

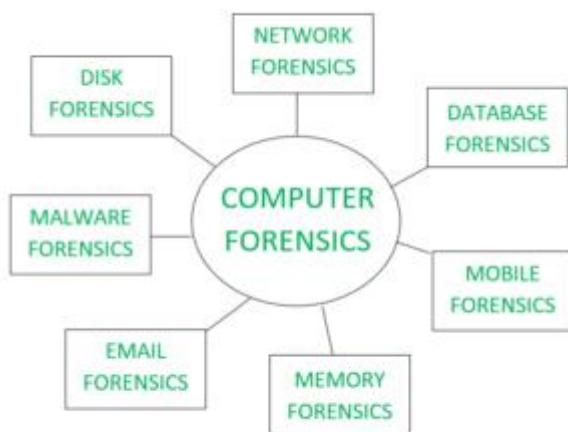
## Introduction of Computer Forensics

### INTRODUCTION

Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from the digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

### TYPES

- **Disk Forensics:** It deals with extracting raw data from primary or secondary storage of the device by searching active, modified, or deleted files.
- **Network Forensics:** It is a sub-branch of Computer Forensics which involves monitoring and analysing the computer network traffic.
- **Database Forensics:** It deals with the study and examination of databases and their related metadata.
- **Malware Forensics:** It deals with the identification of suspicious code and studying viruses, worms, etc.
- **Email Forensics:** It deals with emails and its recovery and analysis, including deleted emails, calendars, and contacts.
- **Memory Forensics:** Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analysing it for further investigation.
- **Mobile Phone Forensics:** It mainly deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc. and other data present in it.



### CHARACTERISTICS

- Identification: Identifying what evidence is present, where it is stored, how it is stored (in which format). Electronic devices can be personal computers, Mobile phones, PDAs, etc.
- Preservation: Data is isolated, secured, and preserved. It includes prohibiting unauthorized personnel from using the digital device so that digital evidence, mistakenly or purposely, is not tampered with and making a copy of the original evidence.
- Analysis: Forensic lab personnel reconstruct fragment of data and draw conclusions based on evidence.
- Documentation: A record of all the visible data is created. It helps in recreating and reviewing the crime scene. All the findings from the investigations are documented.
- Presentation: All the documented findings are produced in a court of law for further investigations.



## PROCEDURE:

The procedure starts with identifying the devices used and collecting the preliminary evidence on the crime scene. Then the court warrant is obtained for the seizures of the evidences which leads to the seizure of the evidences. The evidences are then transported to the **forensics lab** for further investigations and the procedure of transportation of the evidence from the crime scene to labs are called chain of custody. The evidences are then copied for analysis and the original evidence is kept safe because analysis are always done on the copied evidence and not the original evidences.

The analysis is then done on the copied evidence for suspicious activities and accordingly the findings are documented in a non technical tone. The documented findings are then presented in the court of law for further investigations.

## **Some Tools used for Investigation :**

Tools for Laptop or PC –

- **COFEE** – A suite of tools for Windows developed by Microsoft.
- **The Coroner's Toolkit** – A suite of programs for Unix analysis.
- **The Sleuth Kit** – A library of tools for both Unix and Windows.

### **Tools for Memory :**

- Volatility
- WindowsSCOPE

### **Tools for Mobile Device :**

- MicroSystemation XRY/XACT

## **APPLICATIONS**

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Misuse of the Internet and email in the workplace
- Forgeries related matters
- Bankruptcy investigations
- Issues concern with the regulatory compliance

### **Advantages of Computer Forensics :**

- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies gather important information on their computer systems or networks potentially being compromised.
- Efficiently tracks down cyber criminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

### **Disadvantages of Computer Forensics :**

- Before the digital evidence is accepted into court it must be proved that it is not tampered with.
- Producing and keeping the electronic records safe are expensive.
- Legal practitioners must have extensive computer knowledge.
- Need to produce authentic and convincing evidence.
- If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
- Lack of technical knowledge by the investigating officer might not offer the desired result.

## Incident Response

- What is an incident response plan for cyber security? Learn how to manage a data breach with the 6 phases in the incident response plan.
- An incident response plan is a documented, written plan with 6 distinct phases that helps IT professionals and staff recognize and deal with a cybersecurity incident like a data breach or cyber attack. Properly creating and managing an incident response plan involves regular updates and training.

### How to create an incident response plan

An incident response plan should be set up to address a suspected data breach in a series of phases. Within each phase, there are specific areas of need that should be considered.

The incident response phases are:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

### What Is Incident Response?

[Incident response](#) is a process that allows organizations to identify, prioritize, contain and eradicate cyberattacks. The goal of incident response is to ensure that organizations are aware of significant security incidents, and act quickly to stop the attacker, minimize damage caused, and prevent follow on attacks or similar incidents in the future.

### What Is SANS?

The SANS Institute is a private organization established in 1989, which offers research and education on information security. It is the world's largest provider of security training and certification, and maintains the largest collection of research about cybersecurity. SANS also operates the Internet Storm Center, an early warning system for global cyber threats.

### SANS Incident Response Plan

The SANS Institute published a 20-page handbook that lays out a structured 6-step [plan for incident response](#). Below is a brief summary of the process, and in the following sections we'll go into more depth about each step:

1. **Preparation**—review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Computer Security [Incident Response Team](#) (CSIRT).
2. **Identification**—monitor IT systems and detect deviations from normal operations, and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.
3. **Containment**—perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.
4. **Eradication**—remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.
5. **Recovery**—bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.
6. **Lessons learned**—no later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.

## Step 1: Preparation

The goal of the preparation stage is to ensure that the organization can comprehensively respond to an incident at a moment's notice.

According to SANS, these are critical elements that should be prepared in advance:

- **Policy**—define principle, rules and practices to guide security processes. Ensure the policy is highly visible both to employees and users, for example by displaying a login banner that states all activities will be monitored, and clearly stating unauthorized activities and the associated penalties.
- **Response Plan/Strategy**—create a plan for incident handling, with prioritization of incidents based on organizational impact. For example,

organizational impact is higher the more employees are affected within the organization, the more an event is likely to impact revenues, or the more sensitive data is involved, such as salaries, financial or private customer data.

- **Communication**—create a communication plan that states which CSIRT members should be contacted during an incident, for what reasons and when they can be contacted. For example, there may be operations staff on call at all hours, everyone in the organization should know, which incident responders to contact to help bring systems back up. The communication plan should state the policy for contacting law enforcement, and who should make contact.
- **Documentation**—documentation is not optional and can be a life saver. If the incident is considered a criminal act, your documentation will be used to press charges against suspects. Any information you collect about the incident can also be used for lessons learned and to improve your incident response process. Documentation should answer the questions: Who, What, When, Where, Why, and How?.
- **Team**—build a CSIRT team with all relevant skills, not just security. Include individuals with expertise in security but also IT operations, legal, human resources, and public relations—all of whom can be instrumental in dealing with and mitigating an attack.
- **Access control**—make sure that CSIRT staff have the appropriate permissions to do their job. It is a good idea to have, as part of the incident response plan, network administrators add permissions to CSIRT member accounts, and then remove them when the incident is over.
- **Training**—ensure initial and ongoing training for all CSIRT members on incident response processes, technical skills and relevant cyberattack patterns and techniques. Carry out drills at regular intervals to insure that everyone in the CSIRT knows what they need to do and is able to perform their duties during a real incident.
- **Tools**—evaluate, select and deploy software and hardware that can help respond to an incident more effectively. All of the tools should be packaged in a “jump bag” that can be quickly accessed by CSIRT members when an incident occurs.

## Step 2: Identification

This step involves detecting deviations from normal operations in the organization, understanding if a deviation represents a security incident, and determining how important the incident is.

The SANS identification procedure includes the following elements:

- **Setting up monitoring** for all sensitive IT systems and infrastructure.
- **Analyzing events** from multiple sources including log files, error messages, and alerts from security tools.
- **Identifying an incident** by correlating data from multiple sources, and reporting it as soon as possible.
- **Notifying CSIRT members** and establishing communication with a designated command center (for example this could be senior management, IT operations)
- **Assigning** at least two incident responders to a live incident, one as the primary handler who assesses the incident and makes the decision, and the other to help investigate and gather evidence.
- **Documenting everything** that incident responders are doing as part of the attack—answering the Who, What, Where, Why, and How questions.
- **Threat prevention and detection capabilities** across all main attack vectors.

### Step 3: Containment

The goal of containment is to limit damage from the current security incident and prevent any further damage. Several steps are necessary to completely mitigate the incident, while also preventing destruction of evidence that may be needed for prosecution.

The SANS containment process involves:

- **Short-term containment**—limiting damage before the incident gets worse, usually by isolating network segments, taking down hacked production server and routing to failover.
- **System backup**—taking a forensic image of the affected system(s) with tools such as Forensic Tool Kit (FTK) or EnCase, and only then wipe and reimage the systems. This will preserve evidence from the attack that can be used in court, and also for further investigation of the incident and lessons learned.
- **Long-term containment**—applying temporarily fixes to make it possible to bring production systems back up. The primary focus is removing accounts or backdoors left by attackers on the systems, and addressing the root cause—for example, fixing a broken authentication mechanism or patching a vulnerability that led to the attack.



## Step 4: Eradication

Eradication is intended to actually remove malware or other artifacts introduced by the attacks, and fully restore all affected systems.

The SANS eradication process involves:

- **Reimaging**—complete wipe and re-image of affected system hard drives to ensure any malicious content is removed.
- **Preventing the root cause**—understanding what caused the incident preventing future compromise, for example by patching a vulnerability exploited by the attacker.
- **Applying basic security best practices**—for example, upgrading old software versions and disabling unused services.
- **Scan for malware**—use anti-malware software, or Next-Generation Antivirus (NGAV) if available, to scan affected systems and ensure all malicious content is removed.

## Step 5: Recovery

The goal of recovery is to bring all systems back to full operation, after verifying they are clean and the threat is removed.

The SANS recovery procedure involves:

- **Defining time and date to restore operations**—system owners should make the final decision on when to restore services, based on information from the CSIRT.
- **Test and verifying**—ensuring systems are clean and fully functional as they go live.
- **Monitoring**—ongoing monitoring for some time after the incident to observe operations and check for abnormal behaviors.
- **Do everything to prevent another incident**—considering what can be done on the restored systems to protect them from recurrence of the same incident.

## Step 6: Lessons Learned

No later than two weeks from the end of the incident, the CSIRT should compile all relevant information about the incident and extract lessons that can help with future incident response activity.



The SANS lessons learned process includes:

- **Completing documentation**—it is never possible to document all aspects of an incident while it is going on, and achieving comprehensive documentation is very important to identify lessons for next time.
- **Publishing an incident report**—the report should provide play-by-play review of the entire incident, and answer the Who, What, Where, Why, and How questions.
- **Identify ways to improve CSIRT performance**—extract items from the incident report that were not handled correctly and can be improved for next time.
- **Establish a benchmark for comparison**—derive metrics from the incident report that you can use to guide you in future incidents.
- **Lessons learned meeting**—conduct a meeting with the CSIRT team and other stakeholders to discuss the incident and cement lessons learned that can be implemented immediately.

SANS suggests this general format for the incident report:

- When was the problem first detected and by whom
- The scope of the incident
- How it was contained and eradicated
- Worked performed during recovery
- Areas where the CIRT teams were effective
- Areas that need improvement

## Computer Forensics: Recovering Deleted Files

*Recovering deleted files is an important job of a data forensic specialist, as an essential part of many computer forensics investigations is retrieving deleted files that could be used as evidence. Here, the data forensics experts at Atlantic Data Forensics provide an overview of the process of recovering deleted files for both files deleted accidentally, and more serious cases where data is purposefully deleted to hide evidence.*

### Deleted Files can be Retrieved from the Recycle Bin

As 93% of information is stored on a digital domain, it is common for files to be deleted accidentally, or for seemingly unimportant documents to be deleted only to become needed later on when the document no longer exists as an original file. Deleted computer files can cause inconvenience and stress for computer users, but luckily, it is possible to retrieve many deleted files from the recycle bin on a computer's desktop. By searching through the contents of your recycle

bin, a temporary storage place for deleted files until they are more permanently erased from a desktop, you may be able to retrieve accidentally lost files.

If files are no longer stored in the recycle bin, there are data recovery tools that can be utilized to possibly retrieve lost data from a hard drive, as the content of a deleted computer file is not always permanently removed from the computer. Deleted files or documents can be retrieved by a process of scanning an entire hard drive and analyzing the file system in order to successfully recover any lost data, methods utilized by experienced data recovery specialists, such as those at Atlantic Data Forensics.

### **Files are Often Damaged or Deleted to Remove Evidence**

Often, the work of a computer forensics expert includes the retrieval of purposefully deleted files, documents, emails, pictures and other digital content that was damaged as a method of destroying evidence. The act of deleting computer files in order to hide evidence of a crime is common, yet the data is rarely ever deleted permanently. At the simplest level, deleted files can be easily retrieved by a computer forensics specialist if the file was merely deleted from the computer—as mentioned above, deleted files are hardly ever removed entirely from a computer's hard drive, especially on a Windows system, as deleted files are solely removed from the original directory.

While the process of retrieving digital evidence may seem complex to the average computer user, data recovery specialists have unique software and forensic tools that allow them to retrieve damaged or deleted computer files or to decipher information surrounding encrypted data. It is important to consult a computer forensics expert in the case that you cannot retrieve lost files, or if you are involved in a lawsuit in which digital data retrieval may be a necessary part of an investigation.

### **Data Encryption and Compression**

According to recent research figures, last year more than 15-million different malware files were detected with nearly 300 000 new malware samples being recorded every day.

Against this backdrop, data file encryption techniques are evolving rapidly to protect information stored on tablets and PCs from theft and unintentional data loss. Data encryption is the ciphering or scrambling of data. The only way to decipher or unscramble it is via a deciphering mechanism. This can be in the form of a key, long passcode, portable radio frequency identification (RFID) chip, or a combination of these and other techniques.

Data encryption is a strongly advised method of not only securing tablets and PCs, but also network-attached devices and the often-critical information they contain. More specifically, data encryption is growing increasingly popular in today's approach to email security with "clientless" methods pioneered by industry leaders who are setting the standard for effectiveness and also for ease of setup and customisation to suit diverse requirements and environments.

