

**UNIVERSITY OF PIRAEUS**



**DEPARTMENT OF DIGITAL SYSTEMS**

**Postgraduate Programme**

**in**

**SECURITY OF DIGITAL SYSTEMS**

**Registration, classification and presentation  
of digital forensics and incident response  
tools**

**Argyro Liakopoulou**

**Supervising Professor:**

**Konstantinos Lambrinoudakis**

**December 2015**



## Abstract

The objective of this thesis is to record, categorize and present the tools available, freely and commercially, for the needs of digital forensics and security incident response process.

Initially, this study presents the structure of the security incident response team and, then, the procedures and techniques applicable for a successful response to a security incident. The same procedure is followed for the digital forensics team.

Afterwards, the specific procedures, that should be followed for the collection and processing of electronic evidence in order to be valid for legal use, are analyzed.

Then, an overview of the legal framework within the EU, surrounding the security incident response and digital forensics procedures, is presented.

Next is presented the structure of the web page created containing the collection of forensics tools categorized according to their functionality.

Finally, some tools for digital forensics and security incident response are presented and categorized according to their functionality.



## Table of Contents

<b>ABSTRACT</b> .....	<b>3</b>
<b>TABLE OF CONTENTS</b> .....	<b>5</b>
<b>TABLE OF FIGURES</b> .....	<b>7</b>
<b>1. INTRODUCTION</b> .....	<b>9</b>
<b>2. SECURITY INCIDENT RESPONSE</b> .....	<b>11</b>
2.1. EVENTS AND INCIDENTS .....	11
2.2. THE NEED FOR SECURITY INCIDENT RESPONSE CAPABILITY.....	11
2.3. COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT).....	11
2.3.1. <i>Structure Types</i> .....	12
2.3.2. <i>Titles and Roles</i> .....	14
2.3.3. <i>Knowledge and Skill Set Requirements</i> .....	15
2.4. THE SECURITY INCIDENT RESPONSE PROCESS .....	16
2.4.1. <i>Preparation</i> .....	16
2.4.2. <i>Detection and Analysis</i> .....	17
2.4.3. <i>Containment, Eradication and Recovery</i> .....	19
2.4.4. <i>Post-Incident Activity</i> .....	20
<b>3. DIGITAL FORENSIC</b> .....	<b>23</b>
3.1. INTRODUCTION .....	23
3.2. THE DIGITAL FORENSICS TEAM .....	23
3.2.1. <i>Knowledge and Skill Set Requirements</i> .....	23
3.2.2. <i>Forensic Specialist</i> .....	23
3.2.3. <i>Forensics Investigator</i> .....	24
3.2.4. <i>Forensics Examiner</i> .....	24
3.3. THE DIGITAL FORENSIC PROCESS .....	24
3.3.1. <i>Data Collection</i> .....	25
3.3.2. <i>Examination</i> .....	28
3.3.3. <i>Analysis</i> .....	29
3.3.4. <i>Reporting</i> .....	29
<b>4. CRIME SCENES AND EVIDENCE COLLECTION</b> .....	<b>31</b>
4.1.1. <i>Identification</i> .....	31
4.1.2. <i>Order of Volatility</i> .....	32
4.1.3. <i>Documenting the Scene</i> .....	32
4.1.4. <i>Chain of Custody</i> .....	32
4.1.5. <i>Imaging and Hashing</i> .....	33
4.1.6. <i>Analysis</i> .....	33
4.1.7. <i>Repeatability</i> .....	34
<b>5. LEGAL FRAMEWORK WITHIN THE EU</b> .....	<b>35</b>
<b>6. DIGITAL FORENSICS TOLLS WEB PAGE</b> .....	<b>39</b>

6.1.	THE WEB PAGE .....	39
6.2.	THE FORUM .....	41
<b>7.</b>	<b>INCIDENT RESPONSE AND DIGITAL FORENSIC TOOLS .....</b>	<b>43</b>
7.1.	COMPUTER FORENSIC .....	43
7.1.1.	<i>Disk and data acquisition</i> .....	43
7.1.2.	<i>Filesystem and Data Analysis</i> .....	52
7.1.3.	<i>Memory Acquisition</i> .....	79
7.1.4.	<i>Memory Analysis</i> .....	81
7.1.5.	<i>Data Recovery</i> .....	85
7.1.6.	<i>Specific Tools</i> .....	87
7.2.	NETWORK FORENSICS .....	91
7.3.	MOBILE FORENSICS .....	112
7.3.1.	<i>Acquisition</i> .....	112
7.3.2.	<i>Analysis</i> .....	114
7.4.	MACINTOSH FORENSIC TOOLS .....	120
7.5.	FORENSIC DISTRIBUTIONS .....	126
<b>8.</b>	<b>CONCLUSION.....</b>	<b>129</b>
	<b>TOOL INDEX.....</b>	<b>130</b>
	<b>BIBLIOGRAPHICAL REFERENCES.....</b>	<b>132</b>

## Table of Figures

Figure 1 Central Incident Response Team model.....	12
Figure 2 Distributed Incident Response Team model.....	13
Figure 3 NIST Incident Response Process.....	16
Figure 4 NIST Incident Handling Checklist .....	22
Figure 5 Digital Forensic Process, NIST .....	25
Figure 6 Collecting digital evidence Flow Chart .....	28
Figure 7 Home Page.....	39
Figure 8 Computer Forensics Subcategories .....	40
Figure 9 Table Structure .....	40
Figure 10 Forum Home Page .....	41
Figure 11 Forum Login Section.....	42
Figure 12 EnCase Forensic Imager .....	44
Figure 13 FTK Imager .....	44
Figure 14 dc3dd .....	46
Figure 15 Bulk Extractor .....	47
Figure 16 Guymager.....	50
Figure 17 Autopsy, Windows version.....	53
Figure 18 Autopsy Linux version.....	54
Figure 19 EnCase .....	56
Figure 20 ILook .....	58
Figure 21 FRED .....	60
Figure 22 OSForensics Compare signature.....	60
Figure 23 Registry Browser .....	62
Figure 24 Hex Editor Neo.....	65
Figure 25 Log Parser .....	66
Figure 26 Nagios Log Server.....	71
Figure 27 Nagios Incident Manager.....	75
Figure 28 GRR Rapid Response.....	76
Figure 29 Goldfish .....	80
Figure 30 Belkasoft Live RAM.....	80
Figure 31 RAMMap.....	83
Figure 32 WindowsSCOPE .....	85
Figure 33 Catfish.....	88
Figure 34 MacForensicsLab.....	89
Figure 35 Wireshark.....	91
Figure 36 Wireshark captured packets.....	92
Figure 37 Nmap .....	93
Figure 38 Xplico System Architecture .....	95

Figure 39 Interface .....	96
Figure 40 TCPView.....	98
Figure 41 Xprobe2.....	99
Figure 42 Web Debugger.....	100
Figure 43 Web Session Manipulation .....	100
Figure 44 Microsoft Message Analyzer .....	104
Figure 45 Nagios XI Interface .....	105
Figure 46 Network Analyzer Custom reports.....	106
Figure 47 NetworkMiner Free Edition .....	107
Figure 48 NetworkMiner Professional Edition .....	108
Figure 49 CapAnalysis.....	109
Figure 50 Maltego.....	110
Figure 51 Maltego CaseFile .....	111
Figure 52 Oxygen Forensic Suite .....	114
Figure 53 Mobilyze details view.....	117
Figure 54 MacQuisition .....	121
Figure 55 SoftBlock.....	124



## 1. Introduction

The global technological, economic and political developments have led to a society without borders where the volume and the value of electronic information handled are constantly increasing. The rise of new technologies, the new digital services and the continuously increasing computing power of information systems, combined with the advances in communications technologies, have led to a global distributed computing environment, where personal and financial data are processed on computers located anywhere in the world or transmitted over a network. Global economy has increased the need for handling personal and financial data between company groups or between cooperating companies, while the advances in communication technologies facilitate a multi-level delegation of the company's information systems management to third parties. All of the above have inevitably led to the incensement of crimes carried out through digital systems.

The term cybercrime is a broad concept which is typically used to cover all offenses committed using an electronic device or over the internet. Cybercrime falls into two categories. The first category is when the target of the offence is a computer connected to a network; this is a case of attacking the network's confidentiality, integrity and availability. The second category is when a digital device assists the offender in committing a "traditional" offence; this is the case of fraud, organized crime, theft and so on. Therefore, in 2012, SA law for "Electronic Communications and Transactions Amendment Bill" proposed the definition of cybercrime as *"any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them"*. Cybercrime encompasses a broad range of activities such as fraud and financial crimes, cyber-terrorism, computer viruses, denial-of-service attacks, unauthorized access to computer or systems, information warfare, phishing scams, spams, and much more.

Nowadays, with the dominant role of technology in our daily lives and this new form of crime, a new branch of forensics emerged; it's called digital forensics. According to NIST, digital forensics is considered as *"the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data"*. The field of digital includes investigations in all digital devices, mobile devices, networks and cloud systems. It is not only used in criminal investigations, but also in civil litigations, information gathering, surveillance and administrative matters.

The incidences of cybercrime and their complexity are constantly increasing and, alongside, the need for computer and network security grows. Corporations must evolve and fortify their computer systems in order to protect their assets.

Furthermore, when security breaches do occur, the most important is to immediately respond effectively by taking all the appropriate actions. Out of this necessity, it was born the need to create the security incident response team (CSIRT) which will handle every security breach. Thus, CSIRT's main goal is to investigate every suspicious event and to determine if an incident is occurring or if it is about to occur. When an incident do occurs, CSIRT must take all the possible actions to minimize information loss and functionality impact, to restore functionality, and to use the information gathered, during each incident handling, for improving current security, handling protocols and procedures.

## 2. Security Incident Response

### 2.1. Events and Incidents

NIST defines *events* as “any observable occurrence in a system or network”. These include a server receiving a request, receiving an email, a connection attempt blocked by a firewall and so on. An *adverse event* is any event that has a negative impact on a system or network such as system crashes, unauthorized access to a system, packet floods and so on.

There is no single accepted definition of what an incident is. According to NIST, a computer *security incident* is “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices”. Therefore, it is clear that all incidents are also events but events are not always incidents.

### 2.2. The Need for Security Incident Response Capability

As mentioned above, along with the growth of new technologies, combined with the advances in communications technologies, a similar growth was inevitable in the ways in which it could be exploited. Companies and agencies rely heavily on computer systems; therefore, when a security breach occur, it is crucial to respond to it rapidly and effectively in order to protect its assets. For an organization to be able to quickly respond to a security breach, it must first establish who will coordinate the team and make the decisions on how to respond. Moreover, standard procedures must be developed step-by-step instructions to efficiently contain and recover from the incident.

So, the organization, according to its needs, should determine what services should the incident response team provide and select the appropriate team structure. Next, it should create the strategies and procedures which should be followed when an incident occurs.

Having a security incident response capability ensures that the company will be able to respond to incidents systematically so take all the proper actions, and consequently minimize information loss and disruption of services. Furthermore, the knowledge gained during incident handling can be used to improve policies and strategies for more effective handling of future incidents.

### 2.3. Computer Security Incident Response Team (CSIRT)

A Computer Security Incident Response Team the part of the organization that receives reports of potential security breaches and analyzes them, and if valid, responds with the appropriate measures. Once there is a suspicion of a security

incident, an incident response team should be available to investigate and, depending on its severity, the appropriate amount of team members will handle the incident. The awareness and the skill of the incident responders are vital to the successful handling of any incident as they will have to analyze the incident, to determine the impact on the organization, and to take the appropriate countermeasures for reducing the damage and restoring normal operations. Response time is essential in assembling, organizing and maintaining an effective CSIRT.

### 2.3.1. Structure Types

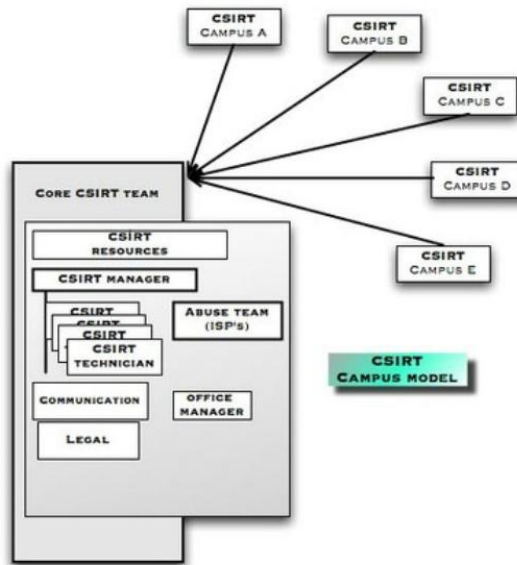
Depending on the distribution of the responsibilities among various centers, there are three types of CSIRT structures.

The *Central Incident Response Team* model is centrally located and has full responsibility for all incident's reporting, analysis, and response. It has a single incident response team for handling incidents within an organization and should be selected for organizations with small geographical distribution in terms of computational resources.



Figure 1 Central Incident Response Team model

The *Distributed Incident Response Team* is a model in which teams will be distributed within an organization according to business sectors or to geographic location. Nonetheless, the team must communicate as single unit so that incidents can be handled in the same manner. This model should be selected for organizations with their major computing resources distributed in various locations.



**Figure 2 Distributed Incident Response Team model**

The *Coordinating Team model* focuses on coordinating and facilitating incident handling across a broad, diverse, and usually external area. This may include sharing information, providing mitigation strategies and recommendations for incident response and recovery, researching and analyzing trends and patterns of incident activity as well as providing resources and references for incident management such as vulnerability databases, clearinghouses for security tools, or advisory and alert services. The coordinating CSIRT can provide high-level analysis and suggest recovery and mitigation strategies, but it can only act as an advisor, it has no authority and takes no actions, while it is up to the organization to decide to follow the recommendations.

The CSIRT should be composed with suitable skilled resources otherwise incident response may be delayed or ineffective. Organizations may not have internal capability to create an effective incident response team. They may need to combine their internal recourses with external expertise to effectively handle an incident. Depending upon the IT's infrastructure robustness, the company's critical assets and the probability of incidents, a Response Team can be formed with full time members or/and part time members that will be available if needed. If the organization has sufficient internal capability, then the Incident Response Team can be formed by full time employees with the internal expertise already available. Otherwise, the organization may completely outsource its incident response tasks, usually to an onsite contractor. This type of team is usually found in smaller organizations which must have a 24/7 incident response capability but they don't have skilled personnel. Another way to structure an Incident Response Team is using partially employees and outsourced contractors. There are two common ways by which this structure may be implemented. The first and most common is that the organization outsources

the monitoring of its systems. The offsite managed security services provider identifies and analyzes suspicious activity and reports each detected incident to the organization's incident response team. The second is that the organization monitors its systems and handles incidents when they occur and it requests assistance only with handling incidents that are more serious or widespread. There are many factors to consider in the selection of a team's model structure and staff such as: if the incident response team needs to be available 24/7, the cost, the geographical distribution of its computational resources and the necessity for experienced and adequate skilled personnel that can handle responsibilities and work under pressure. All the above must be carefully considered when constructing CSIRT.

### 2.3.2. Titles and Roles

There may be many different titles and roles for Incident Response Team members. Each organization's environment is unique, therefore a careful research must be conducted to specify the organization's requirements and then a plan must be build that will satisfy those needs. Generally, CSIRT staff roles could be:

- ✓ *General Manager*. In case of a fully outsourced model, a single employee, with one or more chosen replacer, should usually be in charge of incident response.
- ✓ *Incident response Team manager*. The managers usually perform diverse tasks such as: coordinating activities between all of its respective groups and organizations, resolving emergency situations, and verifying the team's adequacy in skilled personnel and resources. They should be experienced, with high technical knowledge and exceptional communication skills as they are utterly responsible for the proper performing of all incident response activities.
- ✓ *Incident Response Assessment Team*. This is a group which is consisted of the various areas serviced by the Incident Response team. In case of an incident, the Incident Response Manager would collect details on the incident and then he would activate the Assessment Team which would discuss the details of the incident and, based on their experience and knowledge of the business, they could then initially assign a degree of severity and report back to Incident Response Manager.
- ✓ *Remote Incident Response Coordinator*. These individuals report to the Incident Response Manager but in their geographic region they are recognized as Incident Response leaders.
- ✓ *Technical Leader*. The technical leader is the person who should have exceptional technical skills as well as incident response experience, who

assumes oversight of the team's technical work and takes responsibility for its quality.

- ✓ *Incident leader.* The incident leader is responsible for the incident's handling. Depending upon the extent of the incident and the composition of the incident response team, he may not actually perform incident response actions, but rather coordinate the handlers' actions, gather information from the handlers, provide incident updates to other groups, and ensure that the team's needs are met.

Additionally other roles could be:

- ✓ Legal consultant, hotline, help desk, incident handlers, vulnerability handlers, artifact analysis staff, support staff, technical writers, network or system administrators, auditors or quality assurance staff, etc.

### 2.3.3. Knowledge and Skill Set Requirements

The success of the Incident Respond Team in handling any incident lies essentially in the knowledge and the skill set of its members. The set of basic skills, that CSIRT staff members should have, are both *personal* and *technical*.

The members should be *thorough* in every action they take, approach every situation in a *logical* manner and be *observant* of all activities and *objective* and, above all, they must be *accurate* in their findings, results, and reports. It is significant for CSIRT staff to have a wide range of personal skills, since a main part of the daily tasks of an incident handler's will involve communicating with their own team members, other response teams, and other persons who may have different levels of technical understanding. Consequently, they should have high oral and written communication skills, strong presentation skills, the ability to follow policies and procedures and be able to work in a team environment. The CSIRT may often handle sensitive information and, sometimes, some of high value. Therefore, CSIRT staff must be honest and discrete. It is also important for them to be able to realise and to admit it, when the limit of their knowledge and expertise is reached, in order to seek help from other experts. Finally, within their range of personal skills, there are the ability to solve problems and the ability to manage their time effectively. That is mostly due to the fact that they will usually have to determine the relevance of the data collected and identify its importance, and to discover missing, or misleading information, all in the best possible timing.

The CSIRT staff should have excellent technical skills. They should understand how systems and software are configured and the risks they may include, as well as the strategies for protecting and securing the systems. They should have knowledge about basic security principles which are confidentiality, availability, authentication,

integrity, access control, privacy and non-repudiation, so they will be able to acknowledge possible problems that can emerge from insufficient security. They should have a detailed knowledge of network protocols, applications and services as well as how these interact with each other, the ability to identify risks and threats to the system, a profound knowledge of network infrastructure components and knowledge of current security vulnerabilities along with the corresponding attack methodologies. Finally, skills such as system and network administration, programming, technical support, or intrusion detection and individuals specialized in particular techniques will be needed.

## 2.4. The Security Incident Response Process

NIST organization has developed an Incident Response Methodology that consists of four phases: preparation; detection and analysis; containment, eradication and recovery; and post-incident activity. Each of these phases are simple in their design, but detailed in implementation and they have an iterative nature.

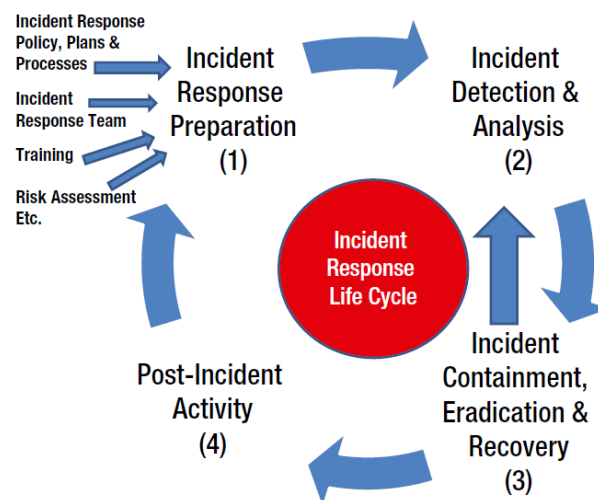


Figure 3 NIST Incident Response Process

### 2.4.1. Preparation

The first stage of NIST’s methodology is the *Preparation* and it has two objectives; the creation of Incident Response mechanisms to handle incidents when they occur and the prevention of incidents by setting a security baseline in the organization’s IT and network infrastructure. While the incident response team may not be responsible for incident prevention, the NIST incident response guide suggests that being prepared is the best defence, rather than responding by jumping into the remediation and consuming a considerable amount of time and resources to identify, contain and recover from an incident when it occurs.



Naturally, all security incidents are not equal, therefore the defences against potential incidents should be planned depending on the impact they could have on an organization, the criticality of the assets affected and the likelihood of them to occur. Those are usually determined using formal risk assessment, that identifies potential IT vulnerabilities, so to enable an organization to implement the proper protection and prevention countermeasures. Once this has been accomplished, the organization must then develop an incident response plan IRP and a Computer Security Incident Response Team CSIRT to manage each of the NIST phases.

The Incident Response handling procedure describes the communications methods and facilities available to the team, as well as the existing tools and resources and, also, it provides examples of all that should be available during incident handling. Those are divided into four categories.

*Incident Handler Communications and Facilities*, focuses on how the team members and others should communicate inside and outside the organization, on the reporting mechanisms, the tracking system needed for tracking incident information and status, and the devices that should be at their disposal.

*Incident Analysis Hardware and Software*, describes all the Digital forensic tools, devices and resources required.

*Incident Analysis Resources*, is the collection of documentation for OSs, applications and protocols, port lists, network diagrams and lists of critical assets, baselines of expected network, system, and application activity as well as cryptographic hashes.

*Incident Mitigation Software*, are images of clean OS and application installations in order to restore and recover.

## 2.4.2. Detection and Analysis

The second stage is the *Detection and Analysis* and it happens when the actual incident has been detected. Since there is a wide variety of ways in which incidents could occur, NIST puts in groups incidents according to their common attack vectors.

The revised NIST incident response guide no longer assigns security incidents to specific categories and introduces the concept of attack vectors which is a list of methods an attacker might use. All attack vectors should have the according response strategies, so NIST provides a list of common methods of attack, to be used as a starting point for defining more specific handling procedures.

Nowadays, there are many methods available to help automated detection of possible incidents both software and hardware. Those include alerts and notifications to detect changes in network, in sizes of the files and in file directory

structures, or even the behaviour of files on the servers or network, but they also include periodic or continuous monitoring and follow-up, and any notifications from users for any uncommon behaviour. All those potential incidents should be reviewed, prioritized, and evaluated.

The prioritization and evaluation of those incidents is the most exigent task, given that the daily amount of potential incidents may be extremely high. NIST sets two categories of signs of an incident relatively to the time they occur. A precursor is a sign according to which an incident may occur in the future and an indicator is a sign according to which an incident may already have happened or may be happening now. When there is a sign of an incident, this doesn't necessarily indicate that an incident has happened. In order to define whether a specific event is a security incident, it may be necessary to collaborate with other technical and information security personnel and to correlate events. Prior to incident analysis, the team should have profiled the networks and systems and should have knowledge of the normal behavior of networks, systems, and applications and also built a log retention policy to define how long log data should be maintained. In addition, an information knowledge base should be maintained, so that handlers could refer to during an incident analysis. So, it does become obvious how important is to have people with the required skills, who can identify which of those signs are real security incidents, for proper and efficient analysis, and who are able to provide the needed actions in response to each incident. Without proper analysis, it will be difficult to continue to the next phase.

Moreover, as soon as an incident occurs, the team should document everything related to that incident, all communications, system events, observations on networks, systems, applications and files, and every action taken, must be documented and timestamped. Therefore an application or a database must be used so that it will contain the current status of the incident, as well as a summary of the incident, all the indicators related to it, any other incidents if related, all the actions taken, a chain of custody, an assessment of its impact, the contact information for every people who got involved, the list of all evidence collected during the incident investigation, comments from incident handlers and the next steps to be taken.

As mentioned above, NIST defines that once an incident is detected, an organization should conduct an analysis of the impact of the incident. So there is a need to prioritize analysis of what other systems could be affected by, in order to prevent deeper penetrations into the networks. To prioritize analysis, NIST introduces three impact-based criteria. The first is the functional impact that describes how the business functions are affected by the system incidents with a high functional impact result in a situation where the organization is unable to provide one or more critical services to all users. The second is the information impact that describes the

sensitivity of the data breached. The third is the recoverability impact that describes the resources required for recovery from the incident. Thus, incident analysis will help identify the source of an incident, the extent, the impact on the functionality of the affected systems, the impact on the confidentiality, integrity, and availability of information, the amount of time and resources needed for recovery and the details of the breach.

### **2.4.3. Containment, Eradication and Recovery**

Once identified, the incident needs to be contained and eradicated. After remediation, all affected systems and applications need to be restored to the state they were in before the incident. However, if there was no analysis conducted upon initial detection, remediation failed to contain or to limit damage in 25% of the incidents.

After identifying the incident, the containment of the incident is usually the next step taken in order to provide time for the developing of the proper remediation strategy and it is mostly a decision-making step where it becomes essential to take the proper actions and to allow the right resources to be applied during the response. In order to choose the appropriate containment strategy, various questions need to be answered, such as whether shutting off the system or disconnecting it from the network or not, or if certain ports, protocols, or services should be disabled. Such decisions could be facilitated by predetermined strategies and procedures.

The containment strategy must not only be depending upon the type of incident, while other facts must also be considered such as the potential damage or theft of resources, the need for evidence preservation, the service availability, the time and resources needed to implement the strategy, the effectiveness of the strategy and the duration of the solution, but also it will facilitate the decision-making step. In some cases, even the containment itself may trigger additional damage such as encryption or deletion of data.

The eradication of the cause of the incident is the next step within this framework of response. Eradication actions could include deletion of the malicious software or code snippet, disabling compromised accounts on the system, closing certain ports, as well as identifying and diminishing all vulnerabilities that were exploited. In some cases, depending on the type of incident, full eradication may not be needed and could actually cause further damage or may be achieved during recovery.

The recovery of operations is the end objective of this stage and includes restoring of systems to their normal operation and verifying that they are functioning normally, and the remediation of vulnerabilities so that similar incidents could be prevented in the future.

Recovery actions may include restoring the system affected from backups, installing patches, changing passwords, replacing compromised files and applications with clean versions, hardening security to prevent other occurrences in the future, adding new or expanded security parameters on boundary devices. The appropriate planning for breaches and uncontrollable security breaches will greatly reduce the cost, time and effort required for this phase.

#### 2.4.4. Post-Incident Activity

Post-incident analysis is an essential step to an effective incident response management where procedures will be reviewed for effectiveness and, if needed, changed accordingly.

Once the incident has been contained and remediated and operations have been normalized, each incident response team should conduct post-incident meetings to focus on lessons learned by reviewing the effort and the techniques used to handle the incident, the timing of the response and the actions taken. These lessons learned meetings could improve the security of the organization, as well as the incident handling and response mechanisms for each incident. Furthermore, the team could estimate whether there is a need for updating incident response policies and procedures, create a follow-up report as a reference that it can be used to support in handling similar incidents, or even be used for training new team members by showing them how experienced team members respond to incidents.

Questions that should be answered in those meetings include:

- ✓ Exactly what happened, and at what time.
- ✓ How well did staff and management perform in dealing with the incident, if the documented procedures followed and if they were adequate.
- ✓ If there was a need for certain information sooner.
- ✓ If there were any steps or actions taken that might have inhibited the recovery.
- ✓ If there is something that the staff and management should do differently the next time that a similar incident occurs.
- ✓ If the information sharing with other organizations could be improved.
- ✓ If there is a way to prevent similar incidents in the future and what precursors or indicators should be watched for in the future to detect similar incidents.
- ✓ If there is a need for additional tools or resources to detect, analyze, and mitigate future incidents.

The lessons learned meetings will produce a set of objective and subjective data, regarding each incident, measuring the success of the incident response team. These

data could also help to define whether additional funding of the incident response team is needed to indicate systemic security weaknesses and threats, as well as changes in incident trends which could lead to the selection and implementation of additional.

The decision of which data should be collected must be based on the reporting requirements and on the expected profit.

An example of such data could be:

- ✓ The *number of incidents handled* for each incident type that could measure the relative amount of work of the incident response team and if improved security measures could reduce them.
- ✓ The *time per incident* totally or for each stage of the incident handling process.
- ✓ The *objective assessment of each incident* to define how effective was the response by reviewing logs, forms, reports, and other incident documentation, by pinpointing which precursors and indicators were those to effectively log and identify the incident, by examining if there was further damage, if the real cause of the incident was determined and if they were any measures that would have helped to prevent the incident.
- ✓ The *subjective assessment of each incident* where the incident response team members assess their own performance, as well as the performance of other team members.

For all those data, policies must be created to define how long evidence from an incident should be retained. Things that must be considered are whether there will be a prosecution, thus the need to retain them until all legal actions have been completed, whether there is a data retention state which defines how long certain types of data will be retained and the cost of the hardware where the evidence is stored.

Finally, NIST provides a checklist with guidelines on the main steps that should be executed.

	<b>Action</b>	<b>Completed</b>
<b>Detection and Analysis</b>		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
<b>Containment, Eradication, and Recovery</b>		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
<b>Post-Incident Activity</b>		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

**Figure 4 NIST Incident Handling Checklist**

## 3. Digital Forensic

### 3.1. Introduction

As mentioned above, digital forensics is essentially the collection and analysis of digital data, using scientific methods. Digital forensics encompasses not only laptops or desktop computers but any mobile devices, network, and cloud systems. It also includes the analysis of images, videos, and audio. In order to be admissible to court, digital evidences must be *relevant*, *obtained using scientific methods*, and *supported by appropriate validation*. Digital forensics is highly technical and therefore relies in computer science and mathematics.

### 3.2. The Digital Forensics Team

Digital Forensics is a highly technical field that requires a combination of skills in computer software and technology, good investigative and evidence handling methods and judgment.

#### 3.2.1. Knowledge and Skill Set Requirements

The criteria for the forensics team members are various and each team member should be trained and certified in his areas of expertise accordingly. The members should be *thorough* in every action they take, approach every situation in a *logical* manner and be *observant* of all activities and, also, objective and, above all, they must be *accurate* in their findings, results, and reports. After all, performing a forensic analysis on great amount of information can be a daunting and time-consuming task. The team manager should define the needs of his forensics team, the skills and expertise required, and whether each team member can perform forensic activities under pressure circumstance. Generally, the members of forensics team fall into three groups.

#### 3.2.2. Forensic Specialist

The *forensic specialist* is the one who initially performs all the data capture actions to gather the evidence at the beginning of the forensics process. Thus, he must apply image capture techniques to collect the data from storage devices from any place data stored and apply proper chain of custody for the forensic evidence acquired. That process includes using of clean media that have been formatted and examined for computer viruses, recording all the hardware and noting the condition of the device when obtained, checking the date and time values in the system's CMOS after removing the drive from the computer and performing a cryptological "hash" of the data.

### 3.2.3. Forensics Investigator

The *forensics investigator* is responsible for the examination of the evidence collected by the forensic specialist. He documents the different types of data sized, selects the parameters of the search and researches technical specifications of the storage devices, as well as, describes the location and the nature of the data. Among the skills required of a forensics investigator is the deep knowledge of the operating system under examination, the application and its data structures, hardware, databases and network devices and their data. The process includes processing the data methodically and logically, accurate documenting of how the data was obtained from the device, recording all folders and files on the device, inspecting the contents of all data files in all folders, attempting to recover the contents of all password-protected files, identifying the function of every executable file with a suspicious hash value and documenting every action taken during the examination along with the reason he took it.

### 3.2.4. Forensics Examiner

The *forensics examiner* is responsible for analyzing evidence, presenting the nature and purpose of the evidence, as well as the logical conclusions and what was revealed by the examination of the evidence. In other words, he provides professional evaluation of what the data is about and its use. This evaluation is later documented into the forensics report which is forwarded to the law enforcement officers who handle the case.

The forensics examiner must have exceptional knowledge of and should be certified with “court accepted” tools since his findings will probably serve as evidence in a court of law, while he typically becomes the expert witness based on his expertise, conclusions, and background. Hence, he presents the sequence of cause and effect based on the evidence he examined, the correlations he made of the activities and artefacts found, thus he presents without doubt what happened, when and where and who was the perpetrator. The forensics examiner will need to clarify the forensic report, so that the average person can understand the evidence that has been found, where the evidence came from and how it was obtained.

## 3.3. The digital forensic Process

The main purpose of a forensic investigation is to find and to analyze facts related to an event, in order to gain a better understanding of it. So the forensic process transforms media into evidence. The first step of this transformation happens during the examination of the collected data, where the data is extracted from media and converted into a format that can be processed by forensic tools. Afterwards, during



analysis, it is transformed into information and finally, during the reporting phase, it is transformed into evidence.

According to NIST, the process for performing a digital forensics investigation consists of four phases. The first one is the collection of the evidence, where the team must identify, obtain, label, and record data from all the possible sources, while following procedures that preserve their integrity. Next is the examination of the data, where the forensic process of the collected data starts, using a combination of manual and automated methods, and assess as well as extracts data of particular interest, while preserving their integrity. The third phase is the analysis of the results of the examination with legally justified methods and techniques, in order to obtain information regarding the investigation. Finally, the last phase is the reporting of the results of the analysis which may include the methods used, the tools and the procedures selected, determining whether other actions need to be performed and if the needed make proposals for improvements in every aspects of the forensic process. Some details of these steps may differ, depending on the specific needs for forensics. The four main sources of data, within any network or computer where the forensics process is conducted, are files, operating systems, network traffic and applications.

