Global Information Assurance Certification Paper

Overcoming Reasonable Doubt in Computer Forensic Analysis

By Jim Garrett, GCFA

July 2006

Gold Certification

FINAL

Table of Contents

Overcoming Reasonable Doubt in Computer Forensic Analysis

Section 1.0 - Introduction

Computer Forensic Analysis requires good tools, excellent training, broad experience, and solid critical thinking skills. The volume of data to review is usually massive and gaps can exist between the few known facts, the assumptions, a hand full of symptoms, and a number of plausible conclusions. Without correlating data carefully, it is difficult to make accurate and compelling claims about a computer attack. As if gigabytes of raw data weren't enough, the forensic data is not just within the computer, it also exists on the outside with the social context of the perpetrator or victim. Clues from behavior, skill-set, relationship, equipment, location, and motive can strengthen or weaken the data found on a computer. The forensic challenge can be like finding the proverbial needle in a hay stack.

So how can the forensic analyst meet this challenge? How is critical thinking practiced, and how is reasonable doubt removed from the analysis? The capable forensic analyst must use the logic models of abduction (generating a hypothesis), deduction (using facts to prove the conclusion), and induction (building a case backwards from the evidence) to overcome reasonable doubt. Good forensic tools and techniques draw out the computer data required to solve a case, but skillfully applying logic models and critical thinking to both the technical and sociological contexts does the rest. This paper will describe classical logic models for use in computer forensic analysis to assist in attaining reasonable certainty during an investigation.

Section 2.0 - Using Logic to Solve Crime

The logic models of abduction, induction and deduction have been used in modern criminal justice for over one hundred years. They are frequently applied in the investigation of traditional criminal offenses such a robbery, theft, fraud and burglary (Benny, 2006). They have also been extensively used in the investigation of criminal profiling of serial killers, sexual predators, drug dealers, and as recently as Sept. 11, 2001, terrorists (Turvey, 2001).

A recognized and famous use of the concept of inductive and deductive reasoning is in the works of Sir Arthur Conan Doyle in the Sherlock Holmes stories, first appearing in 1892. Sherlock Holmes used logic models to not only solve crime but to build a profile of an individual (Benny, 2006). Based on observations of the facts, Holmes would build a hypothesis and then deduce further hypothesis around the facts. For example, when Holmes first met Dr. John Watson he observed that Watson had an injury and hypothesized that he had recently received it during combat in Afghanistan while serving as a surgeon in the British Army. How did he do this?

Holmes used logic. First he observed that Watson was favoring one of his shoulders and so he deduced that he had a recent wound. Then, because of the rigid and formal way in which Watson carried him self, Holmes deduced that he was a military man. Looking at Watson's face, Holmes observed it was deeply tanned. Holmes already knew from Watson's title and admissions that he was a Medical Doctor, and he also knew that the British Army was engaged in a battle in Afghanistan (a place where an individual could obtain a tanned complexion). So Holmes correctly concluded that Watson was an Army Officer and Surgeon recently back from battle in Afghanistan, where he was wounded in the shoulder (Doyle, 1882).

The Holmes stories so effectively dramatized the theory of inductive and deductive reasoning that they are used today by the Metropolitan Police Department, Scotland Yard, at their detective school located at the Peel Academy outside of London (Benny, 2006). If we refer back to the narrative above, we can see that Holmes used the basic techniques of logic that the Computer Forensic Analyst must apply, also: 1) Observe the world and gain experience (Induction); 2) Theorize about what we are experiencing (Abduction); and 3) Reuse this combined experience and theory to predict events in the world (Deduction). These are three primary models in logic: Induction, Abduction, and Deduction, respectively.

Section 3.0 - A Quick Logic Overview

Induction is commonly referred to as empirical logic – logic derived from observations about the world. Induction is the process of reasoning where the premises of an argument support the conclusion but do not ensure it. Each observation of the world, although yielding the same results (e.g., the sun rises each day), is unique. Just because we have seen the sun rise everyday does not mean it will rise tomorrow. Each observation is a complete and separate instance from the one before. With induction, we observe as much as we can about the world and then define general laws based on one or a small number of observations or experiences of recurring patterns: the sun always rises is a rule that people hold to be true.

Induction is used to infer the general from the specific. Specific instance can add up to one big generalization. There are two types of induction, strong and weak, differentiated by sample size and statistical factors:

All ***observed*** crows are black.

Therefore,

All crows are black.

(Strong induction)

Hackers consume lots of caffeine.

Therefore,

All hackers drink coffee.

(Weak induction)

Abduction is simple. It is a hypothesis. What do we believe to have happened and when, where, why, how, and by whom based on our observations? Abduction and induction are closely tied - where abduction is the end result of the induction process. It is important for us to focus on and single out abduction, because in Computer Forensic Analysis forming the hypothesis is critical. A couple of things to consider:

1. Data must be collected before the Abduction can be made.

2. Abductions can change, emphasizing or de-emphasizing certain leads.

Deduction is used in axiomatic mathematics to prove theorems and is sometimes referred to as rational logic. A deduction is a sequence of statements such that every statement can be derived from the statements before it. This leaves open the question of how we prove the first statement (since it cannot follow from anything). In mathematics, this is

solved by defining axioms or primitives that all logic can follow from. Unfortunately, these axioms and primitives cannot be proven without circular logic (referring back to the axiom or primitive itself as part of the proof). For example, we can define a line as a set of points, but to then define a point as the intersection of two lines would be circular. So the axioms and primitives are assumed true, even though they can't be proven without circularity. Because of this interesting characteristics of deductive systems, Bertrand Russell (widely acclaimed 20th Century British Mathematician and Philosopher, 1872-1970) jokingly referred to mathematics as "the field where we don't know what we are talking about, nor whether or not what we say is true".

In the real world (i.e., not the world of pure mathematics), we use deductive formulas (*if A and B then C; if not (A and B) then not C*) to help explain observations, but we don't have axioms or primitives that always hold true, therefore we cannot conduct deductive proofs for the observations the way we can deductively prove theorems in mathematics. We'll pursue this important philosophical point later. Still, we can and do make observations about the real world using deductive constructs "If A and B, then C":

All men are mortal.

Socrates is a man.

Therefore Socrates is mortal.

(All it takes is the observation of one immortal man to make this false)

All birds have wings.

