is often the result of man's sin against another human, God put principles in place that allow investigators to solve these crimes using the scientific method and mathematical predictability. Dr. Dana Sneed relates how math confirms the biblical Creator God:

> Math is predictable because our God, who upholds the universe (Hebrews 1:3), is consistent—he does not change (Malachi 3:6). In fact, we see the foundation of math in Genesis 1, when God counted the days of creation and marked the beginning of time. The concept of infinity or even irrational numbers (that have decimal places that continue on into infinity) remind us that God is beyond measure (Psalm 147:5); infinity can only exist because God is infinite. Math, like operational science, depends on the uniformity of universal laws and the certainty of absolute truths, which depend on the God of truth (Isaiah 65:16).[421]

Leviticus 17:11:

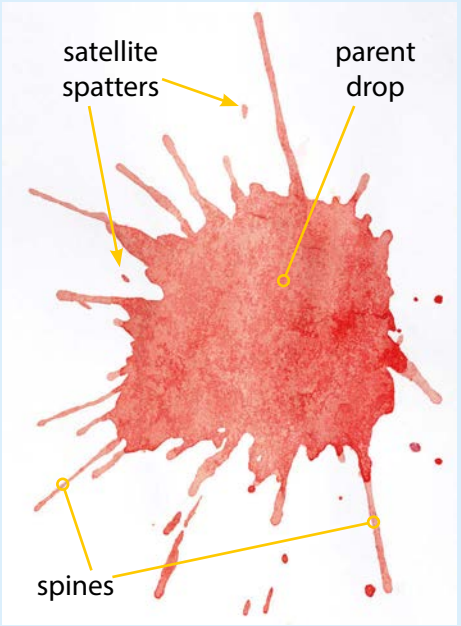
"For the life of the flesh is in the blood, and I have given it for you on the altar to make atonement for your souls, for it is the blood that makes atonement by the life."

HISTORY OF BLOOD SPATTER

The history of blood spatter analysis is young compared to other forensic disciplines. The first detailed study of blood spatter analysis was published in 1895 by Dr. Eduard Piotrowski and was titled *Concerning the Origin, Shape, Direction and Distribution of the Bloodstains Following Head Wounds Caused by Blows*. His research laid the groundwork for future pioneers such as Dr. Victor Balthazard (1939), who was the first to use physical interpretation of stains to determine point of origin, and Dr. Paul Kirk (1902–1970), who was the first to use bloodstain pattern analysis in court during the Sam Sheppard case in 1955 (see the case study at the beginning of this lesson). In 1983, the International Association of Bloodstain Pattern Analysts (IABPA) was formed to standardize this branch of forensic science. The science of blood spatter stains continues to develop into a very accurate and predictable form of analysis.

A DROP OF BLOOD

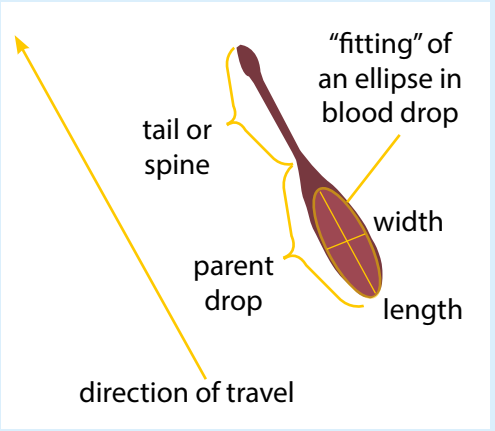
A single drop of blood has three characteristics: the parent drop, spines, and satellite spatter. The parent drop is the drop of blood from which the satellite spatter originates. The spines are pointed edges on the parent drop that radiate out like a sun. Spines help pinpoint direction. The satellites are small drops of blood that broke free from the parent drop when the blood hit the surface.



If the parent drop falls at an angle less than 90 degrees, it will have a tail. The tail always points toward the direction of travel. The type of surface the droplet falls upon will affect its characteristics. A smooth, hard surface will leave no distortion of the blood around the edges. Examples of a smooth, hard surface are glass, tile, finished hardwood floors, etc. Textured surfaces, like linoleum flooring, will result in a bloodstain with visible spines and satellite droplets.