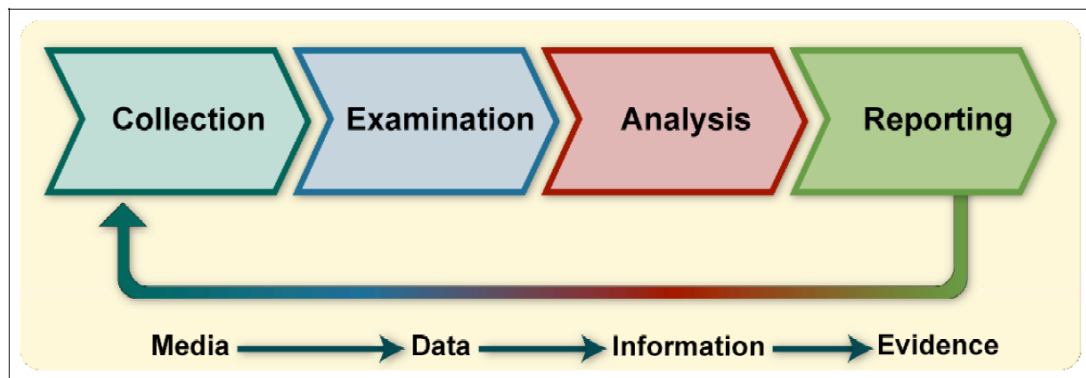


Figure 5 Digital Forensic Process, NIST

### 3.3.1. Data Collection

The first step of the forensic process is the identification of the possible sources which may contain data. Apart from desktop computers, laptops, servers and network storage devices, data can also be extracted from other types of portable digital devices like cell phones, digital cameras, digital recorders and audio players. Furthermore, within an organization, there are usually many sources of information about network activity and application usage such as logs, so the first responder should be able to immediately identify all possible data sources within a physical area. The analysts should also have knowledge of the owner of each data as it may have consequences on the collecting data procedure and they may have to follow

precise organization policies or have legal considerations especially if a data source is located outside the organization's control. In some cases, when it is not possible to obtain the data from the original sources, there may be other data sources that might contain some or all of the same data.

The analysts should also be aware of any measures that an organisation may have taken to facilitate the collecting useful data for forensic purposes as such as configurations to audit and record specific events and, in some cases, forwarding copies of their logs to secure central log servers as an anti-forensic technique countermeasure. In addition, there other security monitoring controls, such as intrusion detection systems, antivirus and spyware detection systems and removal utilities, can create logs which indicate when and how an attack or intrusion took place.

The neat step, after the identification of all possible data sources, is to obtain the data. NIST defines a three step process which is developing a plan to acquire the data, acquiring the data, and verifying the integrity of the acquired data.

Developing a plan to acquire the data is needed only when there are multiple potential data sources and there is a need for prioritization to define the order in which the data must be acquired according to the relative likely value of each potential data source, the type of data (volatile or not) and the amount of effort required to extract the data regarding the time needed for extraction and the cost of equipment and services. So, there are many things to consider when prioritizing the collection of data and there may be cases where the amount of data sources is such that it is not practical to acquire them all. Therefore, depending on the complexity, there must be written plans, guidelines, and procedures to guide the analysts.

Next is the acquiring of the data where, when it has not already been acquired by security and analysis tools or other means, forensic tools must be used to collect volatile or non-volatile data, while securing the original non-volatile data sources. This may happen locally and it is usually preferred, but it can also happen over a network if needed and, in that case, an assessment must be made regarding the type of data to be collected and the amount of effort to use.

After acquisition follows the verification of the integrity of the data acquired, where the analysts should be able to verify and, if needed, to prove that the data has not been tampered. Additionally, prior to the collection of any data, the analysts must be aware of whether there is a need to collect and to preserve evidence in a way that it may be used in the future for legal or internal disciplinary purposes since, in such circumstances, a well defined chain of custody must be followed as it is necessary to prove the absence of alteration, substitution, or change of condition. Proof of a chain of custody is required when the relevance of the evidence depends on its analysis

after seizure. A proper chain of custody requires three types of testimony; testimony in which a piece of evidence is what it purports to be, testimony of continuous possession by each individual who has had possession of the evidence from the time it is seized until the time it is presented in court, and testimony by each person who has had possession that the particular piece of evidence remained in the same condition from the moment one person took possession until the moment that person released the evidence into the custody of another. Therefore, a log must be kept where every person who had possession of the evidence and all the actions, that they are performed on the evidence, are recorded and timestamped, as well as every step taken to collect the data and information about every tool used. Also, the storage location must be secure and the analysis must be conducted on copied evidence. Moreover, the first responder should follow departmental policy for securing scenes. He should remove anyone from the scene or the surrounding area where evidence is to be collected, secure all electronic devices and ensure that their condition is not altered, and that only authorized personnel can access the electronic devices at the scene. And if a computer or electronic device is found turned off, he should leave it off. When documenting a scene, it is essential to precisely record the entire location of the scene, including the type, location, and position of computers, the location of their components and peripheral equipment, the state and condition of all network devices, as well as all electronic and data storage devices and any internet and network access. He should also include a detailed record using photography or video and notes to help convey the details of the scene later, and all activities and processes on display screens should be fully documented. The first responders should also have in mind that not all digital evidence may be found close to the computer or other devices and that the scene may expand to multiple locations. The existence of network and wireless access points may indicate that additional evidence exists beyond the initial scene.

In cases where forensics is conducted during incident response, the analysts may have to collaborate with the incident response team for making decision concerning the containment of the incident based on the existing policies and procedures and, also, based on the team's assessment risk. Thus, it may be essential to define how and when the incident should be contained, so that evidence would be protected and no further damage occurs to the system and its data. For this reason, it is often required to limit access to the device for unauthorized personnel, while the data is collected, and all users who had access to the device should be documented, as they may provide important information about the location of data and passwords on their devices. The ultimate goal is to select the containment strategy that minimizes the impact on the organization's capacity to operate effectively with minimum risk, while preserving the reliability of potential evidence.

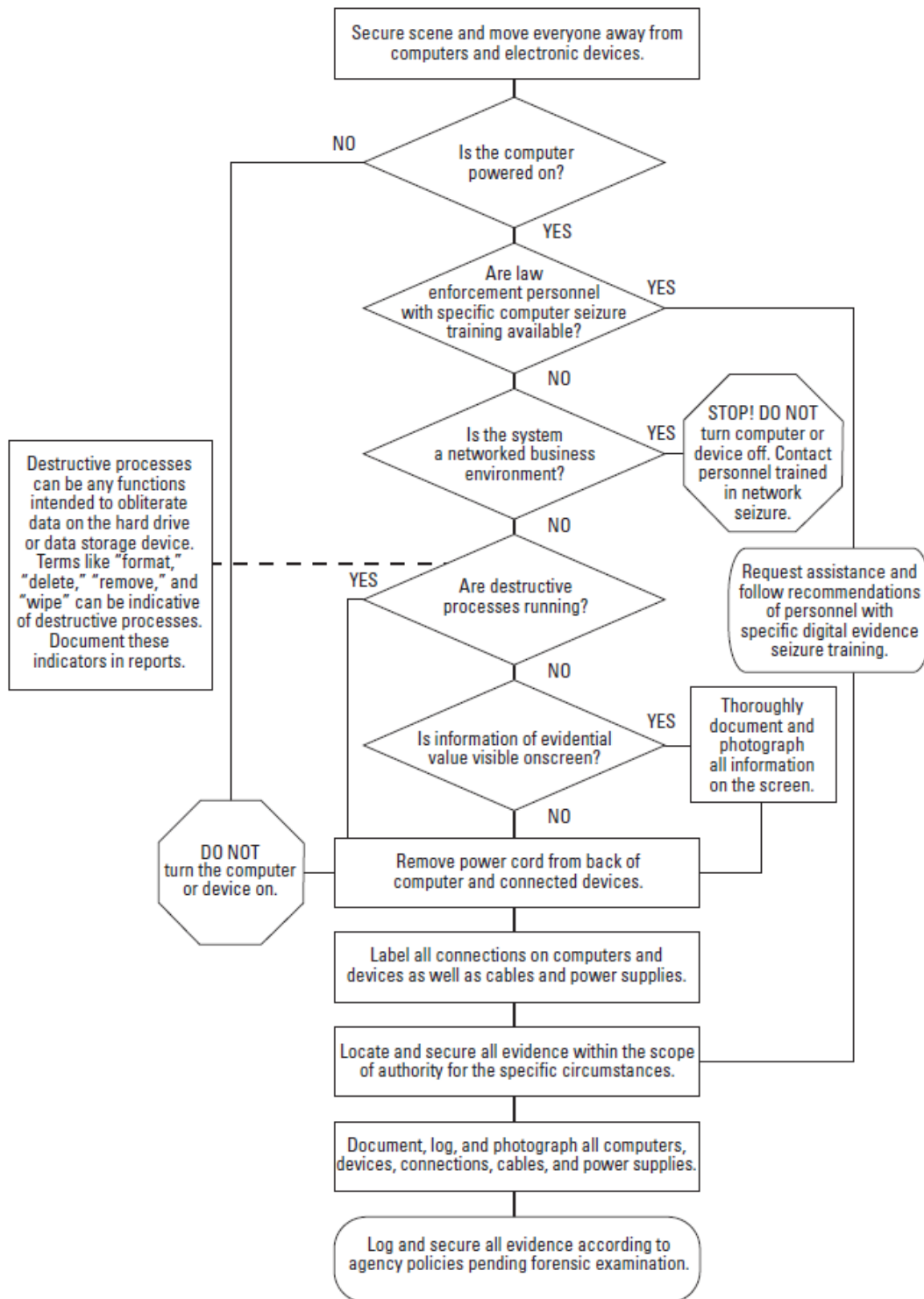


Figure 6 Collecting digital evidence Flow Chart

### 3.3.2. Examination

Once the collection of data has been completed, the next step is their examination, where the most challenging part is to assess and to extract only the information relevant to the incident. That task is not only limited to the distinguishing of which

files contain information about the incident, but also filtering may be required, since each file may contain an enormous amount of information unrelated to the incident. But, there are diverse tools and techniques that can be used to diminish the amount of data that has to be filtered such as text and pattern searches or tools to verify the type of contents of a data file, as well as databases that include information about known files that will help the analyst to determine whether a file should be excluded or not.

Nowadays, the technology allows the storage of data in multiple areas commonly unavailable to ordinary processing software, therefore data can be stored anywhere there is a storage activity with memory, real or virtual. So, the analyst must search for hidden storage locations such as unallocated space, slack space, and in front of FAT space on hard drives, and must use the according tools and mechanisms for the retrieval of those data. There are also many techniques, used to hide or disguise files or to impede access, such as password protection, encryption and compression, saved in places that usually contain only innocent system files, in the effort to avoid detection. So, it is imperative to examine registry entries and root directories for potential indicators of data storage activity for external storage devices and smartphones, as well as for any internet-based program which also retains some or all of the action related data.

### **3.3.3. Analysis**

The examination of the data is followed by the analysis, which will lead to conclusions regarding the incident. The analyst will re-examine the data to ensure that data is comprehensible and relevant to investigation and, then, he will evaluate it to define its type and whether it is direct evidence or it is evidence related to the issue. In legal cases they are two types of incidents, the circumstantial evidence which require making assumptions to reach a desired conclusion and the direct evidence which lead to certain conclusion. So, the analyst must apply a methodical approach to either of them for reaching definitive conclusions or to decide that no conclusion can yet be drawn. Usually, this will require correlating data between several sources, therefore security tools centralized logging and security event management may assist this task by automatically assembling and correlating the data.

### **3.3.4. Reporting**

The last step of the forensic process is reporting, which include the preparation and presentation of the outcome of the analysis of the data. During the forensics process, it is essential to the outcome of the investigation that every event and every action taken is documented, especially if legal actions are to be taken. Therefore, the

documentation and reports should conceal the objective of the investigation, the framework, the interpretation of the evidence and the results. The investigation must be proven valid and objective in every step, so all the technical and operational procedures have to be well defined so that every step can be repeated, all the items related to the case should be documented as to their importance and kept together, and all the documents and reports should be verified for completeness of the process. The reports must not include assumptions or interpretations and they should only contain facts, and when an event has more than one probable explanation, each must be presented and analyzed. It may also contain information that could lead to the examination of new sources, that could prevent future breaches or possible improvements to guidelines and procedures. Usually, the details of the report also depend on how this is intended to be used, for example in a court of law or for corporation's internal purposes.

## **4. Crime Scenes and Evidence Collection**

The Forensics Team Manager have the responsibility of how, when, and where evidence is collected, stored, analyzed and evaluated during any investigation, and determine the assignments, roles, and responsibilities of human resources. Therefore, strict policies and controls must be implemented about the collection, the storage and maintaining of the chain of custody during the entire cycle of the forensic process. In digital investigations, digital evidence is considered as any information or data, that is stored, transmitted or received by an electronic device that could potentially be of value to the investigation.

In contradiction of the traditional crime scene, a scene with digital evidence presents some particularities in the issue of access. Most computers and digital devices are usually connected in some kind of network allowing the remote access which may put the evidence at risk. Therefore, the access to computers and wireless devices must be interrupt once the safety of volatile data is ensured. For computers, this can be done by unplugging a wireless router or by removing the Ethernet cable. For cell phones and other wireless devices, they must be isolated from network signals

When managing digital evidence, forensic and procedural principles should be implemented to ensure that the collection and the transportation of evidence should not in any way affect the evidence. Only trained specialists should have access to it and everything done while collecting, transporting and storing digital evidence should be fully documented, preserved, and available at any time for review. First responders should also be careful and aware of the Federal laws when collecting digital evidence and they may need to obtain additional legal authority before proceeding with the evidence collection.

### **4.1.1. Identification**

Once the first responder or the investigator access a scene, he must initially determine the location of all possible digital scenes, gather the evidence and assess what primary preservation procedures must be followed. So, the primary step is to secure, recognize and identify all the potential evidence. Those could include the desktop computers and laptops, hard drives, external storage devices, cell phones, printers, copiers, PDAs, digital cameras, and any other device that could contain digital data.

### 4.1.2. Order of Volatility

In order to prioritize the evidences to be collected, the first step is to consider which of them are the most volatile. This is known as the *order of volatility*. This descending list shows from the most volatile to the least volatile, that is:

1. CPU, cache, and register content
2. Routing table, ARP cache, process table, kernel statistics
3. Memory
4. Temporary file system/swap space
5. Data on hard disk
6. Remotely logged data
7. Data contained on archival media

### 4.1.3. Documenting the Scene

There are many different types of documentation. The most common way in terms of digital forensics is using notes, photos or videos depending on what is most appropriate, including the screens of systems and devices that may be running at the time. The documentation process begins as soon as investigators arrive at the scene and includes the date and time of his arrival, as well as the identification of all the people at the scene. Then, for every piece of evidence, the first responder or the investigator must create an evidence log, where all actions performed with the evidence will be logged and documented, including the location, the state of each evidence file and the time they were collected. Moreover, the documentation process must include the type and model, the serial number and other similar descriptors, and whether the device is connected to a network or to other devices. The evidence log will remain with the evidence until the end of the investigation, where it will be either handed to the authorities or returned to the owner. This will provide documentation of the actions performed not only for legal purposes, but also this can facilitate further analysis for future lessons learned activities.

### 4.1.4. Chain of Custody

One of the main requirements for all investigations is the chain of custody, where every person of the team who has access to the evidence, must record and log every time he interacts with the piece of evidence. The minimum requirements for a well preserved chain of custody for electronic evidence, is be able to prove that no information has been added or changed, that a exact copy was made, that the copying process used was reliable, and that all media was secured. A well documented chain of custody is crucial for maintaining the integrity of the evidence. The chain of custody accounts on every piece of evidence from the moment it's



collected and until the end of the investigation. Whenever the evidence is accessed it should be recorded. So, it becomes clear that the fewer people have access to the evidence, the easier it is to control. Especially, when the evidence is to be presented in court of law, it is important that all the process of evidence handling, every access, and action taken, including the reason and the exact time of access, are reviewed by the team manager. The reason for this is that should the chain be broken, the integrity of the evidence could be questioned in a court of law. The Prosecutor's primary means in authenticating electronic evidence is proving the chain was unbroken.

#### **4.1.5. Imaging and Hashing**

The next step is to create images of the data to be investigated, since the original evidence must never be in any way processed. This step is for eliminating the danger of destroying or modifying the original evidence during investigation. Therefore, a bit image of the data is captured and hashing techniques are applied in order to prove mathematically that the image is identical to the original data. This way, the investigator can examine and analyse a copy of the data and avoid any alteration or corruption of the original evidence.

#### **4.1.6. Analysis**

Examiners using their technical knowledge and the appropriate tools must locate and interpret the artifacts on the media being analyzed. This analysis could include creating a timeline of events, recovering deleted files, breaking encryption, identifying which websites have been visited and what searches the user performed on the web, discover whether a USB storage device was at any point connected to the machine under investigation, and much more.

During the analysis, investigators must log their actions thoroughly in the evidence notebook. The minimum information logged include the date and time of analysis, the tools used, the detailed methodology of the analysis, and the results of the analysis. In the process of examining a data storage device, the first thing that should be examined is its size, its storage capacity and the system parameters with the help of the manufacturer's technical specifications, since each operating system and formats may present different storage capacity. Therefore, the investigator will know if he must look for potentially hidden data, erased files, slack space or encrypted partitions where valuable data may be concealed.

Nowadays, platforms, storage devices, network devices and applications log their activities and have event capture mechanisms or they can be configured to do so. These logs may contain background data on the events under investigation, or may

be the evidence of a possible suspicious event. The Team Manager must review the logs of each potential device, check timestamps on each event, review the correlations made between the event recorded, the logs and any recorded activity.

The Team Manager must ensure that all evidence is identified, collected, and examined during any investigation, so he should reviewed all data capture activities, the steps the investigator took, and the examiner's reports to confirm whether all possible device, which contains data relevant to the case, is examined.

#### **4.1.7. Repeatability**

Repeatability is a key aspect of digital forensics. The results of a forensic examination as well as the processes applied should be able to be replicated by another examiner. This means that given the same evidence and following the same steps while using same tools, the produced results should be the same. Repeatability ensures the quality of the forensic process and help to secure the accuracy of the findings. This quality assurance includes a variety of issues such as the technical skill of the analysts, the trustworthiness of the tools, the security of the storage facility of the evidence, and so on.

As stated before, the team manager has to follow the standard audit and recovery techniques, as the evidence is collected during the collection and analysis phases. These processes will also allow reassessing an investigation, using a different technical means if needed. Apart for those standard techniques, there may be needed for data discovery, when valuable data may be inaccessible or damaged and can't be accessed in a standard way. The most common data recovery cases are an operating system failure, a drive-level failure, a malfunction or an accidental damage of a storage device or on purpose deletion of data.

Digital evidence must be handled with caution to preserve the integrity of state and contain. Some digital evidence requires unusual collection, packaging, and transportation techniques, since their data could be damaged by electromagnetic fields. Communication devices should be packaged, using material that prevents them from transmitting or receiving data. Corporations usually have complex computer systems and networks, and they could be proved quite difficult for securing the scene and collecting the evidence. When a system is running, it is generally better to leave it open, since, if not done properly, it may result in lost evidence.

## 5. Legal Framework within the EU

The European Union considers privacy and the protection of personal data as two independent fundamental rights, although data protection is closely connected to the right to privacy.

The protection for "private and family life" initially came into effect in 1953 within the framework of the European Convention of Human Rights, the international treaty to protect human rights and fundamental freedoms in Europe. The respect for privacy was established in article 8, and it prevented public authorities from interfering in a privacy invasive manner, unless certain legal conditions have been met.

Under the *article 8* of the European Convention of Human Rights, every individual has "the right to respect for his private and family life, his home and his correspondence". A public authority has no right to interfere, unless it is in accordance with the law and it is required in the interests of national security, public safety or the economic safety of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. The *article 10* of the European Convention of Human Rights provides for the right to freedom of expression. Public authority has no right to interfere with personal opinions, information or ideas, unless it is in accordance with the law.

In 1980, the Organization for Economic Cooperation and Development provided its "Recommendations of the Council concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data" with seventh underlying principles. According to those principles, the data subjects should be notified when their data is being collected, be informed about the purpose of the data collection and those data should not be used for any other purpose. Furthermore, the data subjects should consent to this collection, should be informed as to who is collecting their data and they should have access to them in order to correct them, if inaccurate. Finally, the collected data should be protected from any potential abuse and the data subjects should have a method available to hold data collectors responsible for following all the above. However, those guidelines were not mandatory, so there were a variety of data privacy laws across Europe. All seven principles were later included into the Data Protection Directive (95/46/EC).

The Data Protection Directive (95/46/EC) is a European Union directive adopted in 1995, in an effort to establish a comprehensive data protection system. Its principles aim to found the circumstances under which the process of personal data is lawful, so that the rights and freedoms of persons are protected by preventing the misuse of their information. The Data Protection Directive defines that data should not be

processed at all, unless that process is transparent, proportional and for legitimate purpose, while setting up an independent supervisory authority to monitor the data protection level in each state.

Under the articles 7 and 12, data processing is considered lawful when:

- ✓ The data subject has given his consent.
- ✓ The processing is necessary for the performance of or the conclusion of the contract.
- ✓ For compliance with a legal obligation.
- ✓ When processing is necessary, in order to protect the vital interests of the data subject.
- ✓ When processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.
- ✓ When processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. The data subject has the right to access all data processed about him. The data subject even has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules.

There are also data quality principles, so that data processing is considered lawful:

- ✓ Personal data must be processed fairly and lawfully, and collected for specified, explicit and legitimate purposes. They must also be adequate, relevant and not excessive, accurate and, where necessary, kept up to date, must not be stored for longer than necessary and solely for the purposes for which they were collected;
- ✓ Special categories of processing: it is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. This provision comes with certain qualifications concerning, for example, cases where processing is necessary to protect the vital interests of the data subject or for the purposes of preventive medicine and medical diagnosis.

Under articles 10 and 11, the data subject can exercise the following rights:

- ✓ The right to be informed when his personal data is being processed, access them and correct them if inaccurate,

- ✓ The right to obtain information: the controller must fully identify himself to the data subject, inform for the purposes of the processing the recipients of the data,
- ✓ The right to object to the processing of data, on legitimate grounds, to the processing of his data.

The data subject's rights, regarding the quality of and the access to the data and the right to be informed, don't apply when protecting aspects such as national or public security, defense, the prosecution of criminal offences, an important economic or financial interest of a Member State or of the European Union or the protection of the data subject.

The confidentiality and security of processing must be ensured. Thus, a person, acting under the authority of the controller, must not process them except when he instructed by the controller. Moreover, the controller must apply proper measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, otherwise the data subject has the right to obtain compensation for the damage suffered.

The transfer of personal data from a European Member State to a third country is permitted, when the third country has adequate level of protection. However, there are exceptions to this rule listed in the Directive.

The Charter of Fundamental Rights of the EU contains the fundamental rights protected in the EU, and has entered into force of the Treaty of Lisbon, in December 2009. The rights and freedoms contained in the Charter can be described by six titles; Dignity, Freedoms, Equality, Solidarity, Citizens' Rights, and Justice. Individual's rights within the EU were founded at different times, in different ways and in different forms. Therefore, in the effort to clarify things, the EU decided to include them all in a single document updated according to social, scientific and technological developments. It establishes the rights and freedoms protected in the European Convention on Human Rights and other rights and principles resulting from the common constitutional traditions of EU countries and other international instruments. The *article 7* of the Fundamental Freedoms and the Charter of Fundamental Rights of the European Union provide the protection of private and family life, home, and communication.

The article 13a of the Framework Directive (2009/140/EC) for electronic communications declares that providers of public communication networks and services should implemented technical and organizational measures to assure the security and integrity of their networks thus ensure the availability of services provided and, if any major security breach, report it to national authorities. When necessary, the national regulatory authority should inform their counterparts, others

EU Member States as well as ENISA. Moreover, every year, national authorities must report to the Commission and ENISA about the incidents. Finally, the Commission, taking into account of the opinion of ENISA, may implement proper technical measures, if needed.

The Directive 2002/58/EC on privacy and electronic communications concentrate on data protection and privacy related to the provision of public electronic communication networks or services. It defines rules to guarantee security in the processing of personal data, the notification of personal data breaches, and confidentiality of communications. It also forbids unsolicited communications where the user has not given their consent. The article 4 of the directive requires providers to take appropriate technical and organizational measures to maintain security of their services, to notify security breaches to the authority and to the subscribers and whether that security breach had affected their privacy, and to keep a list of breaches, including the facts, the impact and the counteractive actions.

In January 2012, the European Commission proposed a Reform of the Data Protection Directive (95/46/EC) to support online privacy rights and encourage Europe's digital economy. The regulation concerns organizations that process personal data, regardless of the business sector they are in. The articles 30, 31 and 32, among others, declare that, depending on risks presented by the processing, organizations should apply proper technical and organizational security measures to ensure security. National authority must be notified, if personal data breaches occur without undue delay and, if possible, within 24 hours, or else a justification should be provided. Individuals must be notified, if personal data breaches occur only when there is a possible impact on their privacy.

The European Commission recently released a proposal for a regulation on electronic identification and trust services for electronic transactions in the internal market, where it establishes obligations regarding security measures and incident reporting. Trust service providers must implement proper technical and organizational measures to ensure security, while they must notify supervisory authorities of any security breaches. The supervisory authority sends a review of breaches to ENISA and the European Commission.

## 6. Digital Forensics Tolls Web Page

In the context of this dissertation is the development of a web page that will include a collection of the tools available both free and commercial. Furthermore, the web-page will include a forum where registered members will be able to discuss news and issues about forensic news and issues, discuss issues about the tools, and share their opinion.

The purpose of this Website is to facilitate digital forensic professionals in their search for tools and to interact sharing their knowledge and experience.

### 6.1. The web page

The web page is organized as follow:

The index page contains a brief description of the purpose of the page.

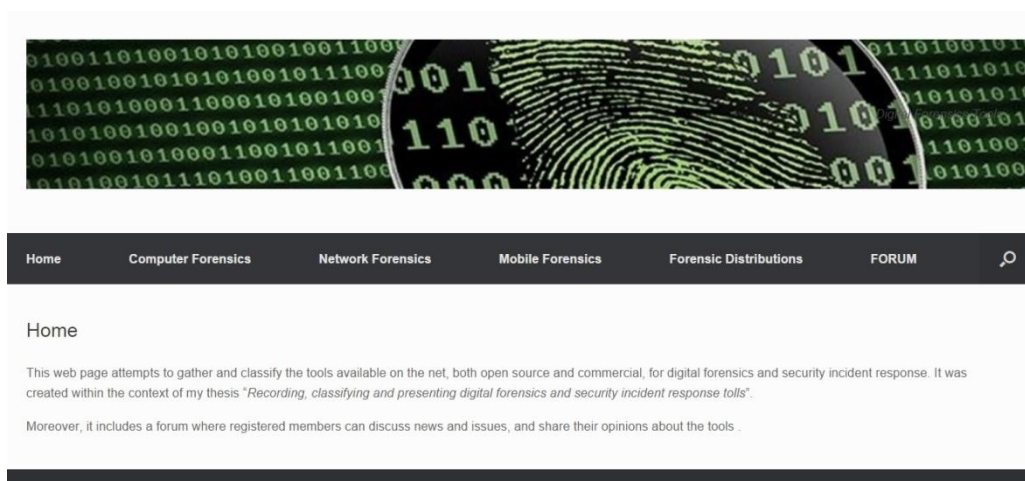


Figure 7 Home Page

The main menu contains four categories; these are *computer forensics*, *network forensics*, *mobile forensics* and *forensics distributions*

The category *computer forensics* is divided into subcategories for disk and data acquisition, file and data analysis, memory acquisition and memory analysis, data recovery and specific tools.

The category *mobile forensics* is divided into three subcategories. These are acquisition tools, analysis tools and specific tools.

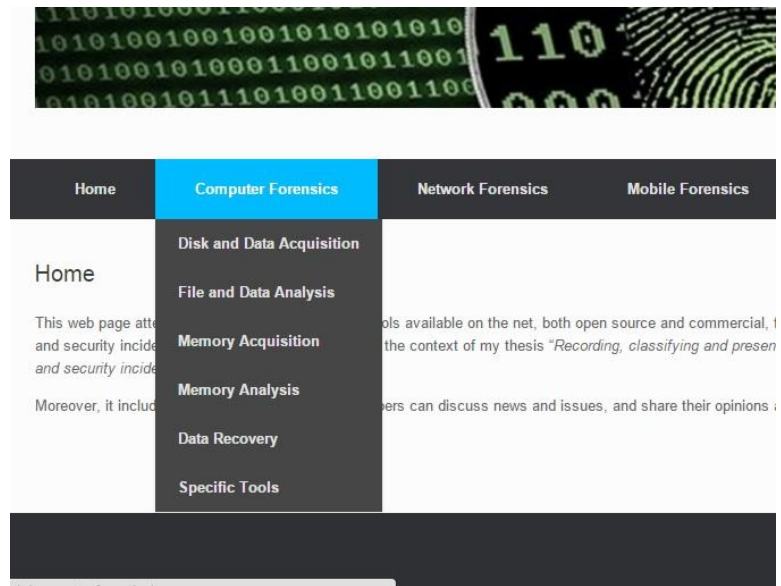


Figure 8 Computer Forensics Subcategories

Each of these subcategories includes a table where the tools concerning this subcategory are listed.

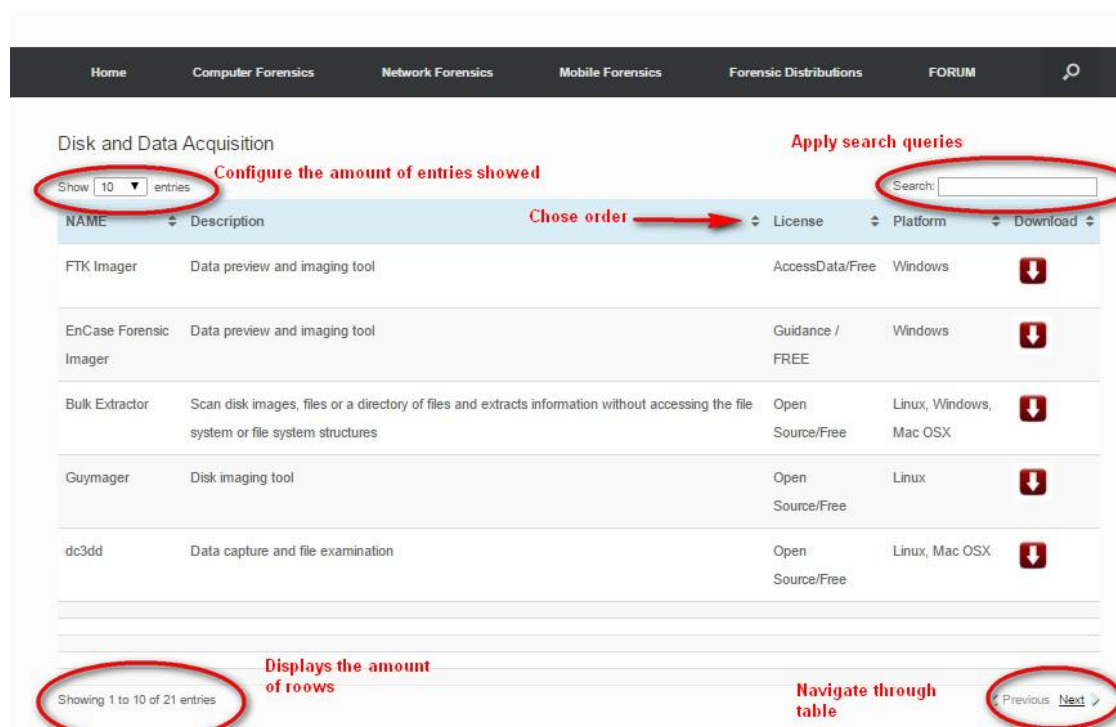


Figure 9 Table Structure

Each row consists of five columns containing information about one tool. That information is:

- ✓ The name of the tool,
- ✓ The description of what is the tool used for,
- ✓ Its license,



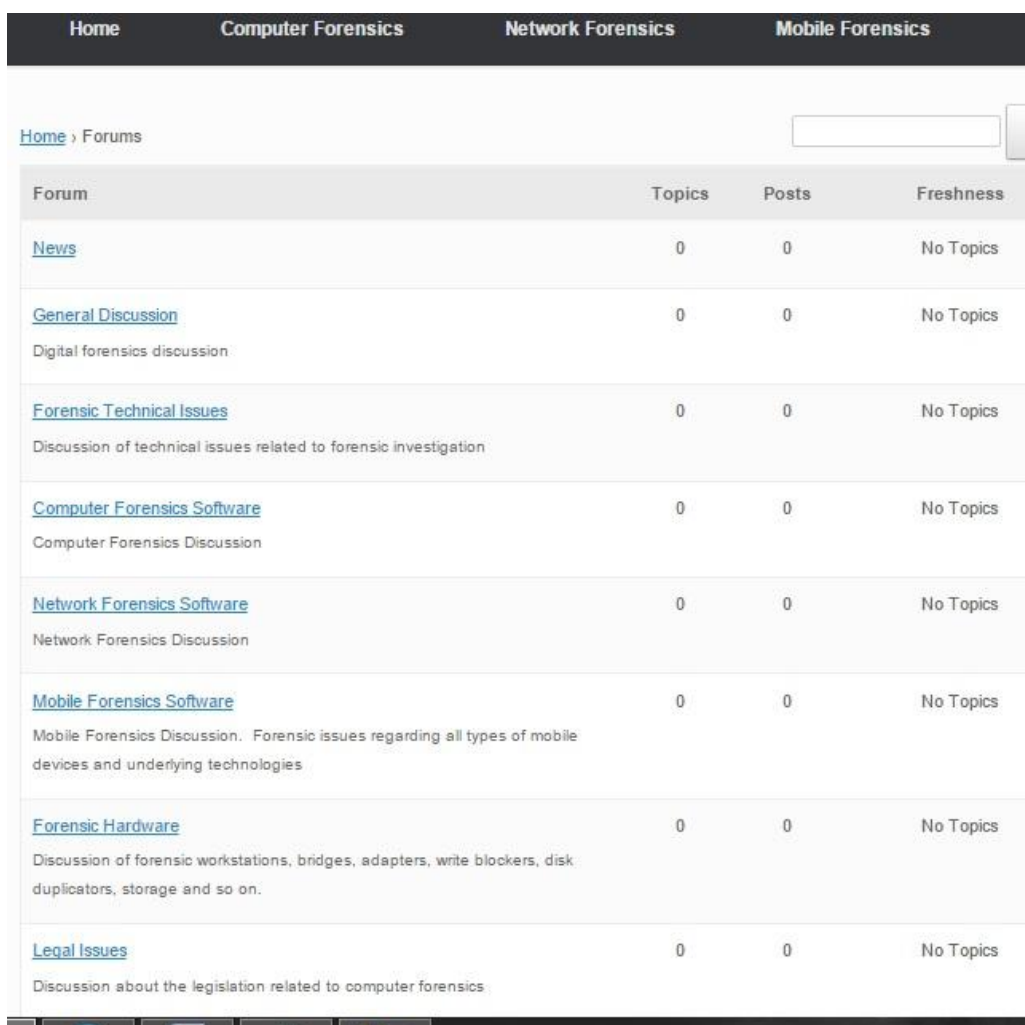
- ✓ Which platform it can run,
- ✓ A download link that opens a new page from where the user can obtain the tool.