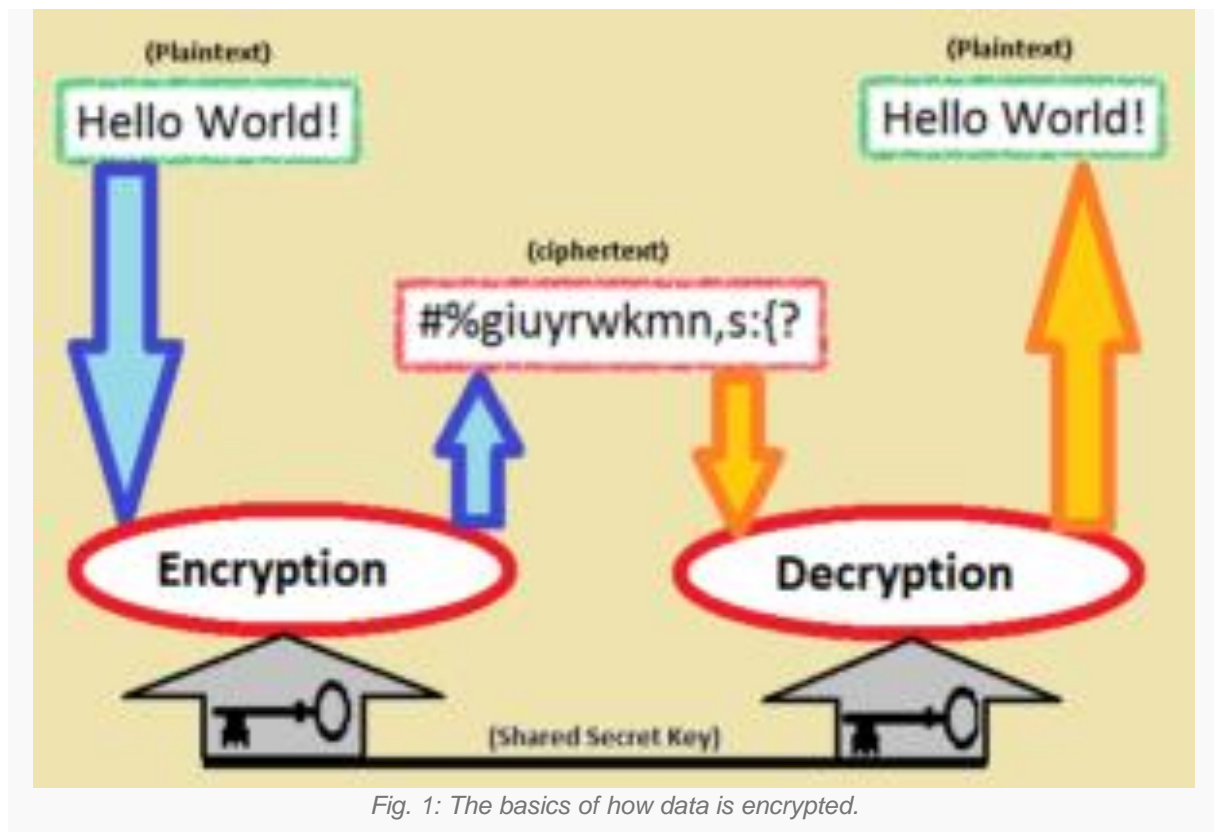


Fig. 1: The basics of how data is encrypted.

### The importance of encryption

Encryption is being accepted as a fundamental element of data protection and the overall threat protection landscape. In this light, are three key reasons why businesses need to consider encryption.

The first is protection for sensitive data against hacking and data breaches. The second is to safeguard against unintended information disclosure through accidental exposure of critical data. Thirdly, the migration to cloud-based services presents a security issue, and encryption is able to assist companies to protect data that may be vulnerable in this scenario.

In order for encryption to be effective, it has to be easy to manage, transparent to users, and able to work with multiple platforms and file types. On-going developments in this field are enabling users to adopt “always on” file-level encryption to protect data accessed from mobile devices, laptops, desktops, on-premises networks and cloud-based file sharing applications.

These advances allow for the encryption of individual files by default while facilitating the continuous validation of users, applications and devices for secure collaboration.

There is a fourth – and most important – reason for the adoption of data encryption solutions: Encryption helps companies comply with new legislation requirements mitigating potentially large fines.

In the European Union (EU) the General Data Protection Regulation (GDPR) recently came into effect. It mandates all companies holding customer or employee data to secure the data or face severe financial penalties of up to 4% of annual worldwide revenue. In South Africa, the Protection of Personal Information (PoPI) Act focuses on how organisations store, protect and secure private customer information. The Act requires organisations that collect personal data about their customers to adhere to specific criteria and regulations – including the encryption of data on all company and employee-owned devices as a standard technical and security measure. Failure to comply with PoPI could see the SA Regulator levy administrative fines on organisations of up to R10-million.

Legislation confirms that encryption is accepted as one of the best – if not the best – security measures available. From an endpoint perspective, the latest and most powerful encryption solutions use Windows BitLocker and Mac FileVault as native disk encryption platforms to ensure simplicity and the best protection of personal information.

BitLocker provides the most protection when used with a trusted platform module (TPM) version 1.2 or later. The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline. FileVault is Apple's implementation of encrypting data on MacOS and Mac hardware.

Data compression techniques can complement data encryption in a comprehensive data security application. They are often key components of commonly deployed cybercrime fighting regimes. Data compression removes redundant character strings in a file leaving the compressed file with a more uniform distribution of characters.

However, the use of compression algorithms should depend on operational constraints. For example, if an organisation has storage or bandwidth challenges and there is a need to compress data, many specialists advise that it should be compressed first then encrypted.

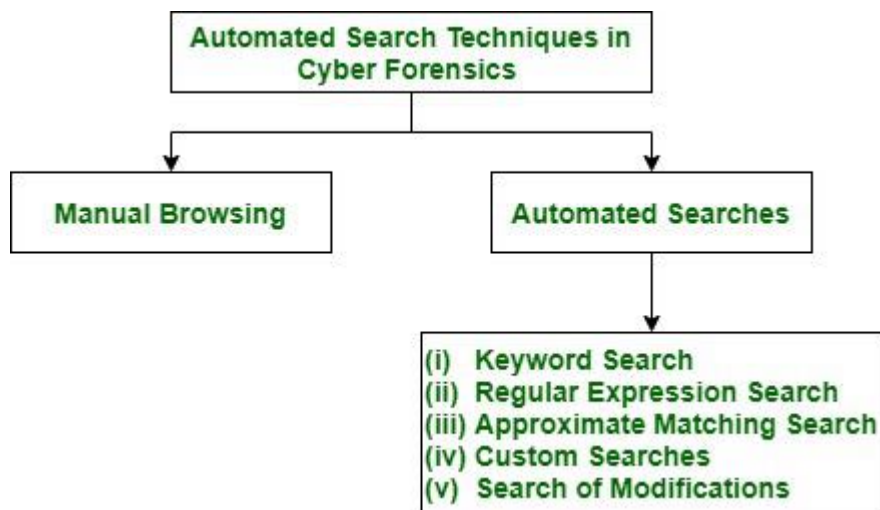
Until recently, compressing encrypted text was not advised as the cryptogram is, in essence, a random series of bytes that do not compress well.

However, newer data storage methods efficiently couple data compression with encryption in simultaneous compression/encryption schemes that can help limit the performance penalty that certain data compression algorithms present.

## Search Techniques in Cyber Forensics

Computer forensic examinations use computer generated data as their vital source. The goal of any given computer forensic examination is to find facts, and through these facts they try to recreate truth of an event. These Automated Search Techniques are used to find out whether given type of object such as hacking tools or pictures of specific type are present in information that is collected.

There are two types of Automated Search Techniques : Manual Browsing and Automated Browsing.



**Figure –** Types of automated search techniques in cyber forensics

### **What is Manual Browsing ?**

Forensic Analyst browses information that has been gathered and selects objects of preferred type in Manual Browsing. The tool used for this browsing is type of Watcher. It takes data object, e.g., file, decodes that file and gives result back in human-readable format. Manual Browsing is slow and time consuming as there is massive amount of data that is to be gathered in lot of investigations.

### **What are Automated Searches ?**

The word Automated comes from Greek word automatos, meaning “acting of oneself.” Something that is automated can do what it’s meant to do without having person to help run it. An automated search procedure provides direct access to automated files of another party where response to search procedure is fully automated.

The types of automated Searches are : Keyword Search, Regular Expression Search, Approximate Matching Search, Custom Searches, Search of Modifications.

#### **1. Keyword Search –**

The cyber forensic keyword search is feature used to find evidence from large amount of electronic data. During the cyber crime investigation forensic email search is performed on basis of keywords that you enter in computer forensics tool. Keyword search consists of specific keywords. It is widely used easy technique that speeds up manual browsing. The list of

found data objects is output of keyword search. However, there are two problems with keyword search: False Positive and False Negative.

- **(i). False Positive :**

Keyword searches gives approximate required type of data objects. Because of this output of this could have false positives. False Positives means objects that do not belong to any particular type even though they contain specified keywords. A Forensic Analyst has to browse keyword search data objects manually to discard false positives.

- **(ii). False Negative :**

False Negatives means that there are objects of particular given type but they are missed by search. If search utility fails to correctly interpret data objects then result is false negative. Encryption, Compression or lack of ability of search utility to interpret new data might be reason for this to happen.

## 2. **Regular Expression Search -**

Regular expression (Regex) is powerful way used to search anything in text based files for data with an identifiable pattern. This search gives more expressible language for describing object of interest than keywords. This is an extension of keyword search. These are also used to specify searches of e-mail addresses and files of precise type. To perform regular expression searches Encase Tool is used. Not all type of data can be sufficiently described using regex. Regular Expression Search also results in false positives and false negatives.

## 3. **Approximate Matching Search -**

An expansion of regular expression search is Approximate Matching Search. It uses Matching algorithm. Approximate matching Search algorithm allows character mismatches while searching for keyword. It detects misspelled words which gives mismatches and raises lot of false positives. The agrep is used for approximate matches.

## 4. **Custom Searches -**

Heuristic procedure is used by this tool to find full names of people in gathered information/data. These programs are written for more complex searches like FILTER\_1 tool from new Technologies Inc. because regular expressions have limited expressiveness. This too suffers from false positives and false negatives.

## 5. **Search of Modifications -**

This is used for data objects that have been modified since specified instant in past. The modifications of data objects that are not frequent like operating system utilities. These utilities are detected by comparing their current hash with their expected hash. A library of expected hashes is built before search.



[Encrypted Disk Detector](#) can be helpful to check encrypted physical drives. It supports TrueCrypt, PGP, Bitlocker, Safeboot encrypted volumes.



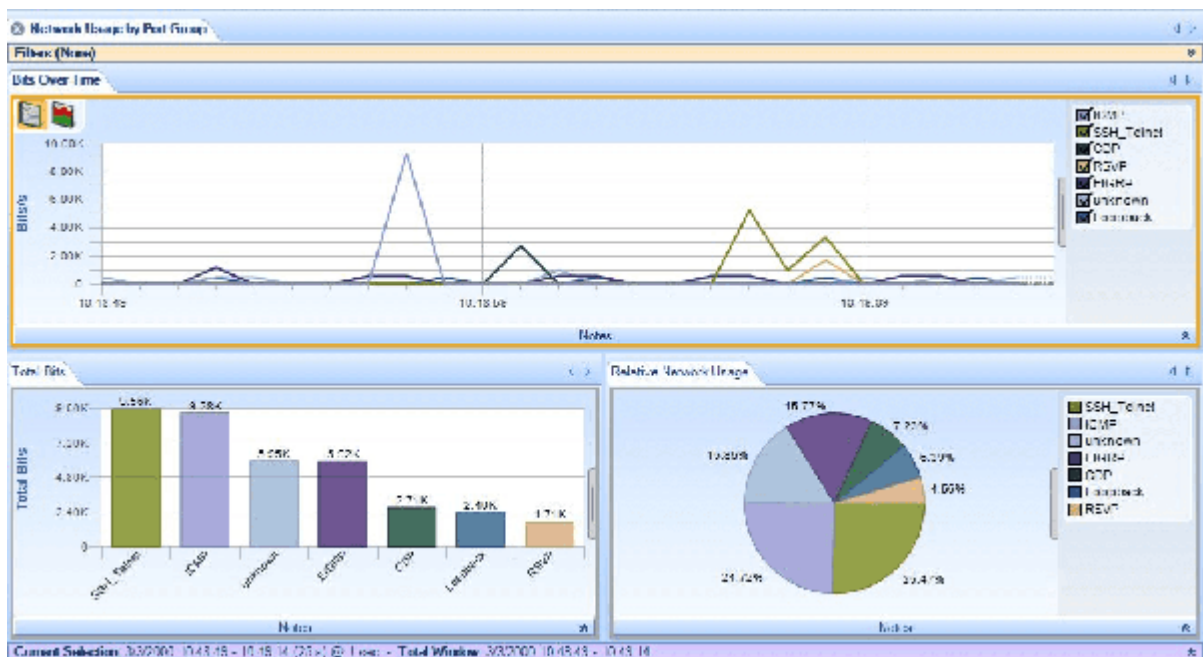


# MAGNET

FORENSICS®

### 3. Wireshark

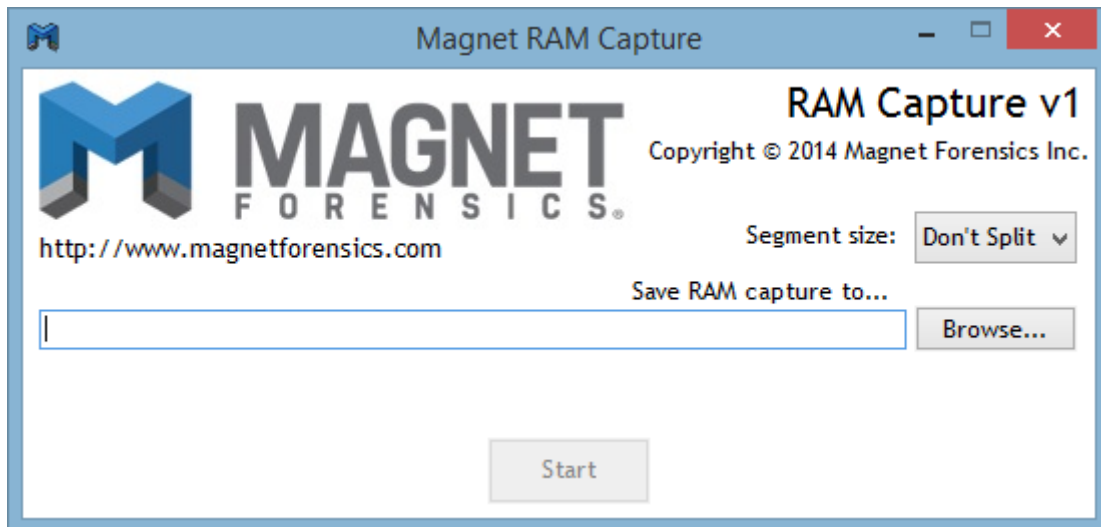
[Wireshark](#) is a network capture and analyzer tool to see what's happening in your network. Wireshark will be handy to investigate network related incident.



### 4. Magnet RAM Capture

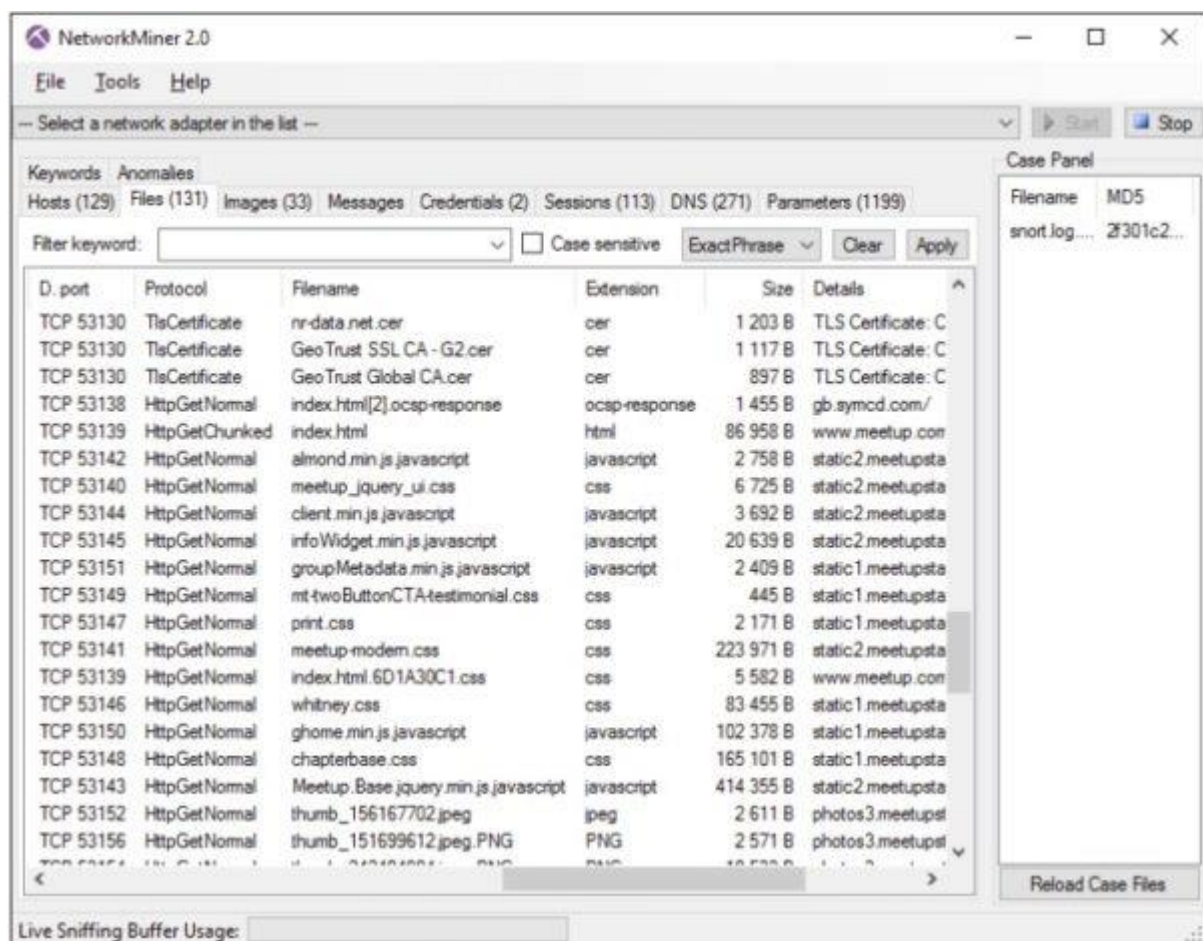
You can use [Magnet RAM capture](#) to capture the physical memory of a computer and analyze artifacts in memory.

