Global Information Assurance Certification Paper

Zork as a Computer Investigative Mind Set

GIAC (GCIA) Gold Certification

Author: Timothy Cook, tcbcook@yahoo.com
Advisor: Manuel Humberto Santander Peláez
Accepted: December 19, 2015

Abstract

Zork is a very popular text adventure game of the 70's and 80's, which challenged players to explore their surroundings and solve puzzles/problems to advance and complete the game. Unlike today's graphics intensive games, in text adventure games everything you need to know is not thrown onto the screen in high-resolution detail, rather the player has to choose from the provided commands to explore the in-game environment and solve the puzzles encountered. This need to explore the environment and examine situations and associated items for clues to solve-problems encourages players to develop problem solving skills that translate well to computer investigations. This paper draws similarities between text adventure games and computer investigations and discusses some of the basic principles and approaches needed for both.

1. Zork?

While not the first text adventure (alternatively known as "interactive fiction genre") game, *Zork* is possibly the most well-known one. It was created in the late 1970's on a PDP-10 mainframe computer by Massachusetts Institute of Technology (MIT) students Tim Anderson, Marc Blanc, Bruce Daniels and Dave Lebling. "Just as home computers were becoming more commonplace, a commercial version of *Zork* was released by Infocom, a company founded by Anderson, Lebling and Blank. However, they didn't initially intend to sell *Zork*. They set out to create serious productivity software for the home and business market, but when they realized they didn't actually have any of those programs written yet, they decided *Zork* sales could fund their future endeavors. Since the game was too big to operate on these early home computers, they had to break it into three parts: *Zork I: The Great Underground Empire* (1980), *Zork II: The Wizard of Frobozz* (1981), and *Zork III: The Dungeon Master* (1982). Although *Zork* was first released for the TRS-80 computer, it was eventually ported to just about every home computer, like Apple II, Atari Computers, and the IBM PC. It was a pretty big hit, selling over a million copies" ("Eaten by a Grue: A Brief History of Zork | Mental Floss," n.d.).

Text adventure games differ from most modern games in the absolute lack of video game graphics. Instead of being presented with a graphical representation of the environment and the events occurring, the player has to use the simple commands that the game provides to explore the environment and artifacts of the game and to solve the puzzles encountered. Often the small details of an artifact in the game or the order in which a user has to complete certain actions are critical to the successful completion of the game. A player's success, or lack thereof, was determined by his or her skill at leveraging the commands to explore the environment, documenting encountered geography and artifacts, and developing a plan to overcome obstacles, such as resolving anomalies or solving puzzles. Because of this, text adventure games help players develop problem-solving skills that translate well to computer investigations ranging from simple troubleshooting to post exploitation.

Timothy Cook, tcbcook@yahoo.com

Many of the complex solutions available to the computer investigator today are comparable to modern graphics intensive games in that they do not require the investigator to see the raw data or allow them to know how the data is processed. They are similar to a "magic box", in which the analyst provides it with all of the available information, "turns a handle" and an answer pops out. The investigator just needs to "point and shoot." While this is a fast and convenient method to produce answers and to potentially solve problems it does not provide the investigator with any understanding of the data or the processes involved. Because of this, the investigator may not be able to identify false positives or be alert for false negatives. Additionally, the creators of these solutions cannot take every possible variation in a computer environment into account when they develop their product. As a result, nuances in the investigator's network, such as proprietary hardware or software, may not be accurately reflected and can lead to inaccurate or misleading results.

Similar to text adventure games, command line tools allow, or one might argue "require", the investigator to interact with and review the data and control the processing of it. This interaction with the raw data gives the investigator a greater understanding of its significance. By doing so the investigator can come to recognize what data is normal for their architecture and what data is not.

While there are excellent training courses available to computer analysts, most of them concentrate on specific applications of specific tools, which enables the analyst to complete some of the tasks involved in an investigation, but fails to prepare them to conduct an investigation on their own. While an analyst's ability to complete individual tasks or run specific commands is important the ability to conduct a computer investigation will enable them to not only validate alerts that are received but also to look for indicators that did not generate an alert. Whether the first indication of an issue comes from an Intrusion Detection System (IDS) or a help desk ticket, the responding analyst's computer investigation skills can be the key factor in a company's incident response.

