CYBER ENRICH TRAINING PROGRAM | MODULE II

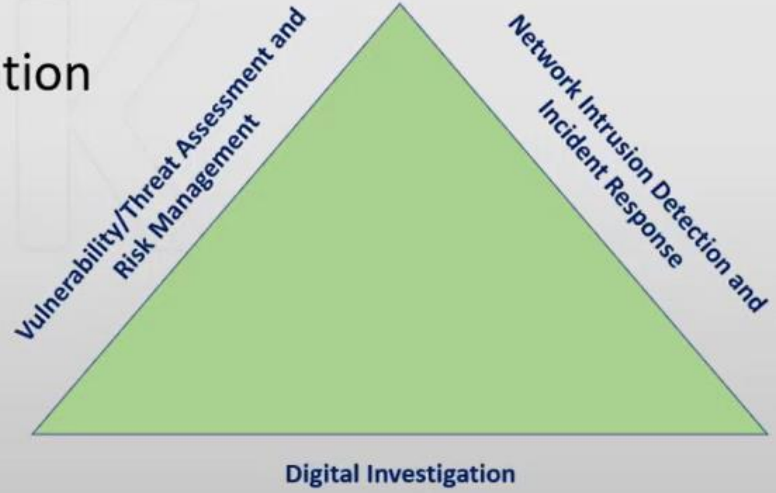
Digital Forensics and Investigation - Overview

What is Digital Forensics?

- Computers as a source of crime/evidence
- Application of scientific methods on computers to extract digital evidence
- Determining the past actions
- Involves identification, collecting, preserving, analyzing computer-related evidence
- Digital forensics vs data recovery

What is Digital Investigation?

- A part of the computing security triad
- Public sector and private sector investigation
- Criminal and Civil investigation


Vulnerability/Threat Assessment and Risk Management
Network Intrusion Detection and Incident Response
Digital Investigation

What is Digital Evidence?

- Any information that can be extracted from a computer
- Must be in human-readable format
- The Forensic Examiner is not biased
- Digital Systems
  - Open Computer Systems
  - Communication Systems
  - Embedded Computer Systems

Need of Digital Investigation

- Many crimes involve digital devices to
  - Store information
  - Communicate with colleagues
  - Navigate
  - Threat someone
  - Launch cyber attack against an organisation

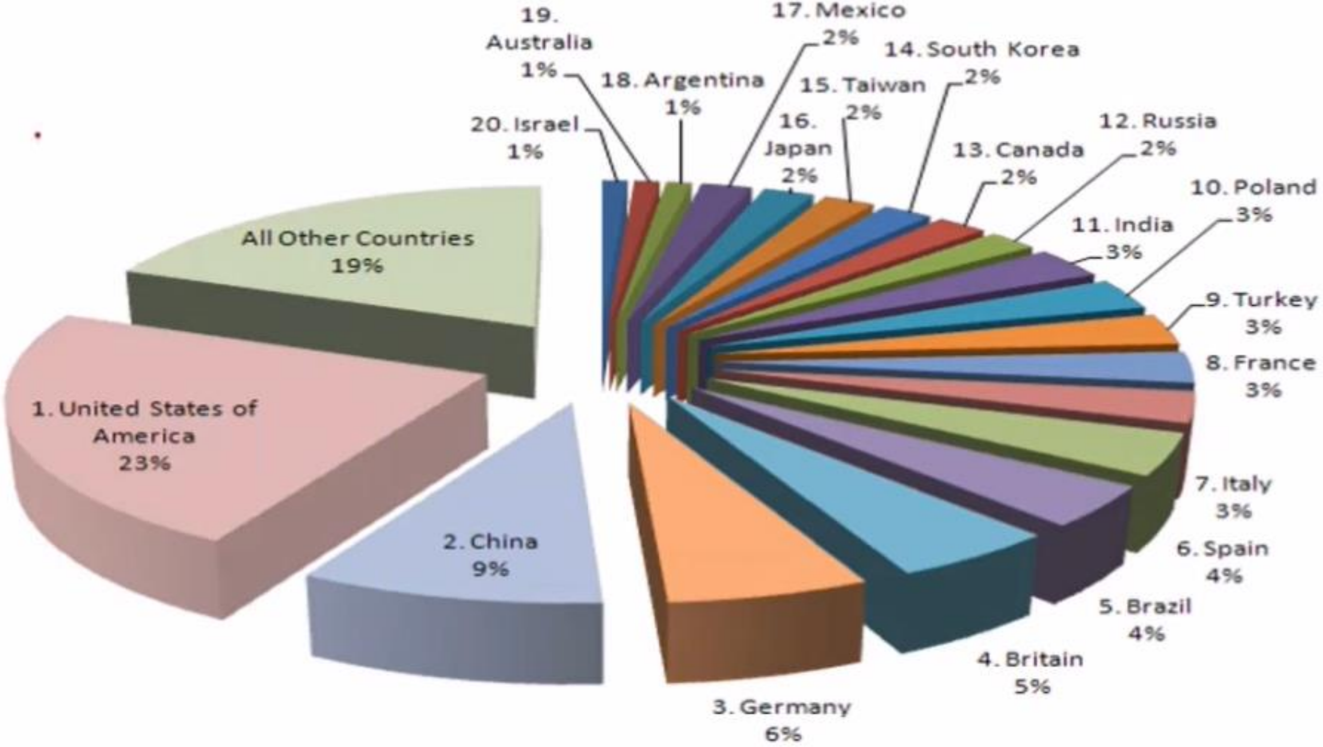
Who Uses Digital Forensics?

- Law Enforcement Officials
- Private Corporations
- Criminal Prosecutors
- Individual/Private Citizens
- Civil Litigations
- Insurance Companies

Who are the Victims?

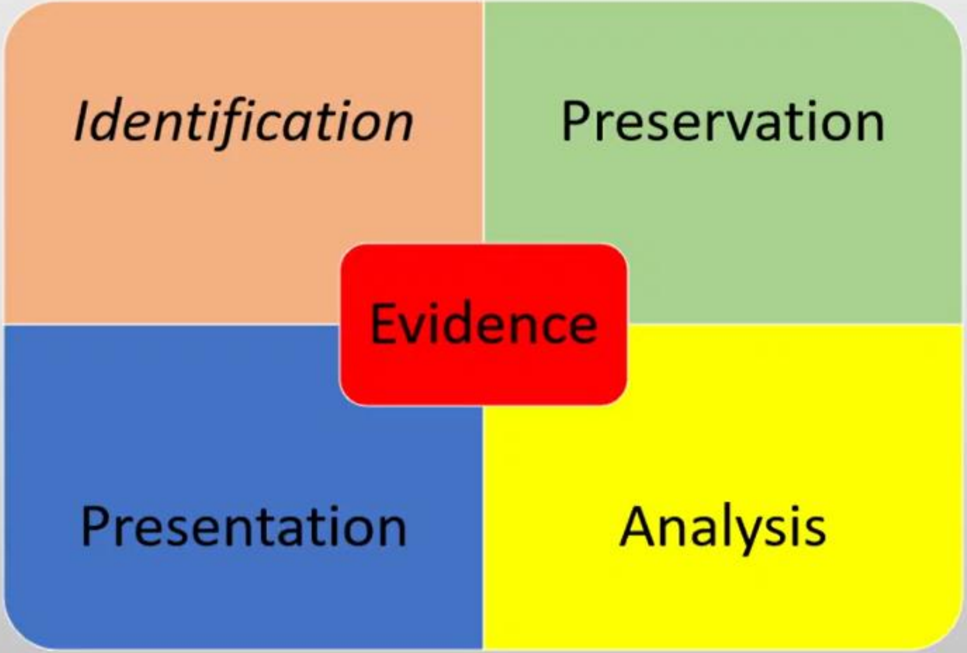
- Private Business
- Government
- Private Individuals