It supports Windows operating system.



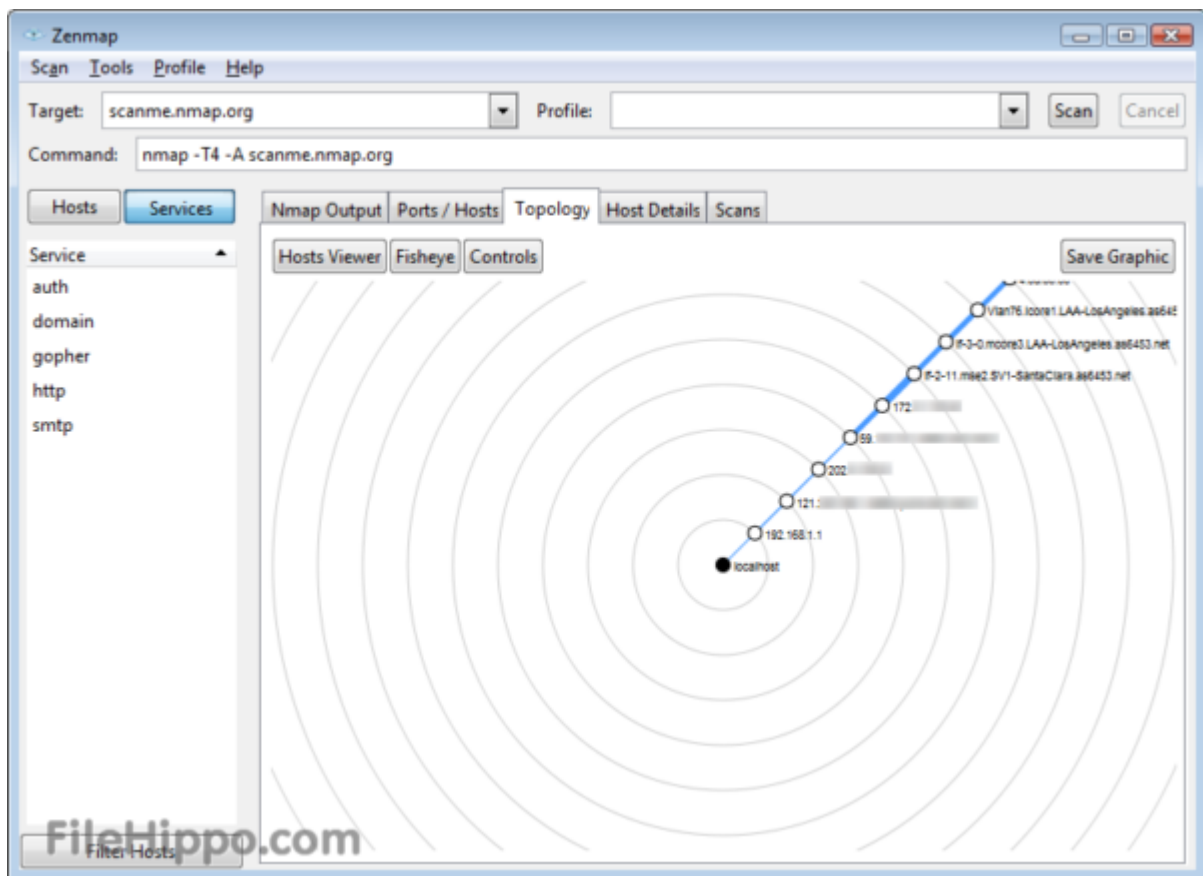
## 5. Network Miner

An interesting network forensic analyzer for Windows, Linux & MAC OS X to detect OS, hostname, sessions and open ports through packet sniffing or by PCAP file. [Network Miner](#) provide extracted artifacts in an intuitive user interface.



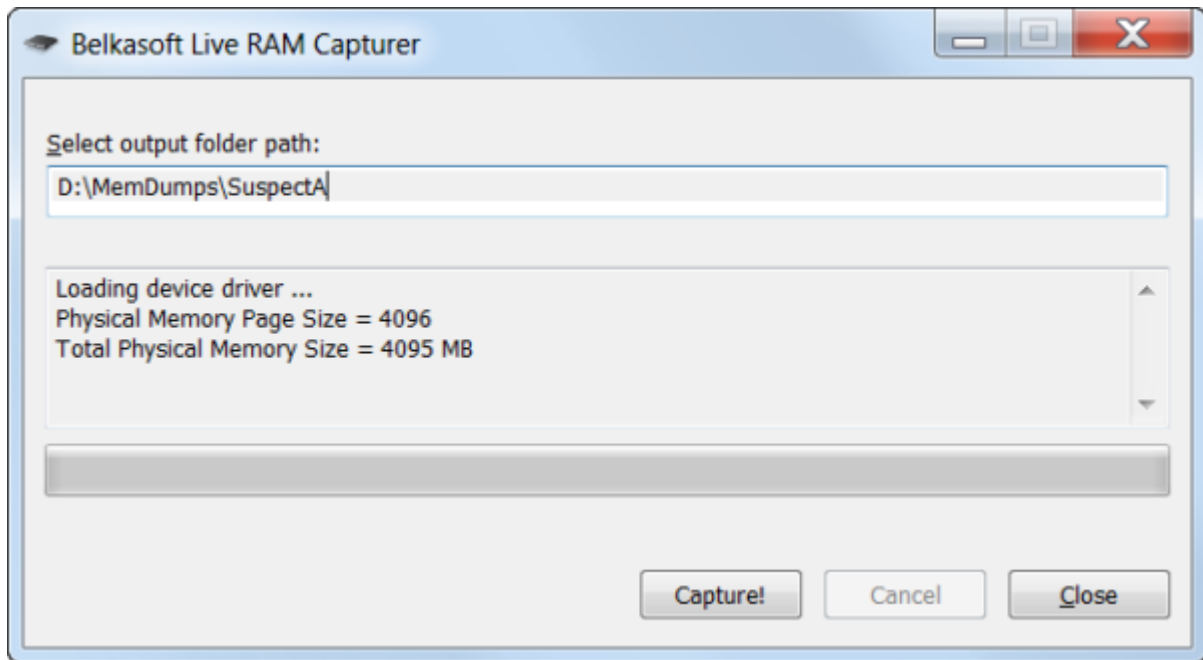
## 6. NMAP

[NMAP](#) (Network Mapper) is one of the most popular networks and security auditing tools. NMAP is supported on most of the operating systems including Windows, Linux, Solaris, MAC OS, HP-UX etc. It's open source so free.



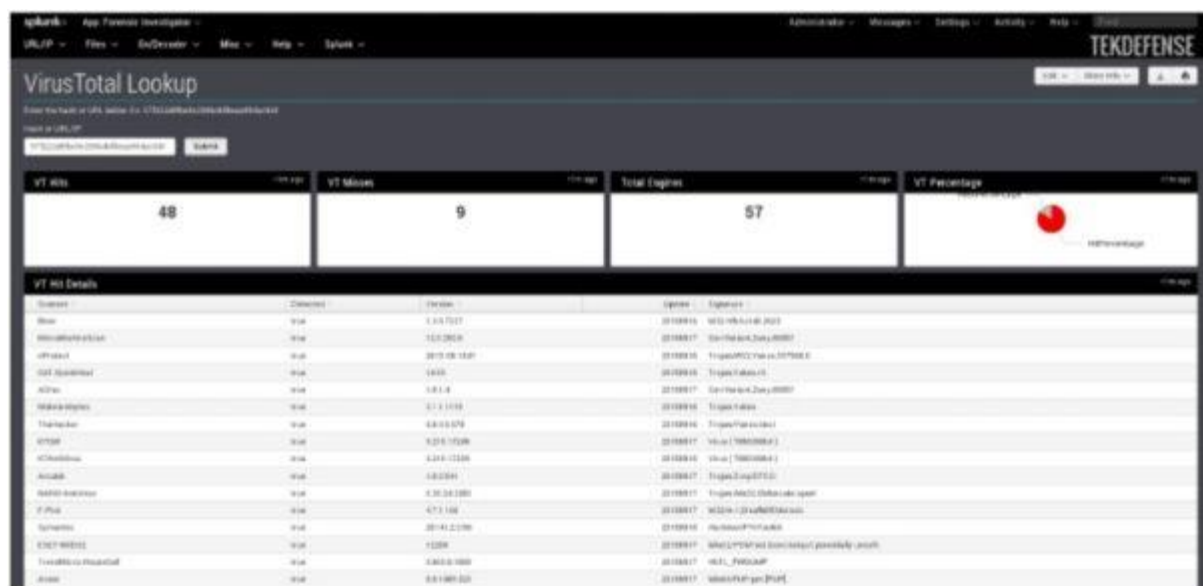
## 7. RAM Capturer

[RAM Capturer by Belkasoft](#) is a free tool to dump the data from computer's volatile memory. It's compatible with Windows OS. Memory dumps may contain encrypted volume's password and login credentials for webmails and social network services.



## 8. Forensic Investigator

If you are using Splunk then [Forensic Investigator](#) will be a very handy tool. It's Splunk app and has many tools combined.



## 9. FAW

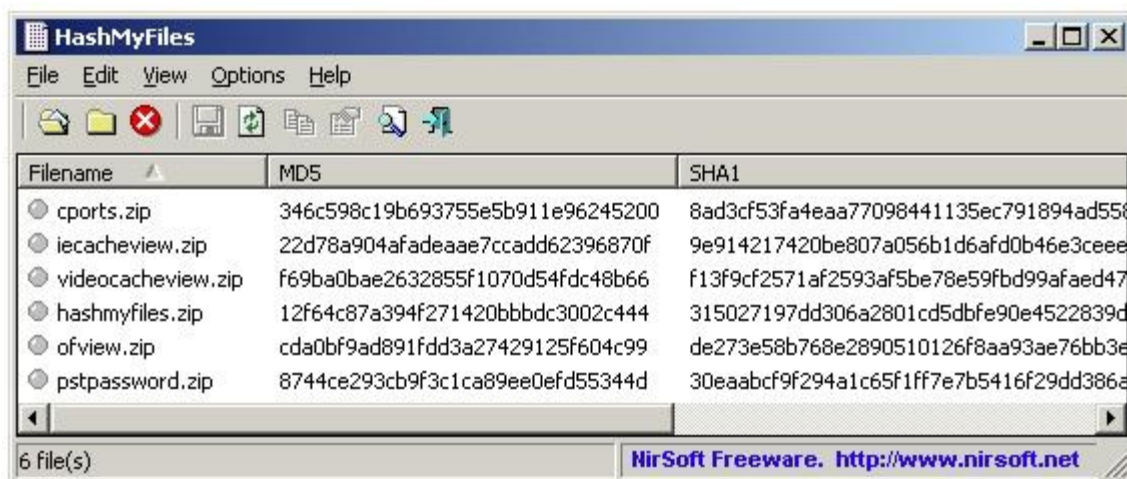
[FAW](#) (Forensics Acquisition of Websites) is to acquire web pages for forensic investigation which has the following features.

- Capture the entire or partial page
- Capture all types of image
- Capture HTML source code of the web page
- Integrate with Wireshark



## 10. HashMyFiles

[HashMyFiles](#) will help you to calculate the MD5 and SHA1 hashes. It works on almost all latest Windows OS.



## 11. USB Write Blocker

View the USB drives content without leaving the fingerprint, changes to metadata and timestamps. [USB Write Blocker](#) use Windows registry to write-block USB devices.






## 12. Crowd Response

[Response](#) by Crowd Strike is a windows application to gather system information for incident response and security engagements. You can view the results in XML, CSV, TSV or HTML with help of CRConvert. It runs on 32 or 64 bit of Windows XP above.

Crowd Strike has some other nice tools for investigation.

- Tottrilla – anonymously route TCP/IP and DNS traffic through TOR.
- Shellshock Scanner – scan your network for shellshock vulnerability
- Heartbleed scanner – scan your network for OpenSSL [heart bleed vulnerability](#)

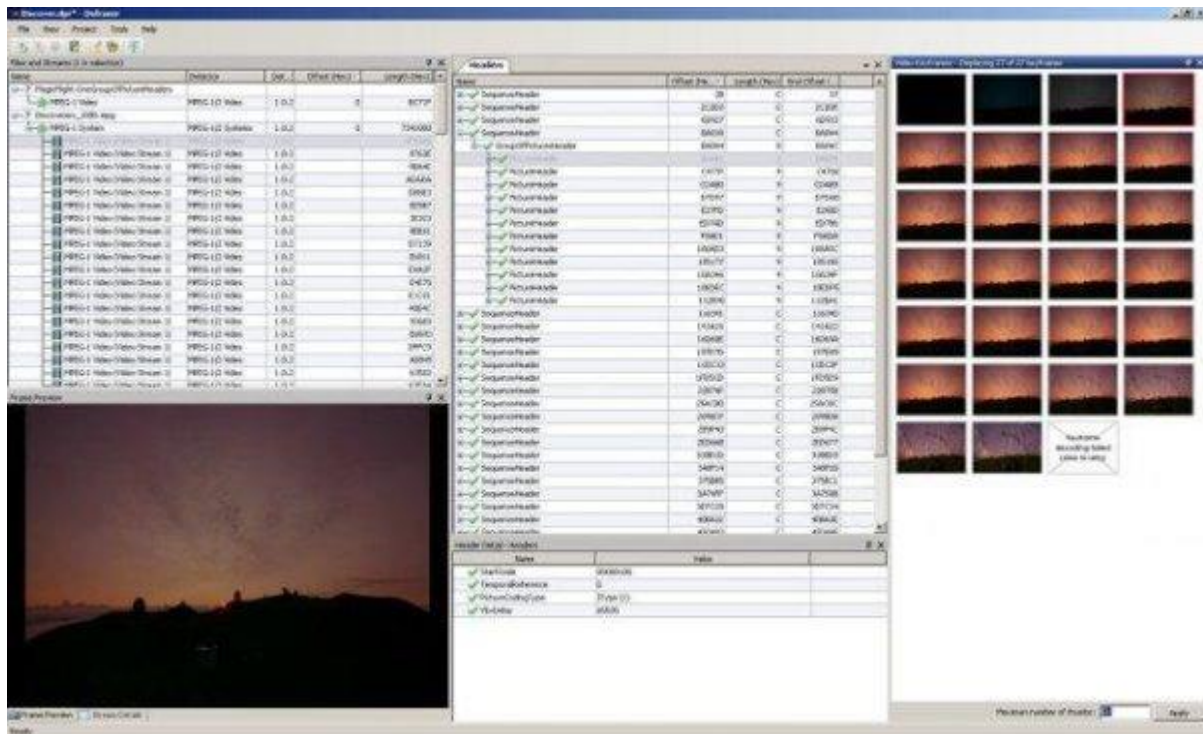
Let us show you how we stop breaches

		
Learn how to prevent, detect, and respond to all attack types in real time with CrowdStrike Falcon.	Request information about next-gen endpoint protection, threat intelligence, or incident response services.	Need immediate assistance? Get back to business faster with CrowdStrike's pre and post incident response services.
<a href="#">SEE DEMO</a>	<a href="#">REQUEST INFO</a>	<a href="#">EXPERIENCED A BREACH?</a>