Furthermore, the user may apply search queries to the table to narrow his search, or apply ascending or descending order to any of the columns.

In exactly the same way are listed the tools in each of the remaining categories.

## 6.2. The Forum

The Forum is organized in eight sections.



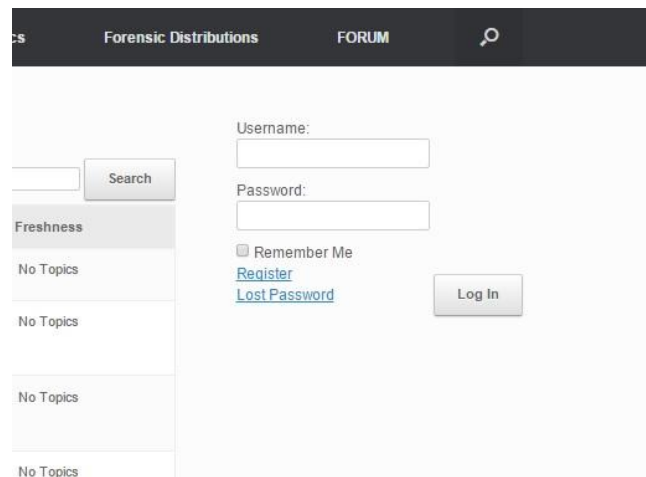
Forum	Topics	Posts	Freshness
<a href="#">News</a>	0	0	No Topics
<a href="#">General Discussion</a> Digital forensics discussion	0	0	No Topics
<a href="#">Forensic Technical Issues</a> Discussion of technical issues related to forensic investigation	0	0	No Topics
<a href="#">Computer Forensics Software</a> Computer Forensics Discussion	0	0	No Topics
<a href="#">Network Forensics Software</a> Network Forensics Discussion	0	0	No Topics
<a href="#">Mobile Forensics Software</a> Mobile Forensics Discussion. Forensic issues regarding all types of mobile devices and underlying technologies	0	0	No Topics
<a href="#">Forensic Hardware</a> Discussion of forensic workstations, bridges, adapters, write blockers, disk duplicators, storage and so on.	0	0	No Topics
<a href="#">Legal Issues</a> Discussion about the legislation related to computer forensics	0	0	No Topics

Figure 10 Forum Home Page

The first is the *News* section where users can post news topics concerning digital forensics. Next is the *general discussion* section where user can discuss general issues and concerns about digital forensics followed by the *technical issues* section where users may discuss about technical issues related to forensic investigations. The fourth, fifth and sixth sections are the *computer forensics software*, the *network forensics*

*software* and the *mobile forensics software*. In those sections the users may post topics about the software of each category. Next is *forensic hardware* section for discussions concerning forensic workstations, write blockers, disk duplicators, storage, and other forensic devices. And finally, in the *legal issues* section users may post topics about the legislation related to digital forensics.

The forum is designed to be visible to anyone who visits the webpage with no registration. Users need to login only if they want engage in the discussion.



**Figure 11 Forum Login Section**

Once a user has logged in, he can then post a new topic in any section, reply to a post, and subscribe to any existed topic in order to be informed of any change via email.

## 7. Incident Response and Digital forensic tools

There are many different types of tools available for commercial and open source as well as forensic distributions for proper incident response and forensics analysis. The types of tools required for an investigation depend on the type of data and files and on the operating systems being analyzed. Every operating system has its own kernel code, drivers and libraries.

### 7.1. Computer Forensic

#### 7.1.1. Disk and data acquisition

This section contains tools that perform data acquisition and disk imaging.

##### *EnCase Forensic Imager*

The EnCase forensic imager is a free application for acquiring, evidence files that include CRC block checks, hash values, compression, and encryption. It allows browsing and viewing of evidence files, including folder structures and file metadata. It can acquire images of local drives and it uses AES 256-bit encryption to protect Lx01 and Ex01 files.

The EnCase Forensic Imager can acquire evidence in four basic formats which are current encase evidence files (.ex01), current logical evidence files (.lx01), legacy encase evidence files (.e01) and legacy logical evidence files (.l01)

Some of its features are:

- ✓ Preview memory or local devices such as hard drives, memory cards, or flash drives.
- ✓ Evidence files supported are DD images, VMware files, or virtual PC files.
- ✓ Single files selected to create a Logical Evidence File from an existing evidence file or an acquired device.
- ✓ Network crossover using LinEn and EnCase forensic imager to create .E01 files or .L01 files for previewing a device without disassembling the host computer.

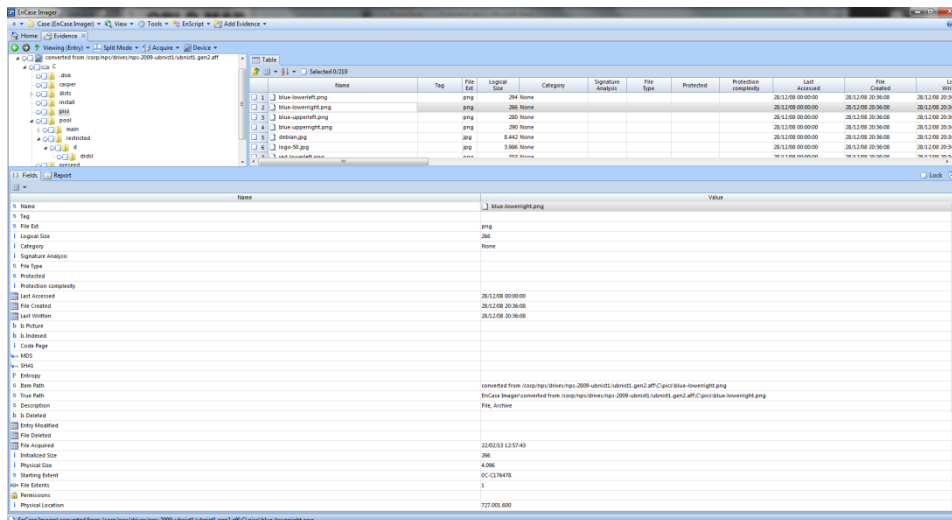


Figure 12 EnCase Forensic Imager

The EnCase Imager is a standalone product which requires no installation and can be loaded via USB stick to perform acquisition of a live device.

### FTK Imager

The FTK Imager is a free data preview and imaging tool for Windows. It creates forensic images of computer data without making changes to the original evidence. It can show preview of files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, and DVDs; it can create forensic images of them. It can preview the contents of forensic images stored on the local machine or on a network drive, export files and folders from forensic images, and generate hash reports for regular files and disk images.

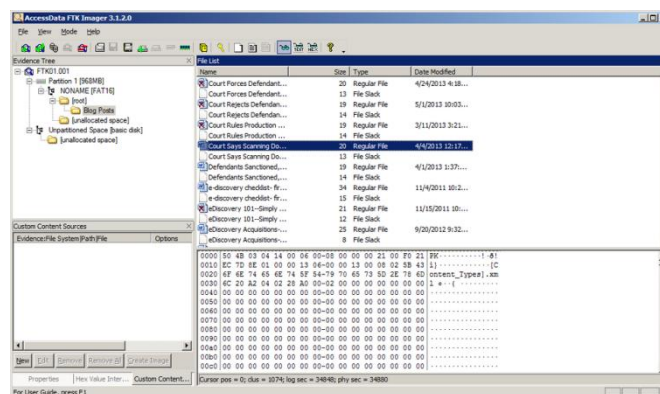


Figure 13 FTK Imager

The FTK Imager has three modes for previewing electronic data. The *automatic mode*, which automatically chooses the best method for previewing a file's contents. The *text mode* that allows to chose preview a file's contents between ASCII and Unicode characters, even if the file is not a text file. The *hex mode*, allows viewing every byte of data in a file as hexadecimal code.

The FTK Imager is also able to create forensic images of physical disks, logical volumes and previously created images. Another interesting feature of the FTK Imager is the ability to create a directory listing of all files within the image. After creating the image, if it can parse the file system, it will output a directory listing to a separate CSV file using the naming convention. During the image creation process, the FTK also offers encryption. The output format of the created image can be Raw, SMART, E01 or AFF.

The FTK Imager supports the handling of a great amount of forensic image formats which are listed below, according to what the image is for.

For file systems, the file formats supported are all FATs, NTFS, Ext2/3/4FS, HFS, HFS+, CDFS, ReiserFS3, VXFS and exFAT.

For whole disk encryption, the file formats supported are PGP, Utimaco, Credant, Guardian Edge, SafeBoot, EFS, JFS,LVM,VMware, LVM2, UFS1, UFS2. The FTK Imager can't perform cracking, therefore the password to open them must be provided.

For hard disk image formats, the file formats supported are Encase, SnapBack, Safeback 2.0 and under, Expert Witness, Linux DD, ICS, SMART, AD1, and AFF.

For CD and DVD Image Formats, the file formats supported are all types of CD and DVD and Alcohol), IsoBuster, PlexTools, CloneCD, Nero, Roxio, ISO, Pinnacle, Virtual CD, CloneCD, Pinnacle, Virtual CD.

### *Dump Data*

The DD is a standar UNIX command line utility that allows data capture and file examination. The dd command is standard in all UNIX distributions. It can be used to duplicate data from a media device and a data file. It creates a file in raw format that most computer forensics analysis tools can read. The DD can perform data transfer, data modification, disk wiping, data recovery, can create master boot record backup and restore, generate a file with random data and convert a file to upper case.

### *dc3dd*

The *dc3dd* is a patched version of GNU dd with added features for computer forensics. Unlike the GNU dd's version, on a partial read with dc3dd, the whole block is wiped with zeros allowing of repeatable reads of a drive with errors.

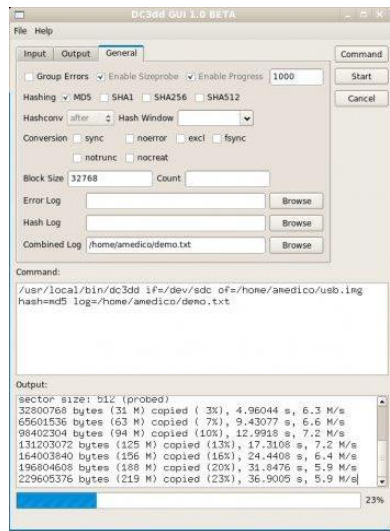


Figure 14 dc3dd

The dc3dd's features are:

- ✓ Hashing with multiple algorithms,
- ✓ Is able to write errors directly to a file,
- ✓ Combined error log, groups errors together,
- ✓ Wipe output files with a single hex digit or a text pattern,
- ✓ Seeing the progress of the operation while it's running,
- ✓ Able to split output files into fixed size chunks.

The dc3dd supports Linux, BSD, Solaris, Mac OS X.

The dcfldd is an enhanced version of the dd. The dc3dd and the dcfldd programs are based on slightly different code bases. The dcfldd is a fork of the GNU dd, whereas the dc3dd is a patch to the current version of dd. Therefore, every time GNU dd is updated so it will be dc3dd, whereas dcfldd has its own release schedule.

Dcfldd command, offers some additional capabilities, including:

- ✓ Specify hexadecimal patterns or text for clearing disk space,
- ✓ Log errors to an output file for analysis and review,
- ✓ Hashing options,
- ✓ S status display indicating the progress of the acquisition in bytes,
- ✓ Split data acquisitions into segmented volumes with numeric extensions,
- ✓ Verify the acquired data with the original disk or media data.

### **Bulk Extractor**

The Bulk Extractor is an open source computer forensics tool which is used to scan disk images, files or a directory of files and it extracts information without accessing the file system or file system structures. Then, the results can be analyzed with

automated tools. The Bulk Extractor also creates histograms of features that it finds and these can be used for law enforcement, defense, intelligence, and cyber-investigation applications.

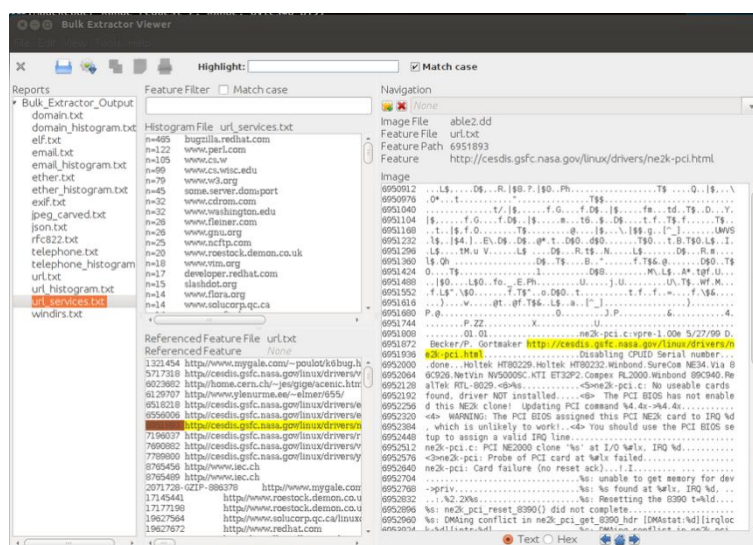


Figure 15 Bulk Extractor

As the Bulk Extractor ignores file system structure, it can process simultaneously different parts of the disk. In fact, it divides the disk up into 16MiByte pages and processes one page on each available core. Furthermore, the compressed data are automatically detected, decompressed, and recursively reprocessed. In addition, Bulk Extractor can be used to process any digital media such as hard drives, SSDs, optical media, camera cards, cell phones, network packet dumps, and other kinds of digital information. Moreover, the Bulk Extractor creates a digital forensics XML report which contains information about the source media, the time it took to process the digital evidence, and a meta report of the information that was found.

The extracted information is outputted to a list of text files:

- ✓ *ccn.txt* which contains credit card numbers,
- ✓ *ccn\_track2.txt* which contains credit card “track 2” information,
- ✓ *domain.txt* which contains internet domains found on the drive,
- ✓ *email.txt* which contains email addresses,
- ✓ *ether.txt* which contains ethernet mac addresses found through ip packet carving of swap files and compressed system hibernation files and file fragments,
- ✓ *exif.txt* which contains exifs from jpegs and video segments. This feature file contains all of the exif fields, expanded as xml records,
- ✓ *find.txt* which contains the results of specific regular expression search requests,
- ✓ *ip.txt* which contains ip addresses found through ip packet carving,

- ✓ *telephone.txt* which contains telephone numbers,
- ✓ *url.txt* which contains urls, usually found in browser caches, email messages, and precompiled into executables,
- ✓ *url\_searches.txt* which contains a histogram of terms used in internet searches from services such as google, bing, yahoo, and others,
- ✓ *wordlist.txt* which contains a list of all “words” extracted from the disk, useful for password cracking,
- ✓ *wordlist\_\*.txt* which contains the wordlist with duplicates removed, formatted in a form that can be easily imported into a popular password-cracking program,
- ✓ *zip.txt* which contains a file containing information regarding every zip file component found on the media..

The Bulk Extractor is supported in a Linux/Unix, Mac OS X and Windows systems.

### *OSFClone*

OSFClone is a free, Unix based self booting tool for creating of raw disk images and is independent of the installed operating system. It also supports imaging drives to the advance forensics format AFF. OSFClone creates a forensic image of a disk, preserving any unused sectors, slack space, file fragmentation and undeleted file records from the original hard disk.

Some of its features are:

- ✓ Creates disk clones of FAT, NTFS and USB connected drives
- ✓ Can be booted from CD/DVD drives, or from USB flash drives.
- ✓ Can create disk images in the dc3dd format.
- ✓ Can compare the MD5 or SHA1 hash between the clone and the source drive
- ✓ Can save forensic metadata such as case number, evidence number, examiner name, description and checksum, for cloned or created images.

### *Paragon Backup and Recovery*

Paragon Backup and Recovery is a free imaging software for disaster recovery and system migration that runs on Windows systems. Some of its features are:

- ✓ Graphical representation of the data
- ✓ Allows previewing the resulting layout of hard disks before actually executing operations.
- ✓ Can backup to local mounted or unmounted partitions, to an external mounted storage, to external media (CD/DVD), to a network drive or to a special secured place on the hard disk



- ✓ It can perform *sector backup* to save the system service structures or *differential backup* to a sector image to only archive changes since the last full sector-based image.
- ✓ Restores an entire disk, separate partitions, or only files.

The supported file systems are all FAT, NTFS, Linux and PTS DOS, Ext2/3/4FS, and Apple HFS+. It can restore data from hard disks, USB, SSD, AFD, optical discs and PC card storage devices.

### *Clonezilla*

Clonezilla is an open source software for partition disk imaging or cloning. There are two types of Clonezilla, Clonezilla live and Clonezilla server edition. Clonezilla live is suitable for single machine backup and restore, while Clonezilla SE can clone many computers simultaneously.

Some of its features are:

- ✓ All file systems are supported
- ✓ LVM2 under GNU/Linux is supported.
- ✓ Boot loader, including grub and syslinux, could be reinstalled.
- ✓ Both MBR and GPT partition formats of hard drive are supported. Clonezilla live also can be booted on a BIOS or UEFI machine.
- ✓ Unattended mode is supported. Almost all steps can be done via commands and options.
- ✓ Supports restoring one image to multiple local devices.
- ✓ Image encryption.
- ✓ Clonezilla SE supports multicast, which is suitable for massively clone.
- ✓ The image file can be on local disk, ssh server, samba server, NFS server or WebDAV server.
- ✓ AES-256 encryption could be used to secures data access, storage and transfer.
- ✓ Can save and restore not only partitions, but also whole disks.

### *Guymager*

Guymager is an open source graphical disk imaging tool for Linux. It provides various formats for forensic images such as raw, AFF, and EWF image files and includes case management functionality.

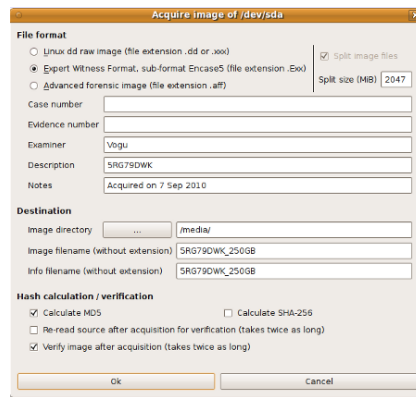


Figure 16 Guymager

Once launched, Guymager begins to scan the system. It finds internal and external drivers, and optical drives if a disc is inserted. Then it displays them with their names and the model names. The default format that the application uses is EWF which is the typical format for professional forensic application but it can also be configured to raw or AFF.

If the EWF format is selected the case management functions are enabled and additional information can be added such as the evidence number, the case number, and a description. There also the option to split the image into several parts depending on the size of the data source and the target disk.

The integrity of the existing data and the image is checked and documented with hash functions such as MD5 or SHA-1 and SHA-256 algorithm. By default, the software works with MD5. After completing the image, the application verifies the image through the checksums and shows matching information under the state heading.

It only runs on Linux.

### *xmount*

xmount is a free Linux command tool that allows to convert multiple input and output hard disk image types. It creates a virtual file system using FUSE that contains a virtual representation of the input image. The virtual representation can be in raw DD, DMG, VHD, VirtualBox's virtual disk file format or in VmWare's VMDK file format. The input images can be raw DD, EWF or AFF files. In addition, xmount also supports virtual write access to the output files that is redirected to a cache file. It runs on Linux and Mac OS X

### *Passware Kit Forensic*

Passware Kit is commercial forensic software for Windows that performs data collection from computers, mobile devices, cloud systems, that can also detect all password-protected items on a computer and decrypts them. Some of its features are:

- ✓ Acquires backups and data from cloud services: Apple iCloud, MS OneDrive, and Dropbox.
- ✓ Process thousands of files simultaneously and larger dictionary files
- ✓ Runs password recovery for groups of files without manual intervention
- ✓ Instantly decrypts hard disk images with live memory analysis or recovers their passwords with accelerated brute-force attacks
- ✓ One-click password recovery directly from EnCase
- ✓ Recovers Passwords for Apple iPhone/iPad and Android backups, as well as Android images. Extracts data from Windows Phones' images.
- ✓ Recovers passwords
- ✓ Scans computers for encrypted evidence and detects all encrypted files and hard disc images, reports encryption type and decryption complexity
- ✓ Live memory analysis
- ✓ GPU, TACC, distributed computing, and rainbow tables

### **SAW**

SAW is a commercial data acquisition and optimization software for creating forensic images from storage media. It runs under Windows, Mac and Linux operating systems. The created images can be used for searching, authenticating, analyzing, carving, and indexing and interacting with data stored within many other forensic image formats.

### **Reflect (Macrium)**

Reflect is a software for Windows that has a free and commercial version. It is a disk cloning and imaging software that supports backup to local, network and USB drives as well as burning to all DVD formats.

Some of its features are:

- ✓ VSS support for data integrity
- ✓ Drag and drop user interface
- ✓ Reorder and resize partitions
- ✓ GPT support
- ✓ UEFI Support
- ✓ Creates differential images for faster backups and reduced storage space.
- ✓ Automatically verify images after creation to ensure integrity.
- ✓ Supports scheduled backups.
- ✓ Additional drivers required for disk or network access will be automatically identified and if possible copied from the host operating system.
- ✓ Allows to add a boot menu for easily restore a system image without inserting rescue media.

### *Forensic Replicator*

Forensic Replicator is a commercial tool for creating bit stream forensic images of hard drives and media. It can also perform password protection, compression, and image splitting. Some of its features are:

- ✓ SHA1 hash value calculation
- ✓ DOD standard media wiping
- ✓ Drive to drive image option
- ✓ Preview image files
- ✓ Encrypt images
- ✓ Split images to specific sizes
- ✓ Compress images to save space
- ✓ Restore images to physical drive
- ✓ Create self extracting files

The supports images are PFR images, raw images, fixed size VHD images and dynamically expanding VHD images.

### *Oxygen Forensic Cloud Extractor*

Oxygen Forensic Cloud Extractor is a commercial application that can acquire data from cloud storage such as: iCloud contacts and calendar, Google Drive, Google Location History, Live contacts and calendar, OneDrive, Dropbox and Box as well as from social media like Twitter and Instagram. To retrieve data, it can use either account credentials or token to enter the cloud account.

### *DriveImage XML*

DriveImage XML is a software for imaging and backing up partitions and logical drives for Windows platforms and has a free and commercial version. Image creation uses Microsoft's Volume Shadow Services (VSS), and store them in XML files. Furthermore, it offers two different compression levels and will backup, image and restore drives formatted with FAT 12, 16, 32 and NTFS.

DriveImage XML runs under Windows XP, Windows Server 2003, Vista, Windows 7, and Windows 8 but it can also boot from the Runtime Live CD or the BartPE boot CD-ROM.

## **7.1.2. Filesystem and Data Analysis**

### *Sleuth Kit / Autopsy*

The *Sleuth Kit* is a framework, a collection of Linux command line tools that perform different aspects of a file system analysis. The *Autopsy* Forensic Browser is a graphical interface that provides a user friendly interface to the Sleuth Kit.

The Autopsy is an open source forensic suite for analysing Microsoft and UNIX file systems, disk images and smart phones. It enables investigators to identify and recover evidence from images acquired during incident response or from live systems. The file system tools allow an examiner to perform an examination in a non-intrusive manner. Since the tools do not depend on the operating system for the file systems processing, the access to deleted and hidden content is achievable. The media management tools allow an examination of the layout of storage devices. It supports OS partitions, BSD partitions, Mac partitions, Sun slices, and GPT disks. Once the investigator identifies the location of the partitions, he may extract them and, then, he may conduct analysis with the file system analysis tools. The tools can be run on a live Windows or UNIX system during Incident Response, they will show hidden files by rootkits and will not modify the access time of viewed files.

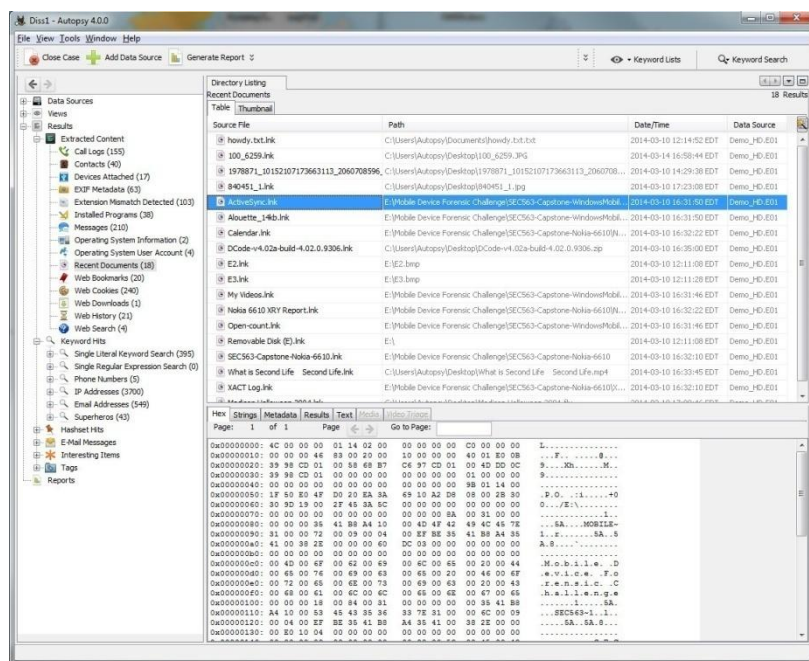


Figure 17 Autopsy, Windows version

The types of input data, that the Sleuth Kit supports, are raw images, Expert Witness and AFF file system and disk images. It fully supports the NTFS, FAT, ExFAT, UFS 1, UFS 2, EXT2FS, EXT3FS, Ext4, HFS, ISO 9660, and YAFFS2 file systems.

In Linux environment, Autopsy has a web based front end. The investigator can either open an existent case or create a new one. When creating a new case, initially all the information and details about the case must be entered. This will include the name of the case and a description of the case as well as the details about the investigators if more than one. Then it displays where the evidence directory is created.



Figure 18 Autopsy Linux version

Next, is the option for adding an image or capturing one. When adding an existing image, rather than working on the original image, we can select the move option, to copy the image to the analysis host and have a separate copy of the image for the analysis.

Then the host must be added to the case where the timezone and timeskew can be configured. Also, a list of known good or bad hashes can be added at this point.

Autopsy has two analysis modes. The *dead analysis* take places when Autopsy and Sleuth Kit are running in a lab. The *live analysis* take places when the suspect system is being analyzed while it is running. In this case, Autopsy and Sleuth Kit are running from a CD in an untrusted environment.

Some of its features are:

- ✓ *Timeline Analysis* - Advanced graphical event viewing interface.
- ✓ *Hash Filtering* - Flag known bad files and ignore known good.
- ✓ *Keyword Search* - indexed keyword search for finding files that contain specific expressions.
- ✓ *Web Artifacts* - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.
- ✓ *Data Carving* - Recover deleted files from unallocated space using photorec
- ✓ *Multimedia* - Extract EXIF from pictures and watch videos.
- ✓ *Mindicators of Compromise* - Scan a computer using STIX.
- ✓ *Logging*: Audit logs are created on a case, host, and investigator level. The entire Sleuth Kit commands are logged exactly as they are executed on the system.
- ✓ *Reports*: Autopsy can create ASCII reports for files and other file system structures.

The Autopsy's search functionality is to:

- ✓ List allocated and deleted ASCII and Unicode file names,
- ✓ Display the details and contents of all NTFS attributes including all alternate data streams,
- ✓ Display file system and metadata structure details,
- ✓ Create time lines of file activity, which can be imported into a spread sheet to create graphs and reports,
- ✓ Lookup file hashes in a hash database, such as the NIST NSRL, hash keeper, and custom databases that have been created with the 'md5sum' tool,
- ✓ Organize files based on their type. The pages of thumbnails can be made of graphic images for quick analysis.

It support Linux, Mac OS X, Windows, CYGWIN, Open and FreeBSD and Solaris.

### *Digital Forensics Framework (DFF)*

DFF is an open source computer forensics software which facilitates digital investigations by collecting, preserving and analysing digital evidences without compromising systems and data. It runs on Windows and Linux both 32bit and 64 bit systems. DFF has also a commercial version. Its functionalities include preserving digital chain of custody, accessing local and remote devices, reading standard digital forensics file formats, virtual machine disk reconstruction, triaging and searching for metadata, recovering hidden deleted files, unallocated spaces and carving, and performs volatile memory forensics by analyzing processes, local files and network connections

Some of its features are:

- ✓ Logical write blocker
- ✓ Raw format analysis, encase EWF, AFF file format compatibility
- ✓ Cryptographic hash calculation, file signature detection
- ✓ Advanced filtering and search engine
- ✓ Gallery view, video thumbnailer
- ✓ EXIF metadata extraction, LNK files parser
- ✓ Prefetch analysis and registry analysis
- ✓ Microsoft Outlook PST mailboxes
- ✓ Volatility Framework integration
- ✓ Graphical process tree reconstruction
- ✓ VAD access with RWX page tagging as suspicious
- ✓ PDF, texts and web viewers
- ✓ Extracts office document metadata, text and embedded images

### *EnCase Forensic*

The EnCase is a commercial non-invasive computer forensic tool for Windows. It has a graphical user interface that to manage large amount of computer evidence and to

view files, file slack and unallocated data. As it is a case management system, therefore, among its functions is case tracking of individual evidence and data carving. The EnCase can obtain data from a wide variety of devices; it can expose potential evidence with disk-level forensic analysis, and create complete reports, while protecting the integrity of evidence. It contains tools for acquisition, analysis, reporting and can create forensic images of media.

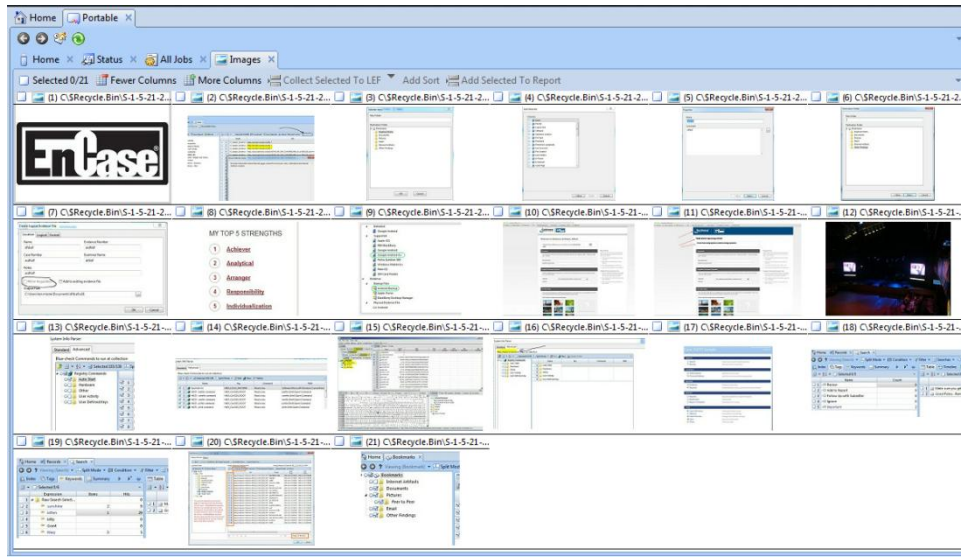


Figure 19 EnCase

The EnCase's features are:

- ✓ Mobile, Cybersecurity, eDiscovery, court approved forensic file format,
- ✓ Memory analysis,
- ✓ Custom tablet for mobile phone acquisition,
- ✓ Built in decryption and password cracking,
- ✓ Email analysis,
- ✓ Distributed analysis,
- ✓ Viewing images on the target machine,
- ✓ Reviewing documents in real-time,
- ✓ Using keywords, metadata, hash values, and other criteria to perform targeted triage and collection,
- ✓ Performing memory acquisition, and full-disk imaging,
- ✓ Two functionality mode (Easy / Advanced),
- ✓ Able to collect evidence from Apple iOS, RIM BlackBerry, Google Android, Windows Mobile Operating Systems, SIM cards, iTunes and backup files,
- ✓ Processing even huge files at speeds faster than any solution in the industry,
- ✓ Creating templates based on case profiles.
- ✓ Dynamic disk support for Windows 2000/XP/2003 Server.
- ✓ Ability to preview and acquire select palm devices.