The intent of this paper is not to provide a computer investigative model or teach currently accepted digital forensic techniques, procedures or tools, but rather to discuss a mindset that is fundamental to computer investigations of all kinds as "[t]he fundamental

tenets of an investigation remain consistent regardless of the domain being examined" (Hagen, 2014).

2. Identify and Master Available Commands

The authors of *Zork* "got the idea for *Zork* from the first text-based computer game, Adventure (also called Colossal Cave Adventure or ADVENT, because the computer it ran on could only use so many letters in the command line). Adventure was created in 1976 by Will Crowther, a student at Stanford, as a simulation of Mammoth Cave in Kentucky, with a few Tolkien-esque fantasy elements thrown in by fellow Stanfordite Don Woods. The MIT guys weren't impressed with Adventure's limited two-word command structure ("kill troll"), so they wrote *Zork* to understand complete sentences ("kill troll with sword")" ("Eaten by a Grue: A Brief History of Zork | Mental Floss," n.d.). Even though the authors of *Zork* increased the commands available to the player they are limited and if the player is not familiar with all of these commands and understands what they are capable of, or what actions they accomplish, they will not be able to complete the game (a list of *Zork* commands and their associated actions can be found at http://zork.wikia.com/wiki/Command_List).

While there are significantly more commands, and more powerful commands, available in the typical computer environment the same principle applies. Indeed, the sheer number and complexity of commands (or tools) available make it more imperative that the computer investigator knows what tools will assist them in acquiring information pertinent to the investigation and how to best use the tools to do so. "As the field of network forensics continues to thrive and mature, the number and scope of available tools that address this unique domain must scale to meet the demand. To be certain, the only way investigators will be able to provide high-quality results will be to learn these tools and understand their particular strengths and weaknesses. This knowledge will emerge from direct experience with each tool, but also from vendors' tool-oriented training, as they seek to maximize the value to their customers" (Hagen, 2014).

One of the most important preparatory steps an investigator can complete is to assemble their toolkit. A toolkit is a collection of tools that the investigator has selected

for specific data collection, manipulation or presentation tasks. These should be tools that the investigator knows and trusts and has experience using in the context of an investigation. While an investigator may know how to use an administrative tool to perform administrative functions on a computer or network, they also need to know how the tool will benefit them in an investigation.

Investigators should be aware that they are not restricted to the tools that are available on the device under investigation and, in cases of potential system compromise, should not fully trust software resident on the device. Options include accessing a storage device with a trusted toolset, conducting the examination from another device that has network access to the suspect device or removing the digital media storage components from the device and reviewing them forensically, either through a review of the physical component or an analysis of a forensically sound image of the component (see section 2.3).

An important consideration when selecting tools is that they provide the information that the investigator is looking for in a manner that is understandable and useful. In other words, the tools need to allow the investigator to eliminate the clutter and isolate the pertinent or interesting data. Sometimes it may be necessary to filter the output of one tool or command through another, perhaps with a pipe command or by exporting data in a commonly readable file format, to accomplish this. A solid working knowledge of the options or switches available with a tool, their resulting effect on the tool's output and the significance of the output will prove invaluable to the investigator.

Regardless of the tools chosen, the investigator needs to acquire, test and master them prior to an investigation. An old artists' aphorism states essentially that the finest tools in the hands of an amateur will at best produce a passable product while the crudest tools in the hands of a craftsman will produce a masterpiece. Investigators should not wait until a tool is needed to acquire or master it. Tool requirements should be predetermined and validated and the tools acquired before they are needed. Additionally, the investigator should be proficient with them before they are to be used in an investigation.

The investigator can acquire this proficiency through experience or a combination of training and experience. Once the investigator has completed training they need to utilize their new skills soon and often in order to complete the learning process. The phrase "use it or lose it" certainly applies in this case.

