

A decorative graphic on the left side of the slide consisting of white lines and circles on a dark blue background, resembling a circuit board or a stylized tree structure.

FORENSIC ANALYST PROCESS

JAMES NOLEN

NOLENJGN@MY.GVLTEC.EDU

THE 6 PHASES OF FORENSIC ANALYST PROCESS

1. Pre-Investigation
2. Preparing the Investigation
3. Search and Seizure
4. Analyzing the Evidence
5. Reporting and Testifying
6. Post-Investigation

A decorative graphic on the left side of the slide consisting of a network of thin, light-gray lines and small circles, resembling a circuit board or a digital network. The lines are vertical and horizontal, with some diagonal connections, and the circles are placed at various points along these lines.

PHASE 1

PRE-INVESTIGATION

- Setup a Forensic Workstation with the appropriate tools to conduct a secure and accurate analysis.
- Understand Policies and Laws to include laws about forensics so the investigation is properly.
- Train with the forensic tools and equipment to ensure they will perform during an actual investigation.



PHASE 2

PREPARING THE

INVESTIGATION

- Establish the who, what, when, where, why, and how of the investigation.
- Create the initial plan and case assessment.
- Get permission: Determine if a warrant is required.

A dark background with a light gray circuit board pattern. The pattern consists of vertical and horizontal lines of varying thickness, with small circles at the intersections and endpoints, resembling a printed circuit board (PCB) layout. The lines are more dense on the left side and become sparser towards the right.

PHASE 3

SEARCH AND SEIZURE

- Secure the crime scene to ensure the integrity of all evidence when it is collected.
- Sketch and document everything. Use evidence form and proper procedures.
- Seize the evidence and collect using appropriate methods.

A decorative background pattern resembling a circuit board or network diagram, with thin white lines and small circles on a dark gray background.

PHASE 4

ANALYZING THE EVIDENCE

- Ensure the integrity of the evidence and make copies
- Physical and logical analysis
- Conduct time-frame analysis, data-hiding analysis, application and file analysis, and ownership/possession analysis

A decorative background pattern of thin, light gray lines and small circles, resembling a circuit board or a network diagram, is visible on the left and right sides of the slide.

PHASE 5

REPORTING AND

TESTIFYING

- Complete the final investigative report
- Complete the threshold report
- Testify in court as an evidentiary or technical witness.

A dark background with a light gray circuit board pattern. The pattern consists of vertical and horizontal lines of varying thickness, with small circles at the intersections and endpoints, resembling a printed circuit board (PCB) layout. The lines are more dense on the left side and become sparser towards the right.

PHASE 6

POST-INVESTIGATION

- Do not disclose any confidential information
- Archive evidence, notes, and other items per policy and procedures
- Conduct lessons learned. What did we do well and what can we do better.

MOST IMPORTANT PHASE OF THE FORENSIC ANALYST PROCESS

The most important phase of the Forensic Analyst Process in the Pre-Investigation. This phase is the keystone to everything that follows.

3 EXAMPLES OF THE MOST IMPORTANT PHASE

- An analyst must follow laws and procedures, or they may become liable for improper handling or damage to evidence.
- Train, train, and train again.
- The analyst must conduct training prior to an actual investigation to ensure evidence integrity and the investigation is conducted properly with the appropriate outcome.



THANK YOU FOR YOUR ATTENTION IN THIS
PRESENTATION OF THE FORENSIC ANALYST PROCESS.

REMEMBER, WHEN YOU SET YOUR SECURITY POLICY AND
PROCEDURES, THEY WILL NOT WORK IF YOU DON'T
FOLLOW THEM.

Contact for more information:

James Nolen

nolenjgn@my.gvltec.edu