- ✓ Supports the imaging and analysis of RAID arrays, including hardware and software RAIDs
- ✓ Ability to interpret and analyze VMware, Microsoft Virtual PC, DD and SafeBack v2 image formats.

EnCase supports Windows, Linux, Solaris, AIX, OSX and all file systems.

### *SMART for Linux*

SMART for Linux is a commercial software that performs acquisition, authentication and analysis. Some of its features are

- ✓ Allows the creation of image copies and quasi-proprietary formats that support seekable compression.
- ✓ Can acquire and clone a single source to any number of images and devices simultaneously.
- ✓ Data authentication through hashes
- ✓ Allows mounting devices, partitions, and images.
- ✓ Rules based flexible regex searching. Auto-export, auto-name with collision avoidance and save searched terms into a library.
- ✓ Raw data viewer can recognize certain data structures automatically.
- ✓ Export log events into a simple HTML report.
- ✓ Multi-pass secure wipe with any chosen repeating stream of bytes.

SMART for Linux can be used for local or remote preview of a target system, for post mortem analysis of a dead system as well as for testing and verification of other forensic programs.

### *ProDiscover IR and ProDiscover Forensic Edition*

The ProDiscover Incident Response assists the examination of a live operating system anywhere on a network to determine if that system has been compromised, and if so, provides the evidence needed. It uses an agent that runs on the suspect system, and examines the disk at the bit level. This way, it examines all files, including hidden by Trojans or rootkits. It also prevents the alteration of metadata, it can search for known Trojans or rootkits, and examine all files while comparing their hash signature to the signatures it provided as baseline or from the National Drug Intelligence Center Hashkeeper database, so that the integrity of the OS is verified. In case where the system has been found compromised, the system administrator can make a bit-stream image of the disk for later analysis. The quality of the data that it gathers is admissible to a court of law.

Some of its features are:

- ✓ It creates evidentiary reports admissible to court,



Some of its features are

- ✓ Data capture, analysis, investigation and dissemination, e-mail deconstruction and analysis, reporting features,
- ✓ Unallocated space data salvaging capability,
- ✓ Password protected file detection,
- ✓ Explorer for all evidence, email, archive, registry and salvage explorer,
- ✓ Functions for hashing, indexing, searching, salvage, data reduction, events, virus and trojan detections, illicit image detection
- ✓ Dictionary Generation,
- ✓ Five built-in, search engines,
- ✓ Built-in development environment and file viewers for hundreds of file types
- ✓ Filesystem, file and e-mail recovery,
- ✓ Virus and Trojan search and identification,
- ✓ VMware virtual disk production from devices or images,
- ✓ IVault data store preparation and production,
- ✓ Support for all common archive file formats,
- ✓ Deconstruction of evidentially useful file types,
- ✓ Sorting, grouping and filtering of files and e-mail,
- ✓ MS Outlook e-mail recovery.

### **Forensic Toolkit (FTK)**

FTK is a platform for Windows that provides tools forensic examinations. FTK has function for text indexing, searching, deleted file recovery, data carving, email and graphics analysis. Furthermore, it is a court accepted digital investigations platform.

Since it is a basic IT forensic tool, it includes features such as a registry viewer, logging, standalone disk imager, and direct email and zip file analysis. Moreover, all data is stored in one case database, which allows teams to use the same data, reducing the cost and complexity of creating multiple case datasets. It provides the password recovery, for gaining access to protected files, and the *Distributed Network Attack*, which can be used to crack encrypted files over a network.

Some of its features include:

- ✓ Provides processing and indexing up front.
- ✓ Can be setup for distributed processing and incorporate web-based case management and collaborative analysis.
- ✓ Provide distributed processing and multi-threaded/multi-core support
- ✓ Provides built-in data visualization and explicit image detection technology
- ✓ Cerberus add-on, allows determining the behavior and intent of suspect binaries, without having to wait for the malware team to perform deeper,

more time consuming analysis. This automated malware triage and analysis allows to:

- ✓ - Gain actionable intelligence in seconds to validate threats and take decisive action.
- ✓ - Achieve signature-less malware detection with proactive threat scans.

### FRED

Forensic Registry EDitor is a free GUI based registry editor and viewer that has a built in hex viewer and data interpreter. Furthermore, it also has reporting features.

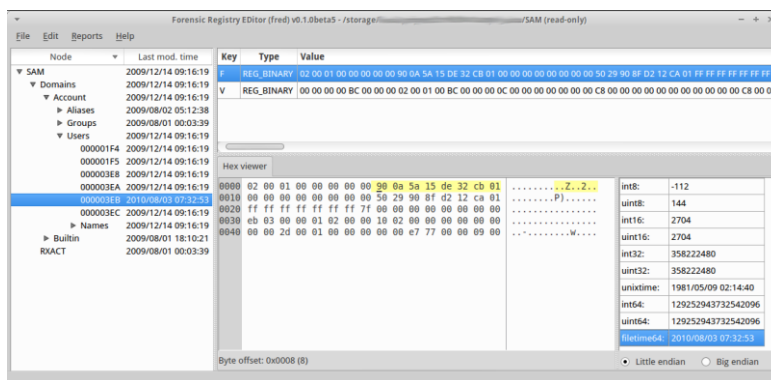


Figure 21 FRED

### OSForensics

The OSForensics is a commercial digital investigation suite for windows that can extract forensic evidence from computers, and perform file searches and indexing. It can identify suspicious files and activity using hash matching, drive signature comparisons, e-mails, memory and binary data. Moreover, it can manage a digital investigation and create reports from collected forensic data.

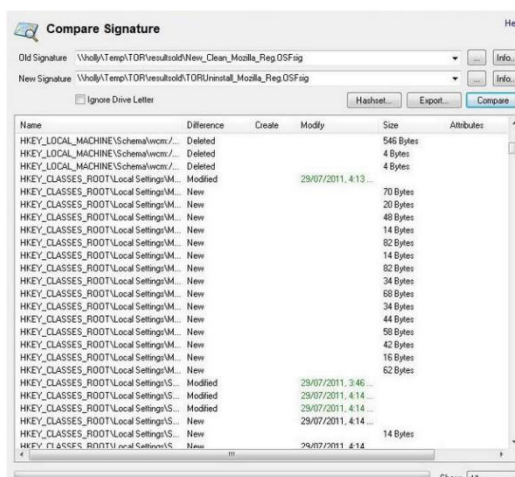


Figure 22 OSForensics Compare signature

The features of the OSForensics free version:

- ✓ It finds files faster, searches by filename, size and time,
- ✓ It searches within file contents, through email archives and searches for deleted files.
- ✓ It uncovers recent activity of website visits, downloads and logins, password recovery from web browsers, decryption of office documents
- ✓ Finds hidden areas in hard disks, browses through volume shadow copies to see past versions of files and verifies and matches files with MD5, SHA-1 and SHA-256 hashes,
- ✓ It finds misnamed files where the contents don't match their extension,
- ✓ Timeline viewer provides a visual representation of system activity over time,
- ✓ File viewer that can display streams, hex, text, images and meta data,
- ✓ Email viewer that can display messages directly from the archive,
- ✓ Registry viewer to allow easy access to Windows registry hive files,
- ✓ File system browser for explorer-like navigation of supported file systems on physical drives, volumes and images,
- ✓ Raw disk viewer to navigate and search through the raw disk bytes on physical drives, volumes and images,
- ✓ Web browser to browse and capture online content for offline evidence management,
- ✓ ThumbCache viewer to browse the Windows thumbnail cache database for evidence of images/files that may have once been in the system,
- ✓ SQLite database browser to view and analyze the contents of SQLite database files,
- ✓ ESEDB viewer to view and analyze the contents of ESE DB (.edb) database files, a common storage format used by various Microsoft applications,
- ✓ Prefetch viewer to identify the time and frequency of applications that been running on the system,
- ✓ Case management and HTML case reports to summarize all results and items
- ✓ Drive imaging for creating or restoring an exact copy of a storage device,
- ✓ It rebuilds RAID arrays from individual disk images,
- ✓ It maintains a secure log of all activities carried out the investigation.
- ✓ It can be installed on a USB flash drive for more portability,

The OSForensics free version limits to 3 cases at a time the amount of cases being managed, and the files can be restored only one at a time. It is available only for personal, educational or home use only; therefore it adds a watermark on web captures.

## RegRipper

RegRipper is an open source tool, written in Perl, for extracting the registry for later analysis. RegRipper comprises two basic tools, that both of them provide similar capability.

The RegRipper GUI allows the selection of a hive to parse, an output file for the results, and a profile to run against the hive. When the tool is launched, it runs either a list of plugins or an individual plugin against the hive, with the results being sent to a previously specified file. RegRipper doesn't log its activity

## Registry Viewer

Registry Viewer is Windows application that allows viewing the contents of Windows operating system registries. Unlike the Windows Registry Editor, which can only display the current computer's registry, Registry Viewer can view registry files from any computer. Furthermore, it allows access to the registry's protected storage which may contain passwords, usernames, and other information that is not accessible in Windows Registry Editor.

- ✓ The Full Registry view presents all the contents of a registry file, while the Common Areas view displays sections of the registry that are most likely to contain significant data.
- ✓ The Report view displays the selected keys and prints only the relevant information.
- ✓ All of the views also contain two detail panes: a Key Properties viewer and a hexadecimal viewer.

## Registry Browser

Registry Browser is a free forensic software application designed which aims to examine the Windows Registry..

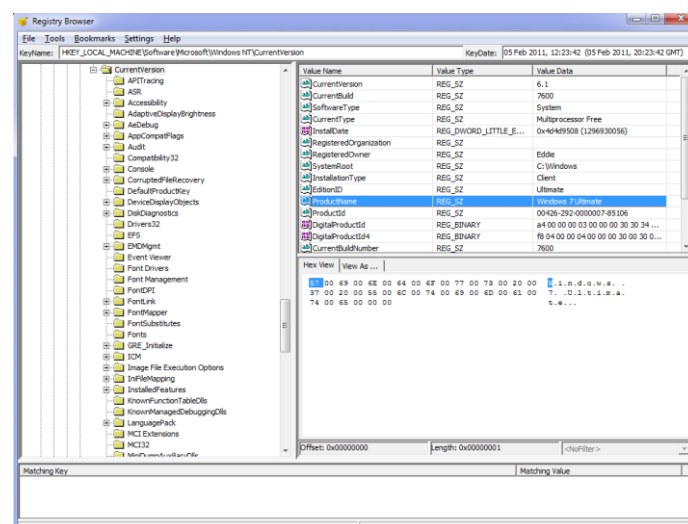


Figure 23 Registry Browser

Registry Browser opens the individual hives files which reside on disk and then re-assembles their contents into a complete Windows Registry. Additionally, it provides several modules to delve deeper into key areas of the registry where necessary.

Registry Browser is available for Windows, Mac OSX and, by request for Linux.

### *Grok-NTFS*

*Grok-NTFS* is a commercial NTFS file system analysis tool with data visualization. It supports all types of forensic images as well as dd images and VMWare disk images. Furthermore, it can look directly at physical disks and RAID arrays. Some of its features are:

- ✓ Displays information without clutter such as volume information and top-level file system information
- ✓ Allows navigation to any location in the file system.
- ✓ Shows all the metadata related to any selected object, whether it is a file, deleted file, directory, deleted directory or orphaned item.

### *SmartMount*

SmartMount is a commercial image mounting and virtualization engine. It is a utility that allows to mount filesystems contained in logical and physical disk image files. It automatically detects the partitions and filesystems within images.

Filesystems mounted in SmartMount behave just like regular volumes. They are assigned a drive letter in Windows and a filesystem mountpoint in Linux. It contains tool that index, search, recover, carve, repair or examine images and filesystems. Some of its features are:

- ✓ Mounts EnCase, VMWare disk, FTK, SMART or dd files locally or over the network.
- ✓ Converts EnCase and .vmdk files to “flat” image files
- ✓ Mounts password protected EnCase files without the password
- ✓ Mounts file systems from within dd images or Macintosh .dmg images
- ✓ Mounts file systems from within FTK images

### *Summation*

Summation is a web based platform for e-discovery that combines native and image ingestion, data processing, early case assessment, case organizer, transcript management and final review.

Summation covers the post data collection stages of the e-discovery process as well as transcript and case management functionality.

Summation included the following features:

- ✓ Data processing, ECA, and final review
- ✓ Case Organizer
- ✓ Advanced visualization graphics of case data relationships and custodian communication patterns
- ✓ Email threading, deduplication, and near duplicate analysis
- ✓ Imports and exports load files for multiple review platforms
- ✓ Offline mobile case review
- ✓ Transcript support with Realtime
- ✓ Concordance migration wizard
- ✓ Near native document viewer with word boundary redaction capability and multiple color selection
- ✓ Case data filtering
- ✓ Process many data types while maintaining chain-of-custody
- ✓ Interoperability with AccessData's FTK and MPE+

### *Evidence Center*

Belkasoft Evidence Center is a commercial tool for searching, analyzing, storing and share digital evidence found inside computer and mobile devices. The toolkit will quickly extract digital evidence from multiple sources by analyzing hard drives, drive images, memory dumps, iOS, Blackberry and Android backups, UFED, JTAG and chip-off dumps. Some of its features are the following

- ✓ Mobile and Computer device examination.
- ✓ Smart and Comprehensive Analysis.
- ✓ File Carving.
- ✓ SQLite Parsing.
- ✓ Live RAM Analysis.

### *Binwalk*

Binwalk is opens source tool for analyzing and extracting firmware images. It searches a given binary image for embedded files and executable code. Specifically, it attempts to identify files and code embedded inside of firmware images. It uses the libmagic library therefore it is compatible with magic signatures created for the Unix file utility. Additionally, it includes a custom magic signature file which contains improved signatures for files that are commonly found in firmware images such as compressed or archived files, firmware headers, Linux kernels, bootloaders, and filesystems.

### *Hex Editor Neo*

The Hex Editor Neo is a free binary code data editing software utility for Windows. It can edit large files such as ASCII, hex, decimal, float, double and binary data. It allows viewing, modifying and analyzing hexadecimal data and binary files, editing



exchange data with other applications through the clipboard, inserting new data and deleting existing data. It is able to manipulate EXE, DLL, DAT, AVI, MP3, JPG files.

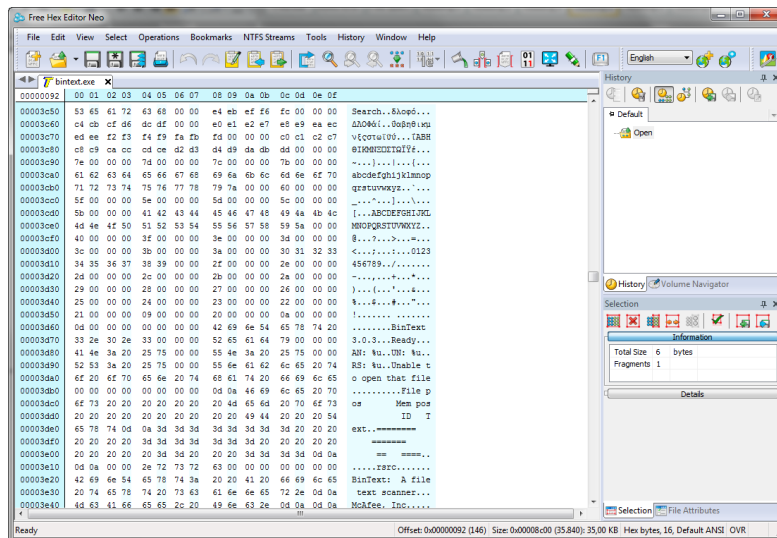


Figure 24 Hex Editor Neo

The Hex Editor Neo's basic functionality are unlimited undo/redo, find, replace, visual history save and load, patch creation, clipboard operations, bytes, words, double words, quad words, floats and doubles edit mode.

### *iBored*

iBored is a free hex editor for disk sectors, but can also be used to edit files, including disk images. It runs on Mac OS X, Windows and Linux. Some of its features are:

- ✓ Can view disks in custom block sizes even if with read errors: It can copy a partially damaged disk to an image file and will turn bad blocks to zero.
- ✓ When modifying data, a "journal" file is written to the desktop that contains the previous data of the altered blocks, and it can be used to undo the changes.
- ✓ Can view partitions and other subranges as containers with their own start, length and block size.
- ✓ Detects connected iPods, showing their firmware partition contents.
- ✓ Can access disks remotely over a network connection.
- ✓ Can save a range of blocks to a file and write a file back to disk.
- ✓ Has a powerful template system to view and analyze disk structures.
- ✓ Can edit MBR and GPT partition tables.
- ✓ Can install a PC BIOS bootloader dealing with both MBR and GPT.

### *Log Parser*

The Log Parser is free query software which searches through information using SQL queries without storing log data into database.

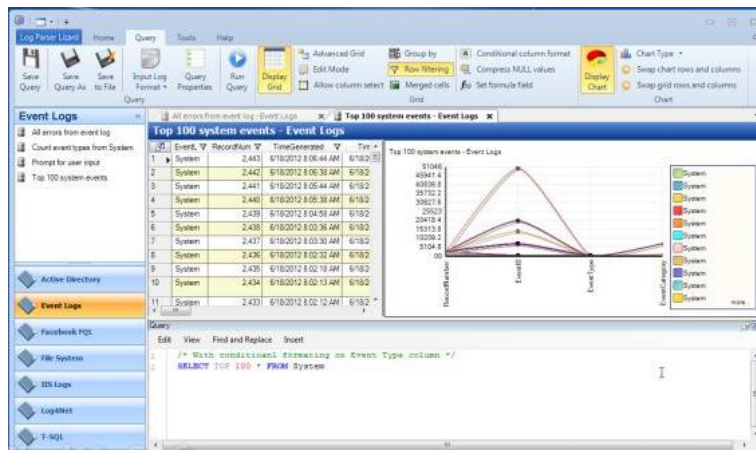


Figure 25 Log Parser

The Log Parser provides universal query access to text-based data such as:

- ✓ Supports log files, XML files, and CSV files, as well as, key data search in Event Log, the Registry, the filesystem, and active directory,
- ✓ Exports results to Excel, charts, dashboards,
- ✓ Contains input filters for custom RegEx and log4net input log formats and Android logs,
- ✓ Creates and manages queries for Microsoft SQL Server, OLEDB queries, Facebook Query Language (FQL),
- ✓ Analyzes big data in the cloud using Google BigQuery services.

### *InfinaDyne CD/DVD Inspector*

InfinaDyne CD/DVD Inspector is commercial software for analysis and extraction of data from optical discs and all types of DVD media. It can read all major CD and DVD filesystem formats and if a disk contains multiple filesystems, they are all found are displayed. Some of its features are:

- ✓ Reports can be produced for print, HTML, text file or CSV output
- ✓ Automatically collect all content from every disc and create reports for each disc processed. Then, the results can be directly imported into EnCase or FTK.
- ✓ Can create an image file containing all of the information required to completely process any disc
- ✓ Captures all files, even those that are deleted or damaged.
- ✓ One-step image collection from otherwise inaccessible CD or DVD discs.
- ✓ Use of "hard links" minimizes size of the image file while retaining complete content of the disc.
- ✓ Files can be searched using scan specification syntax, including regular expressions.
- ✓ Has a built-in image viewer
- ✓ Allows direct examination of the contents of files on the disc

### *Exiftool*

Exiftool is an open source tool for reading, writing, and manipulating image, audio, and video metadata. It can extract EXIF data from a huge list of file types. It is a platform-independent Perl library plus a command-line application for reading, writing and editing meta information in a wide variety of files.

It supports many different metadata formats including EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, ICC Profile, Photoshop IRB, FlashPix, AFCP and ID3, as well as the maker notes of many digital cameras.

Its features are:

- ✓ Supports a large number of different file formats
- ✓ Reads and writes many formats including EXIF, GPS, IPTC, XMP, JFIF, MakerNotes, GeoTIFF, ICC Profile, Photoshop IRB, FlashPix, AFCP and ID3.
- ✓ Reads and writes maker notes of many digital cameras
- ✓ Decodes a riddle wrapped in a mystery inside an enigma
- ✓ Geotags images from GPS track log files
- ✓ Generates track logs from geotagged images
- ✓ Shifts date/time values to fix timestamps in images
- ✓ Renames files and organizes in directories
- ✓ Extracts thumbnail images, preview images, and large JPEG images from RAW files
- ✓ Copies meta information between files
- ✓ Reads and writes structured XMP information
- ✓ Deletes meta information individually, in groups, or altogether
- ✓ Sets the file modification date from EXIF information
- ✓ Processes entire directory trees
- ✓ Creates text output file for each image file
- ✓ Creates binary-format metadata-only files for metadata backup
- ✓ Conditionally processes files based on value of any meta information
- ✓ Ability to add custom user-defined tags
- ✓ HTML-based hex dump outputs

The tool is also available as a stand-alone Windows executable and a Macintosh OS X package.

### *Dumpzilla*

Dumpzilla is a free application is developed in Python for extracting all forensic interesting information from Firefox, Iceweasel and Seamonkey browsers for later analysis. It is supported in Unix and Windows systems. Dumpzilla works in command line interface, so information dumps should be redirected by pipes with tools such as grep, awk, and cut.

This tool enables to visualize following sections, search customization and extract certain content.

- ✓ Cookies and DOM Storage .
- ✓ User preferences like domain permissions and proxy settings.
- ✓ Downloads, web forms like searches, emails and comments.
- ✓ Historial, bookmarks.
- ✓ Cache HTML5 visualization and extraction.
- ✓ Addons or extensions and used paths or urls.
- ✓ Browser saved passwords.
- ✓ SSL Certificates added as an exception.
- ✓ Session data.

Dumpzilla will show SHA256 hash of each file to extract the information and finally a summary with totals.

### *Findwild*

Findwild is an open source GUI wildcard file search application for linux. It is a file search utility allowing extensive wildcard selection, has exclusion criteria which comes with a GUI interface and can recall past searches.

The following search criteria are available:

- ✓ Directory path to search, with multiple wildcards placed anywhere
- ✓ File names to search for, with multiple wildcards anywhere
- ✓ File content strings to search for or exclude, with multiple wildcards anywhere
- ✓ File creation or modification date within a desired range
- ✓ Search the list of files produced by the previous search
- ✓ Search criteria can be saved and recalled.

### *X-Ways Forensics and WinHex*

WinHex is a commercial application for Windows. It is essentially a universal hexadecimal editor, used in computer forensics, data recovery, low-level data processing, and IT security. It can inspect and edit any type of file, recover deleted files or lost data from hard drives with corrupt file systems or from digital camera cards. Some of its features are:

- ✓ Disk editor for hard disks, floppy disks, CD-ROM and DVD, ZIP, Smart Media and Compact Flash
- ✓ Support for all FAT, exFAT, NTFS, Ext2/3/4, Next3, CDFS and UDF
- ✓ Built-in interpretation of RAID systems and dynamic disks

- ✓ RAM editor, providing access to physical RAM and other processes' virtual memory
- ✓ Data interpreter
- ✓ Editing data structures using templates
- ✓ Concatenating and splitting files, unifying and dividing odd and even bytes or words
- ✓ Analyzing and comparing files
- ✓ Search and replace functions
- ✓ Disk cloning, drive images and backups
- ✓ Programming interface and scripting
- ✓ 256-bit AES encryption, checksums, CRC32, hashes
- ✓ Erase confidential files securely, hard drive cleansing
- ✓ Import all clipboard formats, including ASCII hex values
- ✓ Convert between binary, hex ASCII, Intel Hex, and Motorola
- ✓ Character sets: ANSI ASCII, IBM ASCII, EBCDIC, (Unicode)

WinHex and X-Ways Forensics share the same code base. X-Ways Forensics offers several additional forensic features over WinHex, but doesn't allow to edit disk sectors or interpreted images and lacks various functions to wipe data known from WinHex.

X-Ways Forensics, opens only in read-only mode all disks, interpreted image files, virtual memory, and physical RAM, in order to enforce forensic procedures, where no evidence must be altered in the slightest. This strict write protection ensures that no original evidence can possibly be altered accidentally.

Some additional features of X-Ways Forensics are the following:

- ✓ Ability to read and write .e01 evidence files, optionally with real encryption
- ✓ Ability to create skeleton images, cleansed images, and snippet images
- ✓ Ability to copy relevant files to evidence file containers, where they retain almost all their original file system metadata
- ✓ Complete case management.
- ✓ Ability to tag files and add notable files to the case report. Ability to enter comments about files for inclusion in the report or for filtering.
- ✓ Support for multiple examiners in cases, users may work with the same case at different times or at the same time and keep their results separate, or not.
- ✓ Automated activity logging
- ✓ Write protection to ensure data authenticity
- ✓ Remote analysis capability for drives in network
- ✓ Memory analysis for local RAM or memory dumps of Windows.

- ✓ Compensation for NTFS compression effects and Ext2/Ext3 block allocation logic in file carving
- ✓ Carving of files also within other files
- ✓ FuzZyDoc hashing to identify known textual. PhotoDNA hashing to identify known photos
- ✓ Create personal hash sets or import hash sets
- ✓ Computation of two hash values of different types at the same time
- ✓ Ability to print the same file types directly from within the program with all metadata on a cover page
- ✓ Internal viewer for Windows Registry files
- ✓ Extracts metadata and internal creation timestamps from various file types and allows filtering accordingly.

X-Ways runs under Windows XP/2003/Vista/2008/7/8/8.1/2012, 32 Bit/64 Bit, standard/PE/FE.

### *X-Ways Investigator*

X-Ways Investigator is a Windows application for investigating, documenting, analyzing and reporting evidences and covers the analysis part of computer forensics and electronic discovery. It is based on X-Ways Forensics. Some of its features are the following:

- ✓ File viewer, case management, logging, and automated reports
- ✓ Can read media/images from most file systems and can interpret raw image files and .e01 evidence files
- ✓ Ability to run keyword searches, both conventional and index searches
- ✓ Search hit listings with context preview,
- ✓ Gallery view for pictures, Calendar view for timestamps
- ✓ Ability to tag files and add them to customized report tables of notable items
- ✓ Directory tree on the left, ability to explore and tag directories including all their subdirectories
- ✓ View of all existing and deleted files in all subdirectories
- ✓ Skin color detection

### *X-Ways F-Response*

F-Response in combination with X-Ways Forensics examines media that are attached to remote computers, over a network. It provides full access to a storage device on a remote computer. The connection is completely read-only, functioning like a software write blocker and allows access to target computers that are running Linux and Mac OS X.

## Field Agent

MacForensicsLab Field Agent is a commercial tri-platform tool designed specifically to help combat Crimes Against Children. It has the ability to quickly and effectively identify files of interest based on the percentage of skin tone contained within. It supports Windows, Mac OS X, Linux.

MacForensicsLab Field Agent's features are:

- ✓ Performs automated analysis of drive images, network drives, stand alone live computers, DVD's, CD's, and other removable media
- ✓ Extracts digital evidence in minutes
- ✓ Uses pixel-based image analysis technology to identify suspect images based on skin tone values.
- ✓ Identify, isolate, and store images from a suspect's computer on a thumb drive.
- ✓ Images of interest can quickly be exported out to a flash drive or generated into a report containing information about the picture.
- ✓ Skin color detection provides a gallery view sorted by skin tone content to greatly accelerate a search
- ✓ Quick and easy reporting feature and display findings in a universal format

## Nagios Log Server

The Nagios Log Server is a commercial application for searching log data. It allows filtering data for auditing and setting up alerts to notify for potential threats. It allows additional Log Server Instances to current monitoring cluster. The logs can be viewed in real-time, providing the ability to analyze and solve problems as they occur. Moreover, it sends alerts from the web-interface based on queries and thresholds and it notifies users via Nagios XI / Nagios Core, email, SNMP traps, Nagios Reactor Event Chains or executes a script to ensure quick problem resolution.



Figure 26 Nagios Log Server

The Nagios Log Server features are:

- ✓ *Comprehensive Analysis Dashboards*. It provides users with the ability to query, filter, and analyze incoming log events. Dashboards can be customized, saved, and shared with others.
- ✓ *High Availability and Failover*. Log Server uses a cluster of servers to automatically store log data for preventing data loss and ensuring availability of log information.
- ✓ *Alerting*. It creates alerts based on queries with thresholds.
- ✓ *Configuration Wizards*. It allows to easily set up devices to be monitored.
- ✓ *Quick Search and Query*. The data are in one location that helps search with multiple queries and filters, and easy correlation of events on multiple systems.
- ✓ *Extendable Architecture*. Full access to the back-end API allowing customization with in-house and third-party applications.
- ✓ *Real-Time Data*. It allows seeing log data from all of your servers in real time.

#### *Incident Response Collection Report (IRCR)*

The Incident Response Collection Report is an open source script based incident response tool. It calls a collection of tools for collecting and analyzing data on Windows systems. It is essentially take a snapshot of the system and its primary purpose is data collection rather than analysis.

The main idea of IRCR is that anyone could run the tool, with no expertise, and send the output to a professional for further analysis.

#### *Regimented Potential Incident Examination Report (rapier)*

The RAPIER is a free script based incident response tool released under the GPL by Intel. It is a modular framework built to facilitate first response procedures for incident handling. The RAPIER is a Windows based information gathering framework. It was designed to streamline the acquisition of information off of systems in a large scale enterprise.

The RAPIER is a security tool built to facilitate first response procedures for incident handling. It can acquire commonly requested information and samples during an information security event, incident or investigation. The RAPIER automates the entire process of datacollection. Some of its main features are:

- ✓ It limits the amount of 1st Responder decisions by automating where possible,
- ✓ It provides a complete lifecycle for information gathering from start to delivery of data,
- ✓ It tries to gather all data that could be requested by analysts,



- ✓ SHA1 verification checksums,
- ✓ Auto-update functionality,
- ✓ The results can be auto-zipped,
- ✓ Auto-uploaded to central repository,
- ✓ Email Notification when results are received,
- ✓ Two Default Scan Modes,
- ✓ Separated output for faster analysis,
- ✓ Pre or Post run changes report,
- ✓ Configuration File approach,
- ✓ Process priority throttling.

### **AD Lab**

AccessData Lab is a commercial centralized investigative platform for Windows that allows dividing the caseload, collaborative analysis, centralized case management and web-based review. Additionally, AD Lab enables distributed processing, permitting the use of additional hardware to increase case processing and resolution speed. Some of its features include:

- ✓ Distributed processing
- ✓ Job queuing for distributed processing farm
- ✓ Share and centralized database infrastructure
- ✓ FTK investigator collaborator
- ✓ Case management
- ✓ Role-based permissions to control access and activity
- ✓ Near native Web review
- ✓ Active directory integration for authentication
- ✓ Load file and responsive data set production
- ✓ eDiscovery de-duplication
- ✓ Custom data views

### ***Windows Forensic Toolchest***

The Windows Forensic Toolchest is designed to provide an organized and repeatable automated live forensic response, incident response, or audit on a Windows system and, in the same time, it collects security information from the system. The WFT produces HTML based reports and it is basically a forensically enhanced batch processing shell which can run other security tools.

It searches for signs of an incident, intrusion or misconfiguration and it produces outputs admissible in court proceedings. It provides thorough logging of all its actions along with computing the MD5/SHA1 checksums along the way to ensure integrity. Some of its features are:

- ✓ Provision of live forensic response, incident response, or audit,

- ✓ Generation of both raw text and html reports,
- ✓ User editable config file controls execution,
- ✓ Ability to run locally, via cd/dvd, or thumb drive,
- ✓ Configurable toolpath,
- ✓ Macros which expand dynamically based on run time values,
- ✓ Detailed run time logging,
- ✓ Verification of all executed tools,
- ✓ Detailed hashing of output,
- ✓ Support for md5 hash, sha1 hash
- ✓ Ability to verify wft config files,
- ✓ Automatic updating of wft hash values for tools,
- ✓ Offline report generation,
- ✓ Ability to run sysinternals tools without '-accepteula',
- ✓ Color output highlights important info,
- ✓ Automatic OS and drive detection,

### *Nagios Incident Manager*

The Nagios Incident Manager is a web-based application that allows teams and individuals to track and resolve problems. It offers security, mobility, third-party integration, and tools for collaboration, for managing infrastructure incidents and for facilitating faster problem resolution across the IT infrastructure of an organization.

