European Commission
Directorate-General Home Affairs
Prevention of and Fight against Crime Programme

HOME/2010/ISEC/AG/INT/002

ForToo – Forensic Tools against Illegal Use of the Internet

D0: Requirements Analysis

Workpackage:	WP0: Requirements Analysis
Contractual delivery date:	31 Oct 2011
First publication date:	29 Jan 2012
Actual delivery date:	04 Apr 2012
Leading partner:	AEGIS RESEARCH
Contributing partners:	FORTH
Editor:	Vassilis Prevelakis
Contributors:	Sotiris Ioannidis, Nikos Toulios
Internal Reviewers:	Theo Tryfonas
Version:	1.0

Executive Summary:

In this deliverable we present our findings about the state of the art in digital forensics tools and techniques. Furthermore, we have interviewed experts in the field, from a variety of organisations, including ISPs, security companies, search providers, research institutions, etc. to provide guidelines about their needs and requirements in preventing, detecting and analysing network-based incidents. Using these inputs we have selected the areas where we intend to concentrate our efforts within the ForToo project and a set of requirements that our deliverables should meet.

With the support of the Prevention of and Fight against Crime Programme.
European Commission - Directorate-General Home Affairs

This project has been funded with the support of the *Prevention of and Fight against Crime* Programme of the European Commission - Directorate-General Home Affairs. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

REVISIONS AND QUALITY CONTROL

Version	Date	Lead contributor	Action summary
0.7	29 Jan 2012	Vassilis Prevelakis	Final draft circulation
0.8	22 Feb 2012	Theo Tryfonas	Review input
0.9	18 Mar 2012	Vassilis Prevelakis	Commit final to file repo
1.0	04 Apr 2012	Theo Tryfonas	Delivery to Home DG
1.1	TBD	Theo Tryfonas	Advisory Board feedback incorporation

1 Introduction

The term *digital forensics* has become popular only very recently. In earlier times the term "*computer forensics*," was used instead, but that has a more limiting scope: that of computers. Whereas *computer forensics* is defined as "the collection of techniques and tools used to find evidence in a computer" [Calo01], *digital forensics* has been defined as

"*the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations*" [Digi01].

As the popularity of the Internet increases, so does the number of miscreants who abuse the net for their nefarious purposes. Malicious actors come in many guises, terrorists, enemy states, organised crime, even petty criminals and script kiddies. In the past, illegal activities involved fast spreading worms taking over thousands of systems or large-scale, synchronised attacks against popular sites such as Amazon or Microsoft. Nowadays this has changed. The profiles and motives of attackers have changed. They now employ stealthy techniques, aimed at avoiding detection, quietly stealing or manipulating information, for profit, or other, more sinister goals. The European Internet, European information systems, European countries, and ultimately, Europe's citizens are targets and victims of such illegal activities. In our ongoing quest to secure our networks and systems we must first be able to detect and understand illegal actions as they happen and discover the attack infrastructures the miscreants are using, but also analyse and dissect the results of compromised systems.

To accomplish these goals it is necessary to create the appropriate tools that will help us in the above tasks. These digital network forensics tools must be designed in a way to enable the appropriate authorities to counter the developing threats landscape.

In order to arrive at the requirements of the work to be undertaken under this project we first have to define the problem area. We present this in the following section (section 2). Section 3 examines the requirements and the last section contains a preliminary design for the system that will be the key deliverable of the ForToo project. Additionally, in Appendix A we include a survey of computer forensics tools and techniques.

2 Problem Definition

In this section we define the problem. We ask the question what are the issues associated in digital forensics in the Internet. The scope of this work is quite large as what is considered "illegal" varies between jurisdictions. On-line gambling is a good example because it is not considered to be illegal in many legal jurisdictions. Even computer hacking is not considered a crime in some countries.

In the following paragraphs we delineate the problem through the examination of case studies, interviews with experts in the field and looking at the work that has already been carried out in various legal jurisdictions.

2.1 Interviews with the Experts

In order to have a more complete and clear view of the issues involved in detecting illegal activities in the Internet, we conducted a series of interviews with experts in the field. To get a well-rounded view, we selected those experts from a large cross-section of industry and also academia. Specifically from, law enforcement, legal experts, security companies, companies such as financial institutions that are likely to be the targets of attacks, CERTs, research institutions, etc.

To conduct these interviews we compiled, but were not limited to, a set of discussion points, which we used as guidelines. Here we summarise the core list of these points:

1. What is the most common digital forensic activity that you are engaged in?
2. Which, in your opinion, are the emerging threats?
3. What information would be useful to present to a user of the system?
4. What digital forensics tools are you familiar with and/or use regularly?
5. Which features of the digital forensics tools that you use you consider important and which additional functionality would you like to see implemented?
6. What are the criteria that you base your selection decision for a new digital forensics tool?
7. What are major activities in digital forensics (e.g. network analysis, computer memory analysis, code breaking, network monitoring etc.)?
8. Are criminals becoming better informed about computer forensics procedures and becoming more skilled at covering their tracks?

2.2 Case studies of illegal use of the Internet

In the next few paragraphs we present case studies as examples of the types of malicious activities that digital forensics investigators are likely to face.

2.2.1 Case Study 1: Vodafone-Greece Wiretaps.

In the run up to the 2004 Olympics an unknown group infiltrated the network of a Greek mobile operator (Vodafone) and carried out extensive wiretaps of various

highly placed individuals in the Greek government, security forces and industry. A cell phone used by the Greek Prime Minister himself was also tapped.

In this case, the intruders subverted the victim's system by installing software that allowed them complete access to the victim's system while remaining hidden from the casual inspections of administrators (rootkit).

Eventually, the intruders made a technical error which lead the mobile operator to ask Ericsson (the equipment manufacturer) to investigate, thereby bringing the affair into the open.

In the weeks and months that followed the discovery, the forensic analysis was hampered because key material was lost or was never collected. For instance, in July 2005, while the investigation was taking place, Vodafone upgraded two of the three servers used for accessing the exchange management system. This upgrade wiped out the access logs and, contrary to company policy, no backups were retained. Some time later a six-month retention period for visitor sign-in books lapsed, and Vodafone destroyed the books corresponding to the period where the rogue software was modified, triggering the errors that alerted the operator.

Traces of the rogue software installation might have been recorded on the exchange's transaction logs. However, due to a paucity of storage space in the exchange's management systems, the logs were retained for only five days, because Vodafone considered billing data, which competes for the same space, a lot more important. Most crucially, Vodafone's deactivation of the rogue software on 7 March 2005 almost certainly alerted the conspirators, giving them a chance to switch off the shadow phones. As a result investigators missed the opportunity of triangulating the location of the shadow phones and catching the perpetrators in the act. [Prev07] Once the infiltration was discovered, Vodafone had to balance the need for the continued operation of the network with the discovery and prosecution of the guilty parties.

The responses of Vodafone and that of Greek law enforcement left a lot to be desired. Through Vodafone's actions, critical data were lost or destroyed, while the perpetrators not only received a warning that their scheme had been discovered but also had sufficient time to disappear.

The response of Greek law enforcement officials was also inadequate. Police could have secured evidence by impounding all of Vodafone's telecommunications and computer equipment involved in the incident. Instead it appears that concerns about disruption to the operation of the mobile telephone network led the authorities to take a more light-handed approach – essentially interviewing employees and collecting information provided by Vodafone – that ultimately led to the loss of forensic evidence. They eventually started levelling accusations at both the operator (Vodafone) and the vendor (Ericsson), turning the victims into defendants and losing their good will, which further hampered their investigation.

2.2.2 Case Study 2: Unintentional Data Leaks

In this example we look at cases where, either though the use of 3rd party software (not necessarily malicious), or though lax security configuration, a user allows network access to the filesystem on his or her computer.

For example, a junior employee of the US Congress allowed data pertaining to the investigation of the Ethics Committee of the US House of Representatives on a number of members of Congress, to be leaked. The employee – who was later fired – copied the file with the data in the investigation to his home computer so that he could work from home. The employee did not, however, realise that since he was using "peer to peer file-sharing software" that file, along with other files on his hard disk would be accessible from the network. Eventually the file was made available to the Washington Post newspaper which publicised the incident. [Marg09]

Earlier in 2009, in a similar incident, a file containing details of the VH-60N Presidential Helicopter's CAAS avionics architecture, was also leaked via a file sharing network. Reports indicate that a high-level executive copied the confidential data to his laptop and then took them home, where the information was shared over a P2P network called Gnutella, which is actually an open source standard used by a number of file sharing programs. [Defe09]

2.2.3 Case Study 3: Detecting and decommissioning malicious sites

The following is an extract from the Verizon's 2011 Data Breach Investigation Report [Veri11]:

"In 2010, the Dutch National High Tech Crime Unit (NHTCU) decided to start a public-private partnership to combat botnets. Getting together with members of the CERT community, industry, and Internet infrastructure they devised a three stage approach, consisting of intelligence, intervention, and investigation. Project Taurus was born. All partners combined their state of the art botnet information and all botnets were tracked real time using a university-developed tool. The goal was a notice and takedown for most of the botnets and a deeper investigation into some of them. Then, one of the partners, a large Internet service provider, found a botnet command and control server in their infrastructure.

The partners started investigating and found a cluster of 143 malicious servers, seven of which were directly related to a botnet called Bredolab. At that point, Bredolab had been able to infect 30 million unique IP addresses. In a ten week period the partners were able to draw a picture of the botnet infrastructure based on the network traffic. They were also able to identify the suspected operator of the network, an Armenian who planned to come to the Netherlands for a dance party. The network was set to be dismantled on the day the Armenian would arrive at Amsterdam airport. The Armenian was to be arrested on arrival but due to visa problems he never showed up.

Instead, he noticed someone attacking his botnet, assumed it was a competitor and fought back. After trying several backdoors, he decided to DDoS what was left of his own botnet. Due to good international co-operation, the command and control server of the DDoS botnet was quickly dismantled. An Interpol red notice led to the arrest of the suspect the following day at Yerevan airport.

A piece of code was written and put on the botnet server to be downloaded by the bots. This code would cause a warning window containing cleaning instructions to pop up at the victims' computers. The law enforcement obligation of helping the victims was judged to precede potential judicial concerns in this action. The combination of creativity, new techniques, close co-operation, and hard work enabled the Taurus partners to go further than any of them would have been able to go alone."

2.2.4 Case Study 4: WiFi hotspot hijacking

In 2009 the life of a couple living in Minneapolis, USA, suddenly became very complicated. A number of incriminating messages had apparently been sent from the IP address of their home network. These messages implicated the couple in various illegal activities including child pornography, sexual harassment, various kinds of professional misconduct and even threatening e-mail messages addressed to politicians, including Vice President Joe Biden (a federal crime in the US).