Cybercrime: Top 20 Countries



Cybercrime: Top 20 Countries

Phases of Digital Investigation



Identification

Preservation

Evidence

Presentation

Analysis

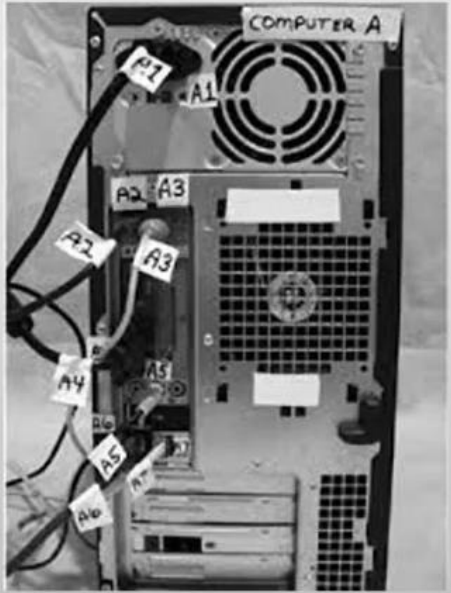
Identification

Identify and seize potential sources of digital device in a forensically sound manner

- Hardware
- Software
- Removable Media(s)
- Relevant Documents
- Password/Telephone Number
- Photographs

Identification

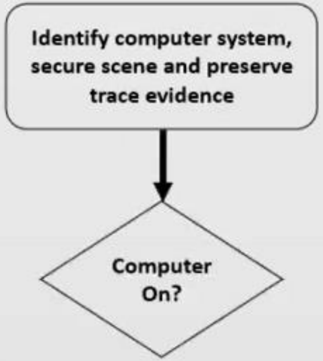
Identify and seize potential sources of digital device in a forensically sound manner



Identification

Identify computer system, secure scene and preserve trace evidence

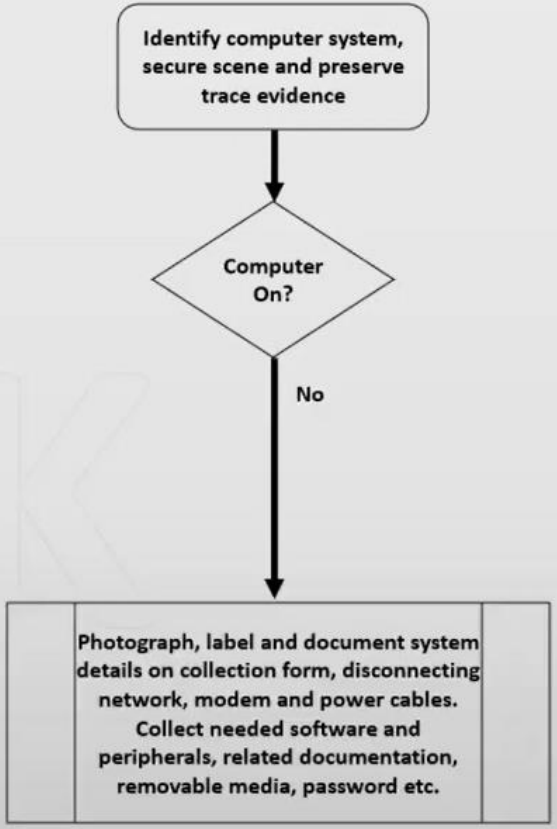
Identification



Identify computer system, secure scene and preserve trace evidence

Computer On?

Identification

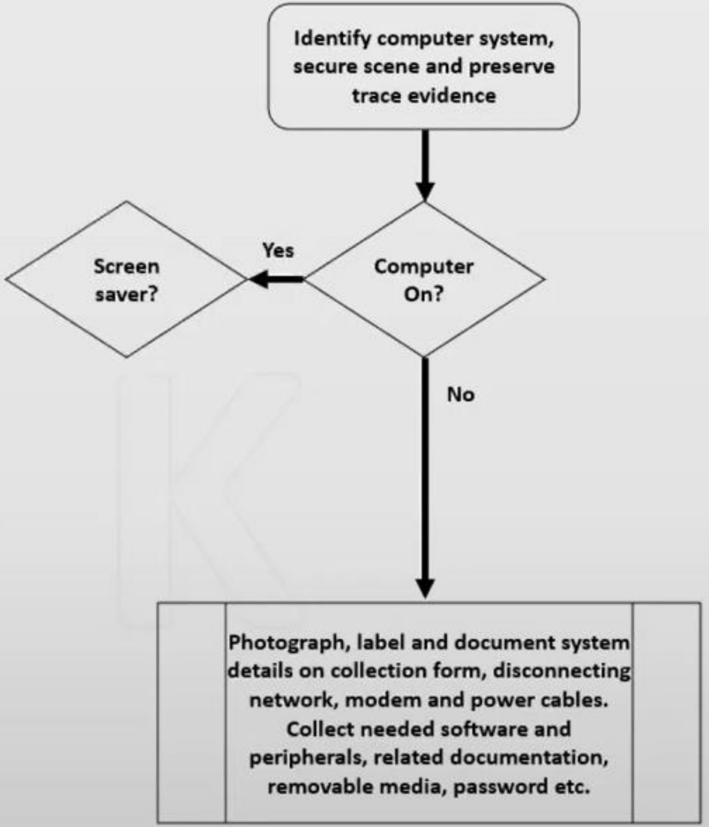

Identify computer system, secure scene and preserve trace evidence

Computer On?

No

Photograph, label and document system details on collection form, disconnecting network, modem and power cables. Collect needed software and peripherals, related documentation, removable media, password etc.

Identification


Identify computer system, secure scene and preserve trace evidence

Computer On?

