**Questions:**

1. What does the term “hacker” mean to you? Was it in line with the view/origin from the documentary? Did your view of the word “hacker” changed after watching the documentary? – **Hacker means to me in many different ways. When I was younger I usually saw them through the perspective of movies and how the news portrayed them. The more I learn about them, the more I support which are usually the white hats. Basically in their use of skills towards good. Many companies require them for their skills and they are very advanced in what they do and how fast they are. There will always be mixed connotation of hackers.**

-  **the documentary defines hackers as one who applies ingenuity to apply and create a clever result. After watching the documentary, my view did not change of how I saw and felt about hackers. In the end I still think and agree that they are very clever with their skills.**

1. What are the differences between a black/grey/white hats? – **The black hat is classified as the ones who fall under what media usually portrays them as. They violate computer security for such personal gain and are criminals for stealing personal information such as credit card accounts. Secondly, the grey hat is in between a white and black and fall under the intention of those who don’t work for their own personal gain or the cause damages. It is hard to fully realize and know what a grey hat hacker would do based on their thoughts. White hat is the opposite of black hat and are considered ethical in their pursuit. They use their abilities for the good.**
2. Do you feel it is okay to find vulnerabilities, exploit them, and then report them to the victim? How should people best handle finding issues with systems? – **There is always a reason as to why flaw occur and it just shows that there is always room for improvement. There is nothing wrong in the sense of finding vulnerabilities. Although, I don’t truly agree with them being exploited, but should be reported back to the victim. People should handle thins more of a constructive criticism and not as a slap in the face. When systems are hacked or broken into just means for better ways to improve and become stronger.**
3. Which country do you fear the most in a cyberwar and explain why? What do you think the US should do to defend themselves from an attack? -  **I would believe either China or Russia to fear the most in a cyber war. They both very large countries with a lot of money, tech and people. Although, there are so many countries capable of holding a cyberwar to the u.s. but just because of prior issues with these countries and their power to do so is why I fear them. To further protect and defend ourselves from such attacks would be to really utilize and help out hackers within our country to create a strong set of team. All we can really utilize is to be prepared and support hackers within our country.**
4. Who is Dmitry Sklyarov? What is he known for? Is what he did right/wrong? What is his situation now? – **Sklyarov was known for a case that regarded the FBI and himself on July 2001. Sklyarov is a Russian programmer and was caught for unauthorized copying of adobe products and sold the software program Advanced ebook processor. In the case of Sklyarov who did all of this in Russia, where it was legal has no problem and would not see this to be a wrong thing to do. However, I do not think that what he did was right. As a hacker I believe that if he was doing this to an American company, I would think he should have known better than to come onto American soil for Defcon. As of now he is not really brought to much attention besides his charges were dropped that same year and was allowed to return back to his country.**
5. Who is Adrian Lamo? What is he known for? Is what he did right/wrong? What is his situation now? – **Adrian Lamo is a Columbian American hacker who later became a threat analyst. He was like any other hacker before hitting the media for breaking into several large high profile companies including Microsoft. He was largely known for wikileaks regarding a US Army authority leaking footage of a collateral murder video. He got in between and turned the conversation and files over to the government. Based on his action, I firmly believe that he did the right thing to avoid harm to this country and the people of this country. As of now Adrian lamo is considered a “ex” hacker and recently have been having trouble with his health. He was institutionalized on 7/29/11 at a California mental institute for aspergers.**
6. “If I get a job, it will not be security-related. I have no intention of letting them whore out my talents at their command.” Do you agree with this statement? Research Desmond Morris: Biology of Art. What is you impression on the work that was done with the book? – **I don’t necessarily agree with the statement however, I can see where they’re coming from.**
7. What is ICANN? How do you feel about the organization? -  **ICANN is the Internet Corporation for Assigned Names and Numbers. They are a private non-profit corporation that manages the internet protocol numbers and root name serves. This allows for a stable internet and based off the help of the community.**
8. Use Google and try to find as much information you can about Midnight Maze. -  **Also referred to as “ Moonlight maze”. This is an FBi examination into a cyber attack. This is a code name for infiltration into the American defense institutions such as the Pentagon. During this important time, cyber attack happened and hackers were able to access thousands of American maps of military institutions and blueprints of important hardware.**
9. Research SCADA? Do you see any news about issues with these systems? -  **SCADA system is a short word for Supervisory control and data acquisition. The system allows for a remote monitor and control with coded signals over communication channels. SCADA has the power of controlling may industrial processes such as power generation as well as infrastructure which varies from water treatment to waste collection. These controls can be physically done through the control of a human machine interface and also a centralized system which monitors.**