These messages resulted in the issue being investigated by the Law firm that the husband was working for and eventually the US Secret Service (due to the emails regarding the vice president). With the permission of the couple, a private forensics firm installed a packet sniffer in the home network which eventually collected enough evidence to implicate the next door neighbour allowing the law enforcement authorities to get a search warrant for his house. The search revealed evidence that proved that the neighbour had cracked the password of the WiFi router of the couple and then used it to gain access to the home network which, in turn, allowed him to spy on the couple and send the incriminating emails from their IP address. [Krav11].

2.3 Illegal activities in the Internet

Based on the above we can roughly segregate illegal activities in two categories, the key distinction being whether "hacking" is involved. In the non-hacker category the criminals use the network as a tool, a glorified typewriter–filing cabinet, so to speak. This category includes people who collect and distribute illegal material (child pornography, pirated material etc.), run illegal on-line gambling sites and so on. The second category includes the hackers. Here we have activities that involve penetration of computer system or network defences in order to install malware or carry out denial of service attacks. Countermeasures proposed over the years include passive defences (e.g. firewalls, malware detection systems, etc.), *network traceback* [Sava00] (where we attempt to follow the path of the attack upstream towards the attacker), "organic" responses of the network fabric itself (e.g. *pushback* [Ioan02] where the network responds to malicious flows using its built-in congestion-avoidance mechanisms), and so on.

Scale is also a problem. What may start as a simple DOS attack may escalate into full-blown cyber-warfare as in the case of Estonia. Both national and international organisations have instituted actions to protect against large-scale attacks, e.g. security audits (US DHS), mock cyber attacks (NATO), response centre against cyberthreats (ITU).

However, all these efforts leave the "little guy" out in the cold. Law enforcement is often playing technological catch up with the criminals and not doing particularly well at that. "*Computer forensics are hugely expensive and laborious, and police investigating major e-crimes will need access to specialised and well-equipped forensic laboratories*" [HoL006]. A similar situation exists in the UK, as indicated by Deputy Assistant Commissioner Janet Williams who works in the Metropolitan Police's Specialist Crime Directorate.[Blin09]

A common point that was carried across by most people interviewed was that law enforcement is fighting a losing war. New threats emerge all the time, while more

people keep trying their hand in more traditional areas of attack. For example, consider the so-called *Nigerian scam*[1] where we still have people falling for it, despite the wide publicity given and the many warnings issued by law enforcement authorities and public interest groups.

To make matters worse, scarce investigators are allocated to high visibility cases such as child pornography and related crimes, leaving few resources for computer intrusions.[2] At the same time "intrusions into corporate networks, personal computers and government systems are occurring every single day by the thousands."[3]

Another aspect of the problem is the technological divide. Although described as an arms race, a better description is of a playing field that is changing continuously. E.g. complex software systems for analysing hard drives of Windows-based systems are useless against proprietary devices such as digital video recorders or network-based hard drives.

Digital forensics is entering a new era mainly because we are leaving behind the Windows/Intel (Wintel) monoculture. Despite the security implications of having all our services based on a single platform, the Wintel monoculture implied that digital forensics experts only needed to specialise (and be concerned with) just the Wintel platform. Although different platforms always existed (e.g. Linux), the past few years we are noticing the presence of many alternate platforms. In addition to Linux, Apple's OSX is also gaining market share in the traditional operating system (OS) area, but at the same time, new areas, such as intelligent cellphones and PDAs, VoIP telephones, ADSL gateways, even TV sets, now have some proprietary network-aware operating system.

To make matters worse, additional factors are also hindering forensic analysis: these include the use of encryption [Case08] cloud-based services (e.g. file storage), the ever increasing size and type of mass storage devices, as well as the ever increasing size of network transfers. For example simply copying a multi-terabyte stack of confiscated disk drives in order to preserve the state of the original devices takes many hours and requires a similar stack of disk drives to hold the copied data.

Nevertheless, certain areas of digital forensics analysis – hard disk drive analysis in particular – have already benefited from work by law enforcement agencies. For example the US NIST has issued document NISTIR 7490 ("Digital Forensics at the National Institute of Standards and Technology") describing standards for carrying out routine digital forensics work.

[1] In the "Nigerian scam" the adversary tries to solicit the help of the victim in order to withdraw money from a blocked account belonging to a dead or seriously ill relative in exchange for a share of the proceeds. The objective is to convince the victim either to hand over bank account details, or even to visit a third world country – e.g. Nigeria, which is how the scam got its name) for a meeting. In the first case unauthorised withdrawals are made from the account, in many cases sucking it dry, while in the second case, the victim may be held hostage until money is handed over as ransom.

[2] Keith Chval, former chief of the Illinois Attorney General's Office's High Tech and Computer Crime Unit.

[3] Shawn Henry, FBI executive assistant director.

In addition to the NIST efforts, the European Union has funded CTOSE (2003), a research project that created the world's first network forensics standards. The goal of CTOSE was to enable anyone from system administrators, IT security staff, forensic investigators, and law-enforcement agencies to follow consistent and standardised procedures when investigating computer incidents using "computer forensic tools."

Moreover, the EU Digital Agenda proposes to reinforce co-operation at European and international levels to combat cybercrime and other forms of cyber attacks, identity theft and spam. (EC, 5/2010).

2.3.1 Emerging Network Threats

As mentioned earlier in this section, technological advances are creating new opportunities for miscreants. Specifically new protocols (such as VoIP and IPv6) and architectures (SOAP). In these areas there has not been sufficient time for the necessary expertise and countermeasures to be developed, or even software bugs in commercial implementations to be identified and patched. Hence, hackers can benefit from "low hanging fruit" while keeping "under the radar" of intrusion detection systems and network security monitors. In fact, only recently did sysadmins start deploying IPv6-specific policy in their firewalls. In many cases the IPv4-only firewall configuration would allow IPv6 packets to go through without any filtering. The same thing applies to VoIP packets that are often allowed in and out of firewalls with little or no analysis at all.

New devices such as ADSL routers, VoIP devices, Digital Video Recorders, even network printers [Cui11] can be fairly easily made to host malware thus becoming observation platforms for monitoring the internal network, or even staging areas at the time of the attack. In [Cui11] the authors state that there are "1.4 Million Embedded Devices on the Internet with Default Passwords." In fact this number may be too conservative as many Cisco-Linksys VoIP phones come without a password and Cisco has sold millions of these products. In many cases the owners are not even *aware* that the device is accessible from the Internet because of the common myth that NAT protects internal devices from Internet-based attackers.

In some cases legacy infrastructure becomes vulnerable through the introduction of new networked data acquisition and control instrumentation. The lack of expertise can even cause embarrassing false alarms as in the case of a pump failure in a water plant in Springfield, Illinois that was thought to have been caused by Russian hackers [Zett11]. Contrariwise, a recent report about hacker attacks to the US Chamber of Commerce, including the infamous thermostat that contained malware [Gorm11, Naka11]

Cellphones, net books, and tablet PCs, may well become the next cyber-crime battlefront. These devices are becoming as powerful as a typical computer was only a few years ago and are increasingly storing huge amounts of personal and confidential data. We have already seen limited examples of hacking on these devices, but as they become ever more popular, they will attract the attention of more hackers.

2.3.2 Conclusions

The discussion in this section lead us to the following observations:

Technological advances open new areas of exploitation by criminals. This creates an arms race where law enforcement authorities must continuously develop new tools and new competencies to be able to cope with the new challenges.

Close co-operation between law enforcement and academia can produce the necessary technological breakthrough and achieve tangible results.

Reacting to incidents is important, but prevention is even better. In the first two case studies, preventive measures could have alleviated the threat.

Inadvertent disclosure of sensitive information. The analysis in [John08] demonstrates that such disclosures in the area of large financial firms result in both a substantial threat and vulnerability.

3 3. Areas of Interest and Requirements

Given the prior work done in the field, along with the input we have come across from a diverse set of experts in network security and malware, we will focus our work on: Unauthorised use of WiFi hotspots, visualisation of suspicious network traffic, and tools to handle IPv6-based intrusions. In the following paragraphs, we will explain the issues behind each of these major problem areas.

3.1.1 i) Unauthorised use of WiFi hotspots

Wireless Internet is now ubiquitous, and almost every ADSL router is bundled with WiFi functionality, often enabled by default. This prevalence together with vulnerabilities in the, numerous, WiFi authentication protocols has created a huge backdoor to practically every network on the planet.

The implications are far ranging, as this activity enables criminals to hide illegal activities behind some else's network, bypass network defences (e.g. firewalls), even steal network bandwidth.

Until very recently we could simply advise people to turn off WiFi access to their networks, but the appearance of WiFi-only devices (tablet PCs, printers, etc) makes this advice no longer practical.

Instead we need to develop tools that essentially standardise the efforts such as those of the forensic company in case study 4 above, and create a suite of tools that (a) detect illegal use of the WiFi network, (b) collect data on the intruder, and (c) protect the forensic data so that they are admissible in court.

3.1.2 ii) Visualisation of suspicious network traffic

In the early days of the PC-era, diskettes were the principal method of data exchange. As a consequence, they quickly became the primary attack vector of malware so that eventually we would need to check each diskette with an anti-virus software package before accessing the data contained in it. The spread of networks and the Internet in particular provided a more effective attack vector to the malware, leading to the development of bump-in-the-wire anti-virus systems in most networks. But now we have travelled a full circle as malware, once again, spread using the new generation of flash-memory storage devices. In fact *any* device with flash memory can be used to introduce malware in a network. There is even an example where the attacker sent a mouse with doctored firmware as a promotional gift to an employee of the victim organisation which allowed the malware to be infect the computer of that employee and from there other PCs in the network [Sams11].

But, regardless of the point of entry, the spread of the malware still relies in the network. So an effective network monitoring system can be used to detect the information that the infected PCs exchange between them and their attempts to contact "home" to upload the stolen data and receive new instructions.

3.1.3 iii) IPv6 Specific Tools

IPv6 suffered extreme delays in its introduction, but now it is finally gaining traction, mainly because IPv4 addresses are finally running out, and most vendors are offering

IPv6-ready systems by default. In fact new versions of Windows do not support configurations where IPv6 is disabled. [Pers11]

What this means is that we have to consider the implications of having IPv6-aware systems in our network, whether we actually use IPv6 or not. To make matters worse, all these systems are running fairly immature code and applications that have been hastily converted to IPv6, so we can expect lots of bugs and vulnerabilities to be ready for the first criminal to use.

Coupled with the early software implementations is the lack of experience in configuring and administering IPv6 systems by the technical personnel. This is likely to lead to buggy configurations and/or deficient security policy that may allow an intruder to go undetected.

It is, therefore, imperative to address the IPv6 security gap, and provide tools and procedures for monitoring IPv6 networks for buggy configurations, software and procedures.

3.2 Requirements

Designing, implementing and deploying the proposed system presents several challenges. We classify them in the following paragraphs and go into detail about the specific requirements.