A cardinal is a bird.

Therefore a cardinal has wings.

(Is there a wingless bird that we have not observed?)

Deductive logic constructs (*if a then b*) are used throughout the inductive reasoning process to reach the Abductions. It is important to understand these constructs, but they are straightforward and dry and do not offer the techniques that are the goal of this paper, so a table is attached in Appendix B to reference for the interested reader.

Section 4.0 - The Logic 3 Step

There are important logic techniques for the Computer Forensic Analyst to use during the forensic investigative process. First, before we go there, we must understand the basic inductive reasoning process because it is the cornerstone of reasoning about observations made in the world, as we defined above. The deductive reasoning process is simple on the surface and involves three easy steps:

1) Gather data,

2) Make generalizations leading to the Abduction (hypothesis)

3) Use the new Abduction as a premise to "prove" other Abductions

This seems iterative, and it is. We gather, generalize, deduce the Abduction (hypothesize), gather more data, apply our new premise to the new observations and deduce more generalizations, and so on. Here's an example:

1) Gathering data from a hard-drive we observe the executable Dameware.exe.

2) We research Dameware.exe using an authoritative source and determine it is a freeware administrative tool closely associated with the hacker community.

3) We make a generalization (the Abduction) that a hacker used Dameware.exe to run a compromise on the computer.

Now we move our Abduction to the premise because that's the inductive reasoning process, and our *new premise* becomes:

New Premise - Dameware.exe is used to compromise the computers in question,

From this new premise we can make *new generalizations,* and if we gather more data and observe these generalizations to be true, then we become more confident:

New Generalization – A future compromise of this type will involve Dameware.exe

New Generalization - We will find that the DWRCS.exe process is running on the compromised computers, since it is the dameware.exe process name

New Generalization - Administrator passwords are compromised, since Dameware.exe needs them to be used.

The generalizations we reach from the new premise must each be tested by pursuing further observation. Then we can possibly make a new Abduction, more generalizations, and so on. With enough compelling generalizations and testing, we have a good case.

Section 5.0 - What is Reasonable Doubt?

Let's now discuss the philosophy behind the generalizations made through the inductive reasoning process. Not to burst Sherlock Holmes' bubble, but his observations did not "prove" that Dr. Watson was an Army Surgeon recently back from Afghanistan, they only inferred it through use of the inductive reasoning process. Holmes observed, made generalizations, formed the Abduction (hypothesis), probably made other observations and generalizations, and then formed the final Abduction. Is there any reasonable doubt?

1. Watson carries his shoulder as if it has been injured
2. Watson carries himself with an air of authority, honor, valor, dignity
3. Military men carry themselves with an air of authority, honor, valor, dignity
4. There is a war going on in Afghanistan
5. People with tan skin spend time in hot climates
6. Afghanistan is a hot climate
7. Dr. Watson is an MD
8. A qualified MD could work as a surgeon in an Army hospital

Would all British MDs with an air of authority, a tan, and a shoulder problem have spent time in Afghanistan as a surgeon with the British Army? We can imagine a circumstance where Holmes' reasoning is countered. It is possible that Dr. Watson was an accomplished MD, from a smug aristocratic family, who was recently on vacation in the hot climate of the South of France and injured his shoulder playing cricket on the beach. This seems reasonable, too. But maybe Holmes observed some other clues that made him more certain. The point is that it is possible to reason differently from the same information.

The Scottish philosopher David Hume provided some interesting critiquing of inductive reasoning one hundred years before Sir Arthur Conan Doyle was using it. His writings were controversial because they were intended to critique the Catholic Church's reasoning of divine morality. Hume attempted to disprove the Catholic Church supposition that moral human reasoning leads to moral human behavior. Hume disconnected the morality of actions from the morality of human reason. To do so, he highlighted that the actions observed in the world (inductively) could not be proven (deductively) - in the same way that Sherlock Holmes could not prove that Dr. Watson was a British Army Surgeon returning from Afghanistan - because the observations were of "original facts and realities, complete in themselves" and independent of human reason. Hume's argument is "heady stuff" and I've left it for the interested reader in Appendix A.

Hume highlighted that our everyday reasoning depends on patterns of repeated experience with the world rather than deductively valid reasoning innate to human thinking. For example, we might believe we will stay nourished with bread from the baker because we have done so in the past, but this is not a guarantee (the baker may die, the wheat crops may wither, the bakery may burn down). As Hume once said, someone who insisted on sound deductive justifications for everything would starve to death.

Preoccupation with questioning the observations of the world could lead to what Hume referred to as "unproductive radical skepticism" (i.e., nothing in life is certain, because reality is only based on our last observed moment in life) and paranoia. Instead, Hume recommended *practical skepticism* based on common sense, where the likelihood of an inductive conclusion is accepted but with a little skepticism.

In fairness to the reader, David Hume's work was not the "end all, be all". Immanuel Kant, a 17th Century German philosopher, published The Critique of Pure Reason in 1781. Kant's objective was, in particular, to counter the empirical thinking of David Hume. Kant argued that there are synthetic *a priori* truths – truths that are "built in" to nature but that humans can never readily experience. He reasoned that statements such as those found in geometry and Newtonian physics are synthetic *a priori* knowledge.

A good and recent example of how Hume's practical skepticism challenged Kant's theory of synthetic *a priori* truths occurred in the 20th century, directly against Newtonian physics. Newton formed a law of gravity (the force of gravity is directly proportional to the product of the two masses, and inversely proportional to the square of the distance between them). For over 170 years, all observations seemed to validate his equation. However, telescopes eventually became powerful enough to detect a slight discrepancy in the orbit of Mercury. Scientists tried to explain it, but they could not. Eventually Einstein developed his theory of General Relativity and it explained the orbit of Mercury and other known observations dealing with gravity. So for a long time scientists were making observations that seemed to validate Newton's theory but did not prove his theory to be true.

Observations that seem to validate a theory about nature do not prove it is true, and one counter-example can prove it false. This is typical of inductive logic. Einstein's theory of General Relativity has been supported by many observations using scientific instruments and well constructed experiments. However, his theory now has the same status as Newton's theory of gravity prior to seeing the problems in the orbit of Mercury. It is highly credible and validated with the best scientific methods, but it is not proven.