The elongated shape of these droplets can be measured to determine the following characteristics:

- The direction from which the blood originated
- Angle from which the blood originated
- The time of the attack
- Location and position of the victim
- Movement of the bleeding suspect or victim
- Number of blows to the victim
- The type of injuries
- The location of the attacker



CATEGORIES OF BLOODSTAINS

Bloodstains are categorized into three broad categories: passive, transfer, and projected.

- **Passive.** Passive drops of blood are pulled down by gravity alone. The distance between the source and the surface affects the size of the blood droplet. The greater the height, the larger the spatter.

  - There are four types of passive patterns, which are identified as drops, drips, pools, and clots.

- **Transfer.** Transfer bloodstains are the result of a bloody surface coming into contact with a clean surface, thereby leaving bloody residue. This direct transfer can occur from a bleeding body being dragged across a floor or when an assailant rubs bloody hands on a door frame. Transfers have the potential to leave identifiable, individualized characteristics like fingerprints, palm prints, and shoe prints. Types of transfer bloodstains include:

  - *Swipe or smear*: This is when wet blood is transferred to a surface that did not originally have blood on it.
  - *Wipe or smudge*: Occurs when a clean, non-blood-bearing object moves through a wet bloodstain and alters the appearance of the original stain.
  - *Contact bleeding*: A simple person-to-person transfer of blood.

- **Projected.** Projected bloodstains are the result of a force or action that causes exposed blood to be expelled. The amount of spatter and the spatter area is directly affected by the force applied. This force is greater than the force of gravity. Analyzing the cast-off patterns is crucial to determine the direction and location of the force.
  - *Back spatter*: The result of blood spatter on the perpetrator from the attack on the victim.

TYPES OF SPATTER

Learning to distinguish between the various types of blood spatter is key to an investigator's analysis. Each type of spatter holds distinguishing characteristics that will help in the interpretation of events at the crime scene.

impact spatter

Impact Spatter. This is when a blood source is impacted by a blow that causes a random dispersion of smaller drops of blood. The surface texture and velocity greatly impact the appearance of the blood drops. Velocity is defined as an object's speed and direction of motion.

- Low velocity: 0–5 ft/sec, with stains 3 mm or greater in diameter. These reflect dripping blood due to gravity.
- Medium velocity: 5–25 ft/sec, with stains 1–3 mm in diameter. These reflect a blunt force trauma or cast-off pattern.
- High velocity: 100+ ft/sec, with stains less than 1 mm and resembling a fine mist.

There are four phases of impact that every blood drop will progress through:

1. Contact and collapse is the flattening of the blood droplet upon impact.
2. Displacement is the spreading out of the blood droplet.
3. Dispersion is the separation of spatter or small droplets from the main droplet.
4. Retraction is the adhesion of blood particles that do not completely separate and are drawn back into the parent droplet.


gunshot spatter

Gunshot Spatter. This is the forward blood spatter emitted from the exit wound and back spatter from the entrance wound. If the bullet becomes lodged in the body, only back spatter is visible.

If the gunman is near the victim, the gunman will likely have back spatter visible on their clothing, hands, and other parts of their body. Occasionally, blood spatter will spray into the muzzle of the firing gun. This is called drawback effect.


cast-off spatter

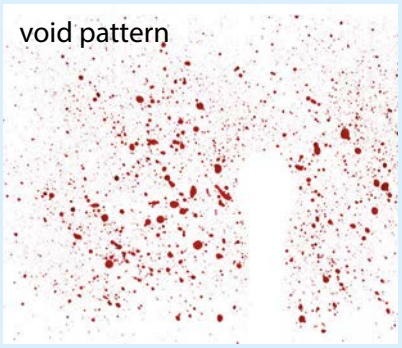
Cast-off Spatter. This is caused by the blood released from a bloody projectile. For example, a blood-covered fist, knife, baseball bat, gun, or other object flings blood onto the walls and surfaces as it is in motion. The pattern may resemble an arc shape. The amount and range of spatter is dependent on the object inflicting the blows, the amount of bleeding incurred from the injury, and the direction of the object at impact. Cast-off provides clues to the minimum number of blows inflicted on the victim. The investigator will count the number of forward/backward spatter patterns. Other factors that can be gleaned from cast-off patterns are the height of the attacker, angle of impact, and direction of the weapon.

