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 no 1:

A Russian national, La Citrix, accidentally affected his own computer with his own malware. Ad sold his own data on the dark web and posted his own credentials and identity. An information security company found his own data, and the company Hudson Rock was able to identify him. Hudson Rock sources compromised credentials from the threat actor. Entered credentials into the database. Notified companies of compromised employee areas. While analyzing data, they found a credential dump from one machine with a record of almost 291 companies. When they further dug into the La Citrix machine, they found a software inventory. Then, HR turned in this entire data to law enforcement. This came out in July of this year. There is a lot of data on this attack out there. Also, there aren’t any updates on it yet.

Video no 3:

An account manager in India was scammed in India by six individuals for giving him an international part-time job; the mastermind behind all this fraud was operating from China.

The attackers were doing small tasks by the victims, like liking the videos, commenting, and watching videos, and paying them to gain trust. As time went on, they didn’t pay afterward. By reporting fraud, the police arrested the criminals in India and seized all their laptops, mobile phones, and data devices. Now, police are investigating this case to the next level, but the mastermind behind this group is in China or Dubai, which needs international cooperation to arrest them.

Network forensics and media forensics were involved in this case by investigating the logs and the devices that were seized by the criminals and getting the links to the mastermind and his links to China and Dubai.

Video No. 4:

There were fake investment scams all around the globe. The advertisement of these investments was done through Facebook. The advertisement was about investing in the top world 35 companies. The financial damage was about $280000 in 4 months.

By clicking on the link in a website, they redirect the user to a scam website where they fake stokes and make investments. The victim receives daily emails about his investments from that fake portal. Group IB started investigating this scam in June 2022. This group uses AI technology to find scam pages. This case usually uses computer forensics to find the logs and trace the origins of scams to identify the infrastructure of the scam. Group IB collected the evidence and blocked fraudulent investment websites.

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

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

I am responding to Robby Ballard's Video.

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

The headline of the video is “WHOOPS”.

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

The presenter shared how the company Hudson Rock was able to find La Citrix data and how they identified him and found stolen data from almost 300 different companies. HR also found lost credentials of employees of so many companies. Also, they entered the credential into databases and notified the companies of the affected employees. Also, La Citrix unintentionally affected his own computer and sold his information on the dark web. Now, here, karma comes in place, as mentioned by the presenter.

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?

One thing that wasn’t mentioned in the video, but I found on this website is that The la Citrix attack has been active on the Russian-speaking cybercrime forums since 2020. Offered access to the hacked companies. La Citrix has been observed hacking into organizations and compromising Citrix, VPN, and RDP servers to sell illicit access to them.

SOURCE: <https://www.securityweek.com/black-hat-hacker-exposes-real-identity-after-infecting-own-computer-with-malware/>

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

The author did not really give an opinion on the use case of computer forensics, but everything covered by him tells me that a lot of computer forensics was involved in the investigation done by the company Hudson Rock on this case. The investigative techniques applied by HR were related to computer forensics. They found the data. Put it into a database and found all the software and employee records through different techniques.