A good question is: when have we performed enough observation to achieve reasonable certainty? The answer is: In nature, time is the ultimate enemy. Just ask the high number of District Attorneys who have had their convictions overturned by DNA evidence. They were once certain and had presumably removed all reasonable doubt from a jury! The important point for the Computer Forensic Analyst is that logical reasoning about nature cannot prove the truth of an observation in nature. More skeptically, logical reasoning about observations in nature is inherently erroneous because although empirical evidence can be used to induce a conclusion, that conclusion cannot be proven. Creating a compelling argument is an awesome responsibility because it can lead to indictment (social, political, moral, or criminal) with severe consequences for the suspect even though it ***may*** be wrong! The Computer Forensic Analyst must be a critical thinker, always applying practical skepticism, and using solid techniques of logic to organize and defend against the fallacies of human thinking.

Section 6.0 - Striving for Reasonable Certainty

Now that we are armed with some definitions and philosophical background, it is time to get down to business. To make a compelling argument, we must employ as many inductive reasoning techniques as we can so that we have overwhelming evidence to implicate our Abduction. Inductive reasoning is so important to investigative analysis that we must know the fundamental techniques well - and not only their proper usage but their pitfalls. The fundamental inductive reasoning techniques discuss here are: **Generalization, Statistical Syllogism, Simple Induction, Causal Induction, an Argument from Analogy, and an Argument from Authority.**

1. Generalization

What is it - It is what it sounds like. People make generalizations every day.

> *That guy is standing at the bus stop eating an apple;*
>
> *So, all guys standing at bus stops eat apples.*

That's a broad and bad generalization. We can already see when it might not be true. All it takes is for us to observe one guy standing at the bus stop who is not eating an apple, and the generalization no longer holds.

Hasty generalizations lead to false positives and questionable credibility. It is human nature to theorize and generalize, but do the raw stuff in your head or behind closed doors or always couch it as "brain storming." No one want wants to be known as a "Chicken Little" – "…the sky is falling, the sky is falling…"

How do we apply it - Define the population, first. Generalizations are made about observations of a population (types of things). With a computer security incident we can choose to narrow our population to one computer or broaden it to include all computers on which the incident occurred. We can even include computers on which the incident potentially could have occurred.

To determine the population, it's best to take a concentric ring approach, starting with where the incident is suspected to have occurred and then moving out from there. To do this, we may use many different reasoning tools, but the most powerful is Argument from Analogy (discussed further below) where we include items that have the similar attributes. If one computer on a Local Area Network (LAN) with a particular vulnerability is attacked, then other computers on the network having the same configuration, protocols, and vulnerability may be included in the population. Further, if a local area network is also connected via WAN to international locations, the possible population of the incident could increase as incidents may have occurred at other locations.

Even if we are dealing with a single computer, the need to identify the population still applies. In data stream analysis, we need to focus the population around certain types of

transactions, IP addresses, protocols or ports (e.g., 80, 21, FTP), or where a particular process is being run. The volume of data for any one of these protocol streams can be significant and accounting for the entire population of one of these areas, through capturing and parsing the data stream, is typically a required task.

Accounting for the population (location, devices, users, etc) is critical because it allows us to know where we can make valid observations to help build our case and where to look further if we run into a dead end. Whether at the macro level of the network or micro level of the transaction, the population for the observations must be clearly noted.

Fallacies to watch for – Knowledge of the population is important. A Computer Forensic Analyst is not necessarily qualified to conduct forensics on a human corpse. Training and certification are of high importance.

Hasty Generalization: Good generalizations come from good experience about a population which comes from making good (and bad) generalizations. Brainstorming or communicating with a close confident are the best ways to flush out the bad generalizations. A generalization based on too little evidence, or on evidence that is biased, results in a hasty generalization. Example: John is a gamer (likes and plays computer games online) and he has two computers at home, therefore John is a hacker.

Either/Or Fallacy - False Dilemma: Inductive reasoning can lead to assuming that there are only two alternatives, such as X and Y. Usually, this occurs when premises are weak, and only less than desirable suspects can be identified from the parts of logic (poor sample size). A false dilemma exists when a choice must be made between two undesirable alternatives, and the persuasion in the argument is limited to choosing the least undesirable alternative. If this is the case, there always is a Z factor, or third alternative. Ramsland, K. Ph.D. (2000).

2. Statistical Syllogism

What is it – This is a statistical weighting of the observation. A statistical syllogism leads to a conclusion based on statistical data.

> *A man standing at the bus stop was seen eating an apple, so there is a probability that John, currently standing at the bus stop, will eat an apple*.

How do we apply it - Observe the right sample size. Once the population, or scope, is determined, the data must be observed or "sampled" to proclaim a generalization. Strong inductive generalizations require a good sample size so that we can make a statement that we can say is representative of the population. It's not good practice to say that because we saw one FTP transaction going to a suspicious source IP address that it is through FTP that the computer was compromised or that the IP address is the source of the attack (this is a *Hasty Generalization*). More samples of FTP transactions or transactions from the source IP address must be taken, and correlations with other data must be made. This seems like a lot of work. If the population is large (thousands or millions of transactions),

we can't expect to observe all activity in the population. So, how much of the population do we need to observe? What is the proper sample size?

Size matters only in a relative sort of way. It's all relative to the population size being sampled. If there are only 15 workstations on the network, then the universe of workstations is just 15 so a good sample of workstations could be a small number – say 3. If a network attack is made across a network having thousands of machines, collecting enough forensic images of specific computers will be required to build a strong inductive generalization. But it is not as many as you think. Based on statistical sampling tables, it does not take a large sample size of a given population to derive a statistically significant (accurate) result. For example, to determine with 95% accuracy, +/- 5%, that the abduction is true for a population of 1 million entities, one need only sample approximately 384 of the entities.

> In simple random sampling from a population of size N, what sample size n is necessary to determine the mean μ to within the maximum allowable difference D with confidence P. Thus we want n = prob ($|m-\mu| < D) > P$. (Thompson, S, 1992)

If we have a pretty compelling abduction, it will be well worth randomly picking 384 of the 1 million and then personally inspecting each one.

