

A decorative graphic consisting of thin, grey, stylized circuit lines with small circles at the ends, extending horizontally from the left and right sides of the central black box.



# INFORMATION SECURITY INTRODUCTION

HAUTE-ÉCOLE LÉONARD DE VINCI

CHAPTER 7 – DIGITAL FORENSICS



# CHAPTER 7

- 7.1 Concepts
  - 7.2 Conducting Digital Forensics
  - 7.3 Acquiring Forensics Data
  - 7.4 Acquisition Tools
  - 7.5 Analysis
  - 7.6 Reporting
  - 7.7 Intelligence
- 
- 

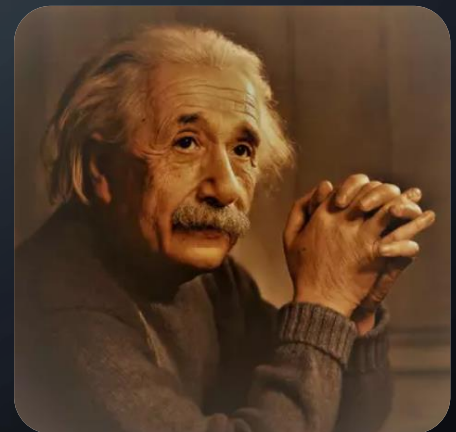


## CHAPTER 7

- What is digital forensics ?
- What are the process to follow ?
- How is it performed ?
- What tools are used ?

*Condemnation without investigation is the height of ignorance.*

- Albert Einstein



A decorative graphic consisting of thin, grey, stylized circuit lines with small circles at the ends, extending horizontally from the left and right sides of the central black box.

# 7.1 CONCEPTS

## 7.1 DEFINITION

Digital forensics is the investigation and analysis tools and techniques to determine what happened on a system or device.

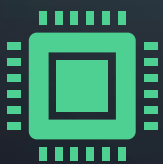
Digital forensics may be carried out to respond to legal holds or as part of an incident response process.

Digital forensics has, also, a role to play in intelligence and counterintelligence efforts.

## 7.1 CONCEPTS

A key element of digital forensics is the **acquisition** and **analysis** of digital forensics data.

Data can be in the form of drives, files, copies of live memory, and any of the other multitude of digital artifacts that we create in the normal process of using computers and networks.



## 7.1 CONCEPTS

Since forensics information can be found in many different places, planning forensic information gathering is crucial to having a complete and intact picture of what occurred.

Gathering that forensics data is just the start of a process that involves careful documentation and detailed analysis.

Throughout the process, the creation of documentation is necessary to properly identified what happened.



## 7.1 CONCEPTS

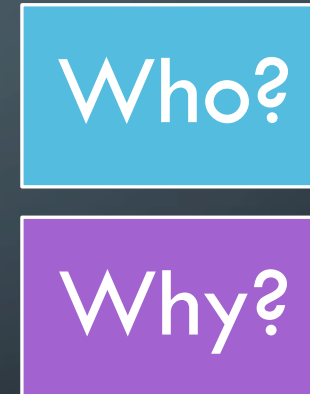
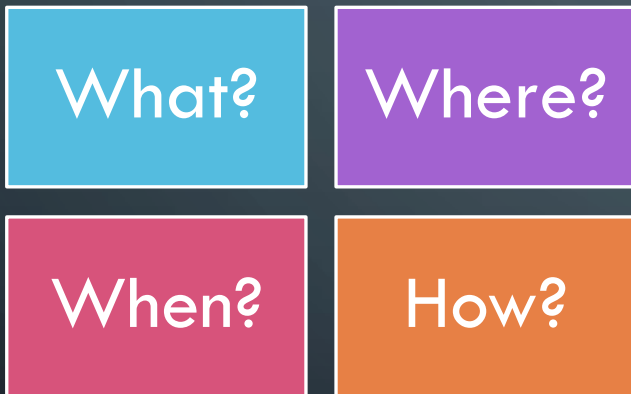
The human side of digital forensics is also very important; interview with individuals can provide important clues.

It means that technical forensics expert must have a technological knowledge but also a human behaviors knowledge to complete their forensic efforts.



## 7.1 CONCEPTS

The question that digital forensic analyst will try to answer are:



The "Who?" And "Why?" are answered by the overall investigation process of which digital forensics is only a part!