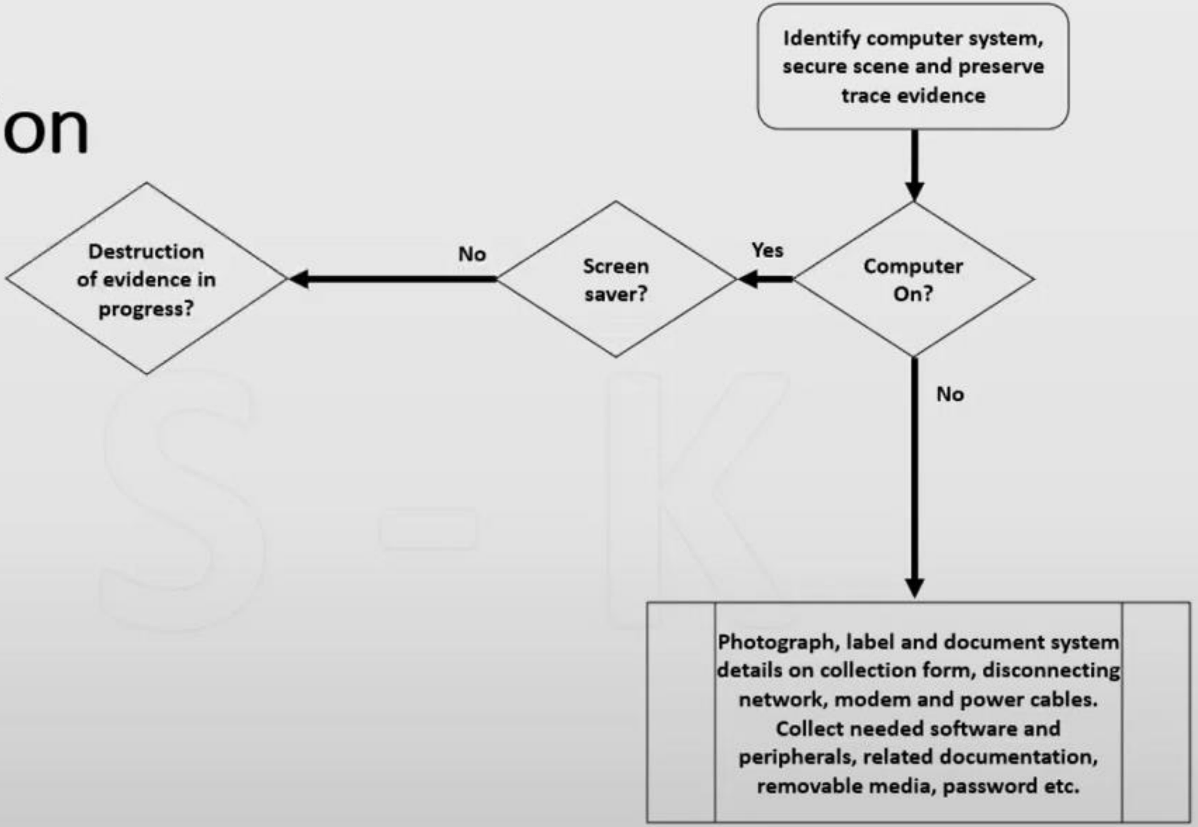
Yes

Screen saver?

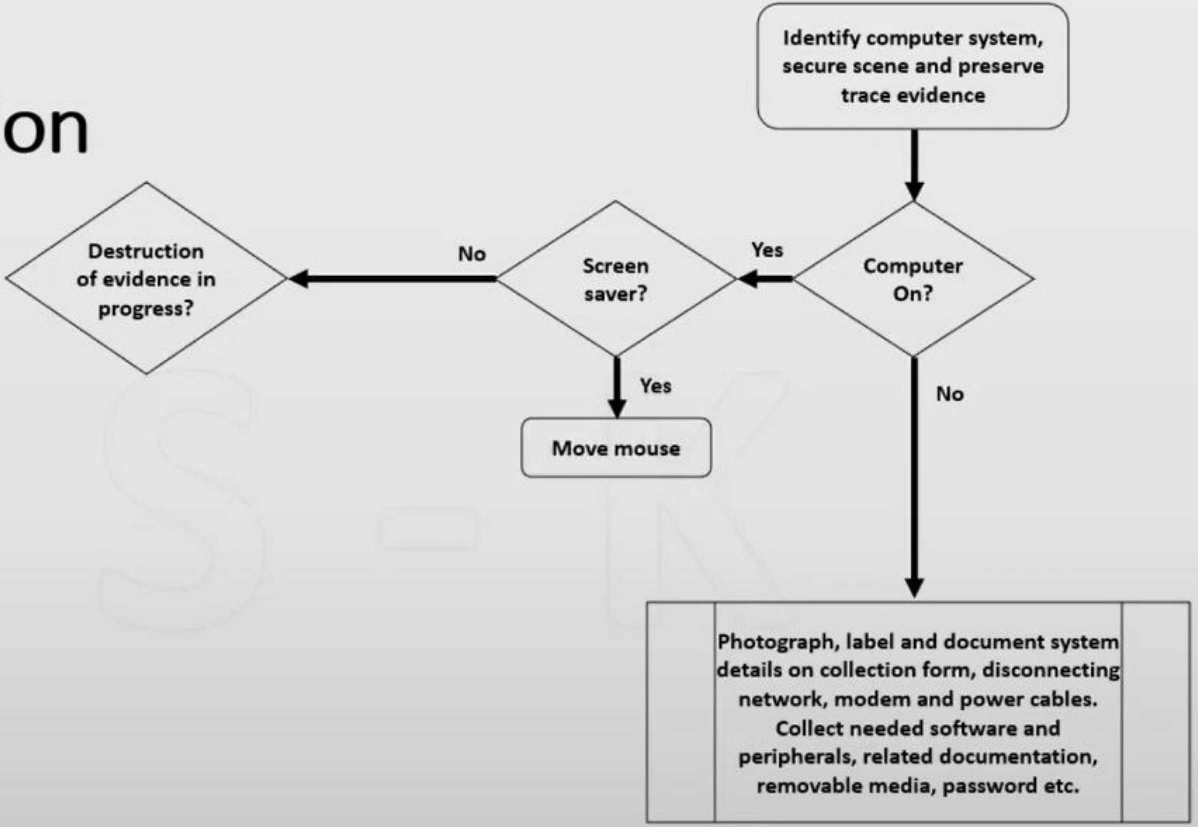
No

Photograph, label and document system details on collection form, disconnecting network, modem and power cables. Collect needed software and peripherals, related documentation, removable media, password etc.