3.2.1 i) Speed

As network bandwidth doubles every few years, it is getting increasingly difficult to perform sophisticated malware detection and identification at line speeds. Currently it is possible to perform such tasks at 100Mbits to 1Gbit per second relatively easy. We can also do it at speeds up to 10Gbit per second with some extra effort and additional or specialised resources.

From the input we had from the interviews with the experts, it is safe to assume that this will not suffice in a few years time. We are moving to networks of speeds that will reach 40 to 100Gbits per second. Any techniques, protocols and tools we develop must cope with the aforementioned traffic rates.

3.2.2 ii) Preservation of Evidence

When collecting forensic evidence a key requirement is that strict procedures are followed in order to ensure that they are admissible in court. Proper care must be taken to ensure that any possibility of tampering with the data is minimised. For example the use of write-once devices or digital hashes of the collected data ensures that no one can claim that the data were modified during the investigation.

Moreover, certain data such as wiretaps, cannot be simply collected without proper authorisation. The system should ensure that the legal process is followed at every stage of the investigation.

3.2.3 iii) Coverage

Since up to a few years ago, attacks had been large-scale high, impact, and to some extent, short lived. This trend has been reversed in the last few years. Cyber-attackers continuously develop even stealthier methods making it increasingly difficult to detect them. Taking this further, these attacks may take the form of targeted attacks.

That is, attacks that may be customised to strike a certain target in a particular and unique way.

Detecting this type of malicious activity can prove very hard. However, we should strive to offer as much coverage as possible in any mechanisms we develop. Good coverage may translate in capturing a large percentage of attacks, even if some, very stealthy and limited scope attacks get through.

3.2.4 iv) False Positives

Malware detection systems often suffer from false positives: detection of behaviour that seems anomalous, but is not malicious. One may think that this is not a significant problem as it is better to be "safe than sorry." On second thought, however it becomes clear that things are not that simple. False positives create extra workload for the defender, that is the more time the defender spends on examining ultimately benign traffic, the less time they have to deal with actual threats. This has been identified as one of the main problems when dealing with attacks. Our malware analysis system must be able to quickly and accurately decide what is malicious and what is not. This will off-load the detection engine making it more capable when dealing with the high rates of traffic we expect in the next few years.

3.2.5 v) Device Heterogeneity

End user devices come in all shapes and forms. Detection systems may need to take this heterogeneity into account and provide solutions for the different types of devices. The variety of devices, often translate to different operating systems, libraries and applications. Any malware analysis and detection system that will be developed has to take this into account.

In the context of the current project we do not expect to implement systems that provide protection from attacks against all possible combinations of devices and software stacks. That would be infeasible given the limited time provided for this project. What we do plan however is to implement solutions for the more popular hardware devices and software stacks. We also plan to create solutions that can be applied to a broad set of hardware devices and software stacks.

3.2.6 vi) Network Heterogeneity

We are evolving from DSL and leased lines, to fibre to the customer, while on the wireless front we are witnessing an explosion of different technologies for cellular, broadband and personal networks, and on the logical side, intranets, extranet and overlays. All these types of networks create new opportunities for the attackers. For example, now the attackers have a lot of capacity in terms of the rate of attack, should they try to be aggressive. They also have multiple avenues in terms of reaching the victim, by selecting which network to use in order to carry out an attack. The malware identification system we develop must take these new topological realities in mind. The placement of detectors must be such that they can counter attacks following variable attack paths.

3.2.7 vii) Protocol Diversity

The richness of the application space in today's Internet generates data traffic at rates and richness that seemed unimaginable a decade ago. This data traffic on modern

networks is transferred over a plethora of network protocols. Protocols are being developed to address specific application needs such as, HTTP, SOAP, a plethora of P2P protocols, FTP, VoIP etc.: Any malware detection and forensics system must be able to identify attacks propagating on any of the protocols being used today. This is necessary as attackers launch their attack vectors against any, and every, potential target application. This requirement forces us to closely look at data packets instead of simply relying on a quick inspection. The algorithms and systems we develop must be capable of performing deep packet inspection on traffic flows when trying to identify covert attacks.

4 4. Preliminary Design

In this section we outline the design of the tool set for the detection of illegal activities in the Internet.

Our design is based on the proven concept of sensors. We will develop a set of sensors that can be deployed in networks preventively to detect any activity that may occur in the future, or to monitor a suspicious activity that is already in progress.

The sensors may communicate with each other, or send their data to a central monitoring station. The monitoring station will collect the data and process them according to pre-compiled activity profiles. Visualization tools will be used to aid the operator in interpreting the data.

Two particular types of equipment offer extremely useful platforms for our sensors. These are ADSL routers, and cell-phone pico-cells. Both form the locus of activity in data and voice networks respectively. Also we believe that we can modify existing platforms to include out monitoring software in order to reduce the development costs and minimize risks.

For the ADSL routers we will select devices that include WiFi functionality and include support for IPv6 and VoIP protocols. This is so that we can address as many of the issues we identified in the previous section in one platform. We intend to release our software modifications so that users, outside our project can try it out and provide feedback to us with respect to possible bugs, problems etc.

The cell-phone pico-cells are essentially mobile telephony cells small (and cheap) enough to be located in a typical home. Their function is to provide low-cost relaying of mobile telephony services over the Internet when the cell-phone owner is at home.

Since pico-cells may also be used to intercept mobile telephone calls, we would like to investigate their use in lawful wiretaps.

Finally a lot of effort will be developed in integration activity, as all these separate components will have to be able to work together and exchange information reliably.

5 Bibliography

[Blin09] Robert Blincoe, "Police sitting on forensic backlog risk, says top e-cop" The Register, 13th November 2009

[Calo01] Caloyannides, Michael A. *Computer Forensics and Privacy*. Artech House, Inc. 2001.

[Case08] Casey, E., & Stellatos, G. J. (2008). *The Impact of Full Disk Encryption on Digital Forensics*. New York: ACM.

[Cui11] Ang Cui, Salvatore J. Stolfo; "*Print Me If You Dare: Firmware Modification Attacks and the Rise of Printer Malware*" The 28th Chaos Communication Congress.
http://www.hacktory.cs.columbia.edu/sites/default/files/CuiPrintMeIfYouDare.pdf

[Defe09] http://www.defenseindustrydaily.com/P2P-Network-Leaks-The-VH-60N-Helicopter-05318

[Digi01] Digital Forensics Research Workshop. "*A Road Map for Digital Forensics Research*" 2001. www.dfrws.org

[Gorm11] Siobhan Gorman, "*China Hackers Hit US Chamber*", Wall Street Journal, 21/12/2011.

[HoL006] UK House of Lords Report HL165I 2006-07.

[Ioan02] John Ioannidis and Steven M. Bellovin. "*Implementing pushback: Router-based defense against DDoS attacks*," In Proc. Internet Society Symposium on Network and Distributed System Security, 2002.

[John08] Johnson, M.E. "*Information Risk of Inadvertent Disclosure: An Analysis of File-Sharing Risk in the Financial Supply Chain"*. Journal of Management Information Systems 25(2), 97–123 (2008).

[Krav11] David Kravets, "*Wi-Fi-Hacking Neighbor From Hell Sentenced to 18 Years*," Wired Magazine July 12, 2011
http://www.wired.com/threatlevel/2011/07/hacking-neighbor-from-hell

[Marg09] Larry Margasak, "US Congress Ethics Reports Leaks, Revealing Names," Associated Press, Nov. 2, 2009.
http://www.memphisdailynews.com/news/2009/nov/2/us-congress-ethics-report-leaks-revealing-names//print

[Naka11] Ellen Nakashima, "Report on 'Operation Shady RAT' identifies widespread cyber-spying," Washington Post, August 3, 2011.

[Pers11] Susan Perschke, "Hackers target IPv6," ComputerWorld, Nov. 28, 2011
http://www.pcworld.com/businesscenter/article/245068/hackers_target_ipv6.html

[Prev07] Vassilis Prevelakis, Diomidis Spinellis,"The Athens Affair," IEEE Spectrum, 44(7), pp. 26-33, July 2007.

[Sams11] Ted Samson, "Security company infects client's network with 'Trojan mouse'", Infoworld, June 28, 2011.
http://www.infoworld.com/t/insider-threats/security-company-infects-clients-network-trojan-mouse-576

[Sava00] Savage, Stefan; D. Wetherall, A. Karlin, and T. Anderson "*Practical Network Support for IP Traceback*," ACM SIGCOMM. Stockholm, Sweden, 2000.

[UKHO0] UK Home Office, *Interception of Communications, Code of Practice*, ISBN 978-0-11-341281-5, 2007

[Veri11] *Verizon's 2011 Data Breach Investigation Report*

[Zett11] Kimm Zetter, "*Comedy of Errors led to false water-pump hack report*," Wired Magazin, Nov. 2011.
http://www.wired.com/threatlevel/2011/11/water-pump-hack-mystery-solved

6 Appendix A: Computer Forensics Papers and tools

6.1 Papers:

1) Exploiting the Rootkit Paradox with Windows Memory Analysis

This paper explores how an examiner can create such a memory image and use the inherent properties of rootkits to find them in those memory images.

Memory	Improve Rootkit detection in memory images

2) A Recursive Session Token Protocol For Use in Computer Forensics and TCP Traceback

The Session TOken Protocol (STOP), enhances the Identification Protocol (ident) infrastructure by sending recursive requests to previous hosts on the connection chain. The protocol has been designed to protect user's privacy by returning a token that is a hash of connection information; a system administrator can later decide whether to release the information relating to the token depending on the circumstances of the request.

Network	-

3) Sharing Network Logs for Computer Forensics: A New Tool for the Anonymization of NetFlow Records

CANINE (Converter and ANonymizer for Investigating Netflow Events) is a unique, new tool that anonymizes Net-Flows to multiple levels. It handles Argus, NCSA Unified Format, Cisco 5, Cisco 7 and Cisco 5/7 mixed logs. Multiple levels of anonymization that trade-off between the security of the anonymization scheme and the utility of the anonymized logs is supported through multiple algorithms that anonymize the 8 most common NetFlow fields (Source IP Address ,Destination IP Address, Source Port, Destination Port, Start Timestamp, End Timestamp, Protocol and Byte Count) in different ways. This is the only log anonymizer that we are aware of that supports multiple levels of anonymization, and it is the only Net- Flow anonymizer we know of besides a previous tool we created that just anonymized IP addresses in one NetFlow format

Memory - Network	Log anonymization for multiple levels

4) A Theoretical Framework for Organizational Network Forensic Readiness

This paper discusses breaking the escalation cycle that locks cyber intruders and their targets in a state where targets are perennially resigned to attacks and intruders are at liberty to exploit and disrupt networks without much risk of suffering consequences. Using systems and case analyses, several research questions are explored, resulting in the identification of conditions that must change in order to interrupt this unproductive relationship between attackers and targets. As an

outcome, network forensic readiness (NFR) is proposed as a solution to digital forensic investigations that have become too resource intensive to encourage broad application to the growing numbers of computer crimes.