## 13. NFI Defraser

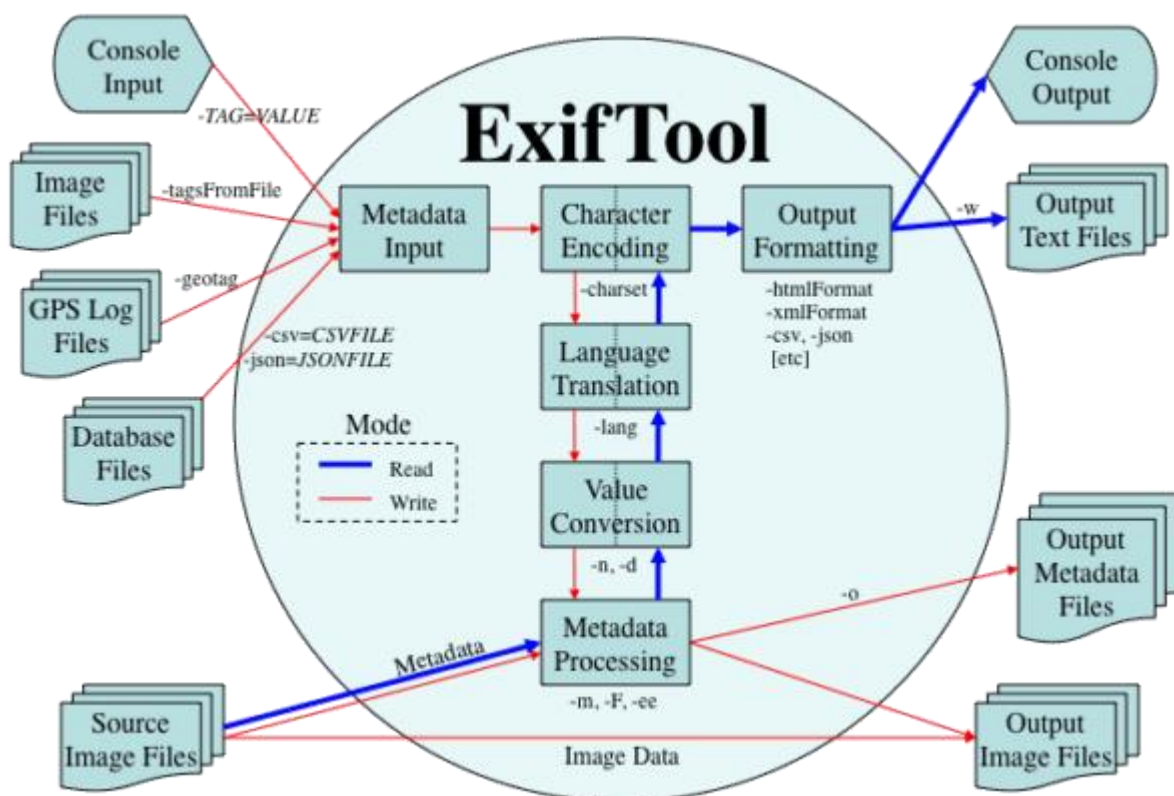
[Defraser](#) forensic tool may help you to detect full and partial multimedia files in the data streams.





## 14. ExifTool

[ExifTool](#) helps you to read, write and edit meta information for a number of file types. It can read EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, Photoshop IRB, FlashPix, etc.

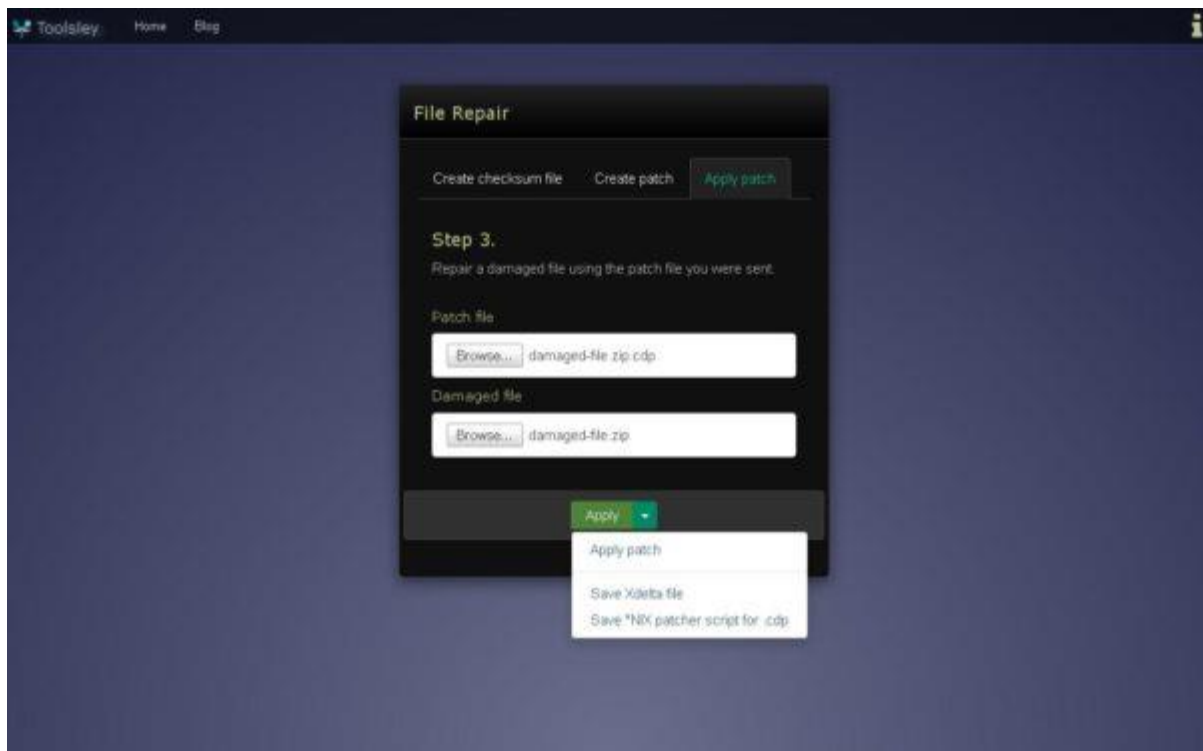




## 15. Toolsley

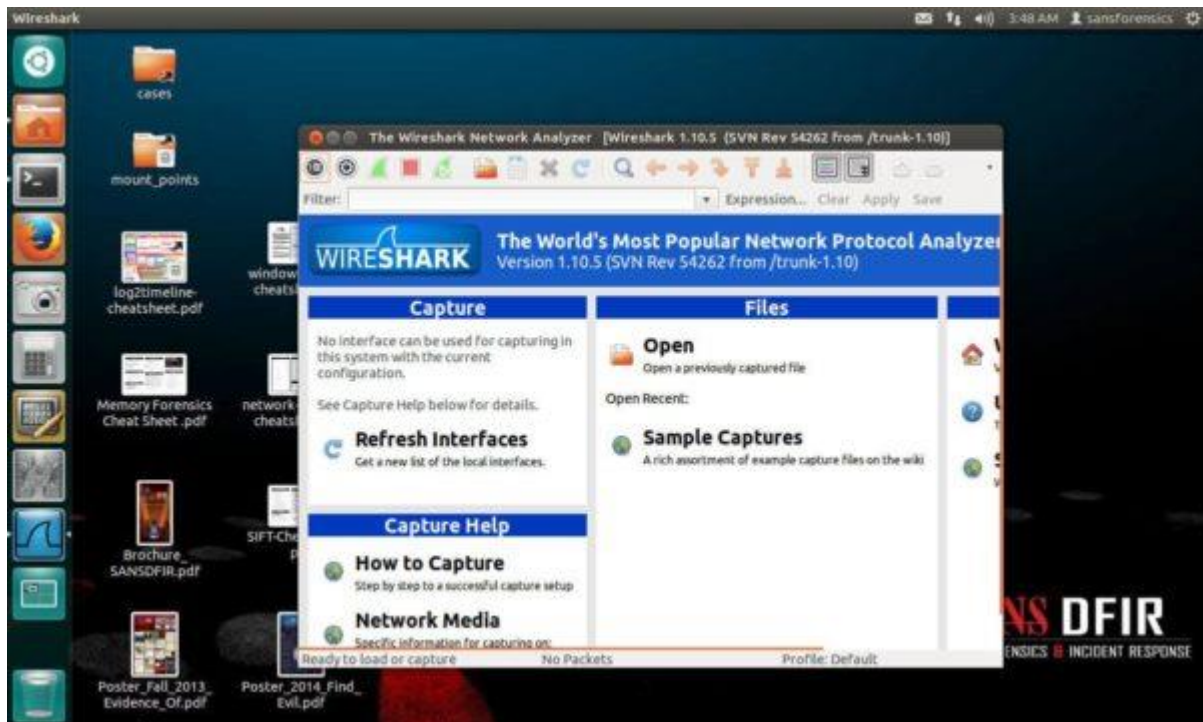
[Toolsley](#) got more than 10 useful tools for investigation.

- File signature verifier
- File identifier
- Hash & Validate
- Binary inspector
- Encode text
- Data URI generator
- Password generator



## 16. SIFT

[SIFT](#) (SANS investigative forensic toolkit) workstation is freely available as Ubuntu 14.04. SIFT is a suite of forensic tools you need and one of the most popular open source incident response platform.



## 17. Dumpzilla

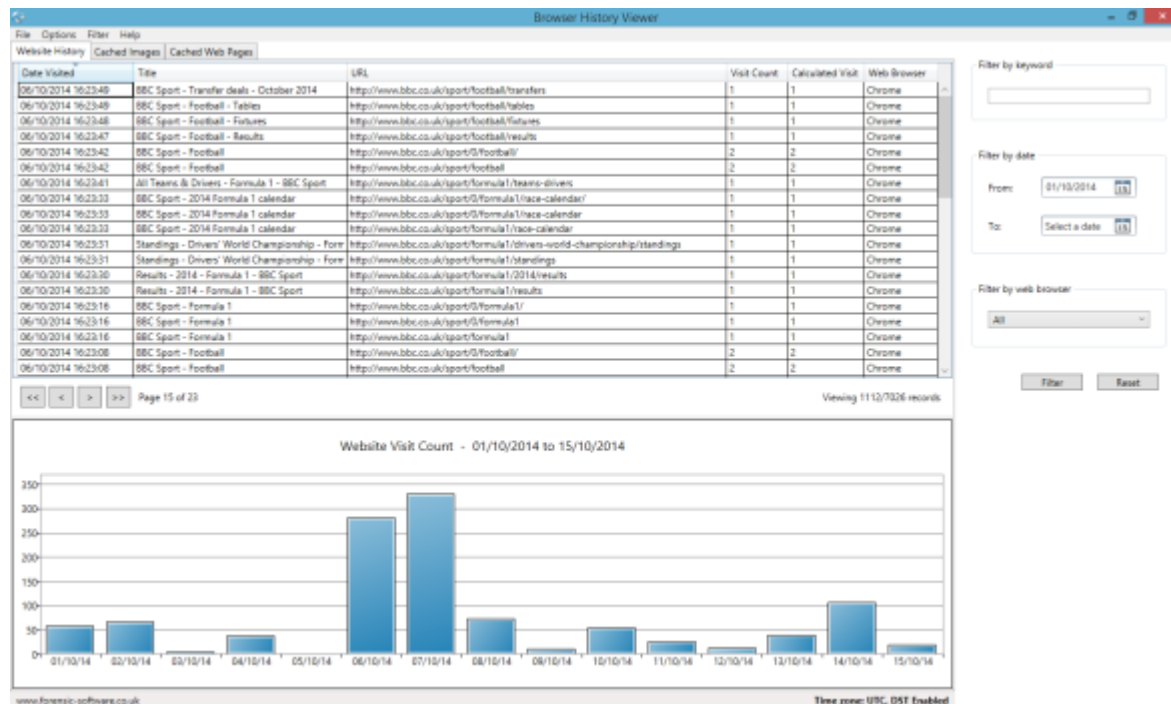
Extract all interesting information from Firefox, Iceweasel and Seamonkey browser to be analyzed with [Dumpzilla](#).



## 18. Browser History

Foxtton has two free interesting tools.

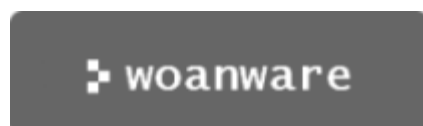
1. Browser history capturer – capture web browser (chrome, firefox, IE & edge) history on Windows OS.
2. Browser history viewer – extract and analyze internet activity history from most of the modern browsers. Results are shown in the interactive graph and historical data can be filtered.



## 19. ForensicUserInfo

Extract the following information with [ForensicUserInfo](#).

- RID
- LM/NT Hash
- Password reset/Account expiry date
- Login count/fail date
- Groups
- Profile path



## 20. Kali Linux

[Kali Linux](#) is one of the most popular platforms for penetration testing but it has forensic capability too.



## 21. Paladin

[PALADIN](#) forensic suite – the world's most popular Linux forensic suite is a modified Linux distro based on Ubuntu available in 32 and 64 bit.



## 22. Sleuth Kit

[The Sleuth Kit](#) is a collection of command line tools to investigate and analyze volume and file systems to find the evidence.



## 23. CAINE

CAINE (Computer Aided **I**nvestigate **E**nvironment) is Linux distro that offers the complete forensic platform which has more than 80 tools for you to analyze, investigate and create an actionable report.



## 24. Volatility

[Volatility](#) is the memory forensics framework. It used for incident response and malware analysis. With this tool, you can extract information from running processes, network sockets, network connection, DLLs and registry hives. It also has support for extracting information from Windows crash dump files and hibernation files. This tool is available for free under GPL license.





## 25. WindowSCOPE

[WindowsSCOPE](#) is another memory forensics and reverse engineering tool used for analyzing volatile memory. It is basically used for reverse engineering of malwares. It provides the capability of analyzing the Windows kernel, drivers, DLLs, virtual and physical memory.

