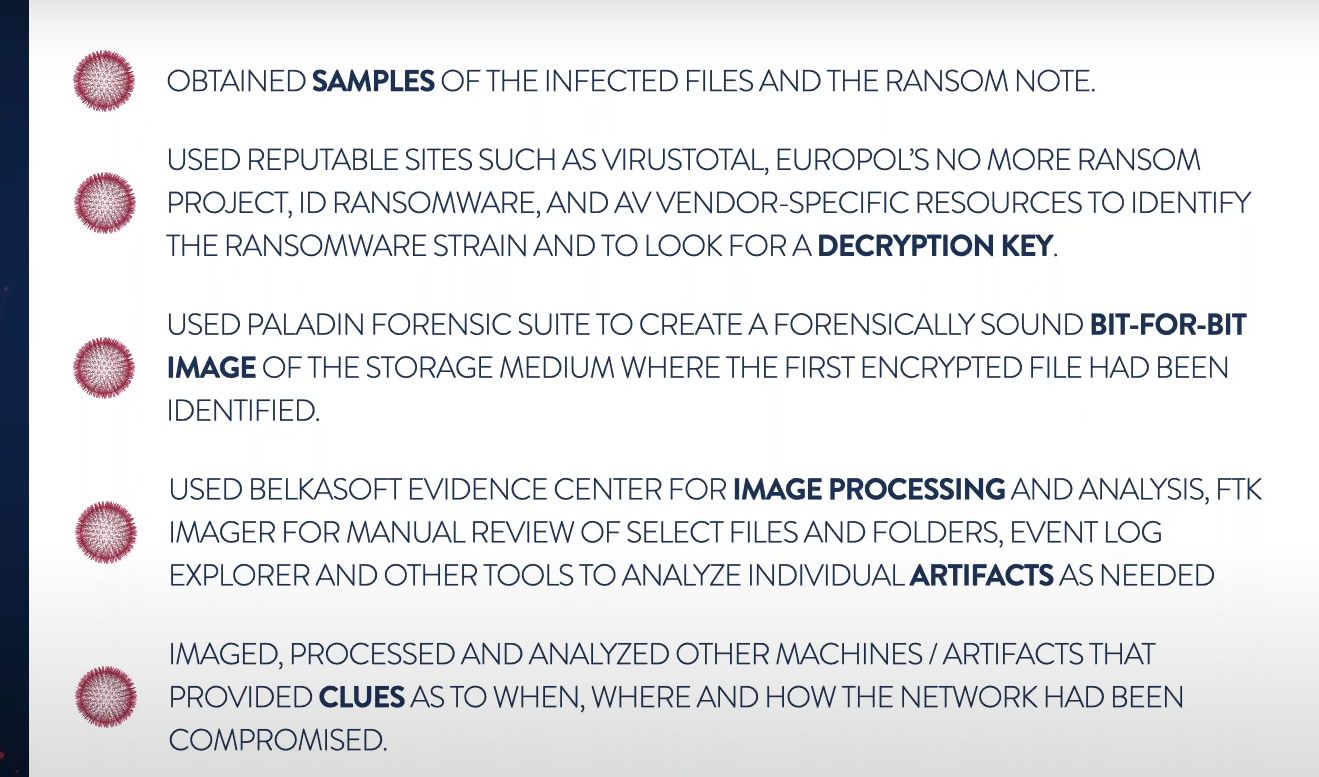
Question: (it's about an hour and 15 minutes) before class, as it may make more sense to see the process than to simply read it. What are 5 key "take-aways" that you discovered from the video? How does this vary from the book data acquisition process? What are 5 key "take-aways" that you discovered from the book? After reading the book or watching the video does this change your mind about working in the forensics field? How has work and preparation in the Computer Science field or Information Technology field prepared you for your career field? Explain.

