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

Video 1:

3 People use raspberry PI to steal money from ATMs. Most of the Crimes took place in West Texas and they stole around $5700 from 1 ATM so now imagine how much they stole in total.

They were caught by one of the witnesses during the robbery and he informed the police. Police raided the hotel where they were staying and seized some raspberry pi devices. They used raspberry PI to trigger the alarm system of the ATM, so no one could be if they are doing something with the ATM. This Case was related to Network forensics and computer forensics because the FBI search the cameras, raspberry PI devices, their mobile phones, text messages and all. Searching this evidence were reason of the forensics.

Video 2:

Genesis Market sold account access information, it already sold 1.5 million computers data. Malware installed on the infected computer continually steal the information. They got assistance from many departments and officers worldwide for the investigation, a lot of servers were seized and searched plus 119 were arrested and 208 locations were searched. Computer Forensics was used in this case because they had to check the computer logs and locations of the infected computers. The data and information’s collected from the affected were also examined through forensics.

Video 3:

16 shop was a platform which provide fully automated phishing scams to the users, specifically they provide the hacks, domain names, stolen credentials. They were basically subscription-based service. They sold around 70,000 hacks to different users. They usually send email which has links and pdf which redirect the user to website asking for personal information and credentials. This platform was closed by Interpol and other agencies and many people were arrested. Computer Forensics play vital role in identifying the phishing attacks by examining the emails, links, many different computers and servers.

Video 4:

Department of justice started the project save the childhood. It’s been expanded upon since “the protect our children” act came out. It was designed to get the public entities, various law enforcement entities and government to all work together to stop the sexual exploitation of children. “The protect the children act” helped expanded this effort in virtual space where their department of justice maintains a database and they search and filter by date and got articles that involve individuals and their acts involving a minor. Offender streaming is also part of the sexual crimes against children. This is where the offender sexually exploits the children and stream it live was a significant increase in the amount of crime against children and criminal activities happening because of the internet to other offenders that are paying to watch. There is federal case regarding this: The US vs Sarah the main focus is to raise awareness rather than talking about each case or issue in detail.

Video 5:

Ex-Employee of a software company who was working as a senior Engineer in company conducted cybercrime and ransomware. He used to sell the software outside the company which harms the company. He was caught by FBI due to his own mistake by not turning the VPN and all evidence were against him when FBI start the investigation. This case was related to computer Forensics because FBI collected the data and looked into the computers and logs. Also examined the evidence which were against the Ex-Employee.

PART 2 ==>

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

I am responding to 1st video of YASHWANTH REDDY MARIPEDDI

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

The Headline for the video I am responding to is **GANG USES RASPBERRY PI TO STEAL THE MONEY** and Source is <https://www.tripwire.com/state-of-security/thousands-dollars-stolen-texas-atms-using-raspberry-pi>

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

The key concept shared by the presenter about the case was that there were 3-member gang who uses Raspberry PI to steal money from ATM specially from West Texas. The main function of Raspberry PI device was that it triggers the security of the ATM and don’t let the anyone know that there is something wrong with the ATM or someone is messing with the ATM. They were caught during one of their robberies when someone just noticed that there is group of people doing something wrong with the ATM and notify the police. The Police identified the group and went to the hotel where they were living. Police searched their room and seized some of the raspberry PI devices and other devices. This case was related to Computer Forensics because the evidence was in the CCTV cameras, and the Raspberry PI devices itself were evidence so examining these devices are part of forensics. After that the text messages and phone call examine are also forensics and examining the mobiles phones. Network forensics are also involved in this case.

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?  
    READ THE OTHER REPLIES THAT HAVE BEEN MADE TO THIS VIDEO ...   
    if someone else has already used the same source and made the same point, please either choose a different video, a different source, or make sure you are making a NEW point from that source.

Source: <https://www.howtogeek.com/devops/how-hackers-are-using-raspberry-pi-to-hack-atms/>

The significant points I read in my source and was not mentioned in the video of the presenter was that most of the ATM uses old OS like window XP or Window 7 still now which has a lot of vulnerabilities which are known by many cybercriminals and attackers. There are many malwares in the market which compromises the ATM very easily. You have to just install the Malware in the ATM and the ATM is yours lol. In every ATM there is USB port which only accept keyboard or Mouse of the servicemen who come for the maintenance of the ATM. You have to load your Raspberry PI with the Malware so that when you plug into the USB port so ATM can Identify your Raspberry PI as a mouse or keyboard so it could run on it. The Malware is written in such a way that ATM get convinced that Raspberry PI is a keyboard or mouse. And Raspberry PI just start its work and ATM allow every thing attacker wants to do. And ATM start spitting the bills for the attacker.

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, I agree with the presenter opinion on the use of Computer Forensics because in this case all the evidence were In the Computer and Raspberry PI. Plus, you also have to check the CCTV camera and the mobile phones of the attackers for getting more evidence against them. Also network Forensics is also include in it.