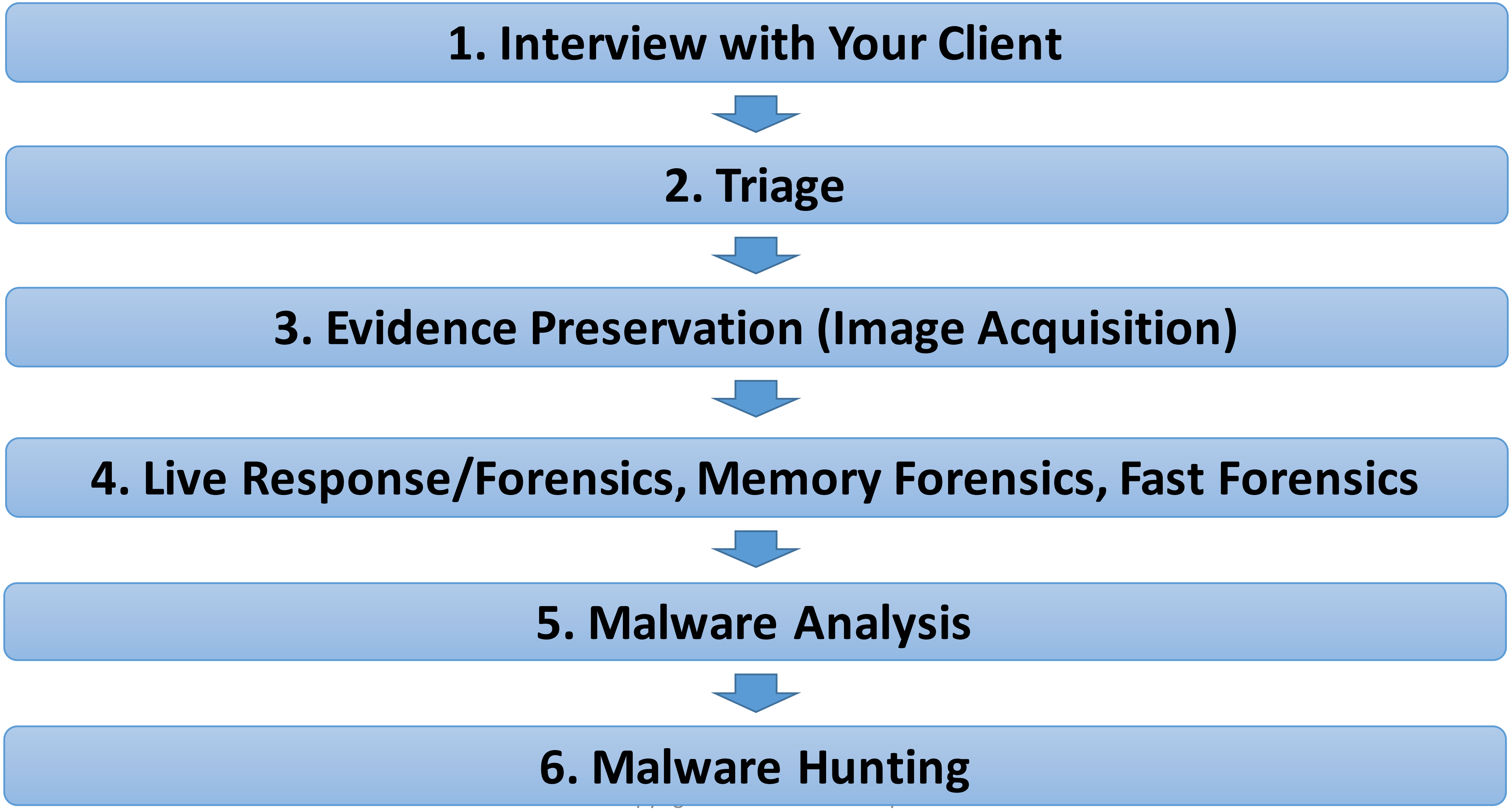
Initial Response
(First Response)

Initial Response (First Response)

- When a security incident occurs, the **<u>initial response</u>** (first response) becomes necessary.
- The amount of evidences that can be obtained for investigations may be affected by **<u>how quick</u>** the initial response is done.
  - Therefore, it is important to run through the initial response procedures as fast as possible.
- To run the procedures quickly, it is important to know appropriate method of the initial response.