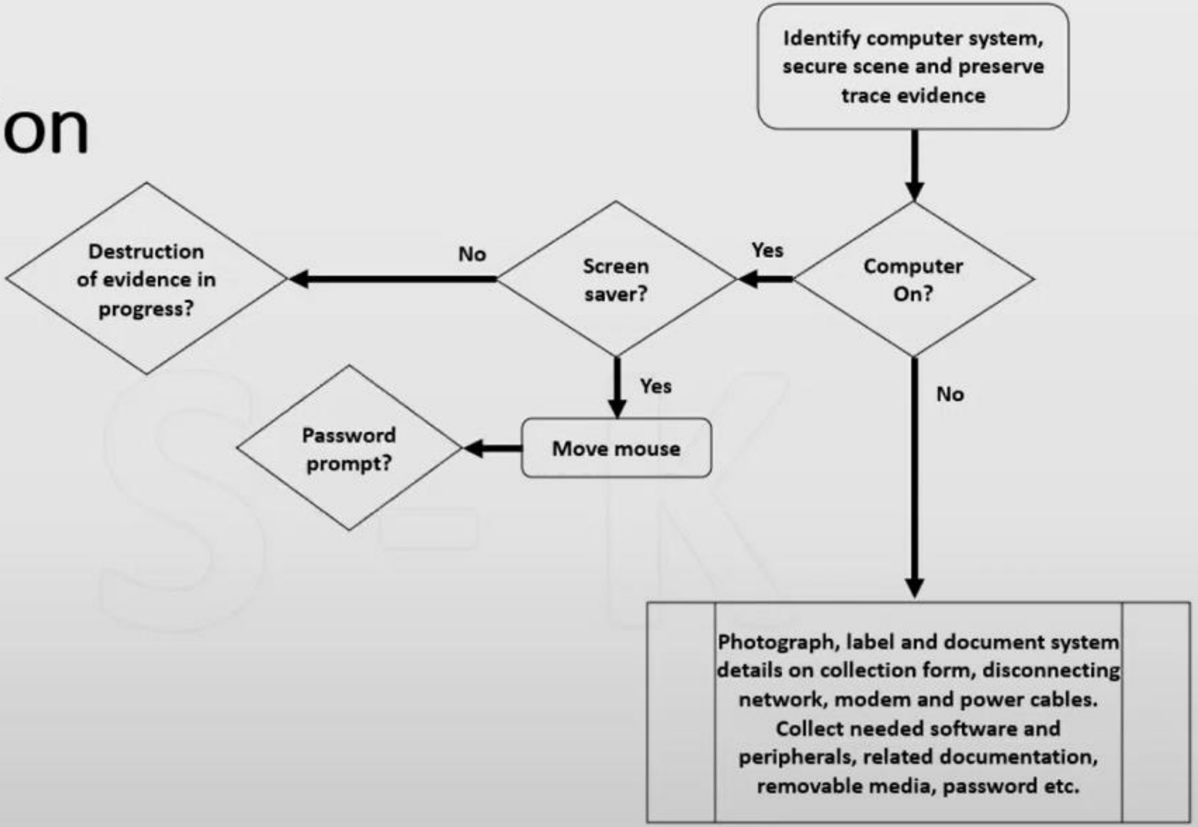
Identification


Identify computer system, secure scene and preserve trace evidence
Computer On?
Yes
Screen saver?
No
Destruction of evidence in progress?
No
Photograph, label and document system details on collection form, disconnecting network, modem and power cables. Collect needed software and peripherals, related documentation, removable media, password etc.

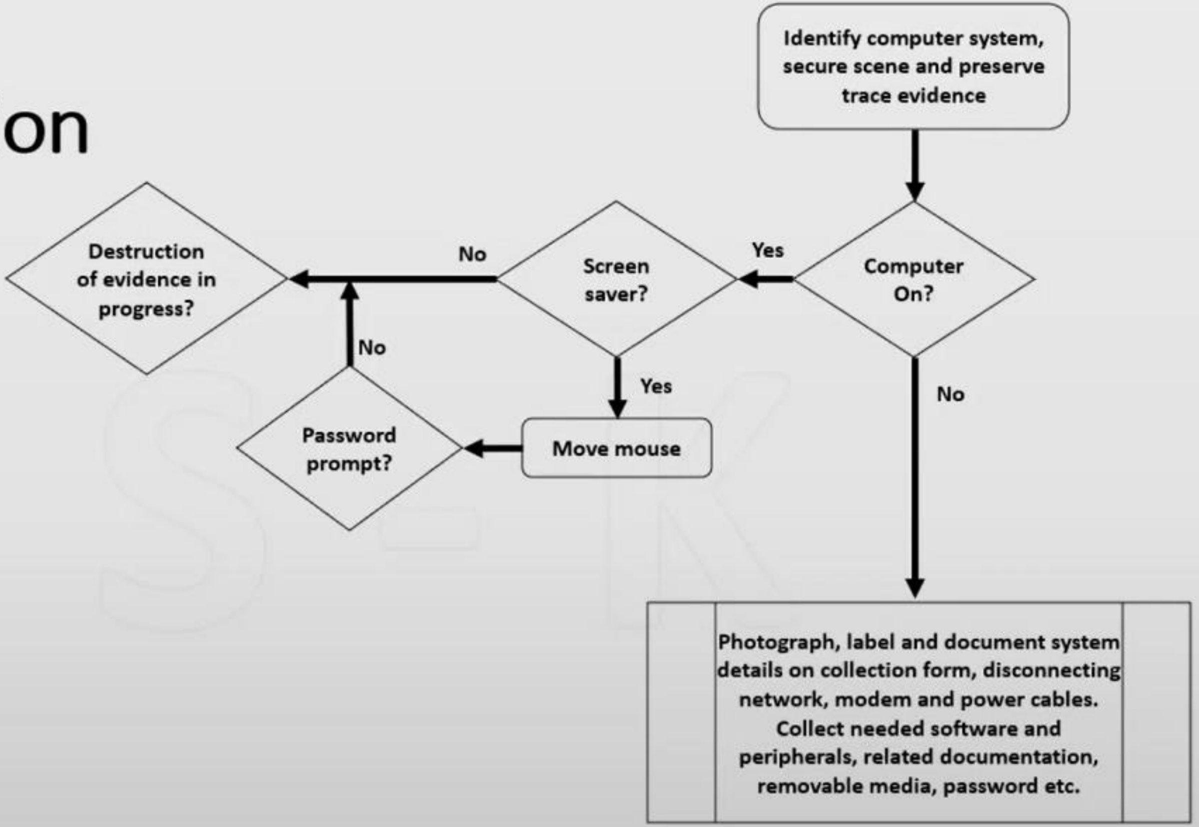
Identification


Identify computer system, secure scene and preserve trace evidence
Computer On?
Yes
Screen saver?
No
Destruction of evidence in progress?
Yes
Move mouse
No
Photograph, label and document system details on collection form, disconnecting network, modem and power cables. Collect needed software and peripherals, related documentation, removable media, password etc.

