CHAPTER 1

The Glue

The global fabric that holds together social, political, and business structures is largely dependent on—or, at the very least, highly impacted by—the movement of electronic data at the speed of light. Routed through an endless array of devices, switches, cables, fibers, satellites, and the atmosphere itself, these systems have their own inherent vulnerabilities and strengths.

But aside from the obvious impact that is so widely reported that the global networks have had on society and the world as we know it, this information revolution has taken within its clutch the mechanics of such precious and unique human qualities as trust, privacy, and truth and in very meaningful ways has either enhanced or modified these constructs or in some cases threatens to obliterate them.

The converse, however, may also be true that these same precepts that provide the glue that society thrives on may over the long haul be strengthened and enhanced by these predictable, self-healing, and potentially transparent networks—networks that may allow the population of the planet to police itself in real time.

Is it possible that the global networks are not the instrument of an evil Big Brother but are in fact the technical incarnation of an earth-coating truth serum that will disallow and prevent antisocial behavior on the part of individuals, groups, and institutions? Could it be that the greater good of humankind finally transcends the individual negatives of petty criminals, Ponzi scheme fraudsters, banal corporations, and megalomaniac two-bit dictators? All on Facebook?

Until our descendants learn the answers to these altruistic questions, we will need to be satisfied knowing that we are all doing our part to keep the glue *sticky*—to use a cool, recent Internet term—by ensuring that we are pursuing the adoption and sanctity of the truth, privacy, and trust within the realm of the global networks.

The role of the computer forensic investigator is front and center in this epic challenge for humanity to find the right equation, structure, and balance in its new relationship with instantaneous and ubiquitous computing power, which theoretically will eventually allow for all of humanity to interact with all of humanity in real time.

Although any one computer forensic investigation may have inconsequential impact on these larger issues, collectively the framework that the field is creating provides part of the roadmap to the future mechanics of how society will function in the actual information age.

I say the *actual* information age, because I am of the belief that we are still very much in the information revolution and have many challenges ahead before the global information ecosystem has matured to adulthood.

If we allow our journey to adulthood to do away with the vital interests of truth, privacy, and trust, the glue that holds it all together, then the infant will be stillborn and our world may truly find itself in an Orwellian apocalypse.

This chapter, which I call "The Glue," deals with some of these issues in a practical sense and provides analysis from a number of points of view. These include truth, privacy, and trust as well as a discussion on the foundations of digital evidence and its historical context, an analysis of investigative objectives, and a discussion of the investigative process.

The Relevancy of Truth

The pursuit of truth requires objective observation. The fact-finder needs as much clarity as can be achieved through methodical analysis of the available data points. In some cases this is achieved through real-time observation of events that are unfolding in front of the observer's eyes, or for the benefit of the observer's ears. In other cases the observer must reconstruct the events that took place by using available evidence. This evidence can include a wide variety of things from electronic data to physical artifacts to eyewitness accounts.

The relevancy of truth is central to the human experience. This is because human relationships, from a simple relationship between two friends to the complex relationships of 100 million citizens of a country to its leadership, all seek the power of truth to strengthen the bonds of the relationship. Without the foundation of truth in a relationship, it will soon find itself on rocky ground, the results of which are found in divorce, hatred, and revolution.

Therefore, the relevancy of truth is in itself a universal truth that humans far and wide in ancient times, modern times, and the future have and will understand, value, and protect. Unfortunately, truth can often be easily obscured and as a result other human traits can come into play—lying, cheating, failing to perform. Lying through deception, for example, has as a matter of course been commonplace throughout the human experience. Whether it is for the personal benefit of a child who wants more food or of a global corporation that wants more market share, the act in itself is so pure that it is often difficult to distinguish, on the face of things, the family man from the fraud, the good corporate citizen from the predator. But because it is so vital to the structure and security of human relationships that truth prevail, we have also gone to great lengths to root out untruths and to identify falsehoods as expeditiously as possible. Countless checks and balances exist, from the reaction that you may

have to a cheater's body language to the analysis that a U.S. Securities and Exchange Commission examiner may undertake when reviewing corporate filings related to complex derivatives.

