PART 1 ==> Watch the five current events videos posted in the discussion this week. These are no more than 3 minutes each.  
Share a one to two sentence summary of what each video was about.  You will have a summary FOR EACH VIDEO (2 points each, 10 points)

**Video 1:**

MGM an American company faced a major cyber security attack, where their customers could not use their services like hold card and casinos slots machines. It was a ransomware attack launched by the group shattered spiders. It was a vishing attack the hacker used reconnaissance to find employee and system detail. The link was sent to the user via SMS. The attacker used either of the two approaches for this attack:

1: called IT helpdesk and fold them to have their password reset.

2. pretended to be the IT team and approached a user with privileged account and ask them for their credentials.

Even though we have so many practices for cyber security humans still act as the weakest link in the chain. MGM system was down for days. And the hackers were able to steal SSN, bank info of the customers. This could be stopped by training and awareness for employees, proper incidence response etc.

Computer forensics was used to assess the damage caused by the attack.

**VIDEO 2:**

USDOD leaked the details of the Airbus employees’ details on 22nd Anniversary of 9/11 attack. USDOD also threatened the US contractors with sending them message that “I’m Coming”. Last time they leaked around 80,000 FBI members contact on online forum in 20e0 dec. The reason behind this attack was that an employee at Turkish airline downloaded a pirated framework. Which led attacker to install the red line Info Stealer. The Turkish airline has 3rd party access to Airbus which led to leak their employee data. The network forensics was used to took investigation that how malware entered the system, finding all the intrusion and method of how attacker transferred the data, these all were done through network forensics.

**VIDEO 3:**

Kenya Faced a cyber-attack on its financial transactions’ platforms. This was a DDOS attack which blocked customers from using banking apps, money services etc. this was going for 3 days. A group known as Sudan anonymous was behind this attack. The main reason was not to steal the data, but the main reason was to damage the Kenyan economy because they thought Kenyan government is interfering in Sudan politics. By attacking M-PESA the economy of Kenya affected very much. M-PESA is like a bank and their everyday transactions are around $569 million. The government didn’t catch any of the Sudan anonymous member yet but trying to increase and improve their security. Since this was DDOS attack so network forensics was involved in this. There was too much traffic that server was down.

PART 2 ==>   
Choose one post and answer the following questions in a word document (You cannot choose your own article):

1. Whose video are you responding to? (1 point)

-> I am responding to Hope Ndalima Video.

2. What is the headline / source for the video you are responding to? (1 point)

-> The headline of the video is “Cyber-attack in Kenya impacts online Government Platforms”.

3. What key concepts were shared by the presenter about that source/case/investigation? (3 points)

-> Kenya Faced a cyber-attack on its financial transactions’ platforms. This was a DDOS attack which blocked customers from using banking apps, money services etc. this was going for 3 days. A group known as Sudan anonymous was behind this attack. The main reason was not to steal the data, but the main reason was to damage the Kenyan economy because they thought Kenyan government is interfering in Sudan politics. By attacking M-PESA the economy of Kenya affected very much. M-PESA is like a bank and their everyday transactions are around $569 million. The government didn’t catch any of the Sudan anonymous member yet but trying to increase and improve their security. Since this was DDOS attack so network forensics was involved in this. There was too much traffic that server was down.

4. Find the same topic or event from a different source.  DOCUMENT YOUR SOURCE.   
    What significant points are raised in your source that are not mentioned in the video you are responding to?  
    -> I came up with some information which was not mentioned by the presenter that, the attackers attack the Kenya’s e-citizen portal, which is used by every person to access around 5,000 government services. This attack was not just on the government by some private entities were also affected by this attack. The services like passport application, visa issuing, driving license and many more.

Source: https://www.bbc.com/news/world-africa-66337573

5. Do you agree with the video author's opinion on the use of Computer Forensics? (Media/Network ... was it handled properly?)  Why or why not? (2 points)

-> Yes, the author opinion on the use of computer forensics was correct because this was a DoS attack which means that network forensics played vital role for detecting it, but still the companies are still figuring out who did the attack and how they did.