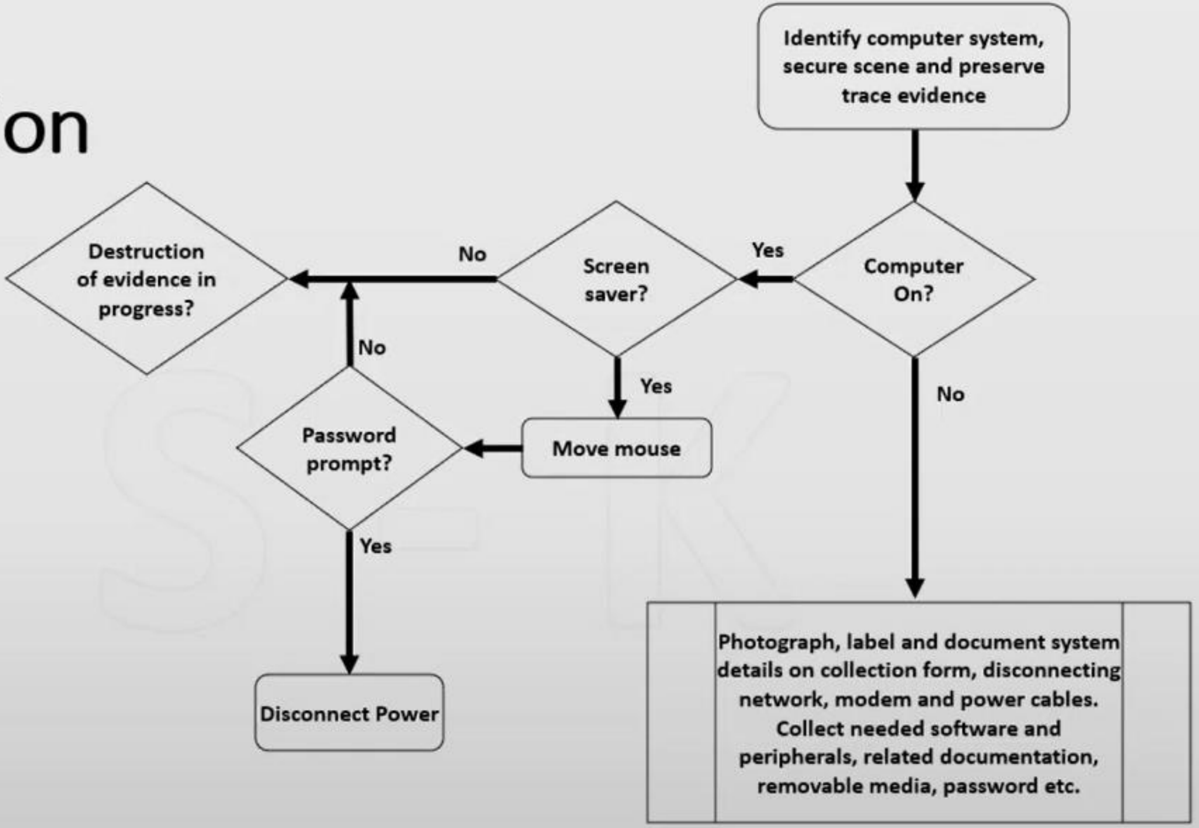
Identification


Identify computer system, secure scene and preserve trace evidence
Computer On?
Yes
Screen saver?
No
Destruction of evidence in progress?
Yes
Move mouse
Password prompt?
No
Photograph, label and document system details on collection form, disconnecting network, modem and power cables. Collect needed software and peripherals, related documentation, removable media, password etc.

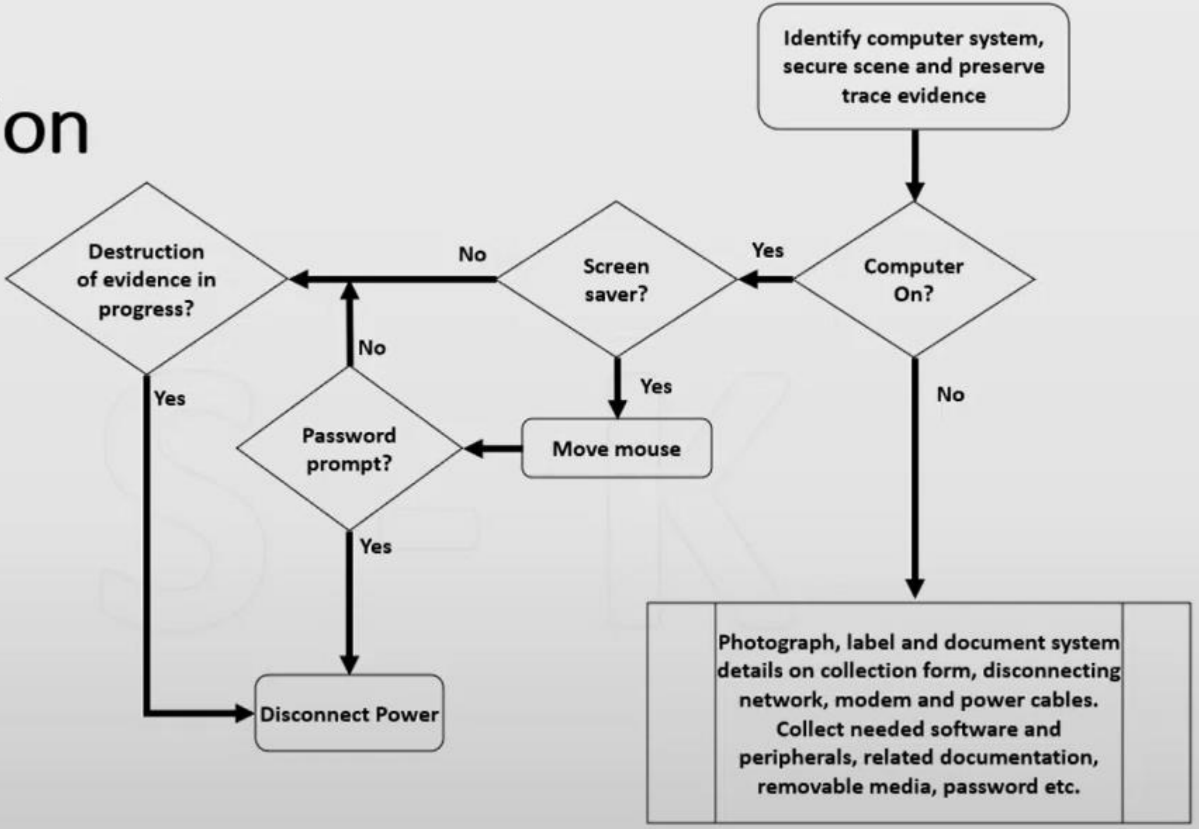
Identification


Identify computer system, secure scene and preserve trace evidence
Computer On?
Yes
Screen saver?
No
Destruction of evidence in progress?
Yes
Move mouse
Password prompt?
No
No
Photograph, label and document system details on collection form, disconnecting network, modem and power cables. Collect needed software and peripherals, related documentation, removable media, password etc.