A decorative graphic consisting of thin, grey, stylized circuit lines with small circles at the ends, extending horizontally from the left and right sides of the central black box.

## 7.2 CONDUCTING DIGITAL FORENSICS

## 7.2 CONDUCTING DIGITAL FORENSICS

The U.S. National Institute of Justice identifies the following three principles that should guide every investigation:

### Integrity

- Action taken to secure and collect digital evidence should NOT AFFECT the integrity of that evidence.

### Experience

- Persons conducting an examination of digital evidence should be trained for that purpose.

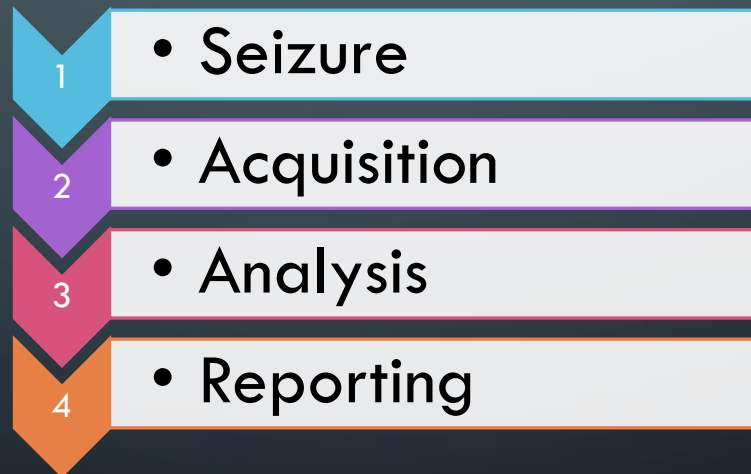
### Process

- Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review.

## 7.2 PHASE OF AN INVESTIGATION

Like many other things, a digital forensics can be conducted in phases.

We normally recognize 4 phases:



## 7.2 SEIZURE

The goal of seizure is to ensure that neither the perpetrators nor the investigators make any change to the evidence.

An excellent example of protecting evidence is putting up the yellow "Crime Scene" tape.



## 7.2 SEIZURE

Controlling the crime scene is of high importance. Some of the steps that should take place to protect the scene are:

1. Allow only authorized individuals access to scene.
2. Ensure that each person involved in technical tasks is trained and certified for his/her role
3. Document who is present at the crime scene
4. Document who last interacted with the systems.
5. If the crime scene becomes contaminated, document it. The contamination may not negate the derived evidence, but it will make investigation harder.

## 7.2 SEIZURE

After having secured the area and documented the environment, you can prepare to begin acquiring data.

This involves:

- Collecting evidence at the scene
- Unplug electronic device
- Photograph the scene and individual elements
- Properly label and inventory everything
- Antistatic bag everything
- Transport during appropriate weather condition (no extreme temperatures, snow or rain)



## 7.2 CHAIN OF CUSTODY

A *chain of custody* is a document history that shows how evidence was handled, collected, transported and preserved at every stage of the process.

Because digital evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence has not been tampered with and is trustworthy.

The chain of custody process should follow evidence through its entire lifecycle, from identification to destruction, archiving or return to owner.



## APPLIED TECHNICAL SERVICES, INCORPORATED

1190 Atlanta Industrial Drive Marietta, GA 30066 (770) 423-1400 Fax (770) 424-6415 e-mail fire@atslab.com

### EVIDENCE TRANSMITTAL

Date: \_\_\_\_\_ Verbal Report To: \_\_\_\_\_

Phone #: \_\_\_\_\_

Submitted By: \_\_\_\_\_ Written Report To: \_\_\_\_\_

File #: \_\_\_\_\_ Invoice To: \_\_\_\_\_

Insured: \_\_\_\_\_

Claim Number: \_\_\_\_\_

Date of Loss: \_\_\_\_\_

ATS Reference # \_\_\_\_\_

Description of Evidence: Container, Size Type of  
Material, Condition of Material (burned or unburned)