Network	A generalized model for designing calibration tests for low layer network devices and an exemplar test case of an aggregator tap are described. Additional work is needed to extend this model to more complex network devices and to assist in the development of a standard calibration protocol.

5) Network Support for IP Traceback

This paper describes a technique for tracing anonymous packet flooding attacks in the Internet back toward their source. This work is motivated by the increased frequency and sophistication of denial-of-service attacks and by the difficulty in tracing packets with incorrect, or "spoofed," source addresses. In this paper, we describe a general purpose traceback mechanism based on probabilistic packet marking in the network. Our approach allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs). Moreover, this traceback can be performed "post mortem" – after an attack has completed. We present an implementation of this technology that is incrementally deployable, (mostly) backward compatible, and

Network	Several areas remain to be addressed in future work, such as improving robustness under distributed attacks and tracing past points of indirection such as reflectors.

6) Anti-computer forensics

In this paper, we propose a preventative anticomputer forensics framework and brief demonstration. This framework will assist organizations with strengthening their approach to thwarting tools and procedures conducted by criminals.

Memory - Network	In future work, PACF will be the basis for the development of a knowledge management system to track human and computer methods involving anti-computer forensics methods to disseminate in an organization.

7) Computer Intrusion Forensics

This paper views a forensic application within the framework of Intrusion Detection and details the advantages and disadvantages of each IDS.

IDS	-

8) XIRAF – XML-based indexing and querying for digital forensics

This paper describes a novel, XML-based approach towards managing and querying forensic traces extracted from digital evidence. This approach has been implemented in XIRAF, a prototype system for forensic analysis. XIRAF systematically applies forensic analysis tools to evidence files (e.g., hard disk images).

Network- XML Database	an open-source mobile phone analysis tool, into XIRAF

9) Distributed forensics and incident response in the enterprise

the GRR Rapid Response Framework (GRR), a new multi-platform, open source tool for enterprise forensic investigations enabling remote raw disk and memory access. GRR is designed to be scalable, opening the door for continuous enterprise wide forensic analysis. This paper describes the architecture used by GRR and illustrates how it is used routinely to expedite enterprise forensic

Memory - Remote Raw Disk	data snapshots and non-interactive analysis, requiring the development of new data models and user interface designs

10)Dynamic recreation of kernel data structures for live forensics investigations.

This paper describes techniques developed to allow automatic adaptation of memory analysis tools to a wide range of kernel versions. Dynamic reconstruction of kernel data structures is obtained by analyzing the memory dump for the instructions that reference needed kernel structure members.

Memory - Kernel	provides future researchers a solid starting point to delve into memory forensics and develop even further reaching tools

11) BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections

The BLADE (Block All Drive-by download Exploits) system asserts that all executable files delivered through browser downloads must result from explicit user consent and transparently redirects every unconsented browser download into a nonexecutable secure zone on disk. BLADE thwarts the ability of browser-based exploits to surreptitiously download and execute malicious content by remapping to the filesystem only those browser downloads to which a programmatically inferred user-consent is correlated, BLADE provides its protection without explicit knowledge of any exploits and is thus resilient against code obfuscation and zero-day threats that directly contribute to the pervasiveness of today's drive-by malware.

Browser	Extension of BLADE support to other network-capable applications subject to drive-

	by download attacks

12) HoneyStat: LocalWorm Detection Using Honeypots

The HoneyStat nodes generate three classes of alerts: memory alerts (based on buffer overflow detection and process management), disk write alerts (such as writes to registry keys and critical files) and network alerts. Data collection is automated, and once an alert is issued, a time segment of previous traffic to the node is analyzed. A logit analysis determines what previous network activity explains the current honeypot alert. The result can indicate whether an automated or worm attack is present.

Network - IDS	Further work could include identification of additional logistic models to sort through large sets of data, coordination of shared honeypot events, integration with other intrusion detection techniques, and response.

13) Windows operating systems agnostic memory analysis

This paper proposes using the debug structures embedded in memory dumps and Microsoft's program database (PDB) files to create a flexible tool that takes an arbitrary memory dump from any of the family of Windows NT operating systems and extract process, configuration, and network activity information.

Memory	there is no reason that these techniques have to be limited to memory dumps. By incorporating them either into system modules or into an underlying hypervisor, these tools can function as sensors for intrusion detection systems.

14 Stealthy Malware Detection Through VMM-Based "Out-of-the-Box" Semantic View Reconstruction

In this paper, we present the design, implementation, and evaluation of VMwatcher an out-of-the-box approach that overcomes the semantic gap challenge. A new technique called guest view casting is developed to systematically reconstruct internal semantic views (e.g., les, processes, and kernel modules) of a VM from the outside in a non-intrusive manner.

Virtual Machines	–

15) Minos: Control Data Attack Prevention Orthogonal to Memory Model

Minos, a microarchitecture that implements Biba's low-water-mark integrity policy on individual words of data. Minos stops attacks that corrupt control data to hijack program control flow but is orthogonal to the memory model.

Memory	detect and stop unknown polymorphic worms in their incipiency this way.

The Minos approach could be extended to the kernel and to other kinds of data.

16) Live memory forensics of mobile phones

In this paper, we proposed an automated system to perform a live memory forensic analysis for mobile phones. We investigated the dynamic behavior of the mobile phone's volatile memory, and the analysis is useful in real-time evidence acquisition analysis of communication based applications.

Mobile Phone's Memory	–

17) ForNet: A Distributed Forensic Network

In this paper we present the design of a network forensics system, ForNet, that aims to address the lack of effective tools for aiding investigation of malicious activity on the Internet. ForNet is a network of two functional components. A Synopsis Appliance, called SynApp, is designed to summarize and remember network events in its vicinity for a prolonged period of time and be able to attest to these events with certain level of confidence. A Forensic Server is a centralized authority for a domain that manages a set of SynApps in that domain.

Network	–

18) Attacks Detection Based on IP and TCP Protocols Violations

This work presents a packet analysis methodology for detecting anomalous behaviors, not based on attack signatures, but on verifying whether the network protocols are being violated, and on the content of the respective headers. The biggest benefit of this methodology is the possibility of detecting anomalies or inadequate behaviors that can correspond, totally or partially, to variations on well-known and unknown attacks

Network	Support more protocols

19) Botnets as a Vehicle for Online Crime

An analysis of real-world botnets1 demonstrates the increasing sophistication of bot2 malware and its thoughtful engineering as an effective tool for profi t-motivated online crime. The purpose of this paper is to increase understanding of the capabilities present in bot malware and the motivations for operating botnets.

Network	–

20)BodySnatcher: Towards reliable volatile memory acquisition by software

In this paper we propose a method of acquiring the contents of volatile memory from arbitrary operating systems in a manner that provides point in time atomic snapshots of the host OS volatile memory.

Memory	Next steps will involve widening the availability of the approach by supporting a wider range of OS's and hardware configurations. Secondly, we are currently working on utilizing USB as a high speed and ubiquitous output channel, due to the small number of drivers required to support it. Future work could explore the potential of resumption of the host OS post acquisition

21) The persistence of memory: Forensic identification and extraction of cryptographic keys

The increasing popularity of cryptography poses a great challenge in the field of digital forensics. Digital evidence protected by strong encryption may be impossible to decrypt without the correct key. We propose novel methods for cryptographic key identification and present a new proof of concept tool named Interrogate that searches through volatile memory and recovers cryptographic keys used by the ciphers AES, Serpent and Twofish.

Memory	Furthermore, research is needed on software and hardware based memory dumping and analysis of their impact on system state, including files like pagefile.sys. Finally, where legislation and EULAs allow, efforts on reverse engineering closed-source cryptographic applications are needed to put uncovered keys to good use.

22) Defending against Pathbased DoS Attacks in Wireless Sensor Networks

This paper proposes a solution using one-way hash chains to protect end-to-end communications in WSNs against PDoS attacks.

Network	–

23) Practical Network Support for IP Traceback

This paper describes a technique for tracing anonymous packet flooding attacks in the Internet back towards their source.

Network	Several areas remain to be addressed in future work, such as the combination of widely distributed attacks and points of indirection such as reflectors

24) Identification of High-Resolution Images of Child and Adolescent Pornography at Crime Scenes

This paper presents an approach of image resizing to optimize the runtime of the automatic nudity detection provided by the NuDetective Forensic Tool. The results of several experiments performed to evaluate the efficiency of this approach showed a runtime reduction of about 90%, with minimal changes in the accuracy of nudity detection.

Network - Disk	Video Analysis

25) Automated Extraction of Threat Signatures from Network Flows

The generation of network threat signatures used in intrusion detection and prevention systems is mostly a manual process, thus prone to errors and slow. Reaction to a new threat must be fast if it is to be effective, and at the same time appropriate so as to reduce any chance of unexpected, even negative side effects. An attempt to achieve this is the goal of automatic extraction of network threat signatures being developed as part of the ARAKIS Early Warning project of the CERT Polska team.

Network	–

26) utomated Worm Fingerprinting

In this paper, we propose an automated approach for quickly detecting previously unknown worms and viruses based on two key behavioral characteristics a common exploit sequence together with a range of unique sources generating infections and destinations being targeted. More importantly, our approach called content sifting automatically generates precise signatures that can then be used to lter or moderate the spread of the worm elsewhere in the network.

Network - Memory	–

6.2 Tools:

1) System logs:

Syslog-ng is a flexible and scalable audit-processing tool. It offers a centralized and securely stored log for all the devices on a network.

- It guarantees the availability of logs.
- It is compatible with a wide variety of platforms.
- It is used in heavily firewalled environments.
- It offers proven robustness.
- It allows a user to manage audit trails flexibly.
- It has customizable data mining and analysis capabilities.

- It allows a user to filter based on message content.

Socklog is a small and secure replacement for syslogd. It runs on Linux (glibc 2.1.0 or higher, or dietlibc), OpenBSD, FreeBSD, Solaris, and NetBSD.

- It selects and deselects log entries.
- It has a small code size.
- It provides modular and reliable network logging.
- It merges different logs and sorts them in order.
- Log file rotation is based on file size.
- It receives syslog messages from a UNIX domain socket (/dev/log) and writes them to various files on the disk, depending on facility and priority.
- It receives syslog messages from a UDP socket (0.0.0.0:514) and writes them to various files on the disk, depending on facility and priority.
- It writes received syslog messages to a UDP socket

Kiwi Syslog Daemon is a freeware syslog daemon for Windows. It receives logs and displays and forwards syslog messages from routers, switches, UNIX hosts, and any other syslog-enabled device. There are many customizable options available.