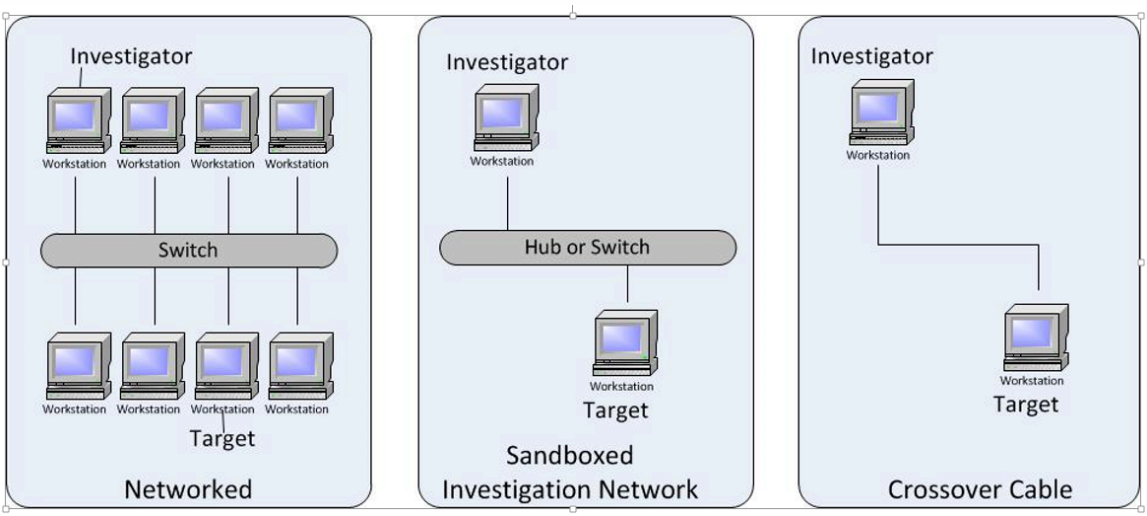
2.1. Local Device OS

Most operating systems include commands and tools that are intended to perform administrative tasks and troubleshoot issues. Additionally, many operating systems have software bundles available from the vendors that provide additional administrative tools or have specially developed distributions designed to provide tools not found in the standard release, such as Linux distros. These same commands can be useful in an investigation as well because they can enable an investigator to determine if hardware or software configurations have changed and to review systems and application logs.

There is sound argument not to trust software that resides on a potentially compromised system. In such cases it is commonly advised that the investigator utilize a portable external device, perhaps a DVD or other read-only medium that contains their toolkit. These should not rely on any software, libraries or processes on the potentially compromised system to function. Additionally, it is important that the investigator validates their tools on each new operating system version and potentially after each patching cycle.

2.2. Remote Connected Investigation

If the investigator desires to use tools that are not available or supported on the target device, or does not trust the software on a potentially compromised device there is the potential to connect to the device remotely. This can be accomplished either by utilizing the standard network, by switching the device to a sandboxed investigation network or via crossover cable.



One advantage of the remote connection approach is that it allows for the examination of the device without shutting it down or rebooting it. This allows the investigator to review the processes and services that are running and potentially the contents of memory.

Another advantage to the remote connection is that it can allow the investigator to review devices with different operating systems without requiring them to master the specific tools available on each operating system. It also allows the investigator to select what they consider to be the best tool for the task at hand regardless of the target devices operating system.

Finally, network connected investigations allow the investigator to collect and correlate information from multiple devices, as evidence of a compromise may reside in more than one location on the network and data in one location may conflict with data in another, indicating to the investigator that data tampering has potentially occurred.

2.3. Sandboxed Forensic Examination

An option available to the investigator not concerned with reviewing running processes, services or memory, or who specifically does not want the device to be able to run processes and services, is to remove the digital storage device and perform a sandboxed, or network isolated, forensic examination of it. This review can either be done on the digital storage device itself utilizing a write-blocker to prevent changes to the media or on a forensic image created from the device. A forensic image can be defined as

"a forensically sound and complete copy of a hard drive or other digital media, generally intended for use as evidence. Copies include unallocated space, slack space, and boot record. A forensic image is often accompanied by a calculated Hash signature to validate that the image is an exact duplicate of the original" ("Forensic Image," 2015).

In its most basic form a sandbox (see illustration above) is an isolated environment that prevents software or processes on one system from affecting another. It is often used to prevent viruses under review from spreading but can also be useful when it is desirable to prevent communications between systems, such as downloaders and Command and Control communications. Because a typical sandboxed forensic examination entails reviewing one system from another, it allows the investigator to take advantage of their chosen collection of tools that they are proficient in to conduct an investigation, to use protected media to store the data retrieved and to control potential interaction with the data from actors other than the investigator.

