DOWNLOAD PDF COLLECTING IN CYBERSPACE

Chapter 1 : Insect Field Trips

Collecting in Cyberspace By ARTnews Posted 01/01/00 am The online art market is growing as auction houses and dealers rush to establish a presence on the Web.

Under this name the two made a series of installations and images entitled "sensory spaces" that were based on the principle of open systems adaptable to various influences, such as human movement and the behaviour of new materials. In a interview with Scandinavian art magazine Kunstkritikk, Carsten Hoff recollects, that although Atelier Cyberspace did try to implement computers, they had no interest in the virtual space as such: There was nothing esoteric about it. It was just a tool. The space was concrete, physical. And in the same interview Hoff continues: Our shared point of departure was that we were working with physical settings, and we were both frustrated and displeased with the architecture from the period, particularly when it came to spaces for living. We felt that there was a need to loosen up the rigid confines of urban planning, giving back the gift of creativity to individual human beings and allowing them to shape and design their houses or dwellings themselves â€” instead of having some clever architect pop up, telling you how you should live. We were thinking in terms of open-ended systems where things could grow and evolve as required. For instance, we imagined a kind of mobile production unit, but unfortunately the drawings have been lost. It was a kind of truck with a nozzle at the back. Like a bee building its hive. The nozzle would emit and apply material that grew to form amorphous mushrooms or whatever you might imagine. It was supposed to be computer-controlled, allowing you to create interesting shapes and sequences of spaces. It was a merging of organic and technological systems, a new way of structuring the world. And a response that counteracted industrial uniformity. We had this idea that sophisticated software might enable us to mimic the way in which nature creates products â€” where things that belong to the same family can take different forms. All oak trees are oak trees, but no two oak trees are exactly alike. And then a whole new material â€” polystyrene foam â€” arrived on the scene. It behaved like nature in the sense that it grew when its two component parts were mixed. Almost like a fungal growth. This made it an obvious choice for our work in Atelier Cyberspace. The portion of Neuromancer cited in this respect is usually the following: A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts A graphic representation of data abstracted from the banks of every computer in the human system. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding. Now widely used, the term has since been criticized by Gibson, who commented on the origin of the term in the documentary No Maps for These Territories: All I knew about the word "cyberspace" when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page. Metaphorical[edit] Don Slater uses a metaphor to define cyberspace, describing the "sense of a social setting that exists purely within a space of representation and communication Author Bruce Sterling , who popularized this meaning, [13] credits John Perry Barlow as the first to use it to refer to "the present-day nexus of computer and telecommunications networks". Barlow describes it thus in his essay to announce the formation of the Electronic Frontier Foundation note the spatial metaphor in June To enter it, one forsakes both body and place and becomes a thing of words alone. You can see what your neighbors are saying or recently said , but not what either they or their physical surroundings look like. Town meetings are continuous and discussions rage on everything from sexual kinks to depreciation schedules. Whether by one telephonic tendril or millions, they are all connected to one another. Collectively, they form what their inhabitants call the Net. It extends across that immense region of electron states, microwaves, magnetic fields, light pulses and thought which sci-fi writer William Gibson named Cyberspace. Virtual environments[edit] Although the present-day, loose use of the term "cyberspace" no longer implies or suggests immersion in a virtual reality, current technology allows the integration of a number of capabilities sensors, signals, connections, transmissions, processors, and controllers sufficient to generate a virtual interactive experience that is accessible regardless of a geographic location. It is for these reasons cyberspace has been described as the ultimate tax haven. Kramer there are 28 different definitions of the term cyberspace. See in particular the following links: The most recent draft definition is the following: Cyberspace is a global and dynamic domain subject to constant change characterized by the combined use of electrons and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate information and disrupt physical resources. Often, in common parlance and sometimes in commercial language , networks of networks are called Internet with a lowercase i , while networks between computers are called intranet. Internet with a capital I, in journalistic language sometimes called the Net can be considered a part of the system a. A distinctive and constitutive feature of cyberspace is that no central entity exercises control over all the networks that make up this new domain. To cyberspace, a domain without a hierarchical ordering principle, we can therefore extend the definition of international politics coined by Kenneth Waltz: On the contrary, cyberspace is characterized by a precise structuring of hierarchies of power. Internet metaphors While cyberspace should not be confused with the Internet, the term is often used to refer to objects and identities that exist largely within the communication network itself, so that a website , for example, might be metaphorically said to "exist in cyberspace". The philosopher Michel Foucault used the term heterotopias , to describe such spaces which are simultaneously physical and mental. Firstly, cyberspace describes the flow of digital data through the network of interconnected computers: There have been several attempts to create a concise model about how cyberspace works since it is not a physical thing that can be looked at. Cyberspace draws attention to remediation of culture through new media technologies: Finally, cyberspace can be seen as providing new opportunities to reshape society and culture through "hidden" identities, or it can be seen as borderless communication and culture. Not inside your actual phone, the plastic device on your desk. The place between the phones. Light has flooded upon it, the eerie light of the glowing computer screen. This dark electric netherworld has become a vast flowering electronic landscape. Since the s, the world of the telephone has cross-bred itself with computers and television, and though there is still no substance to cyberspace, nothing you can handle, it has a strange kind of physicality now. It makes good sense today to talk of cyberspace as a place all its own. It does not have the duality of positive and negative volume while in physical space for example a room has the negative volume of usable space delineated by positive volume of walls, Internet users cannot enter the screen and explore the unknown part of the Internet as an extension of the space they are in , but spatial meaning can be attributed to the relationship between different pages of books as well as web servers , considering the unturned pages to be somewhere "out there. Video games differ from text-based communication in that on-screen images are meant to be figures that actually occupy a space and the animation shows the movement of those figures. Images are supposed to form the positive volume that delineates the empty space. A game adopts the cyberspace metaphor by engaging more players in the game, and then figuratively representing them on the screen as avatars. Games do not have to stop at the avatar-player level, but current implementations aiming for more immersive playing space i. Laser tag take the form of augmented reality rather than cyberspace, fully immersive virtual realities remaining impractical. Although the more radical consequences of the global communication network predicted by some cyberspace proponents i. The metaphor has been useful in helping a new generation of thought leaders to reason through new military strategies around the world, led largely by the US Department of Defense DoD. It has also been critiqued as being unhelpful for falsely employing a spatial metaphor to describe what is inherently a network. Visual arts have a tradition, stretching back to antiquity , of artifacts meant to fool the eye and be mistaken for reality. This questioning of reality occasionally led some philosophers and especially theologians[citation needed] to distrust art as deceiving people into entering a world which was not real see Aniconism. The artistic challenge was resurrected with increasing ambition as art became more and more realistic with the invention of photography, film see Arrival of a Train at La Ciotat , and immersive computer simulations. Influenced by computers[edit] Philosophy[edit] American counterculture exponents like William S. Burroughs whose literary influence on Gibson and cyberpunk in general is widely acknowledged [26] [27] and Timothy Leary [28] were among the first to extol the potential of computers and computer networks for individual empowerment. David Deutsch in The Fabric of Reality employ virtual reality in various thought experiments. For example, Philip Zhai in Get Real: A Philosophical Adventure in Virtual Reality connects cyberspace to the platonic tradition: Let us imagine a nation in which everyone is hooked up to a network of VR infrastructure. Immersed in cyberspace and maintaining their life by teleoperation, they have never imagined that life could be any different from that. Note that this brain-in-a-vat argument conflates cyberspace with reality , while the more common descriptions of cyberspace contrast it with the "real world". This interplay has several philosophical and psychological facets Papadimitriou, A New Communication Model[edit] The technological convergence of the mass media is the result of a long adaptation process of their communicative resources to the evolutionary changes of each historical moment. Thus, the new media became plurally an extension of the traditional media on the cyberspace, allowing to the public access information in a wide range of digital devices. Forwards, arise instant ways of communication, interaction and possible quick access to information, in which we are no longer mere senders, but also producers, reproducers, co-workers and providers. New technologies also help to "connect" people from different cultures outside the virtual space, what was unthinkable fifty years ago. New media art Having originated among writers, the concept of cyberspace remains most popular in literature and film. Although artists working with other media have expressed interest in the concept, such as Roy Ascott , "cyberspace" in digital art is mostly used as a synonym for immersive virtual reality and remains more discussed than enacted. Computer crime Cyberspace also brings together every service and facility imaginable to expedite money laundering. One can purchase anonymous credit cards, bank accounts, encrypted global mobile telephones, and false passports. Such advisors are loath to ask any penetrating questions about the wealth and activities of their clients, since the average fees criminals pay them to launder their money can be as much as 20 percent. According to this model, cyberspace is composed of five layers based on information discoveries: This original model links the world of information to telecommunication technologies. Popular culture examples[edit] The anime Digimon is set in a variant of the cyberspace concept called the "Digital World". The Digital World is a parallel universe made up of data from the Internet. Similar to cyberspace, except that people could physically enter this world instead of merely using a computer. The anime Ghost in the Shell is set in the future where cyberization of humanity is commonplace and the world is connected by a vast electronic network.