The Nagios Incident Manager allows support teams to track their performance, eventually resulting in greater efficiency and less downtime. With statistics such as mean time to resolution and first response time, the Incident Manager gives to the admins and users the ability to create a goal-oriented response system, focused on incident resolution turn-over and increased overall team performance. The control of incoming tickets can be assigned to different users and teams. Multiple teams can be managed and each team and individual can manage their own tickets based on priority and status or categorize them based on user, team, or incident type.

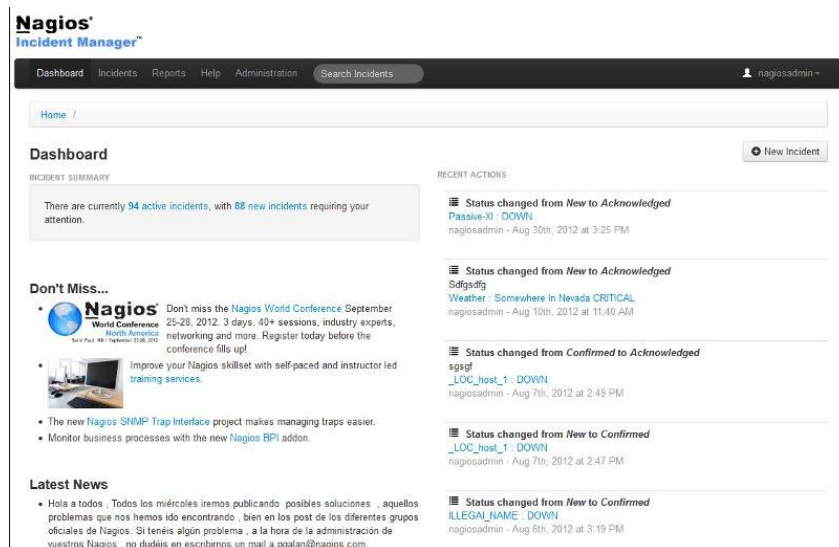


Figure 27 Nagios Incident Manager

The Nagios's Incident Manager features are:

- ✓ The dashboard provides an overview of incidents related to the network.
- ✓ Statistics on incident resolution time with Mean Time To Resolution and first response time report to allow evaluation support.
- ✓ Customizable with in-house and third-party programs and applications for quick access to network incident information and for adapting to current organizational structure with minimal implementation impact.
- ✓ It provides the ability to sort, acknowledge, and organize incidents to better understand the situation and properly assess whether incidents are being handled in a timely manner.
- ✓ It creates custom incidents and assigns users or teams to them, chooses the type, title, priority, and status to track incident progress, and connects, prioritizes, and collaborates to resolve incidents quickly in the IT environment.
- ✓ It creates users and teams to help segment the work, manages the entire support staff and quickly resolves incidents.

### Google Maps Tile Investigator

Google Maps Tile Investigator is a free windows tool that allows users to download the coordinates found in the tile filenames as well as surrounding tiles and will convert them to their corresponding longitude, latitude coordinates, to show more context around an individual tile. The coordinates can either be manually entered or found in filenames that match the Google Maps tile filename format.

## GRR Rapid Response

GRR Rapid Response is open source incident response framework for performing forensic tasks remotely. It is a multi-platform tool for enterprise forensic investigations which enables remote raw disk and memory access.

GRR can extend to many thousands of machines, be managed collaboratively via a web interface, and support all major platforms. It can remotely perform live forensics, by tackling, auditing, privacy issues and provides a set of features for forensic analysis.

The GRR's extensibility the approach a "continuous forensic analysis" model rather than the traditional "one system at a time" approach. All assets can simultaneously be automatically analyzed.

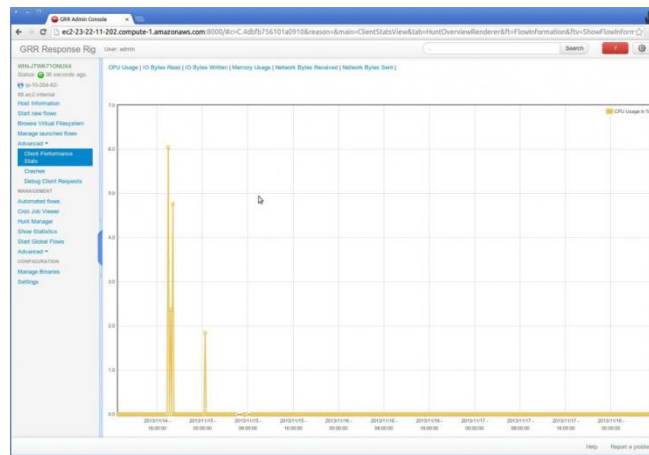


Figure 28 GRR Rapid Response

The GRR consists of a client agent that can be deployed to a target system, and server infrastructure that can manage and talk to the agent.

The client features are:

- ✓ Live remote memory analysis using open source memory drivers for Linux, Mac OS X and Windows, and the Rekal memory analysis framework.
- ✓ Search and download capabilities for files and the Windows registry.
- ✓ Secure communication infrastructure designed for Internet deployment.
- ✓ Client automatic update support.
- ✓ Detailed monitoring of client CPU, memory, IO usage and self-imposed limits.

The server features are:

- ✓ Fully fledged response capabilities handling most incident response and forensics tasks.
- ✓ OS-level and raw file system access, using the SleuthKit (TSK).

- ✓ Enterprise hunting support.
- ✓ Automated scheduling for recurring tasks.
- ✓ Fast and simple collection of hundreds of digital forensic artifacts.
- ✓ Asynchronous design allows future task scheduling for clients, designed to work with a large fleet of laptops.
- ✓ Ajax Web UI.
- ✓ Fully scriptable IPython console access.
- ✓ Basic system timelining features.
- ✓ Basic reporting infrastructure.

Cross-platform support for Linux, Mac OS X and Windows clients.

### *MacLockPick*

MacLockPick is a commercial forensics triage tool designed for first responders performing live forensic triage on most computer systems. It is provided on a USB Flash drive that once inserted into a computer that is running or sleeping, it will extract the necessary data that may otherwise be unreadable due to modern encryption programs, hardware malfunctions, or powering the system down. MacLockPick 3.0 provides results that can be accepted in a court of law. It runs and can acquire from Microsoft Windows, Mac OS X or Linux,

MacLockPick 3.0 uses a plugin architecture so that the investigator can have control over which processes are run in the field

- ✓ Built-in Plugins that gather data from the suspect's system and deliver that information to the logs.
- ✓ Copy Files or Folders - logical acquisition with hashing in MD5, SHA1, and SHA256. Target data can be specified with filters.
- ✓ Terminal Commands MacLockPick can be configured to transparently open a shell environment, execute specified command, and then record the output to the logs.
- ✓ External Commands, allows the investigator to configure execution of third party command-line tools programs.

Furthermore, MacLockPick has the following features:

- ✓ Gather information stored by the Apple iPhone and other devices using the Apple Mobile Sync system on Windows and Mac OS X computers
- ✓ Capture any text contents or graphics found in the clipboard and store it in the logs. Any graphics will be converted to jpeg form and saved to the output log folder.

- ✓ Creates a summary of the online activity by collecting information from browsers (Firefox, Internet Explorer and Apple Safari). The information includes bookmarks, history, cookies and downloads
- ✓ An analysis of the network activity on the suspect's computer.
- ✓ Use the OS to list all active applications running on the suspect's computer at the time of analysis.
- ✓ Capture and save a screen shot of the main screen on the suspect's system.
- ✓ Create transcripts of communications the suspect has made using Skype.
- ✓ Create a profile of the hardware in use by the suspect.
- ✓ USB Flash Drive History.
- ✓ Extract all settings from the registry on Microsoft Windows systems.

### *Encrypted Disk Detector*

Encrypted Disk Detector (EDD) is a free command-line tool for Windows that checks the local physical drives on a system for encrypted volumes. If no disk encryption signatures are found, it also displays the OEM ID and, where applicable, the Volume Label for partitions on that drive, checking for Bitlocker volumes. Thus help to determine if further investigate is needed and whether a live acquisition needs to be made in order to secure and preserve the evidence that would otherwise be lost.

### *Vinetto*

Vinetto is an open source forensics tool to examine Thumbs.db files. It is a command line python script that works on Linux, Mac OS X and Cygwin.

Vinetto extracts the thumbnails and associated metadata from the Thumbs.db files. Moreover it runs according to three following modes:

- ✓ In elementary mode it extracts thumbnails and metadata from a chosen Thumbs.db file.
- ✓ In directory mode it checks for consistency between the content of the directory and the related Thumbs.db file. It will report the thumbnails that are not associated to a file into the directory.
- ✓ In filesystem it will process the whole FAT or NTFS partition.

### *Email Examiner and Network Email Examiner*

Email Examiner is a commercial tool that performs deep analysis, deleted email recovery, email conversion, and more for PST, OST, Thunderbird, Gmail Mbox, AOL, Eudora, Maildir, and MIME formats. It can analyze email attachments, recover deleted email from outlook, thunderbird, eudora, and the bat and produces full reports. Network Email Examiner is for email analysis over the network.

### *pdfid*

pdfid is a free Linux tool that will scan a file to look for certain PDF keywords, in order to identify PDF documents that will execute an action when opened. PDFiD will also handle name obfuscation.

### *pdf-parser*

pdf-parser is a Linux open source tool that will parse a PDF document to identify the fundamental elements used in the analyzed file.

### *pdgmail*

pdgmail is a Python script to gather gmail artifacts from a pd process memory dump. It'll find what it can out of the memory image including contacts, emails, last access times and IP addresses.

### *peepdf*

peepdf is a Python tool to explore PDF files in order to find out if the file can be harmful or not. Through this tool it's possible to see all the objects in the document thus detect the suspicious elements. It supports the most used filters and encodings, it can parse different versions of a file, object streams and encrypted files. It provides Javascript and shellcode analysis wrappers too. Additionally, it can create new PDF files, modify existent ones and obfuscate them.

### *P2C*

P2C is a commercial digital forensic software for complete computer investigations to targeted email, internet, data triage, or even gaming system analysis. It can analyze digital evidence, email, network email archives, internet history, chat logs, registry data, Xbox data and smartphone data. It is multi-threaded and has a built in database that doesn't require a separate install or hard drive to run.

## **7.1.3. Memory Acquisition**

### *Goldfish*

Goldfish is an open source set of linux utilities. It performs acquisition of Apple Mac RAM content over FireWire connection. It can extract login password and any open AIM conversation fragments. Goldfish software can be used against 32 bit versions of Mac OS X up to and including Mac OS X (

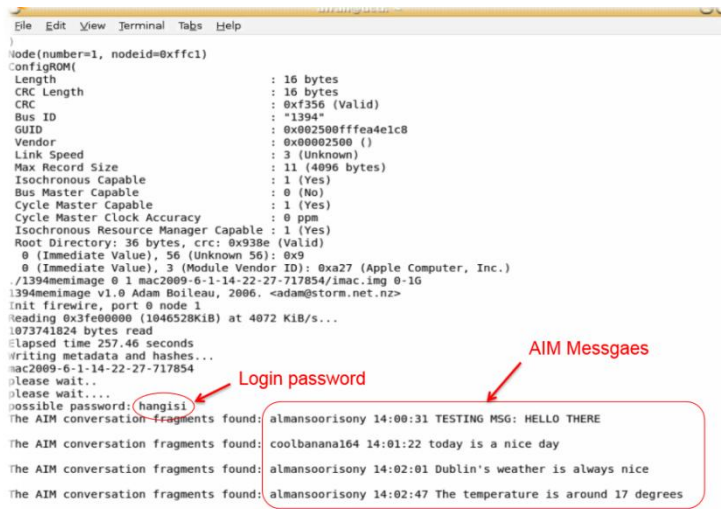


Figure 29 Goldfish

### Magnet RAM Capture

Magnet RAM Capture is a free imaging tool for windows for capturing a computer's physical memory. Thus it recovers and analyzes artifacts that are often only found in memory. It has a small memory footprint, and captured memory data is exported in DMP format. It allows to discover process and programs running on the system, network connections, evidence of malware intrusion, registry hives, username and passwords, decrypted files and keys, and evidence of activity not typically stored on the local hard disk.

### Live RAM Capturer

The Belkasoft Live RAM Capturer is a small free forensic tool that allows extracting of a computer's volatile memory, even though it may be protected by an active anti-debugging or anti-dumping system. There are both 32-bit and 64-bit builds implementations for the purpose of reducing to the minimum the tool's footprint.

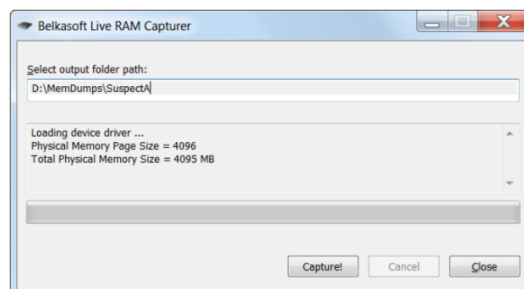


Figure 30 Belkasoft Live RAM

The Belkasoft Live RAM Capturer has the smallest footprint possible. No installation is required, therefore it can be run from a USB flash drive. It is set with both 32-bit and 64-bit kernel drivers, allowing the tool to operate in the most privileged kernel mode.



The Belkasoft Live RAM Capturer is compatible with 32-bit and 64-bit editions of Windows.

### *MoonSols Windows Memory Toolkit*

The MoonSols Windows Memory Toolkit is a commercial toolkit for performing memory acquisition or conversion during an incident response, or a forensic analysis for Windows desktops, servers or virtualized environment.

The MoonSols Windows Memory Toolkit had been designed to deal with Microsoft Windows hibernation file, Microsoft full memory crashdump, and raw memory dump files from memory acquisition tools like DumpIt or virtualization application like VMWare. Moreover, it also contains new version of DumpIt.

The MoonSols Windows Memory Toolkit features are:

- ✓ It converts any Windows memory dump file in a Microsoft crash dump file,
- ✓ It decompresses complex memory hibernation files,
- ✓ It works on every Microsoft Windows version,
- ✓ It contains DumpIt, an improved version of win32dd and win64dd, for live acquisition on a local disk file or to a remote target, which can be used from the external paths and can be called from scripts,
- ✓ It contains hibr2dmp and bin2dmp to create a synergetic ecosystem within all the different file formats used by memory snapshots files such as Windows hibernation file and Microsoft crash memory dumps analysable by Microsoft WinDbg.

### *Linux Memory Grabber*

Linux Memory Grabber is a Linux command tool which creates Linux Volatility profiles and dump memory, using LiME, from an USB Key, with no installation on local HDD required.

## **7.1.4. Memory Analysis**

### *Volatility*

The Volatility is an open source memory forensics framework for incident response and malware analysis. It provides a platform to analyze and extract objects from images such as raw dumps, crash dumps, VMware dumps (.vmem) and virtual box dumps. The Volatility doesn't acquire memory from target systems. It can extract information about running processes, open network sockets and network connections, DLLs loaded for each process, cached registry hives, process IDs, and

more. It uses address space voting rounds to automatically identify the file format. Moreover, it provides several plugins for exploring the metadata associated with many of the common file formats such as Crash dump, Hibernation file, HPAK, Mach-o, VMware and VirtualBox.

The Volatility automates the extraction and visualization of digital objects found in physical memory. It enables the extraction, analysis, aggregation, and visualization of forensic data at various levels of abstraction and data complexity. The framework also includes tools to automate the development of forensic profiles for applications, from web browsers to the operating system kernel. Currently, it includes modules for virtual address space reconstruction, virtual to physical address translation, and visualization. The framework employs a number of visualization and data mining techniques to improve analysis and to facilitate searching through large amounts of data.

It is written in Python and it supports 32- and 64-bit windows, Linux, Mac, and Android systems.

### *Rekall*

Rekall is a free memory analysis framework for incident responders and forensic analysts. It is an open collection of tools, implemented in Python for the extraction and analysis of digital evidence from volatile memory. The extraction process doesn't interfere with the system being investigated but offer visibility into the runtime state of the system. Its design philosophy is to exact symbol information for the analyzed system and store profiles in a public profile repository directly accessible at runtime.

Rekall has three user interfaces, the *command line*, the *interactive console* and the *Webconsole*. The same plugin works in all environments.

Rekall's export system is customizable. The default is the *text renderer*, the *Data Export renderer* produces rich JSON and the *XLS renderer* produces Excel sheets.

Rekall Framework can run on any platform that supports Python. It supports investigations of 32bit and 64bit memory images for Windows, Linux Kernels, and Mac OS X. Moreover, Rekall has an implemented GUI for writing reports, and driving analysis

- ✓ Is designed to run on the same platform it is analyzing
- ✓ In the *aff4acquire* plugin, Rekall supports the acquisition of the pagefile and all relevant mapped files.
- ✓ Support for customized output formats.

- ✓ The Worksheet GUI allows the analyst to create a report, merging marked up text, images, embedded files, shell and python code snippets as well as the output of Rekall plugins in the same document.
- ✓ Uses symbols obtained from operating system vendors' debugging information directly. Therefore, it is able to know the position of critical operating system constants.
- ✓ Supports writing plugins

### RAMMap

RAMMap is a free windows application that analyzes physical memory usage and gives insight on how Windows manages memory and allows to analyze the memory usage of application or to answer specific questions about how RAM is being allocated. Additionally it can take memory snapshots and store them for later analysis.

It can be installed on client Windows Vista and higher and on server Windows Server 2008 and higher.

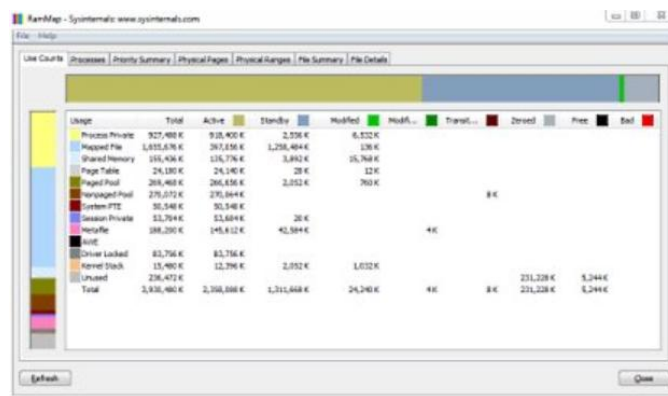


Figure 31 RAMMap

### Second Look

Second Look is commercial memory forensics product for performing Linux threat detection. It enables visibility into the state of systems software while executing in memory on Linux systems, performs malware detection, allows the integration of memory forensics into enterprise security information and event management systems, and confirms the integrity of a remote system's kernel and the integrity of the executable in all processes without doing a complete memory dump. Furthermore, it can be configured to automatically scan of remote systems throughout an enterprise and includes a wide set of reference software.

Second Look has to edition, the Professional edition which can perform memory acquisition and analysis and the Enterprise edition which is an extended version of the Professional and provides for memory forensics of remote systems over the

network without full memory acquisition, capability for automated scanning, and SIEM integration.

The features of Second Look Professional and Enterprise Edition are:

- ✓ Memory acquisition and analysis
- ✓ Analysis via command line interface (CLI) or graphical user interface (GUI) applications
- ✓ Automatic kernel version identification.
- ✓ Supports raw physical memory images, SLM memory images, LiME memory images, VMware virtual machine snapshot and suspend files, VirtualBox snapshots and Libvirt/KVM snapshots.
- ✓ Supports analysis of memory images from systems running either distribution stock kernels or custom kernels.
- ✓ Has access to a repository of Zipped Reference Kernels providing the metadata and baseline for analysis and verification of Amazon, CentOS, Debian, Fedora, Oracle, RHEL, and Ubuntu stock kernels.
- ✓ Integrity verification of the kernel and processes in memory.
- ✓ Detection of kernel rootkits, backdoors, and other kernel-mode malware
- ✓ Detection of shared library rootkits, keyloggers, spyware, injected libraries, injected threads, and other user-mode malware.
- ✓ Detection of unknown or unauthorized processes.
- ✓ Recovery of device mapper crypto keys for LUKS, TrueCrypt, and other full disk encryption schemes.
- ✓ Extraction of system state from captured memory images, including loaded kernel modules, running processes, memory mappings, open files and active network connections.

In addition, the Enterprise edition has the following features:

- ✓ Memory acquisition from remote systems, and live remote memory analysis, via the Second Look agent.
- ✓ Verify the integrity of a remote system's kernel and the integrity of the executable code in all processes, without doing a complete memory dump.
- ✓ An engine for automated scans of remote systems throughout an enterprise, with automated alerting.
- ✓ Integration of alerts with any SIEM via syslog or JSON data.
- ✓ Support for the SLM high-performance compressed memory image format.

### *WindowsSCOPE Cyber Forensics*

The WindowsSCOPE Cyber Forensics is a commercial memory forensic capture and analysis toolkit. It allows the import of WinDD memory dumps which are then automatically reverse engineered and presented for forensic analysis.

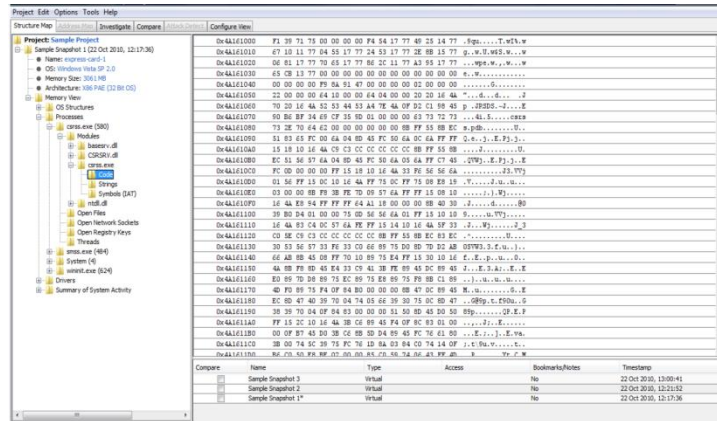


Figure 32 WindowsSCOPE

The WindowsSCOPE's features are:

- ✓ It provides full capabilities for analyzing the Windows kernel and software applications, drivers, and DLLs as well as user activity,
- ✓ It can generate virtual and physical memory snapshots and then compare, annotate, and analyze them,
- ✓ The system includes disassembling, annotations, and program graphing capabilities,
- ✓ It comes with WinDD compatible fetching mechanism and import capabilities,
- ✓ Compatible with optional CaptureGUARD hardware-based physical memory acquisition and Phantom Probe USB dongle memory fetching mechanism.

The WindowsSCOPE Cyber Forensics supports Windows XP, Windows Vista, Windows 7, and Windows 8/8.1 WinDD compatible memory dumps.

## 7.1.5. Data Recovery

### Foremost

Foremost is a Linux file carving program for recovering files based on their headers, footers, and internal data structures. It uses only command line and has no graphical interface. It can investigate image files or directly on a drive. The headers and footers can be specified by a configuration file or by using command line switches to specify built-in file types.

Foremost ignores the type of underlying filesystem and directly reads and copies pieces of the drive into the computer's memory. It takes these pieces one segment at a time, and by applying file carving searches this memory for a file header type that matches the ones found in Foremost's configuration file. When a match is found, it

writes that header and the data following it into a file, stopping when either a footer is found, or until the file size limit is reached.

### *Forensic Emule Analyzer*

Emule Analyzer is an open source tool for Linux that parses unallocated clusters of EnCase Image Files (\*.e01) mounted with Access Data's FTK Imager for deleted known.met records. EmuleAnalyzer searches and parses active known.met files recursively too. It analyzes the internal structure of files and so it works with corrupted files or partial files which crash most of the other known.met parser. Results can be searched for keywords.

### *Ddrescue*

The GNU *ddrescue* is a data recovery tool. It copies data from one file or device to another and, in case of read errors, it attempts first to rescue the good parts.

The *Ddrescuelog* is a tool that manipulates *ddrescue* mapfiles. It shows mapfile contents, converts mapfiles to other formats, compares mapfiles, tests rescue status, and it can delete a mapfile, if the rescue is done. The *Ddrescuelog* operations can be restricted to one or several parts of the mapfile, if the domain setting options are used.

The *Ddrescue* doesn't write zeros, when it finds bad, and it doesn't truncate the output file, if not asked to. So, every time it runs on the same output file, it tries to fill in the gaps without wiping out the data already rescued.

### *extundelete*

*Extundelete* is an open source utility for the recovering of deleted files from an ext3 or ext4 partition. When attempting recovering of a file that has been deleted from the partition, it uses information stored in the partition's journal. It searches the file system's journal for an old copy of an inode for information to determine the file's location within the file system. Then it reads the corresponding data and copies it to a file in the recovery directory. Some features are:

### *ReclaiMe File Recovery*

*ReclaiMe File Recovery* is a free software for data recovery which runs on Windows systems. It can also recover deleted files. Some of its features are:

- ✓ Recover data from a formatted disk
- ✓ Recover deleted files and folders.
- ✓ Recovers data in case of boot failure.
- ✓ Recover media from memory cards used by digital cameras, mobile phones, PDAs.

- ✓ NAS recovery for QNAP, NETGEAR, Synology, WD MyBook, LaCie, and similar devices.
- ✓ Recovers RAW filesystem drive.
- ✓ Recovers files from filesystems used by Windows, Linux, NETGEAR ReadyNAS devices and Mac devices.

ReclaiMe File Recovery recovers data from hard drives, internal or external, memory cards used in cameras, mobile phones, PDAs, MP3 players, USB drives, RAID arrays and multi-disk NAS devices.

### *Distributed Network Attack (DNA) and Password Recovery Toolkit*

PRTK and DNA are commercial Window-based applications and have the same program interface and they work essentially the same way. Both programs analyze file signatures to find encryption types and determine which recovery modules to use.

PRTK and DNA recover passwords for protected files, while creating hash values that can be used to verify whether the content of a file changed during the password recovery.

PRTK and DNA can recover protected files using methods like decryption and dictionary attacks.

For difficult password key values, PRTK performs dictionary attacks using various types of dictionaries, including the golden dictionary, as well as biographical, custom user, and default dictionaries.

PRTK and DNA have following basic functions:

- ✓ *Recover passwords*: PRTK can recover the password to files created in many popular industry applications.
- ✓ *Hash files*: Hashing a file uses an algorithm that creates a unique hash value for a file, allowing verification that the contents of a file remain unchanged.
- ✓ *Open encrypted files*: To recover keys or passwords to open recovered files
- ✓ *Generate reports*: Top print job information reports for password recovery jobs in PDF format.
- ✓ *Utilizing graphics processing units (GPU)*: In order to harness additional processing capabilities to increase

### **7.1.6. Specific Tools**

#### *Catfish*

The Catfish is a GUI adaptable file searching tool which supports popular search engines, such as *locate*, *slocate*, *tracker* or *beagle*. The advanced settings sidebar will

allow the organization of search results by modification date, as well as search by file type. Therefore, it gives the ability to search only images, videos, music, documents or applications.

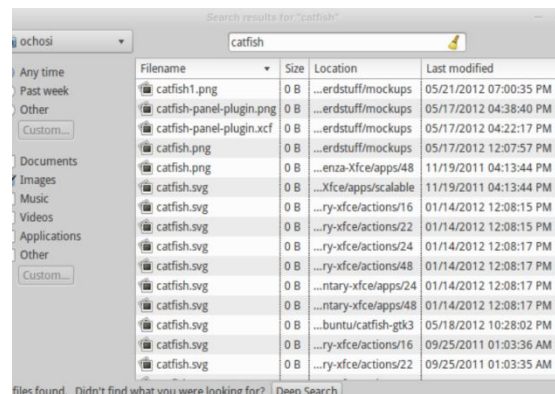


Figure 33 Catfish

### *Md5deep*

Md5deep is a suite of hashing utilities designed to produce hash lists of a set of input files or directories. The output can be configured based on the requirements and includes similar tools implementing not only MD5 as the name suggests but also SHA, tiger and whirlpool. It can be used to generate multiple hashes for files and then audit the set of hashed data. Once having generated a base state, then it can report on matching files, missing files, files that have been moved from one location to another, and files that did not appear in the original set.

*Dhash* – calculates the similarity between images. If two images have a similar dhash, then the likelihood is that they both are depicting the same image.

### *Dropbox Decryptor*

Dropbox Decryptor is a free tool for decrypting the Dropbox filecache.dbx and config.dbx files, which are both encrypted SQLite databases, and then can be viewed with any SQLite browser. These two locations store information about files that have been synced to the cloud using Dropbox. This tool provides access to the host ID, the list of files that have been synced to Dropbox including their metadata, the email address of the Dropbox user, the list of recently changed files, and to the local path to the user's Dropbox folder.

### *ElcomSoft Password Recovery Bundle*

ElcomSoft Password Recovery Bundle is a commercial suite of ElcomSoft password recovery tools allows to remove protection from disks and systems and decrypts files and documents. It can recover document and system passwords to various file formats and allows using a number of multi-core and multi-processor workstations connected over a LAN or the internet with linear increase of recovery speed.



## ProcDump

ProcDump is a command-line utility whose primary purpose is to monitor the CPU consumption of applications and generates crash dumps during a spike. This can be used to determine the cause of the spike. ProcDump also includes:

- ✓ Monitor hung window,
- ✓ Monitor unhandled exception
- ✓ Generate dumps based on the values of system performance counters.
- ✓ Can serve as a general process dump utility that can be embed in other scripts.

## John the Ripper

John the Ripper, is an open source software that performs password cracking and can attach several different hashes. To perform password cracking it needs a password file and optionally specify a cracking mode. It is available for Unix, Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. There are two commercial versions, John the Ripper Pro for Linux and John the Ripper Pro for Mac OS X

## Web Agent

MacForensicsLab Web Agent is a commercial website crawler for hunting child pornography, with a built-in skin tone analyzer to quickly and efficiently identify images of evidentiary value. This program enables investigators to identify, isolate, and store images from a website. It can run on Mac OS X and Linux.

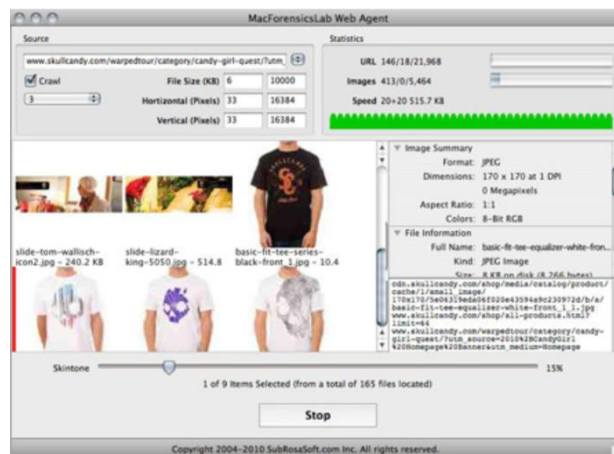


Figure 34 MacForensicsLab

MacForensicsLab Web Agent can download images from suspect websites and then perform automated analysis. It uses pixel-based image analysis technology to identify suspect images based on skin tone values. Furthermore, allows reviewing the results, to output a report containing information about images of interest. It supports a variety of graphic formats and protects valuable digital evidence.

Skin color detection provides a view sorted by skin tone content to accelerate a search and has a quick and easy reporting feature for displaying findings in a universal format. Reports include thumbnails of images of interest, path to the image location, hashing with MD5, SHA1 and SHA256, and more in a customizable HTML format.

### *Mount Image Pro*

Mount Image Pro is a commercial forensics tool for mounting forensic images. It runs on Windows and supports all major image formats including EnCase, AccessData, DD and RAW images, .AFF, ProDiscover, SMART and XWays. It can map images as a single drive letter or map specific drive letters to any or all partitions within the image files. Furthermore, it maintains the MD5 hash integrity and can open EnCase password protected image files without the password.

### *chkrootkit*

chkrootkit is a free Linux command tool to locally check for signs of a rootkit. It contains:

- ✓ chkrootkit: shell script that checks system binaries for rootkit modification.
- ✓ ifpromisc.c: checks if the interface is in promiscuous mode.
- ✓ chklastlog.c: checks for lastlog deletions.
- ✓ chkwtmp.c: checks for wtmp deletions.
- ✓ check\_wtmpx.c: checks for wtmpx deletions. (Solaris only)
- ✓ chkproc.c: checks for signs of LKM trojans.
- ✓ chkdirs.c: checks for signs of LKM trojans.
- ✓ strings.c: quick and dirty strings replacement.

### *Capstone*

Capstone is a free disassembly framework for binary analysis and reversing. Some of its features include:

- ✓ Support multiple hardware architectures: ARM, ARM64, Mips and X86
- ✓ Provide details on disassembled instruction
- ✓ Provide semantics of the disassembled instruction, such as list of implicit registers read and written
- ✓ Implemented in pure C language, with lightweight wrappers for C++, Python, Ruby, OCaml, C#, Java and Go available

Supports Windows, MacOSX, Linux and BSD.

### *Cuckoo*

Cuckoo Sandbox is an open source tool for performing malware analysis. It will execute any suspicious code or file inside an isolated environment and will report

some detailed results outlining of what happened and what the file did when executed.