Location Collected

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_

4. \_\_\_\_\_

5. \_\_\_\_\_

6. \_\_\_\_\_

Special Instructions: \_\_\_\_\_

### Chain of Evidence (Signature Required)

From: \_\_\_\_\_ To: \_\_\_\_\_ Date: \_\_\_\_\_ Time: \_\_\_\_\_

From: \_\_\_\_\_ To: \_\_\_\_\_ Date: \_\_\_\_\_ Time: \_\_\_\_\_

From: \_\_\_\_\_ To: \_\_\_\_\_ Date: \_\_\_\_\_ Time: \_\_\_\_\_

From: \_\_\_\_\_ To: \_\_\_\_\_ Date: \_\_\_\_\_ Time: \_\_\_\_\_

ATS 800 (10/99)

Professional Engineers

Design • Consulting • Testing and Inspection

Members in AAFS, ACS, ASM, ASME, ASNT, ASQC, ASTM, AWS, FSCT, IAAI, NACE, NCSL, NFPA, SAFS  
GEORGIA SOCIETY OF PROFESSIONAL ENGINEERS, NATIONAL SOCIETY OF PROFESSIONAL ENGINEERS

A decorative graphic consisting of thin, grey, stylized circuit lines with small circles at the ends, extending horizontally from the left and right sides of the central text box.

## 7.3 ACQUIRING FORENSICS DATA

## 7.3 ACQUIRING FORENSICS DATA

*Forensics acquisition* is the process of extracting digital content from seized evidence so that it may be analyzed.

This is commonly known as "*taking forensic image of a hard drive*" but it actually involves more than just that.

The main reason you extract the data is to conduct your analysis on a copy of the data evidence and **NOT** on the original; this protects the original content from changes, to ensure that it can be used later as evidence.

Preserving the integrity of the original evidence is PARAMOUNT.

## 7.3 ACQUIRING FORENSICS DATA

To acquire the original digital evidence in a manner that protects and preserves it, the following steps are considered best practice:

### Prepare the destination media

- Secure any media on which you will store evidence (USB/HD/SD/SAN/NAS). Wipe the media by overwriting it with a fixed pattern of 1's and/or 0's.

### Prevent changes to the original

- The simple act of attaching a device to a computer will normally cause its content to change in small but potentially significant ways. You must use write-protection mechanism such as hardware write-blocker.

### Hash the original evidence

- Before you copy anything, you should take a cryptographic hash of the original evidence. MD5 or SHA-1 are admissible. The best is to have multiple hash algorithm used.

### Copy the evidence

- Specific applications exists to make forensics copy of digital media. The dd utility on Linux systems. A copy of the files is insufficient, the complete image bit to bit is necessary to retrieve deleted or unallocated spaces.

### Verify the acquisition

- After the copy is complete, compare the cryptographic hash of the copy against the original. If they match, you can perform analyses of the copy and be assured that it is perfectly identical to original.

### Safeguard the original evidence

- Now that a perfect copy of the evidence is done, you must store the original in a safe place and ensure that no one gain access to it.

## 7.3 ACQUIRING FORENSICS DATA

Acquiring data must be done in a specific order! All data do not have the same order of volatility.

The order of volatility documents what data is most likely to be lost due to system operations or normal process being executed on the computer.

We will gather information from the most volatile to the least volatile.

Unless there is a compelling and immediate reason to differ, the following list is of application.

## 7.3 DATA VOLATILITY

- 1 • CPU cache and registers
- 2 • Routing table, ARP cache, process table, kernel statistics
- 3 • System memory -RAM
- 4 • Temporary files and swap space
- 5 • Data on the hard disk
- 6 • Remote logs
- 7 • Backups



## 7.3 DATA VOLATILITY

CPU cache and registers: are rarely directly captured as part of normal forensic effort. Although it's possible to capture some of this information using specialized hardware or software, most investigations do not need this level of detail. The CPU cache and registers are constantly changing as processing occurs, making them very volatile.

Process table, Kernel statistics, ARP cache: are ephemeral data and can be captured through a combination of memory disk acquisition. It's important to remember that the capture will be of the moment in time when the acquisition is done.

## 7.3 DATA VOLATILITY

Random Access Memory: can be very helpful for both investigations and incident response. Memory can contain encryption keys, ephemeral data from applications, and information that may not be written on the disk.

Swap and pagefile: is the disk space used to supplement physical memory. Much like capturing information from RAM, capturing the swap and pagefile can provide insight into running processes.

