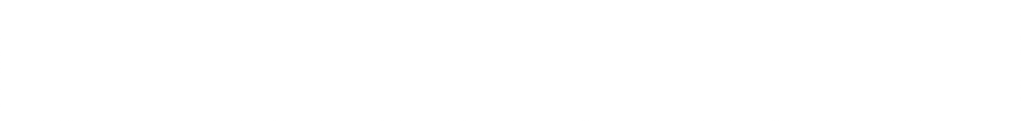


**QUESTION 1 OF 78**

**DLMCSECSNF01\_E\_Offen\_leicht/Lektion 01**



Name and explain three components that can be attached internally to the motherboard.

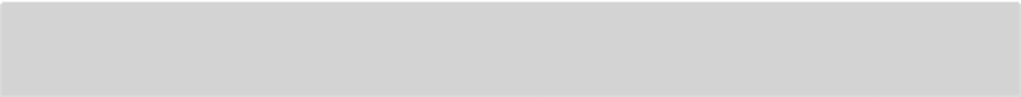
CPU - central processing unit (CPU), is the electronic circuitry that executes instructions comprising a computer program.

RAM - Random-access memory is a form of computer memory that can be read and changed in any order.

Video Card or Graphics card - A graphics (video) card (display adapter) is an expansion card which generates a feed of output images to a display device.

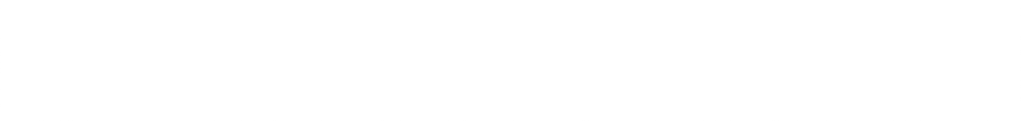
Sound Card or Audio Card - A sound (audio) card provides input and output of audio signals to and from a computer.

# (2 pts each, only 3 components + explanations needed)



**QUESTION 2 OF 78**

**DLMCSECSNF01\_E\_Offen\_leicht/Lektion 01**



Name and explain the two interfaces used by a user to interact with the operating system.

Graphical user interface (GUI) - The graphical user interface is a form of user interface that allows users to interact with electronic devices through graphical icons. The actions in a GUI are usually performed through direct manipulation of the graphical elements.

Command-line interface (CLI) - A command-line interface processes commands to a computer program in the form of lines of text. The program which handles the interface is called a command- line interpreter or command-line processor.

# (3pts each)



Name three different methods the operating system may use to communicate with the I/O device.

Programmed I/O–in this method, when the processes are executed and have an I/O instruction, the processor will then issue the command to the device controller. **(2 pts)**

Interrupt driven I/O – instead of waiting for the “status of operation” to be completed; an interrupt schema is used. **(2 pts)**

I/O using DMA – when the processor needs to access a large data set, the interrupt-driven method is inefficient. Direct Memory Access (DMA) completes the operation without processor intervention. **(2 pts)**

Port-mapped I/O (PMIO) - Will use a particular class of processor instructions (IN and OUT) that have been designed specifically for handling I/O devices. **(2 pts)**

Memory Mapped I/O – like port mapping, the same address space will address the I/O device and system memory. **(2 pts)**

Channel I/O – is used in mainframe computers and is considered to be a high-performance architecture. **(2 pts)**

# (Any combination of three answers, max. 6 pts.)



Name and explain three artifacts you may find when performing forensic analysis of RAM.

CLI commands – text representation of the commands issued in a command line interface (CLI). Encryption keys – Keys used to create encrypted containers.

Unencrypted data – Data that was present on the system, but may/may not be found on non- volatile storage.

IP addresses - An Internet Protocol address (IP address) is a numerical label such as 192.0.2.1 that is connected to a computer network that uses the Internet Protocol for communication.

Internet history (Browser history) - Internet history is a term for a tool or resource in a Web browser that keeps track of sites and pages that a user visits. Through tabulating URLs, Internet history facilitates a quick reference or lookup of previously visited pages.

Malware - software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

# (2pts each, 3 artifacts + explanations sufficient)



**QUESTION 5 OF 78**

**DLMCSECSNF01\_E\_Offen\_schwer\_F1/Lektion 01**



You have responded to the incident scene and your supervisor has told you you need to create a forensic image of desktops and laptops. Your supervisor further relates that it is important to capture the data stored in RAM, but the passwords needed to unlock the systems are not available.

Name and explain to the supervisor what other options are available that may contain similar data to what is stored in RAM.

Hibernation file - hiberfill.sys Hibernation mode occurs the system is being powered down. In Windows, the RAM is compressed and stored in the hiberfill.sys file.

Swap file - swapfile.sys With the release of Microsoft Windows 8, Microsoft introduced the swapfile.sys file. It is very similar to the page file but has some differences. Microsoft created the swap file for use for paging operations with suspended Metro/Modern Windows applications.

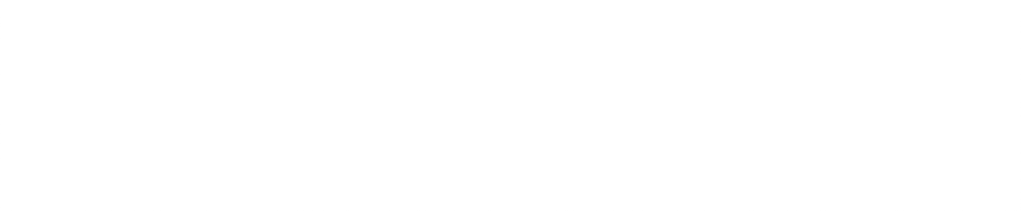
Pagefile - pagefile.sys Paging is a method of storing and retrieving the data in RAM with a "virtual memory file" on a traditional storage device.

