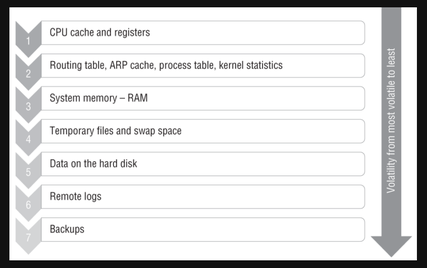
Conducting Digital Forensics

Acquiring Forensic Data



It lists down the data by how likely it's to be volatile the higher the data up the list the more volatile it is. Thus, unless there is a special event the list should be followed from top to bottom when collecting the data

The order of volatility

CPU cache and registers are rarely directly captured as part of a normal forensic effort.

Most investigations do not need this level of detail.

When capturing data in level 2 it's important to remember that the capturing happens only for the moment of capturing meaning that If events occurred in the past, this data may not reflect the state that the system was in when the event occurred.

The content of random access memory (RAM) can be very helpful for both investigations and incident response. As it might have important data that aren't written into the disk

Files and data on a disk change more slowly but are the primary focus of many investigations. It is important to capture the entire disk, rather than just copy files so that you can see deleted files and other artifacts that remain resident.

The operating system itself can contain useful information. The Windows registry is a common target for analysis since many activities in Windows modify or update the registry.

Devices such as smartphones or tablets may contain data that can also be forensic targets.

Firmware is a less frequently targeted forensic artifact, but knowing how to copy the firmware from a device can be necessary if the firmware was modified as part of an incident or if the firmware may have forensically relevant data.

Snapshots from virtual machines are an increasingly common artifact that forensic practitioners must deal with.

Network traffic and logs can provide detailed information or clues about what was sent or received, when, and via what port and protocol amongst other useful details.

Artifacts like devices, printouts, media, and other items related to investigations can all provide additional useful forensic data.

Chain of custody documentation

Chain of custody forms are simple sign-off and documentation forms.

Each time the drive, device, or artifact is accessed, transferred, or otherwise handled, it should be documented

Case Number: _____ Item Number:_____
Evidence Description: _____
_____
_____
Collection method:_____
_____
Evidence storage method: _____
How is evidence secured? _____
Collected by: (Name/ID#) _____
Signature of collector:_____

Copy History

Date	Copied method	Disposition of original and all copies

Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

FIGURE 15.2 A sample chain of custody form

Cloud Forensics

On-site forensics have made up the bulk of traditional forensic work. However, the widespread move to cloud services has created new challenges for forensic analysts.

Right-to-audit clauses

It's a part of the contract between the cloud service provider and the organization

Provides either a direct ability to audit the cloud provider or an agreement to use a third-party audit agency.

Auditing is the comprehensive analysis and review of an IT infrastructure

Regulatory and jurisdiction concerns

Regulatory requirements may vary depending on where the cloud service provider operates and where it is headquartered.

The law that covers your data, services, or infrastructure may not be the laws that you have in your own locality, region, or country.

Cloud providers often have sites around the world, and data replication and other services elements mean that your data or services may be stored or used in a similarly broad set of locations.

Organizations that have significant concerns about this typically address it with contractual terms.

Sometimes also using technical controls such as handling their own encryption keys to ensure that they know if the data is accessed.

Data Breach Notification

Data breach notification laws, like other regulatory elements, also vary from country to country

Contracts often cover the maximum time that can elapse before customers are notified, and ensuring that you have an appropriate breach notification clause in place that meets your needs can be important.

These considerations mean that acquiring forensic data from a cloud provider is unlikely.

Network Forensics

Network forensics have an increasingly large role to play.

Because network data changes quickly, it's important to have solid capturing and logging methods in advance

If network traffic isn't actively being logged, forensic artifacts like firewall logs, IDS and IPS logs, email server logs, authentication logs, and other secondary sources may provide information about when a device was on a network, what traffic it sent, and where it sent the traffic.

When forensic examiners do work with network traffic information, they will frequently use a packet analyzer like Wireshark to review captured network traffic.

Other Sources

Virtual Machines

Unlike a server, desktop, or laptop, a virtual machine is often running in a shared environment where removal of the system would cause disruption to multiple other servers and services.

Imaging the entire underlying virtualization host would include more data and systems than may be needed

A virtual machine snapshot will provide the information that forensic analysts need and can be captured and then imported into forensic tools

Containers

Containers have grown significantly in use and create new challenges for forensic examiners.

Since containers are designed to be ephemeral, and their resources are often shared, they create fewer forensic artifacts than a virtual or physical machine.

Container forensics require additional planning, and forensic and incident response tools are becoming available to support these needs.