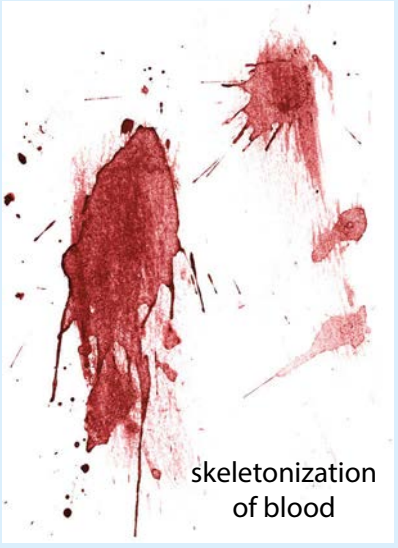

arterial spray spatter

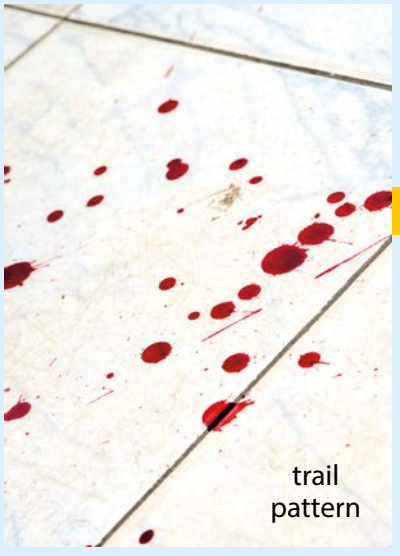
Arterial Spray Spatter. This pattern occurs when a main artery or the heart is ruptured. As the blood builds up, the pressure of the pumping blood will spurt blood outward from the injuries. The area with the biggest spurt is the location of the first burst artery. Since this blood is highly oxygenated, it can be distinguished by its bright red color.


expirated spatter

Expirated Blood. These patterns are caused by a bleeding mouth or nose from an internal injury. Often in expirated blood, oxygen bubbles expressed in the blood spatter provide another characteristic for comparison by providing insight into the type of injuries present in the victim.







Void Pattern. This is a space where there is no visible blood spatter. The void is created when an object or person blocks projecting blood spatter from reaching a surface. The blood adheres to the blocking material instead. Analyzing void patterns can alert the investigator to the height, size, and shape of the object or person causing the void.

Flow Patterns. These are the result of the flow of blood downward due to the force of gravity. There are two types of flow patterns, active and passive. Active flow is blood emitting from an open wound, while passive flow is blood patterns due to arterial spurt. Flow patterns provide clues to the movement of the victim and/or perpetrator.

Pool Patterns. These are the collection of blood in a pool on an undisturbed, nonporous surface. If blood collects on a porous surface, it will either be absorbed or, if there is sufficient blood, will diffuse to the surface beneath.

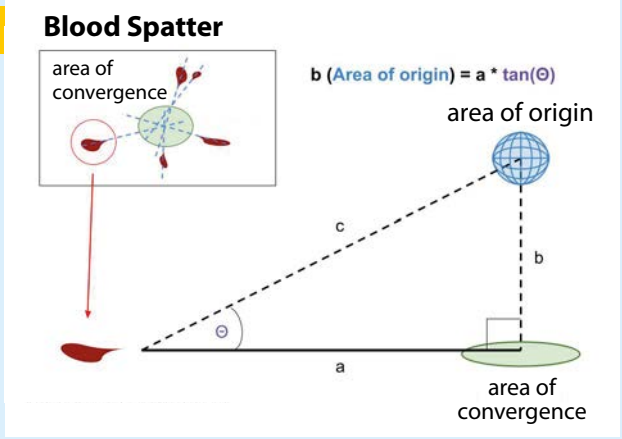
Splash Patterns. These are visible when a pool of blood splashes outward and resemble the shape of an exclamation point.