Chapter 2 : Understanding Digital Evidence - Law Enforcement Cyber Center

*Collecting in Cyberspace: A Guide to Finding Antiques & Collectibles On-Line [Shawn Brecka] on blog.quintoapp.com *FREE* shipping on qualifying offers. Lists more than two thousand Web sites, arranged by topic from animation art and Barbie dolls to trains and vintage clothing.*

IT Security and Data Protection In the previous article in this series I talked about developing your cyber intelligence analyst skills. The approach largely relied on becoming tool agnostic and developing a strong base through education. As the analyst it is your opinion and expertise that matters most. I also highlighted three of the more talked about sub-disciplines of cyber intelligence which are Intelligence Collection Operations, Cyber Counterintelligence, and Threat Intelligence. In this blog we will cover Cyber Intelligence Collection Operations. What is Cyber Intelligence Collection Operations? When an analyst goes about collecting information or data it should more often be a part of a larger effort to reach some goal or answer some question instead of just being a singular event. When thinking of the military or government aspect, there also tends to be an over valuation on information the government obtained or classified material. While government operations or material that was deemed classified can be enticing one must always remember it was conducted or written by other analysts; while not always the case sometimes analysts get it wrong or over hype their own products. Where collection operations are concerned there does not have to be anything classified or cryptic about them. Channeling the concept of the ongoing process, or operation, think back to the first blog post in this series and you will remember the intelligence lifecycle. In this blog we are specifically taking a look at the second step of an ongoing cycle â€" collection. To perform any sort of analysis on data you must have access to data. This seems simple enough but identifying the right sources of data can be one of the most difficult jobs an analyst has. Often, data that is mentioned in reports and threat feeds is already analyzed and lacks the original, or raw, data that the other analyst looked at. There is benefit in viewing the analysis of other analysts and companies but access to raw data can be critical especially for the purpose of validating the information. There are many ways to collect data. For the purpose of this blog I will highlight the three categories of collection I use to understand where data comes from and then discuss the three types of data. There is not a de facto standard but this is an approach that has helped me and I hope that it helps you as well. The three types of data collection: Passive â€" data collected on networks or information systems you have responsibility over. An example would be analysts capturing internal network traffic, collecting system logs, monitoring internal company forums, and other activities internal to their organization such as performing red team assessments. The key here is to highlight that the term passive refers to an analyst not directly engaging with an adversary or their infrastructure. Hybrid â€" data shared from other networks or information systems or collected from networks designed to entice adversaries. Here, an example of hybrid data would be Bank 1 sharing information off of their networks with Bank 2. Bank 1 may have recently been targeted by an adversary and sharing that information with Bank 2 can help them better prepare. Another example would be honeypots established to entice adversaries into interacting with them. Hybrid data collection is a key aspect of Threat Intelligence which will be discussed later in this blog series. Active â€" data obtained from external networks or information systems under the influence of an adversary. It is important to understand that networks or information systems under the influence of an adversary might not actually be owned or controlled by the adversary. An example would be a Command and Control C2 server being utilized to connect to malware. The C2 server may belong to an unwitting victim while it is being used by the adversary. Active data collection usually requires analysts to have access to sensitive data, participate in takedown operations performed by the government, or conduct law enforcement operations issued with legal warrants. This type of data collection must be performed carefully so that the legal and privacy rights of members are protected. After determining the type of data collection performed, it is imperative to understand the type of data collected. Three types of data classifications I use are: Raw Data â€" unevaluated data collected from a source. This type of data can be the most fruitful but requires extra time to process and analyze it; this type of data would be found in step two of the intelligence lifecycle. It should include raw details such as IP addresses, network logs, or full forum posts by a potential adversary. Exploited Data â€” data processed and exploited analyzed by another analyst which contains selected raw data. This is the type of data that might be available to an analyst after the third step in the intelligence lifecycle. It should contain raw data and technical details if available but it might only be raw data that the analyst found interesting and not all of the data. This type of data should include analysis on what the data means or indicates. An example would be malware or computer campaign reports with technical information and analysis on a threat. Production Data â€” data finalized into a report meant for dissemination that may include limited or no raw data. This type of data that would be available after the fourth step in the intelligence life cycle. Often, production data may only be intended for the awareness of a reader or customer or it might be intended for suggested actions. An example would be advisories given to users or Intrusion Detection System signatures readymade for deployment. However, the most important aspect of Cyber Intelligence Collection Operations is correctly identifying the right sources of data and making sure the data is valid. Any time you try to conduct intelligence operations you must be aware that data or analysis can be incorrect and that false data can be placed for the purposes of counterintelligence and deception. The next article in this series will discuss the aspect of cyber counterintelligence. He is also Co-Founder of Dragos Security LLC , a cyber security company which develops tools and research for the control system community. Additionally, Robert is an active-duty U. Air Force Cyberspace Operations Officer â€” his views and this article are his own and do not represent or constitute an opinion by the U. He has published and presented on cyber security topics in publications and conferences around the world, and is the author of SCADA and Me. The opinions expressed in this and other guest author articles are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc.