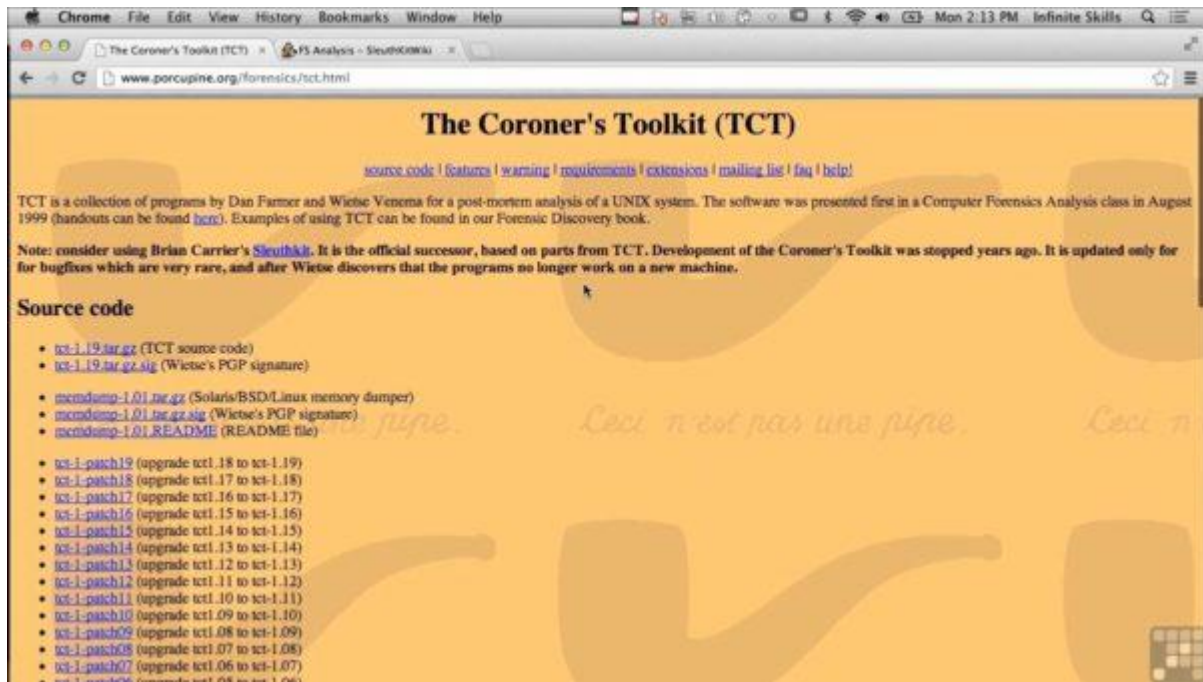
The screenshot displays the WindowsSCOPE application window. The main area is divided into two panes, each showing a 'Process Table, Type: Virtual, Timestamp: 29 Oct 2018, 12:57:20'. The left pane shows a comparison of two snapshots, with 'Compare' and 'Compare Statistics' buttons visible. The right pane shows a single snapshot. Both tables list processes with columns for Process Name, PID, and Hidden status. Processes are color-coded: green for 'Not Checked', yellow for 'Checked', and red for 'Not Checked'.

Process Name	PID	Hidden
winsrv4.exe	3944	Not Checked
plg.exe	3952	Not Checked
Audio.exe	4092	Not Checked
argmax.exe	1984	Not Checked
chassis.exe	3432	Not Checked
avgsrv.exe	3512	Not Checked
ApMgPcd.exe	4444	Not Checked
ApMgEx.exe	4480	Not Checked
hidfind.exe	4488	Not Checked
Wapnetfg.exe	4520	Not Checked
Wapnetwk.exe	4592	Not Checked
taskeng.exe	5088	Not Checked
Wusvcit.exe	5152	Not Checked
Win.exe	6112	Not Checked
svchost.exe	2940	Not Checked
office.exe	4552	Not Checked
office-bin	3540	Not Checked
plg.exe	3952	Not Checked
plugin-container.exe	4480	Not Checked
Wusvcit.exe	2396	Not Checked
Wusvcit-all.exe	5524	Not Checked
WLDSPVC.EXE	3968	Not Checked
WLDSPVC.EXE	5140	Not Checked
googletalkplugin.exe	4656	Not Checked
SearchIndexer.exe	5828	Not Checked
argmax.exe	8076	Not Checked
cmd.exe	5136	Not Checked
wpdbsvc.exe	544	Not Checked
java.exe	8092	Not Checked
SearchProtocolHost.exe	6560	Not Checked
SearchFilterHost.exe	6864	Not Checked

## 26. The Coroner's Toolkit

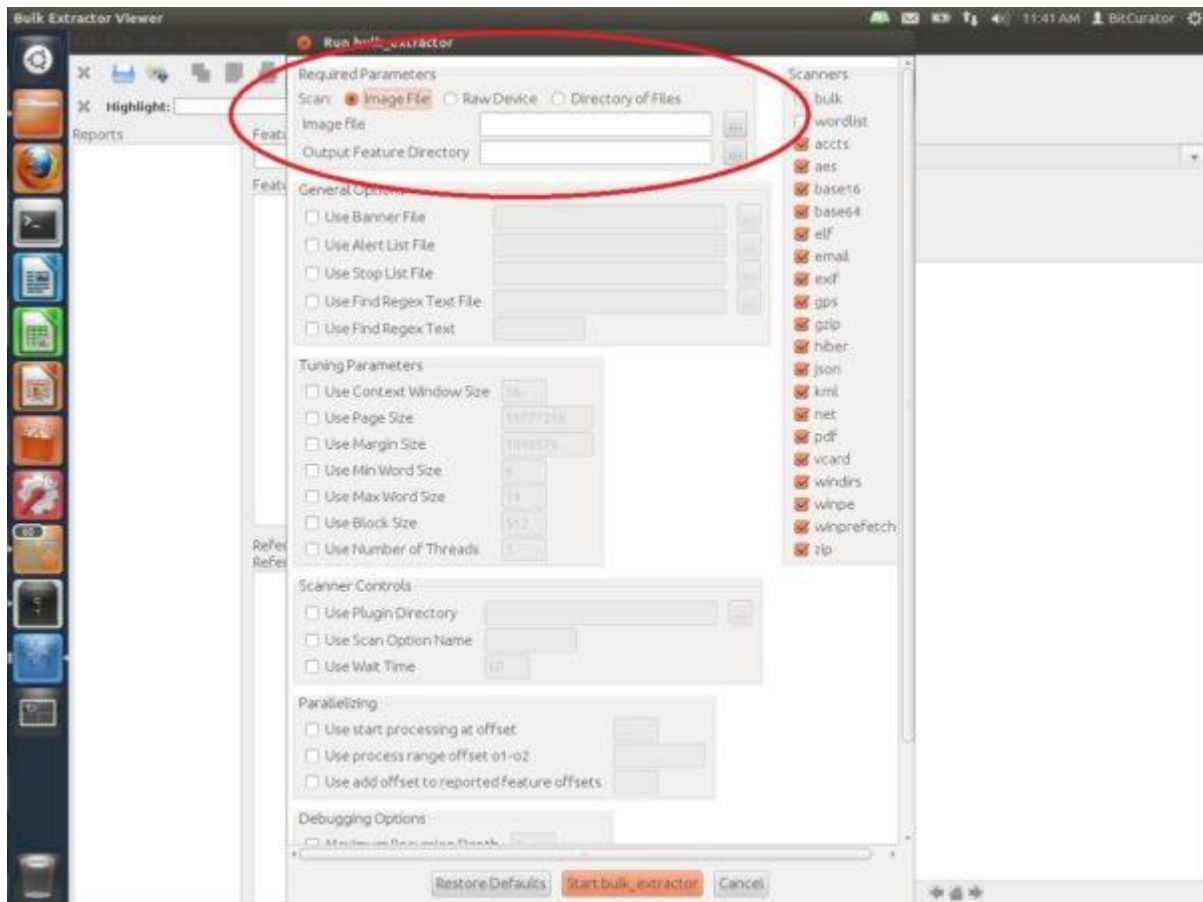
[The Coroner's Toolkit](#) or TCT is also a good digital forensic analysis tool. It runs under several Unix-related operating systems. It can be used to aid analysis of computer disasters and data recovery.





## 27. Bulk Extractor

[Bulk Extractor](#) is also an important and popular digital forensics tool. It scans the disk images, file or directory of files to extract useful information. In this process, it ignores the file system structure, so it is faster than other available similar kinds of tools. It is basically used by intelligence and law enforcement agencies in solving cyber crimes.



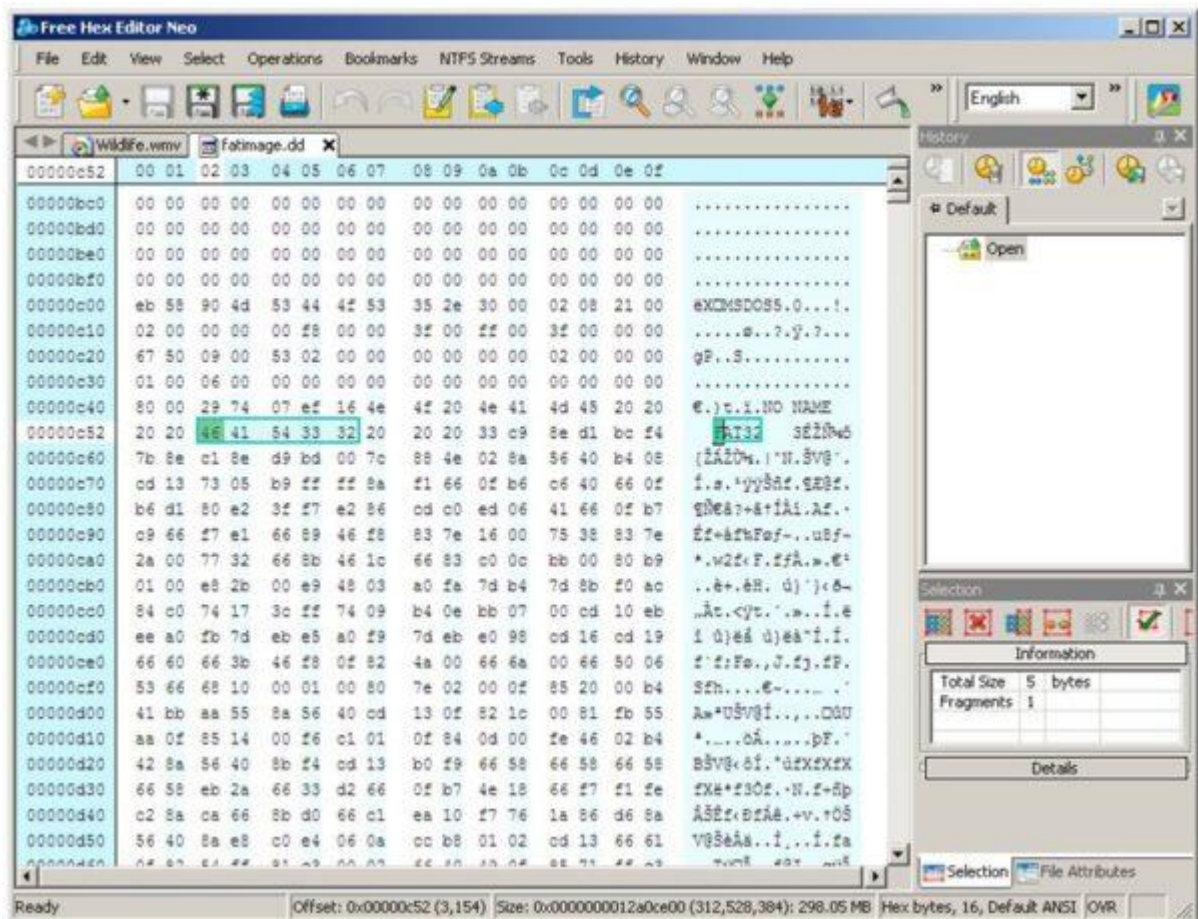
## 28. Oxygen Forensic Suite

If you are investigating a case that requires you to gather evidence from a mobile phone to support your case, [Oxygen Forensics Suite \(Standard Edition\)](#) is a tool that will help you achieve this.



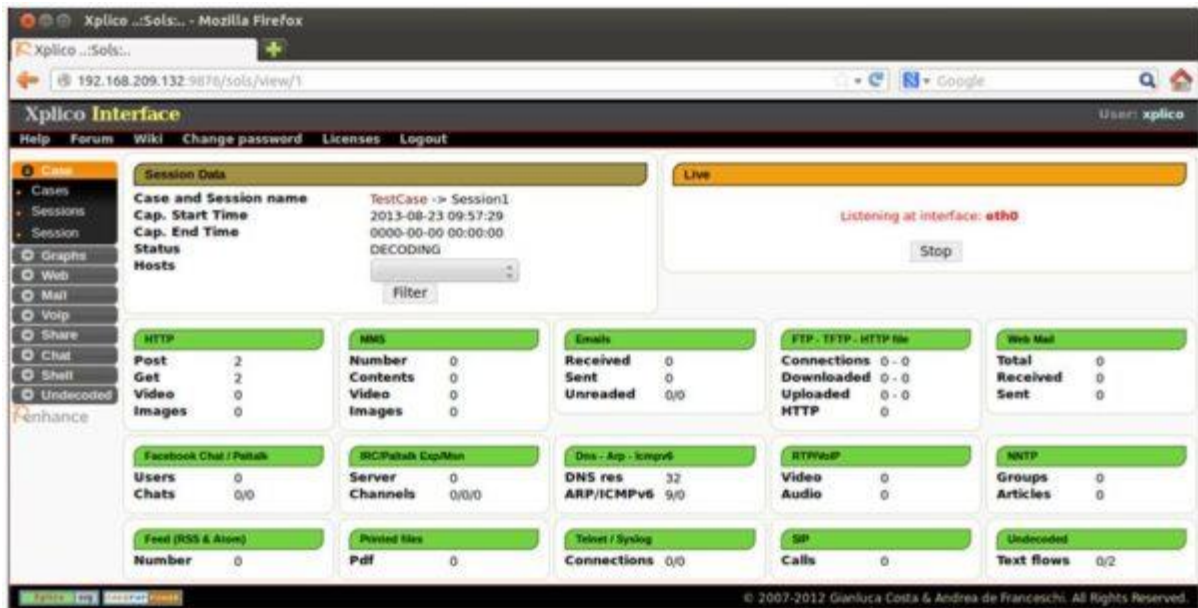
## 29. Free Hex Editor Neo

[Free Hex Editor Neo](#) is a basic hex editor that was designed to handle very large files. While a lot of the additional features are found in the commercial versions of Hex Editor Neo, I find this tool useful for loading large files (e.g. database files or forensic images) and performing actions such as manual data carving, low-level file editing, information gathering, or searching for hidden data.



## 30. Xplico

[Xplico](#) is an open source Network Forensic Analysis Tool (NFAT) that aims to extract applications data from internet traffic (e.g. Xplico can extract an e-mail message from POP, IMAP or SMTP traffic). Features include support for a multitude of protocols (e.g. HTTP, SIP, IMAP, TCP, UDP), TCP reassembly, and the ability to output data to a MySQL or SQLite database, amongst others.



# Mobile Forensic Process: Steps and Types

## Introduction:

Mobile forensics is a branch of digital forensics related to the recovery of digital evidence from mobile devices. “Forensically sound” is a term used extensively in the digital forensics world to qualify and justify the use of a particular forensic technology or methodology. The central principle for a sound forensic examination is that the original evidence must **not be modified**. Let’s understand this very important process step by step.

## Steps:

1. **Identifying** is the location of evidence (on a mobile phone).
2. **Preserving** it means making sure that the integrity of the digital evidence is not manipulated in any way, shape, or form. Preservation must also consist of protecting or shielding the evidence from any radio interference such as a mobile data network, Wi-Fi, Bluetooth, or any other application which can give the device a remote connection. One of the best ways to isolate a mobile device is by putting it into a Faraday Bag which prevents the transmission of the electromagnetic waves. **Seizing** the evidence is the process to protect it from physical damage which includes the secure evacuation of evidence and proper transportation of it to protect it from



any electromagnetic, electric shock, excessive heat, etc. This is to protect from any tampering.

In hand with these steps, clear **documentation** is to be maintained (aka the “Chain of Custody” forms) for future reference, such as in a court of law. This **Chain of custody** contains details pertaining to evidence values, any special notes, a chain which describes the handover of the evidence from an individual to another entity, with the date and time captured in these instances. Another part of documentation is taking pictures (photographs) of the crime scene, capturing the original state of the mobile device, as well as the make, model, serial numbers and so on. The other of the phone – such as IMEI number or operating system version – which would help during the acquisition phase and need to be captured as well.