Typical Initial Response Flow



1. Interview with Your Client

2. Triage

3. Evidence Preservation (Image Acquisition)

4. Live Response/Forensics, Memory Forensics, Fast Forensics

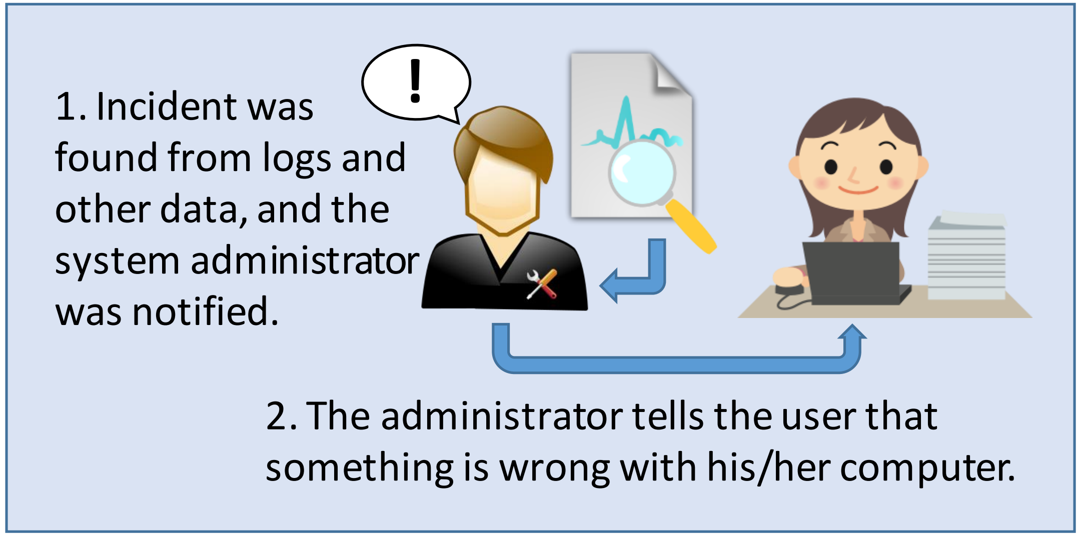
5. Malware Analysis

6. Malware Hunting

Step 1:
Interview with the Client

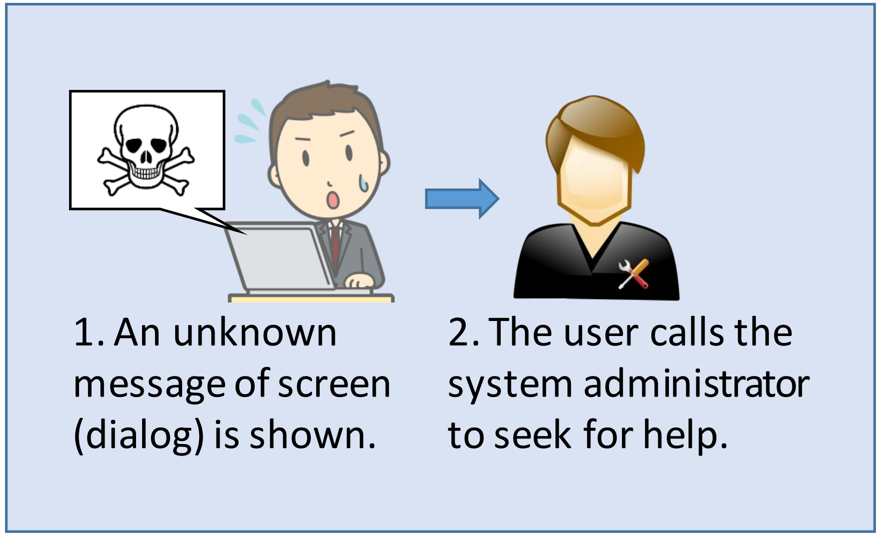
Interview with the Client

- There are several ways when an incident is discovered in an organization. Two example situations might be:



1. Incident was found from logs and other data, and the system administrator was notified.

2. The administrator tells the user that something is wrong with his/her computer.



1. An unknown message of screen (dialog) is shown.

2. The user calls the system administrator to seek for help.

- It is important to hear from the users about what has happened when the incident occurred.
  - The user may or may not noticed something being wrong.