The statistical syllogisms used in inductive reasoning can strengthen or weaken an argument. Here's an example. If 15 separate hacks to 15 separate network computers have occurred and it is found forensically that the each and every one of the 15 computers contains an unauthorized peer-to-peer connectivity executable, a 100% statistical syllogism can be drawn linking the executable with the attack. This does not mean that the peer-to-peer executable was used in any way to execute the attack. There must be evidence of cause-and-effect correlation between the two entities, discussed below.

Fallacies to watch for - Usually a fallacy here involves not having a proper sample size or making generalizations using a low statistical ratio. If we observe something occurring only 10% of the time, we should not infer that there is a *high* likely hood that it will happen – this is common sense, but in the heat of an investigation, sometimes the pressure of finding an answer can lead to poor interpretations of the data.

The Fallacy of Composition: This is the mistake of inferring that a property of the parts must also be a property of the whole (Gocsik, K., 2004). Example: Spy ware was discovered on the computer of two of the company executives, therefore all company executives have spy ware on their computers.

3. Simple Induction

What is it - This combines a generalization and a statistical syllogism into a hypothesis.

> 10% of the men at the bus stop have been observed eating apples.

John is standing at the bus stop

Therefore,

There is a 10% chance that John will eat an apple while standing at the bus stop.

How do we apply it – Use the 3 Step Process. The 3 step inductive reasoning process noted above is used here: Observe the data, calculate statistical syllogisms when possible, and then make the Abduction (hypothesis). Abductions must be declared and then critiqued – this leads to further questions, efforts, and subsequent discoveries that can in turn strengthen or weaken the argument for the abduction. So at some point the behind closed doors thinking must come out. It is still worth the self restraint to confine the abductions to the investigative team (the need-to-know team) or even a smaller group (a trusted brain storming partner).

Fallacies to watch for – The pitfalls in this area are similar to those in the generalization area. Basically, coming up with a good Abduction takes good data (a large sample size) and experience, but there are some embarrassing logic traps that can be fallen into.

Non Sequitur: The conclusion does not follow logically from the premise. Example: His computer was expensive; therefore he knows a lot about computers.

Red Herring: Distracting the audience by drawing attention to an irrelevant issue (Gocsik, K., 2004). Example: The network is so slow anyway, so don't worry about getting a computer virus.

Circular Reasoning: Asserting a point that has just been made - sometimes called "begging the question" (Gocsik, K., 2004). Example: We were hacked into because hackers found a way in.

Equivocation: This is equating two meanings of the same word falsely. Example: The hacker owned the network; so laptops personally owned by associates should not be allowed on the network. (The argument is fallacious because there are two different definitions of the word "owned" involved in the argument.)

Affirming the Consequent: Inductive reasoning is "bottoms-up" and "backward-looking" because testing involves moving the conclusion to the premise. This involves treating the conclusion as a hypothesis, and going back to each other premises seeking any dissimilarities, flaws, or differences that would disconfirm the conclusion. The obvious flaw is when there is no witness of the event (Ramsland, K. Ph.D., 2000). The flaw is in saying: A hacker entered our network and John is a hacker, therefore John entered our network. Unless we have further data to substantiate that the hacker that entered our network is John (through time stamp, witness, or other correlation to test the conclusion) we can't say as a premise: John entered our network.

4. Causal Inference (Prediction)

What is it - This is the classically known cause-effect relationship. A prediction leads to a conclusion about the future from a past sample.

> 10% of men standing at the bus stop eat apples
>
> *Therefore*,
>
> There is a 10% chance that the next man coming to the bus stop will eat an apple.

How do we apply it – Predict the result of future observations. Using statistical syllogisms, it may be possible to predict future events. Though the prediction may be obvious, that is the point – it becomes obvious enough based on all the previous observations and to create a generalization, and it should be tested to strengthen the abduction, *formally*. For example, if the analyst can predict that the next attack will be on a particular network segment or that a specific peer-to-peer executable will be found on the next attacked computer that can be enough to confirm assumptions and to justify the further efforts in investigatory focus. We can use prediction to make ourselves look good, to build our confidence, and to prove to our peers and boss that we are thorough and accurate. .

Fallacies to watch for – False cause and effect relationship is very common.

Post Hoc, Ergo Propter Hoc: The mistake of assuming that because event "a" is followed by event "b", event "a" caused event "b". Example: He didn't agree with the security proposal, that's why his computer was hacked into.

5. Argument from Analogy

What is it - An inductive analogy is derived from known similarities between two things to a conclusion about a new similarity common to both things:

> Jane is a woman, and women are similar to men,
>
> 10% of men eat an apple while standing at the bus stop,
>
> *Therefore***,**
>
> There is a 10% chance that Jane will eat an apple while standing at the bus stop.

How do we apply it – Form a hypothesis using similarities. Use this technique to *stretch* the hypothesis, going outside of the safety envelope. Analogies can be particularly insightful when drawn using data outside of the computer data. For example, if the attack on the network appears to be random, there may be similarities of the victims that link the attacks. What if the computer of one marketing executive and the computer

of one product manager are attacked? Could an analogy connecting product pricing data and marketing pricing rebate data be made? The product data and pricing data have similarities that could lead to the Abduction that competitive espionage or intelligence gathering is underway.

Fallacies to watch for – The key to making good analogies is ensuring the entities compared are indeed similar (physically, functionally, temporally, geographically, etc). This is can be important when narrowing the population of scope of the investigation.

False Analogy: Wrongly assuming that because two things are alike in some ways, they must be alike in all ways (Gocsik, K. 2004). Example: Bob is a young IT professional and is also a gamer Jim is also a young IT professional, so Jim must be a gamer too.

6. Argument from Authority

What is it - An argument from authority is when determination of the truth of a statement is based on the credibility of the source of the statement, which in turn is based on the proportion or percentage of past truthful statements made by the source. It has the same form as a prediction.