Identification

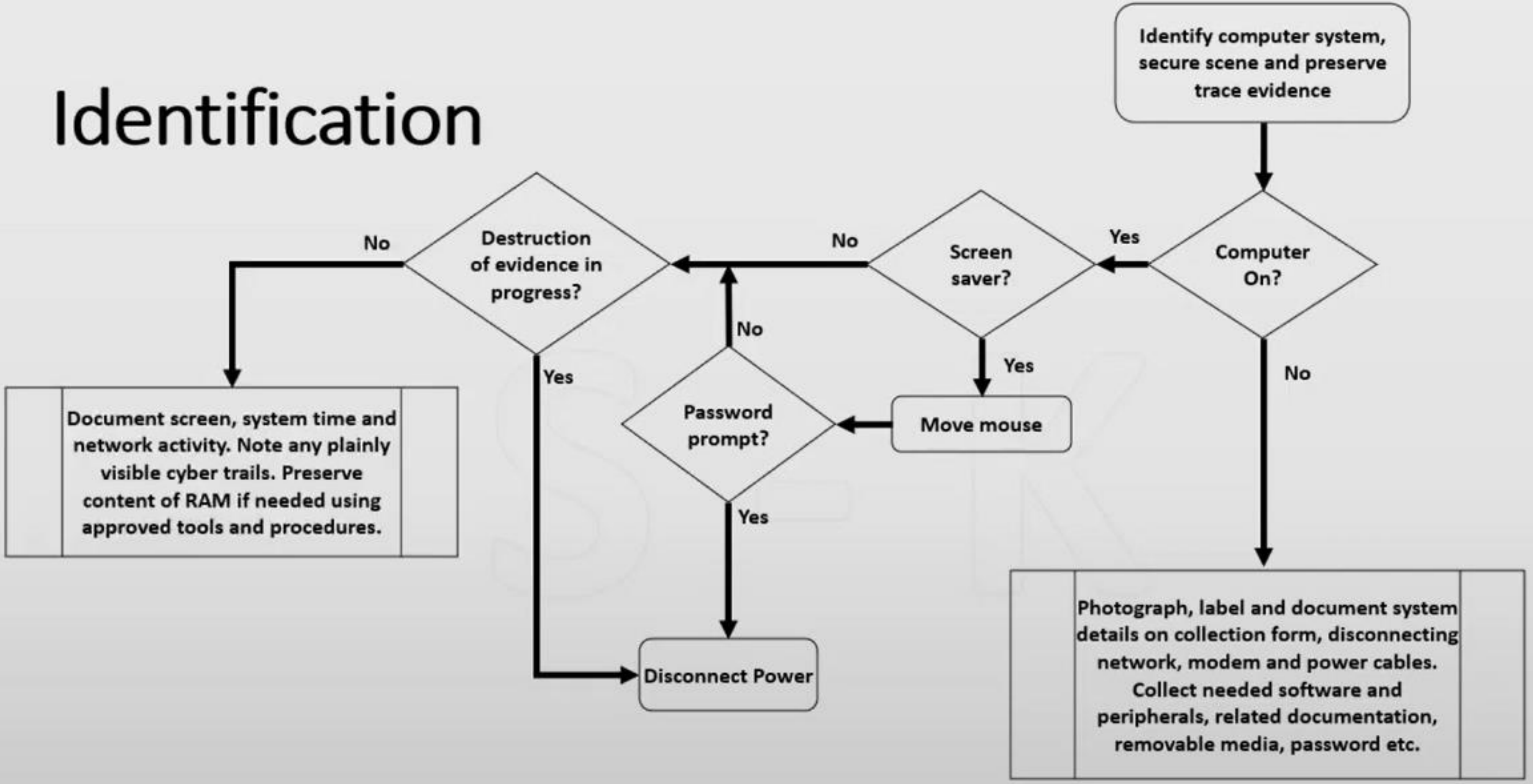

Identify computer system, secure scene and preserve trace evidence
Computer On?
Yes
No
Screen saver?
No
Yes
Destruction of evidence in progress?
Move mouse
Password prompt?
No
Yes
Disconnect Power
Photograph, label and document system details on collection form, disconnecting network, modem and power cables. Collect needed software and peripherals, related documentation, removable media, password etc.

Identification

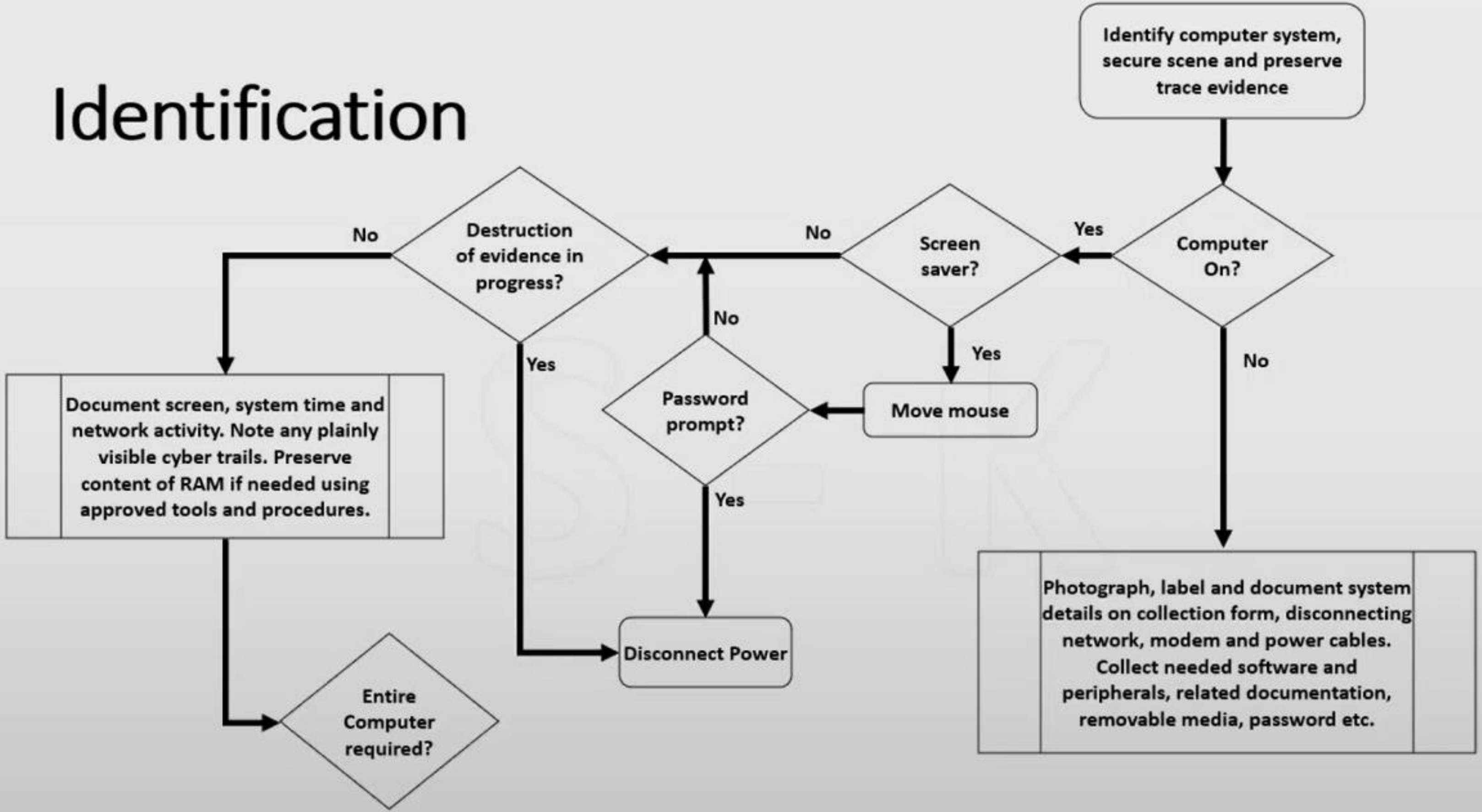


Identify computer system, secure scene and preserve trace evidence
Computer On?
Yes
Screen saver?
No
Destruction of evidence in progress?
Yes
Move mouse
Password prompt?
No
Yes
Disconnect Power
No
Photograph, label and document system details on collection form, disconnecting network, modem and power cables. Collect needed software and peripherals, related documentation, removable media, password etc.

Identification


Identify computer system, secure scene and preserve trace evidence
Computer On?
Yes
No
Screen saver?
No
Yes
Move mouse
Password prompt?
No
Yes
Destruction of evidence in progress?
No
Yes
Document screen, system time and network activity. Note any plainly visible cyber trails. Preserve content of RAM if needed using approved tools and procedures.
Disconnect Power
Photograph, label and document system details on collection form, disconnecting network, modem and power cables. Collect needed software and peripherals, related documentation, removable media, password etc.

Identification



Identify computer system, secure scene and preserve trace evidence

Computer On?

Yes

Screen saver?

No

Destruction of evidence in progress?

No

Document screen, system time and network activity. Note any plainly visible cyber trails. Preserve content of RAM if needed using approved tools and procedures.

Entire Computer required?

Yes

Disconnect Power

Yes

Move mouse

Password prompt?

