Classification of Digital forensics

Digital forensics

Digital forensics deal with the recovery and investigation of digital storage media to get the evidence, to prove the crime in court.

Classification of Digital forensics

- Computer Forensics
- Mobile device forensics
- Network forensics
- Database Forensics
- Malware Analysis

Computer forensics

- Computer forensics is the practice of identifying, extracting and considering evidence from digital media such as computers, embedded systems and static memory (such as USB pen drives).
- Computer forensics can deal with a broad range of information like
- logs (such as internet history) through to the actual files on the drive.
- Window registry Analysis
- OS Analysis
- Memory analysis

Mobile device forensics

- Mobile device forensics is a sub-branch of digital forensics relating to recovery of digital evidence or data from a mobile device.
- It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g. GSM).
- Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data.
- Mobile devices are also useful for providing location information; either from inbuilt gps/location tracking or via cell site logs, which track the devices within their range.
- Use of mobile phones to store and transmit personal and corporate information.
- Use of mobile phones in online transactions.

The Big Difference

- Computer Forensics: – Only a Few Major Operating System Standards: Windows, Mac, Linux. Standard practice is to image the Harddrive and Examine Data.

- Cell Phone Forensics: – Multiple Operating Systems. Various Communication Standards. Each manufacturer has their own: Nokia, Samsung, Motorola, Blackberry, etc. Communication Standards Evolving.

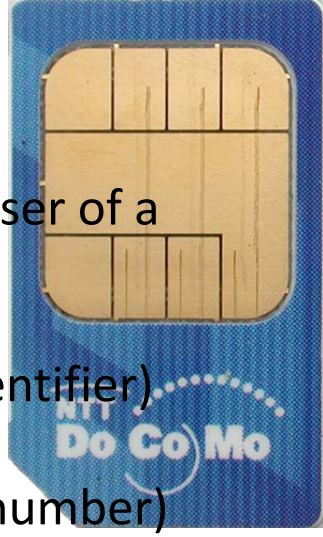
- Mobility Aspect: - Phones are Live Things Roaming Around. It's not just about what's on the device, but where has it been and what connections have been made?

Another Difference: Phones Are Always Updating

A phone is always updating with the network, and remote destruction is possible. Proper isolation of the device from the network and immediate analysis is best when possible.

What evidence can be obtained?

SIM on GSM Phones



- IMSI: International Mobile Subscriber Identity (used to identify the user of a cellular network)
- ICCID: Integrated Circuit Card Identification (SIM Serial No.)
- (Each SIM is internationally identified by its integrated circuit card identifier)

- MSISDN: Mobile Station Integrated Services Digital Network (phone number) (**MSISDN**) is a number used to identify a mobile phone number internationally.

- LND: Last Number Dialled (sometimes, not always, depends on the phone)

- Phonebook (AND): Abbreviated Dialled Numbers
- SMS: Text Messages, Sent, Received, Deleted, Originating Number, Service Center (also depends on Phone)
- SMS Service Center Info: GPRS Service Center Info:

- IMEI: International Mobile Equipment Identity. – unique for each phone to identify valid devices and therefore can be used for stopping a stolen phone from accessing that network.

Evidence

- Phonebook
- Call History and Details (To/From)
- Call Durations
- Text Messages with identifiers (sent-to, and originating) Sent, received, deleted messages
- Multimedia Text Messages with identifiers
- Photos and Video (also stored on external flash)
- Sound Files (also stored on external flash)
- Network Information, GPS location
- Phone Info (CDMA Serial Number)
- Emails, memos, calendars, documents, etc. from PDAs.
- GPS Info, Social Networking Data

- Logical Tools Getting Contacts, Call logs, SMS, MMS, Pics – Much more.
- Facebook Contacts, Skype, YouTube data, whatsapp data
- Myspace Username and Passwords
- Location from GPS, Cell Towers and Wi-Fi networks