Hearing Details

- Hear details from the users and build an investigation plan.
  - Questions to draw case details, such as:

What happened?

What is the current status?

How do you know the current status is right?

What is being observed?

  - System and network details
    - Software version, patch status, operations, etc…
    - System operators’ and users’ operation histories

Considerations for Hearing

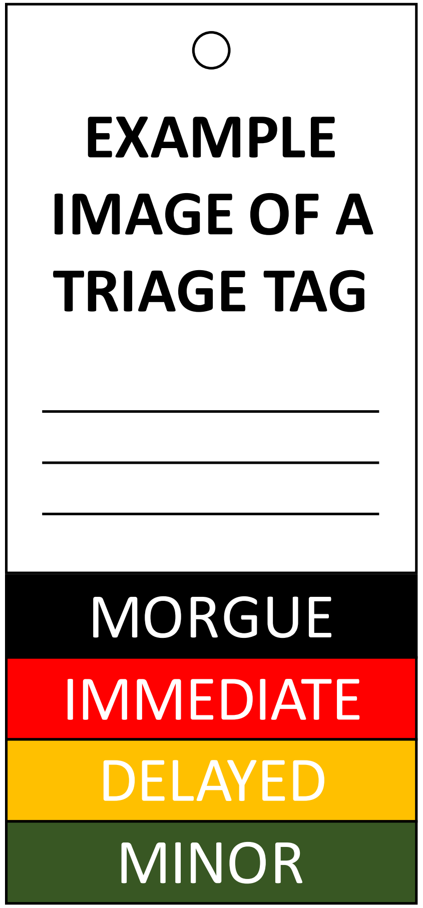
- Note that you should not believe every single witnesses. Use them as a consideration, as there might be cases where:
  - he/she is intentionally or unintentionally hiding inappropriate details
  - he/she doesn’t remember details

- “***Trust but verify***” *– Ronald Reagan, December 1987*
  - It is okay to trust the users. However, make sure that what they are saying make sense.

Step 2:
Triage

Triage – Terminology

- Based on the interviews, triage is necessary.
- Triage is:
  - A medical terminology for determining priority of patients based on their conditions, when there are emergencies such as a large-scale disaster or an accident.
  - In an incident response, triage is to select the host(s) that should be investigated based on the interview and the knowledge about the incident.