> 95% of the time, what Jerry tells us about activity at the bus stop is true
>
> Jerry says he saw a dog eating an apple at the bus stop
>
> *Therefore,*
>
> It is 95% likely that a dog ate an apple at the bus stop

How do we apply it – Use credible sources. This technique is used in every day social situations. They key is in drawing conclusions based on credible and trusted sources, or experts. In the computer security field, we have many recognized sources of authority: SANS, CERT, CIAC, Symantec, ISS, Verisign, etc. And when conducting computer forensics, we reference these sources to establish generalizations about our observations. For example, we find KaaZa, an open IRC port on the firewall, and an unknown executable process running. A quick look to Symantec for the process may tell us that it is a Trojan horse. Symantec is the source from which we can make the Argument from Authority. At another level, in the world of Incident Response, there is normally an authoritative document or entity that defines attacks, risks, and can trigger an investigative event (the IDS blade is the authoritative source). An incident Argument from Authority may come for a recognized commercial source such as CERT or SANS, where reputable resources communicate observations about the world to a set of subscribers. At the detailed level, the Computer Forensic Analyst should conduct technical analysis using tools recognized and validated by credible security organizations, such as SANS and GIAC, and descriptions of computer attacks and signatures should be only be heeded from credible security organizations such as Symantec, SANS, CERT.

Fallacies to watch for – *Credible* and ***impartial*** are the watch words. Expert witnesses, commercial tools, formal training and certifications (GIAC), recognized organizations (SANS, CERT, GIAC and CIAC) are good Arguments from Authority sources. Tools from a hacker site or warnings from an email chain letter are not good Arguments from Authority sources.

Emotional Reasoning: Is there any emotional tie to the reasoning? Are there any specific words used that may portray any special meaning or that conjure up images of a perpetrator or cause? With inductive reasoning, it is best to remain impartial and impersonal (Ramsland, K. Ph.D., 2000). Example: I hired John therefore he wouldn't have hacked into the HR server.

Ad Homine: One can think of this as "Arguing against the man instead of against the issue" (Gocsik, K. (2004)). Example: We can't promote him to security manager because he's not a member of Toastmasters!

Section 7.0 - Testing for Reasonable Certainty

The goal of a prosecuting attorney in a criminal case is to remove *reasonable doubt* from the minds of the jury. Similarly, but on the opposite end of the spectrum, the goal of the Computer Forensic Analyst is to achieve evidence with *reasonable certainty* using the data at hand. To do this, collecting the right data and creating overwhelming evidence (observations that logically follow) is required. So how can we use the six inductive reasoning techniques to build the case for *reasonable certainty*?

We can create a table representing the two ends of a reasonableness spectrum and illustrate that the inductive reasoning techniques can be used to demonstrate a case for reasonable doubt or a case for reasonable certainty:

Table 1 – Reasonable Doubt versus Reasonable Certainty

Reasonable Doubt	***Reasonable Certainty***
Small sample size	*Generalizations* using a large sample size
Low statistical ratios (probability)	High *Statistical Syllogism* (probability)
Weak, fallacious induction	*Abduction* with large sample size and statistics
Inaccurate predictions	Accurate *Predictions* from large sample size
Poor or fragmented analogy	*Analogy* based on known, demonstrable similarities
Witnesses with poor credibility	Expert witnesses with *Argument from Authority*

An important question is how can we test that our inductive reasoning approach has achieved reasonable certainty? We must check to see that we have applied the techniques correctly, starting with the Argument of Authority. Having the proper training, experience, and authority to act (e.g., through policy or contract, etc) is critical before proceeding with any analysis. Conclusions reach using non-credible or unauthorized sources can compromise the case or result in rework to validate. From there, we must check to see whether we have used the right population. If we make great analogies with the wrong population, then we are expending a lot of worthless effort. Next, we follow with the other techniques, and check that each is used correctly, e.g., if we make predictions based on poor sample sizes, the predictions could be inaccurate.

Drawing from the discussion above, we can construct a series of questions to apply as a means of testing any hypothesis of a computer forensic analysis as in Table 2 below. There is a deliberate ordering in the testing. The Argument from Authority and generalizations from the right population are critical. Using non-credible resources and examining the wrong population result in suspect conclusion of the other techniques:

Table 2 – Six Tests To Achieve Reasonable Certainty

1. Are the tools, techniques, and individuals used to collect the data and reach hypothesis qualified through a proper authority (commercially available tools, industry acceptable tools and techniques, training from authoritative sources, best scientific instruments and methods, validations or declarations made by authoritative sources or experts and eyewitnesses)?
2. Is there a complete accounting for the population of data involved in the incident (do we have an inventory of media, users, devices, and network connections that may be involved in the incident?)? Do we know the entire boundary?
3. Is the sample size of the population used to reach an Abduction large enough and random enough to represent the population?
4. Are statistical ratios correctly applied to strengthen (or weaken) the data leading to the Abduction?
5. Are successful predications attempted and achieved to prove the correctness of the Abduction?
6. Are all analogies or comparisons used to reach the Abduction made using close examination and validation of the similarities between the entities compared? (i.e., Apples to Apples).

Interestingly enough, failing a test does not make the hypothesis wrong. Sometimes guesses are right. What it does is weaken the case and compelling argument necessary to reach reasonable certainty of inductive reasoning. It casts doubt with the receiver of the conclusion – if the receiver is a jury, then even though the conclusion may be right, the jury may still have reasonable doubt.

Section 8. 0 - A Case Example

The case study is based on an incident that occurred early in the 1990's. It took place at a multi-national U.S. company, involved economic espionage (or more accurately, economic sabotage) of a projected $3B in revenues, resulted in a tidy conclusion, and involved engagement of the FBI. We won't go into any details of the indictments, penalties, or prosecutions that may or may not have resulted, but we will discuss the "sources and methods" leading to the tidy conclusion, and additionally we will post mortem attempt to apply the logic reasoning techniques discussed in this paper.

Our goal is to discover where we did apply or, in hindsight, could have applied the inductive reasoning techniques above and then provide judgment on the reasonable certainty of the conclusion reached in the case. For obvious reasons, we will intentionally attempt to mask the identity of the company, its location, and individuals involved in the case and just focus on the "sources and methods" applied to reach the conclusion. The particulars of the case are as follows:

The legal department of a multi-national company receives a certified envelope from the legal department of another multi-national company (a competitor). In the envelope the legal department found two objects: 1) a letter and 2) another small envelop addressed to the competitor multi-national company inside which is found another letter and a computer CD disk. The letter read, to the effect:

> *Dear Legal,*
>
> *Enclosed is an envelope that we assure you our company received unsolicited and anonymously. We read the letter and it indicated that the enclosed computer CD contains highly confidential and proprietary research information belonging to your company. Upon reading the letter, we immediately notified you and as per our discussion we have forwarded the original envelope, letter, and computer CD to you. We emphasize that we did not attempt to open or read the computer CD and we have not made any attempt to identify the anonymous sender.*
> *If you have any questions, please contact me directly.*
>
> *Cordially,*
>
> *Legal Counsel*

The receipt of the envelope launched a number of actions, the first of which was contacting the company Corporate Security organization and the Chief Information Security Officer (CISO). Leaving to the reader's imagination all the other contacts, activities, and phone calls that were made, we can jump directly to the kick-off of the investigation and the collection of data.