Network Call Data Records

Data Available For Investigators
Call Data Records “CDR”

Cell Site Analysis

Other Data Available For Investigators - Cell Site Analysis

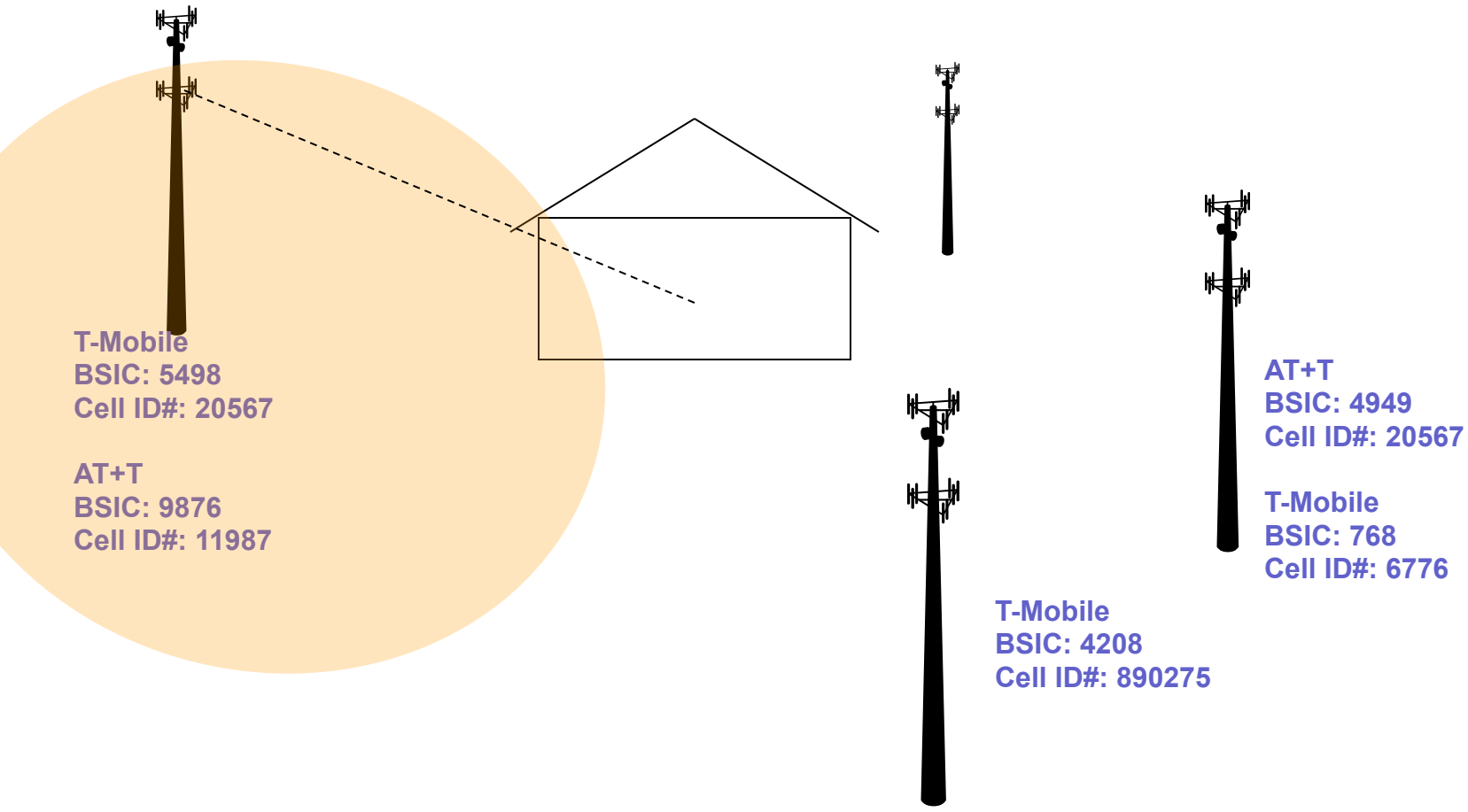
What Is It?