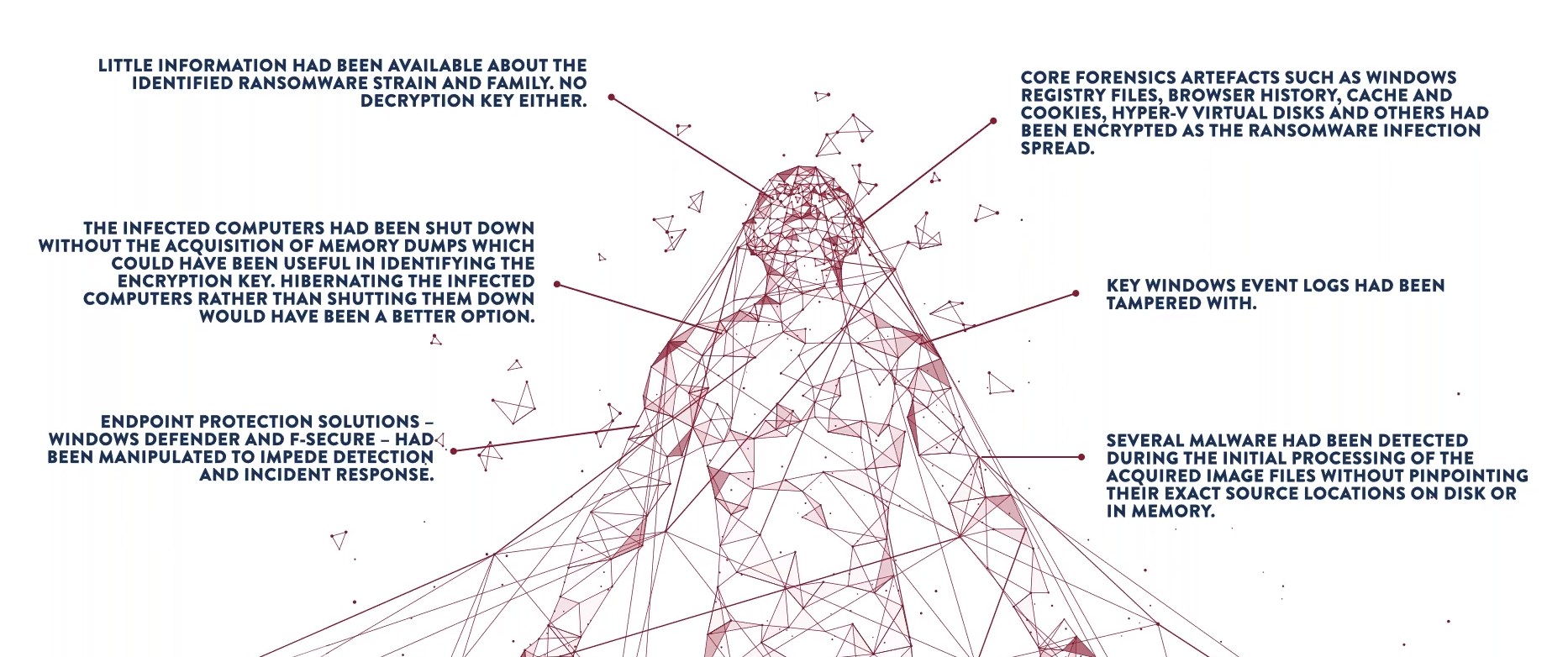
Answer:

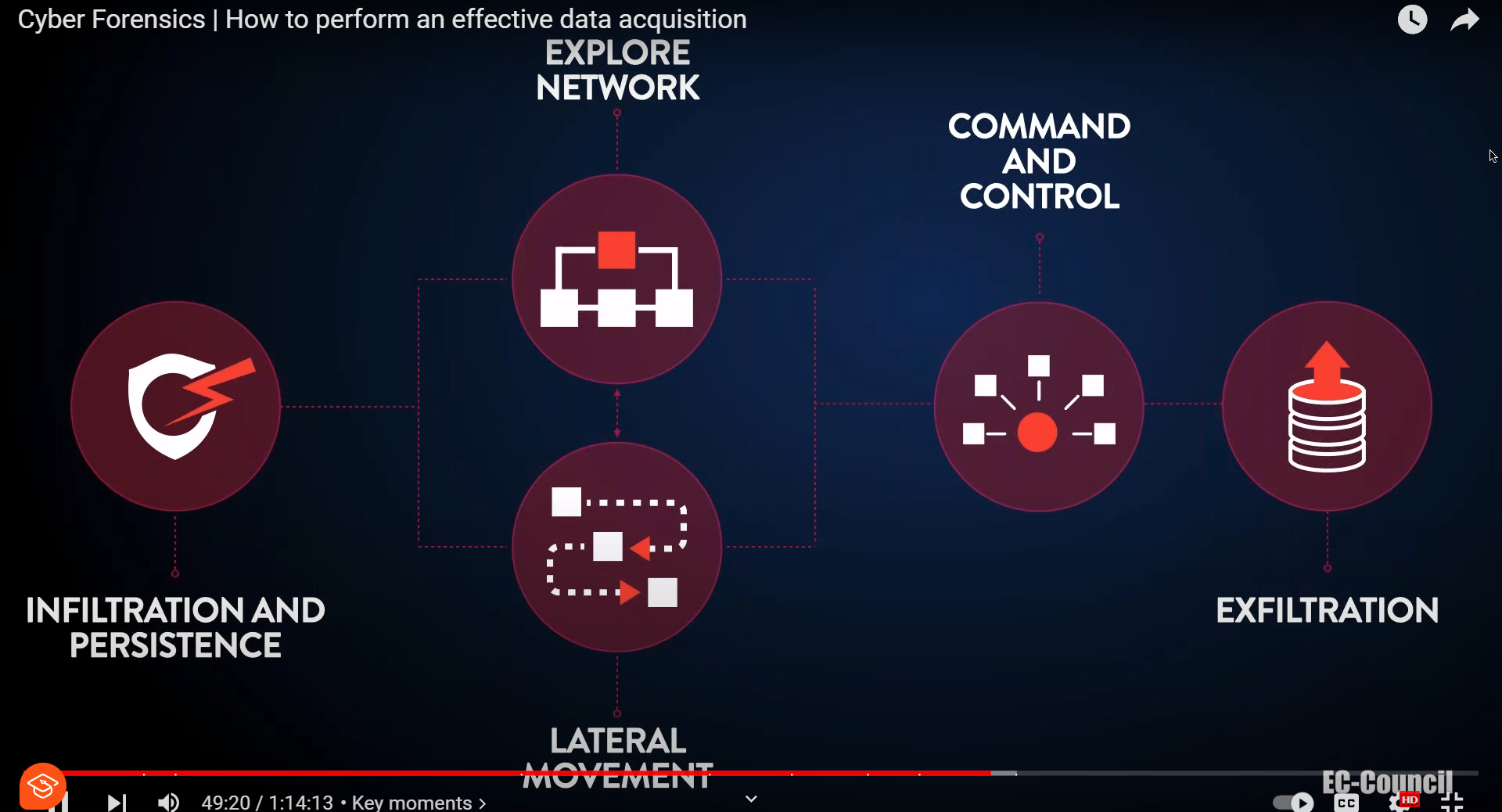
5 key take-aways from the video are as follow:

* Compression of forensics in real life and from movie’s/ series
* Top 5 Forensic cases: Cheating wife, kidnapping, serial killer, Pedophile, Suitcase killer
* Code spaces – 17th June 2014 – Ddos attack – Hotmail- asking money- how they got back access- lose partial/full resources of data and backup
* Digital evidence
* The doll woman
* Paladin forensic suite – F-Response, Belkasoft, Cellebrite
* Faraday bag
* Analyzing the ransomware attack on a company who’s working remotely due to covid:



* Forensics challenges:





My Answer:

1.The 5-take-aways from the video are as follows:

* Compression of forensics in real life and from movie’s/ series
* Top 5 Forensic cases: Cheating wife, kidnapping, serial killer, Pedophile, Suitcase killer
* DDos attack at Code spaces on 17th June 2014
* The doll woman case
* Analyzing the ransomware attack on a company who’s working remotely due to covid.

The article by Miller on Forensics in reality v/s movies (Miller, 2020). It is a broad field that encompasses many different specialized disciplines. The scientists work to collect, analyze, and interpret evidence to help solve crimes. This work is often portrayed in a glamorous and fast-paced way on television/movies, but in reality It is much more complex and time-consuming process. It is always a team effort. Evidence is collected by law enforcement officers and then processed by forensic scientists in specialized laboratories. Each type of evidence, such as DNA, fingerprints, and ballistics, is analyzed by a different team of experts. This process can take several weeks or even months, depending on the complexity of the case.