EXAMPLE IMAGE OF A TRIAGE TAG

MORGUE

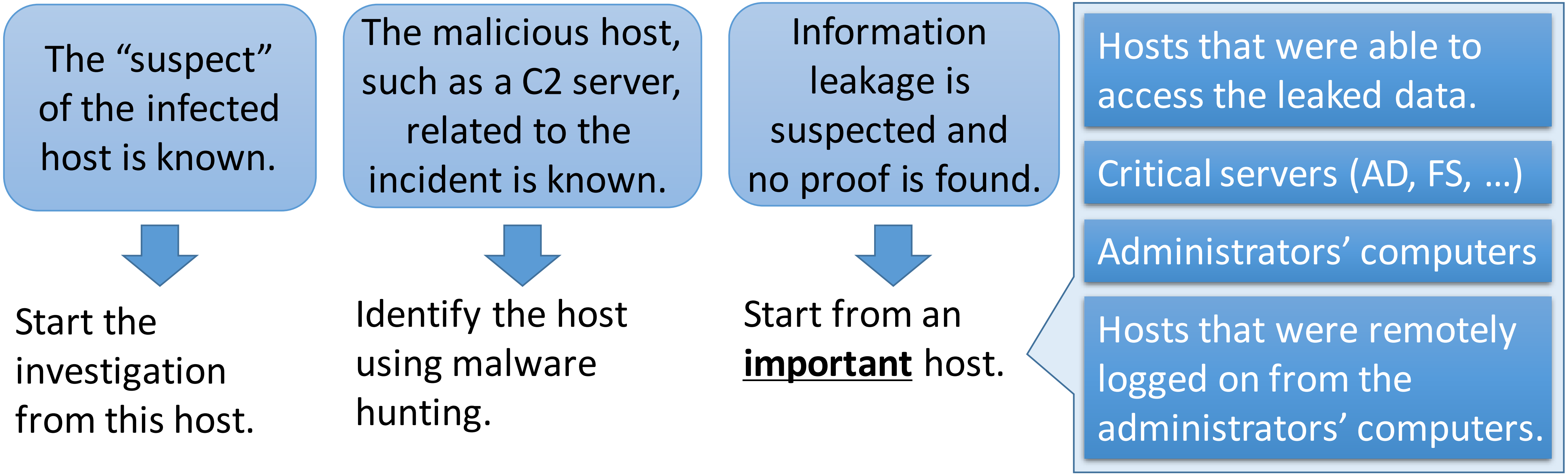
IMMEDIATE

DELAYED

MINOR

Triage Procedures

The procedure should be determined based on the facts that are known when the incident was discovered.



The "suspect" of the infected host is known.

Start the investigation from this host.

The malicious host, such as a C2 server, related to the incident is known.

Identify the host using malware hunting.

Information leakage is suspected and no proof is found.

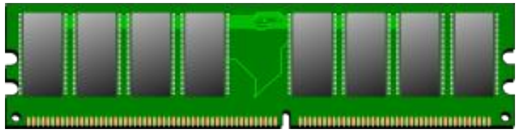
Start from an **<u>important</u>** host.

- Hosts that were able to access the leaked data.
- Critical servers (AD, FS, …)
- Administrators' computers
- Hosts that were remotely logged on from the administrators' computers.

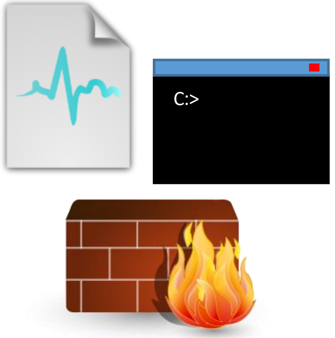
Step 3:
Evidence Preservation
(Image Acquisition)

Evidence Preservation (Image Acquisition)

- When the triage is completed, start preservation.
  - We will focus on acquisition in the next chapter.
- Volatile artifacts such as memory are first. Then acquire other artifacts.
- In computer forensics, these three steps are taken:



1. Memory acquisition



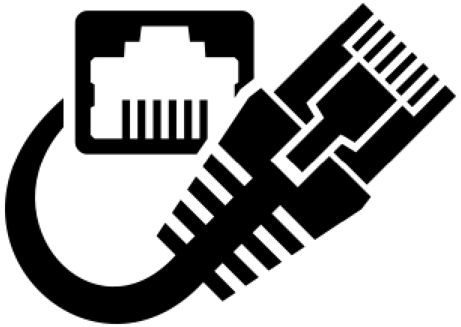
2. Triaged artifacts acquisition

3. Disk acquisition

While Obtaining Evidences…

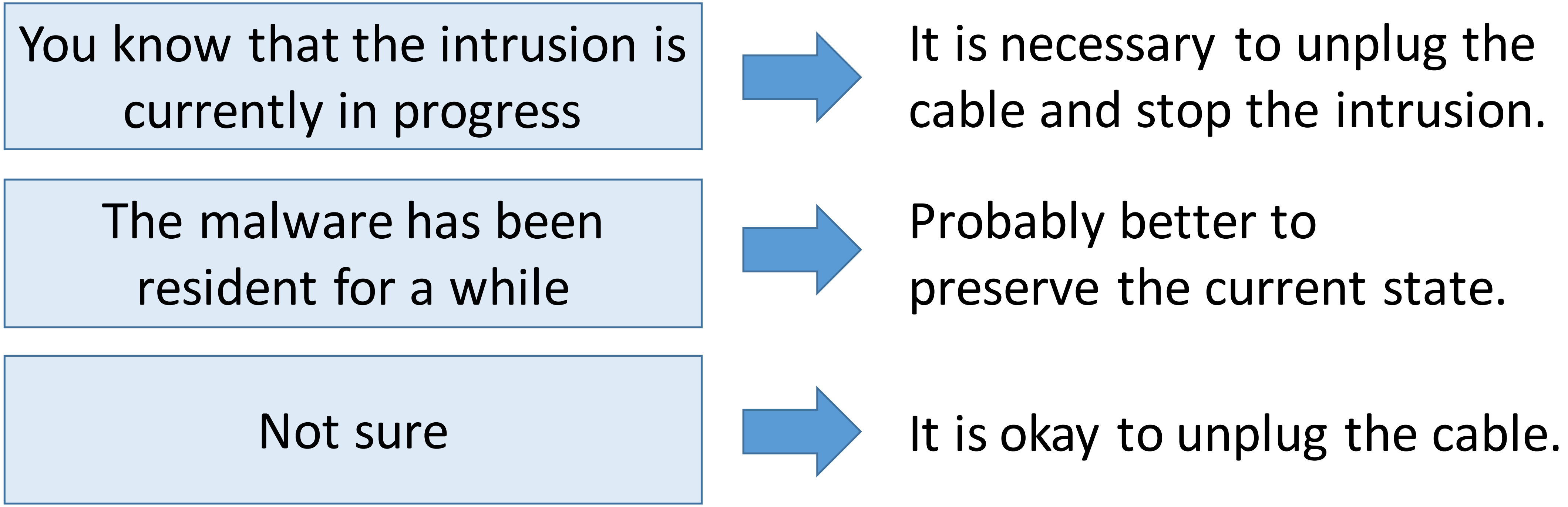
- To obtain sufficient evidences, it is important to keep modifications of the hosts **<u>as small as possible</u>**.