The Analysis of a Mobile Network's Radio Signal Coverage Relative to Its Users.

Network Call Data Records to Prove / Disprove Users Location on the Network.

Cell Site Analysis – What The Network Says…

What The Network Data Would Indicate as to Cell Coverage



The Mobile Device Forensic Process Tools and Techniques

Data Capture Options

- **Screen Captures:** The simplest way. Use a camera to take pictures of what's on the screen. Reporting tools available. Sometimes this is the only way.

- **Logical Analysis:** – Extracting the data on the device that you see and can access on the device. No deleted information with this method. Call logs, phone books, sms messages, pictures, email, browsing etc. The "active" information on the device can be extracted using a "Logical" extraction tool. This is the standard method today. Plenty of tools and easy to use.

- **Physical Analysis:** – The practice of extracting data from the physical memory of the device, and removable memory. Like PC forensics, you are getting the raw binary / hex data. Requires decoding and understanding of language and techniques used by device manufacturers. Physical analysis is the way to get deleted information, but it is difficult and sparsely supported.

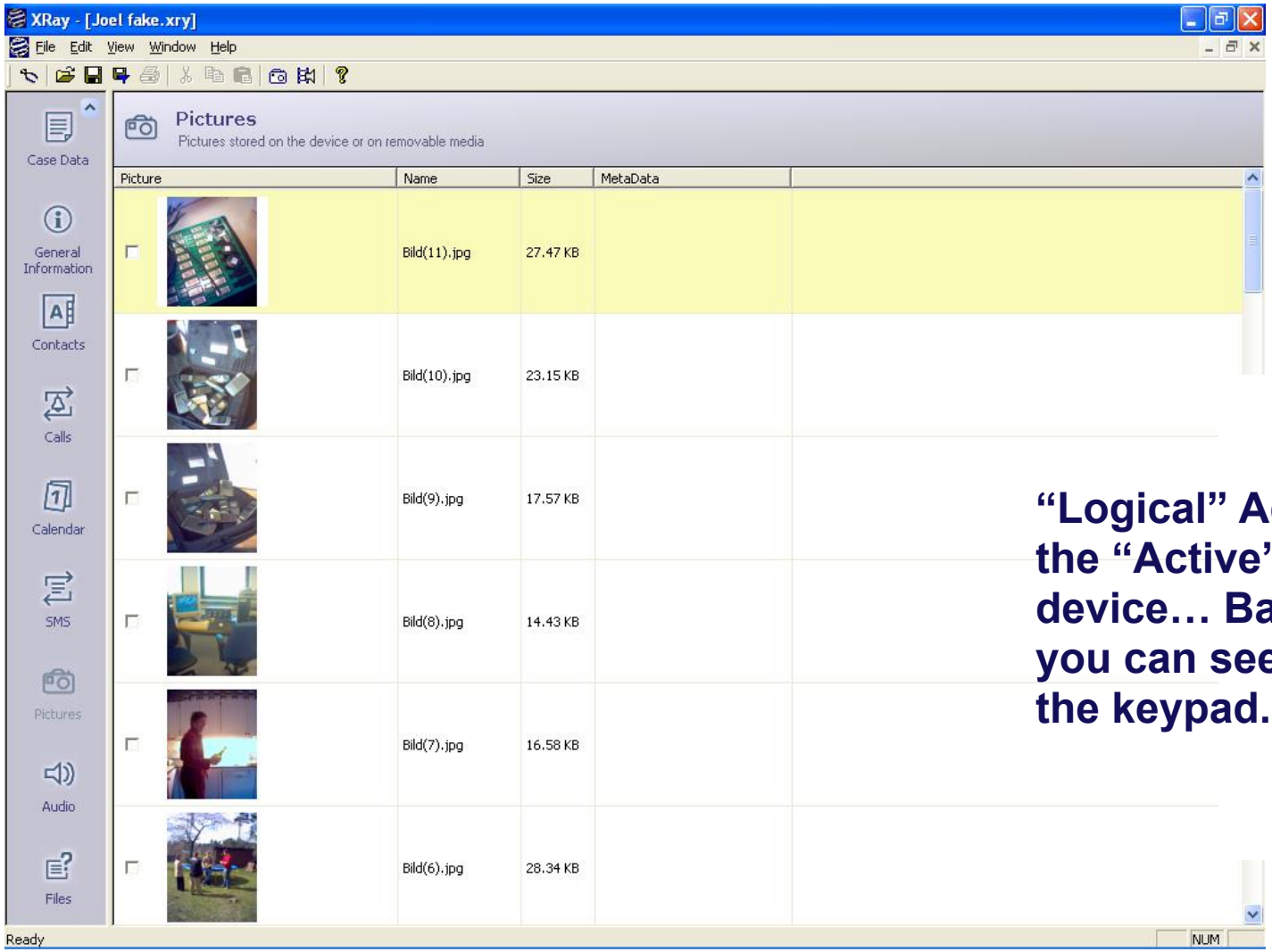
- **Chip Level Analysis:** - Analysis of the chips in the phone by removing them from the device and probing for data, or rebuilding another phone. Extremely technical. Broken SIMs analyzed this way.