## 7.3 DATA VOLATILITY

Files and data: 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.

Remote logs and backup: are defined to be specifically not changed so no particular actions need to be taken here.

## 7.3 ACQUIRING FORENSICS DATA

Let's not forget also:

- Smartphone or tablets
- Firmware can also be targeted and contains forensics data
- Virtual Machine snapshot
- Network traffic logs
- Printers

## 7.3 CLOUD

On-site forensics can be quite straightforward as everything is at disposal but what about the Cloud?

Well... new challenges ahead but, basically, 3 concepts:

Right to audit  
clauses

Regulatory  
and  
Jurisdiction

Data breach  
notification

## 7.3 RIGHT TO AUDIT CLAUSES

A right to audit clauses is part of the contract between the cloud service and an organization.

A right to audit clause provides either a direct ability to audit the cloud provider or an agreement to use a third-party audit agency.

Many cloud providers use standard contracts and may not agree right-to-audit clauses for smaller organizations.

In those cases, they may instead provide access to regularly updated third-party audit statements.

## 7.3 REGULATORY AND JURISDICTION

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

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

Local jurisdiction may claim rights to access that data with a search warrant or other legal instrument. This might be something you do not want to face as a company with sensitive information.

## 7.3 DATA BREACH NOTIFICATION

Data breach notification also vary from country to country and in the USA even from state to state.

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.

Some vendors delay for days, weeks or even months, potentially causing significant issues for customers who are unaware of the breach.



## 7.3 CLOUD

All these above points mean that acquiring forensics data from a cloud provider is unlikely.

You may recover data from logs or from systems and infrastructure but forensic data from the service itself is rarely handed over to customers.

A decorative graphic consisting of thin, grey, stylized circuit lines with small circles at the ends, extending horizontally from the left and right sides of the central black box.

## 7.4 ACQUISITION TOOLS

## 7.4 ACQUISITION TOOLS

Windows most famous acquisition tools:

- FTK Imager: <https://www.youtube.com/watch?v=OUORBch0zaE>
- WinHex:

Linux most famous acquisition tool:

- dd

To copy a drive mounted as `/dev/sda` to a file called `forensics.img` you can execute:

```
dd if=/dev/sda of=forensics.img bs=4k conv=noerror,sync
```

## 7.4 FTK IMAGER

FTK Imager is a free tool for creating forensic images. It supports physical drives, logical drives, image files, folders, multi-CD/DVD volumes and live memory on a system.

FTK Imager is widely used by forensics team as it also generates reports of the acquisition performed, making work easier.

FTK Imager RAM dump: <https://www.youtube.com/watch?v=1OxR4KLj-4I>

Under Linux the Volatility framework is able to do a RAM dump.

## 7.4 NETWORK TOOLS

The most famous tool to gather and investigates network traffic are the widely known:

- Wireshark
- tcpdump



A decorative graphic consisting of thin, grey, stylized circuit lines with small circles at the ends, extending horizontally from the left and right sides of the central black box.

## 7.5 ANALYSIS

## 7.5 ANALYSIS

Analysis is the process of interpreting the extracted data to determine its significance to the case.

Examples of the types of analysis that may be performed include the following:

- **Timeframe:** *What happened and when?*
- **Data hiding:** *What has been intentionally concealed?*
- **Applications and files:** *Which applications accessed which files?*
- **Ownership and possession:** *Which user accounts accessed which applications and files?*

## 7.5 ANALYSIS

One of the most important tools to a forensic analyst is the **TIMELINE** which establishes a basis for comparing the state of the system at different points in time.

The timeframe provides a chronologically ordered list of actions taken on the system, which can be categorized as read, write, modify, delete operations.

At each step of the process, you should take copious notes on each specific action you take, down to the command and parameters you use.



## 7.5 ANALYSIS

Sometimes you may face only partial file information and it's important to use every information at disposal.

Have you ever heard of "Magic-bytes"?

Common files format have signature that clearly identify them. Looking at the first few bytes is often enough to know which type of files it is.

## 7.5 MAGIC-BYTES

File Type	Signature
DOS Executable	0x4D 0x5A
ELF Executable	0x7F 0x45 0x4C 0x46
Zip archive	0x50 0x4B 0x03 0x04
PNG Image	0x89 0x50 0x4E 0x47 0x0D 0x0A 0x1A 0x0A
BMP Image	0x42 0x4D
...	...

