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:

23andme is a system that connects you to people with the same DNA. A hacker named Golem claims that he has millions of genetic profile information. He specifically targeted people from Germany and the UK. 23andme also confirmed this incident. The hacker golem confirms that he has 4 million 23andme profiles, which have emails, photos, DOB, and DNA information. The company says that there are a limited number of accounts that were breached. All information was available for sale on a forum with their prices with them. The hackers say he also has many celebrities' information. The hacker used a credential-stuffing method to hack all this information. The credential-stuffing works when the hacker uses weak credentials or stolen credentials of different users in different sites and login portals. Network forensics was used in this incident by tracking the hackers and also tracking the data that was transferred to the hacker's location.

VIDEO 2:

The Ukrainian Cyber Alliance (UCA) is an alliance of individual hackers and hacker groups that was established in 2016 with the main goal of taking down companies and individuals that back Russia's war against Ukraine. UCA stated in October 2023 that it performed many hacking efforts that revealed Russian propaganda and actions. They were able to eliminate the Trigona ransomware hacker group by making use of a known weakness in the Confluence software that the group was using (CVE 2023-22-515). Through the use of this attack, UCA administrators were able to get access to Trigona's servers, map out the server infrastructure, take over the website, and steal different files, including source code, database records, and different crypto wallets. While the UCA said they would share the decryption keys if they were found, they did not confirm if they had found any in the seized material. The operation was a "grey hat" operation because it was conducted independently and without the support of any law enforcement agency. The identities of Trigona's members are unknown as per the information.

VIDEO 3:

In this case, Russian businessman Klyushin received a 9-year prison sentence for his involvement in hacking and insider trading activities. The M3 IT company, which claims to work for the Russian presidential administration, is owned by Klyushin. He is connected to the Russian leadership and is seen as powerful. It is also well known that Klyushin is good friends with Ermakov, whose US government is looking for possible involvement in the 2016 presidential election. As part of his illegal activities, Klyushin broke into the DFI and Financial Solutions networks and used malware to get employee login credentials. He then participated in insider trading, making investments in well-known firms, including HubSpot, Microsoft, Tesla, Roku, and others, using this insider knowledge. He reportedly invested about $9 million into these projects and made more than $94 million, with profits of more than $33 million between 2018 and 2020. Swiss authorities arrested Klyushin in the Alps in 2021 while he was out skiing. Later on, he was charged with conspiracy, wire fraud, securities fraud, and unauthorized computer access in Boston. Klyushin was hiding his activities behind a curtain of confidentiality by purchasing cryptocurrencies and using virtual private networks, foreign-based servers, and fake identities. Computer forensics was used in this case to examine malware and preserve data. In an attempt to find the hacker responsible for the crimes, network forensics was also used to track the IP addresses of devices connected to the network during the hacking attack.

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 Prakyath Janga current event.

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

The headline/source of the video I am responding to is a Russian businessman sentenced to 9 years for insider trading and hacking schemes.

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

In this case, Russian businessman Klyushin received a 9-year prison sentence for his involvement in hacking and insider trading activities. The M3 IT company, which claims to work for the Russian presidential administration, is owned by Klyushin. He is connected to the Russian leadership and is seen as powerful. It is also well known that Klyushin is good friends with Ermakov, for whom the US government is looking for possible involvement in the 2016 presidential election. As part of his illegal activities, Klyushin broke into the DFI and Financial Solutions networks and used malware to get employee login credentials. He then participated in insider trading, making investments in well-known firms, including HubSpot, Microsoft, Tesla, Roku, and others, using this insider knowledge. He reportedly invested about $9 million into these projects and made more than $94 million, with profits of more than $33 million between 2018 and 2020. Swiss authorities arrested Klyushin in the Alps in 2021 while he was out skiing. Later on, he was charged with conspiracy, wire fraud, securities fraud, and unauthorized computer access in Boston. Klyushin was hiding his activities behind a curtain of confidentiality by purchasing cryptocurrencies and using virtual private networks, foreign-based servers, and fake identities.

4. Find the same topic or event from a different source.  DOCUMENT YOUR SOURCE. (8 points)   
    What significant points are raised in your source that are not mentioned in the video you are responding to?

It states that Klyushin, Ermakov, and Rumiantcev were employed by M-13, an IT business that was operated from Moscow. That business has governmental and commercial clients' penetration testing and other services. More information about the hacking techniques performed by Klyushin and his co-conspirators, including the usage of proxy computer networks and malicious ways to hide their crimes. It also reveals that the two victims of Klyushin's cyberattack lost more than $8 million.

SOURCE: https://www.justice.gov/usao-ma/pr/russian-businessman-sentenced-nine-years-prison-93-million-hack-trade-conspiracy

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, Computer forensics was used in this case to examine malware and preserve data. In an attempt to find the hacker responsible for the crimes, network forensics was also used to track the IP addresses of devices connected to the network during the hacking attack.