- Some security analysts **<u>might</u>** instruct users to unplug network cables when an infection is found.



Network Cables and Acquisitions

- Unplugging network cables **will** change memory contents, so it is necessary to think about if it is appropriate or not.



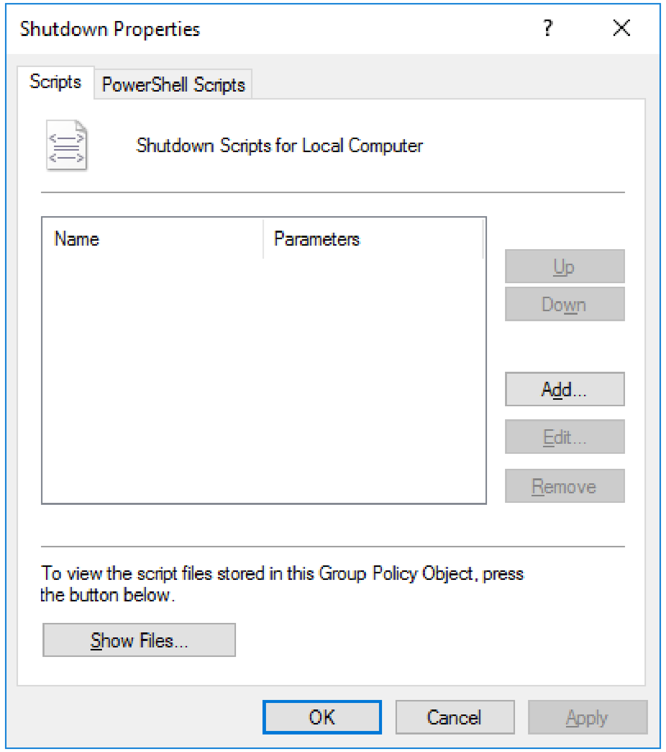
You know that the intrusion is currently in progress → It is necessary to unplug the cable and stop the intrusion.

The malware has been resident for a while → Probably better to preserve the current state.

Not sure → It is okay to unplug the cable.

Power Cables and Acquisitions

- Some might say that the power cable should be unplugged to terminate the machine without shutdown procedure, to avoid the shutdown procedure from being executed.
    - The malware might use “logoff script” and/or “shutdown script” to add another malware or to remove evidences.
- On the other hand, if the machine was shutdown inappropriately, the file system (data, journals, metadata, etc…) and/or the physical disk might break.



Shutdown Properties

Shutdown Scripts for Local Computer

To view the script files stored in this Group Policy Object, press the button below.

Handling Cables

- For both network and power cables, either method is okay.
  - It’s the matter of policies.
- It is important to plan the base guidelines **before** an actual incident happens.

Step 4:
Live Response (Live Forensics), Memory Forensics, Fast Forensics

Live Response/Forensics, Memory Forensics, Fast Forensics

- Live Response/Forensics
  - After the volatile data, such as memory, is preserved, run a quick search on the suspected machine to determine malware or run the forensic on a running machine.