- PIX firewall logging
- Linksys home firewall logging
- SNMP trap and TCP support
- SNMP MIB parsing
- Ability to filter, parse, and modify messages and take actions via VBScript/JScript engine
- GUI-based syslog manager
- Real-time message display as messages are received
- Ten virtual displays for organizing messages
- Message logging or forwarding of all messages, or based on priority or time of day
- Message receipt via UDP, TCP, or SNMP
- Message forwarding via UDP or TCP
- Automatic log file archiving based on a custom schedule
- Messages per hour alarm notification with audible sound or e-mail
- Log file size alarm notification with audible sound or e-mail
- Daily e-mailing of syslog traffic statistics

- Maintenance of source address when forwarding messages to other syslog hosts
- DNS resolution of source host IP addresses with optional domain removal
- DNS caching of up to 100 entries to ensure fast lookups and to minimize DNS lookups
- Preemptive DNS lookups using up to 10 threads

Microsoft Log Parser is a powerful, versatile, robust command-line tool that offers a SQL interface to various log file formats and is fast enough for log file analysis of many Web sites.

- It enables a user to run SQL-like queries against log files of any format.
- It produces the desired information either on the screen, in a file, or in an SQL database.
- It allows multiple files to be piped in or out as source or target tables.
- It generates HTML reports and MS Office objects.
- It supports conversion between SQL and CSV formats.

Firewall Analyzer is a Web-based firewall monitoring and log analysis tool that collects, analyzes, and reports information on enterprise-wide firewalls, proxy servers, and RADIUS servers.

- Bandwidth usage tracking
- Intrusion detection
- Traffic auditing
- Anomaly detection through network behavioral analysis
- Web site user access monitoring
- Automatic firewall detection and configuration
- Anomaly filtering
- Historical trend reporting
- Predefined reports
- Customizable reports
- Report scheduling
- Rule-based alerting
- Flexible archiving
- Portability
- Multiplatform support

Adaptive Security Analyzer (ASA) Pro is a security and threat intelligence application that continuously monitors dynamic, high-volume, heterogeneous security-related data; recognizes and quantifies the extent of event abnormality; and advises security personnel of the factors that contributed most to the event's classification.

- Model security specialist expertise
- Baseline what is normal for a computing environment
- Identify published threats
- Identify activity matching predefined criteria
- Identify, measure, and prioritize all anomalous events
- Generate root cause insight of threats
- Feed new knowledge back into the system

GFI EventsManager collects data from all devices that use Windows event logs, W3C, and syslog, and applies rules and filtering to identify key data. GFI EventsManager also provides administrators with real-time alerting when critical events arise, and it suggests remedial action.

- Network-wide analysis of event logs: GFI EventsManager contains an intelligent event processor that processes logs and available data in a centralized way. It controls and manages Windows event logs, W3C logs, and syslog events.
- Explanations of cryptic Windows events: Cryptic logs make the log analysis process difficult. GFI EventsManager translates these cryptic events into clear and concise explanations.
- Centralized event logging: Event logs can be generated by users or automatically by background processes. These logs are stored in different locations. GFI EventsManager stores all these logs in one SQL database.
- High-performance scanning engine: GFI EventsManager contains a high-performance event-scanning engine. It is able to scan and collect up to six million events an hour.
- Real-time alerts: GFI EventsManager alerts administrators when it detects any key events or intrusions. It can send this alert to multiple people by e-mail or SMS.
- Advanced event filtering features: GFI EventsManager's filtering process sieves through recorded event logs. It allows administrators to select the events they want, without deleting any event from the database.
- Report viewing for key security information happening on the network: GFI EventsManager allows administrators to detect security trends. These standard reports consist of:
- Policy-change reports
- Windows event log system reports

- Event trend reports
- Account usage reports
- Application management reports
- Account management reports
- Object access reports
- Print server reports

NTsyslog service runs under the LocalSystem account. The service can also be run as a local if that user is given the right to log on as a service and manage auditing and security logs. NTSyslogCtrl is a GUI tool that an administrator can use to configure which messages to monitor and the priority to use for each type. By default, sending all messages utilizes the user alert priority. This GUI tool is used for configuring the registry. To configure the syslog host manually, an administrator can create the following registry entry:

[HKEY_LOCAL_MACHINE\SOFTWARE\SaberNet] “Syslog” = “host.domain.com”

An administrator can specify the syslog host by domain name or by IP address.

EventReporter is a tool that processes Windows event logs, parses them, and forwards the results to a central syslog server. EventReporter automatically monitors Windows event logs. It detects system hardware and software failures that damage the network. EventReporter integrates Windows systems with UNIX-based management systems.

- Monitoring
- Filtering
- Data collection
- Alerting

EventLog Analyzer is a Web-based syslog and event log management solution that collects, analyzes, archives, and reports on event logs from distributed Windows hosts and syslogs from UNIX hosts, routers, switches, and other syslog devices.

- Centralized event log management
- Security analysis
- Automated event archiving
- Importing event logs
- Real-time alerting
- Scheduled reporting
- Multiple report export formats
- Compliance reporting
- Host grouping

- Built-in database
- Event archiving
- Automatic alerting
- Predefined event reports
- Historical trending

Analog analyzes log files from Web servers.

Deep Log Analyzer analyzes the logs for small and medium Web sites.

AWStats, short for Advanced Web Statistics, is a log analyzer that creates advanced Web, FTP, mail, and streaming server statistics reports, presented in HTML format. Use of AWStats requires access to the server logs as well as the ability to run Perl scripts

Server Log Analysis analyzes server logs by changing IP addresses into domain names with the help of httpdanalyse.c.

WebLog Expert gives information about a site's visitors, including activity statistics, accessed files, paths through the site, referring pages, search engines, browsers, operating systems, and more. The program produces HTML reports that include both tables and charts.

AlterWind Log Analyzer Professional generates reports for Web site search engine optimization, Web site promotion, and pay-per-click programs. It is specifically made to increase the effects of Web site promotion.

Webalizer is a fast, free, and portable Web server log file analysis program. It accepts

standard common log file format (CLF) server logs and produces highly detailed, easily configurable usage statistics in HTML format. Generated reports can be configured from the command line or by the use of one or more configuration files.

eWebLog Analyzer is another Web server log analyzer that can read log files of popular Web servers, including Microsoft IIS, Apache, and NCSA, as well as any other Web server that can be configured to produce log files in Common or Combined standard format, or W3C Extended format. It supports compressed logs and can also download log files directly from FTP or HTTP servers.

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

HijackThis Trend Micro HijackThis has been a free utility that generates an in-depth report of registry and file settings from your computer. HijackThis makes no separation between safe and unsafe settings in its scan results – this offers you the ability to selectively remove items from your machine. In addition to this scan-and-

remove capability, HijackThis comes with several tools that are useful for manually removing malware from a computer.

Debug Diagnostic The Debug Diagnostic Tool (DebugDiag) is designed to assist in troubleshooting issues such as hangs, slow performance, memory leaks or fragmentation, and crashes in any user-mode process.

Aro ARO is an advanced repair and optimization utility designed to help improve and maintain computers running the Windows operating system (both 32- and 64-bit). ARO focuses on finding errors that hide out in the Windows registry, identifying PC and web browser clutter that may be hindering PC performance and ensuring computers have adequate security solutions installed and up to date. With its advanced scanning engine, ARO provides deep scanning capabilities to identify and repair registry errors. ARO also searches for and removes "junk" files that accumulate over time and can put a damper on PC performance.

2) Network

2.1) Network traffic

Tcpdump is a powerful tool that extracts network packets and performs statistical analysis on those dumps. It operates by putting the network card into promiscuous mode. It may be used to measure the response time and packet loss percentages, and to view TCP/UDP connection establishment and termination. One major drawback to Tcpdump is that the size of the flat file containing the text output is large.

WinDump is a port of Tcpdump for the Windows platform. WinDump is fully compatible with Tcpdump and can be used to watch and diagnose network traffic according to various complex rules.

NetIntercept, from Sandstorm Enterprises, is a network analysis tool that allows an organization to increase its network security. NetIntercept captures LAN traffic using a standard Ethernet interface card placed in promiscuous mode and a modified UNIX kernel. The capture subsystem runs continuously, whether or not the GUI is active.

Wireshark, formerly known as Ethereal, is a GUI-based network protocol analyzer. It lets the user interactively browse packet data from a live network or from a previously saved capture file. Wireshark's native capture file format is the libpcap format, which is also the format used by Tcpdump and various other tools. In addition, Wireshark can read capture files from snoop and atmsnoop, Shomiti/Finisar Surveyor, Novell LANalyzer,Network General/Network Associates DOS-based Sniffer (compressed or uncompressed), Microsoft Network Monitor, and other tools. Wireshark can determine the capture file type by itself, without user intervention. It is also capable of reading any of these file formats if they are compressed using gzip.

CommView is a network monitor and analysis tool that provides a complete picture of the traffic flowing through a PC or LAN segment. It captures every packet on the wire and displays information and vital statistics about the captured packets, as shown in Figure 2-12. A user can examine, save, filter, import, and export captured packets.

SoftPerfect Network Protocol Analyzer debugs, maintains, analyzes, and monitors local networks and Internet connections. It captures the data passing through network connections, analyzes this data, and then represents it in an easily readable form. The SoftPerfect Network Protocol Analyzer presents analysis results in an easily

understandable format. It also allows a user to defragment and reassemble network packets into streams. The tool can analyze network traffic based on a number of different Internet protocols

EffeTech HTTP Sniffer is an HTTP packet sniffer, protocol analyzer, and file reassembly tool for Windows. This sniffer captures IP packets containing HTTP messages, rebuilds the HTTP sessions, and reassembles files sent through HTTP. HTTP Sniffer provides real-time analysis of content while capturing, analyzing, parsing, and decoding HTTP messages.

EtherDetect Packet Sniffer is a connection-oriented packet sniffer and network protocol analyzer. A user can capture full packets, organize packets by TCP connections or UDP threads, passively monitor the network, and view packets in hex format.

OmniPeek is a network analysis tool that an administrator can use to quickly analyze and troubleshoot network problems at the enterprise level

Iris Network Traffic Analyzer provides network traffic analysis and reporting functionality. This tool captures network traffic and can automatically reassemble it to its native format, making it much easier to analyze the data going across the network. An investigator can read the actual text of an e-mail exactly as it was sent, or reconstruct exact HTML pages that a user has visited.

SmartSniff provides investigators with the ability to view captured TCP/IP packets as sequences of conversations between clients and servers. Investigators can view these conversations in ASCII mode (for text-based protocols) or as a hex dump for non-text-based protocols).

NetSetMan is a network settings manager that allows a user to easily switch between six different network settings profiles.