Skeletonization of Blood Patterns. These occur when the edges of a bloodstain begin to dry. Under normal conditions, this occurs within 50 seconds of deposit. The drying of the edges is referred to as skeletonization. Once the edges have skeletonized, any disturbance to the stain, whether wiping or smearing, will leave the perimeter of the original stain intact. Depending on how much blood is deposited, the center of the stain may dry and flake away if disturbed. This characteristic provides clues to the timing and movement of anyone involved in the act.

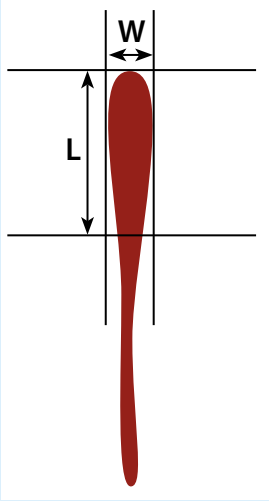
Trail Patterns. These patterns are caused by a series of drops that form by the dripping of blood from an object, weapon, or injury. The size of the drop helps in determining the distance from the ground and possible height. This will be discussed in the next section. Additionally, the shape of the drops allows investigators to determine the speed and direction of the person who was injured. Sometimes, by following the blood trail, the drops will lead directly to the weapon. There is also the potential for DNA evidence.

BLOOD SPATTER CALCULATIONS

Analyzing blood spatter requires measurements, accuracy, and calculations. Three areas that impact this analysis are the impact angle, the area of convergence, and the point of origin.

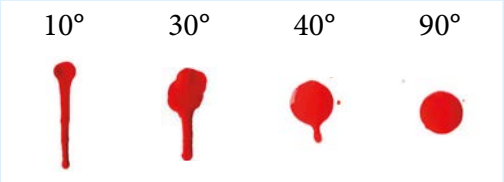


Impact Angles. Bloodstains have a unique shape, a teardrop with a pointed tail. As discussed earlier, the pointed end of a bloodstain always points toward the direction of travel. To determine the direction and angle of impact, only the circular portion of the stain is measured for the length and width. If the length and width are the same, the blood droplet fell perpendicular to the surface and is a 90-degree stain.