Today's Mobile Device Forensic Solutions

Screen Capture

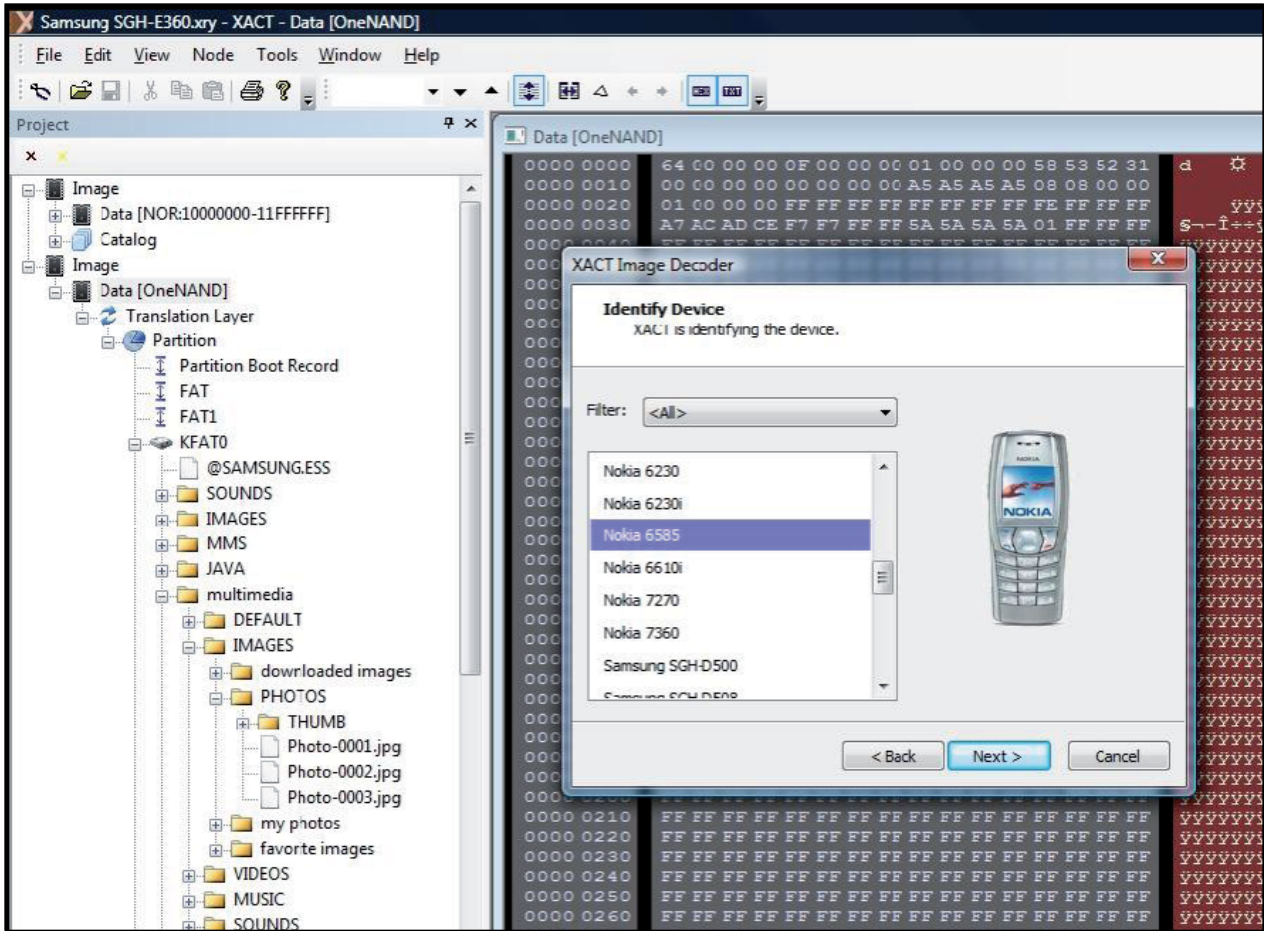
Sometimes Taking A Picture is The Only Way To Get Data Off of a Phone