[https://en.wikipedia.org/wiki/List\\_of\\_file\\_signatures](https://en.wikipedia.org/wiki/List_of_file_signatures)

## 7.5 BINARY ANALYSIS



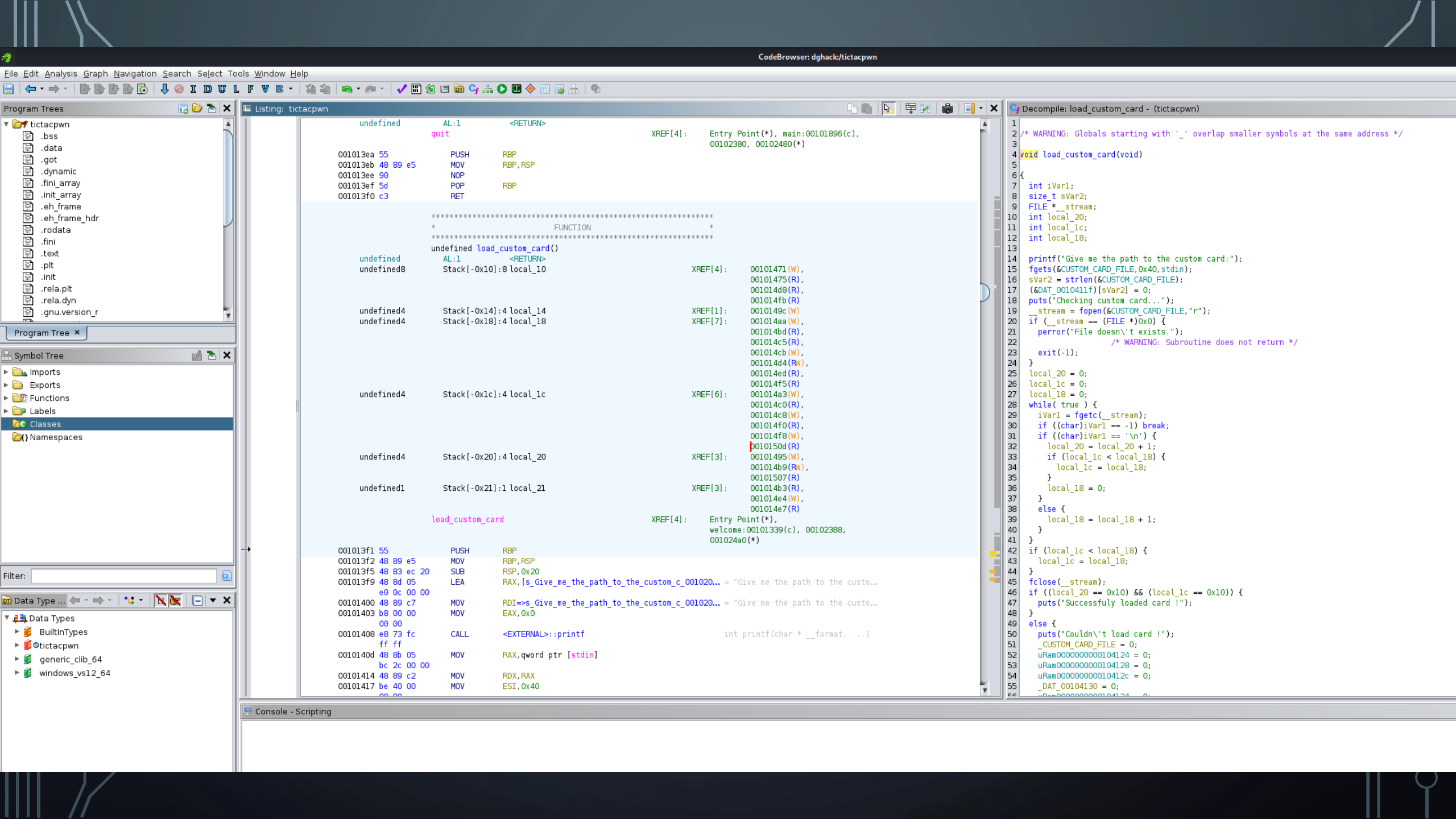
**GHIDRA**

## 7.5 BINARY ANALYSIS

Ghidra is a free and open-source reverse engineering tool, decompiler and debugger developed by the NSA. It has been released in March 2019.