A key advantage of forensic examinations is that when properly conducted they preserve the media, meaning that they prevent changes to the digital media due to the investigation. An example of this would be that when reviewing a file on most operating systems, the file's "Last Access" timestamp is updated. This timestamp update could destroy or obscure key evidence and prevent an investigator from successfully constructing a timeline (see section 4.6) of events.

There are various solutions available for Forensic reviews that include command line tools, including proprietary and Open Source tools and even purpose-built Linux distros that are run in either a virtual environment or installed on a forensic examination workstation. Two examples are The Sleuth Kit (http://www.sleuthkit.org/) which is available in both 32-bit and 64-bit Windows as well as Linux and OS X and the SANs Investigative Forensic Toolkit (SIFT) which is a VMware appliance built on an Ubuntu Operating System (https://digital-forensics.sans.org/community/downloads).

2.4. Multiple tools

There are two key aspects to utilizing multiple tools that perform the same function during an investigation. The first is that one tool might extract data differently than other tools, or produce the data in a different format. This might make one tool

preferable over another at a certain point in an investigation if, perhaps, it is necessary to refine the data, isolate components of its output or to have it read by another tool. As an example, the investigator might prefer to use one tool because it has an option to produce output in a format that can easily be parsed or sorted by another tool. Alternately the investigator may use a different tool to obtain the same data because it can output the data in a format that lends itself more easily to inclusion in a written report.

The second is that utilizing two or more different tools to investigate the same item can provide validation of the data returned by each or perhaps even give the investigator reason to question the output of a specific tool. If the investigator uses two different tools to extract log entries and the output of one tool includes logs entries that the other doesn't, then there is an indication that either there is an issue with the log source or possibly that the investigator may not be using one of the tools correctly. This might cause the investigator to examine the source more carefully to determine whether it can be trusted or to review the tool to determine whether it was utilized correctly. Alternately, if the output of a tool is not what the investigator expected or feels is reasonable then the investigator may use a different tool to verify the output. If both tools return the same data, then there is confirmation that the each tool is accurately extracting the data requested and the investigator needs to find an alternate explanation for the data.

3. Learn Your Environment

Zork starts out very simply, with the player in an open field west of a house, but as the player progresses further into the realm of *Zork* they find themselves in a complex underground labyrinth filled with unusual things. The player's ability to explore the world that the game presents to them and to keep track of what artifacts or items are available, where they are and how they can get to them, is a key to successful completion (players often create maps on graph paper to document the environment). Sometimes the environment or items might not seem right to the player, but are normal for the realm of *Zork*.

In a similar manner, a computer investigator needs to learn the environment in which their investigation will occur in order to know where to look for data and to

recognize significant data when they see it. The physical environment that the investigator is confronted with may range from a single device to a home or small office network or even an international mega-corporation with a Wide Area Network (WAN) that spans multiple continents. In addition to end-user workstations, the environment can include network hardware, such as routers, switches or proxies and peripherals such as Network Storage devices, printers, and plotters. However the environment is more than the hardware, it also includes the Operating System (OS) that runs on the hardware, the installed applications, both those that are incorporated into the environment by design and those that are present for other reasons such as default OS loads, and their respective log files. This concept is important to understand because information pertinent to the investigation might be available in multiple places; "there are potentially dozens of devices that process or observe every single packet during its short lifetime. Each of these devices has its own logging capabilities, formats, retention periods, and level of insight to each networked conversation. This broadens the landscape upon which useful evidence can reside, but diversifies the corresponding means of collection, storage, formatting, and analyzing that evidence" (Hagen, 2014).

But it isn't sufficient to just know the network architecture and have a knowledge of what applications reside where and how to access the logs. The investigator should understand how the components of the system interact and communicate with each other when they are operating as designed and expected. What is a normal system load, what constitutes a normal connection or communication, what processes should be running and what ports should be open and listening? Investigations will be significantly easier and quicker if the investigator knows what the environment looks like before they have to investigate it. Not just what traffic or processes should exist, but what normally exists. It is important for the investigator to understand what constitutes the "expected" so that the "unexpected" is identified when it is encountered because "much of analysis involves finding something that is not normal or expected" (Novak, 2015, p.34). This information can be used by the investigator to build a baseline for the systems that will assist in identifying later anomalies.