Distinct Network Monitor displays live network traffic statistics, It includes a scheduler that allows an administrator to run a scheduled collection of network traffic statistics or packet captures

MaaTec Network Analyzer is a tool that is used for capturing, saving, and analyzing network traffic. The following are some of the features of MaaTec Network Analyzer:

ntop is a network traffic probe that shows network usage. In interactive mode, it displays the network status on the user's terminal. In Web mode, it acts as a Web server, creating an HTML dump of the network status

EtherApe is a graphical network monitor for UNIX. It displays network activity graphically by featuring link layer, IP, and TCP modes, as shown in Figure 2-25. It can filter traffic for display, and it can read traffic from a file as well as live from the network.

Colasoft Capsa Network Analyzer is a TCP/IP network sniffer and analyzer that offers real-time monitoring and data analysis of network traffic. It also offers e-mail analysis, Web analysis, and transaction analysis

Colasoft EtherLook is a TCP/IP network-monitoring tool for Windows-based platforms. It monitors real-time traffic flowing around local networks, and to and from the Internet. The Traffic Analysis Module allows a user to capture network traffic in real time, and display data received and sent by every host in a LAN

AnalogX PacketMon allows an administrator to capture IP packets that pass through a network interface, whether those packets originated from the machine on which PacketMon is installed or from any other machine on the network. Administrators can then use the built-in viewer to examine the packet's header and contents. PacketMon can export the results into a CSV file for further processing

BillSniff is a network protocol analyzer that provides detailed information about current traffic, as well as overall protocol statistics.

IE HTTP Analyzer is an add-in for Internet Explorer that allows a user to capture HTTP and HTTPS traffic in real time.

EtherScan Analyzer is a network traffic and protocol analyzer. It captures and analyzes packets sent over a local network. It decodes the major protocols and is capable of reconstructing TCP/IP sessions

Sniphere is a WinPcap network sniffer that supports most common protocols. It can be used on Ethernet devices and supports PPPoE modems. It allows the user to set filters based on IP, MAC address, ports, and protocols,and it also decodes packages into an easy-to-understand format. In addition, users can save session logs in XML format and copy selected packets to the clipboard

IP Sniffer is a protocol analyzer that uses Windows XP/2000 raw socket features. It supports filtering rules, adapter selection, packet decoding, advanced protocol description, and more. It provides detailed information about each packet in a tree-style view, and the right-click menu allows users to resolve or scan a selected source IP address.

Atelier Web Ports Traffic Analyzer is a network traffic sniffer and logger that allows a user to monitor all Internet and network traffic on a PC and view the actual content of the packets. It provides real-time mapping of ports to processes. It also shows the history since boot time of every TCP, UDP, or RAW port opened through Winsock.

IPgrab is a packet sniffer for UNIX hosts. It provides a verbose mode that displays a great amount of information about packets. It also provides a minimal mode in which all information about all parts of a packet is displayed in a single line of text

Nagios is a host and service monitor designed to run under the Linux operating system.

Give Me Too is a packet sniffer, network analyzer, and network sniffer that monitors any Internet and e-mail activity. It captures all data transferred through the network via HTTP, FTP, SMTP, IMAP, POP3, and IRC protocols.

Sniff-O-Matic is a network protocol analyzer and packet sniffer. It captures network traffic and provides analysis tools that allow a user to analyze the captured data.

EtherSnoop is a packet sniffer and protocol analyzer. It captures the data passing through a dial-up connection or Ethernet card, analyzes the data, and presents it in a readable format.

In the General Packet Radio Service (GPRS) embedding of the Lawful Interception Gateway (LIG), critical network functionality enables interception of GPRS mobile data calls. This technique is entirely different from GSM call interception. The difference lies in interception. In GSM, voice-based audio recording is primarily

intercepted, whereas in GPRS, the data between the mobile station and the access point is captured.

Siemens Monitoring Center is designed for law enforcement and government security agencies. Its design permits integration within all telecommunications networks that use any type of modern standardized equipment compatible with an ETSI recommendation (e.g., Siemens, Ericsson, Alcatel, Nokia, Nortel, Lucent, and Huawei).

NetWitness analyzes network traffic for potential threats. The primary focus of NetWitness is on expanding the efficiency of information gathering. It enables organizations to recognize and respond to network activity promptly.

NetResident captures, stores, analyzes, and reconstructs network events, such as e-mail messages, Web pages, downloaded files, instant messages, and VoIP conversations. NetResident captures the data on the network, saves it to a database, reconstructs it, and displays this content in an easy-to-understand format.

InfiniStream provides the ability to identify, monitor, measure, and resolve high-impact, intermittent enterprise problems. InfiniStream's continuous long-term capture ability enables users to have data for an entire transaction or a series of transactions. Users can then drill down to the area of interest and conduct a postcapture analysis using sniffer decodes and analysis.

eTrust Network Forensics helps an organization secure its network and ensure availability by capturing realtime network data to identify how business assets are affected by network exploits, internal data theft, and security or HR policy violations. eTrust Network Forensics can help the organization mitigate risk, comply with regulations, and reduce analysis and investigation costs by allowing IT and security staff to visualize network activity, uncover anomalous traffic, and investigate security breaches.ProDiscover Investigator investigates disk contents throughout the network. It checks for illegal activity and for compliance with company policies. ProDiscover Investigator can gather evidence for potential use in legal proceedings

P2 Enterprise Shuttle is an enterprise investigation tool that views, acquires, and searches client data wherever it resides in an enterprise. It checks the main communication pass-through for the system as well as the routers and firewalls. P2 Enterprise Shuttle acts as the central repository for all forensic images collected and is integrated with MySQL.

Show Traffic monitors network traffic on a user-specified network interface and displays it continuously. It allows a user to find suspicious network traffic or just monitor the traffic flowing through the network interface.

Network Probe identifies the source of network slowdowns and other problems. It shows who is generating troublesome traffic, and where the traffic is being transmitted to or received from.

Snort is a software-based, real-time network intrusion detection system that notifies an administrator of a potential intrusion attempt. Snort is nonintrusive, is easily configured, and utilizes familiar methods for rule development. Snort has the ability to detect more than 1,100 potential vulnerabilities.

The IDS Policy Manager manages Snort IDS sensors in a distributed environment. Users can modify the configuration files using a GUI. Users can manage Snort by

merging new rule sets, managing preprocessors, configuring output modules, and securely copying rules to sensors.

2.2) Web Attack Investigations

N-Stealth is a vulnerability-assessment product that scans Web servers to identify security problems and weaknesses. Its database covers more than 25,000 vulnerabilities and exploits.

Acunetix Web Vulnerability Scanner determines a Web site's vulnerability to SQL injection, XSS, Google hacking, and more

dotDefender is a Web application firewall that blocks HTTP requests that match an attack pattern. It offers protection to the Web environment at both the application level and the user level, and also offers session attack protection by blocking attacks at the session level.

AppScan runs security tests on Web applications. It offers various types of security testing such as outsourced, desktop-user, and enterprise-wide analysis, and it is suitable for all types of users, including application developers, quality assurance teams, security auditors, and senior management.

AccessDiver contains multiple tools to detect security failures on Web pages.

Falcove audits Web sites to determine if they are vulnerable to attack, and implements corrective actions if any are found. The SQL server penetration module makes Falcove different from other Web vulnerability scanners, because it allows the user to penetrate the system using these vulnerabilities, just like an external attacker would. It also generates penetration reports to detail vulnerabilities.

Emsa Web Monitor is a small Web monitoring program that monitors the uptime status of several Web sites. It works by periodically pinging the remote sites, and showing the ping response time as well as a small graph that allows the user to quickly view the results.

WebWatchBot is monitoring and analysis software for Web sites and IP devices and includes ping, HTTP, HTTPS, SMTP, POP3, FTP, port, and DNS checks.

Paros is a Java-based tool for testing Web applications and insecure sessions. It acts as a proxy to intercept and modify all HTTP and HTTPS data between server and client, including cookies and form fields.

HP WebInspect performs Web application security testing and assessment. It identifies known and unknown vulnerabilities within the Web application layer, and checks to validate that the Web server is configured properly.

keepNI checks the vital services of a Web site at an interval chosen by the user. If the check takes too long, it is considered a timeout fault. When a fault is detected, one or more alerts can be initiated to inform the operator or computerized systems.

Wikto checks for flaws in Web servers.

Mapper helps to map the files, file parameters, and values of any site. Simply browse the site as a normal user while recording the session with Achilles or another proxy, and run Mapper on the resulting log file. It creates an Excel CSV file that shows the directory and file structure of the site, the parameter names of every dynamic page

encountered (such as ASP/JSP/CGI), and their values every time they are requested. This tool helps to quickly locate design errors and parameters that may be prone to SQL injection or parameter tampering problems.

Mapper supports nonstandard parameter delimiters and MVC-based Web sites.

N-Stalker offers a complete suite of Web security assessment checks to enhance the overall security of Web applications against vulnerabilities and attacks.

Scrawlr crawls a Web site and audits it for SQL injection vulnerabilities. Specifically, it is designed to detect SQL injection vulnerabilities in dynamic Web pages that will be indexed by search engines, but it can be used to test virtually any kind of Web site that supports basic HTTP proxies and does not require authentication.

SQL Inject-Me works like XSS-Me, only it tests for SQL injection vulnerabilities. It works by sending database escape strings through the form fields. It then looks for database error messages that are output into the rendered HTML of the page.

Exploit-Me is a suite of Firefox Web application security testing tools. It is designed to be lightweight and easy to use. Exploit-Me integrates directly with Firefox and consists of two tools: XSS-Me and SQL Inject-Me.

XXS-Me tests for reflected cross-site scripting (XSS), but not stored XSS. It works by submitting HTML forms and substituting the form value with strings that are representative of an XSS attack.

2.3) Locating IP addresses

Nslookup queries DNS information for host name resolution. It is bundled with both UNIX and Windows operating systems and can be accessed from the command prompt. When Nslookup is run, it shows the host name and IP address of the DNS server that is configured for the local system, and then displays a command prompt for further queries. This starts interactive mode, which allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain.

The best way to find the route to a target system is to use the Traceroute utility provided with most operating systems. This utility can detail the path IP packets travel between two systems.

McAfee Visual Trace, previously known as NeoTrace, shows Traceroute output visually.

Several operating systems provide a WHOIS utility. The following is the format to conduct a query from the command line:

whois -h <host name> <identifier>

In order to obtain a more specific response, the query can be conducted using flags, many of which can be used with one another. These flags must be separated from each other and from the search term by a space.

Hide Real IP automatically locates anonymous proxy servers and routes Internet traffic through them so the user's IP is invisible. This makes it almost impossible for anyone to track the user.

whatismyip.com can be used to see a computer's external IP address.

IP Detective Suite monitors IP addresses for changes and then reports those changes though the user's FTP site or e-mail.

Enterprise IP-Address Manager assigns, catalogs, and maintains IP addresses and host data for both registered and private TCP/IP-addressed networks. It provides a simple interface for establishing and applying IP addressing schemes and standards.

Whois Lookup is an online tool offering both WHOIS lookup and domain name search.