The role of the investigator is as old as, if not older than, the earliest and perhaps first human relationship. This is because before a human is willing to enter into a relationship, he or she normally will investigate the other side and render a judgment. Is he a strong enough caveman to protect me and secure food? Is the architect educated enough to build the aqueduct? Is the money lender honest or is he giving me imitation silver or gold? Is the doctor competent? Is the general decisive? Will she be true to me? Can I believe my boss has my back? The list goes on forever, and for every one of these questions there is a truthful answer and quite possibly many untruthful answers of varying degrees. Why is this relevant? Because without the possibility of truth entering the equation in the human relationship trust can never be established. Without trust, human bonds cannot be formed and all relationships fail.

Think of it: Do you trust that FedEx will get the package to the sender tomorrow morning by 8 A.M.? Do you trust that the bailiff will draw his gun if the criminal defendant in the courtroom attacks the witness? Do you trust that your child's teacher will teach math and history as opposed to pornography and bestiality? Do you trust that the single malt whiskey in the bottle is in fact 18 years old? Do you trust that the truck will stop at the red light?

In each of these cases we have grown to expect these truths to exist, and as a result we have endowed the relationship with trust. When one of these relationships is violated, however, we are rocked by the consequences. The letter did not arrive on time to the client and you lost the bid. The witness was attacked and as a result refused to testify and you lost the trial. Your child has been traumatized by an errant teacher shattering his innocence. Your whiskey was a counterfeit and made you ill. The truck did not stop and you are now in the hospital fighting for your life.

Should your life be punctured by one of these terrible incidents, you or someone working on your behalf will undoubtedly be charged with establishing the facts of what happened, looking to preserve, protect, and analyze the evidence to establish the truth and to reassemble retroactively what should have been the trust that secured the relationship you had with the offending party.

Through this investigative process, culpability can be established and some measure of balance restored back into the relationship, often through such measures as apology, refund, judgment, restitution, fines, incarceration, execution, or even unconditional surrender. Ultimately the human relationship seeks balance and stability as well as a fair water level that can accommodate and sustain all.

Foundations of Digital Evidence

I have titled this section as a nod to the seminal work of the same name by George Paul as it rightfully contemplates in a deep and meaningful way the origins and provenance of digital evidence in a manner that had not been done before it. Through the

ages, evidence has taken numerous forms, from the direct testimony of witnesses who have observed behavior and facts to circumstantial evidence that casts an inference on a set of assertions and finally to physical evidence, which is presented to support or refute the claim. Digital evidence is somewhat unique insofar as it is both physical evidence, and at the same time, because of its unique properties, can be a recordable and replayable record of the actual activity itself. For example, a murder weapon, such as a knife, that is used in an attack and that has been preserved as evidence is an inanimate object that can be understood to have had a role in the crime but that does not tell the story itself. After all, the knife, the blood that is on the knife, and its placement near the body can imply that this was, in fact, the knife that was used to kill an individual. However, the knife cannot give clues as to intent, methodology, timing, speed, defense culpability, or any of these other important aspects of the investigation.

On the other hand, a digital file that is found at the scene of crime—that scene being a computer—may be preserved at the time and in the fashion in which it was created by the criminal. If the crime that is being investigated is the fraudulent transfer of funds from the accounting department of the company for which the criminal works to an account that he controls, then the digital files that are captured as part of the evidence during the investigation of the crime may in fact provide the investigator with the ability to replay the actual chain of events just as the criminal saw them on his own computer screen.

For instance, the e-mail that was created by the criminal and sent to a colleague for the purpose of authentication can be shown on the screen and the path that that e-mail followed from the moment that it left the computer of the criminal and traversed the network to the computer of the individual to whom it was sent can also be captured and reviewed. The digital files and details may remain precisely as they did at the time of the actual event. Further, the individual who received the e-mail and who subsequently provided the authorization to the criminal to access a particular account can also be captured and reviewed. Continuing down the thread, the activity that occurred online as the criminal accessed the account and authorized the payment to a bogus third party can also be captured and reviewed. Finally, the electronic payment, which is made from account to account, can also be captured and reviewed in precisely the manner in which it took place at the time of the actual event.

Through this process of the analysis of digital data and its timeline, reconstruction of the crime scene and of the crime itself can take place. For this reason, digital evidence is both physical and dynamic and has properties that investigators have not had to contend with at any point in time during humanity's long run of perpetrating fraud and investigating its outcome. Whether we are speaking of clay tablets, cuneiform impressions, papyrus scrolls, or inscribed manuscripts of the Middle Ages, record keeping has essentially remained the same for millennia. As recently as just a few decades ago, most business records were still kept in written form, and at times would also be kept in duplicate or triplicate. The access to and examination of a business record and of communication between individuals during the eighteenth century more than likely rested on handwritten letters with a seal or signature of authenticity coupled with journal entries in ledgers that were kept under lock and key by the clerical manager charged with that task.

Other than this most basic physical evidence, investigators would have had to rely on the statements of individuals, which, as we know, are subject to interpretation, misinterpretation, and certainly biases. I hate to think of the grave number of individuals who have served time as a result of crimes or activities of which they were falsely accused but had little chance of disproving due to the dearth of physical evidence that could be reliably accessed to disprove the claim. However, in today's world, digital evidence is profligate and promiscuous and surrounds our every activity. It is nearly impossible to escape the intertwining vines of digital evidence that permeate our lives in every respect, and the positive aspect of this information age is the ability of both the afflicted and the wrongly accused to more effectively put forth their argument by trusting in physical evidence that can be relied on, and in many cases, can actually re-create the events that are the subject of the investigation.

Investigative Objectives

The purpose of an investigation is to gather factual information. Without gathering factual information, investigators would not have the ability to solve disputes, questions, or matters involving everything from missing persons to the recovery of stolen property to a dispute over a contract to a regulatory investigation. All of these types of investigations require fact-finding. Examples of the types of investigations that are likely to be managed by an investigative computer forensic professional would include employment investigations, trademark and patent infringement investigations, homicides, missing persons, and suicide investigations, slip-and-fall investigations, financial fraud, malpractice investigations, and undercover or internal investigations for private and public parties, to name a few.

Ultimately, regardless of the type of information one is seeking or the systems and applications that are to be queried using information technology as a tool, the goal is to establish facts and evidence. Once the facts and evidence have been firmly established by using proper process and protocol, a summary or report of those facts can be generated and provided to relevant parties. The investigative objectives in the traditional sense of investigations are no different from that of a computer forensic investigator, in terms of the pursuit of dispassionate observation of data and information, as well as related evidence. This is required to properly, reliably, and ethically encapsulate the observer's findings so that they can be provided to third parties for the purpose of disposing of a particular claim.

The Investigative Process

The investigative process, when applied to information technology, requires the same basic building blocks of traditional investigation, which include understanding the objective, compiling and preserving the available evidence, analyzing the evidence within the context of the original mandate, preserving the findings in a manner that they may be replicated and validated, developing a set of findings from the analysis of

the evidence, and finally, providing those findings to third parties. The provision of the findings that the investigator may have developed could be in a variety of formats, including ad hoc conversational meetings; in person or over-the-telephone contact; formal investigative reports, as part of an analytical process that is feeding data into a third-party data analysis or document review platform; or even expert testimony before a judicial body. However, in all cases the goal of the investigator is the same—to provide honest, objective, and thorough analysis of the available evidence as it relates to the mandate provided to the investigator concerning the dispute or issue that must be assessed.

There are ethical and moral obligations to which an investigator must adhere in order to meet his or her mission, and it is vital for clear communication to take place between those parties who are managing the investigation and those parties with whom the investigator must interact so as to ensure that the investigation has met its mandate and that the investigator is provided with adequate information to form conclusions or report on his or her findings. Throughout this volume, I comment on the roles and responsibilities of investigators in the forensic space, from the perspective of interacting with managers, counsel, clients, victims, and others who are likely to come into contact with the investigative computer forensic examiner.

There are numerous treatises on the technology and mechanical processes that forensic examiners may undertake in the pursuit of fact-finding in the digital age. This volume touches on these lightly and instead focuses on the softer issues of technology investigations and how to most effectively balance the relationships between the numerous competing entities within a typical investigation. Whether the investigation is structured around the electronic discovery reference model and is part of an e-discovery exercise or whether the investigation is an internal matter operating in a clandestine form to quickly ferret out fraudulent behavior of executives, there are countless aspects of the process that should be considered and thought through when building an investigative plan, when exercising the investigative process, and when preparing findings to present to third parties.

Computer abuse is rampant and can impact companies large and small, from payroll issues, where fictitious employees are created for the purpose of defrauding the company, to inventory abuse, where falsified records can be leveraged to extract monies from vendors or companies. However, these are not all the areas of computer abuse, which can also include accounts receivable, disbursements, hardware and software thefts, physical theft of property, personal information theft, and intellectual property theft.

This is only the tip of the iceberg, due to the ubiquitous nature of computing technology, which nearly every individual in the modern world leverages. As a result of significant computing power being placed in the hands of billions of individuals around the world, there has been an explosion in the awareness of many of these people as to how to leverage that power for illegal pursuits. With the compounding effect of robust processing power and access to information, coupled with the anonymizing capabilities of the global networks, such as the Internet, it is hard to imagine that illicit behavior in the information age will ever fully be contained.

Trust

Successful human interaction relies on a number of primary building blocks and paramount among them is trust. As old as humanity itself is the pursuit and care for this notion of trust. Trust between individuals, trust between organizations, and trust between nations are all vital for the human experience and for the human condition to thrive. Without trust, the bonds that connect individuals to one another are broken and cooperation fails. Without cooperation between parties, achievement is impossible, and achievement is one thing that human society has been very good at. Whether it is planting and plowing a field, building a barn, or constructing an interplanetary rocket, the ability for humans to achieve is firmly rooted in humanity's ability to form the bonds of trust, which foster cooperation.

Fast forward to the Internet age, this information revolution of which we find ourselves in the opening acts and in which we have already established the primacy of trust, for our communication is now no longer face-to-face. Our commitments are no longer bonded by handshake or an audible acceptance of one's terms and conditions in the proximity of one's peers. Today, our communication takes place electronically over telephone wires, cellular networks, wireless networks, Ethernet networks, wide-area networks, local area networks, ATM networks, microwave networks, and satellite networks.

This results in humans forming the same commitments, while being physically removed from one another, often over great distances of dozens, hundreds, thousands, or tens of thousands of miles, and without the benefit of interpersonal human interaction. These commitments are based on trust. Acceptance with the word *yes* or declination with the word *no*, typed into an electronic communiqué known as an e-mail and sent around the world at the speed of light, across fiber-optic cables running under oceans, requires both parties, sending and receiving, to have trust that what was sent and what was received in fact conveys the intention of the party that sent it and is in fact a bona fide facsimile of that transmission, received by the intended party.

Electronic commerce relies on this notion of trust, for I must believe that my bank, as represented on my computer screen, truly is my bank. I must believe that the balance shown on the screen is truly the balance that is in the bank. I must believe that the transfer that I have made from the bank to the electrical utility company has in fact taken place and that the utility company has received the payment. The utility company, on the other hand, has to trust that I will make that payment electronically from my bank, which the utility company must trust exists.