Ideally, the environment is well documented, the documentation is current, available to the computer investigator and is detailed and exact. Realistically, if

documentation exists it likely only lists the physical hardware with no indication of the applications running, the normal processes or the expected traffic (protocols, ports, etc.). Whenever possible the investigator should become familiar with the environment before they have to conduct an investigation, as even the most detailed map in the hands of a stranger cannot match the knowledge of someone who lives the environment on a daily basis. Similar to playing text adventure games such as *Zork*, keeping notes and diagrams can make the difference between success and failure.

Finally, bear in mind that environments are not static – they change, and if the investigator doesn't stay up to date they will have to discover their environment all over again each time they run an investigation.

4. Collect Artifacts and Solve Puzzles

The first information provided to a *Zork* player is that they are "West of House: This is an open field west of a white house, with a boarded front door. There is a small mailbox here. A rubber mat saying 'Welcome to Zork!' lies by the door" ("Parchment," n.d.). The player's first puzzle is to figure out how to enter the house (it is not as easy as "open door") and then how to reach the labyrinth under the house and eventually complete the game.

In a similar manner, the first information that an investigator receives is likely to be sparse and not indicative of the task ahead of them. The information may be that a process is no longer working as expected, that something new or unusual has been observed or even that their network is attacking another. The information "may be as vague as the network experienced poor performance between certain time periods, or it may be detailed, like a snort alert, and may provide the date and time, the IP addresses, port numbers, and malicious content discovered" (Novak, 2015, p.94).

It will be up to the investigator to determine if the information they receive is significant, whether it is a false positive and if not then whether the information is indicative of the actual problem or a symptom of the problem. If the information is determined to be indicative of a symptom, then it will be up to the investigator to look for further indicators in order to define the actual problem as "the key to a good problem

definition is ensuring that you deal with the real problem – not its symptoms" ("What is Problem Solving? - Problem Solving Skills from MindTools.com," n.d).

The problem encountered may range from a simple investigation including only a single hard drive or other stored data device to a network intrusion investigation that can be more like a horrible math word problem, where the investigator is presented with an end result and has to work backwards determining the actual problem and its associated variables as they go.

As the investigation proceeds, information may be determined to be insignificant at first but in light of data uncovered later may be re-categorized as significant. An example of this might be that a workstation log is determined not to be significant due to a lack of pertinent data but when corroborated against a central log server it may be determined that the lack of log entries on the workstation, or the discrepancy between the logs on the workstation and the log server, is significant in and of itself. It will serve the investigator well to keep track of various puzzle pieces as they discover them so that they can be revisited or re-examined if necessary.

Regardless of a person's chosen profession, at some point they will have to participate in problem-solving at work. Problem-solving "is a mental process that involves discovering, analyzing, and solving problems….the best strategy for solving a problem depends largely on the unique situation" ("Problem Solving," n.d.). Below are some points that the investigator should consider regardless of the Problem-solving methodology or philosophy that they follow.

4.1. S-T-O-P

A useful first step is to follow a mnemonic taught by the Boy Scouts of America: S-T-O-P. It stands for "Stop/Stay Calm, Think, Observe, Plan" ("Lost in the woods! Now what? | Boys' Life magazine," n.d.). While the Boy Scouts teach it for use in wilderness survival, it is sound advice and policy in most any other situation as well. Before an investigator jumps into an investigation and begins mining data in search of answers they should take a step back (Stop), relax (Stay Calm) and Think about the information they have. An investigation can be a hectic time in which the investigator is under a lot of scrutiny and pressure. They should relax, calm down and then proceed to validate the

information and determine its significance. Then they should Observe what other, possibly corroborating, indicators are available and develop a Plan. In text adventure games it is sometimes necessary to plot different approaches or plans and try each one until something works. Periodically during the investigation the investigator should take a moment to S-T-O-P again and reevaluate their plan, as results of the investigation may give cause to modify it

4.2. Procedures are your friend

Procedures are "a series of actions that are done in a certain way or order: an established or accepted way of doing something" ("Procedure | Definition of procedure by Merriam-Webster," n.d.). They are typically derived from past experiences and can range from a general outline to a formalized list of steps that are required for every investigation. Procedures can be very useful in investigations because they can serve as a reminder or check-off list, preventing the investigator from forgetting tasks in the excitement of the moment. They also ensure that investigations are conducted in an approved manner and when followed should protect the investigator from recriminations. Procedures should at the least be revisited periodically and validated, but they are of the most use when updated as seen fit based on recent investigations.