# (3pts for each name) ( 3pts for each explanation)



**QUESTION 6 OF 78**

**DLMCSECSNF01\_E\_Offen\_schwer\_F1/Lektion 01**



Your colleague is responsible for creating forensic images of the solid-state drives (SSD) in an ongoing investigation. When the colleague attempts to verify the forensic images to the source device the hash values do not match.

Name and explain to the colleague the operations controlled by the SSD’s firmware that may cause the verification to fail.

**Wear leveling**–moves data around the chip(s) to ensure the system uses all the chips at the same rate.

**Trim**–This commands wipes (overwrites) the unallocated space of the device.

**Garbage collection**–This function scans the memory modules to identify the deleted data blocks in the pages of the device. This will cause the system to move allocated data to new blocks. After the data is transferred, the system will overwrite (wipe) the now unused data blocks.

# (3pts for each name) ( 3pts for each explanation)



Name and explain the two different process management models.

Two-state process management model – This is the simplest model is because a process is either being executed by a processor or it is not. Thus, a process may be in one of two states, RUNNING or NOT RUNNING.

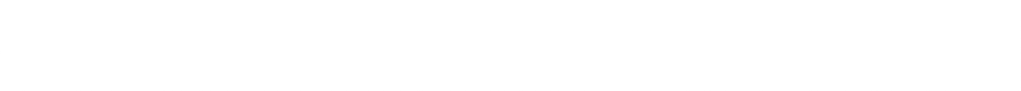
Three-state process management model - The three-state process management model is designed to overcome a problem in the two-state process model, by introducing a new state called the BLOCKED state. The three states in this model are RUNNING- The process that is currently being executed, READY- A process that is queuing and prepared to execute when given the opportunity and BLOCKED- A process that cannot execute until some event occurs, such as the completion of an I/O operation.

# (3pts each)



**QUESTION 8 OF 78**

**DLMCSECSNF01\_E\_Offen\_leicht/Lektion 01**



Name three of the seven process states.

New, Ready, Waiting, Executing, Terminated, Blocked, Suspended **(2pts each)**



Name and explain a nested/hybrid RAID 10. Name the benefits of the nested/hybrid RAID 10 storage scheme. Identify the minimum number of disks needed to implement a RAID 10.

The nested RAID combines the typical RAID schemes to gain additional performance, redundancy, or both.

The naming convention for the nested RAIDs is a combination of the conventional RAID system numbers. For example, RAID 10 is a combination of RAID 1 and RAID 0. RAID 10 is a stripe with a mirror.

You will need at a minimum of four discs to implement a RAID 10.

# (2 pts each)



**QUESTION 10 OF 78**

**DLMCSECSNF01\_E\_Offen\_mittel/Lektion 01**



Name three benefits of using a SSD.

a lighter device, reliability, greater speed for read/writes, longer battery life **(2pts each)**



Your supervisor hands you a hard drive and tells you it is formatted with a master boot record (MBR). You are instructed to examine the hard drive and confirm the partitioning scheme, identify the partition types and any hidden areas that may exist on the device. Name the artifact you would use to confirm the device is partitioned with a MBR. Name and explain the partition types and hidden areas that may be found on the device.

Primary Partition **(3pts)** - The Master Boot Record (MBR) partitioning scheme restricts the device to four primary partitions. **(3 pts)**

Extended Primary Partition **(2 pts)** – The system will take one (and only one) of the primary partitions, and create additional logical partitions **(2 pts)**

Host Protected Area (HPA) **(2 pts)** - The HPA is used by the manufacturer to store recovery and diagnostics tools and cannot be changed or accessed by the user. **(2 pts)**

Device Configuration Overlays (DCO) **(2 pts)** – The DCO is an overlay that allows the manufacturer to use standard parts to build different products. It allows for the creation of a standard set of sectors on a component to achieve uniformity. **(2 pts)**



Your supervisor is complaining about data loss after a hard drive has crashed. The supervisor asks you if you know of any storage options that allow protection from defective hardware or hard drive disk errors.

Name and explain a storage option that meets those criteria.

Name and explain the options that can be deployed using that storage option.

RAID (Redundant Array of Independent Disks or Redundant Array of Inexpensive Disks). A raid is a method of storage that uses more than one disk **(1 pt for name 1 pt for explanation)**

RAID 0 is known as a striped set. The data stored in a RAID 0 configuration is segmented into blocks and written across the drives in the set. This method allows for greater I/O (reads/writes) because of the concurrent use of two or more disks. It will further enhance performance with the use of multiple disk controllers **(2pts for name 2pts for explanation)**

RAID 1 is known as a mirror using two or more hard disks. The dataset is placed on one drive, and it puts an exact duplicate on the second drive. This RAID scheme also does not use parity. Using RAID 1 achieves redundancy at a reduced performance rate. **(2pts for name 2pts for explanation)**

RAID 5 requires a minimum of 3 drives. The dataset is striped across the drives in the array using blocks of data. A parity checksum of the data blocks is also written across the drives. **(2pts for name 2pts for explanation)**

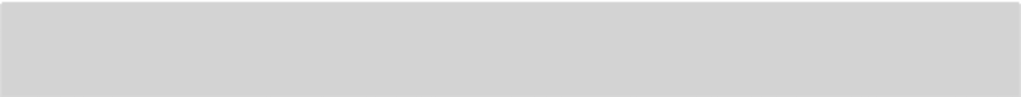
Nested or hybrid RAID. The nested RAID combines the typical RAID schemes to gain additional performance, redundancy, or both. The naming convention for the nested RAIDs is a combination of the conventional RAID system numbers. For example, RAID 10 is a combination of RAID 1 and RAID 0. **(2pts for name 2pts for explanation)**



Name three categories of system calls.