Most of the discoveries took place with a visit to the research facility where the particular research described in the letter was performed. A team consisting of IT, Security, Legal,

Business, and Research leaders was assembled to discuss the incident. The team needed to validate the content of the computer CD and discuss the implications, if any. Did the computer CD really even contain the proprietary research data? Or was the anonymous letter just a hoax?

The computer CD was a read-only CD, but sensitive to and knowledgeable of maintaining the integrity of the computer evidence, the team was hesitant and cautious about reading or copying the entire CD. Since copying a computer CD at the time effectively involved reading it with one computer and copying it to another, the more time efficient and less intrusive approach was to perform a detailed directory and subdirectory listing of the computer CD and writing the listing directly to a file for further review. This would yield a file listing name, size, type, owner, and MAC time stamping of the contents.
The team waited anxiously as the DOS commands were executed to list the content of the CD, and a file was sent to a printer, multiple copies, and then handed out around the table. The eyes of the business and technical research engineers bulged as they scanned over the printout. "These are the names of the files and topics of our research, all right!" One of them exclaimed. "Yep, this is the research that would lead to our advanced products for the next 10 years!" another confirmed.

The printout contained a listing of about 40 to 50 files – mostly spreadsheets and text documents. The team quickly identified a few documents, by name, as being key research papers or technical specifications with dates consistent with the time of the document creations. This set the team into a new focus that up until then had been muted by the unknown:

Who was the anonymous sender?
What did all this research data amount to, really?
Why did the person send it in the first place?
How could we discover who they were?

The team immediately turned to brainstorming the perpetrator's identity. Who was disgruntled, recently disciplined or terminated, and what were the other possible motives? Fortunately the team included seasoned Corporate Security investigators – ex-government agency types. They quickly narrowed on the most likely motive and group of suspects: a disgruntled employee from within the research group. The research group supervisor identified a short list of three, one of which had recently quit the company. With only this very small bit of information, the investigation moved into data discovery mode.

The first order of business was to have all researchers log off of the network – about 12 of them in total. Then a search for the ex-research employee's computer workstation took place. He had left the company 6 weeks earlier and his computer had been refreshed – it was an older machine, and given that he was no longer with the company, it was taken by the IT staff and disposed of. Before disposing of it, the data had been written to a network server and the computer hard drive had been wiped. It was gone. This was

common practice for this company, and so there were no suspicions related to the expediency of disposing of the computer. The next action was to determine if there were any CD burners (a relatively new and uncommon tool at that time) that the research group had access to – and there was one dedicated CD burner in a common cubicle. Then the network was checked. The important question to answer was, were the documents listed on the computer CD directory printout on this network or not? An administrative privileged account was used to search the network using the Microsoft search utility.

The files were discovered on the archived directory where the suspected ex-employee's data had been saved (about 80% of them) and also across the network in a number of other employee server directories. The largest single cluster was on the ex-employee's archived directory. The file sizes were reviewed to better correlate the data, and this validated to the team that, indeed, the data was proprietary research documents that had been created by this research group.

The next step was correlating the creation of the computer CD to a particular associate. The obvious place to start was with the creation dates from the printed directory listing. They had been created on two particular days about 4 weeks earlier: on a Thursday after 6pm and on a Sunday in the morning. The fact that the dates were 4 weeks earlier made it possible that the ex-employee who the group leader offered as a suspect be the perpetrator. The after hours and on weekend creation dates was also consistent with the profile of a perpetrator trying to commit the act without discovery. The next step taken by the team was a strong clincher. The badge access system for the facility was reviewed. The research facility was secured and badge access was mandatory. The ex-employee, the suspected perpetrator, had entered the facility on the two days the proprietary data had been written to CD: on Thursday after 6pm and on that Sunday in the morning. A quick historical search indicated that this employee had rarely if ever come into work after hours or on weekends (likely because, using other data collected, his commute was very long, he didn't have a car and he took the train into work).

The other clincher(s) came from the envelope. Although the envelope in which the computer CD was sent had no return address, the post office which processed and stamped the envelope was in the general geographic area where the suspected perpetrator resided. Also, though the envelope, enclosed letter, and CD contained no finger prints, a finger print was lifted from the sticky side of a piece of scotch tape used to attach the CD to the letter, and it later matched the suspected perpetrator.

From there, the incident was turned over to the FBI, who proceeded to pull workstations and conduct interviews per their protocol. Clearly, things did not turn out well for the ex-employee and suspected perpetrator. The end result of the case was never debriefed to the CISO. So the pressing question remains, was there enough integrity in this investigatory process. Did the team wrongly or rightly indict the ex-employee with the evidence that had been collected and presumptions that had been made? Was there reasonable certainty to turn the data over to the FBI? The team seemed to think so.

Section 9.0 - Applying Logic Techniques to the Case Example

We need to go back through the description of the case above and pick out the empirical observations collected that led to the conclusion. What were the observations, deductions, abductions and the new observations? Let's list the observations:

1. A competitor received the envelope
2. The competitor expeditiously notified the victim company
3. The competitor claims to not have read the computer CD
4. A listing of the files on the Computer CD were validate by the research group leaders
5. The research group leaders narrowed a list of suspects (ex or current associates)
6. The seasoned Corporate Security investigators elected to act on pursuing information about the ex-employee.
7. The team reviewed the files on the network of the researchers and found roughly 80% of them in the archived directory of the ex-employee.
    a. Another 15% of the files were found in various directories of the network.
    b. Not all files were accounted for – only about 95%.
    c. The largest single-cluster of documents (the 80%) were found in the archive directory of the ex-employee. Other researchers had maybe 30-40% of the documents on their server directories.
8. A CD burner was available to the researchers – including the ex-employee.
9. The data and time of the file burning to CD was after hours at times when few other researchers would be in the facility.
10. The facility access swipe of the ex-employee overlay nearly exactly (+/- 40 minutes) the creation times of the files burned to the CD.
11. The post office from which the envelope was sent was in the general geographic vicinity of the ex-employee and s finger print lifted from scotch tape found in the envelope matched the ex-employee.