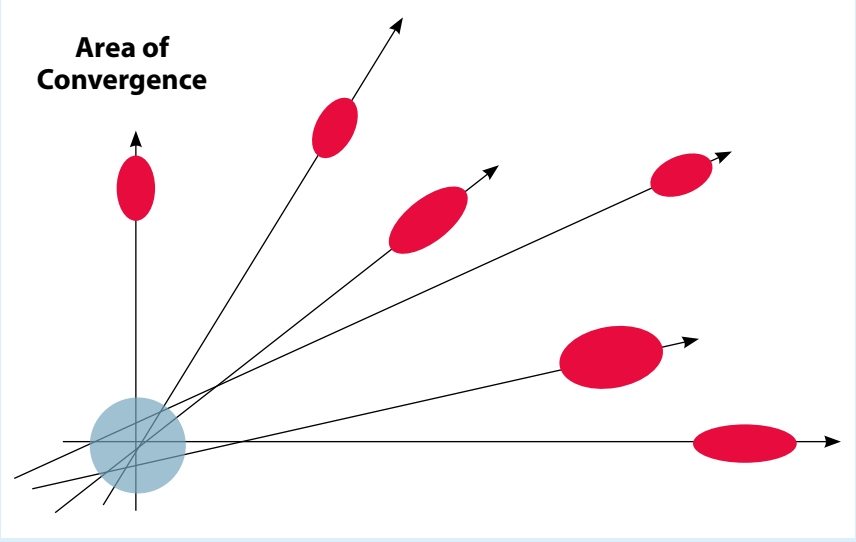


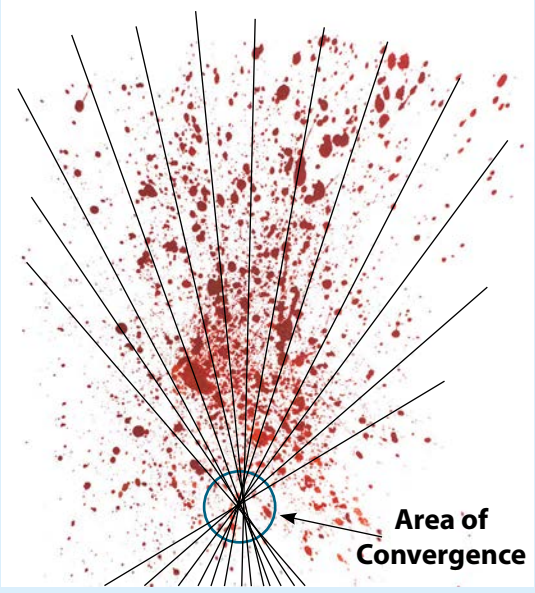
As the angle decreases, the more elongated the stain. The angle of impact is defined as an acute angle formed between the blood drip and the surface. Using trigonometry, the impact angle is calculated. The formula to measure the impact angle is:

$$\sin A = \frac{\text{width of bloodstain}}{\text{length of bloodstain}}$$

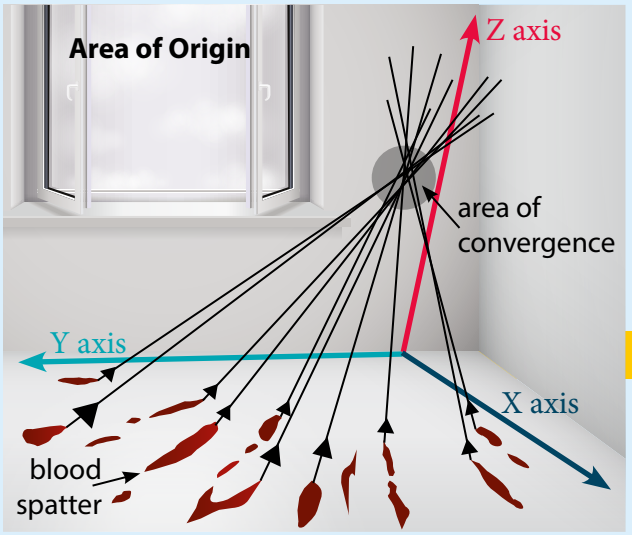


Area of Convergence on a Two-dimensional Plane. The area of convergence is the point at which the drops of blood in an impact pattern originated. To determine this point, lines are drawn from the long axis of several individual bloodstains through their tails to determine the area of convergence.





Area of Origin in a Three-dimensional Space. The area of convergence in a three-dimensional space is the area in which the victim or suspect was present when the blood spatter stain was produced. Investigators use strings or lasers at the point of each bloodstain from the long axis of the stain to the approximate point of origin. They will then use the angle of impact measurement to pinpoint the exact location of the attacker. Any interruption or discrepancy in any of the patterns is a clue in the timeline of events.



DOCUMENTING BLOODSTAINS

As with all evidence, the first step is to photograph each pattern and drop of blood from a distance to observe the overall pattern and then up close to identify spines, tails, or spatter. They should also be photographed with and without a scale measurement. The perimeter rule method is to use a rectangular ruler with scale measurements around each pattern and stain. In addition, the location of each bloodstain is recorded with the size.

Of all the search patterns, the grid method is the best search methodology to locate and identify all blood spatter evidence. In this method, a grid of known dimensions is placed over the pattern for scale and to accurately record the pattern.

CONCLUSION

Bloodstains reveal clues to the direction and angle of the weapon, and the location of the assailant and victim. Based on the patterns, investigators can determine movement through the scene, the number of blows, and other important characteristics. Blood spatter reveals the person was alive when the attack began, and the length of time blood is on a surface allows for an estimated time of attack and possible time of death. Forensic bloodstain experts are expected to be knowledgeable in the different patterns, shapes, and angles of blood spatter.

It is unfortunate that this type of expertise is needed in forensic work, but man has rebelled against their Creator God. In His wisdom, God put into motion mathematical laws that allow crime scene experts to resolve these mysteries.