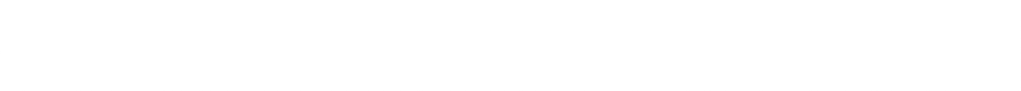
Process control File management

Device management Information maintenance Inter-process communication **(2 pts each)**



**QUESTION 14 OF 78**

**DLMCSECSNF01\_E\_Offen\_leicht/Lektion 02**

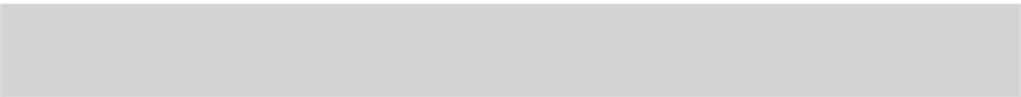


Explain the term thread.

A thread is a subset of a process and can be found within the same address space. The threads will run parallel with the process.

Threads can be created and terminated much faster than if a whole process had to be created.

# (2 pts for each sentence)



**QUESTION 15 OF 78**

**DLMCSECSNF01\_E\_Offen\_mittel/Lektion 02**



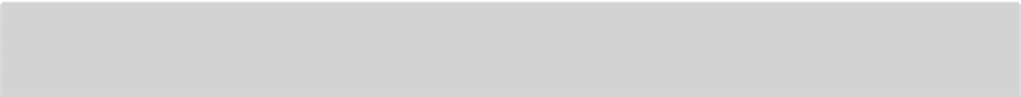
Name three supporting files for HKEY\_CURRENT\_CONFIG.

System, System.alt, System.log, System.sav **(2pts each)**



Name three Registry Hives that are in the HKEY\_LOCAL\_MACHINE.

SAM, System, Software and Security **(2pts each)**



**QUESTION 17 OF 78**

**DLMCSECSNF01\_E\_Offen\_schwer\_F1/Lektion 02**



Your supervisor advises that you are now the primary examiner for an investigation into a Microsoft Windows based system. The supervisor is interested in how to determine which user accounts were created by a user and which accounts were created by the system.

How would you identify which accounts were user created and which accounts were system created?

Name and explain the artifact(s) you would use to identify the different accounts. Name and explain how you identify the Guest account.

A SID is the security identifier used by the Windows operating system to identify objects.**(3pts)** The last three/four digits of the SID are the RID. **(3pts)**

Each user account will receive a RID. **(3 pts)**

A system created account would have a RID under 1001, such as the default administrator account would have a RID of 500. **(3pts)**

A guest account would have a RID of 501. **(3pts)**

A user created account will have a RID equal to or greater then 1001.**(3pts)**



**QUESTION 18 OF 78**

**DLMCSECSNF01\_E\_Offen\_schwer\_F2/Lektion 06**



Identify the phases of the Intelligence Cycle and explain the purpose of each phase.

Direction - This step sets in motion the intelligence cycle; it provides the purpose and the question that needs to be answered. **(3pts)**

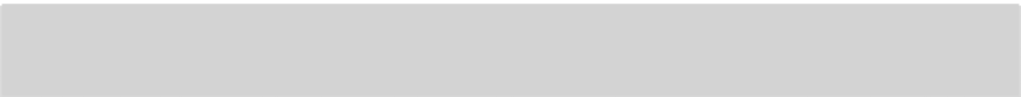
Collection - Collect as many data points (information) as possible. You will also want to gather information from multiple sources that will corroborate other data points. **(3pts)**

Processing - The information that has been collected has not been placed into context. There are bits and pieces of information that have been compiled from a variety of sources that may need to be put into a standard format so that it can be searched and analyzed. **(3pts)**

Analysis - Is used to answer the question that started off the intelligence cycle.**(3pts)**

Dissemination – The process has created intelligence by analyzing the information and providing the correct answer. If you do not disseminate the results of the process to the appropriate audience, then the cycle has failed. The intelligence that has been generated must be disseminated to the relevant audience so that they may act. **(3pts)**

Feedback - To know if the cycle has worked properly, there must be feedback to determine if the answers that the process generated effectively answered the question identified in the Direction phase. This is a binary answer. The cycle was successful, or it was not. If the process was successful. **(3pts)**



**QUESTION 19 OF 78**

**DLMCSECSNF01\_E\_Offen\_leicht/Lektion 03**



Name the six of seven layers of the OSI model.

Application, Presentation, Session, Transport, Network, Data Link, Physical **(1pt each)**



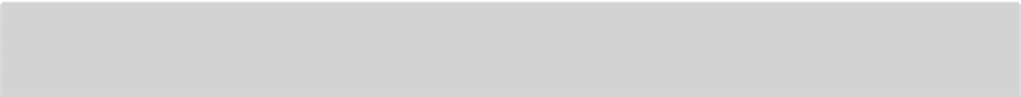
**QUESTION 20 OF 78**

**DLMCSECSNF01\_E\_Offen\_leicht/Lektion 03**



Name three layers of the OSI model that are considered "Hardware Layers".

Network, Data Link, Physical **(2 pts each)**



**QUESTION 21 OF 78**

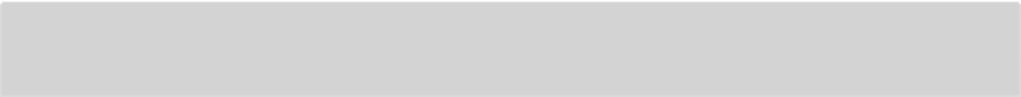
**DLMCSECSNF01\_E\_Offen\_mittel/Lektion 03**



Name and explain the different classes of an IPv6 address.

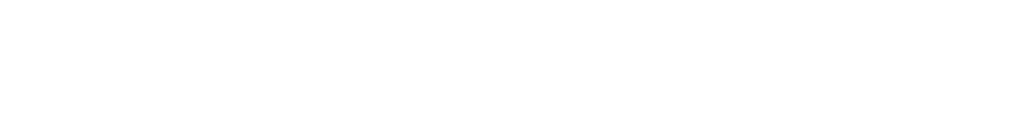
Global Unicast Address – this address is routable on the Internet (Starts with 2001)**(2pts)** Unique Local – used for internal networks, not routable on the Internet**(2pts)**

Link-Local – not routable locally or on the Internet**(2pts)**



**QUESTION 22 OF 78**

**DLMCSECSNF01\_E\_Offen\_mittel/Lektion 03**



Name the device used to move packets between networks and name the information needed to send and receive packets.

A router is used to move packets between networks.**(1pts)**

For a router to send and receive packets, it must have information: a destination address **(1 pts)**

nearby routers **(1 pts)**

knowledge of potential routes to remote networks**(1 pts)** knowledge of the best route to remote networks**(1 pts)** the ability to verify and maintain routing information**(1 pts)**



You are tasked with setting up a new internal network for your organization. Your supervisor wants you to setup the network to utilize all the layers in the OSI model. The supervisor wants to see the equipment you will use to complete a physical model of the network using physical elements of the OSI model.

Is it possible to use the OSI model as a communication protocol? If not, what communication protocol can be used? Name and explain which communication protocol you will use. Name and explain how the layers compare to the OSI model?

It is not possible. The OSI model is a theoretical model not a communication protocol.**(2 pts)**

TCP/IP is a communication protocol to be used. TCP/IP is the set of communications protocols used on networks. The current foundational protocols in the suite are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). Also referred to as the Department of Defense (DoD) model because the development of the networking method was funded by the United States Department of Defense. **(2 pts)**

TCP/IP provides end-to-end data communication specifying how data should be packetized, addressed, transmitted, routed, and received. TCP/IP is organized into four abstraction layers, which classify all related protocols according to each protocol's scope of networking. **(2 pts)**

The layers are the:

Link layer, containing communication methods for data that remains within a single network segment (link) **(2 pts)**

Internet (Network) layer, providing internetworking between independent networks**(2 pts)**

Transport layer (Host to Host), handling host-to-host communication **(2 pts)**

Application layer - providing process-to-process data exchange for applications**(2 pts)**

When comparing to the OSI model to the TCP/IP protocol the following layers are comparable Application Layer > Application, Presentation, Session **(1 pts)**

Transport (host to Host) > Transport Layer**(1 pts)** Network (Internet) Layer > Network Layer **(1 pts)** Link Layer > Dataline layer> Physical Layer **(1 pts)**



You are tasked with setting up a new internal network for your organization. Your supervisor read an article on the “private browsing” has concerns about users accessing the “dark web”, using this feature. The supervisor also relates he does not really understand what the “dark web” is or how to use “private browsing”.

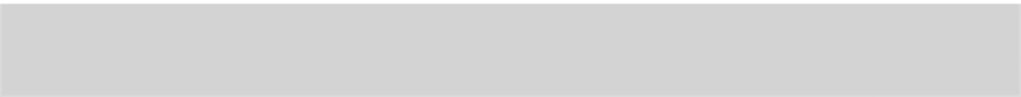
Explain to the supervisor how private browsing works. Identify what the user needs to access the dark web.

Private browsing is a feature that allows the user to keep their browsing history**(2 pts)**, search records **(2 pts)**, or cookies **(2 pts)** from being installed on the local computer they are using.

Each time the private browser mode is activated, the user is presented with a new browser window. When the user closes the private browser window, any artifacts of the user’s actions are deleted/removed from the local system. **(3 pts)**

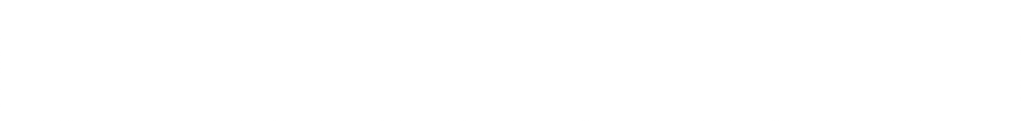
Private browsing does not allow the user to browse the web anonymously. The website, Internet service provider, or employer can still find your identity, location, and viewing history. **(3 pts)**

A user will have to use a Tor browser **(3 pts)** access use the Tor network (3pts) to access the “dark web”.



**QUESTION 25 OF 78**

**DLMCSECSNF01\_E\_Offen\_leicht/Lektion 03**



Identify six actions that Cybersecurity and Infrastructure Security Agency of the United States (CISA) determined that made web browser attacks worse.

users click on links without considering the risk webpage addresses being disguised

security receives less consideration than does functionality

third-party add-ons may not have the ability to obtain a security update

users do not know how to configure the security features of their web browser users are unwilling to disable functionality to increase security**(1 pt each)**



Identify the features of Private Browsing.

Private browsing allows the user to keep their browsing history from being installed on the computer they are using. **(2pts)**

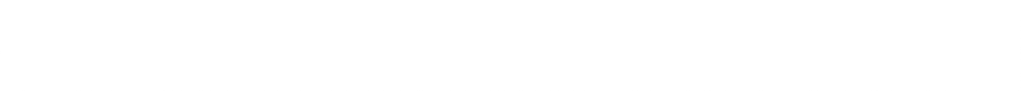
Private browsing allows the user to keep their search records from being installed on the computer they are using. **(2pts)**

Private browsing allows the user to keep their cookies from being installed on the computer they are using. **(2pts)**



**QUESTION 27 OF 78**

**DLMCSECSNF01\_E\_Offen\_mittel/Lektion 03**



Identify and explain two attack vectors against Software Development.

Cross-site scripting (XSS) - Cross-site scripting occurs when an application does not validate or sanitize data inputted into a web page or database entry. The attacker can then use the browser or database to read and execute the untrusted data. The attacker can then execute scripts in the victim’s browser. This can allow the attacker to compromise web pages, redirect a user to a malicious site, or hijack the user’s session. **(1.5 pts for name 1.5 pts purpose)**

SQL injection - occurs when an SQL query is added to a user’s input and is then submitted to a database for processing. **(1.5 pts for name 1.5 pts purpose)**

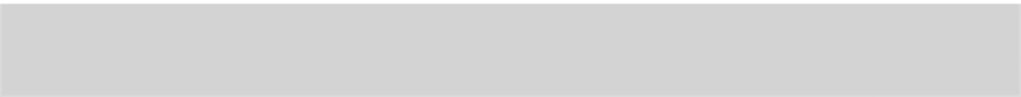


Name and describe the three options when creating a working copy of the digital evidence for examination/investigation purposes.

**Forensic Copy**–**( 1pts)** this is a straight bit for bit copy of the source to the destination. This is not common in today’s environment. Ensure that the destination device does not have old data from previous investigations. This removes the chance to have cross-contamination between the current investigation and a past investigation. The examiner can recover deleted files, file slack, and partition slack. **(1pts)**

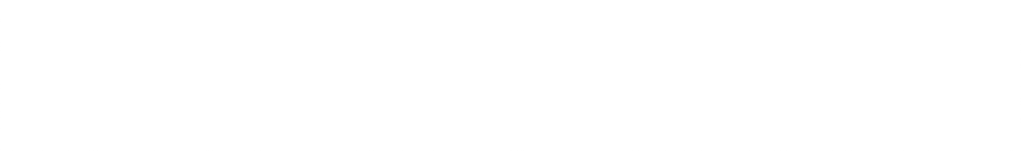
**Forensic image–(1 pts)** creating a bit for bit copy of the source device, but the data is stored in a forensic image format. The source data is wrapped in a protective digital wrapper. The examiner can recover deleted files, file slack, and partition slack. **(1pts)**

**Logical Forensic Image–(1pts)** to be used when there are restrictions allowing the examiner to access specific datasets. The restrictions do not allow access to the entire container and removes the ability to create a bit for bit copy for a forensic image or a forensic copy. This can occur when extracting data from a server, the server cannot be shut down to create a forensic image from the source hard drives. Logical copies of the files and folders pertinent to the investigation are then made. The examiner will NOT be able to recover deleted files, file slack, and partition slack. **(1pts)**



**QUESTION 29 OF 78**

**DLMCSECSNF01\_E\_Offen\_schwer\_F2/Lektion 04**



You are tasked with creating a forensic image of a hard disk drive. Your supervisor told you that you need to create a forensic copy and tells you it must be in a RAW format.

Name and describe the RAW format in detail.

DD Image **(2pts)**

The image format is a bit-for-bit copy of the source device.**(2.5 pts)**

It may store the data as single or multiple files.**(2.5 pts)**

There will not be any metadata stored in the image file(s).**(2.5 pts)**

This format is a fundamental image file that all forensic and non-forensic tools can read.**(2.5 pts)**

This format does not use compression. **(2pts)**

Must ensure your destination device is larger (or the same size) than the source device.**(2pts)** Raw images may have the following file extension: .dd, .raw, .img.**(2pts)**



**QUESTION 30 OF 78**

**DLMCSECSNF01\_E\_Offen\_schwer\_F2/Lektion 04**



You are tasked with collecting RAM from a Microsoft Windows based computer system. Your supervisor asks you what three things are required for you to collect the RAM and which tool you are going to use. Your supervisor is also concerned with overwriting potential evidence when collecting the contents in RAM.

Name the requirements and the tool you will use. Justify why you would use that tool. Explain how you would address the supervisor's concerns.

External storage device (same size or larger than the installed RAM**(2 pts)**

Interactive login for access to the desktop **(2 pts)**

Administrator privileges **(2 pts)**

DumpIt by MoonSols **(2pts)**/Comae **(2 pts)**

Is a combination of Win32dd and Win64dd in one executable.**(2 pts)**

Ease of use. The user will execute the file, which will then create a copy of the physical memory.

# (2 pts)

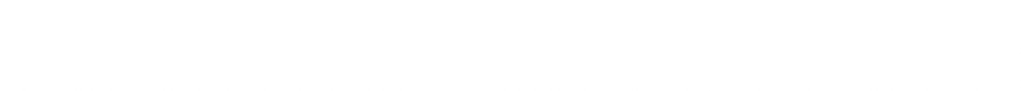
DumpIt can be deployed on a USB key. **(2 pts)**

DumpIt used the smallest footprint in RAM and will have minimal impact on the system.**(2 pts)**



**QUESTION 31 OF 78**

**DLMCSECSNF01\_E\_Offen\_leicht/Lektion 05**



Explain how incident response differs from incident detection.

incident detection handles the identification of the network breach**(3pts)**

incident response develops and executes the response to defeat the attacker**(3pts)**



**QUESTION 32 OF 78**

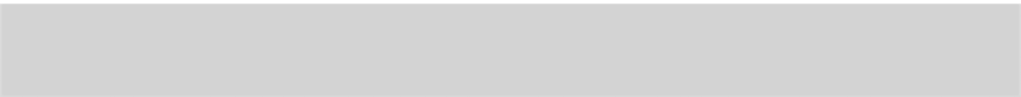
**DLMCSECSNF01\_E\_Offen\_leicht/Lektion 06**



Name three mitigation strategies that can be deployed to reduce the effectiveness of an attacker's actions.

Signature-based Anomaly-based

Tactics, Techniques, and Procedures **(2 pts each)**



**QUESTION 33 OF 78**

**DLMCSECSNF01\_E\_Offen\_mittel/Lektion 05**

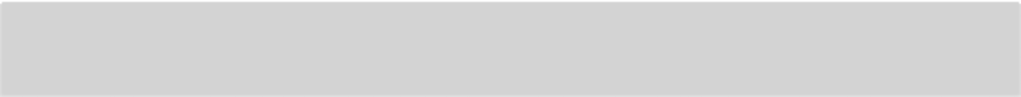


Name three general criteria to determine the strategy that will be used in the Containment phase.

Potential damage to the network Acceptable risk for data loss Evidence collection and preservation Network or organizational downtime

Reaction time to network intrusion, how long will it take to start deploying resources? Resources needed to deploy incident response measures, such as containment Effectiveness of the mitigation controls and containment measures

Time factor–how long will the strategy need to be deployed. Is it a permanent or temporary solution? **(Any combination of three answers 2 points each)**



**QUESTION 34 OF 78**

**DLMCSECSNF01\_E\_Offen\_mittel/Lektion 06**



When using Travis Smith’s TEACH categories for training. Name the category that you would use to train new personal and explain why.

Exploitable to Anyone **(3 pts)**

Identifies easy-to-use techniques. Using accessibility features and registry run keys would fall into this category. **(3 pts)**



You have been notified by your supervisor that you have been put in charge of the new incident response team. You are told you will follow the Incident Response Life Cycle as described in NIST Special Publication 800-61. Explain to your supervisor what is required in the Preparation Phase. Justify your response.

The organization will need to identify its risk tolerance. It is not possible to remove all risk an organization will face; the goal is to reduce the risk level to where it is acceptable to the organization. **(3pts)**

The organization can implement some of the following controls, new definitions for the intrusion detection system, redefine the baseline of the network, deploy new appliances designed to alert on attacks, and ensure the security team has regular training. **(3pts)**

Communication will be essential in the first step in preparation to identify who will be in charge of the response and give employees their tasks and assignments. **(3pts)**

The security team members must also be familiar with the physical topology of the network. They need to be familiar with the locations of the servers, routers, and switches. If an attacker can gain physical access to the network, they can more easily launch their attack because they have created a foothold inside the network itself, bypassing many security controls. **(3pts)**

Identify potential vulnerabilities such as weak physical security, security patches not being deployed, unneeded ports are closed. You should do this security check on a regular schedule. These actions need to be documented and maintained. It will be tough to respond to an incident effectively if the security team lacks knowledge about these items. **(3pts)**

Training is going to be paramount. C-level personnel need to take part in the training. They must understand at a high level what can occur during a response to an attack. The training scenarios will also identify the inadequacies of the plan. What looks good written on paper may not be feasible when executed in the physical environment. This will allow the plan to be adjusted and able to address any deficiencies that were noted. **(3pts)**



You inform your supervisor that additional IDPSs need to be deployed within the network. Your supervisor responds that the current deployment of IDPS is sufficient for threat identification and prevention. Name and describe three additional benefits the additional IDPS may provide to the organization.

**Deterrent control (3 pts)** –if an authorized user is aware that their behavior may be recorded and monitored, their actions are more likely to conform to the authorized use policy. **(3 pts)**

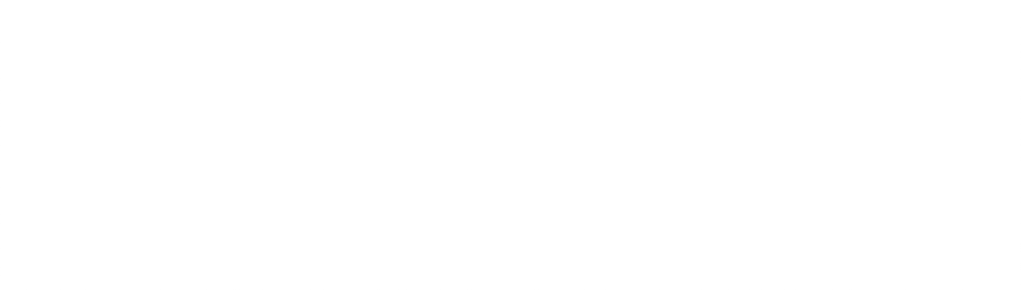
**Quality Control (3 pts)** –can be used to audit current security policies to determine if they are effective, such as whether the existing firewall rules are blocking the desired traffic. **(3 pts)**

**Threat Documentation (3 pts)** –as the IDPS identifies and logs the potential attacks, the security team can show this documentation to the C-level executives (or decision-making supervisors) to justify additional mitigation efforts or identify changes in the security scheme. **(3 pts)**



**QUESTION 37 OF 78**

**DLMCSECSNF01\_E\_MC\_leicht/Lektion 01**



What acts as an intermediate layer between the hardware and the software?

**Select one:**

Computing layer User layer

File System

*Operating system*



When does the operating system start to function?

**Select one:**

After the file system is activated

After the user types in their password *When the power is turned on*

When the monitor turns on



**QUESTION 39 OF 78**

**DLMCSECSNF01\_E\_MC\_leicht/Lektion 01**



Considering Input-Output management, what is an interrupt driven I/O or programmed

I/O which must be implemented to manage the timeframe to respond to the input/output request?

**Select one:**

User Response Information Response *System response* Device Response



Which statement is correct?

**Select one:**

A swap file is only configured by the administrator. A swap file is only configured by the user.

A swap file is space on a volatile storage device.

*A swap file is space on a non-volatile storage device*.



**QUESTION 41 OF 78**

**DLMCSECSNF01\_E\_MC\_mittel/Lektion 01**



When considering Input-Output management, what will create a standard I/O library

that can be accessed for user-level requests?

**Select one:**

Device-level I/O *User-level I/O* System-level I/O Library-level I/O



**QUESTION 42 OF 78**

**DLMCSECSNF01\_E\_MC\_schwer/Lektion 01**



I/O devices such as hard drives and USB sticks are examples of … devices.

**Select one:**

character user network *block*



**QUESTION 43 OF 78**

**DLMCSECSNF01\_E\_MC\_schwer/Lektion 01**



When the processes are executed and have an I/O instruction, the processor will then

issue the command to the device controller. The controller will then interface with the I/O device and create a “status of operation” in the status register. This is known as ...

**Select one:**

Port-mapped I/O. *Programmed I/O*. I/O using DMA. Interrupt driven I/O.



What is the exploit used to access a data set after the users have deleted it from the

system called?

**Select one:**

*Data remanence* Data recovery Data rebound Data replacement



**QUESTION 45 OF 78**

**DLMCSECSNF01\_E\_MC\_leicht/Lektion 02**



Which of the following is the attack where the attacker can monitor electromagnetic

radiation to determine what keystrokes are being used or content displayed on the monitors?

**Select one:**

Typing attack Listening attack Data attack *Tempest attack*



How many broad functions will the fields of the process table deal with?

**Select one:**

*3*

1

2

4



**QUESTION 47 OF 78**

**DLMCSECSNF01\_E\_MC\_mittel/Lektion 02**



Which statement is correct?

**Select one:**

*Process management will maintain information about the registers being used, process state, priority, process ID, when the process started, what is the parent process*.

User management will maintain information about the registers being used, process state, priority, process ID, when the process started, what is the parent process.

Memory management will maintain information about the registers being used, process state, priority, process ID, when the process started, what is the parent process.

File management will maintain information about the registers being used, process state, priority, process ID, when the process started, what is the parent process.



Which of the following is the attack that DDR3 memory is susceptible to?

**Select one:**

Side-channel Vibration-based *Rowhammer* Penciling



**QUESTION 49 OF 78**

**DLMCSECSNF01\_E\_MC\_schwer/Lektion 02**



What maintains control of where the data is stored on a storage device?

**Select one:**

*File System* Windows Registry BIOS

Operating System



**QUESTION 50 OF 78**

**DLMCSECSNF01\_E\_MC\_schwer/Lektion 02**



What could occur when using C or C++ and there is no array-bound checking?

**Select one:**

Underflowing Buffers *Buffer Overflow* Overflowing Buffers Buffer Underflow



**QUESTION 51 OF 78**

**DLMCSECSNF01\_E\_MC\_leicht/Lektion 03**



What is the OSI Model?

**Select one:**

A compilation of procedures A compilation of regulations A compilation of laws

*A compilation of guidelines*



Which of the following can be used in software security?

**Select one:**

Output Validation User Validation *Input Validation* Increased privileges



**QUESTION 53 OF 78**

**DLMCSECSNF01\_E\_MC\_leicht/Lektion 03**



What is an organization that may own/operate/sell access to the backbone

infrastructure?

**Select one:**

Network Internet Provider *Network Service Provider* Network Backbone Provider Network Access Provider



What is the term for when an SQL query is added to a user’s input and is then

submitted to a database for processing?

**Select one:**

Blue screen of death Cross-site scripting (XSS) *SQL injection*

Data corruption



**QUESTION 55 OF 78**

**DLMCSECSNF01\_E\_MC\_mittel/Lektion 03**



Which protocol would you use to securely connect to a web server?

**Select one:**

*HTTPS* SFTP HTTP FTP



**QUESTION 56 OF 78**

**DLMCSECSNF01\_E\_MC\_schwer/Lektion 03**



Which statement is correct?

**Select one:**

*Data sanitization - The developer must check the dataset to ensure it meets the form and format requirements of the secondary system*.

Validate input - The system must check some of data being inputted or accepted by the application to ensure it is in the form and format expected.

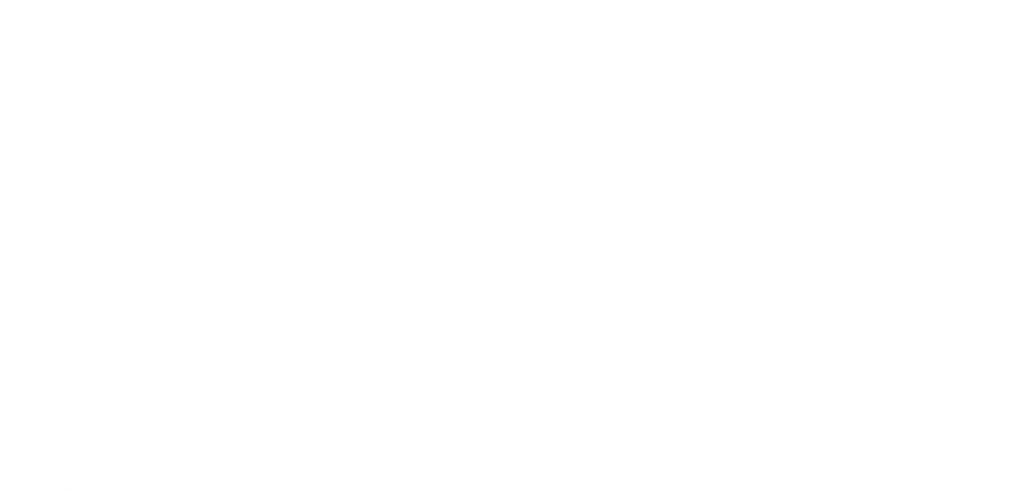
Software Design - Start the design process with user experience as the primary goal, the goal of security can be addressed after the software is deployed.

Principle of least privilege - allow access to all resources.



**QUESTION 57 OF 78**

**DLMCSECSNF01\_E\_MC\_schwer/Lektion 03**



The image depicts which form of cryptography?

**Select one:**

Symmetric cryptography Key cryptography *Asymmetric Cryptography* Public cryptography



The Linux operating system has the … command, which can modify the date and time

stamps to a value decided on by the user.

**Select one:**

modify *touch* create change



**QUESTION 59 OF 78**

**DLMCSECSNF01\_E\_MC\_leicht/Lektion 04**



What is it called when the goal is to leave the smallest footprint during the collection to

minimize the amount of data being changed with the collection?

**Select one:**

Legally Sound Manner *Forensically Sound Manner* Legally Approved Manner Forensically Approved Manner



What is a piece of code used to infect the system, which then allows the attacker to

take control of the system?

**Select one:**

Botnet Worm *Backdoor* User ID



**QUESTION 61 OF 78**

**DLMCSECSNF01\_E\_MC\_mittel/Lektion 04**



Which statement is correct when analyzing malware?

**Select one:**

Conduct a dynamic code analysis of the malware on the production network. If the malware is “packed,” stop the analysis.

Only conduct a static code analysis of the malware.

*The analysis must be done in a controlled environment*.



Which of the following is the utility in the Metasploit Framework that can change a file’s

MAC (modified, accessed, created) date and time stamps?

**Select one:**

MAC destroyer *Timestomp* Timechange MAC change



**QUESTION 63 OF 78**

**DLMCSECSNF01\_E\_MC\_schwer/Lektion 04**



Which of the following is a technique the attacker may use for exfiltration?

**Select one:**

File renaming *External web service*

Changing file extension

Encrypting the data set



**QUESTION 64 OF 78**

**DLMCSECSNF01\_E\_MC\_schwer/Lektion 04**



Which statement is correct?

**Select one:**

Steganography is a form of encryption.

The key is a rule set that determines how the encryption/decryption will be executed. *The cryptosystem will use an “algorithm” in the encryption/decryption process*.

The attacker will not use the scheduling technique for the exfiltration of data.



**QUESTION 65 OF 78**

**DLMCSECSNF01\_E\_MC\_leicht/Lektion 05**



Which field of forensics has the purpose to identify, investigate and remediate attacks

against an organization’s computer network?

**Select one:**

Computer Mobile *Network* DFIR



When comparing information and intelligence, which of the following is an aspect of

information?

**Select one:**

Does not need to be analyzed *Standalone*

Is not shared

Must be kept secret



**QUESTION 67 OF 78**

**DLMCSECSNF01\_E\_MC\_leicht/Lektion 05**



What is the first step of the Incident Response Life Cycle?

**Select one:**

Containment Detection *Preparation* Post Incident



Which statement is correct?

**Select one:**

Information about the target may be available for purchase from only disreputable private sources. Attackers never target subcontractors of the target organization.

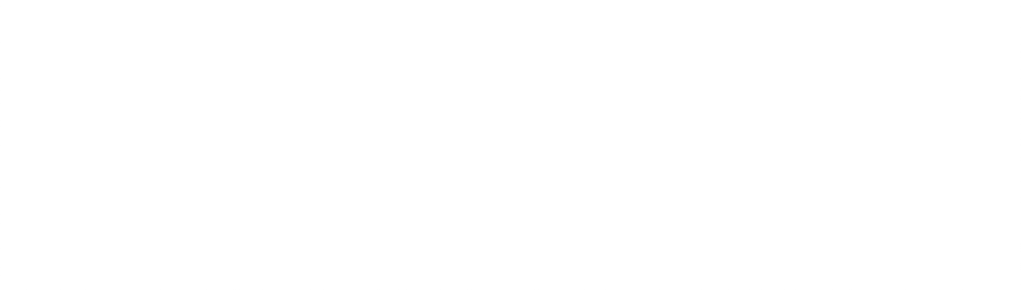
*The attacker may target you because of national origin, economic sectors such as banking, or political*.

Reconnaissance is not a part of the actions taken in the Targeting phase.



**QUESTION 69 OF 78**

**DLMCSECSNF01\_E\_MC\_mittel/Lektion 05**



Which options can the attacker do after the Targeting Phase?

**Select one:**

*Purchase similar equipment used by the organization* Become Facebook friends with the employees

Use LinkedIn to identify employees

Dumpster dive to identify user passwords



**QUESTION 70 OF 78**

**DLMCSECSNF01\_E\_MC\_schwer/Lektion 05**



Why would an attacker use the technique "Packing" to disguise malware?

**Select one:**

By changing the file extension, the true nature of the file is hidden.

*A compressed file will have a different signature than an uncompressed file*.

By changing the first hexdecimal character to a x/E5 , the system will not recognize the file.

The added lines of code will change the file signature without changing how the malware will operate.



**QUESTION 71 OF 78**

**DLMCSECSNF01\_E\_MC\_schwer/Lektion 05**



To bypass the systems file access controls, the attacker would have to have … access

to the volume.

**Select one:**

physical full *direct* indirect



Which of the following is an artifact that suggests that an attacker has compromised the

network?

**Select one:**

Authorized registry or system file changes *Unusual network traffic*

Authorized settings changes

Known applications installed on the system



**QUESTION 73 OF 78**

**DLMCSECSNF01\_E\_MC\_leicht/Lektion 06**



Which strategy uses threat intelligence analysis, defensive engagement and information

sharing and collaboration?

**Select one:**

*Tactics, Techniques, and Procedures* Offensive - based

Signature-based

Anomaly-based



Which are sources the analyst can use?

**Select one:**

Only internal influences Apply security patches Goals of the defender *Data points of past attacks*



**QUESTION 75 OF 78**

**DLMCSECSNF01\_E\_MC\_mittel/Lektion 06**



Which statement is correct?

**Select one:**

The organization can be proactive after the attacker gains a foothold in the network.

Information sharing is not key to being proactive and recognizing the telltale signs of an incoming attack.

*The sharing of information and collaboration with both internal and external organizations will strengthen all the participants*.

The analyst can only use information that has been developed by their organization.



What is the purpose of the MITRE ATT&CK framework?

**Select one:**

Create an individual effort for the organization's identification and response efforts *Help create an organization's detection and response capabilities*

Create an esource that can be used by both attackers and defenders

Help create an attacker's detection and response capabilities



**QUESTION 77 OF 78**

**DLMCSECSNF01\_E\_MC\_schwer/Lektion 06**



Network-based information can be found in which location?

**Select one:**

Only the hosts in the Sales department All hubs on the network

*Appliances on the perimeter of the network*

User's password



**QUESTION 78 OF 78**

**DLMCSECSNF01\_E\_MC\_schwer/Lektion 06**



The … process is designed to give the analyst a way to take all the information thrown

their way and transform it into actionable intelligence.

**Select one:**

collection corruption *correlation* complete