Chapter 3 : Cyberspace - Wikipedia

Note: Citations are based on reference standards. However, formatting rules can vary widely between applications and fields of interest or study. The specific requirements or preferences of your reviewing publisher, classroom teacher, institution or organization should be applied.

There are a number of explanations for this, including the rapid changes and proliferation of digital devices, budgetary limitations, and lack of proper training opportunities. Performing digital forensics can be an expensive proposition involving licenses, equipment and significant personnel costs. Demonstrating cost effective return on investment is crucial to securing command staff buy in. Funding these efforts can involve a complicated mix of local, state and federal budgets, and this can be particularly challenging for smaller departments. Regional models and other forms of collaboration can help, provided officers know where to turn for help. Advanced digital evidence training is not yet part of the core curriculum for police academies, yet officers of all levels of experience may have contact with digital evidence that is sufficient to affect the resolution of the case. Departments face large digital evidence backlogs, limited equipment, and potential turnover of examiners. Contributing to the backlog is the lack of personnel trained in digital evidence extraction. A growing backlog prevents training opportunities since classes would take examiners out of the workplace, and a backlog can undermine requests to replace inadequate, antiquated, or under-funded technology and licenses due to budget constraints of units perceived to be performing slowly. Violation of the law In the early days of digital evidence the focus was predominantly on computer crime. However, now nearly every crime has some digital artifact that might be useful for an investigation. As a result, proactive investigation now considers how digital evidence might be exploited for non-computer crimes as well. As victims of such crimes increasingly turn to law enforcement for assistance, adequate processes for responding need to be in place not only to assist the victim, but also to capture digital evidence and information that might otherwise be lost. Seizure The Fourth Amendment provides protection against unreasonable search and seizure by governmental authorities. This has been an area of much debate with respect to digital evidence. Most recently, the recent Riley Riley v. Riley makes on-scene triage more challenging. When an arrest is made, there is a possibility that a confiscated cell phone could be wiped via a remote command or timed security locks activated resulting in loss of access to data. Even with a warrant, seizure of digital evidence can be present several challenges. First responding officers to an incident or arrest often do not know how to secure and use digital evidence to preserve chain of custody and later admissibility in court. In many cases, considerable jurisdictional challenges exist when the digital evidence required for an investigation does not exist on a physical device at the crime scene, but rather on a server many counties, states, or countries away. International warrants can be complicated by the necessary mutual legal assistance treaty MLAT which can incur significant delays for assistance, if any is even provided. Several trends may further complicate seizure of digital evidence in the future. Developing law suggests that overly broad civil subpoenas may not be sufficient to compel ISPs to provide private information of users as current judicial thinking is tending toward greater restriction on what is included in searches of electronic devices Murphy and Esworthy, Preservation When prosecution is the goal, chain of custody, discovery, and other issues pertaining to the use of digital evidence in the courtroom are paramount. Documentation requirements include authentication i. Some courts are skeptical of digital evidence due to uncertainties about chain of custody and validity of information obtained from devices. Overcoming these challenges requires rigorous documentation of data such as when the evidence was collected and where it was collected from i. Finally, chain of custody involves documenting how the evidence was stored, who has handled the evidence, and who had access. Examination Digital evidence requires different training and tools compared to physical evidence. The range of extraction modes that can be required to obtain digital evidence from different sources or types of devices including those belonging to both suspects and victims means that its collection and use is truly a multi-faceted challenge, potentially requiring building and maintaining a variety of quite different technical capabilities and expertise. Manual techniques involve using standard inputs included with or built into the device, such as touch screens or keyboards. Logical extractions incorporate external computer equipment to provide commands through code to the targeted device. Physical techniques refer to reading information from flash memory sources. The most specialized processing options, chip-off and micro read, are highly technical activities and represent advanced digital evidence extraction. Additional obstacles may need to be overcome even after data is extracted from a device. Apple announced that its new iOS 8 operating system has improved security that prevents Apple from unlocking phones even in response to a request from law enforcement. On phones using the new operating system, photos, messages, email, contacts, call history, and other personal data are under protection of a passcode that Apple is not able to bypass. Google has announced that it will do the same in new Android-based operating systems. The listing and variety of device and products poses challenges as there is no uniform process to obtain information across makes and models, let alone different types of devices. In addition to physical devices that are seized by law enforcement, digital evidence may need to be collected and examined from networked devices, both single servers and entire constellations of IT systems. These networked devices may or may not be beyond the physical reach of law enforcement. Computer â€” There is a wealth of potential digital evidence on a personal computer. When browsing the internet, programs will often maintain temporary internet files, cookies, and a browsing history. Emails and other messages may be found on the physical computer as well. Portable electronics â€” Currently, digital evidence processing from portable electronics such as cell phones is the primary focus of interest to examiners and researchers. There should be no surprise that cell phones are the dominant interest within the field of digital evidence. Internet â€” Some of the first digital evidence used in law enforcement investigations came from communication websites, particularly message boards and chats rooms. File sharing networks are another major source used during investigations. Some internet technologies have been designed specifically to enable the hiding of the identity and location of individuals accessing or sharing information. For example, the Tor Project provides a high degree of anonymity for internet users. In some cases methods and tools for examination from ten years ago are insufficient and incompatible with current technology. This turnover is due to the rapidly changing landscape of personal electronics. Using the most up to date tools can help mitigate challenges to the acceptability of results of digital evidence analysis in court. In contrast, using invalidated tools runs the risk of missing critical information or otherwise jeopardizing an investigation. Analysis As digital devices such as computers, cell phones, and GPS devices become ubiquitous, analysis of digital evidence is becoming increasingly important to the investigation and prosecution of many types of crimes as it can reveal information about crimes committed, movement of suspects, and criminal associates. If departments do not have enough of the right people to process the volume of digital evidence, the result is a large backlog no matter what tools are used. Without the right tools, departments may lack the capability to represent complex data sets in understandable ways for investigation and presentation. Temporal, spatial and network analysis of large troves of digital evidence benefits significantly from software that is explicitly designed to facilitate those specific methodologies. Exploitation of multimedia data presents another emerging analytical challenge. In the course of an investigation time is of the essence and triage has been recognized as an effective means of getting useful information early without waiting for in depth analysis of the entire target system. Scant attention has been given to developing robust capabilities in this area, though some recent attempts have promise. Triage tools could lower the minimum skill threshold for some parts of the analysis of digital evidence and consequently reduce the workload and backlog of the digital evidence lab. Nevertheless, in order to effectively operationalize triage and optimize the use of scarce resources, a systematic method of prioritizing a work queue is required. Reporting The role of law enforcement does not end with an arrest or clearance. Police must give evidence to prosecutors and effectively communicate both the significance of and process to obtain digital evidence to all parties, including a jury. There are significant challenges in the investigative process, up to and including the handoff of evidence to the prosecution that must be addressed to successfully use digital evidence in prosecutions. This can range from inexperience of patrol officers and detectives in preserving and collecting digital evidence, to lack of familiarity of court officials about the nature of digital evidence. Typically issues with evidence in general and with digital evidence in particular include hearsay, admissibility and obligation to the defense. A common exception to the hearsay rule is the business records exception. The Frye test Frye v. United States, 54 App. More recently, the Frye test has been replaced in federal courts by the Daubert test Daubert v. Merrell Dow Pharmaceuticals, U. Daubert uses five criteria to determine the admissibility of scientific evidence: The work of NIST is, for this purpose, very important. The field of digital evidence â€" both the devices to be exploited and the tools to exploit them â€" change rapidly. NIST testing provides the basis for asserting that the data gathered and analyzed by new tools is scientifically valid. Finally, obligations to the defense require that defense attorneys receive a duplicate copy of digital information or access to view it and that exculpatory evidence be brought to the attention of the defense. Information disconnects can emerge between the prosecution and the defense. One reason the defense may be behind is because they receive evidence through discovery weeks after the prosecutors do and therefore have even less time to sift through the amount of information. While defense attorneys can challenge how the records were acquired and chain of custody issues, especially in the context of the cloud, most are ineffective at pushing back against digital evidence presented by the prosecution. However, this balance may shift as the technology improves and if it does defense attorneys will eventually obtain a parity of digital evidence knowledge, which will result in more successful challenges. Execution of the Law Judgment at trial in some ways represents the close of the law enforcement process that began with the violation of a law and ends with the execution of a law. Judges, juries, and defense attorneys clearly have a stake in digital evidence processing. Objections to digital evidence are rarely sustained, provided that the evidence meets the Daubert standard. Juries often find the presentation of digital evidence compelling. Yet, variation remains in the familiarity with digital evidence across different areas of the criminal justice system e. Lack of knowledge about digital evidence on the part of judges can complicate appropriate use in court or echelons of command within law enforcement e. However, consensus is easier to find when successful processing of digital evidence directly results in more cases solved and more successfully prosecutions on the basis of that evidence. The current trend is an increasing number of positive outcomes, and positive feedback that results from showcasing these efforts. Davis, and Brian A.

Chapter 4 : COLLECTING DIGITAL EVIDENCE OF CYBER CRIME. | Historically Digitized - blog.quintoap

Find helpful customer reviews and review ratings for Collecting in Cyberspace: A Guide to Finding Antiques & Collectibles On-Line at blog.quintoapp.com Read honest and unbiased product reviews from our users.