3. **Forensic acquisition** is the process of acquiring the original evidence in a forensically sound manner while maintaining the integrity of it. This process is also known as “Imaging.” It can be done on site (at the scene) and can also be done off-site (in the lab). The acquisition tools of today now possess the technical capabilities to break the passcode/pin/pattern of just about any mobile device.
4. In the **examination phase**, the image is captured from the original evidence. It also consists of data which is deleted or hidden on the mobile device. In these instances, the relevant and irrelevant data is segregated by the forensic analyst based on the case background shared by the investigator. In the analysis phase, the analyst looks for the correlation between the relevant data (revealed during the examination phase) and sets priorities to this data set based on the proceeding investigation. In summary, the examiner looks to collect as much information as he or she can, and builds up the evidence. Some of the common types of evidence are the contacts, call logs, SMS, Audio and Video files, emails, any saved notes (this might contain passwords for other accounts), saved geographic location, web activity, and social media updates and chats.
5. Reporting is a comprehensive summary of the results of the mobile forensics investigation. This phase also explains the reason why a particular step was performed with the result that followed from it. The final report also consists of all the compiled documentation, which include the Chain of Custody forms, photographs, etc.

### Types:

There are several types of Mobile Forensics Processes which are based on the below-mentioned parameters:

1. Type of phone (Make, Model, Manufacture)
2. Operating System
3. Encryption level
4. Availability of necessary passcode/pin code/pattern

## **Manual Method:**

In the manual method, the device is browsed through manually by the forensic specialist. The data on the phone is directly seen/observed/accessed by using its keypad or touchpad. It is a quick method as the examiner is aware of which data to browse first. This method holds the advantage of viewing specific data in a readable format using its native application as it is being observed directly by the forensics investigator. However, this method is prone to human error and biases. Also, it would take a lot of time to capture all the needed data from the mobile device in question.

## **Logical Method:**

The Logical Method is a quick way of extracting data from the user files directly. The advantage of this method is that it can be viewed easily in the mobile forensic tools. The size of the extracted data is less as the data is not acquired from the flash memory. However, the disadvantage of this method is that it cannot recover deleted data/items from the mobile device.

## **Physical Method:**

The Physical Method consists of accessing flash memory of the mobile phone and extracting data from that space. In this case, the flash memory is being accessed directly to garner the existing data, and the deleted data also gets captured as well. This method proves to be very beneficial in many forensics cases. To access the flash memory, tools use a bootloader to bypass the security patch of the mobile device.

## **File System:**

The File System method extracts data from the system level of the mobile device in question. In this process, information and data related to the applications of the mobile device also get extracted. It is the OS which stores information related to the deleted files in the file system.



# Introduction to Mobile Forensics

Mobile Forensics is a branch of Digital Forensics and it is about the acquisition and the analysis of mobile devices to recover digital evidences of investigative interest.

When we talk about Mobile Forensics generally, we use the term “*Forensically Sound*”, commonly used in the forensic community to define the application of methods and techniques, which respect the international guidelines for acquisition, and examination of mobile devices. The principles for the correct application of Forensically Sound techniques assume the primary purpose, which is the preservation and the possibility of non-contamination of the state of things.

All the phases, from the acquisition to forensics analysis of the mobile device, have to totally avoid non-alteration of the examined device. This process is not easy at all, particularly in mobile devices.

The continuous evolution of mobile devices technology, allows the commercialization of new mobile phones, which creates new digital investigations problems.

Hardware and software for these type of mobile device analysis are numerous, but none is able to give an integrated solution for the acquisition and the forensic analysis of all smartphones.

Furthermore, mobile devices are able to contain plenty of digital information, almost like a computer, so not only a call log or SMS messages as old mobile phones. Many of the digital information in a smartphone is reliant on applications installed on it, which evolve in such a variety that analysis software are not able to support them completely.

Often the data acquisition from a mobile device is not compatible with some parameters, which define a *Forensically Sound* method.

In other words to have access to the mobile device it is necessary to use communication vectors, *bootloader* and other agents which are installed in the memory to enable the communication between the mobile phone and the instrument that we use for the acquisition and so it is not possible to use a *write blocking* option.

Often we resort on modify the device configuration for acquisition, but this operation risks to invalidate the evidence in the Court, even though all the techniques are always well-documented. As much as possible it is always fundamental to respect the international guidelines on mobile forensic to ensure the evidence integrity and the repeatability of the forensic process.

A fundamental aspect on device preservation at the crime scene is evidence collection on site; that is the preservation of the device found turned on, safeguarding it from Wi-Fi signals, telecommunication systems, GPS signals and

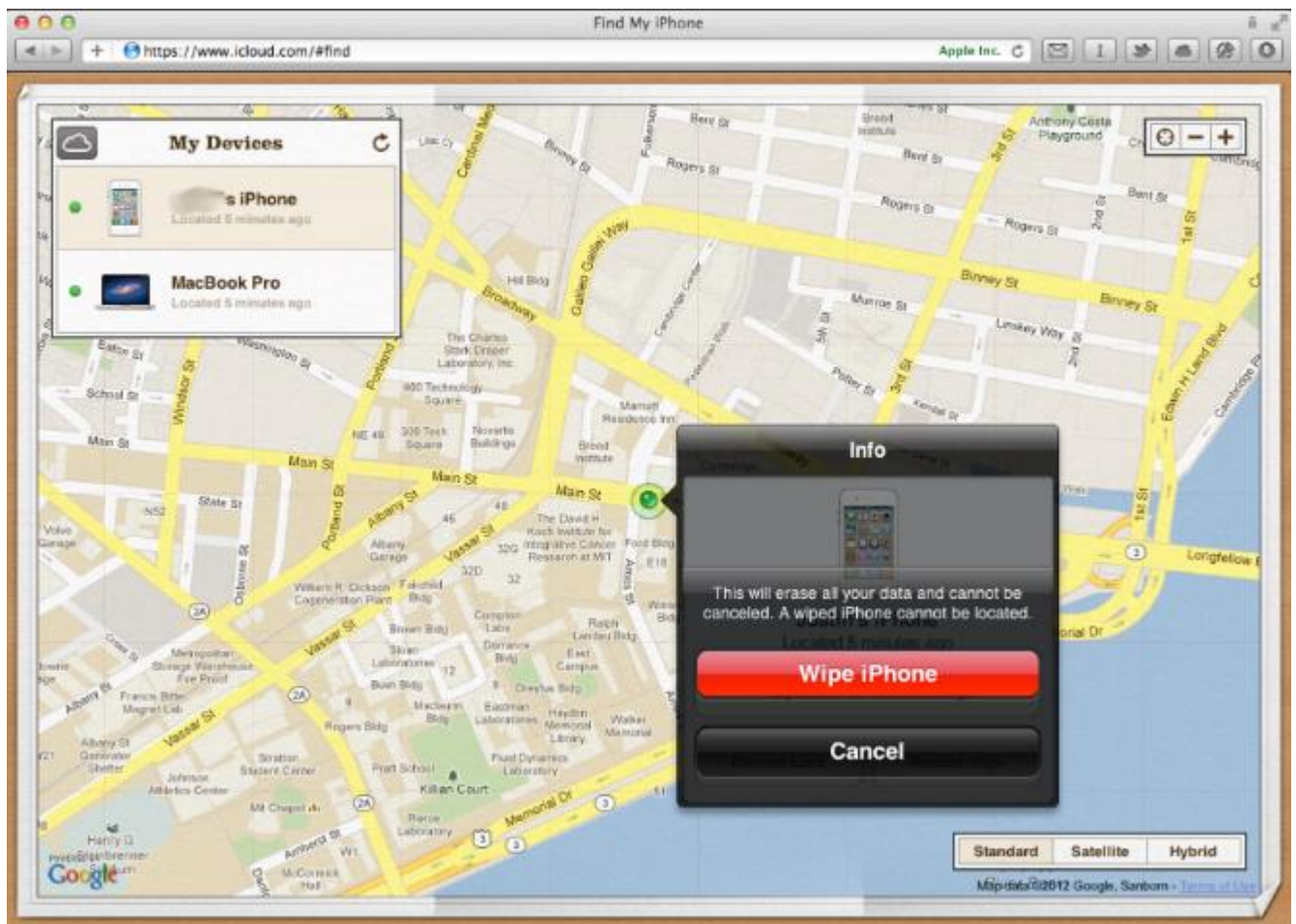
keeping the battery on charge. This is required to avoid its shutdown and the loss of important information such as a PIN.

The shutdown could entail a later PIN bypass or even a data loss because of passwords or cryptography. It is also fundamental to immediately provide electromagnetic isolation using faraday bags; devices or cases, which allows isolating the mobile device, darkened from radio signals.



**Figure 1.0 – Faraday bag**

A practical example of a device found in to a crime scene and, not isolated, it can be the complete remote wiping.



**Figure 1.1 – Remote wiping command of an iPhone**

The production process of the forensic evidence is divided in five main phase: the seizure, the identification, the acquisition and the examination or analysis. Once the data is extracted from a device, different methods of analysis are used based on the underlying case. As each investigation is distinct, it is not possible to have a single definitive procedures for all cases.

Each one of these steps has a basic role in the process of digital evidence production. The international standard are fed by many studies and publications that try to define the best practices and the guidelines for procedures and methods for the digital forensic, such as lots of publications and NIST guidelines.

Although the most recent ISO 27037 certification “*Guidelines for identification, collection and/or acquisition and preservation of digital evidence*” released in 2012 it is not specific for mobile forensic, it concerns the ISO/IEC standard. This standard mostly defines methods and techniques in digital forensic investigations, which is accepted in many Courts.

However, the overall process can be broken into four phases as shown in the diagram Following:



Below will be elucidated the two first steps involved in the production of a forensic evidence. In the next lessons will be explained in detail the remaining three steps.

Handling the device during seizure is one of the important steps while performing forensic analysis. It is important, for device seizure on the crime scene, to document with pictures, writing the “where and when”, mobile condition, if it was damaged, turned on or switched off, picture of the display if switched on, document the event of memory cards.

It is necessary to seizure cables, chargers, SIM card data or any papers or notes which may contain access codes that can also be deduced from the personal papers of the criminals whose devices were confiscated. Statistically many users use password similar on date of birth, celebrations, names, number plates and other personal information to remind themselves of passwords. Look for PIN and password can save much time later to investigators.

On the crime scene, it is fundamental to use proper techniques to protect the device from communicating with other devices, which may be phone calls, SMS, Wi-Fi Hotspot interferences, Bluetooth, GPS and many more. It is necessary to place the device into a Faraday bag and if it is possible add the use of a jammer, to avoid the alteration of the original state of the device. A phone call, an SMS, an email may overwrite the previous ones during the evidence collection phase if the phone was not isolated.

### **MOBILE DEVICE ISOLATION TECHNIQUES**

**Faraday's bag** – The immediate use of a Faraday bag is essential in case finding a turned-on mobile phone. It is important to isolate the mobile phone keeping it on charge with an emergency battery which will allow you to arrive to the lab safely. It is also important for the power cord to be isolated because it may allow the mobile to receive communications. There are different types of Faraday bags on sale that go from simple bags isolated from radio signals (which I do not recommend) to real isolation boxes which allow more efficiency. They are made up of silver/copper/nickel with RoHS double layer conductors. A Faraday bag can be a great solution to isolate the seizure mobile device



**Figure 1.4 – Faraday bag pro**

**Jamming** – The jammers are devices, also known as radio jammers, used to block the use of mobile phones sending radio waves with the same frequency used by mobile phones. This causes an interference, which inhibits the communication between mobiles and BTS, paralyzing every phone activity in its range of action.

Most mobile phones, encounter this disturbance merely as a lack of network connection. In case of mobile evidence collection jammer devices are used to block radio communications from GSM/UMTS/LTE. Obviously, the use of a jammer in these circumstances must be limited to a power that is less ( $<1W$ ), otherwise it can disturb every telephone network around. The use is illegal in some countries and it is often allowed only to police forces.





**Figure 1.5 – Jammer GSM -UMTS – LTE**

**Airplane mode** – The airplane mode is one of the options that can be used to protect the mobile collected into the crime scene to avoid in and out radio transmission. It is a risky option because it is necessary to interact with the mobile phone, and possible only if the phone is not protected with Passcode. To activate iOS on this option, from iOS7 with display locked, airplane mode can be set sliding the dock upward. To set the mode aereoplane in the Android OS:

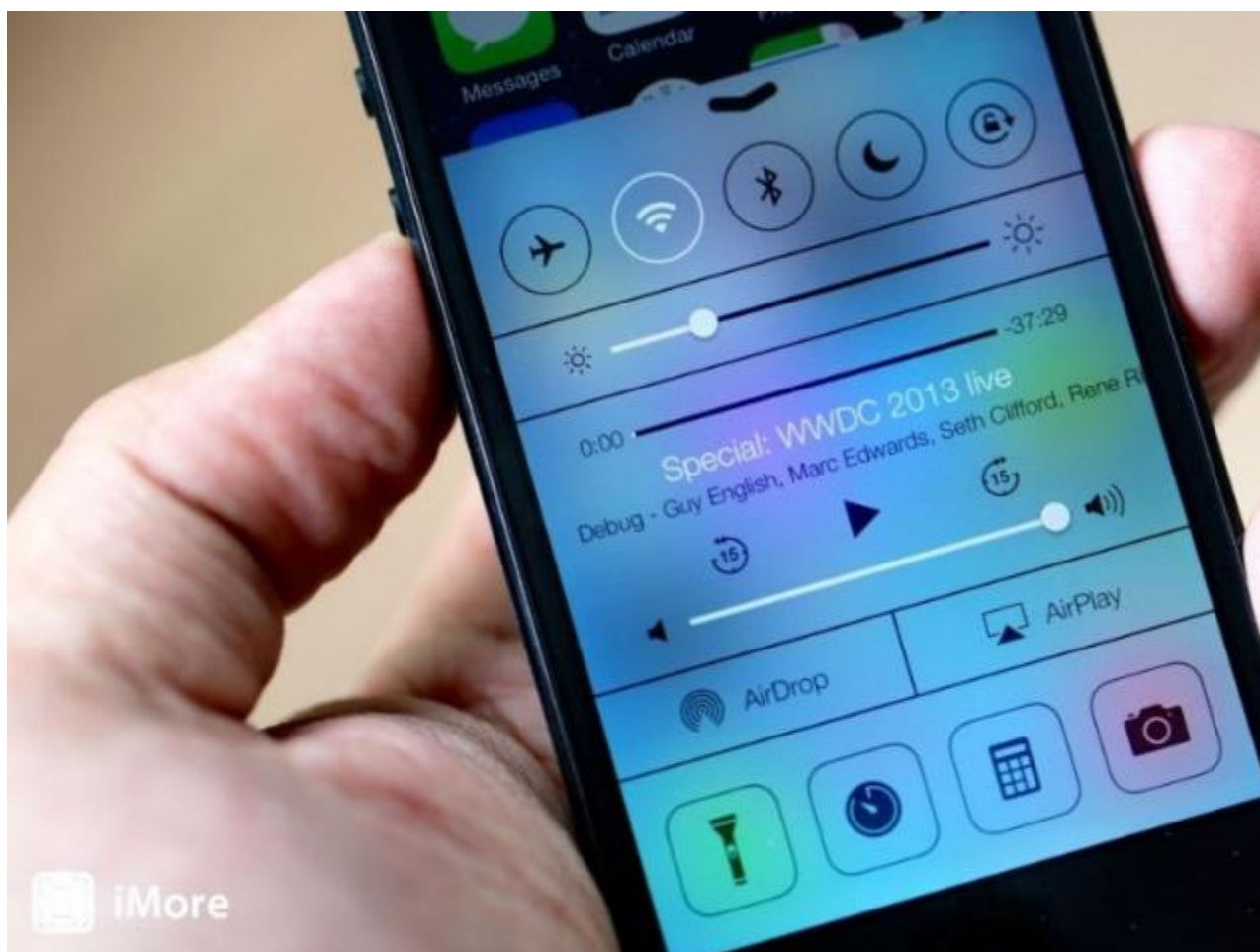
1. Click the menu button on the phone to open the menu.