Some misconceptions from movies are as follows:

* They can always solve crimes.
* They can always get results quickly.
* They are always able to identify suspects.

But In reality, they all are wrong.

Take-aways from book are:

* Data acquisition is the first step in any digital forensics investigation.
* There are a variety of different data acquisition methods.
* There are a variety of different data acquisition tools available, each with its own strengths and weaknesses.
* It is important to maintain a chain of custody for all digital evidence.
* It is important to document the entire data acquisition process.

The book has more information and many different tools and techniques which aren’t mentioned in the video. After watching the video I became more interested about learning about forensics and knowing things we need to do for producing something as evidence to court requires one to explain how it obtained.

Reference:

Miller.T.M. (2020). Reality vs. hollywood: forensic science. FleetScience center. <https://www.fleetscience.org/blog/2020/09/reality-vs-hollywood-forensic-science>

2.

No, we will not be successful in gathering data always. It can be defined as the process of gathering and examining digital evidence to identify, preserve, and analyze data from digital devices. The success rate of data gathering depends on a number of factors, including the type of device, the condition of the device, the skill and experience of the forensic examiner, and the availability of appropriate tools and resources.

Familiarity with tools and technology can improve your ability to gather digital forensics data. Forensic examiners need to be familiar with a variety of tools and software, including tools for data acquisition, data analysis, and data reporting. They also need to be familiar with the latest trends and developments in digital technology. Certifications can improve your odds of success in digital forensics data gathering. The programs typically provide training on the use of specific tools and software. This training can help you to become more proficient in using the tools and software, and it can also help you to understand the capabilities and limitations of the tools and software’s. The article by Petree also states that having knowledge on tools and preparing in advance can increase the success rate of gathering data (Petree,2023).

There are a number of things that I can do to improve my success rates in gathering data, including:

Continue to learn and develop my skills: The field of digital forensics is constantly evolving, so it is important for forensic investigators to continue to learn and develop their skills. This can be done through formal training programs, self-study, and attending conferences and workshops.

Network with other forensic investigators: Networking with other forensic investigators is a great way to learn about new tools and techniques, and to get advice from experienced professionals.

Stay up-to-date on the latest legal developments: Forensic investigators need to be aware of the latest legal developments in order to ensure that they are complying with all applicable laws and regulations.

Have a plan: Before starting any digital forensics investigation, it is important to have a plan. This plan should identify the specific goals of the investigation, the evidence that needs to be collected, and the tools and techniques that will be used.

Petree.S. (2023). Digital forensics: Leverage insight for faster recovery. <https://www.plantemoran.com/explore-our-thinking/insight/2023/07/digital-forensics-leverage-insight-for-faster-recovery>

Bindu:

5 key take-aways from the video are as follow:

* Compression between movies/reality.
* Digital evidence.
* Digital evidence can be found in a variety of devices.
* Paladin forensic suite – F-Response, Belkasoft, Cellebrite- different tools explained in the video.
* Case study of Ransomware attack.

5 key take-aways from the book are:

* Proper preparation is key.
* Use the right tools for the job.
* Maintain a chain of custody.
* Be careful not to modify the evidence.
* Digital evidence can be found in a variety of places, including computers, smartphones, tablets, and external storage devices.
* It is important to identify all potential sources of digital evidence before beginning the acquisition process.

The article by Garfinkel on Digital forensics (Garfinkel,2023) discusses the challenges of collecting and preserving evidence from digital devices. It is used to investigate both computer-related crimes and traditional crimes that leave electronic evidence. These evidence’s can be difficult to collect and analyze because it can be easily changed or deleted. Tools can be used to recover deleted files and other hidden data. He also provided number of examples of how digital forensics has been used to solve crimes. For example, digital forensics investigators were able to recover deleted files from the computer of a serial killer, which helped to convict him of his crimes.