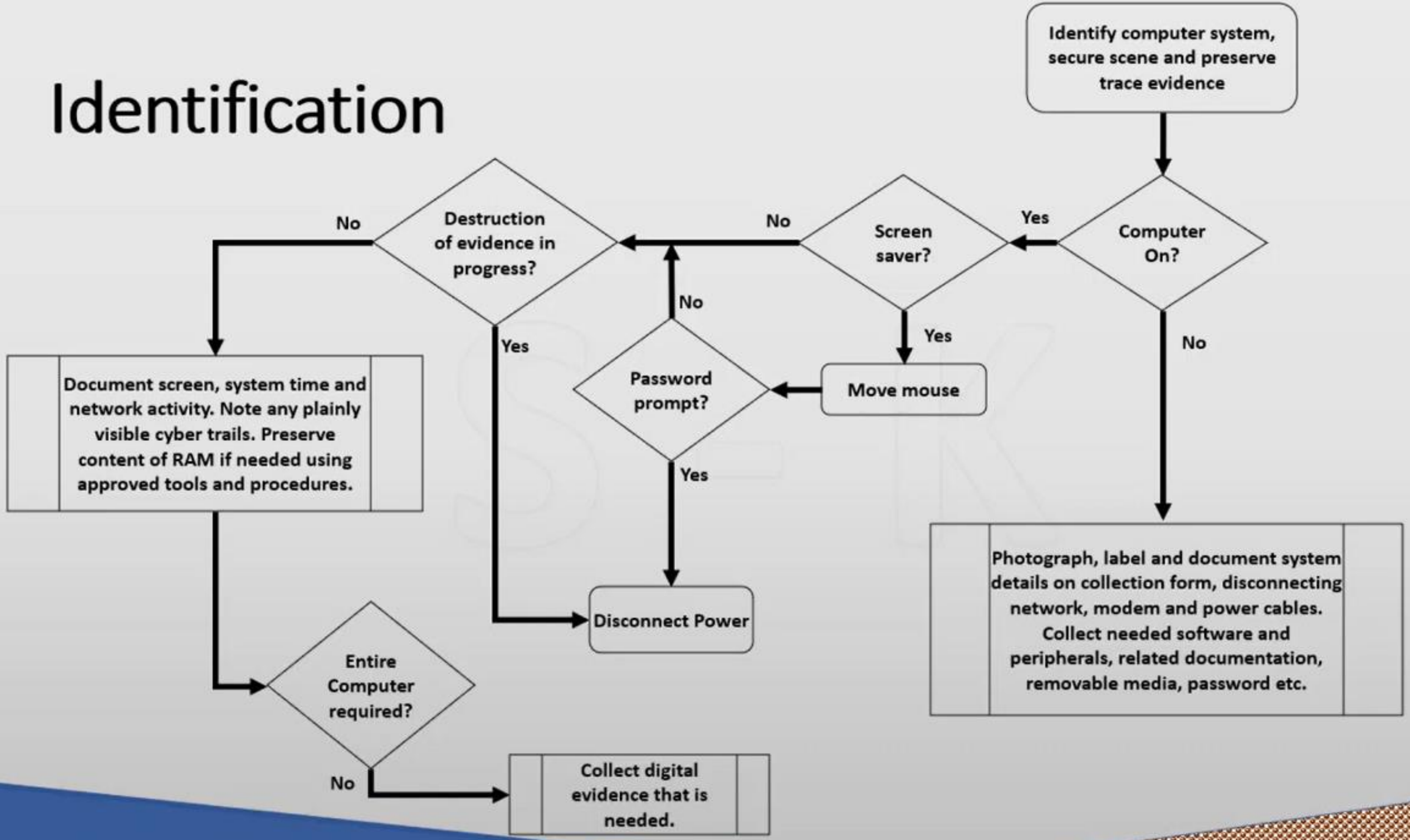
No

Yes

No

Photograph, label and document system details on collection form, disconnecting network, modem and power cables. Collect needed software and peripherals, related documentation, removable media, password etc.

Identification



Identify computer system, secure scene and preserve trace evidence

Computer On?

Screen saver?

Move mouse

Password prompt?

Destruction of evidence in progress?

Disconnect Power

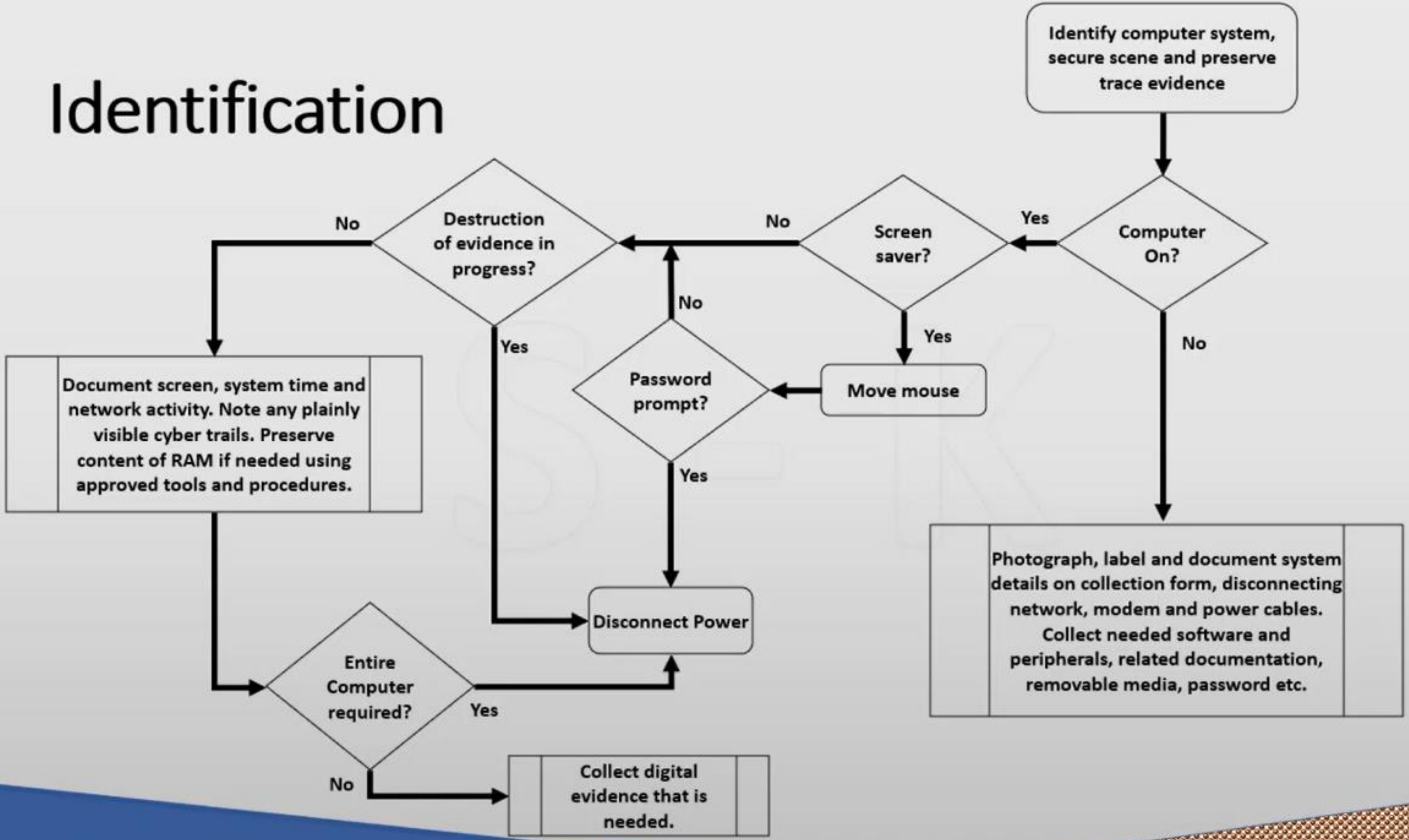
Document screen, system time and network activity. Note any plainly visible cyber trails. Preserve content of RAM if needed using approved tools and procedures.

Entire Computer required?

Collect digital evidence that is needed.