Cuckoo generates different raw data which include:

- ✓ Native functions and Windows API calls traces
- ✓ Copies of files created and deleted from the filesystem
- ✓ Dump of the memory of the selected process
- ✓ Full memory dump of the analysis machine
- ✓ Screenshots of the desktop during the execution of the malware analysis
- ✓ Network dump generated by the machine used for the analysis.

Cuckoo generates different type of reports, which include JSON report, HTML report, MAEC report, MongoDB interface and HPFeeds interface.

### chntpw

chntpw is a free small program that provides a view to information and change user passwords in user database file of all Windows. In addition it also contains a simple registry editor and an hex-editor.

## 7.2. Network Forensics

### Wireshark

Wireshark is an open source network packet analysis software. Its function is to capture packets moving over a network and to display all details about the containing. It essentially displays all information inside a network cable.

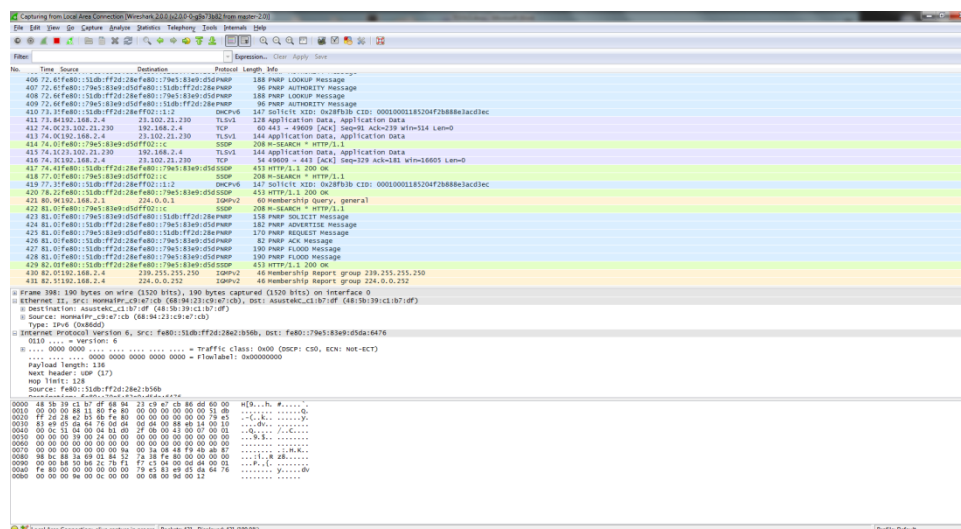


Figure 35 Wireshark

Wireshark is a free software that monitors and decode passing packets in real time. It aims to identify the user, the potential attacks or running malware, to find unsafe

applications running within the network and debugging other applications. It doesn't handle network elements nor act as an intrusion detecting system.

Wireshark can operate in two modes: the *promiscuous* where it monitors the communication between all stations in the network, and the *non promiscuous* where it monitors the communication between the computer on which it is installed and the network. This mode can only be activated if the computer's network card supports it. Furthermore, it can log and store the packet data in one or more files with customizable size.

After launching Wireshark, initially we must select the interface from which Wireshark will capture packets. Then, the packets start to appear in real time as it captures all packet sent to or from the system.

No.	Time	Source	Destination	Protocol	Length
1038	40.422312	192.168.1.77	173.194.33.1	TCP	54
1039	40.659611	fe80::bdca:e67b:5eb7::1	ff02::c	SSDP	201
1040	41.550320	192.168.1.77	207.8.65.23	HTTP	51
1041	41.580992	207.8.65.23	192.168.1.77	TCP	61
1042	42.051665	192.168.1.76	239.255.255.250	UDP	50
1043	42.104199	Actionte_d8:a3:88	Msi_74:82:e6	ARP	61
1044	42.104226	Msi_74:82:e6	Actionte_d8:a3:88	ARP	41
1045	42.119803	192.168.1.74	239.255.255.250	UDP	56
1046	42.910321	192.168.1.77	74.125.53.125	Jabber/;	51
1047	42.929318	74.125.53.125	192.168.1.77	TCP	61
1048	43.659423	fe80::bdca:e67b:5eb7::1	ff02::c	SSDP	201
1049	45.052365	192.168.1.76	239.255.255.250	UDP	50
1050	45.121318	192.168.1.74	239.255.255.250	UDP	56
1051	45.418680	192.168.1.77	72.165.61.176	UDP	121
1052	46.659410	fe80::bdca:e67b:5eb7::1	ff02::c	SSDP	201

Frame 924: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface  
 Ethernet II, Src: CiscoSpv\_4a:df:be (60:2a:d0:4a:df:be), Dst: IPv4mcast\_6f:00:00:00:00:00  
 Internet Protocol Version 4, Src: 192.168.1.76 (192.168.1.76), Dst: 232.239.252.255  
 Internet Group Management Protocol

```

0000  01 00 5e 6f 00 0a 60 2a d0 4a df be 08 00 46 a0  ..A..*.J...F.
0010  00 20 57 53 00 00 01 02 21 f7 c0 a8 01 4c e8 ef  .WS...!...L..
0020  00 0a 94 04 00 00 16 00 01 06 e8 ef 00 0a 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00  .....
  
```

Figure 36 Wireshark captured packets

Wireshark uses colors to distinct the types of traffic. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems.

After stopping the packet capture, we can apply a filter by typing it into the filter box at the top of the window. Wireshark's most powerful feature is considered to be its vast collection of display filters which allows the access the exact needed traffic information. it has preconfigured filters that autocomplete while typing. However, through the display filters, new filter can be created.

Moreover, Wireshark can cooperate with other packet capture applications allowing the exchange of files to and from them.

The Wireshark's features are:

- ✓ Deep inspection of many protocols,
- ✓ Analyzing live captured data as well as offline analysis,
- ✓ Standard three-pane packet browser,
- ✓ Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility,
- ✓ VoIP analysis,
- ✓ Read and write in many different capture file formats
- ✓ Decompression of files captures files compressed with gzip,
- ✓ Decryption support for many protocols,
- ✓ Output can be exported to XML, PostScript, CSV, or plain text,
- ✓ Import packets from text files containing hex dumps of packet data

Wireshark runs on Windows, Linux, Solaris, FreeBSD, NetBSD, Apple Mac OS X, Debian GNU/Linux, Gentoo Linux, HP-UX, Mandriva Linux, OpenPKG, Red Hat Fedora/Enterprise Linux and rPath Linux.

### *Nmap (Network Mapper)*

The Nmap is an open source tool for network discovery and security auditing. It performs network mapping, network management and monitors nodes or services running on the network, it manages service upgrade schedules and monitors host or service uptime. It can scan large networks and single hosts and it uses raw IP packets to determine how many nodes are available on the network, what services those hosts are offering, what operating systems and OS versions they are running and what type of packet filters or firewalls are in use.

Besides the classical command line, the Nmap includes a graphical interface for displaying results, a tool for data transfer, redirection, and debugging, plus an application for comparing detection results.

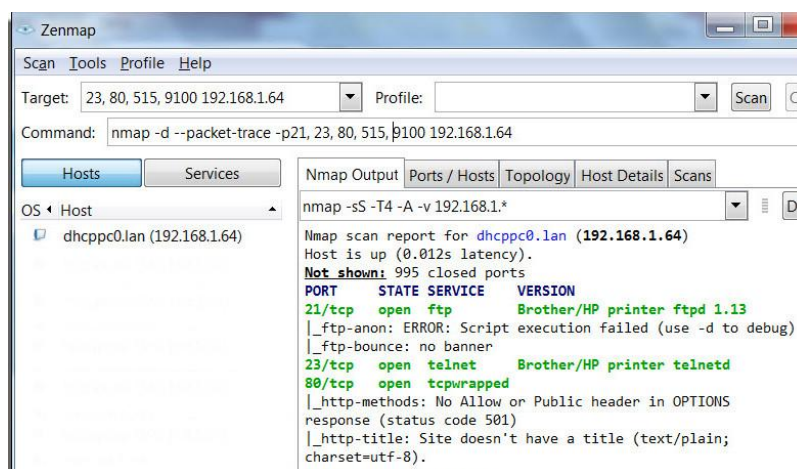


Figure 37 Nmap

Its features are:

- ✓ *Host discovery*. Detects the live host on the network.
- ✓ *Port discovery or Enumeration*. Detects the open ports on the host.
- ✓ *Service discovery*. Detects the software and the version to the respective port,
- ✓ Detects the operating system, the software version and hardware address,
- ✓ *Nmap scripts*. Detects the vulnerability and security holes.

The Nmap's output is available in five different formats. The default is the interactive output, and it is sent to standard output. There is also normal output, which is similar to interactive, but it displays fewer runtime information and warnings. Next, there are the XML output that can be converted to HTML, the grep output which includes most information for a target host on a single line and finally the sCRiPt KiDDi3 OutPUt.

The NMAP is available for all distributions of Linux, for Windows, Mac OS X, D. FreeBSD, OpenBSD, and NetBSD, Sun Solaris, Amiga, HP-UX.

### *Snort*

Snort is an open source software for intrusion prevention that performs real time traffic analysis and packet logging. It can perform protocol analysis, search content and it can be used to detect a wide range of attacks and packages like buffer overflows, hidden ports scans, CGI attacks, SMB prompts and operating system detection. It consists of two main components which are the *snort engine* and the *snort rules*. The *snort engine* is a detection engine that uses a modular architecture of plugins and the *snort rules* is a rule language used to describe the traffic which will be collected. However, those components are distributed separately and the snort rules should be updated regularly as new rules are added constantly.

The Snort can operate as a *sniffer* by capturing the packets moving in the network and displaying them on the screen in real time, as a *packet logger* by logging packages moving on the network for further analysts, as a *network intrusion detection system* by analyzing network traffic according to the rules set by the security administrator and performing the according actions based on those recordings, and in *inline mode* by acting as an IPS allowing drop rules to trigger.

The main features of the Snort are:

- ✓ It captures network packets and displays them on the screen in real time,
- ✓ It displays the network packages for later processing,
- ✓ It detects and reports intrusion attempts while sending alerts to the network administrator,
- ✓ It performs packet content search and then applies filters to reject packets that can be harmful to the network's safety or in violation of the organization's security policy,

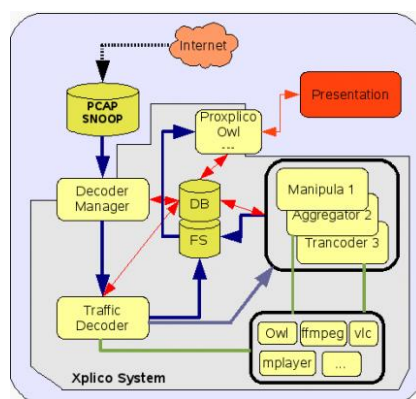
- ✓ It monitors network traffic for every network station and identifies cases where the bandwidth used may be unusually high,
- ✓ It performs protocol analysis,
- ✓ It stores messages and alerts for further analysis as well as produces statistical reports by using third-party applications,
- ✓ It manages intrusion detection errors,
- ✓ Additional rules can be created to meet the security requirements of each network,
- ✓ It can work with other applications and present the recordings in a graphic environment.

Snort can detect if there is an unusual amount of traffic which can lead to denial of service, stealth port scanning, CGI attacks, SMB prompts, OS fingerprinting, virus-like software and threats from peer-to-peer applications. Since Snort works at the network layer, it can't always detect attacks which use MAC addresses. However, it can't take any actions to mitigate them.

Snort is available for Windows, Fedora, Centos, FreeBSD.

### *Xplico*

The Xplico is a free network forensic analysis tool with a web based interface. The main task of the Xplico is to extract data from a network traffic capture, either one of a pcap files or by recording in real time. The Xplico can extract from each email all HTTP contents, each VoIP call from a pcap file. It consists of four subsystems, a decoder manager called *Dema*, an IP network decoder called *Xplico*, a set of applications called *manipulators* for the manipulation of decoded data, and a *visualization system* to view data extracted.



**Figure 38 Xplico System Architecture**

The roles of Dema is to organize the input data, set the configuration, history files for the decoder and the manipulators, launch decoder and manipulators, and to control the execution of decoder and manipulators.

The Xplico can be used either standalone or within architecture and its decoder has three main characteristics; high modularity, scalability and configurability. The decoder has been designed so that the decoding of the protocol had to be disconnected from the formatting of data input, and also from the format used for data output.

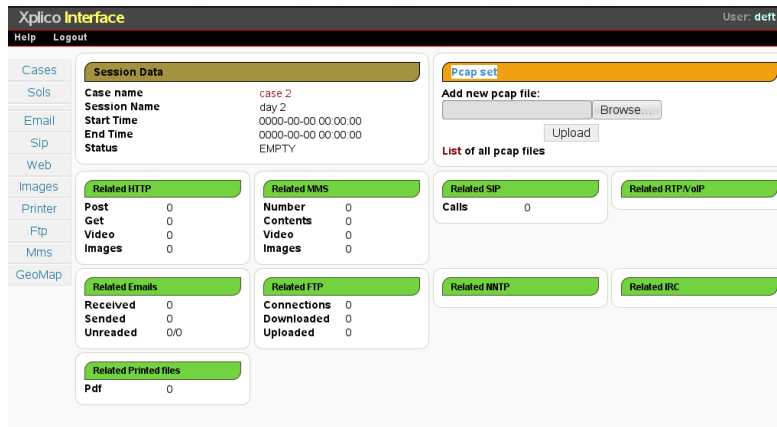


Figure 39 Interface

The Xplico's Features are:

- ✓ It supports the protocols HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv6,
- ✓ Port Independent Protocol Identification (PIPI) for each application protocol,
- ✓ Multithreading,
- ✓ A XML file is associated at each data reassembled by the Xplico which identifies the flows and the pcap containing the data reassembled,
- ✓ Realtime elaboration depending on the number of flows, the types of protocols and by the performance of computer,
- ✓ TCP reassembly with ACK verification for any packet or soft ACK verification,
- ✓ It reverses DNS lookup from DNS packages contained in the inputs files (pcap), not from external DNS server,
- ✓ No size limit on data entry or the number of files entrance,
- ✓ IPv4 and IPv6 support,
- ✓ Every Xplico component is modular. The input interface, the protocol decoder and the output interface are all modules,
- ✓ Output data and information in SQLite database or Mysql database or files.

### Argus

The Argus project is an open source application with a web based interface that monitors network activity. It is an auditing tool that examines the network based on IP protocol, monitors and records information of network traffic, creates logs to solve



network problems and to verify the function of the network security policy. It will send alerts when it detects problems.

The Argus is composed of a network flow data generator, the *Argus monitor*, which processes packets either from pcap files or live data, and generates status reports of network traffic flow and of all flows in the packet stream. It keeps under surveillance all network traffic, IP traffic, data plane, control plane and management plane, and it captures the packet dynamics and semantics of each flow, while reducing data so that it can be stored, examined, processed and analyzed in second time.

The Argus provides accessibility, availability, connectivity, load, duration, rate, retransmission, and delay metrics for all network flows. It captures packet attributes, such as Layer 2 addresses, tunnel identifiers, protocol ids, SAP's, hop-count, options, L4 transport identification, host flow control indications. Furthermore, it has implemented a variety of metrics for packet dynamics which focus on cyber security needs, such as detect human typing behaviour in any flow and key-stroke detection in encrypted SSH tunnels. Moreover, the Argus generates the *producer consumer ratio* which shows whether a network device produces data or consumes data, which is needed when assessing to possibility for a node to be involved in an Advanced persistent threat (APT) mediated exfiltration.

The supported platforms are Linux, Solaris, BSD, OS X, IRIX, AIX, Windows.

### *NetFSE*

The Net/FSE is a server free application for network operations and it provides data capture, search services and indexing. Its can process IP based network log data, from firewalls, intrusion detection systems, routers, and other network in near real time. The web interface is integrated into the codebase, and is build on top of Tomcat and Google Web Toolkit. The user interface has a workflow tool for network operations including security, compliance, troubleshooting, and management.

- ✓ It collects any type of network event data, including flow data.
- ✓ It collects alerts from IDS, IPS, SIM and NBA, firewall logs, web server logs, authentication logs and database server access logs.
- ✓ It identifies events according to criteria set by security analyst.
- ✓ Search results are stored in temporary relational database tables.
- ✓ It can have multiple search results active at once and search history is automatically recorded on the server.
- ✓ The network data can be kept for an extended period of time.
- ✓ It has real-time access to that data.
- ✓ It is able to perform rapid, deep search and analysis on that data.

The Net/FSE is designed to streamline response and recovery operations by helping detection of what other hosts have been involved with the incident, how long has the

event been going on, if the activity that generated the alert is still going on and what ingress and egress points were used for the suspicious activity. It runs on Linux, Mac OS X

### TCPView

The TCPView is a free Windows program that presents detailed listings of all TCP and UDP endpoints and the connection state on the system, including the local and remote addresses.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd P.
[System Proc...	0	TCP	Admin-PC	icnlap	localhost	56014	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	55986	192.34.67.51	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	55987	192.34.67.51	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	55988	192.34.67.51	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	55989	173.194.67.95	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	55990	173.194.67.95	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	55991	173.194.67.95	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	55994	192.34.67.51	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	55995	192.34.67.51	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	55996	192.34.67.51	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	55997	192.34.67.51	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	55998	2.16.173.29	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	56000	2.16.173.29	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	56001	2.16.173.29	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	56002	2.16.173.29	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	56004	198.41.208.139	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	56012	65.52.103.106	hnp	TIME_WAIT			
[System Proc...	0	TCP	admin-pc-bekin	56013	65.52.103.106	hnp	TIME_WAIT			
[System Proc...	0	TCP	Admin-PC	58014	*	*	LISTENING			
Babylon.exe	4216	UDP	Admin-PC	58014	*	*	LISTENING			
chrome.exe	5504	TCP	admin-pc-bekin	55257	54.239.18.235	hnp	ESTABLISHED			
chrome.exe	5504	TCP	admin-pc-bekin	55275	148.251.35.133	hnp	ESTABLISHED			
chrome.exe	1844	TCP	Admin-PC	62514	Admin-PC	0	LISTENING			
cvprnd.exe	1844	UDP	Admin-PC	62514	*	*	LISTENING			
firefox.exe	4576	TCP	Admin-PC	50875	localhost	50875	ESTABLISHED	8	8	
firefox.exe	4576	TCP	Admin-PC	50876	localhost	50875	ESTABLISHED			
firefox.exe	4576	TCP	admin-pc-bekin	56011	2.16.221.31	hnp	ESTABLISHED			
firefox.exe	4576	TCP	admin-pc-bekin	56016	65.52.103.106	hnp	ESTABLISHED			
firefox.exe	4576	TCP	admin-pc-bekin	56019	2.16.221.31	hnp	ESTABLISHED			
firefox.exe	4576	TCP	admin-pc-bekin	56022	2.16.221.31	hnp	ESTABLISHED			
liass.exe	590	TCP	Admin-PC	49159	Admin-PC	0	LISTENING			
liass.exe	590	TCPV6	[0.0.0.0.0.0.0.0]	49159	[0.0.0.0.0.0.0.0]	0	LISTENING			
MFEot_428.exe	3284	UDP	Admin-PC	64167	*	*	LISTENING			
services.exe	590	TCP	Admin-PC	49159	Admin-PC	0	LISTENING			
services.exe	590	TCPV6	[0.0.0.0.0.0.0.0]	49159	[0.0.0.0.0.0.0.0]	0	LISTENING			
Skype.exe	4416	TCP	Admin-PC	hnp	Admin-PC	0	LISTENING			
Skype.exe	4416	TCP	Admin-PC	hnp	Admin-PC	0	LISTENING			
Skype.exe	4416	TCP	admin-pc-bekin	51020	213.159.179.175	40101	ESTABLISHED	6	95	

Figure 40 TCPView

When the TCPView starts, it will enumerate all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions. The Tcview will also show the amount of the TCP and the UDP traffic flowing through an endpoint. By default, the TCPView updates every second, but the rate can be customized. Endpoints that change state from one update to the next are highlighted in yellow, those that are deleted are shown in red, and new endpoints are shown in green. The established TCP/IP connections can be closed and the TCPView's output window can be saved as a txt file.

### TcpDump

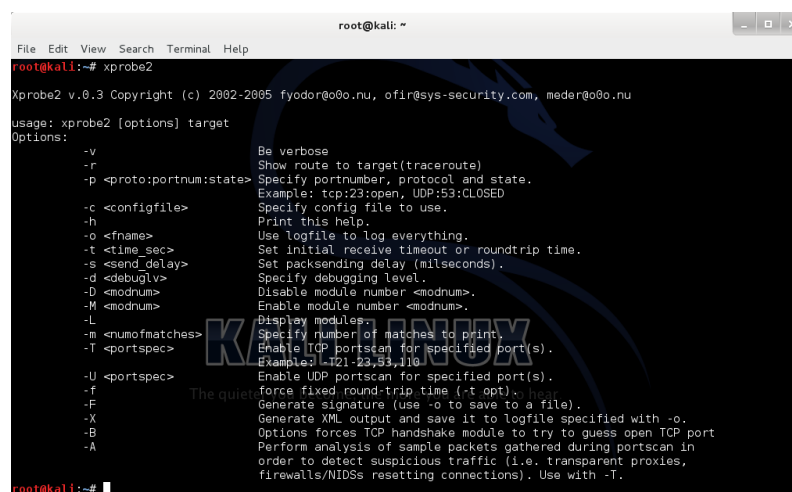
The TcpDump is a command line tool which is used for network monitoring, debugging protocols and acquisition of network data. The TcpDump displays the contents of packets on a network interface that match a given logical expression with timestamps, and records the data in a pcap file format. So this tool can capture filtered network traffic in order to limit the number of connections to those needed for examination. It is usually executed in shared networks so that it can monitor network traffic in other terminals. The TcpDump not only captures live traffic, but it can also read from a saved packet file or a list of saved packet files, however only packets that match the given expression will be processed. Once the capturing

process finishes, the TcpDump will report how many packets it received and processed and how many packets were received by filter. The second report depends on which OS the TcpDump is running on.

The Tcpdump is available for various platforms such as Linux, Solaris, BSD, OS X, HP-UX, Android and AIX. In those systems, the tcpdump uses the libpcap.dll for packets capture. In Windows, the port of the tcpdump is called WinDump and it uses WinPcap.dll, which is the equivalent Windows port of libpcap.

## Xprobe2

The Xprobe2 is a dynamic remote fingerprinting tool for linux which has a different approach than other similar software. The Xprobe2 is based on fuzzy signature matching, probabilistic guesses, multiple matches simultaneously, and a signature database.

A screenshot of a terminal window on a Kali Linux system. The terminal shows the command 'xprobe2' being executed, which displays the help text for the tool. The help text includes the version number (v.0.3), copyright information (2002-2005), and a list of options with their descriptions. The options listed are: -v (Be verbose), -r (Show route to target), -p (Specify portnumber, protocol and state), -c (Specify config file), -h (Print this help), -o (Use logfile), -t (Set initial receive timeout), -s (Set packsending delay), -d (Specify debugging level), -D (Disable module), -M (Enable module), -L (Display modules), -m (Specify number of matches), -T (Enable TCP portscan), -U (Enable UDP portscan), -f (force fixed round-trip time), -F (Generate signature), -X (Generate XML output), -B (Options forces TCP handshake module), and -A (Perform analysis of sample packets).

```
root@kali:~# xprobe2
Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@00o.nu, ofin@sys-security.com, meder@00o.nu
usage: xprobe2 [options] target
Options:
-v          Be verbose
-r          Show route to target(traceroute)
-p <proto:portnum:state> Specify portnumber, protocol and state.
           Example: tcp:23:open, UDP:53:CLOSED
-c <configfile> Specify config file to use.
-h          Print this help.
-o <fname> Use logfile to log everything.
-t <time_sec> Set initial receive timeout or roundtrip time.
-s <send_delay> Set packsending delay (milliseconds).
-d <debuglv> Specify debugging level.
-D <modnum> Disable module number <modnum>.
-M <modnum> Enable module number <modnum>.
-L          Display modules.
-m <numofmatches> Specify number of matches to print.
-T <portspec> Enable TCP portscan for specified port(s).
           Example) -T21-23,53,110
-U <portspec> Enable UDP portscan for specified port(s).
-f          force fixed round-trip time (-t opt).
-F          Generate signature (use -o to save to a file).
-X          Generate XML output and save it to logfile specified with -o.
-B          Options forces TCP handshake module to try to guess open TCP port
-A          Perform analysis of sample packets gathered during portscan in
           order to detect suspicious traffic (i.e. transparent proxies,
           firewalls/NIDSs resetting connections). Use with -T.
```

Figure 41 Xprobe2

The Xprobe2 includes port scanning tool, a port detector, an automatic timeout control for its tools, a full control over all of its functions and a large signature database.

The Xprobe2 operates by applying statistical analysis based on a mathematical algorithm, providing the best possible match between the data received from the target system and the signature database. It also uses a form of optical character recognition software, using a table based on traces matching and statistical calculation results of each audit conducted. The approach of fuzzy logic provides resistance to environmental influences. Furthermore, to fingerprint the remote operating system, the Xprobe2 analyzes the replies from that system. Therefore, to enhance its effectiveness, the Xprobe2 must be provided with as much information as possible.

## Fiddler

The Fiddler is a client based web sniffer developed by Microsoft to fight the spam search engines. The Fiddler is a local proxy server, for gathering all http, https, ftp web traffic. It contains tools to interpret and extract the information, shows which web sites where visited on the way to the target Web site and if they had any malware, and generally it will record in a session log all software downloaded, web site visited and redirections.

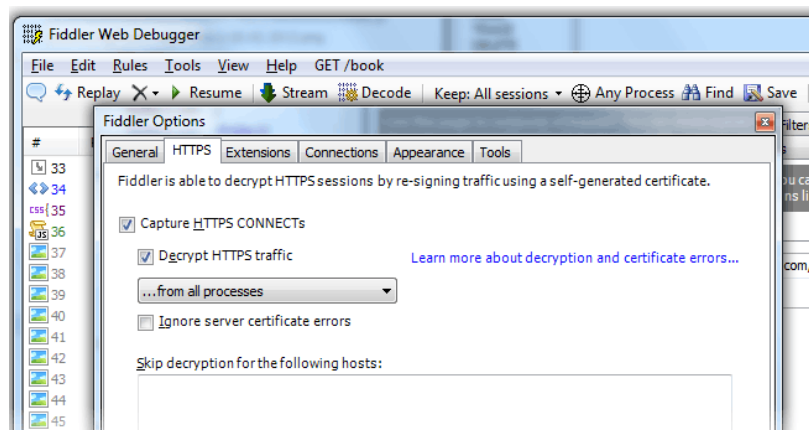


Figure 42 Web Debugger

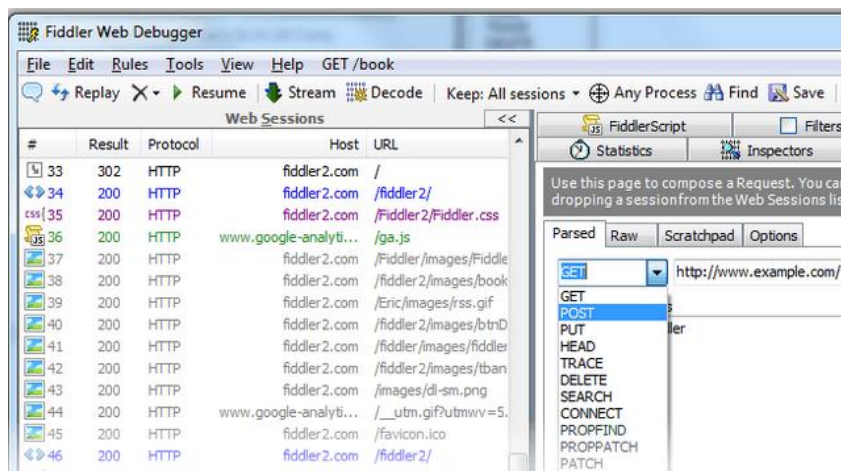


Figure 43 Web Session Manipulation

Its key features are:

- ✓ *Web Debugging.* It can decrypt and decompress web sessions and help the analysis of session data.
- ✓ *Web Session Manipulation.* It can compose http requests, tamper a session by setting breakpoints, manipulate any http or https request or response and simulate original http traffic.
- ✓ *Performance Testing.* It contains custom rules that can be used to indicate problems in performance or security. Furthermore, it can profile the performance of web apps, show the start time and duration of selected

sessions for performance analysis, simulate http compression and improve the speed and performance of web applications by reducing the number of request or response roundtrips and by reducing the amount of bytes transferred from server to client.

- ✓ *HTTP/HTTPS Traffic Recording*. It can record traffic, archive it and playback, capture all http traffic, display the contents of a recorded web session and filter captured traffic.
- ✓ *Security Testing*. It supports automate SSL decryption and it can assist security testing.
- ✓ *Customization*. It supports an extensibility model which ranges from simple fiddler-script to extensions which can be developed using any .NET language.

### **Bro and BroBox**

The Bro is an open source tool for network analysis which passively supervises network traffic and monitors for suspicious activity. It is essentially a *platform* for traffic analysis which is customizable and extensible. It detects intrusions by extracting information at the application level and it then performs analysis of events data related and compares this activity with patterns to determine whether the activity is suspicious. If suspicious activity is detected, then it creates a log entry or sends alerts in real time, or executes a given command.

The Bro uses a domain-specific scripting language that allows site-specific monitoring policies. It doesn't depend on traditional signatures, therefore it is not restricted to any particular detection approach. Moreover, it creates a set of log files that record all networks' activity in high-level terms. Apart from a record of every connection seen on the network, these logs include application-layer transcripts. Furthermore, it supports a wide range of traffic analysis tasks and analyzers for many protocols, even outside of the security domain, such as performance evaluation and helping with troubleshooting and it keeps extensive application layer state of the network it monitors. By default, the Bro writes all this information into structured tab separated log files suitable for post-processing with external software.

The Bro's features are:

- ✓ Passive traffic analysis off a network tap or monitoring port,
- ✓ Standard libpcap interface for capturing packets,
- ✓ Real-time and offline analysis,
- ✓ Cluster-support for large-scale deployments,
- ✓ Unified management framework for operating both standalone and cluster setups,
- ✓ Logging of activity for offline analysis and forensics,

- ✓ Port-independent analysis of application layer protocols,
- ✓ Analysis of file content exchanged over application layer protocols, including MD5 and SHA1 computation for fingerprinting,
- ✓ Tunnel detection and analysis. Bro decapsulates the tunnels and then proceeds to analyze their content as if no tunnel was in place,
- ✓ Support for IDS-style pattern matching,
- ✓ Event-based programming model,
- ✓ Domain-specific data types such as IP addresses, port numbers, and timers,
- ✓ Support for tracking and managing network state,
- ✓ Default output to ASCII logs,
- ✓ Real-time integration of external input into analyses.
- ✓ External C library for exchanging Bro events with external programs. It comes with Perl, Python, and Ruby bindings,
- ✓ Ability to trigger arbitrary external processes from within the scripting language.

It runs on standard UNIX-style systems and Mac OSX. The Bro comes with a BSD license, allowing for free use with no restrictions. The *Broala* is a by-product founded by the creators of the Bro which provides professional Bro support to enterprise customers.

### *Ettercap*

The Ettercap is an open source tools designed for network monitoring. It is multipurpose sniffer content filter, as well as a tool for man-in-the-middle attacks. It has built-in functionality for network and host analysis, and intercepts network traffic to collect user passwords, to detect operating systems and it also supports active and passive dissection of many protocols.

The Ettercap can operate in IP-based mode, MAC-based mode, ARP-based mode, and Public ARP-based mode. In *IP-based mode*, the packets are filtered according to source's and destination's IP. In *MAC-based mode*, the packets are filtered according to the MAC address which is useful for sniffing connections through a gateway. In *ARP-based mode*, it uses ARP poisoning to sniff the traffic on a switched LAN between two hosts. Finally, in *Public ARP-based mode*, it uses ARP poisoning to sniff the traffic on a switched LAN from a victim host to all other hosts.

The Ettercap's features are:

- ✓ It emulates commands or replies while maintaining a live connection,
- ✓ It supports the sniffing of the data of an SSH1 connection,
- ✓ It supports the sniffing of http ssl secured data, even when the connection is through a proxy,

- ✓ It supports the sniffing of remote traffic through a GRE tunnel from a remote Cisco router, and performs a man-in-the-middle attack on it,
- ✓ It supports customizable plugins,
- ✓ It collects passwords
- ✓ It sets up a filter which searches for a particular string or hexadecimal sequence in the TCP or UDP payload and replaces it with a custom string sequence, or drops the entire packet,
- ✓ OS fingerprinting,
- ✓ It kills a connection,
- ✓ It retrieves information about hosts on the LAN, their open ports, the version numbers of available services, the type of the host and estimated distances in number of hops,
- ✓ Hijacking of DNS requests,
- ✓ Actively or passively discovering of other poisoners on the LAN.

The Ettercap is supported in both 32 and 64 bit distributions of Debian/Ubuntu including all its derivatives, Fedora, Gentoo, Pentoo, Mac OSX, FreeBSD, OpenBSD and NetBSD.

### *NTLast*

The NTLast is a free security audit tool for Windows NT. It allows the monitoring of successful and unsuccessful connection attempts to the system. Thus, this tool can be used to discover suspicious user accounts and remote systems connected to the system.