4.3. Keep a log

A log, whether it be written by hand or created in a computer program, serves three very important benefits for the investigator. The first is that it enables the investigator to keep track of what commands they have issued and what the results were. By keeping this data in a log the investigator can keep track of pieces of the puzzle (data) that may be of use later or that might have been forgotten if not recorded. Additionally, by reviewing the log, the investigator may gain insight that will serve to move the investigation forward.

The second is that it documents the investigators actions and their effect or lack of effect on the systems and data. It allows the investigator to keep track of their steps and to document the changes due to their actions or prove that their actions wouldn't have affected the systems or data. It can also be used to record the investigators assumptions and their reason for collecting specific data. This record can be important if the process

used by the investigator, or the data collected, is ever challenged, perhaps in a court of law.

The third is that logs can help an investigator in subsequent investigations, both as a reminder of how they successfully solved a similar problem and as a reminder of approaches or solutions that did not work. In either case, it allows the investigator to be more efficient and productive in subsequent investigations.

4.4. What is really happening?

As discussed in section 4.1, a good starting point is to Stop, Think, Observe, and Plan. The investigator should attempt to determine what is actually happening rather than what is being reported as happening. As previously stated, the information reported may only be a symptom or side effect of the real issue. By taking a step back and observing more, the investigator can get a feel for the "big picture" and potentially prevent the chasing down and solving of a symptom while obscuring the real problem.

4.5. What has changed?

When something that once worked no longer does, one of the most useful things an investigator can do is to determine "what has changed?" Many computer environments involve customizations that take significant time and resource to get working initially. Once the proper configuration has been determined, and the system works as it was intended to, it can speed an investigation to ask the simple question "what has changed?" What is no longer as it was? This determination may be made from timestamps, or from a comparison to either an identical system or documentation of the correct configuration of the system.

4.6. Timeline

A Timeline is "a linear representation of important events in the order in which they occurred" ("Timeline | Define Timeline at Dictionary.com," n.d.). In its most basic form, a timeline of an investigation consists of what the investigator knows happened ordered chronologically. It can be an invaluable tool during an investigation because it can help the investigator put together the story of what happened, keep puzzle pieces in perspective and point to places where the investigator may find further evidence. It can

also highlight events that don't seem to fit the investigation, and therefore may be guiding the investigation in the wrong direction. In its basest form, a timeline is a record of WHAT happened and WHEN it happened though other data that the investigator feels is pertinent to the entry can be included as well.

There are multiple automated and graphical timeline tools available but, in keeping with the sub-theme of this paper, they are just a tool and intelligent human control is vital to their successful incorporation into an investigation.

4.7. After Action Review

An After Action Review (AAR), sometimes called a Lessons Learned meeting, is a post-investigation meeting to review the success and failures of the investigation with a goal of improving the process in the future. It should never be a blame session, but rather an honest, no-fault, review of what worked, what didn't work and post-investigation insights. It can be useful in providing updates to existing procedures as well as driving out a need for new procedures. It can also provide fact-based business cases for changes to a computer environment (sensors/logs/alerts) or for filling gaps in software or training.

An AAR should be documented so that the insights or lessons learned or insights are not lost. The report should be positive in nature and it should be written in such a manner that recommendations are clearly viewed as improvements rather than as criticism of the current procedures or people.

5. Conclusion

A text adventure, or a "Zorkmethod" (K. Kincaid, personal communication, October 20, 2015), approach to computer investigations requires the investigator to have more than a casual knowledge of the computer environment, fundamentals, and processes but allows for an intelligent, investigator-centric investigation. By utilizing command line tools, the investigator has the ability to interact with the data and to interactively guide the investigation. This ability allows the investigator to provide intelligent direction to an investigation based on their knowledge of the computer environment and their experience and familiarity with it. This understanding of the fundamentals and familiarity with the

computer environment can prevent the wasting of resources on chasing false positives as well as the discovery of information that can be used to reduce false negatives.