Garfinkel.L.S. (2023). Digital forensics. Americanscientist.org. <https://www.americanscientist.org/article/digital-forensics>

1. Probably no in some cases. The article "Challenges Faced by Forensic Investigators" Sharma (Sharma, 2020), tells us that there are a number of challenges that can make it difficult to successfully gather data in digital forensics investigations. They are:
   * Data encryption.
   * Data deletion.
   * Data fragmentation.
   * Hidden data.
   * Device complexity.

Despite these challenges, there are a number of things that digital forensics investigators can do to improve their chances of successfully gathering data. These include:

* Using the right tools: Forensic investigators have access to a variety of tools that can help them to recover data from digital devices.
* Following best practices: There are a number of best practices that digital forensics investigators should follow when gathering data.
* Being familiar with the latest technologies: Digital technology is constantly evolving, and it is important for digital forensics investigators to stay up-to-date on the latest technologies and techniques.

Yes, familiarity with tools and technology is essential for digital forensics investigators. Investigators need to be able to use a variety of tools to extract data from different types of devices. And also certifications can improve the odds of success for digital forensics investigators. Additionally, certifications can demonstrate the potential employers that an investigator has the skills and knowledge necessary to perform the job.

Sharma.A. (2020). Let us explore challenges faced by forensic investigators. <https://www.mailxaminer.com/blog/challenges-faced-by-forensic-investigators/>

Frnd B:

5 key take-aways from the video are as follow:

* Digital evidence can be found in a variety of devices.
* It is important to identify all potential sources of digital evidence.
* The acquisition process should be tailored.
* Challenges faced by forensic investigators.
* It is important to use a variety of acquisition techniques.
* It is important to verify the integrity of the acquired evidence before using it in an investigation.

Take aways from the book:

* Data acquisition is the first step in any digital forensics investigation.
* Different data acquisition methods.
* Different tools.
* Need to identify all potential sources of digital evidence.
* Validating the evidence.

There are a number of different methods that to acquire data from digital devices in forensics investigations (EC-Council, 2022). These methods include:

* Logical acquisition: It is the process of copying the data from a digital device without making any changes to the device itself.
* Physical acquisition: It is the process of creating a bit-for-bit copy of a digital device's hard drive. This is done by removing the hard drive from the device and connecting it to a forensic imaging tool.
* Live acquisition: It is the process of copying data from a digital device that is still in use
* Boot acquisition: It is the process of copying data from a digital device before the operating system has loaded.
* File-level acquisition: It is the process of copying specific files from a digital device.
* Sparse acquisition: There are five steps in a digital forensics investigation, the first two of which are the most critical during data acquisition (EC-Council, 2022):
  + Identification
  + Preservation
  + Analysis
  + Documentation
  + Presentation

Reference:

EC-Council. (2022). How to handle data acquisition in digital forensics. <https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/data-acquisition-digital-forensics/>

No, I will not always be able to successfully gather data. There are a number of reasons for this, including:

* Technical challenges: Digital evidence can be stored on a wide variety of devices, including computers, smartphones, tablets, and cloud storage services.
* Legal challenges: Forensic investigators must comply with all applicable laws and regulations when gathering and analyzing digital evidence.
* Resource challenges: Digital forensics can be a time-consuming and expensive process. Investigators may need specialized training and equipment

There are a number of things that I can do to improve my chances of successfully gathering data, including:

* Stay up-to-date on the latest technologies and trends
* Use the right tools and techniques.
* Follow best practices.

Yes, familiarity with tools and technology improves my ability to gather data. Forensic investigators need to have a good understanding of the tools and techniques that they are using in order to effectively collect and analyze digital evidence.

Certifications can improve my odds of successfully gathering data. Certification programs typically require candidates to demonstrate their knowledge and skills in using the tools. This can help to ensure that forensic investigators are using the tools and techniques correctly and effectively. Forensic investigators also need to have a good understanding of the underlying principles of digital forensics, as well as experience in conducting digital forensics investigations.

Reference:

W.Chirath De Alwis. (2017). An introduction to challenges in digital forensics. <https://www.forensicfocus.com/articles/an-introduction-to-challenges-in-digital-forensics/>