Misbah Saboohi Assistant Professor, Law. International Islamic University, Islamabad. The law enforcement community is facing a new challenge today, in the form of information technology age in the wired world. Asking a computer wizard to upgrade our computers or the reporting of computer crimes may be easy but combating this crime and getting successful convictions still remains an uphill task for the present law regimes around the world. Countries are depending more every day on innovative information technology in administering almost every aspect of daily life, ranging from ID cards, credit cards to health records or the security and defense of its borders. Yet, nations are now also concerned about taking specific steps in protecting themselves from losses caused by cyber criminals who act anonymously and may not even be within the national borders. No one can really answer this question. But in terms of financial losses it has cost billions of dollars to the industries annually. If left unchecked, cyber crime can potentially hijack all expansion of electronic commerce and Governance. The Internet has provided a lot of benefits to the society and businesses; likewise, it also provides new opportunities from criminal conduct. Generally cyber crimes fall into three categories: Crimes where a computer is the target, e. Crimes where computers are the medium by which criminal enterprises are executed e. Crimes where the use of a computer is incidental to criminal acts e. The major challenges that cyber crimes pose are that they do not recognize and are therefore not limited by any boundaries. An individual armed with nothing but a PC can target businesses or air traffic controls anywhere in the world without ever stepping a foot outside his room. Anonymity is a major issue of this area of crime. But law enforcement is confined to state borders and the sovereignty of nations has to be respected. If international co-operation or a mutual legal assistance agreement is not in place, many criminals go unpunished. Laws are also not comprehensive to tackle crime or the criminal. There is also a dearth of experts handling computer crimes in the world; even the few that are in the field have a lot of disparity in their work. But even if we put all these problems aside, collection of evidence and its admission in a court of law for successful prosecution in a cyber crime case is a very difficult technical job, which requires huge funds and expertise. So much so that sometimes the criminals themselves are the only experts who can help the law enforcement agencies in collecting forensics of the computer on or through which the actual crime took place. It can therefore be imagined what will be the ratio of successful cases for the police and law enforcement agencies. It is easy to steal, leak, manipulate or destroy electronic data. But just as in the physical world, cyber criminals too leave their electronic fingerprints and footprints at a digital crime scene3. Often when a company is faced with a cyber attack or crime, it does not know where to start, what to do or even whom to turn to. But the best line of defense is to make right policies, procedures and communications in place otherwise the time bomb is ticking. Laptops, digital cameras, mobile phones provide a mountain of data and proof that can solve a case. Email has also become indispensable in prosecuting organized crime5. What can be the best tool to collect evidence of a cyber crime and present it in a court of law to successfully convict a cyber criminal? Traditional methods have not proved useful in this area thus far and therefore a different technique would need to be adopted. Here are some of the necessary steps which one should remember in collecting computer forensic evidence. Planning the response is important. One should not panic, and the person should not touch any button on the computer. It is important that the crime is reported immediately because time is of essence in cyber forensic evidence collection. Usually unaltered digital evidence is available only within the span of a few hours. Sometimes even 24 hours proves to be too late to recover non-tampered digital evidence. In this step the company should be clear as to whom it has to report to so that an investigative team is formed, because the investigators may access sensitive data. There should be a clear privacy policy in place. Only a skilled computer forensic investigator should undertake investigation. Otherwise collection of evidence will almost end up in a failure of an investigation and ultimately a failed prosecution. It is also very important for the investigator to understand the level of sophistication of the suspected criminals6. They must be considered to be experts in any case and ancillary counter-measures must be adopted to guard against the destruction of any digital evidence. If this is neglected, it may modify the data on the computer. Some computers have automatic wiping programmes in case a new person touches the wrong key on the keyboard. It then becomes time-consuming and expensive to recover such data, if at all possible. Electronic evidence is fragile. It can be damaged or altered by improper handling or examination. Special precautions should be taken to document, collect, preserve and examine this type of evidence7. This will ensure the integrity of the electronic evidence at a later stage. When a cyber crime is committed, the room and computer of occurrence should be considered to be a crime scene and sealed off to ensure evidence is not tampered with. It is critical that in early stages nothing is changed in the immediate surroundings of the device. If the computer is off, it may be left off, if it is on, it should be left on. Care is necessary so that standards of admissible evidence can be followed. If the computer is mishandled at that time, the data collected can be challenged later and may not be valid before a court of law e. As a forensic expert, one should have legal authority to seize and read the data from the device. Otherwise the consequence may be that not only the case is thrown out but also that the investigator may find himself being sued for breach of privacy and damages. Other useful tips are to take photographs of the surroundings, seizing and securing any papers, printouts, disks, MP3 players etc lying around in the vicinity of the cyber crime. Likewise, interviewing and recording the statements of people at that place can prove to be helpful. These people can later be potential witnesses in the lawsuit. This can also help in discovering passwords or email addresses of the suspect. This is a crucial stage of digital evidence collection. It is to duplicate the entire hard drive. One has to make a bit- stream copy of every part of user accessible areas, which can store data. The original drives should then be moved to secure storage to prevent tampering. It is important to use some kind of hardware write protection to ensure no writes will be made to the original drive Even if the operating system, such as Linux, can itself be configured to prevent this, it is a better and safer practice to separately use a hardware write blocker. It is possible to image to another hard disk drive, a tape or other media. Tape is a preferred media to store images since it is less susceptible to damage and can be stored for a longer time. It should be ensured that the image is: The SHA-1 message Digest algorithm or other such algorithms can be used to verify the imaging process. To make forensically sound images, it is advisable to make two reads that result in the same output. Generally the drive should be hashed in at least two algorithms to help ensure authenticity. Imaging should be made within the crucial timeframe for collecting electronic evidence, since thereafter its credibility would become questionable and not valid for legal purposes. Every bit of information should be copied. Deleted or even damaged files are actually never deleted or gone and can be recovered by the imaging process, though it may takes days or even weeks to recover them. One tip given by experts is to keep one master copy in some safe place of agency to be used as a back up, and to use the second one as working copy for the investigation and analysis. Everyday computers or media should not be used. New media should be used, e. Now many law enforcing agencies have their own labs for imaging and analysis of digital evidence whose reports are used in legal cases. Imaging software should be forensically sound so that no changes occur during imaging. Such software is commercially available, though expensive and often costing millions of dollars All investigation material should be backed up. It is therefore necessary that the persons involved in evidence collection relating to cyber crimes are specially trained personnel. Investment should be made now in such training, which are available worldwide. Court rooms and universities are welcoming more lawyers and agents to specialize in electronic crime issues, thereby setting stage for evolution of cyber law while the debate over digital evidence and what limits may be put on it is still raging The expert then examines the digital evidence and gives a final report about the act complained of as a crime. This report is a determination of whether an act on a computer was a breach of any penal law or not. Therefore it should be made very carefully. It must be objective, based on indisputable facts, because law enforcers will connect the suspect to the act of the computer performed by a human. This connection therefore has to be beyond reasonable doubt. It is advisable to obtain and rely on professional legal advice at this stage. But above all, the existence of a regulatory framework and laws catering for cyber crimes in the country are the sine qua non. The above discussion is only one part of cyber crime evidence collection. The second equally important phase is presenting all that digital evidence in a court of law as evidence against a suspected cyber criminal to successfully convict. In Pakistan13, it is allowed to use any modern devices through which evidence can be presented in the court. Under the Electronic Transactions Ordinance, , electronic evidence via emails etc. But the real question is how far the digital evidence collected by a computer expert fulfills the criteria set by the general law of evidence to prove guilt of a criminal.