Investigators need to select the tools that they are most comfortable with and acquire training and experience with them as well as an understanding of the significance of their output so that they will be able to use them to best effect during an investigation. Finally, while not engaged in an active investigation, investigators can keep their skills sharp with the training link below:

http://textadventures.co.uk/games/play/5zyoqrsugeopel3ffhz_vq

References

Command List - Zork Wiki - Wikia. (n.d.). Retrieved October 22, 2015, from http://zork.wikia.com/wiki/Command_List

Eaten by a Grue: A Brief History of Zork | Mental Floss. (n.d.). Retrieved from http://mentalfloss.com/article/29885/eaten-grue-brief-history-zork

Forensic Image. (2015). Retrieved from http://www.protegga.com/glossary/forensic-image-definition/

Hagen, P. (2014, January 14). Advanced Network Forensics: Analysis in an Interconnected Landscape. Retrieved from http://www.forensicmag.com/articles/2014/01/advanced-network-forensics-analysis-interconnected-landscape

Lost in the woods! Now what? | Boys' Life magazine. (n.d.). Retrieved from http://boyslife.org/outdoors/1200/trail-tips-lost-in-the-woods/

Novak, J. (2015). *Security 503.1: Fundamentals of traffic analysis part 1* (2015 ed.). SANs Institute.

Novak, J. (2015). *Security 503.5: Network Traffic Forensics and Monitoring* (2015 ed.). SANs Institute.

Parchment. (n.d.). Retrieved from http://textadventures.co.uk/games/play/5zyoqrsugeopel3ffhz_vq

Problem Solving. (n.d.). Retrieved from http://psychology.about.com/od/problemsolving/f/problem-solving-steps.htm

Timothy Cook, tcbcook@yahoo.com

Procedure | Definition of procedure by Merriam-Webster. (n.d.). Retrieved from http://www.merriam-webster.com/dictionary/procedure

SANS Course Types in Information Security and Cyber Security Training. (n.d.). Retrieved from https://www.sans.org/curricula/

Timeline | Define Timeline at Dictionary.com. (n.d.). Retrieved from http://dictionary.reference.com/browse/timeline

What is Problem Solving? - Problem Solving Skills from MindTools.com. (n.d.). Retrieved from https://www.mindtools.com/pages/article/newTMC_00.htm

Timothy Cook, tcbcook@yahoo.com

Last Updated: January 21st, 2019

Upcoming Training

SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC503: Intrusion Detection In-Depth	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
SANS Northern VA Spring- Tysons 2019	Tysons, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS London February 2019	London, United Kingdom	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201902,	Feb 27, 2019 - Apr 04, 2019	vLive
SANS San Francisco Spring 2019	San Francisco, CA	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Madrid March 2019	Madrid, Spain	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS 2019	Orlando, FL	Apr 01, 2019 - Apr 08, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KY	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, Kingdom Of Saudi Arabia	Apr 13, 2019 - Apr 18, 2019	Live Event
Community SANS New York SEC503	New York, NY	Apr 29, 2019 - May 04, 2019	Community SANS
SANS Security West 2019	San Diego, CA	May 09, 2019 - May 16, 2019	Live Event
SANS Northern VA Spring- Reston 2019	Reston, VA	May 19, 2019 - May 24, 2019	Live Event
SANS Amsterdam May 2019	Amsterdam, Netherlands	May 20, 2019 - May 25, 2019	Live Event
SANS San Antonio 2019	San Antonio, TX	May 28, 2019 - Jun 02, 2019	Live Event
San Antonio 2019 - SEC503: Intrusion Detection In-Depth	San Antonio, TX	May 28, 2019 - Jun 02, 2019	vLive
SANS London June 2019	London, United Kingdom	Jun 03, 2019 - Jun 08, 2019	Live Event
SANSFIRE 2019	Washington, DC	Jun 15, 2019 - Jun 22, 2019	Live Event
Security Operations Summit & Training 2019	New Orleans, LA	Jun 24, 2019 - Jul 01, 2019	Live Event
SANS Paris July 2019	Paris, France	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS Rocky Mountain 2019	Denver, CO	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS Columbia 2019	Columbia, MD	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS Boston Summer 2019	Boston, MA	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS Chicago 2019	Chicago, IL	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS Copenhagen August 2019	Copenhagen, Denmark	Aug 26, 2019 - Aug 31, 2019	Live Event
SANS Network Security 2019	Las Vegas, NV	Sep 09, 2019 - Sep 16, 2019	Live Event
SANS Oslo September 2019	Oslo, Norway	Sep 09, 2019 - Sep 14, 2019	Live Event
SANS London September 2019	London, United Kingdom	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS OnDemand	Online	Anytime	Self Paced