Photograph, label and document system details on collection form, disconnecting network, modem and power cables. Collect needed software and peripherals, related documentation, removable media, password etc.

Identification



Identify computer system, secure scene and preserve trace evidence

Computer On?

Screen saver?

Move mouse

Password prompt?

Destruction of evidence in progress?

Disconnect Power

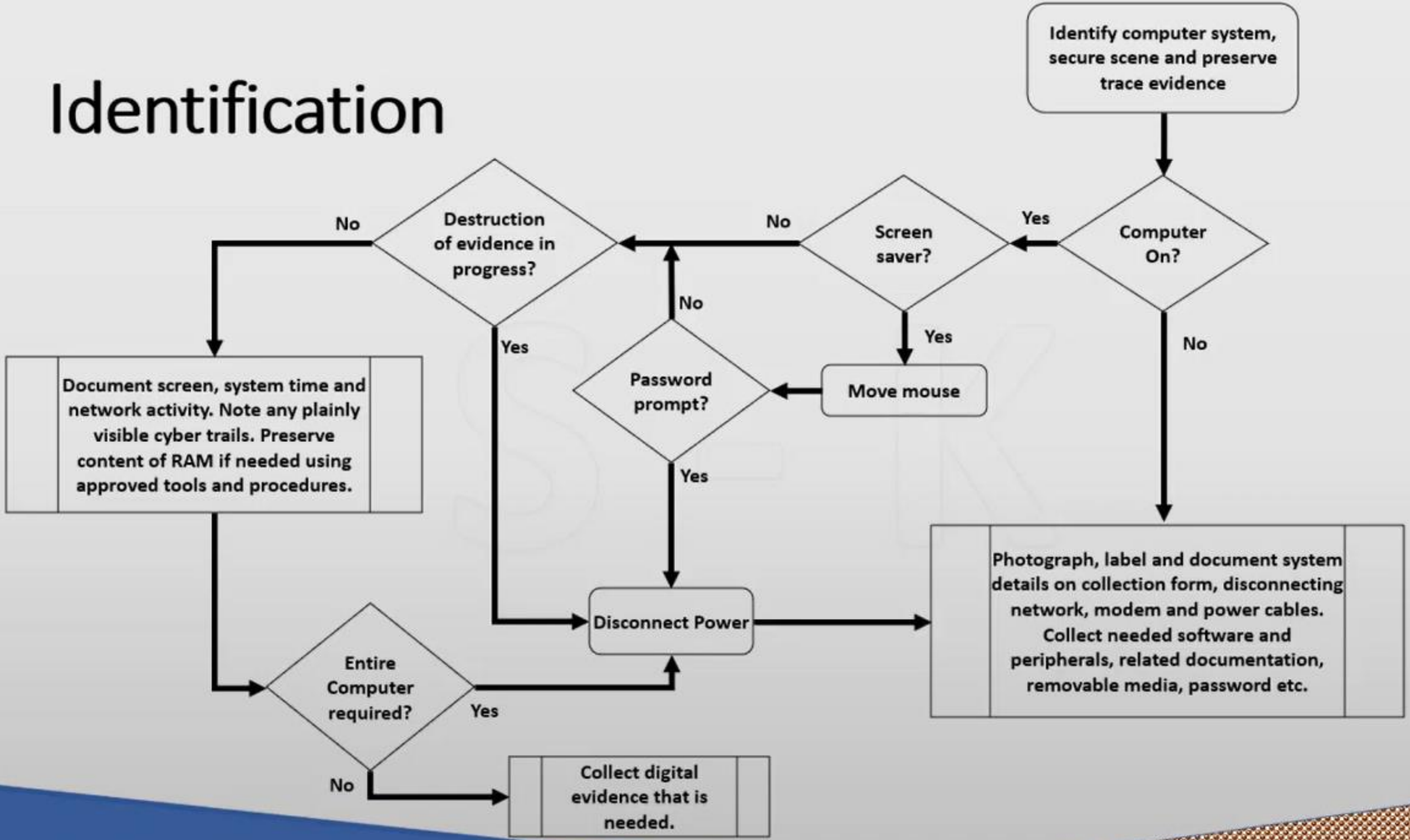
Document screen, system time and network activity. Note any plainly visible cyber trails. Preserve content of RAM if needed using approved tools and procedures.

Entire Computer required?

Collect digital evidence that is needed.

Photograph, label and document system details on collection form, disconnecting network, modem and power cables. Collect needed software and peripherals, related documentation, removable media, password etc.

Identification



Identify computer system, secure scene and preserve trace evidence

Computer On?

Yes

Screen saver?

No

Destruction of evidence in progress?

No

Document screen, system time and network activity. Note any plainly visible cyber trails. Preserve content of RAM if needed using approved tools and procedures.

Yes

Move mouse

Password prompt?

No

Yes

Yes

Disconnect Power

No

Photograph, label and document system details on collection form, disconnecting network, modem and power cables. Collect needed software and peripherals, related documentation, removable media, password etc.

Entire Computer required?

Yes

No

Collect digital evidence that is needed.

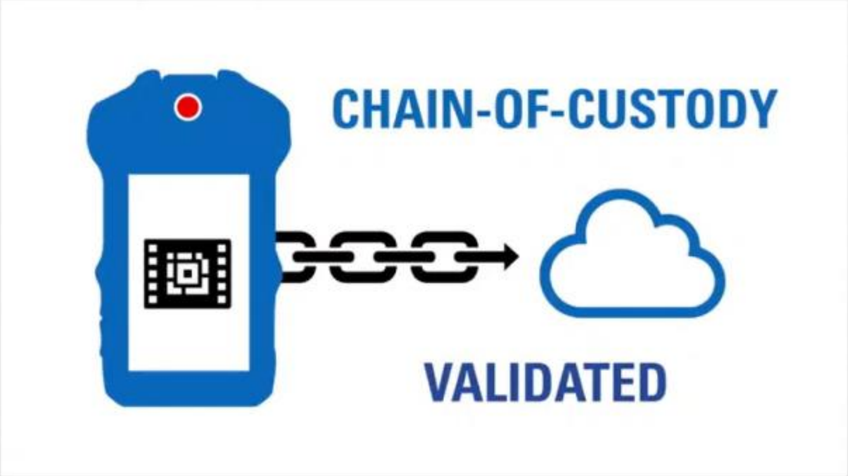
Preservation

- Bagging and tagging
- Secure storage
- Protect the evidence
- Forensic Duplication of evidence
- Calculate Hash (MD5, SHA-1)

Preservation

Chain of custody:

- Where, when, how, and by whom was the evidence
  - **discovered and collected**?
  - **handled or examined**?
  - **Transferred or shipped**?
- Who had **custody of the evidence?**
- How was it stored?



Analysis

- Longest phase
- Levels of Examination
- Preparation for Examination
- Often outsourced
- Apply a scientific method
- Preservation required also

Analysis

EC-council cites 4 ways a digital forensics investigator can use to analyse an evidence:

- Time-frame analysis
- Application and file analysis
- Ownership and possession analysis
- Data-hiding analysis

They are not necessarily performed in isolation during an investigation

Presentation

- A report containing a thorough and unbiased presentation of your findings.
- Must have a clear and logical structure
- Content:
  - Issues of relevance to the case
  - Provide evidence of the facts
  - State the source of the evidence
  - Opinions must be based on facts
  - The report must be understood by the court.