---
2. Select "Settings" at the bottom of the menu that comes up

---
3. Under "Wireless & Networks", tap on "More"

---
4. Look for the "Airplane mode" option at the top of the settings screen. Tap on it to put a "check mark" on the box beside it

---
5. Wait for the on button to turn blue. This tells you that the mode is active and your transmissions are now off.



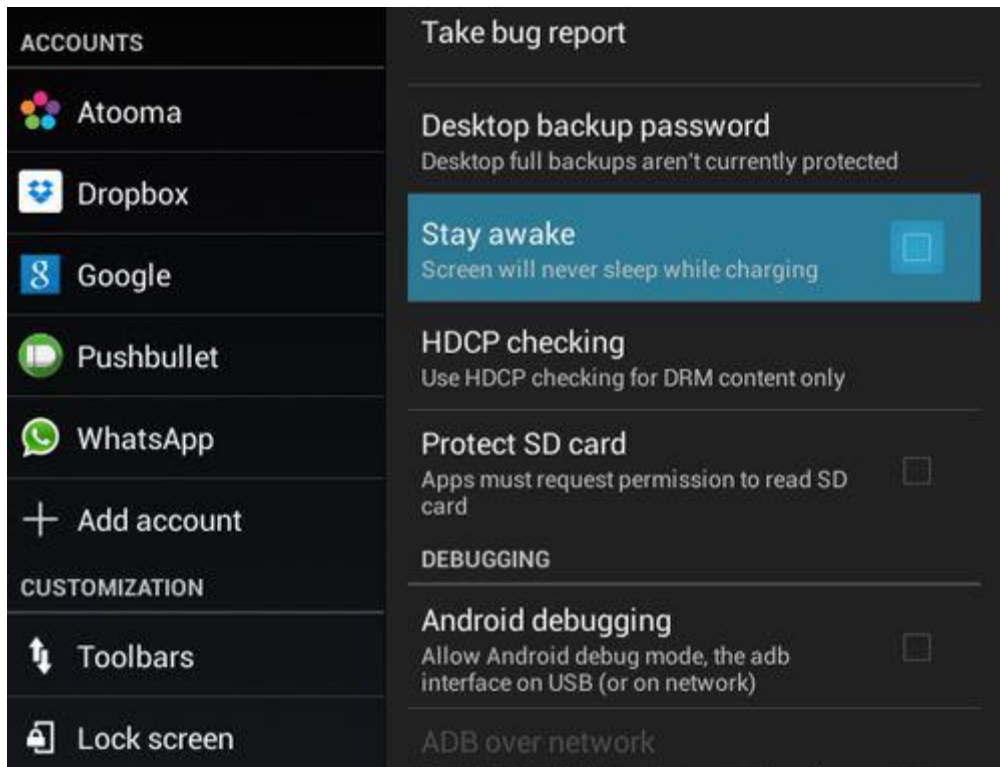
**Figure 1.6 – Airplane mode iOS 7/8 activation**

The technical methods of protection devices, we mentioned in the previous paragraphs, they should be used more attention for Android devices, compared to Apple devices. As they are sequestered, it takes attention to be sure that our actions will not cause any change of data on the device. In the meantime, it is necessary to use every and each opportunity that might help the following analysis.

If the device is found unlocked on the crime scene, in other words without lock screen or access code, it is necessary to change device's settings to have a better access on the device.

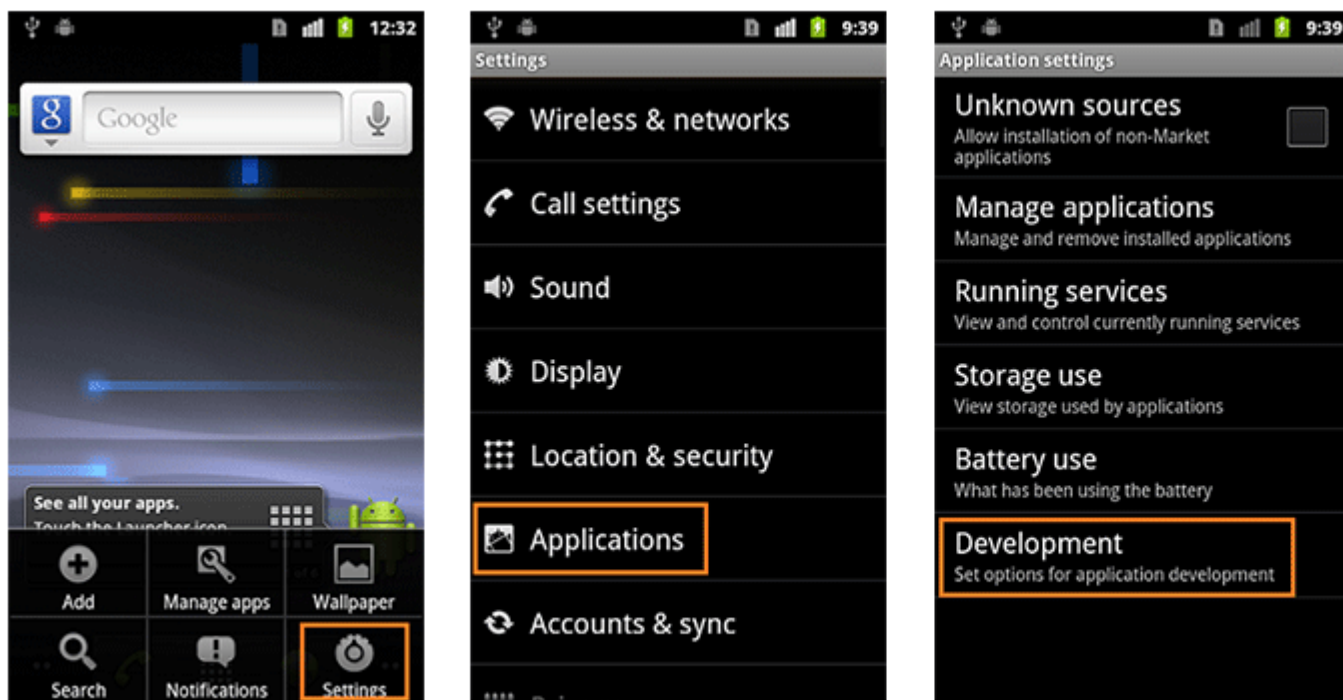
Some of the settings it is necessary to modify in this situation are:

**Enable stay awake setting:** by activating this option and putting the device on charge (it can be used as an emergency charger), it allows keeping the device active and with unlocking setting. On Android devices can be found in Settings | Development, as shown in the following screenshot:



**Figure 1.7 – Enable USB Debugging Android OS 4.2**

**Activation of debug USB:** the activation of this option allows a major access on the device with Android Debug Bridge (ADB) connection. This option will be a great tool for the forensic examiner during the extraction data process. On Android devices, this option can be found in Settings | Development:



**Figure 1.8 – Enable USB Debugging Android OS**

In next Android versions, from 4.2, the development settings are hidden by default setting. For the activation, Settings | About phone and tap Build number seven times.



**Figure 1.9 – Enable USB Debugging Android OS 4.2**

## APPLE IPHONE

Before the analysis of an iPhone it is necessary to identify the hardware type and which firmware is installed on. Easier it is to check the rear of the device's shell, where it is impressed:



**Figure 2.0 – Hardware number iPhone**

About the firmware version, it is possible to check that by accessing on iPhone menu - **Settings/General/About/Version:**

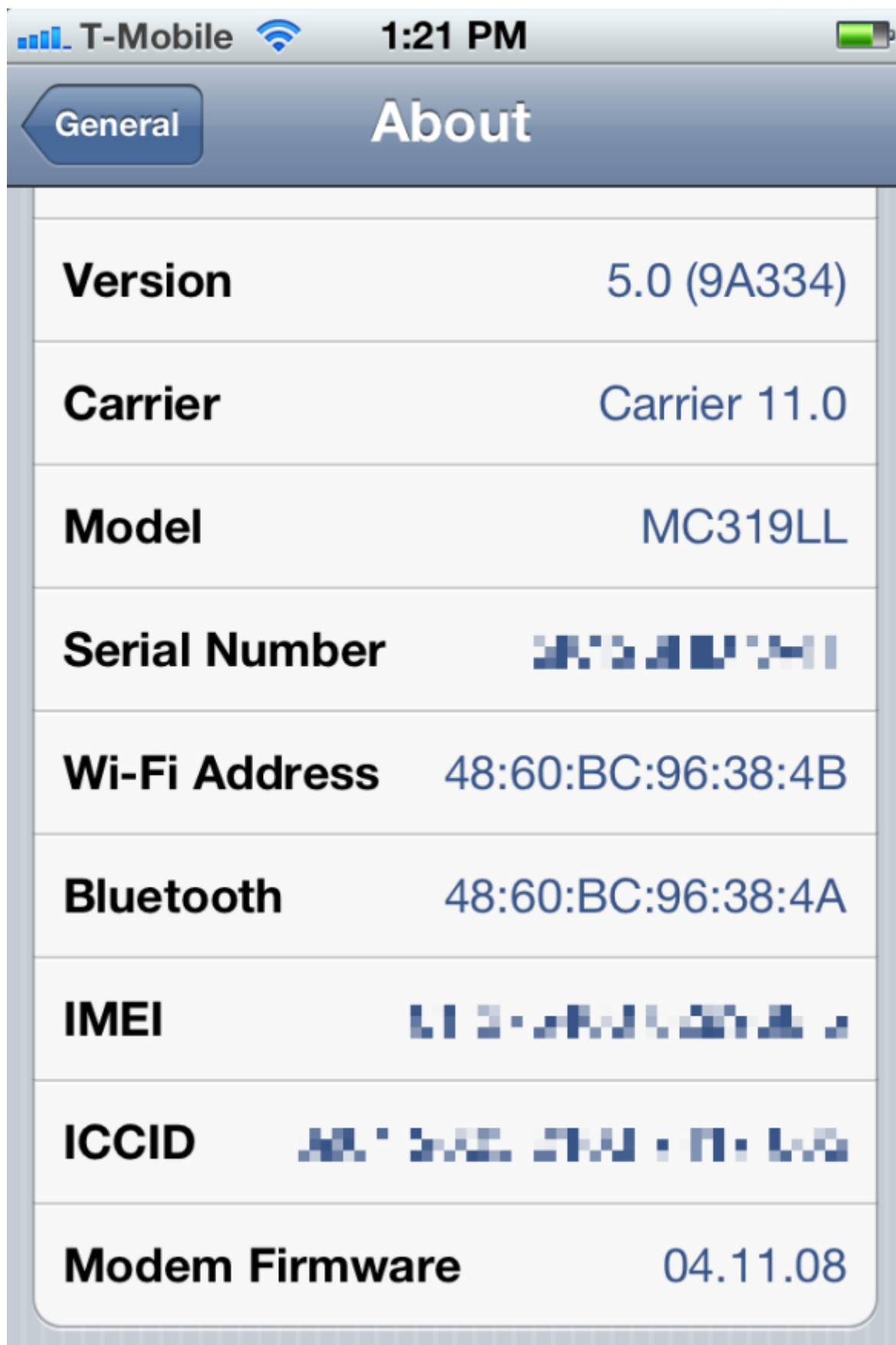


Figure 2.1 – firmware version iPhone



A good alternative to get lots of information from an iPhone is the use of libimobiledevice ( <http://www.libimobiledevice.org> ), currently released in 1.2 version, are a good alternative to communicate with Apple devices among which iPhone, iPad, iPod Touch, Apple TV. They do not need Jailbreak, and they allow reading device's information, backup and restore and similar options on the logical *file system* acquisition. They can be downloaded and used in Linux environment, are integrated in live distro Santoku ( <https://santoku-linux.com/> ).

## **Practical Exercise**

In this practical exercise, we get information from an Apple iPhone Smartphone:

**Step one** – Download to web site <https://santoku-linux.com/>, the santoku live distro – named santoku\_0.5.iso -, burn it in DVD-ROM and start with boot.

**Step two** - Running libimobiledevice, navigate to Santoku → Device Forensics → lib-iMobile



**Figure 2.2 – Running lib-iMobile on Santoku**

**Step three** - This should open a terminal window and list the commands available in the libimobiledevice tool.

```
santoku@santoku: ~  
File Edit Tabs Help  
$ ls /usr/bin/idevice*  
/usr/bin/idevicebackup          /usr/bin/ideviceimagemounter  
/usr/bin/idevicebackup2        /usr/bin/ideviceinfo  
/usr/bin/idevicecrashreport     /usr/bin/idevicename  
/usr/bin/idevicedate           /usr/bin/idevicepair  
/usr/bin/idevicedebugserverproxy /usr/bin/ideviceprovision  
/usr/bin/idevicediagnostics    /usr/bin/idevicescreenshot  
/usr/bin/ideviceenterrecovery  /usr/bin/idevicesyslog  
/usr/bin/idevice_id  
santoku@santoku:~$
```

**Figure 2.3 – list command available on the libimobiledevice tool**

**Step four -** At this point, you can connect your iOS device to Santoku. If you are using a VM, make sure the USB device is “attached” to the VM and not the host.

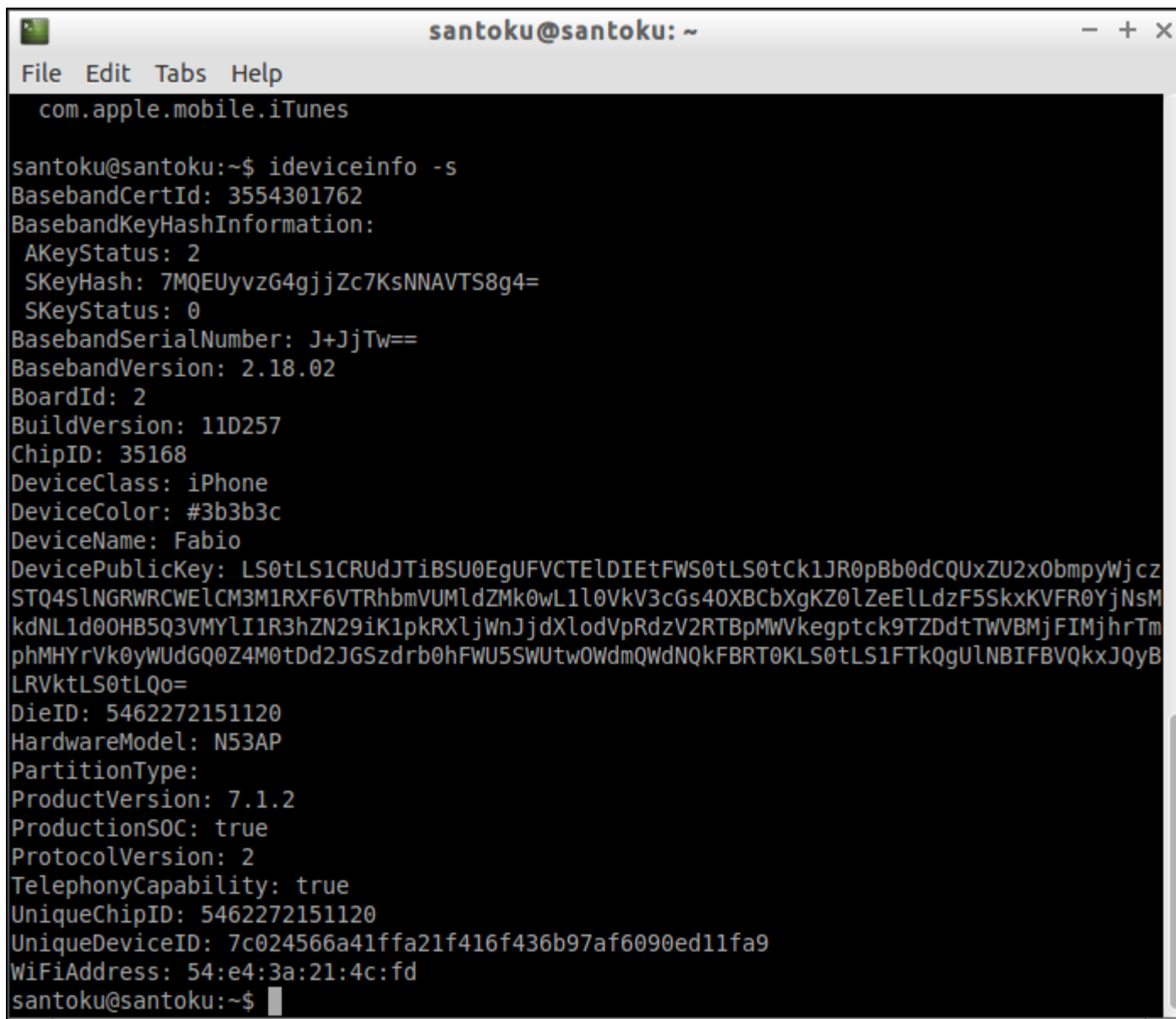


**Figure 2.4 – iPhone connected to Santoku**

**Step five:** You can easily check the connectivity between your iPhone and Santoku by type this command in a terminal window:

## **idevice\_id -s**

The command gives all the information you see in the picture, including the devicename, UDID, the hardware model and many more.