The NTLast's key features are:

- ✓ It reads saved .evt files,
- ✓ It allows to search before, after, and between a specific time period
- ✓ It filters logons 'From' a certain hosts,
- ✓ It can save files in a csv format w/ time field formatted for Excel,
- ✓ It filters out and distinguishes web log usage.

### *Microsoft Message Analyzer*

The Microsoft Message Analyzer is a free tool for capturing, displaying, and analyzing protocol messaging traffic and other system messages. It also allows gathering, importing, and analyzing data from log and trace files. The data can be captured live or can be loaded from archived message collections from multiple data sources simultaneously.

When performing capturing traffic, the Message Analyzer limits network noise and expose the issues that occur at lower levels. This is done by enabling to remove lower-level details, by presenting message summaries and diagnostics to top-level





## Nagios XI

The Nagios XI is a commercial network monitoring tool that helps determine if all critical systems, applications and services are properly and they are running. It provides features such as alerting, event handling and reporting. The heart of the application is the *Nagios Core* which contains the core monitoring engine and a basic web UI. The user can use plugins that will allow him to monitor services, applications, and metrics, a chosen frontend, as well as add-ons for data visualisation, graphs, load distribution, and MySQL database support.

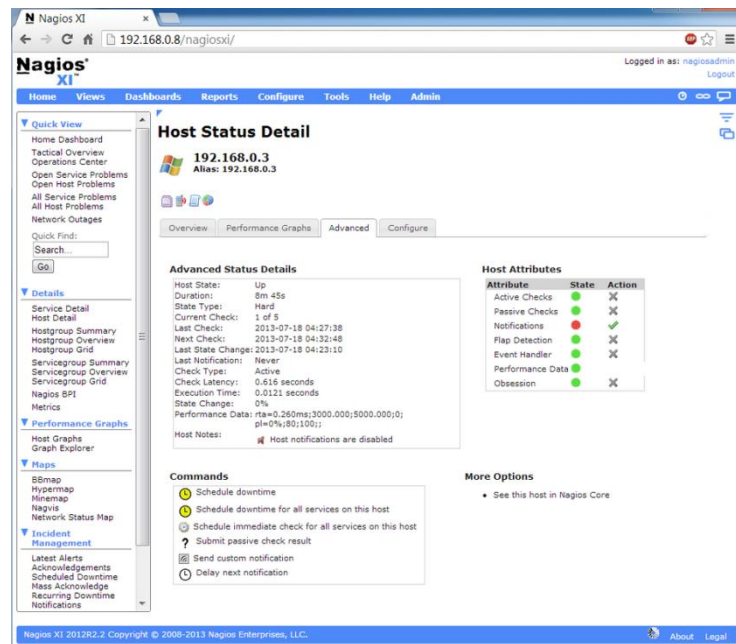


Figure 45 Nagios XI Interface

The Nagios's features are:

- ✓ *Monitoring Engine.* The Nagios Core 4 monitoring engine provides with monitoring of network infrastructure.
- ✓ *Updated Web Interface.* It provides an overview of hosts, services, and network devices.
- ✓ *Graphs and Visualizations.* It allows to quickly view the status of monitoring infrastructure.
- ✓ *Performance and Capacity Planning Graphs.* It allows organizations to plan for infrastructure upgrades before outdated systems occurs.
- ✓ *Configuration Wizards.* It configures network devices.
- ✓ *Infrastructure Management Capabilities.* Improved Bulk-Host Import, Auto-Discovery, Automatic Decommissioning, and Mass Acknowledgment tools.
- ✓ *Configuration Snapshot Archive.* It provides an archive of past configuration snapshots to revert to, if problems occur in the current configuration.

- ✓ *User Management.* It allows to easily setup and manages user accounts, assigns custom roles and sets User-specific notification preferences to customize alert settings and notification messages according to their needs.
- ✓ *Service-Level Agreement (SLA) Reports.* It allows to measure effectiveness of specific hosts, services, and business processes to determine if service-level agreements are being met.

Nagios can only be installed in RHEL or CentOS Linux server. Otherwise it can be used as virtual machine

### Network Analyzer

The Nagios Network Analyzer is a commercial application that provides network traffic and bandwidth information for an entire IT infrastructure, and helps to ensure that systems, applications, services, and business processes are functioning properly. It allows to gather information regarding the health of the network, as well as highly granular data for network analysis. It provides a central view of the network traffic and bandwidth data, as well as potential network compromises. Furthermore, it can send alerts when critical thresholds are exceeded, abnormal network activity occurs, or bandwidth restrictions are met.

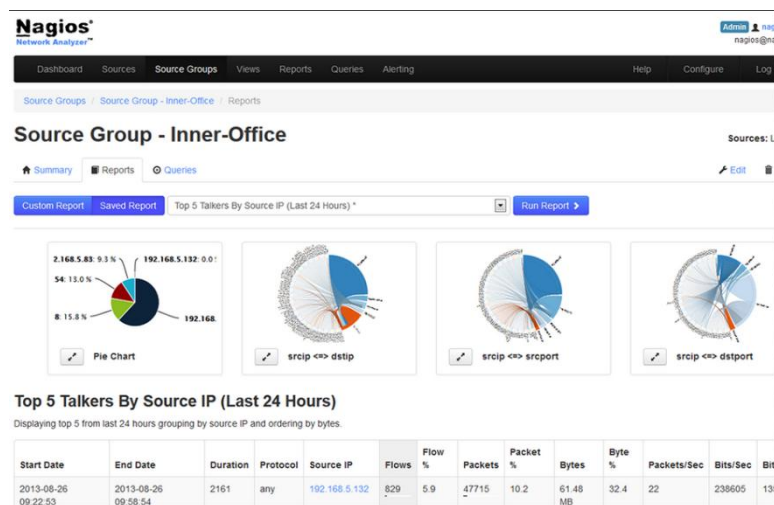


Figure 46 Network Analyzer Custom reports

The Nagios Network Analyzer's features are:

- ✓ *Comprehensive Dashboard.* It provides an overview of sources, checks and network flow data.
- ✓ *Security and Reliability.* Triggers alerts when suspicious activity takes place on the network.
- ✓ *Graphs and Visualizations.* Views of network flow data in graphs.
- ✓ *Custom Application Monitoring.* Individualized queries, views, and reports.
- ✓ *Specialized Views.* Quick access to archived query data in a network snapshot.

- ✓ *Automated Alert System.* It sends alerts when abnormal activity takes place.
- ✓ *Compatible Integration.* It is compatible with all standard flow source types including: NetFlow, jFlow, sFlow, cFlow, IPFIX, etc.

Nagios can only be installed in RHEL or CentOS Linux server. Otherwise it can be used as virtual machine.

### NetworkMiner

The NetworkMiner is a network forensic analysis tool that has a free and commercial version. It is as a passive network sniffer and packet capturing tool that detects operating systems, sessions, hostnames and open ports, without putting any traffic on the network. The NetworkMiner can capture live traffic and can inform which devices or IP address are consuming the most bandwidth, but also parse PCAP files for later analysis and it also can regenerate or reassemble transmitted files and certificates from PCAP files. In contrast to other sniffers, NetworkMiner displays hosts and their attributes rather than raw packets. In the user interface, the information is grouped per host rather than per packets or frames.

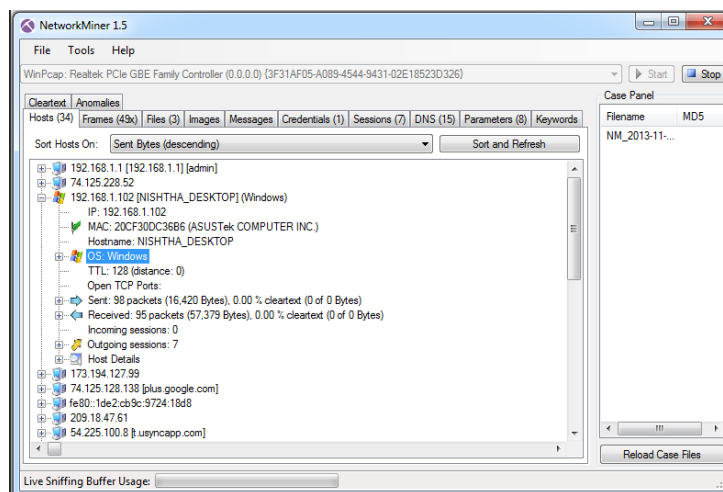


Figure 47 NetworkMiner Free Edition

The NetworkMiner can extract files and certificates transferred over the network in real time by sniffing traffic directly from the network or by parsing a PCAP file. Therefore, it can extract and save media files which are streamed through the network from websites. Supported protocols for file extraction are FTP, TFTP, HTTP, SMB and SMTP. Under the Credentials tab, they are displayed the user credentials for the supported protocols. Moreover, the user can search sniffed or stored data for keywords using arbitrary strings or byte-patterns.

The features of NetworkMiner's free and commercial version are:

	Free Edition	Professional Edition
Live sniffing	Yes	Yes

Parse PCAP files	Yes	Yes
Parse PcapNG files	No	Yes
Receive Pcap-over-IP	Yes	Yes
OS Fingerprinting	Yes	Yes
Port Independent Protocol Identification (PIPI)	No	Yes
Export results to CSV / Excel	No	Yes
Configurable file output directory	No	Yes
Geo IP localization	No	Yes
DNS Whitelisting	No	Yes
Host coloring support	No	Yes
Command line scripting support	No	Yes (through NetworkMinerCLI)

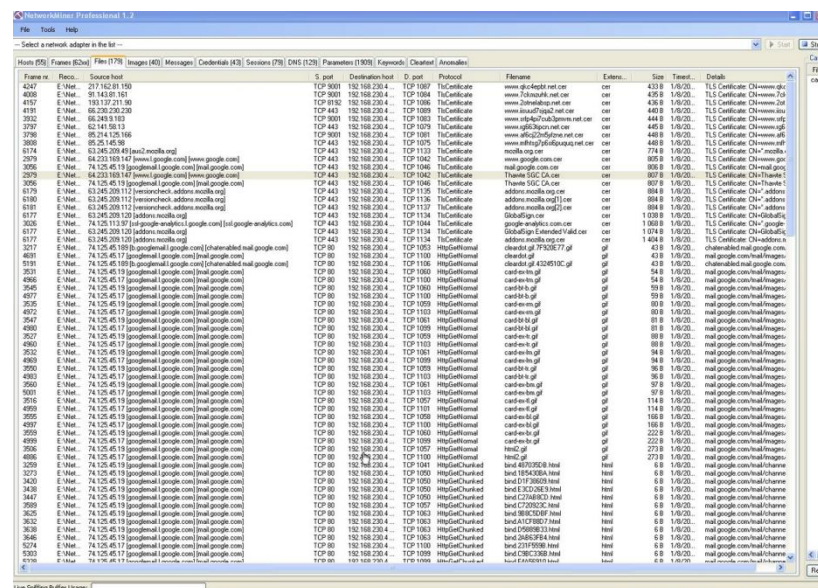


Figure 48 NetworkMiner Professional Edition

The NetworkMiner Professional comes installed on a specially designed USB flash drive which can be run directly from the USB flash drive with no installation required. The NetworkMiner is developed for Windows but it also works in Linux, Mac OS X, FreeBSD.

### CapAnalysis

CapAnalysis is open source software for Linux, for analyzing large amounts of captured network traffic. It lists the data set of PCAP files and presents their contents in many forms, starting from a list of TCP, UDP or ESP streams or flows, passing to the geo-graphical representation of the connections.

Date	Time	Source IP	Destination IP	Source Port	Protocol	Bytes Sent	Bytes Received	Lost bytes Sent	Lost bytes Received	Packets Sent
2013-03-05	19:23:25	212.183.128.245	10.200.59.77	45691	SSH	2.4K	23.8K	0	0	13
2013-02-20	22:01:51	31.205.0.166	10.200.59.77	51244	SSH	2.4K	23.8K	0	0	24
2013-02-20	22:32:58	114.113.226.43	10.200.59.77	52921	SSH	500	18.8K	0	0	1
2013-02-20	22:33:25	114.113.226.43	10.200.59.77	55537	SSH	500	18.8K	0	0	1
2013-02-20	22:33:10	114.113.226.43	10.200.59.77	54045	SSH	500	18.8K	0	0	1
2013-02-20	22:32:38	114.113.226.43	10.200.59.77	50934	SSH	500	18.8K	0	0	1
2013-02-20	22:32:44	114.113.226.43	10.200.59.77	51478	SSH	500	18.8K	0	0	1
2013-02-20	22:33:01	114.113.226.43	10.200.59.77	53212	SSH	500	18.8K	0	0	1
2013-02-20	22:32:55	114.113.226.43	10.200.59.77	52564	SSH	500	18.8K	0	0	1
2013-02-20	22:33:15	114.113.226.43	10.200.59.77	54574	SSH	500	18.8K	0	0	1
2013-02-20	22:32:46	114.113.226.43	10.200.59.77	51765	SSH	500	18.8K	0	0	1
2013-02-20	22:33:12	114.113.226.43	10.200.59.77	54321	SSH	500	18.8K	0	0	1
2013-02-20	22:32:23	114.113.226.43	10.200.59.77	49463	SSH	500	18.8K	0	0	1

Figure 49 CapAnalysis

- ✓ Collects information for each stream or flow of packets UDP and TCP
- ✓ Is able to reassemble the TCP streams to make its analysis.
- ✓ Identifies the number of bytes lost, for each direction, and the total bytes exchanged for the TCP flows
- ✓ Uses the *Deep Packet Inspection* to identify the protocol of each flow.
- ✓ For each connection tries to identify the country of the destination point.
- ✓ Has a powerful set of filters for analysis.

### P0f

P0f is an open source tool for passive OS fingerprinting that can help identify the perpetrator of an incidental TCP/IP communications without interfering in any way. To do so, it uses an array of sophisticated purely passive traffic fingerprinting mechanisms.

It can identify the system or machines that are connected even if the devices are behind a packet firewall. It can also detect what the remote system is hooked up to, how far it is located, what's its uptime and can detect masquerade or illegal network hook-ups. p0f can detect certain types of packet filters and NAT setups, and sometimes can determine the name of the target's ISP. It's still passive thus doesn't generate any network traffic. No name lookups, no traffic to the victim, no ARIN queries, no trace route.

Some of p0f's features include:

- ✓ Identification of the operating system and software on both endpoints of a TCP connection.
- ✓ Measurement of system uptime and network hookup, distance including topology behind NAT or packet filters.
- ✓ Automated detection of connection sharing, NAT, load balancing, and application level proxying setups.
- ✓ Detection of clients and servers that forge declarative statements such as X-Mailer or User-Agent.

## Netcat

Netcat is a simple Linux utility which reads and writes data across network connections, using TCP or UDP protocol. At the same time, it is a network debugging and exploration tool, since it can create almost any kind of connection. Some of its features are the following:

- ✓ Port Scanning
- ✓ Banner grabbing to determine which services are running on a specified port outbound or inbound connections, TCP or UDP, to or from any ports
- ✓ Full DNS checking, with warnings
- ✓ Ability to use any local source port or any locally configured network source address
- ✓ Built-in port-scanning capabilities and source-routing capability
- ✓ Can read command line arguments from standard input
- ✓ Hex dump of transmitted and received data
- ✓ Tunneling mode which permits user-defined tunneling with the possibility of specifying all network parameters.

*Cryptcat* is the standard *netcat* enhanced with twofish encryption.

## Maltego and Maltego CaseFile

The Maltego is a forensics and data mining application that provides information in an easy to understand format. This tool can gather information for all security related work. It has a flexible framework that allows customization to fit the organizations requirements. Also, it provides visually representation of interconnected links between searched items for helping user to see hidden connections and it uses open source intelligence to link the entities.

The Maltego can be used to resolve the relationships and real world links between groups of people, companies, organizations, web sites, and internet infrastructure such as domains, dns names, netblocks, ip addresses, documents and files.

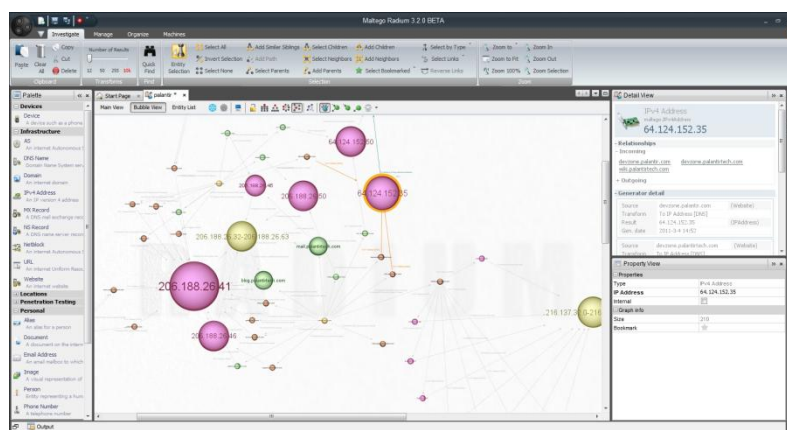


Figure 50 Maltego

The CaseFile, if purchased separately, is used to allow an offline analysis, when the sources of information are not gained from the open source intelligence side or they can be programmatically queried. This tool allows the adding, linking and analyzing data, having the same graphing flexibility and performance as the Maltego without the use of transforms.

The CaseFile can be used by incident response team for the information gathering, analytics and intelligence phases of almost all types of investigations. It has the ability to visualise interconnected links between searched items and the datasets can be stored in CSV, XLS and XLSX spreadsheet formats.

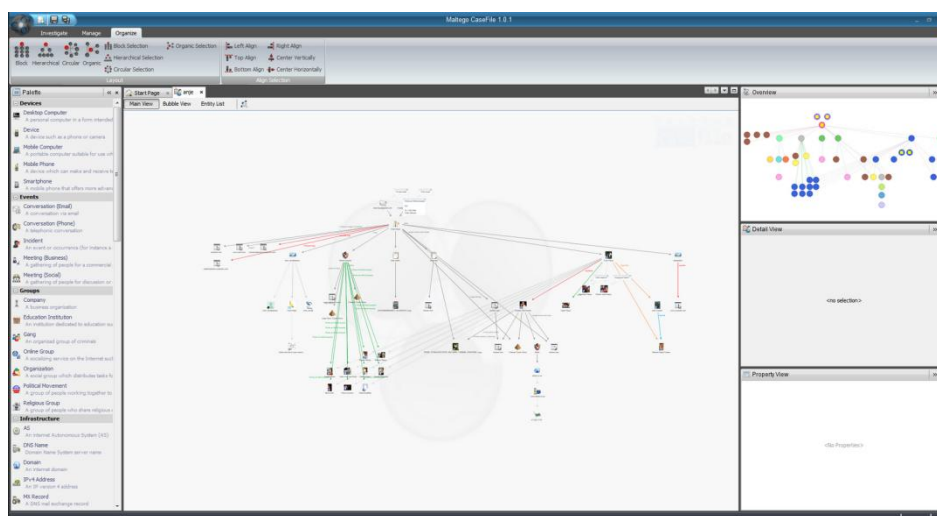


Figure 51 Maltego CaseFile

The Maltego Client is based on Java, therefore it can be installed on all platforms. The Maltego server is delivered as a VMWare image, thus it can run on anything that supports VMWare or a virtual machine system. As such, any operating system with the capability to run a virtual machine system can be used.

### *F-Response TACTICAL*

F-Response TACTICAL is commercial software for analysis over a network. It is designed to streamline live analysis, collection, and authentication. When connected to a remote computer, it will give access to all the physical drives, logical volumes, and physical memory on that remote computer via the network. Some of its features are:

- ✓ Provides direct, live, read-only access to the remote target computer's disks
- ✓ Runs directly from the provided USB storage and licensing devices.
- ✓ Through Flexdisk it provides direct access to the remote target machines Logical and Physical targets in both raw and logical format.

- ✓ Works with all RAID disks, physical drives, logical volumes, and physical memory. In addition, F-Response TACTICAL includes target executables for the three most common operating systems, Windows, Linux, and Apple OSX.
- ✓ Supports the most common target platforms including all Windows 32 and 64bit, Apple OSX and Linux

## 7.3. Mobile Forensics

### 7.3.1. Acquisition

#### *LiME*

LiME is a free command tool that allows full volatile memory capturing from Linux and Linux-based devices. It is a LKM (Loadable Kernel Memory), therefore it supports dumping memory either to the file system of the device or over the network. During acquisition, it minimizes its interaction between user and kernel space processes, which allows it to produce memory captures in a forensically manner.

To obtain a memory dump over TCP tunnel, the device must first listen on specified port which we connect from our host. Once the host has connected to the socket, the RAM image will automatically be sent to the host for analysis. On the host computer, we must use netcat to connect to the same port and to redirect the output to a file.

LiME also supports disk-based acquisition. In this case, LiME has the option to write memory images to the device's file system. On Android, the logical place to write is the device's SD card.

#### *Mobilyze*

Mobilyze is a commercial tool for acquiring data in a forensically sound manner, and reporting for Android and iOS devices. It is also a mobile data triage tool that can provide immediate access to data from iOS and Android devices. It can run on either Mac or Windows, has options for a full or limited data collection and collect the data only by connecting the device via usb.

The Mobilyze's features are:

- ✓ Viewing of data in real time during the device acquisition
- ✓ Unplug the device at any time, preserving all acquired data
- ✓ Get an immediate snapshot of key user info from the device
- ✓ Limit data collection based on search warrant requirements
- ✓ Select the order in which third party application data is collected
- ✓ Collect and preserve all relevant user data in a forensically sound manner
- ✓ Navigate between communications, media, locations, apps, and internet



- ✓ View all messages in native format or an indexed list
- ✓ Has a Filter field to filter any dataset

### *Plan:C*

Plan:C is a free forensic software for capturing forensic information. It can run on multiple platforms and it performs photographic capture of evidence.

Its main features are:

- ✓ All files hashed and fully referenced in evidence report
- ✓ No dongles or license keys needed
- ✓ Live video preview
- ✓ Supports Canon EOS cameras
- ✓ Generates PDF report
- ✓ Creates barcode labels for evidence tagging
- ✓ Embeds agency info in EXIF data

Runs on Macintosh, Windows, and Linux machines.

### *Android Connections Forensics*

Android Connections Forensics is an open source software for mapping each connection to its originating process on an Android mobile. This tool doesn't require root privileges on the system, but do require adb and USB debugging. It creates three output types. The *console output* file and the *acm-log* file which both contains the live connections and the metadata file which contains results about external IP's metadata.

### *UFED 4PC*

UFED 4PC is a commercial Windows based software that enables the extraction of physical, file system, and logical extractions of all data and passwords, included deleted data, from mobile devices. It consists of four products which are the Physical Analyzer, the Logical Analyzer, the Reader and the Phone Detective.

Some of its features are:

- ✓ Physical extraction and decoding while bypassing pattern lock / password / PIN from Android devices
- ✓ Physical extraction from BlackBerry devices
- ✓ Support for extraction and decoding from Apple devices
- ✓ Physical extraction and decoding from locked Nokia BB5 devices
- ✓ Physical extraction and decoding from Windows Phone devices
- ✓ Unrivalled access to locked devices by bypassing, revealing or disabling the user lock code

- ✓ File system extraction from any device running Windows Phone, HTC, Samsung, Huawei and ZTE
- ✓ Logical extraction of apps data, passwords, emails, call history, SMS, contacts, calendar, media files, location information etc
- ✓ Forensic cloning of SIM ID to isolate the phone from network activity during analysis

### *UFED Cloud Analyzer*

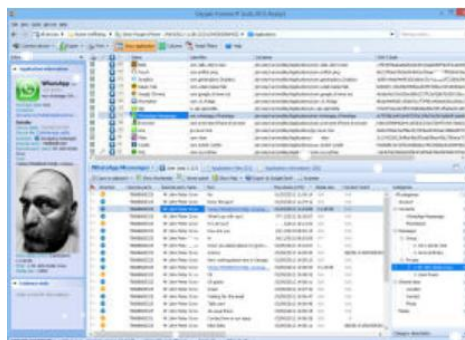
UFED Cloud Analyzer is a commercial Windows based software that provides extraction, preservation and analysis of private social media accounts like Facebook, Twitter, Kik, Instagram, file storage and other cloud-based account and automatically collects both existing cloud data and metadata in a forensically sound manner. It performs extractions of private user data, unifies and organizes disparate data into a common view, and share and integrates data for further analysis. Some of its main features are:

- ✓ Allows access to private cloud data using login information extracted from the mobile device.
- ✓ Can login to private cloud data using usernames and passwords provided via other discovery means.
- ✓ Extracts information from cloud data sources while logging and tracing the entire process to maintain data authenticity.
- ✓ Each piece of extracted data is hashed separately so that it can later be compared against its origin.
- ✓ Normalize different cloud services in a unified format
- ✓ Generate and share PDF reports for entire data sets or filtered information.

## **7.3.2. Analysis**

### *Oxygen Forensic*

Oxygen Forensic is a commercial windows based collection of software for extraction and analysis of data from mobile devices. Some of its features include:



**Figure 52 Oxygen Forensic Suite**

- ✓ Acquires data from a wide range of devices (Android, BB, iOS, WP.)
- ✓ Imports device backups and images
- ✓ Parses data from apps
- ✓ Recovers a wide range of deleted data
- ✓ Offers data analytics such as aggregated contacts, social graph, timeline)
- ✓ Exports data to popular file formats, like PDF, RTF, XLS and XML.
- ✓ Finds passwords to encrypted backups and images
- ✓ Disables screen lock on popular Android OS devices
- ✓ Extracts data from clouds
- ✓ Offers import and analysis of call data records
- ✓ Visualizes routes and common locations of several users

### *Elcomsoft Mobile Forensic Bundle*

Elcomsoft Mobile Forensic Bundle is a commercial mobile forensic kit for acquiring and analyzing the content of mobile devices. The kit allows experts to perform physical, logical and over-the-air acquisition of smartphones and tablets, break mobile backup passwords and decrypt encrypted backups, view and analyze information stored in mobile devices.

Elcomsoft Mobile Forensic Bundle contains the following five products:

*Elcomsoft Phone Breaker Forensic* which is a tool for logical acquisition of iOS, Windows Phone and BlackBerry devices, recover mobile backup passwords and decrypt encrypted backups. It also has a Mac OS X version

*Elcomsoft Phone Viewer* is a tool to view and analyze information extracted with ElcomSoft mobile forensic tools. Allows viewing of deleted messages, including deleted SMS and iMessages in iOS backups.

*Elcomsoft Explorer for WhatsApp* is a tool to download, decrypt and display WhatsApp communication histories.

*Elcomsoft Blackberry Backup Explorer Pro* is a tool for viewing the content of legacy BlackBerry backups.

*Elcomsoft iOS Forensic Toolkit* is a commercial software for Forensic Access to iPhone, iPad and iPod devices running Apple iOS. It allows acquiring bit-to-bit images of devices' file systems, extracting passcodes, passwords, and encryption keys, and decrypting the file system image.

Elcomsoft iOS Forensic Toolkit's features are:

- ✓ Physical acquisition: acquire complete, bit-precise device images
- ✓ Extract information from locked devices

- ✓ Decrypt keychain items
- ✓ File system acquisition
- ✓ Leaves no traces and no alterations to devices
- ✓ Passcode is not required
- ✓ Has an automatic and manual mode

### *iOS Forensic Toolkit*

iOS Forensic Toolkit is a commercial software for forensic acquisition and analysis of iPhone, iPad and iPod devices. It acquires bit-to-bit images of devices' file systems, extracts device passcodes, passwords, and encryption keys and decrypts the file system image. Some of its features are:

- ✓ Acquire complete, bit-precise device images
- ✓ Decrypt keychain items, extract, device keys
- ✓ File system acquisition
- ✓ Zero-footprint operation leaves no traces and no alterations to devices' contents
- ✓ Every step of investigation is logged and recorded
- ✓ Supports all versions of iOS
- ✓ Physical and logical acquisition
- ✓ Works in automatic and manual mode

iOS Forensic Toolkit is available for Mac and Windows systems.

### *LANTERN*

LANTERN is a commercial Mac based mobile forensic application that performs device acquisition and analysis. It can add devices, Macs, Call Detail Record, previous case files, iCloud and computer backups into one case file and then perform link analysis. Furthermore, it has integrated a file system viewer for manual analysis with a built in plist editor.

Some of its key features are:

- ✓ Activity Monitor
- ✓ Date filter on Data and Reports
- ✓ SMS Handle ID's
- ✓ Link Analysis
- ✓ Archive Function for case files and HTML Reports
- ✓ Multiple device acquisitions within one case file
- ✓ Logical Extractions of iOS and Android Devices
- ✓ Physical Extractions of iOS Devices using Lantern Lite
- ✓ Logical extraction via USB and Network of Android Devices
- ✓ Acquisition of Macs

- ✓ Passcode recovery of iOS Devices, A4 SOC and older
- ✓ Importation of Call Detail Records
- ✓ File signature analysis
- ✓ Global and local keyword searching
- ✓ HTML, PDF, and Mobile iPad Reports
- ✓ Exports to CSV and Google Earth
- ✓ Kik Messenger is a permanent Artifact
- ✓ Integrated Plist viewer and file system viewer
- ✓ Hash set analysis

### *iXAM*

iXAM is a commercial Windows based software package for forensic analysis of Apple iPhones. It is composed of iXAM which is an imaging and extraction software and iXAMiner which is a data decoding tool

It performs a non-invasive data extraction, secures extraction by conducting forensic imaging in blocks, and can perform encryption cracking while maintaining an XML log file of all actions performed during the download process. During the analysis process, any new data created is stored in a completely separate folder tree, isolated from the input data.

### *BlackLight*

BlackLight is a commercial software for forensics analysis of Mac, Windows, iPhone or iPad, and Android. It is cross-platform and can analyze common internet artifacts as well as varied data structures such as time machine backup files, virtual images and Windows registry files.

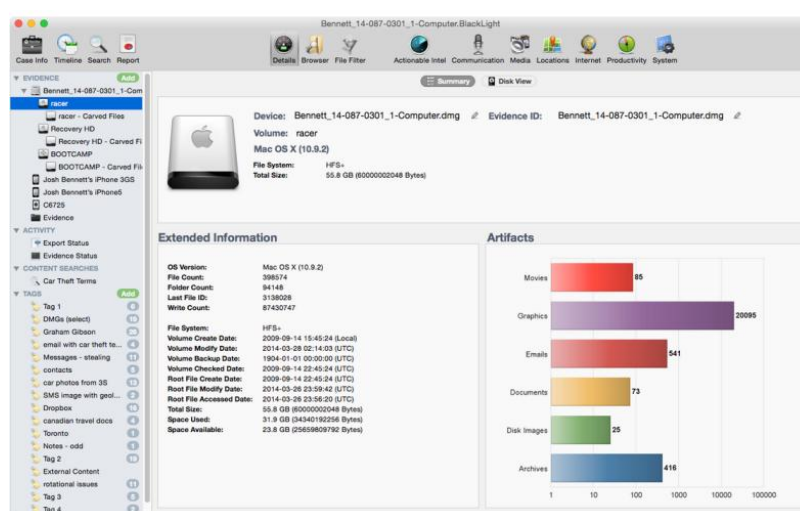


Figure 53 Mobilyze details view

BlackLight has the ability to acquire a snapshot of the device and displays configurations and usage for devices, including device type, OS version, serial

number, UDID, and IMEI. Furthermore, it provides an artifact summary statistics for documents, emails, movies, calls, voicemail, and shows the device user account information and common internet account information for applications such as Twitter and iCloud as well as recent usage history, including dialed phone numbers, last running applications, and most recent web-based location searches.

BlackLight's allows examiners to view traces of potentially important user activity from many disparate locations which are collected and organized. These include:

- ✓ Recently executed files and programs, drawn from the Windows registry, link files, jumplists, Prefetch and Superfetch
- ✓ Device connection data for all devices previously connected to the system, including USB device connection dates and times and the associated user account
- ✓ iOS device backups
- ✓ Recent file downloads
- ✓ Trash (for Mac OS X volumes) and Recycle Bin (for Windows volumes)
- ✓ Current and deleted user account info

BlackLight's has a signature File Filter view where filtering can be done according to the file name, kind, size, or extension, date created, modified, or accessed, picture metadata attributes, including GPS coordinates and camera type and positive and negative hash set filtering.

BlackLight's Media view allows the examiner to find any picture and video evidence. It has a Built-in GPS Mapping which can find all media files containing GPS data and can view media geolocation. Additionally, it has a proprietary skin tone analysis algorithm which can sort picture and video files by the skin tone percentage contained in the file and video frame analysis which allow examiners to prioritize video files in order to locate potential evidence.

Finally, BlackLight can recover every message from text services, messaging apps and social media, and can produce extensive reports in pdf, .html, .docx and .txt format.

BlackLight can be installed in Mac OS X Mountain Lion (10.8.0) or higher and Windows 7 or higher

### *UFED Link Analysis*

UFED Link Analysis is a commercial solution that unifies, correlates, highlights, and analyzes large volumes of disparate data from multiple data sources on a single platform.