Chapter 5 : Cyber-collection - Wikipedia

Data Collection in Cyberspace Some ethicists argue that the very conduct that results in resistance from participants â€”interference, invasiveness in their lives, denial of privacy rightsâ€”has encouraged researchers to investigate topics online. The growth of cyberstudies causes us to question how we gather data online, deal with participants, and present results. Issues relating to.

Sat, 23 Apr Introduction Recent technological advancements in the reproduction and distribution of intellectual property have presented a serious challenge to intellectual property law. Fortunately, these same advancements suggest a new method by which intellectual property could be sold; an overview of this method, called NetRelease, is given in this article. NetRelease is not intended as, nor could it serve as, a replacement for existing intellectual property law. It is merely a method by which, in certain circumstances, some of the problems of protecting intellectual property can be side-stepped. Background Intellectual property law was conceived with the purpose of encouraging creativity and exploration, and the dissemination of the fruits thereof. A government provides legal protection of these fruits as an enticement to creators and explorers to develop their arts and share their results. The practical details of this protection were devised to be effective in a world of physical objects: However, these practical details have not proven so effective in the electronic universe called cyberspace. There are several aspects of cyberspace which frustrate conventional methods of protecting intellectual property. For example, in cyberspace, copies of digitally-representable intellectual property can be made at negligible cost, cannot be distinguished as legitimate or illegitimate, can be instantly sent to thousands of people, and can be instantly destroyed without any trace. The original purpose of intellectual property law is still valid. It is time to develop alternate methods of providing an enticement to creators and explorers--methods appropriate to cyberspace. The Time Factor The protection of intellectual property in the world of physical objects has been tailored to a time scale appropriate to the practicalities of reproducing, advertising and distributing physical objects. Patent protection in the United States has a term of seventeen years, a long enough period to allow a person to gather investment capital, build a factory, run a production line, and collect returns sufficient to pay back the investors, pay royalties to the inventor, and turn a profit. In cyberspace the time scale is much shorter. Digitally-representable intellectual property can be reproduced, advertised and distributed globally in minutes. And the period during which intellectual property can be protected in cyberspace has been similarly reduced: Once something is in cyberspace, it cannot be easily controlled. How NetRelease Works In NetRelease, the period during which a royalty is paid to the creator is compressed to match the period during which intellectual property can be protected: You broadcast an advertisement into cyberspace. People who want to read the book pledge to pay for that privilege. The amount they offer is their own choice. At that instant, two things happen: It may henceforth be distributed freely. Advantages The "instant royalty" of NetRelease is a great advantage to authors and other creators, who get immediate payment in full. Thus, NetRelease encourages creation. In the physical world, putting intellectual property in the public domain is not necessarily the best way to assure its dissemination. For example, a book publisher does not want to compete with a xerox machine -- as it must if a work is not copyrighted -- and publishers are very often responsible for distribution. But in cyberspace, the best works circulate the most widely and quickly. Thus, NetRelease encourages dissemination. With NetRelease, less energy is spent trying to enforce copyright laws in cyberspace. NetRelease "goes with the flow" in that it is improved as the speed and ubiquity of cyberspace increases. Remarks Following are some thoughts about implementation, side-effects, etc. NetRelease could be independent of protection in the physical world. A work could be protected by copyright in the physical world while circulating freely in cyberspace, or vice versa. Or, the two could be tied, in which case NetRelease would also allow anyone to reproduce the work in the physical world. NetRelease need not replace conventional intellectual property law. It requires some legal support: Generally, though, NetRelease removes the issue of enforcement in cyberspace. Reputation would have a lot to do with the amount of pledges that a NetRelease would generate. The advertising function of publishers might be subsumed by agents. An unknown author would submit a work to an agent, who would then promote the work. The reputation of the agent would in this case be more important than the reputation of the author. Software companies using NetRelease could continue to provide services and physical products manuals, etc. NetRelease may only become practical when cyberspace gets bigger, and people develop tools for handling the details: A software company could release outdated versions of its product via NetRelease while keeping the current version under protection of physical world copyright. There are many possible methods by which payment for a NetRelease could be collected. It could be done through an existing mechanism like by credit card or through number , or a new type of brokerage could be established for managing such accounts. Other NetRelease is an idea by Stephen Malinowski.

Chapter 6 : An Introduction to Cyber Intelligence - The State of Security

The following poem was shared by Mark L. Hamburg at philatelic@blog.quintoapp.com STAMP COLLECTOR My worldly wealth I hoard in albums three, My life collection of rare postage stamps; My room is cold and bare as you can see, My coat is old and shabby as a tramp's; Yet more to me than balances in banks, My albums three are worth a million francs.