Logical Acquisition



"Logical" Acquisition Pulls the "Active" Data off the device… Basically, anything you can see or access using the keypad.

Physical Acquisition



Today's Top Tools:

XRY Physical

And

UFED Physical

"Physical" Acquisition Accesses the Internal Memory and Pulls the Raw Data from the Memory. Formats and Storage Differ From Manufacturer to Manufacturer.

RF Protection – Required To Protect Device From The Network.

Faraday Box and Bag

RF Protection – Today Relying on Faraday Bags or Getting Devices in Airplane Mode Immediately and Keep Charged.

A Challenge for Forensic Efforts

- **Mobile is a disposable solution for criminals**
- **Some devices not widely supported by forensic solutions.**
- **Changing OS.**
- **Data Encryption and Password.**

Network Forensics

- Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.
- **More accurately, it is the use of scientifically proved techniques to collect and analyse network packets and events for investigative purposes.**

Analyzing Network Data

- Most critical and most time-consuming task
- Insufficient Tools for discriminating bogus traffic generated by an attacker from genuine traffic.

  So there is need to follow proper investigative procedure so that the evidences recovered during investigation can be produced in a court of law.

Network forensics can reveal the following information:

- How an intruder entered the network
- The path of intrusion
- The intrusion techniques an attacker used
- Traces and evidence

The Intrusion Process

Network intruders can enter a system using the following methods:

1) **Enumeration**(Gathering info about a network)

- Topology of the network
- List of live hosts
- Network architecture and types of traffic (for example, TCP, UDP, and IPX)
- Potential vulnerabilities in host systems

2)**Viruses:**Viruses are a major cause of shutdown of network components. A virus is a software program written to change the behavior of a computer or other device on a network, without the permission or knowledge of the user.

3) **Trojans:** Trojan horses are programs that contain or install malicious programs on targeted system. These programs serve as back doors and are often used to steal information from systems.

4) **E-mail infection**: The use of e-mail to attack a network is increasing. An attacker can use e-mail spamming and other means to flood a network and cause a denial-of-service attack.

5) **Router attacks**: Routers are the main gateways into a network, through which all traffic passes. A router attack can bring down a whole network.