ActiveWhois is a WHOIS program that has a "WHOIS-hyperlink" feature, allowing users to browse its results just like browsing the Web

LanWhoIs is a WHOIS program that saves its results in HTML files for later viewing in Web browsers. It integrates with Internet Explorer and can be launched from other applications.

CountryWhois is a WHOIS program focused on determining the geographic location of an IP address.

IP2country is a lightweight tool for determining the geographical location of an IP address or host.

CallerIP reports the IP addresses of any computer connected to the current system. It can also run a trace on that IP address.

2.4) DoS Attacks

Nmap, short for "Network Mapper," is an open-source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works against single hosts.

Nmap uses raw IP packets to determine what hosts are available on the network, what services and ports they are offering, what operating system they are running, what type of packet filters and firewalls are in use, and dozens of other characteristics.

Friendly Pinger is an application for network administration, monitoring, and inventory.

IPHost Network Monitor allows availability and performance monitoring of mail, database, and other servers; Web sites; applications; and various other network resources

Admin's Server Monitor is a tool to monitor server disk traffic loaded over a network. It gathers data for ranges from ten seconds to a full month and displays it in real time. It can show data from a remote PC with its console program.

Tail4Win, a Windows version of the UNIX tail -f command, is a real-time log monitor and viewer that can be used to view the end of a growing log file. Users can watch multiple files at once and monitor their changes in real time but cannot make any changes to those files. Using Tail4Win is significantly faster than loading an entire log file because it is only concerned with the last part of the log, so users can monitor changes to logs as they occur and watch for suspicious behavior.

Status2k provides server information in an easy-to-read format, with live load, uptime, and memory usage. The administration page displays a number of system statistics such as logs, port connections, users logged into SSH, and more. The whole administration page is in real time, showing how many connections there are to HTTP, SSH, POP3, MySQL, and the current top processes. Status2k can be viewed remotely from a Web browser.

DoSHTTP is an HTTP flood DoS testing tool for Windows. DoSHTTP includes URL verification, HTTP redirection, port designation, performance monitoring and enhanced reporting. DoSHTTP uses multiple asynchronous sockets to perform an effective HTTP flood. DoSHTTP can be used simultaneously on multiple clients to emulate a DDoS attack.

2.5) Cyber crimes

Nslookup is a valuable tool for querying DNS information for host name resolution. It is bundled with both UNIX and Windows and is accessed from the command prompt. When a user runs Nslookup, it shows the host name and IP address of the DNS server that is configured for the local system, and then it displays a command prompt for further queries. This is the interactive mode. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain.

Grab-a-Site is a file-based offline browser that allows a user to grab complete sections of the World Wide Web. When a user grabs a site, it is downloaded onto the user's hard drive. The user can tell Grab-a-Site specifically which sites to grab and which sites to exclude, using filters.

SurfOffline is an offline browser that is capable of downloading up to 100 files simultaneously. The software can save a partial or complete copy of a Web site to a user's hard drive in just a few minutes. Another important feature is a wizardlike interface that enables users to quickly set up downloading rules. The program supports HTTP, SSL (HTTPS), FTP, proxy servers, CSS, Macromedia Flash, and JavaScript parsing.

My Offline Browser is an offline browser that allows a user to automatically download and save entire Web sites, including all pages, images, Flash, and other files to the user's hard disk. My Offline Browser changes all the links in the HTML code to relative local links, so a user can browse the downloaded Web sites offline using a regular Web browser or the built-in browser.

My Offline Browser is a bot that downloads a page and then goes to all the links on that page. It continues following links on the linked pages until it runs out of links.

The Wayback Machine is a Web-based utility that allows users to browse through 85 billion Web pages archived from 1996 to just a few months ago.

VisualRoute is a graphical tool that determines where and how virtual traffic is flowing on the route between the desired destination and the location from which the user is trying to access it. It provides a geographical map of the route and performance information about each portion of that route.

NeoTrace is a diagnostic and investigative tool that traces the network path across the Internet from the host system to a target system. Automatic retrieval of data includes

registration details for the owner of each computer on the route (address, phone number, and e-mail address) and the network to which each node IP is registered. Views of the data include a world map showing the locations of nodes along the route, a graph showing the relative response time of each node along the path, and a configurable list of node data.

NetScan Tools is an advanced Internet information-gathering program for Windows. An investigator can use it to research IP addresses, host names, domain names, e-mail addresses, and URLs automatically or with manual tools.

Online Virus Scan is a fast and free tool that detects and removes threats on your PC.

3) Others

WebAgain detects and repairs damage caused by attackers. When an attack is detected, it automatically reposts the original content and sends an e-mail notification to the user. A single installation can protect multiple Web sites.

Pandora FMS is open-source monitoring software for any operating system. It displays vital information about systems and applications, including defacement, memory leaks, and more. It can also monitor any kind of TCP/IP service, without the need to install agents, and monitors network systems such as load balancers, routers, switches, operating systems, applications, or simply printers. Pandora FMS also supports SNMP for collecting data and for receiving traps.

The CounterStorm-1 suite of network security appliances automatically detects and stops attacks within seconds.

4) Routers

The Router Audit Tool (RAT) downloads configurations of devices to be audited and then checks them against the settings defined in the benchmark. For each configuration examined, RAT produces a report

Link Logger enables users to see and learn about Internet security and their network traffic. Link Logger is designed to take the logging information sent out from a router or firewall, process it, and then display it in a fashion that allows the user to see what is happening at the router or firewall. This allows the user to see how many scans and attacks are occurring, when and where they are coming from, and what kinds of scans and attacks they are. It also provides a link to further information concerning the details of a scan or attack.Link Logger allows users to see when new scans or attacks are released, their effects on the Internet, and if they are a threat to a network.

Sawmill is a Linksys router log analyzer. Sawmill processes router log files, analyzes them, and then generates a report based on the analysis.

5) Emails

SPAM Punisher tool makes the search for a spammer's ISP address easy. It automatically detects forged addresses. SPAM Punisher supports various e-mail client programs such as Microsoft Outlook, AOL,Hotmail, and Eudora. SPAM Punisher generates and sends complaints to the ISP regarding spamming.

Spam Arrest protects accounts against spam. It uses challenge/response antispam technology. It allows a user to access his or her e-mail from any Web browser, without having to install any additional software. Spam Arrest works with a user's existing e-mail address, including AOL, Hotmail, and Yahoo!. A user can also use Spam Arrest with Eudora, Thunderbird, and other standalone e-mail clients.

Email Dossier is part of the CentralOps.net suite of online network utilities. It is a scanning tool that an investigator can use to check the validity of an e-mail address. It provides information about the e-mail address, including the mail exchange records of the e-mail address. This tool initiates SMTP sessions to check address acceptance, but it never actually sends e-mail.

MailDetective is an effective tool for monitoring corporate e-mail usage in Microsoft Exchange Server.

FTK has file-filtering and search functionality. FTK's customizable filters allow investigators to sort through thousands of files to quickly find the evidence they need.

FINALeMAIL can scan e-mail databases to locate deleted e-mails that do not have any data location information.This tool can recover e-mails lost through virus infection, accidental deletion, and disk formatting. FINALeMAIL not only restores single messages to their original state but also has the capability to restore whole database files. Supports Outlook Express and Eudora.

R-Mail is an e-mail recovery tool. It restores deleted Outlook and Outlook Express e-mail messages. R-Mail can also recover Outlook and Outlook Express data files if they have been damaged. Recovered data are stored in .eml, .pst, or .msg format so they can be imported into Outlook or Outlook Express.An investigator can also view recovered messages within R-Mail. This tool is of vital importance if a suspect has deleted e-mail messages intentionally.

E-Mail Detective allows investigators to extract all e-mail contents (including graphics) from cached AOL e-mails stored on a user's disk drive. An investigator can run E-Mail Detective from a USB jump drive for field investigations.

E-mail Examiner allows investigators to recover deleted e-mail messages. It can even recover deleted messages that have been removed from the Deleted Items folder. E-mail Examiner supports over 15 different mail types, including AOL, Microsoft Outlook, Eudora, Mozilla, MSN, and Pegasus.

Network E-mail Examiner allows an investigator to examine a variety of network e-mail archives. This tool views all the individual e-mail accounts in e-mail stores and the associated metadata. Network E-mail Examiner reads Microsoft Exchange, Lotus Notes, and Novell GroupWise e-mail stores. Network E-mail Examiner is designed to work with E-mail Examiner. The outputs are compatible, so an investigator can load one tool's output into the other tool for further analysis.

Recover My Email for Microsoft Outlook is an e-mail recovery tool.

Outlook Recovery restores messages and attachments that have been deleted from the Deleted Items folder in Outlook. It also repairs damaged .pst and .ost files for all versions of Outlook. Outlook Recovery can scan an entire hard drive for damaged Outlook database files. It can often even restore files on damaged hard drives.

Tracing e-mail begins with looking at the message header. All e-mail header information can be faked except the “Received” portion referencing the victim’s computer (the last received).

eMailTrackerPro analyzes e-mail headers and provides the IP address of the machine that sent the e-mail. It also provides the graphical location of that IP address so an investigator can track down the sender

ID Protect protects a domain owner’s contact information from becoming public. The WHOIS database contains a domain owner’s address, phone number, and other private information. ID Protect’s dynamic e-mail system constantly changes the e-mail address visible in the WHOIS database, so any spammer that harvests the address will get an invalid address. A user’s private information is held in confidentiality and protected by the Domain Privacy Protection Service. The Domain Privacy Protection Service secures and maintains the user’s real

e-mail address on file so he or she receives important information regarding his or her domain.

6) Enterprise

Activity Monitor allows an administrator to track how, when, and what a network user did on any LAN. The system consists of server and client parts.

Spector CNE provides an organization with a complete record of employee PC and Internet activity. Spector CNE collects information about every e-mail sent and received, every chat conversation and instant message, every Web site visited, every keystroke typed, and every application launched. It also provides detailed pictures of PC activity via periodic screen snapshots.

Track4Win monitors all computer activities and Internet use. With powerful network support, it can easily collect application running times track Internet use information through the network, log this information in a database, analyze the information, and produce reports.

SpyBuddy monitors the computer usage of employees. It enables an administrator to track every action on a PC, down to the last keystroke pressed or the last file deleted. SpyBuddy is equipped with the functionality to record all AOL/ICQ/MSN/AIM/Yahoo! chat conversations, all Web sites visited, all windows opened and interacted with, every application executed, every document printed, every file or folder renamed and/or modified, all text and images sent to the clipboard, every keystroke pressed, every password typed, and more.

NetVizor is an employee monitoring solution. NetVizor allows an administrator to monitor the entire network from one centralized location. The administrator can track workstations, or he or she can track individual users who may use multiple systems on the network.

Privatefirewall is a personal firewall and intrusion detection application that eliminates unauthorized access to a PC. Its interface allows users to create custom configurations.