How have their investments paid off so farâ€”and what do they hope to achieve in the future? Selling art on the Internet has been likened to trying to hit a moving target. No one knows quite where to aim, but everyone knows there is something out there. At a wild pace, auction houses and art dealers are coming up with ways to sell fine art online. Some have jumped onto the Internet with adolescent vigor, some have dipped in an uncertain toe, and still others are staying clear of the murky waters altogether. No one wants to make a mistake; no one wants to be first; no one wants to be left out. The new millennium will answer the elusive question: Jupiter Communications, a New Yorkâ€”based e-commerce research firm, estimates that 29 million people in the United States made an online purchase, via auction or other method, in How much of this online consumer demand will be directed toward fine art? Neither firm has any idea. The art trade is a discreet, unregulated, and highly fragmented industry. Auction specialists and dealers who have been in the business for decades cannot pin down how many art dealers exist or the breadth of worldwide annual sales. For the most part, auction housesâ€”which have seen an increasing number of collectors bid by telephone and absentee form in recent yearsâ€”have accepted, if not embraced, the idea of selling fine art online as a vital part of their future businesses. You just know how huge it is. That is still a hard sell. Among those who have made the leap are: Despite spreading enthusiasm, many dealers are still unsure about how they will use the Internet to enhance their business. It can serve as an advertisement, an index, an archive, a catalogue, a window, a rack, a magnet, and as an assistant who keeps the gallery open 24 hours a day, takes messages, and never intimidates visitors. The fine-art business is in the business of selling the communication between the viewer and the unique object. The further one gets from that communicative aspect, the less likely one is to make a sale. The painting turned out to be an original by 19th-century American artist Martin Johnson Heade. Already one thing is clear: Giving up things and gaining others. As a private firm, it did not face the same pressures to reveal its Internet plans as did those auction companies with shareholders to appease. Still other companies followed with announcements of their own. The New Yorkâ€”based online art portal artnet. When it first went public, artnet. Some of our best clients were threatening never to do business with us again. The learning curve is steep. It takes superhuman effort to get things right. Meanwhile start-up Internet art companies began popping up daily. But by October, none had launched. The reason for the delays? In a move that altered the traditional relationship between art dealers and auction houses, the firm sent out a slew of invitations to a select group of dealers whom it wished to involve in its new venture. The contract stipulated that dealers could offer their inventory for auction on sothebys. The contract does not prohibit associates from selling works on nonauction sites. Even forward-looking people tend to procrastinate when it comes to change. It forced dealers to think about what they wanted. We are not equipped to handle that much property. We will catalogue the consignments we receive, but we are limited to specialists. The names of underbidders will be released by the auction house with their permission. At press time more than 4, dealers had signed up with sothebys. I believe in a more up-close-and-personal approach. Collectors are not names and numbers, and art is not chips or stocks or bonds. Internet auctions are time-based silent sales, in which Internet users submit bids for items that are posted online for a limited time period. The highest bid at the end of the auction wins the lot. Ebay built its reputation as a person-to-person site that functions much like a classified-ad section in a news-paper: Another example of a person-to- person auction site is auctionuniverse. Online portals also specialize in person-to-person auctions, offering fine-arts sections among other categories. Last September, Microsoft launched person-to-person auctions www. Analysts, however, believe that business-to-consumer auctions, in which property is offered by companies or qualified professionals, will soon outpace person-to-person auctions because they offer consumers a reduced risk of fraud. In a departure from its person-to-person auction model, eBay Great Collections offers fine art, antiques, and collectibles in a business-to-consumer site, where a network of dealers and auction houses provides and guarantees the works offered. This is comparable to bidding by telephone, but in this case the bid is submitted with the click of a mouse. Specific figures detailing how many Internet bidders registered for the sale or how many of the sold lots went to online buyers were not released. Auctioneer Nicholas Lowry at Swann Galleries was not overly impressed by the online technologyâ€”there was a technological glitch that interrupted Internet bidding for a period of timeâ€”or the response the sale received. Still, some major auction houses and online firms are not yet convinced that the live-bidding technology is up to par. An interested party can contact the gallery directly and arrange to see the work in person or can choose to purchase the item sight unseen. New York dealer Joan Whalen, who specializes in American paintings and contemporary works, says that since she started her gallery site with artnet. Our view is that by going online we can get a larger slice of the art market by bringing live clients to our online sales and online clients to our live sales. In its efforts to expand its reach, the firm will use its dealer network to make tens of thousands of valuable objects available on the Internet on any given day. This will be done in two ways: In the future, most large collections consigned to the firm will be auctioned in both a traditional sale and online. We want to see that number expand geometrically. In the week prior to s othebys.

Chapter 7 : Cyber Intelligence Collection Operations - The State of Security

blog.quintoapp.com: Collecting in Cyberspace: A Guide to Finding Antiques & Collectibles On-Line () by Shawn Brecka and a great selection of similar New, Used and Collectible Books available now at great prices.

