Malware Forensic Using Wireshark For Investigation (Cyber Security Assignment)

forensic science definition

any science that has been used to resolve legal disputes

1814

detection of poison in animals

1879

system of personal identification

1900s

blood typing test in dried blood

bullet matched to single fire arm

1910

document examination developed

Edmond Locard (1910)

created first 'crime lab'

what are the two phases when processing a case

investigative

evaluative

investigative

what has happened

speculative and frustration

10% of caseload

fingerprints

recovered from surfaces and compared to those on file

limitations if fingerprints

rigid surfaced

useless if nothing to compare to

DNA

DNA profile can be obtained from most human biological evidence left at scene

including skin cells transferred to a rough surface

can be compared from a known person

DNA limitations

if no known DNA profile, cannot be compared

easily affected by contamination

DNA advantages

high match probability

obtained from very rough surfaces

further info can be gathered from a profile

fingerprints advantages

can be conclusive

only indicative of primary transfer

what are the two components of familial searching

genetic and social

genetic- familial searching

more closely related you are the more similar DNA profiles

social- familial searching

more likely to become an offender if close family is

DNA profile

represented as 20 numbers

one number replaced with wildcard and searched again

time consuming and expensive

what are the 4 defences

outright denial

present but not involved

involved, but not responsible

no comment

Bloodstain Pattern Analysis

how blood came to be deposited on a surface

divided into contact and airborne status