Student: Kurt Williams
Instructor: Diwakar Yalpi
Course: 202410_CYSE201S_19043
Date: 11/24/2024

Reporting Requirements and Best Practices for Forensic Investigations

Digital forensics has become an invaluable resource for criminal investigations and military intelligence operations in the 21st Century. International drug cartels, hacker activists, online scammers, radical terrorist groups, and racially motivated violent extremists all use digital communications and devices to plan, fund, recruit, coordinate, and conduct their activities. Developing a standard of documenting the results of forensic exploitation from these devices is a crucial step in the investigative process (Casey, 2011). This standard of documentation and reporting should fulfill critical information requirements of the organization the forensic analyst is supporting. The reporting requirements and standards may vary between local law enforcement investigating a gun smuggling group and a US military organization capturing insurgents in a war zone, but the goals will remain the same (US Department of the Army, 2006; US Department of Justice, 2014). Ultimately the analysis derived from these reports could directly contribute actionable information to an investigation and help capture malicious actors from various criminal and extremist groups. There should also be a solid forensic investigative team that is properly vetted, trained, and equipped to carry out forensic analysis. The forensic investigative team should always remember that their efforts can help prevent these bad actors from causing further damage to their victims and societies around the world. This forensic team's training should include knowledge and background on several principles from social sciences, such as the psychology behind why cyber actors commit crimes, the human factors affecting their motivations, social forces affecting a cyber actors activities, and the overall social culture of the demographic group that the cyber actor originates from.

Of the seven individual motivations for why people commit cybercrimes, a digital forensics investigator should try to categorize why the cyber criminals they are investigating are committing these crimes. For money: I find this one to make the most sense, since so many cybercriminals commit identity theft or fraud for monetary gain everyday. Crime of many kinds are often committed for financial gain, and cybercrimes are no different. Political: Many cybercriminals are motivated by political/ideological reasons to target government entities or political figures. Sometimes these criminals are acting as private entities without any direction, but other times they are acting on behalf of a rival government to target another nation to undermine their opposition. Many state-sponsored cybercriminals are active throughout the world and are attempting to undermine their rivals, such as those acting on behalf of the Russia to target Ukraine. Multiple Reasons: I think this one is a bit of a cop-out, but honesty many cybercriminals can have multiple reasons for why they commit their crimes. Perhaps they started out for financial reasons, but learned they have fun learning how to formulate phishing attacks or get a thrill from successfully gaining access to confidential information on a company's secure server. Entertainment: I find this very compelling, especially for younger people who are still teenagers or in their early twenties. Sometimes lightheartedly mocking people online can turn into harassment, or even cyberbullying. Swatting has become a common cyberattack against people, with the cybercriminals rejoicing when the police respond to a false shooting at their victim's home with pleasure. Revenge: Revenge can be a powerful

motivator for cybercriminals. Revenge porn especially is a recent phenomenon when the victims' private sexual activities get leaked online without their consent. However, I don't think this type of motive for cybercrime is nearly as prevalent as the others. Boredom: I think this is also a less prevalent motivation for cybercriminals. Yes, people are curious about the world, and they probably do commit crimes out of boredom, but this is a short-lived form of motivation. Cyberbullying is committed out of boredom, but they are often committed more so for the entertainment value. Recognition: I don't find this motivation to be very common outside of black hat circles and very niche groups of online cybercriminals. Most cybercriminals want to remain anonymous, and don't want any attention, adoration or admiration from their peers.

Practically all scientific principles apply to digital forensics just as much as any other field of study, but here are three principles that should be followed when conducting forensic research. A serious study of digital forensics requires a stance of objectivity to rely solely on the facts and the data as they are observed, recorded, and analyzed. There may be multiple hypotheses for how to approach and solve a cybersecurity question/issue, but they all require an independent and objective look at the problem to find the correct solution. Furthermore, digital forensics and cybersecurity overall must also adhere to the principle of parsimony. While there may be multiple solutions found to answering a cybersecurity issue, the easiest to understand and simplest solutions possible should be adopted. Parsimony requires a digital forensics analyst to break down an issue to its most basic parts and in turn come up with as simple a solution as possible. This will maximize efficiency and make it so others can understand the solution and repeat the process. Finally, a third scientific principle that digital forensics investigator should adhere to is empiricism. Only serious discussions and research based on observable facts and data that are repeatable and observable to others should be used during their investigations. This will ensure that any future investigation is well informed and also based on factually correct studies.

Best practices for conducting digital forensics for a military operation can also vary, but there are several practices that carry over from one unit to another. Becoming as familiar as possible with the host nation's online cultural practices and habits can directly contribute to knowing how and where to look for stored data on a digital device. For example, certain social media platforms are more popular in some countries than others or aren't even in use in other countries. A forensic investigator who is familiar with the user interface, basic controls, and how to navigate through a social media profile in common use in a group of interest can save the rest of the team precious time and resources in piecing together relevant information from the rest of the device's memory. Keeping forensic investigators assigned to the same group or geographic region can help them to build up foundational knowledge on how the group operates, saves data, or communicates with the rest of these colleagues. This in turn will help the forensic investigator to notice patterns, trends, tactics, techniques, and procedures that are unique to the specific group or organization more efficiently and more quickly. Finally, sticking to standardized timelines and reporting formats provides much needed structure to an often fast paced and stressful environment.