Let's see how we can apply the inductive reasoning techniques to each of the observations and abductions above and determine the reasonable certainty of the conclusion. See Table 3, below (Mapping Inductive Reasoning Techniques to a Case Study):

Table 3 – Mapping Inductive Reasoning Techniques to a Case Study

A competitor received the envelope	*Argument from Authority*
The competitor expeditiously notified the victim company through certified letter	Empirical observations via time stamping of envelopes
The competitor claims to not have read the computer CD	*Argument from Authority*
The significance of the files on the Computer CD were validate by the research group leaders	Empirical observation with *Argument from Authority*
The research group leaders narrowed a list of suspects (ex or current associates)	*Argument from Authority and Argument from Analogy* (like researchers are suspects)
The seasoned Corporate Security investigator elected to act on pursuing information about the ex-employee.	*Argument from Authority*
The CISO reviewed the files on the network of the researchers and found roughly 80% of them in the archived directory of the ex-employee. Another 15% of the files were found in various directories of the network. Not all files were accounted for – only about 95%.	*Statistical Syllogism* – **large sample size** (all files searched on all devices of the network) and high ratio of document match on **the right population**. **Low ratio** of files found on other researcher directories. **High ratio** of files found on ex-researchers archive directory.
Only one CD burner was available to the researchers – including the ex-employee	Empirical observation
The data and time of the file burning to CD was after hours at times when few other researchers would be in the facility.	*Statistical Syllogism* – low probability that other employee were perpetrators since they were not at the facility at the time of the CD burning
The facility access swipe of the ex-employee overlay nearly exactly (+/- 40 minutes) the creation times of the files burned to the CD	*Causal Inference*– good correlation that the ex-employee burned the CD since he had access to the data, access to the burner, his time in the facility overlapped the time the CD was burned, and he was the only person in the facility who had access to the research information on the network.
The post office from which the envelope was sent was in the general geographic vicinity of the ex-employee. A finger print lifted from scotch tape found in the envelope matched the ex-employee	*Statistical Syllogism* – unlikely that the envelope post office vicinity can be matched to the ex-employee (**low sample size**); but high probability that the physical thumb print match is indisputable.

So we went through an inductive reasoning process to reach the final Abduction (or hypothesis) that one ex-employee was the likely perpetrator. We made a number of observations, generalizations, and then applied the inductive reasoning techniques described above in an iterative way. A number of deductions led to the final Abduction as follows:

1. Proprietary data from a specific research facility was sent to the competitor or the victim company.
2. A ex-employee of the research facility had access to the research data
3. The ex-employee was dissatisfied with his work environment
4. The ex-employee accessed the facility on a Thursday and Sunday and was the only researcher at the facility with access to the data.
5. The research data sent to the competitor was created during the two days, in the same time frame that the ex-employee was in the facility after hours.
6. A CD burner was available at the facility for the ex-employee to use
7. A finger print belonging to the ex-employee was found within the envelope sent to the competitor
8. The ex-employee had means and motive to commit the act.
9. The ex-employee finger print was strong statistical evidence.

The conclusion follows readily from these generalizations and Abductions:

1. The ex-employee was a reasonable suspect to turn over to law enforcement for further investigation.

Section 10.0 – Summary

We cannot over-emphasize the awesome responsibility that lay in the hands of the Computer Forensic Analyst. Because of the technical and seemingly esoteric nature of the computer environment (the "black box" and "black magic" associated with computers), the integrity of gathering and interpreting the data is critical. Inductive reasoning is a cornerstone of the analytical process, and so the Computer Forensic Analyst must be well versed in all the strengths and fallacies of the inductive reasoning techniques. Finally, after all is said and done, and even the clearest and cleanest analysis is performed and conclusions are drawn, the Computer Forensic Analyst must apply practical skepticism. There may become a time when the conclusions drawn are "disproved" by one simple, overlooked or undetectable observation.

To recap, there are six techniques we should be well versed in as Computer Forensic Analysts, and we must understand the right and wrong ways to apply them. Additionally, we need to build a compelling argument using overwhelming evidence whenever possible. Ordering the techniques can help to ensure that the foundation of the case is strong:

1. Argument from Authority: start with the right credentials and authority
2. Generalization: observe a thoughtfully defined population and know the boundaries
3. Statistical Syllogism: use a correct sample size to strengthen generalizations
4. Induction 3 step: create logical Abductions and then venture into new observations
5. Arguments from Analogy: ensure comparisons are based on apple-to-apple attributes, or use analogy to "stretch" the population envelope
6. Predictions: test the Abductions; Can they be predicted?

Critical thinking skills are basic for a Computer Forensic Analyst. Attaining reasonable certainty during an analysis requires application of good critical thinking skills. These logic techniques will help. When applied correctly while using practical skepticism, the Computer Forensic Analysis can achieve conclusion that are accurate and compelling. It should be noted there are other logic models and other categories of investigatory techniques that can also be applied. The interested reader should pursue further information about techniques that can be applied to computer forensics from books or articles related to law enforcement investigatory techniques.

Appendix A: Hume's Argument

Hume wrote:

> Reason is the discovery of truth or falsehood. Truth or falsehood consists in an agreement or disagreement either to the real relations of ideas, or to real existence and matter of fact. Whatever, therefore, is not susceptible of this agreement or disagreement, is incapable of being true or false, and can never be an object of our reason. Now our passions, volitions, and actions, are not susceptible of any such agreement or disagreement; being original facts and realities, complete in them selves, and implying no reference to other passions, volitions, and actions. [It is] impossible, therefore, they can be pronounced either true or false, and be either contrary or conformable to reason (Hume, D. 1740).