In the realm of communications, I must trust that the individual who has sent me the e-mail is in fact the individual that he or she purports to be, even before I begin to trust the content of that person's words. But, oh, how trust has been shaken, for I often do not know the true identity of the individual who has sent me the e-mail, nor do I have the ability to validate the accuracy of the words that he or she has written. Do I send the $5,000 check to Nigeria to help the deported oil minister's wife who wishes to share $10 million of her family money with me, if it will simply allow them access

to a U.S. bank account? Now, the Nigerian 419 scam is a well-known problem in the information age; while tens of thousands of individuals around the world have been and continue to be victimized by this scam, for the most part, possible victims are able to distinguish the scam using common sense when they read the e-mail from the purported widow of the Nigerian president or some other concocted story.

However, what does this do to trust when I have no way of validating the true author of the e-mail and I certainly cannot believe what it says? Should I use the same level of skepticism with every e-mail that I receive? Naturally, this would not work either, for I would spend my entire day questioning every e-mail that I receive. I would be paralyzed by inaction. This is how trust breaks down for the individuals who use the medium of communication used in this discussion—e-mail on the Internet. How, then, will cooperation be established and how can achievement take place?

Commerce and communication depend wholeheartedly on trust and it is vital to the continued development of the technologies that support the information revolution that they have mechanisms built in that allow for the cross-referencing, double-checking, and validation of entities, statements, and facts so that trust can be established, achievement can proceed, and this great new gift to humanity's future can be fully leveraged without enslaving people to Big Brother or to a world information anarchy.

The role of the investigative computer forensic examiner, while seeking out the facts of a given matter, is also, by association, one of establishing and protecting trust within the information age. Computer forensic examiners serve as the final stop on the information superhighway when it comes to ensuring that the data is what the data is, and they provide a vital service to defendants, plaintiffs, the accused, victims, individuals, corporations, government agencies, the judiciary, and society as a whole. Therefore, the imperative that investigative computer forensic analysts exercise good judgment, well-thought-out processes, and the highest ethical behavior is paramount within the discipline.

Privacy

Privacy is dead. Although trust still has a hope in this information age, for the time being, privacy is dying a relatively fast death and there well may be no hope to save the patient. It will be necessary for society to redefine privacy and to compartmentalize aspects of individuals' and organizations' existences in such a way that where there truly must be privacy, it can at least be private for most. However, this will come at a price, and I foresee that privacy, however tenuous it may be, will in the future be enjoyed only by those who have the resources to insulate themselves from the all-knowing electronic agents' grip on the metrics and statistics of each individual's behavior and movement around this fast-shrinking planet of ours.

Gone are the days when one can be born, live, and die in anonymity, for from the moment one enters this world to the moment one departs, there is now an indelible electronic data trail documenting and memorializing the activities of the

individual down to a granular level that would have been inconceivable a mere century ago. Whether your life has been voluntarily added to the human encyclopedia of Facebook or whether you have tried to "get off the grid," there is little way for you to effectively interact with modern society without submitting yourself on a wholesale basis to the altar of the data barons, who are amassing the greatest fortune in history, payable in the currency of our time—electronic data. Richer than the spice traders of the age of Magellan, grander than the captains of industry who built the industrial revolution's factories and railroads, and with greater renewable resources than those of the oil nations of the Middle East, the data barons, whose stock in trade is you and your behavior, are only now beginning to blossom into the forces of nature that they will become.

Bill Gates and Microsoft, Steve Jobs and Apple, Sergey Brin and Google, Mark Zuckerberg and Facebook, Jeff Bezos and Amazon.com are merely the early entrants and the pioneering names of what is now the greatest commodity the world has ever traded. This unending resource of truly valuable data is the aggregate electronic manifestation of all human behavior and thought. So you see, privacy is dead because it must be dead in order for this engine to feed, and this engine is much greater than any the world has ever seen, for its catalyst is the desires and hopes and needs of the very people off which it feasts.

The investigative computer forensic professional will often find himself or herself at the crossroads of these issues of trust and privacy, commerce and freedom, truth and failure, and cast into a cauldron of human expectations, tensions, desires, needs, and forces. Therefore, the role of the investigative computer forensic examiner, while at times mundane and mechanical, is in fact a vital focal point of numerous sociological trends that are of the most extreme relevance and urgency in our society.