A screenshot of a terminal window titled 'santoku@santoku: ~'. The window has a menu bar with 'File', 'Edit', 'Tabs', and 'Help'. The terminal shows the command 'ideviceinfo -s' being executed, which returns a large block of text containing various device identifiers and specifications. The text is as follows:

```
com.apple.mobile.iTunes

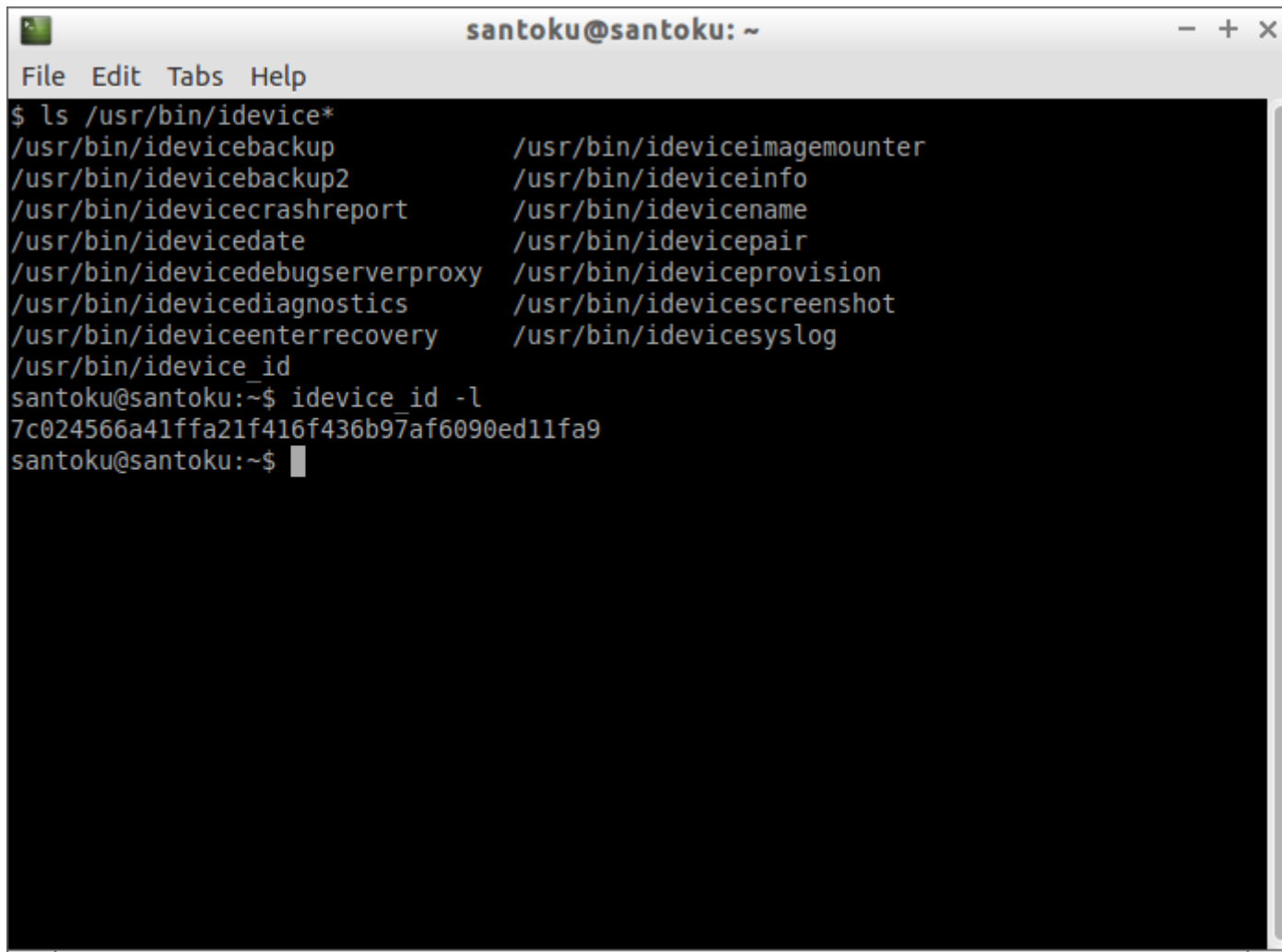
santoku@santoku:~$ ideviceinfo -s
BasebandCertId: 3554301762
BasebandKeyHashInformation:
  AKeyStatus: 2
  SKeyHash: 7MQEUyvzG4gjjZc7KsNNAVTS8g4=
  SKeyStatus: 0
BasebandSerialNumber: J+JjTw==
BasebandVersion: 2.18.02
BoardId: 2
BuildVersion: 11D257
ChipID: 35168
DeviceClass: iPhone
DeviceColor: #3b3b3c
DeviceName: Fabio
DevicePublicKey: LS0tLS1CRUdJTiBSU0EgUFVCTEldIETFSW0tLS0tCk1JR0pBb0dCQUxZU2x0bWpyWjcz
STQ4S1NGRWRCWE1CM3M1RXF6VTRhbmVUMldZMk0wL1l0VkV3cGs4OXBCbXgKZ0lZeElldzF5SkxKVFR0YjNsM
kdNLld00HB5Q3VMYlI1R3hZN29iK1pkRXljWnJjdXlodVpRdzV2RTBpMWVkegptck9TZDdtTWVBMjFIMjhrTm
phMHYrVkyWUdGQ0Z4M0tDd2JGSzdrb0hFWU5SWUt0WdmQWdNQkFBRT0KLS0tLS1FTkQgUlNBIFBVQkxJQyB
LRVktLS0tLQo=
DieID: 5462272151120
HardwareModel: N53AP
PartitionType:
ProductVersion: 7.1.2
ProductionSOC: true
ProtocolVersion: 2
TelephonyCapability: true
UniqueChipID: 5462272151120
UniqueDeviceID: 7c024566a41ffa21f416f436b97af6090ed11fa9
WiFiAddress: 54:e4:3a:21:4c:fd
santoku@santoku:~$
```

**Figure 2.5 – result of the `idevice_id -s` command**

If you want to see only the iPhone's UDID run the command:

## **idevice\_id -l**

This should return the UDID of your phone.

A screenshot of a terminal window titled 'santoku@santoku: ~'. The window has a menu bar with 'File', 'Edit', 'Tabs', and 'Help'. The terminal shows the following commands and output:

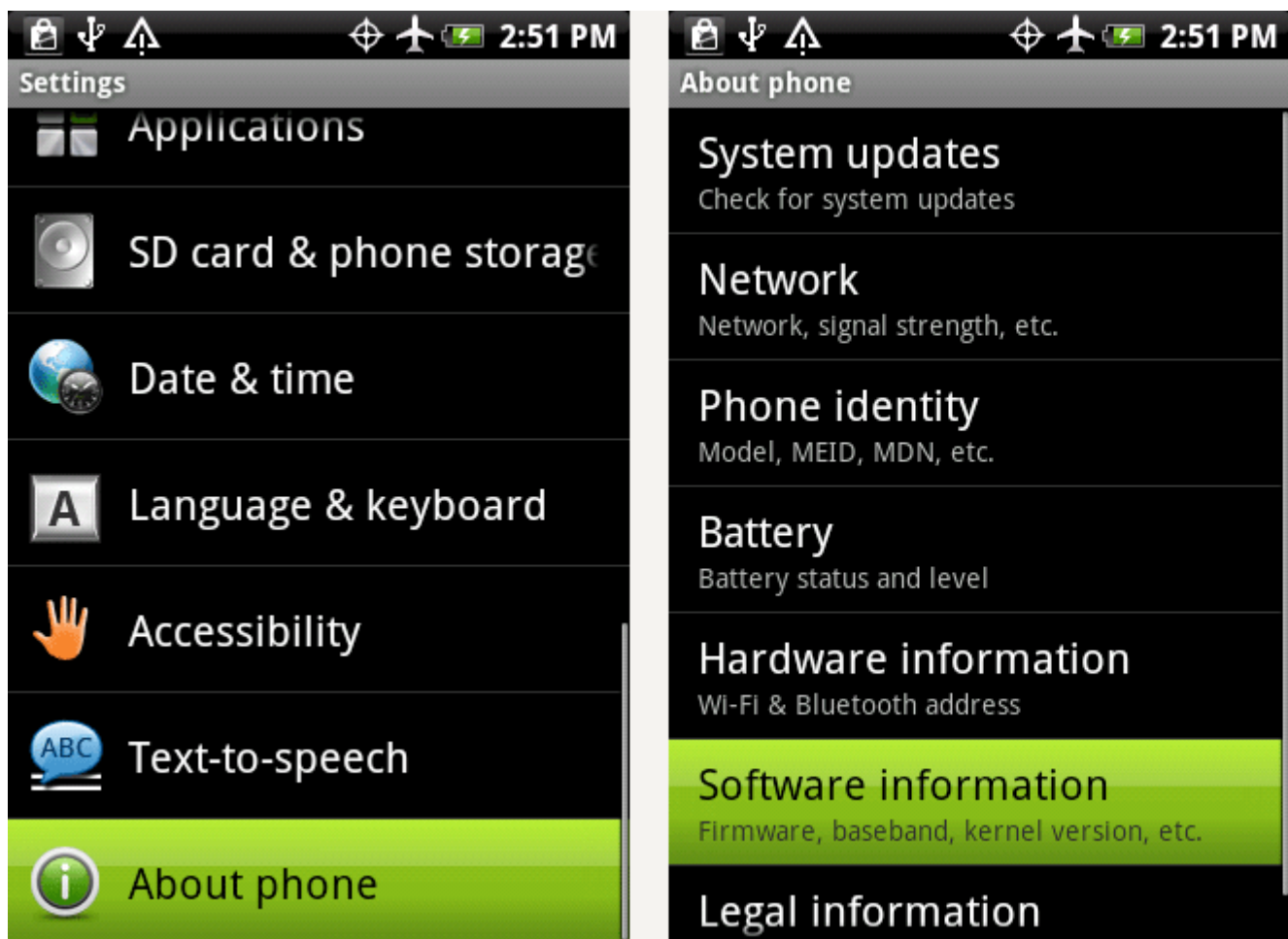
```
$ ls /usr/bin/idevice*
/usr/bin/idevicebackup          /usr/bin/ideviceimagemounter
/usr/bin/idevicebackup2        /usr/bin/ideviceinfo
/usr/bin/idevicecrashreport     /usr/bin/idevicename
/usr/bin/idevicedate           /usr/bin/idevicepair
/usr/bin/idevicedebugserverproxy /usr/bin/ideviceprovision
/usr/bin/idevicediagnostics    /usr/bin/idevicescreenshot
/usr/bin/ideviceenterrecovery  /usr/bin/idevicesyslog
/usr/bin/idevice_id
santoku@santoku:~$ idevice_id -l
7c024566a41ffa21f416f436b97af6090ed11fa9
santoku@santoku:~$
```

Figure 2.6 – result of the `idevice_id -l` command

## ANDROID

To get information from an Android device is easy.

Go on menu Settings/About Phone/Software and Hardware information, as shown in the screenshot:



**Figure 2.7 – Android Settings –About Phone**

### **PRACTICAL EXERCISE**

In this case, we use a Host Windows and Android Software Development Kit. The Android Software Development Kit (SDK) helps developers build, test, and debug applications to run on Android. It includes software libraries, APIs, emulator, reference material, and many other tools. These tools not only help create Android applications but also provide documentation and utilities that help significantly in forensic analysis of Android devices. Having sound knowledge of the Android SDK can help you understand the particulars of a device. This, in turn, will help you during an investigation. During forensic examination, the SDK helps us connect the device and access the data present on the device.

The method to get the serial number of an Android device is the following:

**Step one** – Download from web site the SDK

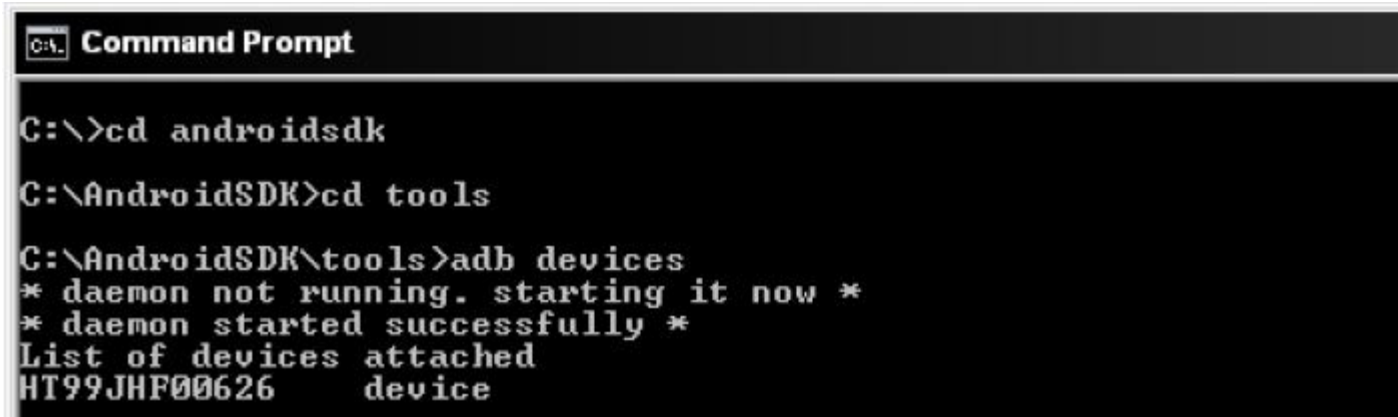
package: [https://developer.android.com/sdk/download.html?v=archives/android-sdk-windows-1.6\\_r1.zip](https://developer.android.com/sdk/download.html?v=archives/android-sdk-windows-1.6_r1.zip)

**Step two** – Create a folder called ANDROIDSDK and unzip the zip file you downloaded

**Step three** – Connect your Android device via USB cable

**Step four** – In the command prompt Windows, browse on the ANDROIDSDK folder, tools, and we run adb device command

**Step five** – If all work properly, a list of linked devices will appear with a serial number, if not present on devices' list, check that the proper work of the driver and *USB debugging enabled*.

A screenshot of a Windows Command Prompt window. The title bar reads "C:\. Command Prompt". The command history shows the user navigating to the Android SDK tools directory and running the 'adb devices' command. The output indicates the adb daemon is started successfully and lists one device: 'HT99JHF00626 device'.

```
C:\>cd androidsdk
C:\AndroidSDK>cd tools
C:\AndroidSDK\tools>adb devices
* daemon not running. starting it now *
* daemon started successfully *
List of devices attached
HT99JHF00626    device
```

**Figure 2.8 – Windows Command Prompt – adb devices**