1. Please describe the differences between forensic investigation and incident response.

Both are important part of IT-Forensics, but they have different objectives and focus on different stages of an incident.

Which approach is used depends on the situation and is different for each individual. Often, however, both approaches share common techniques that cannot be precisely separated. Reasons for consideration could be e.g. the estimated downtime and amount of damage, but also legal issues such as data protection authorities and possible insurance claims (e.g. towards customers).

Forensic

(a) Forensic is mostly a post-incident process that involves gathering and analyzing evidence to reconstruct events and identify key factors after an incident has occured.

(b) Goal to determine what happened and how to prevent similar incidents in the future.

(c) Results can be used as evidence for legal proceedings and insurance claims.

Incident

(a) Process of detecting, containing, and mitigating the effects of an incident as quickly as possible, with the goal of minimizing damage and restoring normal (business) operations.

(b) Reactive process that is triggered when an incident is detected or reported.

(c) Primary focus of incident response is to contain the incident and prevent further damage, rather than to gather and analyze evidence.

(d) Incident response may involve collecting some evidence for later analysis or investigation. But depending on the used incident techniques important evidence could be destroyed or get lost (e.g. see backup example in chapter 5.3.1).

2. Please identify how and where the forensic principles by BSI, Casedy and Freiling differ

BSI

- Focus only on forensics and evidence preservation.
- Practical process that examines specific symptoms and anomalies for their causes.
- So no static/predetermined process that you follow, but dependent on the respective situation.

Casey

- More structured/step-by-step approach and more formal than the BSI approach.
- Strong focus on proper preservation of evidence and clean chains of evidence for court cases
- Particular attention is paid to the correctness/reliability of the tools used so that the results can be validated correctly.

Freiling

- Consolidates forensics and incident response methods into a single framework.
- They aim to complement each other and combine their advantages.
- It is a management-oriented approach that prepares the entire organization and infrastructure for incidents and how to deal with them.
- During an incident, various criteria can be used to decide whether a full forensic examination is necessary.

3. For the following cases, argue why you prefer either a clean forensic process or incident response - and how you would mix and match to optimise your result:
Reacting to a ransomware attack
Suffering of a dDoS-attack
Suffering of DoS due to a buffer overflow in a network daemon

Ransomware

The goal here would be to recover the encrypted/lost data (hopefully a backup (process) exists), prevent further damage to other systems, and stop the attacker's access.

Considering that the majority of ransomware attacks happen via social engineering using, for example, malicious attachments in email, a mixed method would be considered here. So, since a successful attack usually requires active employee interaction, it is unlikely that an attacker will be able to successfully re-enter immediately. However, this requires appropriate company communication.

A fast incident response process can therefore minimize the damage and restore the operating state. In parallel or afterwards, forensic methods can be used to search for and eliminate the entrypoint (e.g., specific employee/computer, software updates, training).

dDoS

DDoS attacks are designed to overwhelm systems and networks with traffic, so the focus here is on minimizing the damage and surviving the attack.

Some incident response techniques are helpful here:

- Increase network capacity for a short time, e.g. scale servers.
- Find out traffic source(s)
- Block malicious traffic

DoS

Here, I would prefer a forensic process. The focus is on finding the particular exploited vulnerability and eliminating it as quickly as possible to prevent further attacks. However, this requires a deeper analysis.

Parallel incident response techniques are also feasible here. For example, one could try to block malicious traffic with a WAF and reduce the impact of the overflow. However, the focus should be on eliminating the vulnerability.

4. Could you provide an automated script to identify files with a "tampered" extension - i.e. a .jpg hiding as .odt?

There are many possible solutions. One with Unix board tools would be the following:

```bash
#!/bin/bash

# Set the directory to check
dir_to_check="/path/to/directory"

# Loop through each file in the directory
for file in "$dir_to_check"/*
do
    # Get the expected file extension based on the file extension
    expected_extension="${file##*.}"

    # Get the actual file type with possible types returned by --extension option
    actual_type=$(file --extension -b "$file")

    # Check if the expected extension is in the list of possible types
    if echo "$actual_type" | grep -q "/$expected_extension"
    then
        echo "File $file: OK"
    else
        echo "File $file: MISMATCH (actual: $actual_type, expected: $expected_extension)"
    fi
done
```

5. How would you suggest to delete a file in a forensically sound manner?

Depending on the medium and filesystem used, there are some general techniques:

(a) Physical destroy the hard disk.

(b) Since when “deleting" a file the operating system often only removes the associated references, but the data itself continues to lie unused in the hard disk, one should overwrite all used sectors of the file with random/zero values and thus make recovery impossible.

How and how often the data has to be overwritten depends on the medium used. The Gutmann method is one such method. It recommends performing 35 write passes on earlier hard disks and floppy disks. Each pass is performed with a different write pattern to ensure that every single bit is actually overwritten. Nowadays, one to eight passes should be sufficient (see: https://link.springer.com/chapter/10.1007/978-3-540-89862-7_21).

(c) For SSDs you can use the ATA Secure Erase command. This overwrites the entire SSD including defective memory areas and restores the factory settings. The exact process and implementation depend on the manufacturer.
Alternatively, with SSDs there is also the option of using the trim command to delete unused memory areas during use. This makes it possible to inform the SSD after deleting a file that it should also delete the associated areas. However, since the command is mainly used for performance optimization, a complete 100% deletion is not always guaranteed.

(d) Encrypting your entire disk adds another layer of security to your data. If your disk is encrypted, even if someone manages to recover a deleted file, the data will be unreadable without the encryption key.

6. Looking at VeraCrypt's hidden volumes: Does a tool like tchunt actually find these? If not, what does it find - and if so, how?

No, TCHunt does not find hidden volumes within a TrueCrypt volume. What it finds are normal TrueCrypt volumes that the user may have hidden in the file system.

To do this, it scans the system for files with certain properties:

- The suspect file size modulo 512 must equal zero.
- The suspect file size is at least 19kb.
- The suspect file contents pass a chi-square distribution test.
- The suspect file must not contain a common file header.

Since it is only a statistical pattern search, not all found files are automatically TrueCrypt volumes.

For VeraCrypt itself there is also a PoC tool to find such volumes: VC_Hunter.
It is also based on examining statistical properties of it.