IT Security and Data Protection This is the beginning of a short blog series on the topic of cyber intelligence, its sub-disciplines, and its uses. Cybersecurity program on topics including cyber intelligence and cyber counterintelligence. One of my observations while building the course syllabus and instructing the students is that there is a general lack of information on what cyber intelligence is and how to appropriately use it. There are a few resources out there but cyber intelligence is more often thrown around as a buzz word for company statements and contracts than it is actually defined and used. The first step to understanding cyber intelligence is to realize that intelligence tactics, techniques, and procedures TTPs as well as various types of operations existed long before cyberspace was conceived. Intelligence is most often seen as offensive in nature when viewed from the lens of spying and collection operations but its ultimate purpose is also equally rooted in defense. In a military context commanders want to know the intent of the adversary to either make better strategic choices on the battlefield offense or to more aptly prepare for an attack defense. The definitions and tradecraft used by various government and military organizations serve as the best foundation for understanding cyber intelligence. These definitions and processes will be reviewed in this first blog post and set the theme for the series as we explore the specific discipline of cyber intelligence more in depth. From that document we can extract three very important pieces of information for use in cyber intelligence. The first is the definition of intelligence: The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The activities that result in the product. The organizations engaged in such activities. From this definition we see that the DoD views intelligence as a product, the activities in that product, and the organizations performing the activities. Most civilian organizations and uses of intelligence will not include goals defined by foreign nations. A useful and more simplistic definition for general use thus can be presented as: Intelligence is both a product and process from collecting, processing, analyzing, and using information to meet an identified goal. This definition is applicable to cyber intelligence and we can simply apply the sources and efforts of the collection, processing, analyzing, and using of the intelligence to cyberspace related topics. The second important piece of information from JP is the way the DoD intelligence community defines its intelligence disciplines. This would be a much longer blog post to go through each discipline and define them but it is well worth the read to understand how the DoD defines specific categories of intelligence disciplines. As examples, there are those that are more commonly referenced such as HUMINT human intelligence derived from human to human interaction , OSINT open source intelligence gathered from publicly available sources and SIGINT signals intelligence usually refers to electronic mediums from sources such as satellites. It can be helpful to understand these terms but the biggest takeaway is realizing that there are disciplines of intelligence and that it is useful to categorize the intelligence by both its intended use and collection source so that you can evaluate it and apply it quickly and correctly. Cyber Intelligence would be a specific discipline in intelligence some have tried to use CYBINT as this term although it has never truly caught on. The JP document contains a lot of other great pieces of information such as how the DoD fuses their intelligence products together to use them. This can be useful to provide a baseline of how others do it so you do not have to train yourself or others from nothing. However, the final useful piece of information I want to highlight is the intelligence lifecycle. The intelligence lifecycle is something we will want to use extensively in cyber intelligence. The intelligence cycle is a circular and repeated process to convert data into intelligence useful to meeting a goal of a user or customer; it has the following steps: Planning and direction â€” Determine what your requirements are. To appropriately create any amount of intelligence out of information you should have a defined goal and intentions. This could be something as simple as wanting to know the command and control servers of a piece of malware so that you can block it on your network to wanting to know the type of information systems your target uses so that you can infiltrate them. As you move through the intelligence cycle you can go back and address the steps again as an example if you get new data which reveals something you did not know, an intelligence gap, you may define a new goal. Collection â€" Where and how you acquire the data and information to process. You should know most of your available collection options while in the planning and direction phase so you can make reasonable goals or intelligence needs. Processing â€" The conversion of your collected information into something you can use. This may apply to how you store and access the data or the actual parsing of data such as converting it to human readable information such as ASCII from binary data. Production â€" This is the step in which you will take your data and turn it into an intelligence product. This is done through analysis and interpretation and thus is heavily dependent on the analyst. All produced reports should meet a defined intelligence need or goal from your planning and direction phase. Dissemination â€" Supplying your customer or user with the finished intelligence product. If your users cannot access your product or cannot use it then it is useless and does not meet a goal. From the above, we gather a great start into understanding cyber intelligence and moving to a point where we can use it appropriately. We also see the theme that intelligence is highly dependent on analysts and their interpretation of data. In the next blog we will take a look at what it means to be a cyber intelligence analyst and some tips on developing your skills. To learn more about how Tripwire can help you with your cyber intelligence, click here. He is also Co-Founder of Dragos Security LLC , a cyber security company which develops tools and research for the control system community. Additionally, Robert is an active-duty U. Air Force Cyberspace Operations Officer â€" his views and this article are his own and do not represent or constitute an opinion by the U. He has published and presented on cyber security topics in publications and conferences around the world, and is the author of SCADA and Me. The opinions expressed in this and other guest author articles are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc. Related Cyber Intelligence Articles:

Chapter 8 : Digital Evidence - Law Enforcement Cyber Center

This easy-to-use guide identifies more than 2, sites of particular interest to the collecting community. It also includes getting connected and using the Internet, and the pros and cons of on-line buying, selling, and trading.

Specific technical details of these attack methods often sells for six figure sums. GPS, WiFi, network information and other attached sensors are used to determine the location and movement of the infiltrated device Bug: Likewise, audio streams intended for the local speakers can be intercepted at the device level and recorded. Hidden Private Networks that bypass the corporate network security. Keylogger and Mouse Logger: Combined with screen grabs, this can be used to obtain passwords that are entered using a virtual on-screen keyboard. In addition to showing sensitive information that may not be stored on the machine, such as e-banking balances and encrypted web mail, these can be used in combination with the key and mouse logger data to determine access credentials for other Internet resources. Collected data is usually encrypted at the time of capture and may be transmitted live or stored for later exfiltration. Likewise, it is common practice for each specific operation to use specific encryption and poly-morphic capabilities of the cyber-collection agent in order to ensure that detection in one location will not compromise others. Because the malware agent operates on the target system with all the access and rights of the user account of the target or system administrator, encryption is bypassed. For example, interception of audio using the microphone and audio output devices enables the malware to capture to both sides of an encrypted Skype call. Cyber-collection agents usually exfiltrate the captured data in a discrete manner, often waiting for high web traffic and disguising the transmission as secure web browsing. USB flash drives have been used to exfiltrate information from air gap protected systems. Exfiltration systems often involve the use of reverse proxy systems that anonymize the receiver of the data. Agents may replicate themselves onto other media or systems, for example an agent may infect files on a writable network share or install themselves onto USB drives in order to infect computers protected by an air gap or otherwise not on the same network. Manipulate Files and File Maintenance: Malware can be used to erase traces of itself from log files. It can also download and install modules or updates as well as data files. This function may also be used to place "evidence" on the target system, e. Some agents are very complex and are able to combine the above features in order to provide very targeted intelligence collection capabilities. For example, the use of GPS bounding boxes and microphone activity can be used to turn a smart phone into a smart bug that intercepts conversations only within the office of a target. Since, modern cellphones are increasingly similar to general purpose computer, these cellphones are vulnerable to the same cyber-collect attacks as computer systems, and are vulnerable to leak extremely sensitive conversational and location information to an attackers. For instance if the victim were parked in large parking lot the attackers may call and state that they saw drug or violence activity going on with a description of the victim and directions to their GPS location. Infiltration[edit] There are several common ways to infect or access the target: An Injection Proxy is a system that is placed upstream from the target individual or company, usually at the Internet service provider, that injects malware into the targets system. For example, an innocent download made by the user can be injected with the malware executable on the fly so that the target system then is accessible to the government agents. A carefully crafted e-mail is sent to the target in order to entice them to install the malware via a Trojan document or a drive by attack hosted on a web server compromised or controlled by the malware owner. Usually this device is placed at the Internet service provider. The Carnivore system developed by the U. FBI is a famous example of this type of system. Based on the same logic as a telephone intercept , this type of system is of limited use today due to the widespread use of encryption during data transmission. A wireless infiltration system can be used in proximity of the target when the target is using wireless technology. This is usually a laptop based system that impersonates a WiFi or 3G base station to capture the target systems and relay requests upstream to the Internet. Once the target systems are on the network, the system then functions as an Injection Proxy or as an Upstream Monitor in order to infiltrate or monitor the target system. A USB Key preloaded with the malware infector may be given to or dropped at the target site. Cyber-collection agents are usually installed by payload delivery software constructed using zero-day attacks and delivered via infected USB drives, e-mail attachments or malicious web sites. In the Flame operation, Microsoft states that the Microsoft certificate used to impersonate a Windows Update was forged; [20] however, some experts believe that it may have been acquired through HUMINT efforts.

Chapter 9 : Threat Intelligence Collection Specialist - Orpheus Cyber

In the previous article in this series I talked about developing your cyber intelligence analyst blog.quintoapp.com approach largely relied on becoming tool agnostic and developing a strong base through education.