Student: Kurt Williams
Instructor: Diwakar Yalpi
Course: 202410_CYSE201S_19043
Date: 11/24/2024

Popular culture often depicts digital forensics as something highly specialized where only a select few “master hackers” conduct black magic on a computer to break exotic forms of encryption and instantly connect random bits of data to uncover a criminal’s plans before they happen. While reality is far less dramatic and can sometimes be more mundane, digital forensics can still be highly impactful to investigations of all types and forms, particularly when the forensic team is supporting a military operation to capture insurgents overseas. For example, within the realm of human intelligence (HUMINT) collection is the requirement to conduct interrogations on captured enemy combatants of an adversary state or non-state actor. One key contributor to detainee interrogation operations is document exploitation (DOCEX), also known as document and media exploitation (DOMEX) (US Department of the Army, 2006). Another contributor is the exploitation of capture enemy equipment (CEE), also known as captured enemy material (CEM).

Per US Army field manual (FM) *2-22.3 Human Intelligence Collector Operations*, ‘‘DOCEX operations are the systematic extraction of information from open, closed, published, and electronic source documents. These documents may include documents or data inside electronic communications equipment, including computers, telephones, Personal Digital Assistants (PDAs), and Global Positioning System (GPS) terminals.” (US Department of the Army, 2006). One of the key differences between digital forensic analysis in support of military operations from law enforcement is the prioritization of analyzing what is of immediate tactical value to the military unit being supported. Furthermore, law enforcement often focuses on identifying criminals, safeguarding victims, and obtaining convictions for the cybercrimes committed. For military operations, this often means greatly reduced timelines (sometimes days and weeks, rather than months or even years for law enforcement) to translate, screen, categorize, and exploit the data from devices of interest. Not every bit of data will be completely scrutinized at the tactical level, but a properly prepared forensic team with the right amount of linguist support can conduct a thorough enough analysis to provide immediate results for the supported military unit. The key pieces of information needed to support tactical operations in a military campaign can include but are not limited to: Identifying key leaders and enablers of the adversary, such as commanders, financiers, and suppliers. Obtaining updated physical descriptions with distinguishing markings to include scars and tattoos or photographs if available. Frequently used bed down locations, weapons caches, and meeting locations of the adversary. Close associates such as subordinates, colleagues, and superiors must also be identified. The offensive and defensive capabilities of the adversary (both kinetic and non-kinetic). Identifying the primary and secondary forms or communication as well as forms of transportation will greatly help the supported unit when planning future operations. Finally, pattern of life information will help to better inform the unit when and where to focus their efforts to conduct future operations.

The size of a DOCEX team can change depending on the unit and operations supported, but the basic functions of the team should include supervision and administrative support, accountability, screening, security, translation, exploitation and

reporting, and quality and control. This paper shall focus on the exploitation and reporting functions. Per FM 22.3 exploitation and reporting "is the identification and extraction of information in response to collection requirements and requires a high level of expertise. The individual must be totally knowledgeable of collection requirements and must be able to readily identify indicators of activity or identify the significance of minute pieces of information that could contribute to answering requirements. Reporting involves placing that extracted information into a coherent, properly formatted report so that the all-source analyst can add it to the intelligence picture." (US Department of the Army, 2006). Furthermore, according to FM-22.3, "Information collected from documents is normally reported in a SALUTE (Size/who, Activity/what, Location/where, Unit/who, Time/when, Equipment/how) report or an IIR (Information Intelligence Report)." (US Department of the Army, 2006). A SAULTE report should provide the most fundamental information that could be used to capture the next target and should be completed as quickly as possible with frequent updates as the forensic analyst continues their exploitation. However, the SALUTE report should never be treated as the final result of a forensic examination and is only meant to answer immediate tactical objectives. Once the devices have been exploited for their immediate value, they can then be transported to a higher echelon facility with more resources and time available to them, where a more thorough IIR is usually created to provide the full extent of a forensic analysis.

Some examples of digital data worth reporting that could provide immediate tactical results include but are not limited to: GPS data and waypoints from the captured device can provide a geospatial footprint of the captured individual's whereabouts and known locations for the military unit to focus future collection efforts. Recent photographs of known associates and GPS tagged locations can provide an updated snapshot on key leaders or members of the captured individual's network and where they are known to operate. If the photographs of associates are up to date they can aid in the positive identification of other network members in future operations. Social media messaging applications which can provide a reliable timeline of the captured individual's recent activities and closest associates within their organization, and thus build a network analysis chart and pattern of life information.

From a temporal perspective, the trends and patterns derived from a digital forensics investigation could provide the investigator with greater information on how cyber actors have used different methods to conduct their attacks over time, what types of attacks are trending or waning in their use, and how long it takes for a new attack method to gain more prevalence in cyberspace until network defenses can be implemented. From a geospatial perspective, the locations of the victims' can help investigators to determine where in the United States cyber actors are directing their attacks and what kinds of victims they are targeting. This could help inform investigators about the areas with the most threats to their data integrity, as well as identify locations that have not experienced as many cyber attacks but may still be vulnerable due to a lack of experience in defending against these attacks.

Setting expectations early and properly training forensic investigators on the tools and techniques needed to perform will go a long way in ensuring their quality of work is

maintained to the proper standards. Another key difference to remember between digital forensics in support of military operations and US law enforcement agencies is in the legal limitations and requirements to conduct exploitation of digital evidence. Adversaries and their digital devices captured during a declared war are not afforded the same 1st and 4th amendment protections as a US citizen who is under criminal investigation (US Department of Justice, 2014). For more information on normal military operations conducted during peacetime and in support of national defense, reference Title 10 of the US Code. For further information on the differences between activities conducted in a declared theater of war, reference Title 50 of the US Code.

References:

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition*. Academic Press.

US Department of the Army. (2006). *FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations*. Headquarters, Department of the Army. www.train.army.mil

US Department of Justice. *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*. (2008). www.ojp.usdoj.gov/nij

US Department of Justice. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. (2014). https://www.justice.gov/d9/criminal-ccips/legacy/2015/01/14/ssmanual2009_002.pdf