Per Hume, morality (i.e., manifested by human actions, excited passions, volitions) cannot be the consequence of moral reasoning because reason is inert to human actions. He goes on to say, referring to the passage above:

> This argument is of double advantage to our present purpose. For it proves directly, that actions do not derive their merit from a conformity to reason, nor their blame from a contrariety to it; and it proves the same truth more indirectly, by showing us, that as reason can never immediately prevent or produce any action by contradicting or approving of it, it cannot be the source of moral good and evil, which are found to have that influence. Actions may be laudable or blamable; but they cannot be reasonable: Laudable or blamable, therefore, are not the same with reasonable or unreasonable. The merit and demerit of actions frequently contradict, and sometimes control our natural propensities. But reason has no such influence. Moral distinctions, therefore, are not the offspring of reason. Reason is wholly inactive, and can never be the source of so active a principle as conscience, or a sense of morals. (Hume, D. 1740)

Appendix B – Deductive Logic Tables

Name	Sequent	Description
Modus Ponens	$[(p \rightarrow q) \square p] \vdash q$	if p then q; p; therefore q
Modus Tollens	$[(p \rightarrow q) \square \neg q] \vdash \neg p$	if p then q; not q; therefore not p
Hypothetical Syllogism	$[(p \rightarrow q) \square (q \rightarrow r)] \vdash (p \rightarrow r)$	if p then q; if q then r; therefore, if p then r
Disjunctive Syllogism	$[(p \square q) \square \neg p] \vdash q$	Either p or q; not p; therefore, q
Constructive Dilemma	$[(p \rightarrow q) \square (r \rightarrow s) \square (p \square r)] \vdash (q \square s)$	If p then q; and if r then s; but either p or r; therefore either q or s
Destructive Dilemma	$[(p \rightarrow q) \square (r \rightarrow s) \square (\neg q \square \neg s)] \vdash (\neg p \square \neg r)$	If p then q; and if r then s; but either not q or not s; therefore rather not p or not r
Simplification	$(p \square q) \vdash p,q$	p and q are true; therefore p is true
Conjunction	$p, q \vdash (p \square q)$	p and q are true separately; therefore they are true conjointly
Addition	$p \vdash (p \square q)$	p is true; therefore the disjunction (p or q) is true
Composition	$[(p \rightarrow q) \square (p \rightarrow r)] \vdash$	If p then q; and if p then r; therefore if p is true then q and r are true

	$[p \rightarrow (q \square r)]$	
De Morgan's Theorem (1)	$\neg (p \square q) \vdash (\neg p \square \neg q)$	The negation of (p and q) is equiv. to (not p or not q)
De Morgan's Theorem (2)	$\neg (p \square q) \vdash (\neg p \square \neg q)$	The negation of (p or q) is equiv. to (not p and not q)
Commutation (1)	$(p \square q) \vdash (q \square p)$	(p or q) is equiv. to (q or p)
Commutation (2)	$(p \square q) \vdash (q \square p)$	(p and q) is equiv. to (q and p)
Association (1)	$[p \square (q \square r)] \vdash [(p \square q) \square r]$	p or (q or r) is equiv. to (p or q) or r
Association (2)	$[p \square (q \square r)] \vdash [(p \square q) \square r]$	p and (q and r) is equiv. to (p and q) and r
Distribution (1)	$[p \square (q \square r)] \vdash [(p \square q) \square (p \square r)]$	p and (q or r) is equiv. to (p and q) or (p and r)
Distribution (2)	$[p \square (q \square r)] \vdash [(p \square q) \square (p \square r)]$	p or (q and r) is equiv. to (p or q) and (p or r)
Double Negation	$p \vdash \neg\neg p$	p is equivalent to the negation of not p
Transposition	$(p \rightarrow q) \vdash (\neg q \rightarrow \neg p)$	If p then q is equiv. to if not q then not p
Material Implication	$(p \rightarrow q) \vdash (\neg p \square q)$	If p then q is equiv. to either not p or q

Material Equivalence (1)	$(p \leftrightarrow q) \vdash [(p \rightarrow q) \square (q \rightarrow p)]$	(p is equiv. to q) means, (if p is true then q is true) and (if q is true then p is true)
Material Equivalence (2)	$(p \leftrightarrow q) \vdash [(p \square q) \square (\neg q \square \neg p)]$	(p is equiv. to q) means, either (p and q are true) or (both p and q are false)
Exportation	$[(p \square q) \rightarrow r] \vdash [p \rightarrow (q \rightarrow r)]$	from (if p and q are true then r is true) we can prove (if q is true then r is true, if p is true)
Importation	$[p \rightarrow (q \rightarrow r)] \vdash [(p \square q) \rightarrow r]$	
Tautology	$p \vdash (p \square p)$	p is true is equiv. to p is true or p is true

References (a.k.a. Arguments from Authority)

1. Benny, Daniel J (2006). "The Uses of Inductive and Deductive Reasoning in Investigations and Criminal Profiling"
2. Encyclopedia Britannica. "Mercury." 2006. Encyclopedia Britannica Premium Service <http://www.britannica.com/eb/article-241978>.
3. Doyle, C. (1882). A Study in Scarlet, London, UK: Doubleday
4. Gocsik, K. (2004). "Logic and Argument", Dartmouth College,
5. Hoeller, S (1989). Jung and the Lost Gospels.
6. Hume, D. (1740). A Treatise of Human Nature: Being an Attempt to Introduce the Experimental Method of Reasoning into Moral Subjects.
7. Kant, I. (1781). The Critique of Pure Reason.
8. Ramsland, K. Ph.D. (2000), "The Forensic Mind – From Evidence to Theory"
9. Thompson, S. K (1992). Sampling, New York, Wiley.
10. Turvey, B. (2001). Criminal Profiling, San Diego, CA: Elsevier Academic Press
11. Wikipedia Online Encyclopedia "Logic Tables" (2006) - en.wikipedia.org/wiki/Deductive.
12. Wikipedia Online Encyclopedia "Inductive Reasoning Types" (2006) - en.wikipedia.org/wiki/Inductive

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Columbia FOR508	Columbia, MD	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Data Breach Summit & Training	Chicago, IL	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS vLive - FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting	FOR508 - 201710,	Oct 16, 2017 - Nov 22, 2017	vLive
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
Mentor Session - FOR508	Brasilia, Brazil	Oct 18, 2017 - Oct 21, 2017	Mentor
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Milan November 2017	Milan, Italy	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MD	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS New York City Winter 2018	New York, NY	Feb 26, 2018 - Mar 03, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CA	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced