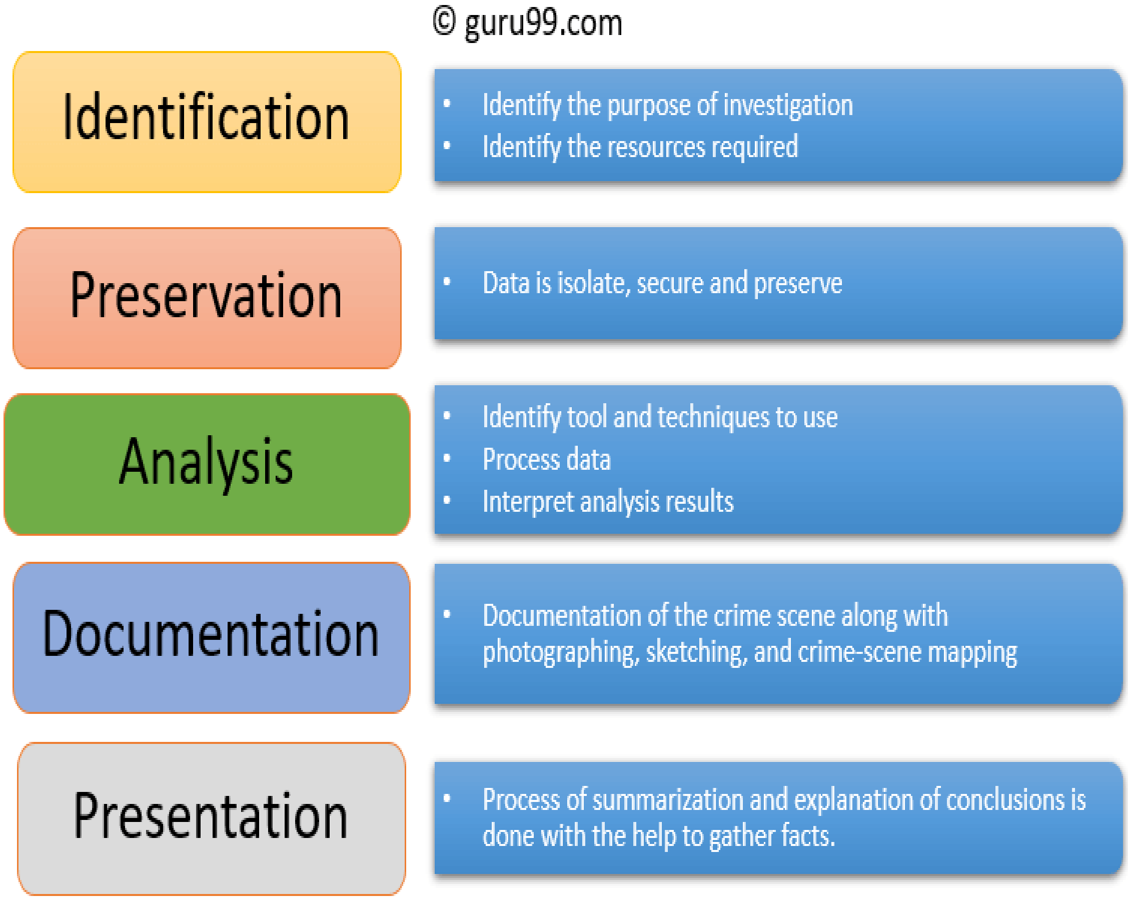
Digital Forensics explained - notes



© guru99.com

Identification

- Identify the purpose of investigation
- Identify the resources required

Preservation

- Data is isolate, secure and preserve

Analysis

- Identify tool and techniques to use
- Process data
- Interpret analysis results

Documentation

- Documentation of the crime scene along with photographing, sketching, and crime-scene mapping

Presentation

- Process of summarization and explanation of conclusions is done with the help to gather facts.

- Forensics is the application of the scientific method to answer a question
- **Trust but verify**

The ACPO principles - [ACPO Guidelines & Principles Explained | Forensic Control]

1. No action must be taken that will change data held on a digital device that could later be relied on as evidence in Court.
2. If it’s necessary to access original data held on a digital device, you must be both competent to do so and able to explain your actions, as well as explain the impact of them on any digital evidence used in a Court.

3. A trail or record of all the actions taken and applied to the digital evidence must be created and kept safely and securely. If an independent third party forensic expert examines the processes they should be able to come to the exact same conclusion.
4. The person in charge of the investigation has the overall responsibility of making sure these principles are followed

NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response

The interview phase:

Before an investigator starts examining forensic evidence, they should interview witnesses and case related persons, to help narrow down the type of criminal (or other) case. Additionally, this interview might be essential along the presented evidence in the final report. A starting point may look like this:

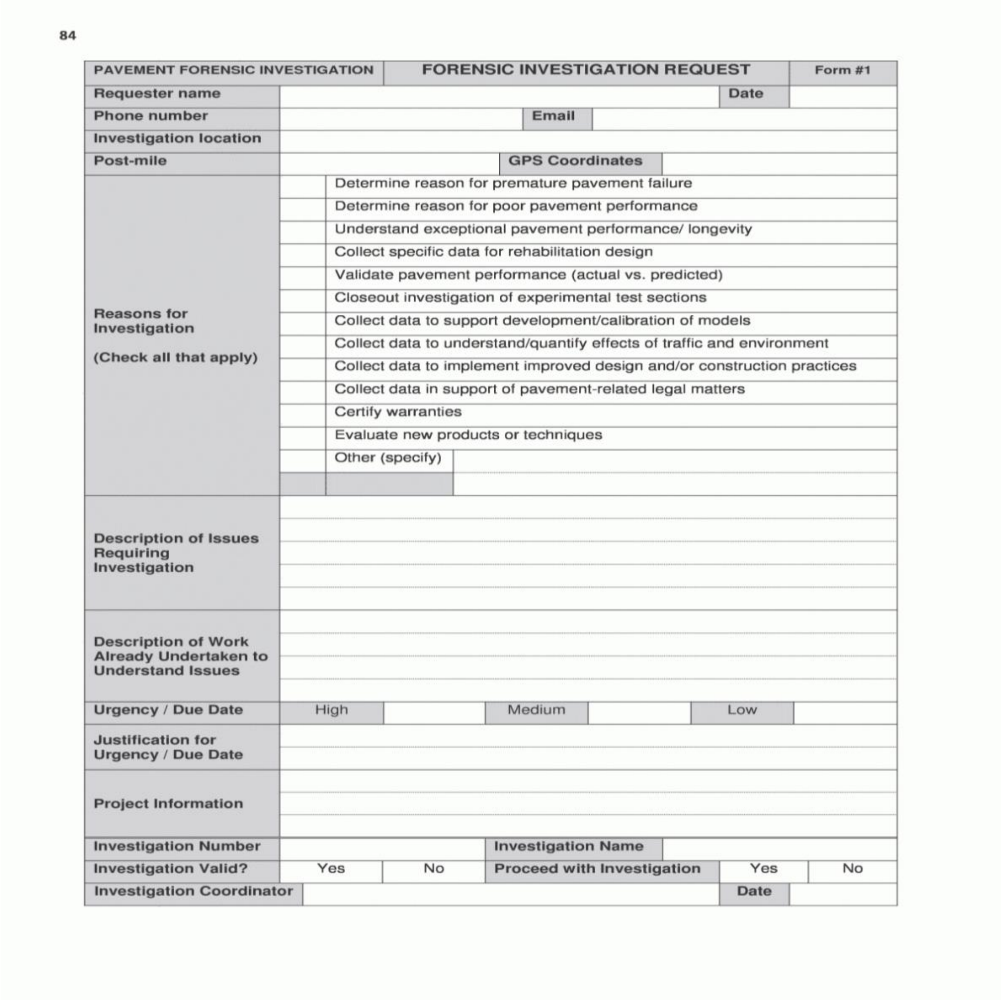
1. What is your name?
2. What is your contact information?
3. **Establish** a relationship to the case (witness, suspect, victim?)
4. Who do you think may be involved?
5. When did you become aware of the situation?
6. What do you know about the situation?
7. What steps have you taken (have you tampered with evidence?)
8. What electronic devices, social media accounts, software etc. might be relevant to the case?
9. Are you aware of any electronic artifacts such as contacts, phone numbers, text messages etc.?
10. Are you aware of any unusual activity?

What to bag for a response:

- Response computer (likely with no internet access)
- Dongles
- Smartphone or internet enabled device
- Imaging device
- Extension cords and power strips
- Digital camera (or smartphone, might be presented as evidence, don't use a personal smartphone)
- Paper and a pencil
- Labels
- Gloves

- Black light
- Tool kit consisting of screwdrivers, also electrical tape, duct tape, zip ties, screws bolts etc.
- Network cables, hub, crossover cable, adapters, IDE/SATA adapters
- Boot discs(or usb sticks)
- Blank usb sticks
- Grounding mechanism
- Write blockers
- Faraday bays
- Bags or carrying devices
- Extra mouse & keyboard
- Suction cups

Example of a digital forensics examination guide:



84

PAVEMENT FORENSIC INVESTIGATION	FORENSIC INVESTIGATION REQUEST					Form #1
Requester name					Date	
Phone number			Email			
Investigation location						
Post-mile			GPS Coordinates			
Reasons for Investigation (Check all that apply)		Determine reason for premature pavement failure				
		Determine reason for poor pavement performance				
		Understand exceptional pavement performance/ longevity				
		Collect specific data for rehabilitation design				
		Validate pavement performance (actual vs. predicted)				
		Closeout investigation of experimental test sections				
		Collect data to support development/calibration of models				
		Collect data to understand/quantify effects of traffic and environment				
		Collect data to implement improved design and/or construction practices				
		Collect data in support of pavement-related legal matters				
		Certify warranties				
		Evaluate new products or techniques				
		Other (specify)				
Description of Issues Requiring Investigation						
Description of Work Already Undertaken to Understand Issues						
Urgency / Due Date	High		Medium		Low	
Justification for Urgency / Due Date						
Project Information						
Investigation Number			Investigation Name			
Investigation Valid?	Yes	No	Proceed with Investigation		Yes	No
Investigation Coordinator					Date	

Awesome courses and knowledge_base: https://www.geeksforgeeks.org/introduction-of-computer-forensics/

Autopsy basics: https://www.sleuthkit.org/ - https://medium.com/@tusharcool118/autopsy-tutorial-for-digital-forensics-707ea5d5994d

https://www.geeksforgeeks.org/mobile-technologies-definition-types-uses-advantages/ - related to mobile phone forensics

https://www.yournavi.com/posts/cell-phone-towers - cell phone technology

https://www.mat.ucsb.edu/~g.legrady/academic/courses/03w200a/projects/wireless/cell_technology.htm - in depth on wireless technology

Tools:

https://www.bluevoyant.com/knowledge-center/get-started-with-these-9-open-source-tools

https://github.com/mesquidar/ForensicsTools - list of various open source tools and toolkits available

Smartphone specific tools:

https://github.com/scorelab/OpenMF - Android open source forensics toolkit

https://github.com/jfarley248/MEAT - Perform different kinds of acquisitions on iOS devices

https://github.com/MobSF/Mobile-Security-Framework-MobSF - an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

https://www.elcomsoft.com/eift.html - IOS forensics toolkit (paid)

https://products.containerize.com/digital-forensic-software/mvt/ - Pegasus malware detection toolkit for IOS and Android

Useful resources:

https://www.nirsoft.net/;

Home - SEARCH - an acronym for System for the Electronic Analysis and Retrieval of Criminal Histories

https://www.nist.gov/