Ghidra used to be a classified tool of the NSA and first public revelation around this tool goes back to March 2017.

It's written in Java and uses Swing framework for the GUI.



A decorative graphic consisting of thin, grey, stylized circuit lines with small circles at the ends, extending horizontally from the left and right sides of the central black box.

## 7.6 REPORTING

## 7.6 REPORTING

The analysis of digital artifacts and evidence is important to the forensic process, the report that is produced at the end is the key product.

Reports need to be useful and contain the relevant information without delving into every nuance and detail that the analyst may have found during the investigation.



## 7.6 REPORTING

A typical forensic report will include:

- 1 • A summary of the forensic investigation and findings.
- 2 • An outline of the forensic process, including tools used and any assumptions that were made about the tools or process.
- 3 • A series of sections detailing the findings for each device or drive. Accuracy is critical when findings are shared, and conclusions must be backed up with evidence and appropriate detail.
- 4 • Recommendation and conclusions in more detail than the summary included.



This Appendix contains examples of 24 forms that may be useful in documenting the various stages of forensic investigations. Use of the forms and the level of detail captured will depend on the specific investigation, the level of detail required, and the level of information needed for implementing the findings. These forms can be modified to suit specific agency requirements (Microsoft Word® fillable forms and instructions on how to modify them are included in the attached CD at the end of the report).

The forms and the section in the guide in which they are referred to are:

- Form #1: Forensic Investigation Request (Section 3.1)
- Form #2: Preliminary Investigation (Sections 3.5.1 and 3.5.2)
- Form #3: Decision to Proceed (Section 3.5.3)
- Form #4: Preliminary Investigation Report (Section 3.6)
- Form #5: Forensic Investigation Team (Section 4.1)
- Form #6: Pre-Investigation Site Visit (Section 4.2)
- Form #7: Photograph Record (Section 4.2)
- Form #8: Visual Assessment Form (Asphalt/Surface Treatment) (Section 4.2.1)
- Form #9: Visual Assessment Form (Portland Cement Concrete) (Section 4.2.1)
- Form #10: Initial Non-Destructive Testing Plan (Section 4.2.4.4)
- Form #11: Initial Forensic Investigation Plan (Section 4.4)
- Form #12: Interim Report Cover Sheet (Section 5.3)
- Form #13: Final Non-Destructive Testing Plan (Section 6.1)
- Form #14: Destructive Testing Plan (Section 6.1)
- Form #15: Final Forensic Investigation Plan (Section 6.1)
- Form #16: Forensic Investigation Site Report (Section 7.2.1)
- Form #17a: Core Log (Single Core) (Section 7.3.1.2)
- Form #17b: Core Log (Multi Core) (Section 7.3.1.2)
- Form #18: Test Pit Profile (Sections 7.3.2.2 and 7.3.2.3)
- Form #19a: Asphalt Concrete/Asphalt Surface Treatment Layer Log (Section 7.3.2.2)
- Form #19b: Portland Cement Concrete Layer Log (Section 7.3.2.2)
- Form #20: Gravel and Stabilized Layer Log (Section 7.3.2.2)
- Form #21: Sample Log (Section 7.3.2.4)
- Form #22: Density and Moisture Content (Section 7.3.2.4)
- Form #23: Dynamic Cone Penetrometer (Section 7.3.2.6)
- Form #24: Final Report Cover Sheet (Section 8.2)

Examples of selected forms are provided for Case #2 in Appendix B.

A decorative graphic consisting of thin, grey, stylized circuit lines with small circles at the ends, extending horizontally from the left and right sides of the central black box.

## 7.7 INTELLIGENCE

## 7.7 INTELLIGENCE

Although digital forensics is primarily used in organizations for legal cases, internal investigations.

Digital forensics also plays a role in both strategic intelligence and counterintelligence efforts. The ability to analyze adversary actions and technology, including components and behaviors of advanced persistent threat tools and process, has become key tool in the arsenal for national defense and intelligence...

Many of the tools seen in this chapter are actually used by intelligence and counterintelligence!