6) **Password cracking:** Password cracking is a last resort for any kind of attack

Looking for Evidence

- **From the attack computer and intermediate computers:** This evidence is in the form of logs, files and tools.
- **From firewalls:** An investigator can look at a firewall's logs. If the firewall itself was the victim, the investigator treats the firewall like any other device when obtaining evidence.
- **From internetworking devices:** Evidence exists in logs and buffers as available.
- **From the victim computer:** An investigator can find evidence in logs, files, altered configuration files, remnants of Trojan files, files that do not match hash sets, tools, Trojans and viruses, stored stolen files, Web defacement remnants, and unknown file extensions.

Network Forensic Investigation Process

Follows basic procedures from beginning to end. The following are some of the elements of an end-to end forensic trace:

1) **The end-to-end concept:** An end-to-end investigation tracks all elements of an attack, including how the attack began, what intermediate devices were used during the attack, and who was attacked.
2) **Locating evidence:** Once an investigator knows what devices were used during the attack, he or she can search for evidence on those devices. The investigator can then analyze that evidence to learn more about the attack and the attacker.
3) **Pitfalls of network evidence collection:**

- Evidence can be lost in a few seconds during log analysis because logs change rapidly
- Gaps in the chain of evidence.
- Logs may be ambiguous, incomplete, or missing.

4) **Event analysis:** After an investigator examines all of the information, he or she correlates all of the events and all of the data from the various sources to get the whole picture.

Forensics Tools

- E-Detective
- Burst
- CapAnalaysis
- Cryptcat
- MaxMind

Network forensics

- Network forensics is concerned with the monitoring and analysis of computer network traffic, both local and WAN/ internet, for the purposes of information gathering, evidence collection, or intrusion detection.
- Traffic is usually intercepted at the packet level, and either stored for later analysis or filtered in real-time.
- Email Forensics, Packet Sniffer, IP Tracking

Database forensics

- Database forensics is a branch of digital forensics relating to the forensic study of databases and their metadata. Investigations use database contents, log files, DML, DDL command, data before and after transaction , previously deleted data and in-RAM data to build a timeline or recover relevant information.

- Incident verification- to examine the sign of penetration
- SQL server penetration
- Active unauthorized SQL server connection
- Past unauthorized SQL sever access from QL server error logs, plan cache, and other session details.

- Collection of artifacts
- Both volatile and non - volatile
- Volatile include data cache, active virtual log files, server state and ring buffers.
- Non volatile includes table stats, SQL server logins, authentication settings, native encryption, database users, database objects, jobs, triggers, SQL server error logs, trace files, data files, endpoints, CLR libraries, time configuration, server version.

Malware Forensics

- Malware Forensics is the process of understanding the behavior and purpose of a malicious codes,suspicious file or URL.

- ****
- A Malware is a set of instructions that run on your computer and make your system do something that an attacker wants it to do

- Steal personal information
- Delete files
- Click fraud
- Steal software serial numbers
- Use your computer as relay

- A trojan describes the class of malware that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the victim computer
- A root kit is a component that uses stealth to maintain a persistent and undetectable presence on the machine

- A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes and do so without any user intervention.

Infection Method

- Executable
- Interpreted file
- Kernel
- Service
- MBR
- Hypervisor

Malware Analysis

- Static malware Analysis - Static analysis is a process of analyzing a malware binary without actually running the code.

- Static analysis is generally performed by determining the signature of the binary file which is a unique identification for the binary file and can be done by calculating the cryptographic hash of the file and understanding each component.

Dynamic analysis

- Dynamic analysis involves running the malware sample and observing its behavior on the system in order to remove the infection or stop it from spreading into other systems.
- The system is setup in a closed, isolated virtual environment so that the malware sample can be studied thoroughly without the risk of damage to your system.
- In advanced dynamic analysis, a debugger can be used to determine the functionality of the malware executable which otherwise would have been difficult to obtain using other techniques. Unlike static analysis, it’s behavior-based so it’s hard to miss important behavior

Memory forensics

- **Memory Forensics** : This is the technique of analyzing the computer's RAM for forensic artifacts.
- Helps in malware analysis will assist in gaining an understanding of the malware's behavior after infection.
- Memory analysis is especially useful to determine the stealth and evasive capabilities of the malware.