- Memory Forensics
  - Using an acquired memory image, you can perform similar analysis to live response/forensics to find out malware quickly.

- Fast Forensics
  - After acquired important artifacts with triaged acquisition from a disk, you can perform quick forensics.

Step 5:
Malware Analysis

Malware Analysis

- After finding out malware, you can perform rapid malware analysis by checking and executing malware to get IoCs (Indicator of Compromise) rapidly.
  - Surface Analysis
  - Dynamic Analysis

Step 6:
Malware Hunting

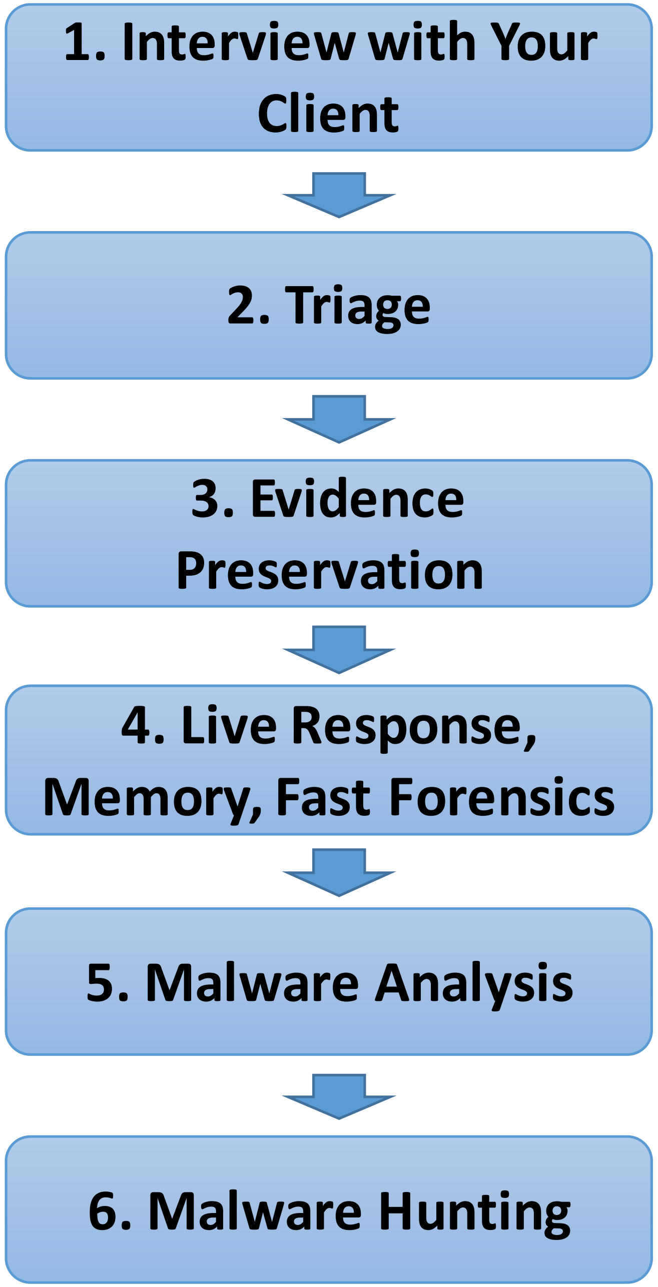
Malware Hunting

- Network Forensics
    - After getting IoCs, you can perform network forensics such as:
        - Network Device Log Analysis (Proxy, Firewall, Router…)
        - Packet Capture Data Analysis
        - Hunting malware with I[DP]S and/or network forensics products
- Large-Scale Response
    - You can check other computers remotely at once with remote live response tools such as EDR products, GRR or osquery.
- They are to find out other infected hosts with the IoCs.

Summary

Summary

- When a security incident occurs, the **initial response** becomes necessary.
- The amount of evidences that can be obtained for investigations may be affected by **how quick** the initial response is done.
- Steps of the initial response are in the right figure.
- The initial response needs to be done appropriately.
  - Plan the base guidelines **before** an actual incident happens.


1. Interview with Your Client
2. Triage
3. Evidence Preservation
4. Live Response, Memory, Fast Forensics
5. Malware Analysis
6. Malware Hunting