UFED Link Analysis features are:

- ✓ Access a wide range of data types
- ✓ Reveal and visualize the connection between parties and identify relationships between suspects/victims in multiple views
- ✓ Highlight relevant case information
- ✓ Normalize the data into a single timeline view
- ✓ View all the connections and identify common locations on a single map
- ✓ Manage the data by tagging data items with customized tags
- ✓ Create reports

### *Mobile Phone Examiner Plus*

Mobile Phone Examiner Plus is a commercial Windows based tool for reviewing mobile device data. Additionally, data extracted from mobile devices can be imported into an FTK case. It can extract information such as phone and address book data, media files, call logs, SMS and MMS messages, calendar, and file system data stored in the memory of a mobile device.

### *UFED Physical Analyzer*

UFED Physical Analyzer is a commercial application for data analysis and reporting. It enables users to present extracted data and passwords.

Some of its features are:

- ✓ File system and physical extractions, including simple passcode recovery are supported for iOS devices
- ✓ Decode a wide range of applications
- ✓ Reveal much more deleted data by carving from unallocated space
- ✓ Generate and customize reports in multiple formats
- ✓ Visualize mobile data with project analytic and timeline tools
- ✓ Reduce manual carving using an automatic decoding process

### *iPhone Backup Analyzer*

iPhone Backup Analyzer is an utility designed for browsing the backup folder of any iOS device. It parses the backup directory and shows the decoded filesystem tree. Thus, it shows the configuration files, browse archives, lurk into databases and their properties

### *DS 7*

DS 7 is a commercial tool that supports logical, physical, and file system acquisitions, as well as password bypassing for mobile devices. It supports

- ✓ Logical and file system acquisitions
- ✓ IOs, Windows, Android phone, pda and tablet
- ✓ SIM cloning and analysis

- ✓ Malware detection
- ✓ Case comparer
- ✓ Hex viewer
- ✓ Physical acquisition
- ✓ Password bypassing
- ✓ Import gps, kml files and cell tower records
- ✓ Deleted data recovery
- ✓ Link analysis
- ✓ Hash Validation

## 7.4. Macintosh Forensic tools

This section contains forensic tools designed only to run in Mac computers.

### *RECON*

RECON for Mac OS X is commercial Mac forensics forensic suite. It includes bootable forensic imager and a software write-blocker.

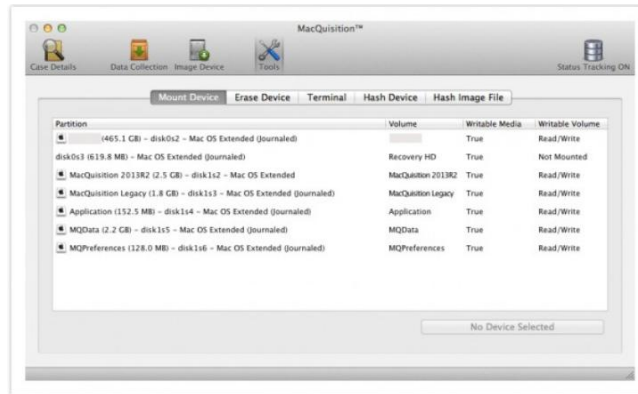
RECON's features are:

- ✓ Timeline analysis.
- ✓ Process forensic images or live Macs.
- ✓ Identify the origin of files.
- ✓ Automatic chat timeline construction for messages and skype.
- ✓ Image mounting supporting popular forensic image formats and fusion drives.
- ✓ Built-in live imaging.
- ✓ Automatic identification of spoliation artifacts.
- ✓ Create customized reports in pdf, html, csv and xml format.
- ✓ Image ram, capture volatile data.

### *MacQuisition*

MacQuisition is a commercial suite for live data acquisition, targeted file collection, and forensic imaging for Mac OS X





**Figure 54 MacQuisition**

MacQuisition acquires data from Macintosh computers but doesn't image iPhone or iPad devices. It runs on the Mac OS X operating system and safely boots and collects data from Xserve, Mac, iMac, Mac mini, MacBook, and MacBook Air computers in their own native Mac OS X environment by booting directly from the MacQuisition USB key.

The MacQuisition features are:

- ✓ Target and forensically acquire files, folders, and user directories while avoiding known system files and other unresponsive data.
- ✓ Preserve valuable metadata by maintaining its association with the original file.
- ✓ Authenticate collected data using any or all MD5, SHA-1, or SHA-256 hash functions.
- ✓ Logs data acquisitions and source device attributes throughout the collection process.
- ✓ Acquires email, chat, address book, calendar, and stickies on a per user, per volume basis.
- ✓ Capture live data such as Internet, chat, and multimedia files in real time.
- ✓ Acquires and save volatile RAM contents to a destination device.
- ✓ Logs live data acquisition information throughout the collection process.
- ✓ Boots from the MacQuisition USB dongle to use the source machine's own system to create a forensic image.
- ✓ Write-protect source devices while maintaining read-write access on destination devices.
- ✓ Logs forensic image acquisition processes, disk and volume attributes, and corresponding hash values.

### **MacForensicsLab**

MacForensicsLab is a commercial tool designed for data recovery and analysis. It maintains and protected evidentiary integrity by producing a bit-for-bit exact replica

of the original media, even with corrupted media. These forensic images are created with integrated segmenting and granular hashing. Moreover, it can find, preview and recover deleted and embedded files and even from swap and unallocated space. The keyword analysis and cataloging includes MD5, SHA-1, and SHA-256 checksum calculations.

The features of MacForensicsLab are:

- ✓ Media acquisition and data recovery.
- ✓ Multiple operations can be simultaneously.
- ✓ Acquisition of devices that retain every detail of the original media.
- ✓ Attempts to recover data even when the drive is damaged.
- ✓ Perform forensic acquisition and analysis on drives from Mac, Microsoft Windows, Linux.
- ✓ The Skin Tone Analyzer and fast traversal with file filtering.
- ✓ Built-in SQL database engine.
- ✓ Built-in file viewing to preview documents.

### *MacImager*

MacImager is a commercial Mac OS X based imaging tool. This tool aims to capture evidence from drives or media for later analysis, in the form of disk images. It doesn't depend on device and file system and uses a proprietary fault tolerant acquisition to bypass disk errors in order to obtain as much valid data as possible.

MacImager's features are:

- ✓ Complete device imaging.
- ✓ Supports all file systems such as HFS, NTFS, FAT, FAT32, and Linux.
- ✓ MacImager works with USB key, PC disk, Linux disk, FAT32 disk, FLASH card, Digital Cameras, and almost any other media or file system that can be recognized in Mac OS X.
- ✓ Image drive in device level.
- ✓ Fault tolerant acquisition that works around disk errors to create disk image.
- ✓ Independent of operating system.
- ✓ MD5 hash support.
- ✓ Images acquired are saved in open ISO standard and can be read by many Mac applications.

### *SpeedImager*

SpeedImager is a commercial Mac OS X based drive acquisition software. It limits the imaging to areas within existing data, and ignores sectors with deleted files and empty space. It copies all information to a disk image while skipping all space with

no data in order to improve the speed of the copy process and to save space for the disk storage, therefore can't retrieve deleted data.

SpeedImager's features are:

- ✓ Supports quick acquisition of Mac OS X volumes
- ✓ Compatible with media and drives that can be mounted on a Mac including SATA, USB, FireWire, and Thunderbolt hard disk
- ✓ Uses a proprietary disk image format
- ✓ Image existing partition using quick and efficient algorithm.
- ✓ Proprietary drive image may be restored to a disk or partition.
- ✓ USB 3 and Thunderbolt support.

### *Volafox*

Volafox is an open source forensics toolkit for Mac OS X for analyzing Mac's RAM images. The tool is written in python and allows investigating security incidents and finding information for malwares and any malicious program on the system.

Volafox can provide following information:

- ✓ Mac Kernel version, CPU, and memory specification
- ✓ Mounted filesystems
- ✓ Kernel Extensions listing, process listing and task listing
- ✓ Syscall table and mach trap table (Hooking detection)
- ✓ Network socket listing (Hash table)
- ✓ Open files listing by process
- ✓ Show Boot information
- ✓ EFI System Table, EFI Runtime Services
- ✓ Print a hostname

### *SubRosaSoft File Copier*

SubRosaSoft File Copier is a commercial Mac OS X file copy tool designed for e-discovery and digital forensics. The copying tool comes with presets to copy files from common locations such as address book, calendars, keychain, system cache, pictures, movies, email messages, and desktop folder

SubRosaSoft File Copier's features are:

- ✓ Supports all drive interfaces.
- ✓ Retains folder structures of the original sources.
- ✓ Files copied are hashed to guarantee the copied versions are identical to the originals.

## SoftBlock

SoftBlock is a commercial software write-blocking tool that runs on Mac OS X forensic analysis machines. It can identify recently attached hardware devices, and mounts the device with read-only or read-write permissions according to user preference. Additionally, provides preview of the data contained on devices before data is imported and blocks data transfer at the kernel level.

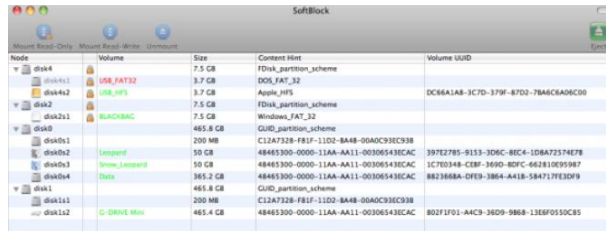


Figure 55 SoftBlock

The SoftBlock features are:

- ✓ Can handle as many hardware devices as a forensic analysis machine allows.
- ✓ No additional hardware is necessary.
- ✓ Mount and preview multiple external devices.
- ✓ Runs in the background.

## MacEntry

MacEntry is a commercial Macintosh application for acquiring the automatic login passwords of Mac OS X based computers.

After start-up, the user will be presented with the MacEntry splash screen. Once this has disappeared, the user will be taken to the 'Main Window'. Under Devices, the user will find the name of the volume, the user name, and the password if automatic login on that drive is enabled.

## Write Controller

Write Controller is a commercial software write-blocker for preventing a Mac from automatically mounting volumes. Thus, ensures the integrity of data and provides a layer of protection when working with evidence. Furthermore, it offers increased security, flexibility, and speed in imaging, previewing and analyzing evidence on Mac workstation.

## LANTERN Imager

Lantern Imager is a free GUI based imaging application for Mac computers. It can create images of all external media and also has a built in a write blocker. The media that can be imaged are Mac computers in FireWire/Thunderbolt Disk Mode, any hard drive, USB thumb drive and external USB drive, and any SD cards including those from Android cell phones and GoPro's

### *DMG Assist*

DMG Assist is a free Mac OS X tool for mounting DMG image files. It is needed to mount disk images when they won't mount with the traditional method. This tool uses a shadow mounting process that mounts dmgs read-only, allowing to shadow mount a disk image without the negative effects of data changes that occur with the normal shadow mounting process.

### *DMG Correct*

DMG Correct is a free Mac OS X utility for correcting full iPhone images so they will mount as dmgs. This tool essentially corrects the partitioning structure of a copy, allowing both the system and data partitions to be mounted.

### *Epoch Converter*

Epoch Converter is a free Mac OS X utility for converting raw timestamp integers to human-readable local and UTC timestamps so that the investigator can easily navigate between epochs and real times in both local and UTC.

### *DMG Rename*

DMG Rename is a free Mac OS X utility for renaming RAW image files to a .dmg extension so they can be processed from tools for Mac systems. In addition, it allows converting .dmg files and to raw files.

### *LockMaster*

LockMaster is a free Mac OS X utility for locking and unlocking multiple files simultaneously using the HFS+ locked flag. It offers the ability to lock individual items or select an entire folder and lock all the items within that folder.

### *IOReg Info*

IOReg Info is a free Mac OS X utility for displaying the Mac OS X Input/Output registry which describes all items connected to the computer. This tool can be used to locate partition information, including sizes, types, and the bus to which the device is connected. Furthermore, it can display various media class types, as well as all the information available via IOReg. The results may be saved to reports.

### *PMAP Info*

PMAP Info is a free Mac OS X utility for displaying the partition map of a specified device and can be used to retrieve all drive information, accounting for all used sectors.

### *MetaData Extractor*

MetaData Extractor is a free Mac utility for extracting metadata from files and map location data on Google Maps

### *DD Converter*

DD Converter is a commercial Mac application for converting dd images to Macintosh dmg image. It can also be used the reverse procedure, to convert Apple DMG format to DD disk images

### *Evidence Collector*

Evidence Collector is a free Mac utility for collecting a selected folder and creating a locked DMG

### *Dirty Mounter*

Dirty Mounter Application is a free Mac tool to force mount a DMG that otherwise won't mount because of a corrupt file system or volume.

## **7.5. Forensic Distributions**

### *Santoku*

Santoku is a free live distribution dedicated to mobile forensics, analysis, and security. It has a bootable Linux environment with preinstalled platform SDKs, drivers and utilities, preconfigured GUI frameworks, such as PyGTK to support GUI tools for deployment and control of mobile apps and auto detection and setup of new connected mobile devices.

It contains tools to forensically acquire and analyze data, firmware flashing tools for multiple manufacturers, imaging tools for NAND, media cards, and RAM, free versions of some commercial forensics tools, and scripts and utilities specifically designed for mobile forensics. Furthermore, it includes tools for examining mobile malware, mobile device emulators, utilities to simulate network services for dynamic analysis, tools for decompilation and disassembly, and access to malware databases.

For mobile forensics, it contains tools such as AFLogical Open Source Edition, Android Encryption Brute Force, BlackBerry Desktop Manager, iPhone Backup Analyzer, ExifTool, libimobiledevice, scalpel, Sleuth Kit, and SQLiteSpy.

Santoku security tools includes utilities for wireless analyzers, reverse engineering, and penetration testing. Along with nmap, BurpSuite, and Metasploit, w3af Console, Ettercap, SQLmap, SSLstrip, and other penetration testing tools. Reverse engineering tools such as APK Tool Flawfinder, and Java Decompiler are included as well as Wireshark and Kismet for network testing, and ChaosReader, which is used to view mobile traffic on a packet level.

### *Helix 3 Pro*

The Helix 3 Pro is a commercial Live CD based on Linux that was built to be used in incident response, computer forensics and e-discovery. It includes various tools for

forensics tasks such as make forensic images of all internal devices, of physical memory, search filesystem for specific file types, determine if disk level encryption is turned on, hex editors, data carving and password cracking.

### *Masterkey*

The Masterkey Linux is a free bootable Linux live operating system based on Slackware. It focuses on incident response and computer forensics and it contains a various range of free and open source tools that can be used for incident response and investigation. The distribution is also installable.

The Masterkey comes with a collection of forensics tools for imaging, data carving, forensic analysis and network analysis, as well as other applications including: editors, office suite, multimedia tools, file and disk management tools. Disk partitions are not mounted automatically, in order to prevent accidental writing to the evidence disks and therefore contaminating the evidence. When mounted, the disk partition will be mounted as read-only. The mounting and use of swap partitions is not allowed to prevent evidence destruction. The user logs in as an administrator, so that tools requiring root privilege can be used directly. The graphic user interface doesn't start automatically, and provides the options of a KDE or Fluxbox desktops.

### *Digital Evidence and Forensics Toolkit (DEFT)*

The DEFT is a free LINUX-based Live CD distribution of multiple tools for forensics and evidence capture process. It can perform acquisition and preservation of mass storage or telematic traffic over IP networks; and case analysis and their management. Included in the kit is the *Digital Advanced Response Toolkit* with freeware windows computer forensic tools.

### *CAIN*

CAIN is a free computer forensics/incident response Linux-based bootable Live system on CD, DVD or USB flash drives that assembles a collection of open source security tools. It's a Live Linux Distribution, which means it runs from a bootable CD in memory without changing the native operating system of the host computer.

### *SANS Investigative Forensic Toolkit (SIFT)*

The SANS Investigative Forensic Toolkit is a computer forensics VMware appliance that is pre-configured with all the necessary tools to perform a detailed digital forensic examination. It is compatible with expert witness format (E01), advanced forensic format (AFF), and raw (dd) evidence formats.

### *PALADIN forensic suite*

PALADIN is a free live Linux distribution based on Ubuntu to perform forensics investigations in a forensically sound manner.

PALADIN Toolbox Key Features are:

- ✓ Image to several formats including .E01, .Ex01, .dmg and .dd, SMART, AFF and VMDK
- ✓ Clone devices
- ✓ Creates two forensic images or clones at the same time
- ✓ Image across a network
- ✓ Format drive as NTFS, HFS+, FAT32 or EXT4 and ExFAT
- ✓ Create a forensic image of only the unallocated space, free space and file slack
- ✓ Search and preview media by file name, keywords or MIME types.
- ✓ Pre-compiled open source forensic tools

### **SMART Linux**

*SMART Linux* is a commercial a universal image, customized and designed for Data Forensics, Electronic Discovery and Incident Response. It produces clean, non-invasive, forensically operations. It is essentially multiple versions of Live CDs customized for forensic work.



## 8. Conclusion

As presented in this project there are many tools available, both open source and commercial, for conducting a successful digital investigation and incident response, provided there are professionals with the expertise, training and technical knowledge to use them at their full potential. This naturally, must be combined with an industry's compliance to the instructions of its security administrator and take all the necessary measures to protect its systems.

Nonetheless, the field of digital forensic and security incident response is and will remain of particular interest for the years to come. New devices and services will lead to the creation of new tools that will need trained experts to handle them.

In June 2014, Macfee issued a study where the annual cost of cyber crime to the global economy is estimated around 400 billion dollars. Having in mind that cybercrime is in fact an industry that will continuously grow since it has low risk but significant incomes, this number is expected to grow. In addition, every new and powerful technology adopted by business or consumers is also available to offenders. As technology evolves new and more sophisticated types of attacks and anti-forensic measures are discovered. After all, there's always been a constant confrontation between cyber-offenders and security specialists regarding new attacks or harmful software and the defenses against them. Furthermore, storage capacity of media and memory increases rapidly, along with the computational power and the amount of possible data evidence sources. Additionally, the variety of data sources increases significantly when an investigation involves social media and furthermore when several participants are involved. Thus, the amount of data collected and analyzed during an investigation is dramatically increasing as well. In the future, it will be quite challenging, with the current digital investigations processes, and procedures to analyse such a vast amount of data in reasonable time while preserving forensic principles so that the results could be presented in a court of law.

## TOOL INDEX

AD Lab, 73  
Android Connections Forensics, 113  
Argus, 96  
Binwalk, 64  
BlackLight, 117  
Bro and BroBox, 101  
Bulk Extractor, 46  
CapAnalysis, 108  
Capstone, 90  
CaseFile, 110  
Catfish, 87  
chkrootkit, 90  
chntpw, 91  
Clonezilla, 49  
Cloud Extractor, 52  
Cryptcat, 110  
Cuckoo, 90  
dc3dd, 45  
dcfldd, 46  
DD Converter, 126  
Ddrescue, 86  
DEFT, 127  
DFF, 55  
Dhash, 88  
Dirty Mounter, 126  
Distributed Network Attack, 87  
DMG Assist, 125  
DMG Correct, 125  
DMG Rename, 125  
DriveImage XML, 52  
Dropbox Decryptor, 88  
DS 7, 119  
Dump Data, 45  
Dumpzilla, 67  
Elcomsoft Blackberry Backup Explorer Pro, 115  
Elcomsoft Explorer for WhatsApp, 115  
Elcomsoft iOS Forensic Toolkit, 115  
Elcomsoft Mobile Forensic Bundle, 115  
ElcomSoft Password Recovery Bundle, 88  
Elcomsoft Phone Breaker Forensic, 115  
Elcomsoft Phone Viewer, 115  
Email Examiner, 78  
EnCase Forensic, 55  
EnCase Forensic Imager, 43  
Encrypted Disk Detector, 78  
Epoch Converter, 125  
Ettercap, 102  
Evidence Center, 64  
Evidence Collector, 126  
Exiftool, 67  
extundelete, 86  
Fiddler, 100  
Field Agent, 71  
Findwild, 68  
Foremost, 85  
Forensic Emule Analyzer, 86  
Forensic Replicator, 52  
FRED, 60  
F-Response TACTICAL, 111  
FTK, 59  
FTK Imager, 44  
Goldfish, 79  
Google Maps Tile Investigator, 75  
Grok-NTFS, 63  
GRR Rapid Response, 76  
Guymager, 49  
Helix3 Pro, 126  
Hex Editor Neo, 64  
iBored, 65  
iLook, 58  
InfinaDyne CD/DVD Inspector, 66  
IOReg Info, 125  
iOS Forensic Toolkit, 116  
iPhone Backup Analyzer, 119  
IRCR, 72  
iXAM, 117  
John the Ripper, 89  
LANTERN, 116  
LANTERN Imager, 124  
LiME, 112  
Linux Memory Grabber, 81  
Live RAM Capturer (Belkasoft), 80  
LockMaster, 125  
Log Parser, 65  
MacEntry, 124  
MacForensicsLab, 121  
MacImager, 122  
MacLockPick, 77

MacQuisition, 120  
Maltego, 110  
Masterkey, 127  
Md5deep, 88  
MetaData Extractor, 125  
Microsoft Message Analyzer, 103  
Mobile Phone Examiner Plus, 119  
Mobilyze, 112  
MoonSols Windows Memory Toolkit, 81  
Mount Image Pro, 90  
Nagios Incident Manager, 74  
Nagios Log Server, 71  
Nagios XI, 105  
Netcat, 110  
NetFSE, 97  
Network Analyzer, 106  
Network Email Examiner, 78  
NetworkMiner, 107  
Nmap, 93  
NTLast, 103  
OSFClone, 48  
OSForensics, 60  
Oxygen Forensic, 114  
P0f, 109  
P2C, 79  
PALADIN, 127  
Paragon Backup and Recovery, 48  
Passware Kit Forensic, 50  
Password Recovery Toolkit, 87  
pdfid, 79  
pdf-parser, 79  
pdgmail, 79  
peepdf, 79  
Plan:C, 113  
PMAP Info, 125  
ProcDump, 89  
ProDiscover, 57  
RAMMap, 83  
rapier, 72  
ReclaiMe File Recovery, 86  
RECON, 120  
Reflect, 51  
Registry Browser, 62  
Registry Viewer, 62  
RegRipper, 62  
Rekall, 82  
Santoku, 126  
SAW, 51  
Second Look, 83  
SIFT, 127  
Sleuth Kit / Autopsy, 52  
SMART for Linux, 57  
SMART Linux, 128  
SmartMount, 63  
Snort, 94  
SoftBlock, 124  
SpeedImager, 122  
SubRosaSoft File Copier, 123  
Summation, 63  
TcpDump, 98  
TCPView, 98  
UFED 4PC, 113  
UFED Cloud Analyzer, 114  
UFED Link Analysis, 118  
UFED Physical Analyzer, 119  
Vinetto, 78  
Volafox, 123  
Volatility, 81  
Web Agent, 89  
Windows Forensic Toolchest, 73  
WindowsSCOPE Cyber Forensics, 84  
Wireshark, 91  
Write Controller, 124  
xmount, 50  
Xplico, 95  
Xprobe2, 99  
X-Ways Forensics, 69  
X-Ways F-Response, 70  
X-Ways Investigator, 70  
X-Ways WinHex, 68

## 9. BIBLIOGRAPHICAL REFERENCES

Altheide, Cory, and Harlan Carvey. *Digital Forensics with Open Source Tools: Using Open Source Platform Tools for Performing Computer Forensics on Target Systems: Windows, Mac, Linux, Unix, etc.* Elsevier, 2011.

Ballou, Susan. *Electronic crime scene investigation: a guide for first responders.* Diane Publishing, 2010.

Carrier, Brian. *The Sleuthkit and Autopsy.* 2008.

*Charter of Fundamental Rights of the European Union.* Office of the Europ. Union, 2010.

Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. *Computer security incident handling guide.* NIST Special Publication 800, 2012.

Cohen, Michael, D Bilby, and G Caronni. *Distributed forensics and incident response in the enterprise.* digital investigation , 2011.

*Computer Forensics: Investigating Network Intrusions and Cybercrime.* EC-Council, 2010.

Council of Europe, European Court of Human Rights. *European Convention of Human Rights.* Strasbourg, 2010.

Dudley, Alfreda. *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices.* IGI Global, 2011.

*Framework Directive (2009-140-EC).* 2009.

Freiling, Felix C, and Bastian Schwittay. *A Common Process Model for Incident Response and Computer Forensics.* IMF 7, 2007.

Garfinkel, Simson L. *Digital forensics research: The next 10 years.* digital investigation 7, 2010.

Johnson, Leighton. *Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response.* 1st Edition. Newnes, 2013.

Kent, Karen, Suzanne Chevalier, Tim Grance, and Hung Dang. *Guide to integrating forensic techniques into incident response.* NIST Special Publication, 2006.

Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. *Organizational models for computer security incident response teams (CSIRTs).* No. CMU/SEI-2003-HB-001. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST,, 2003.

Kral, Patrick. *Incident Handler's Handbook.* InfoSec Reading Room, 2012.

Ligh, Michael Hale, Andrew Case, Jamie Levy, and Aaron Walters. *The art of memory forensics: detecting malware and threats in Windows, Linux, and Mac memory*. John Wiley & Sons, 2014.

Luttgens, Jason T, and Mathew Pepe. *Incident response & computer forensics*. McGraw-Hill/Osborne, 2014.

Malin, Cameron H, Eoghan Casey, and James M Aquilina. *Malware Forensics Field Guide for Linux Systems*. Newnes, 2013.

Manson, Dan, Anna Carlin, Steve Ramos, Alain Gyger, Matthew Kaufman, and Jeremy Treichelt. *Is the open way a better way? Digital forensics using open source tools*. 40th Annual Hawaii International Conference on. IEEE, 2007.

McAfee. *Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II*. McAfee, 2014.

Nelson, Bill, Amelia Phillips, and Christopher Steuart. *Guide to computer forensics and investigations*. Cengage Learning, 2015.

Newman, Robert C. *Computer forensics: evidence collection and management*. CRC Press, 2007.

Pule, Dina. *Electronic Communications and Transactions Amendment Bill*. 2012.

*Reform of the Data Protection Directive*. Brussels: European Commission, 2012.

Sammons, John. *The basics of digital forensics: the primer for getting started in digital forensics*. Elsevier, 2012.

Sara, Hart V, John Ashcroft, and Deborah J Daniels. *Forensic examination of digital evidence: a guide for law enforcement*. Washington DC, USA: National Institute of Justice, 2004.

Shavers, Brett, and Eric Zimmerman. *X-Ways Forensics Practitioner's Guide*. Newnes, 2013.

Shinder, Debra Littlejohn, and Michael Cross. *Scene of the Cybercrime*. Syngress, 2008.

West-Brown, Molra J, Don Stikvoort, and Klaus-Peter Kossakowski. *Handbook for computer security incident response teams*. (No. CMU/SEI-2003-HB-002). Carnegie-mellon univ pittsburgh pa software engineering inst, 2003.

Witter, Franklin. *Legal Aspects of Collecting and Preserving Computer Forensic Evidence*. Bethesda, Maryland: InfoSec Reading Room, SANS Institute, 2001.

[Links](#)

(Last Accessed November 2015)

168/2014, Article from Issue. *Linux Magazine*. <http://www.linux-magazine.com>.

*AccessData: E-Discovery & Computer Forensics*. <http://accessdata.com>.

*AppleExaminer*. <http://www.appleexaminer.com>.

*ArxSys*:. <http://www.arxsys.fr>.

*ASR Data | Data Forensics Software, Services and Training*. <http://www.asrdata.com>.

*Belkasoft: Evidence Search and Analysis Software*. <https://belkasoft.com>.

*Binwalk | Firmware Analysis Tool*. <http://binwalk.org/>.

*BitPim*. <http://www.bitpim.org/>.

*BlackBag Technologies: Mac, iPad, and iPhone Forensics*. <https://www.blackbagtech.com>.

blog, Web Upd8: Ubuntu / Linux. <http://www.webupd8.org>.

*CapAnalysis | PCAP from another point of view*. <http://www.capanalysis.net/>.

*Capstone - The Ultimate Disassembly Framework*. <http://www.capstone-engine.org/index.html>.

*celebrite.com - UFED logical*. <http://www.celebrite.com>.

*chkrootkit -- locally checks for signs of a rootkit*. <http://www.chkrootkit.org/>.

*Clonezilla*. <http://clonezilla.org>.

*Cuckoo Sandbox: Automated Malware Analysis*. <http://www.cuckoosandbox.org>.

*DEFT Linux - Computer Forensics live CD*. <http://www.deflinux.net>.

*Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009*.  
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF>.

*dumpzilla forensic tool*. <http://www.dumpzilla.org/>.

*e-fense :: Cyber Security & Computer Forensics Software*. <http://www.e-fense.com>.

*Elcomsoft*. <https://www.elcomsoft.comElcomsoft>.

*Ettercap Home Page*. <https://ettercap.github.io>.

*ExifTool by Phil Harvey - SNO*. <http://www.sno.phy.queensu.ca/~phil/exiftool/>.

*extundelete: An ext3 and ext4 file undeletion utility.* <http://extundelete.sourceforge.net/>.

*Fool Moon Software & Security.* <http://www.foolmoon.net>.

*Framework Directive (2009-140-EC).* 2009.

*FRED, XMOUNT.* <https://www.penguin.lu>.

*Free Linux Downloads - Softpedia.* <http://linux.softpedia.com>.

*Free Open Source Software - SourceForge.net.* <http://sourceforge.net/projects>.

*Free Tools | McAfee Downloads.* <http://www.mcafee.com/us/downloads/free-tools/index.aspx>.

*F-Response - Extend Your Arsenal.* <https://www.f-response.com>.

*Guidance Software - Endpoint Data Security, eDiscovery ...*  
<https://www.guidancesoftware.com>.

*Guymager homepage - SourceForge.* <http://guymager.sourceforge.net/>.

*ILookIX: Perlustro.* <http://www.perlustro.com>.

*Infinadyne Content Selection.* <http://www.infinadyne.com>.

*iPhone Forensics - iXAM - Advanced iPhone Forensic.* <http://www.ixam-forensics.com/>.

*iSEC Partners - NCC Group.* <https://www.isecpartners.com>.

*Katana Forensics.* <https://katanaforensics.com>.

*Lizard Labs - Software for Microsoft and Professional ...* <http://www.lizard-labs.com>.

*Lock and Code: Home.* <https://lockandcode.com>.

*MacForensicsLab, Cross platform forensics and e-discovery ...*  
<http://www.macforensicslab.com>.

*Macrium Software.* <http://www.macrium.com>.

*Magnet Forensics Inc.* <https://www.magnetforensics.com>.

*Masterkey Linux.* <http://masterkeylinux.com>.

*MoonSols.* <http://www.moonsols.com>.

*Nagios - The Industry Standard In IT Infrastructure Monitoring.*  
<https://www.nagios.com>.

*Nmap: the Network Mapper - Free Security Scanner.* <https://nmap.org>.

*Offline Windows Password & Registry Editor - Pogostick.net.*  
<http://pogostick.net/~pnh/ntpasswd/>.

*Openwall - bringing security into open computing.* <http://www.openwall.com>.

*OSForensics - Digital investigation for a new era.* <http://www.osforensics.com>.

*Oxygen Forensics - Mobile forensics solutions.* <http://www.oxygen-forensic.com>.

*Paraben Corporation - Mobile Forensics & Computer ...* <https://www.paraben.com/>.

*Paragon Software Group.* <http://www.paragon-software.com>.

*Passware: Password Recovery.* <https://www.passware.com>.

*Paterva / Maltego.* <http://www.paterva.com>.

*ReclaiMe File Recovery Software.* <http://www.reclaime.com/>.

*Rekall Memory Forensic Framework.* <http://www.rekall-forensic.com/index.html>.

*Runtime Software.* <https://www.runtime.org>.

*Santoku Linux.* <http://santoku-linux.com>.

*Second Look | Linux Memory Forensics, Detect Advanced...*  
<http://secondlookforensics.com>.

*Snort.Org.* <https://www.snort.org/>.

*SUMURI LLC.* <https://www.sumuri.com>.

*TCPDUMP/LIBPCAP public repository.* <http://www.tcpdump.org>.

*Telerik Mobile App Development Platform, .NET UI Controls ...* <http://www.telerik.com>.

*The ARC Group of NY.* <http://www.arcgroupny.com>.

*The Bro Network Security Monitor.* <https://www.bro.org/>.

*The Sleuth Kit (TSK) & Autopsy: Open Source Digital ...* <http://www.sleuthkit.org/>.

*The Volatility Foundation - Open Source Memory Forensics.*  
<http://www.volatilityfoundation.org>.

*Tools | eternal-todo.com.* <http://eternal-todo.com/tools>.



*Ubuntu Geek | Ubuntu Linux Tutorials,Howtos,Tips & News .*  
<http://www.ubuntugeek.com>.

*Ubuntu Manpage.* <http://manpages.ubuntu.com>.

*What Skills Are Needed When Staffing Your CSIRT?* [http://www.cert.org/incident-management/csirt-development/csirt-staffing.cfm?](http://www.cert.org/incident-management/csirt-development/csirt-staffing.cfm)

*WindowsSCOPE: Windows Memory Forensics,.* <http://windowsscope.com/>.

*Wireshark · Go Deep.* <https://www.wireshark.org/>.

*Xplico - Open Source Network Forensic Analysis Tool (NFAT).* <http://www.xplico.org>.

*X-Ways Software Technology AG.* <http://www.x-ways.net>.