Email forensics

- branch of digital forensics that focuses on the forensic analysis of email to collect digital evidence for cybersecurity attacks and cyber incidents.
- forensic investigation of Message-IDs, transmission routes, attached files and documents, IP addresses of servers and computers,

Email Header Analysis

-
- Email headers contain essential information, including the name of the sender and receiver, the path (servers and other devices) through which the message has traversed, etc.

```
Delivered-To: paul.friedman@gmail.com
Received: by 10.12.174.216 with SMTP id n34csp2326299qvd;
        Wed, 1 Feb 2017 00:39:09 -0800 (PST)
X-Received: by 10.28.27.14 with SMTP id b14mr1702258wmb.82.1485938349292;
        Wed, 01 Feb 2017 00:39:09 -0800 (PST)
Return-Path: <reply@activetrail.com>
Received:    from    i2.a01.ms18.atmailsvr.net    (i2.a01.ms18.atmailsvr.net.
[91.199.29.18])
        by          mx.google.com          with          ESMTPS          id
5si23398790wrr.176.2017.02.01.00.39.08
        for <paul.friedman@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Wed, 01 Feb 2017 00:39:09 -0800 (PST)
Received-SPF: pass (google.com: domain of reply@activetrail.com designates
91.199.29.18 as permitted sender) client-ip=91.199.29.18;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@activetrail.com;
       spf=pass  (google.com:  domain  of  reply@activetrail.com  designates
91.199.29.18 as permitted sender) smtp.mailfrom=reply@activetrail.com;
       dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=gingersoftware.com
X-IADB-IP: 91.199.29.18
X-IADB-IP-REVERSE: 18.29.199.91
DKIM-Signature:    v=1;    a=rsa-sha256;    c=relaxed/relaxed;    q=dns/txt;
d=activetrail.com;      s=at;      h=X-BBounce:X-IADB-URL:Sender:Submitter:X-
Feedback-ID:From:To:Date:Subject:MIME-Version:Content-type:Content-
Transfer-Encoding;          bh=GytDyTyaDleCfGk0d7bL4F2bXbTuWsb/xtpIVyVaCRw=;
b=sgh6nUFjt5FC7rBC2BwXFulNuG+k14R7bBsstb4erjtZfTn4z/NPHNhVb4Ax1yXoOgX+
Il6n5SCcXTCkwQdmaxpxt/BzPjWVziBdzU1WichHhPabVFeKctyp6pCjv4+d2FVIiEuxqi
v5dBTcJjXBVpOwU0mqgRceh3pqcvd5Rj4=
```

Figure 1: Sample Email Header

- The vital details in email headers help investigators and forensics experts in the email investigation. For instance, the **Delivered-To** field contains the recipient's email address, and the **Received-By** field contains:
- The last visited SMTP server's IP address.
- It's SMTP ID.
- The date and time at which the email is received

Email Server Investigation

- investigated to locate the source of an email.
- For example, if an email is deleted from a client application, sender's, or receiver's, then related ISP or Proxy servers are scanned as they usually save copies of emails after delivery. Servers also maintain logs that can be analyzed to identify the computer's address from which the email originated.
- It is worth noting that Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) logs are archived frequently by large Internet Service Providers (ISPs). If a log is archived, tracing relevant emails can take a lot of time and effort, requiring decompressing and extraction techniques. Therefore, it is best to examine the logs as soon as possible.

- https://www.stellarinfo.com/blog/email-forensics-investigation-guide-for-security-experts/
- https://www.tutorialspoint.com/python_digital_forensics/python_digital_forensics_investigation_using_emails.htm