Internet Spy Filter blocks spyware, Web bugs, worms, cookies, ads, scripts, and other intrusive devices. When a user is online, an attacker may be monitoring the user

without his or her knowledge or explicit permission. These attackers may try to obtain private information about the user. Internet Spy Filter removes viruses and spyware, and acts as a personal firewall.

Spybot—Search & Destroy detects and removes spyware. Spyware silently tracks a user's Internet behavior. This tracking data is then often used to create a marketing profile for the user that is transmitted without the user's knowledge and sold to advertising companies. Spybot—Search & Destroy can also clear usage tracks—a useful function if a user shares a computer with other users and does not want them to see what he or she has been working on.

SpyCop finds spy programs designed specifically to record screenshots, e-mail, passwords, and more. It detects and disables all known commercially available PC surveillance spy software products.

Spyware Terminator is an adware and spyware scanner. It can remove spyware, adware, Trojans, keyloggers, home-page hijackers, and other malware threats.

XoftSpySE is a spyware detection, scanning, and removal tool, protecting users from unwanted spyware.

Spy Sweeper detects and removes traces of spyware, including Trojans, adware, keyloggers, and system monitoring tools. It has the ability to run spyware scans automatically, prevent new malware from being installed, and prevent unauthorized system changes to browser settings, startup programs, and so on.

CounterSpy detects and removes adware and spyware.

SUPERAntiSpyware scans computer systems for known spyware, adware, malware, Trojans, dialers, worms, keyloggers, hijackers, and many other types of threats.

iMonitorPC monitors computer activities and Internet use by employees. It helps in discovering employee productivity and documents any computer or network abuse.

7) File Analysis

The Stanford Copy Analysis Mechanism (SCAM) is another system designed for detecting plagiarism, copies, extracts, and strongly similar documents in digital libraries. The main difference between SCAM and COPS is that SCAM is a word-based scheme, whereas

COPS is sentence-based. The problem with simply comparing sentences is that partial sentence overlaps are not detected.

CHECK maintains a database for registered documents in order to compare them with the new document. With the help of the IR system, CHECK filters out the probable plagiarism candidates. Later, the IR process is applied to sections, subsections, paragraphs, and finally individual sentences.

JPlag detects software plagiarism by identifying the similarities between multiple sets of code files. It does not compare the bytes of the text, but it compares the programming language syntax and program structure in order to distinguish the similarities between plagiarized files.

The Visual Analysis of Similarity Tool (VAST) offers an interactive visualization of two different documents and highlights the areas that are plagiarized. It is used to investigate the extent and similarity of the text that is detected by tools like PRAISE

SIM, or Software Similarity Tester, is used to detect the similarity between two computer programs. It examines the correctness, style, and uniqueness of the program

PLAGUE, or Plagiarism in University Environments, is an open repository of resources assisting students and academics in detecting plagiarism in software code and protecting themselves against it.

SPlaT checks documents for any similarity between them.

Sherlock is a command-line program that finds the similarities between textual documents. It uses digital signatures for finding similar pieces of text in the documents. It works with text files, source code files, and assignments that are in digital form.

Urkund checks documents against Web pages, published material, and other documents. After checking the documents, it sends an overview via e-mail. It exempts quotations from comparison and handles 300 different file types.

Plotted Ring of Analyzed Information for Similarity Exploration (PRAISE) examines all the documents that are collected and plots them on a torc in a sequence determined by gross nonoriginality. A group of documents that are associated with a particular document are highlighted. A pair of documents can be selected for further investigation in VAST.

SafeAssignment analyzes any text, sentence by sentence, in order to determine whether the sentences are taken from the Internet or from its databases. It creates convenient and easy-to-read reports where all the unoriginal content is highlighted.

EVE2 determines if information is plagiarized from the World Wide Web. It accepts essays in plain text, Microsoft Word, or Corel WordPerfect format, and returns links to Web pages from which material may have originated, without too many false positives. Once the search is completed, a full report, including the percentage of the essay plagiarized and an annotated copy of the paper showing plagiarism highlighted in red, is presented.

WCopyfind extracts the text portions of a collection of document files. It then searches them for matching words in phrases of a specified minimum length. If WCopyfind finds two files that share enough words in those phrases, it generates a report in HTML format. The report contains the text of both documents with the matching phrases underlined. It can handle text, HTML, and some older word processor files.

iThenticate compares documents to a publications database comprising more than 10,000 major newspapers, magazines, and journals. It is designed to provide service for corporate organisations.

The Glatt Plagiarism Screening Program (GPSP) is a comprehensive computer software program specifically designed for detecting plagiarism.

The Haihaisoft Media DRM Platform enables the secure deployment of digital audio and video media. It provides a media DRM packager and an online management account.

LockLizard is a document security and copy-protection program for PDF files, Flash files, e-books, and Webbased content. It protects information with strong encryption and DRM controls to ensure complete protection against copyright infringement. It can stop copying, prevent printing, disable Print Screen, expire content, and instantly revoke access to information. It provides copyright protection without the use of passwords to ensure maximum security, and to protect information, documents, and Web content from unauthorized use no matter where it resides.

IntelliProtector is a software activation service with a Web-based control panel that helps reduce a form of piracy known as casual copying. Casual copying is when people share software in a way that infringes on the software's end-user license agreement (EULA).

Reveal allows parents to quickly evaluate the files on a system for the presence of child pornography. It works by comparing each word inside text files against special dictionaries of words commonly used by pedophiles, child pornographers, and other types of criminals. It also searches for image, video, and audio files on a system so parents can review those files for objectionable content.

iProtectYou is an Internet filtering and monitoring program that enables users to control when the Internet can be used and which Web sites can be accessed through the computer. iProtectYou is designed for parents who are concerned about the possible detrimental effects of the Internet on the development of their children. iProtectYou is also designed for schools and libraries, so that they can control what is being viewed in public spaces.

Web Control for Parents is a parental control tool, developed specially for protecting children from forbidden materials such as pornography, online gambling, and online drug information. It allows parents to view what Web sites their children visited and block any that the parents find objectionable.

BrowseControl controls access to the Internet and blocks the usage of certain applications. Parents can also use it to block access to floppy disks, CD drives, and USB drives.

ChatGuard is software developed to protect children from online sexual solicitation.

CETS was developed jointly by Microsoft Canada, the Royal Canadian Mounted Police (RCMP), and the Toronto Police Service. CETS is a software solution that allows different law-enforcement agencies to collaborate. It also provides investigators with a set of software tools they can use when investigating child pornography. The tracking system serves as a repository of information. The software enables police agencies to capture, share, and search information.

BinText Finds Ascii, Unicode and Resource strings in a file.

DumpAutoComplete v0.7 Dump Firefox AutoComplete files into XML.

Galleta A Internet Explorer Cookie Forensic Analysis Tool.

Pasco Parses index.dat files.

8) Data Recovery

8.1) Partition Recovery

NTFS Partition Recovery Stellar NTFS Data Recovery Software to recover data from Windows based NTFS/NTFS5 file systems

CD/DVD Diagnostic Recover data and video from CDs/DVDs/Blu-Ray. This is specifically not for forensic purposes but for data recovery. A different tool called CD/DVD Inspector is for forensic examination of optical media.

Partition Table Doctor Recover deleted or lost partitions (FAT16/FAT32/NTFS/NTFS5/EXT2/EXT3/SWAP).

NTFS Recovery DiskInternals : NTFS Recovery is a fully automatic utility that recovers data from damaged or formatted disks.

Gpart is a tool which tries to guess the primary partition table of a PC-type hard disk in case the primary partition table in sector 0 is damaged, incorrect or deleted.

TestDisk is an OpenSource software and is licensed under the GNU Public License (GPL).

Partition Recovery software for NTFS & FAT system that examines lost windows partition of damaged and corrupted hard drive.

8.2) File Recovery

CnW Recovery Data recovery sofware for all file and media types. Recovers corrupted, formatted, repartitioned and deleted files. RAID option and tools for HP MediaVault. Optional forensic logging.

Stellar Data Recovery Data recovery software services & tools to recover lost data from hard drive.

HD Doctor Suite is a set of professional tools used to fix firmware problem

SalvationDATA Claims to have a program that can read the "bad blocks" of Maxtor drives with proprietary commands.

BringBack offers easy to use, inexpensive, and highly successful data recovery for Windows and Linux (ext2) operating systems and digital images stored on memory cards, etc.

RAID Reconstructor Runtime Software's RAID Reconstructor will reconstruct RAID Level 0 (Striping) and RAID Level 5 drives.

e-ROL Erol allows you to recover through the internet files erased by mistake. Recover your files online for free.

Recuva is a freeware Windows tool that will recover accidentally deleted files.

Restoration is a freeware Windows software that will allow you to recover deleted files

Undelete Plus is a free deleted file recovery tool that works for all versions of Windows (95-Vista), FAT12/16/32, NTFS and NTFS5 filesystems and can perform recovery on various solid state devices.

R-Studio is a data recovery software suite that can recover files from FAT(12-32), NTFS, NTFS 5, HFS/HFS+, FFS, UFS/UFS2 (*BSD, Solaris), Ext2/Ext3 (Linux) and so on.

DeepSpar Disk Imager is a dedicated disk imaging device built to handle disk-level problems and to recover bad sectors on a hard drive.

Adroit Photo Recovery is a photo recovery tool that uses validated carving and is able to recover fragmented photos. Adroit Photo Recovery is able to recover high definition RAW images from Canon, Nikon etc.

FreeRecover is a small program that can recover deleted files from NTFS drives.

8.3) Carving

CnW Recovery Data carving tools and will recover most know file types. For some formats the files are verified and intelligent names added based on file metadata. Several video formats can be reconstructed from isolated fragments.

NFI "Defraser is a forensic analysis application that can be used to detect full and partial multimedia files in datastreams. It is typically used to find (and restore) complete or partial video files in datastreams (for instance, unallocated diskspace)." Written in C#; runs on Windows.

Foremost is a console program to recover files based on their headers, footers, and internal data structures.

Scalpel is a fast file carver that reads a database of header and footer definitions and extracts matching files from a set of image files or raw device files. Scalpel is filesystem-independent and will carve files from FATx, NTFS, ext2/3, or raw partitions.

EnCase comes with some enScripts that will do carving.

CarvFs A virtual file system (fuse) implementation that can provide carving tools with the possibility to do recursive multi tool zero-storage carving (also called in-place carving). Patches and scripts for scalpel and foremost are provided. Works on raw and encase images.

LibCarvPath A shared library that allows carving tools to use zero-storage carving on carvfs virtual files.

midi-carver is a data carver for MIDI files.

PhotoRec is file data recovery software designed to recover lost files including video, documents and archives from Hard Disks and CDRom and lost pictures (thus, its 'Photo Recovery' name) from digital camera memory.

PhotoRescue Advanced is picture and photo data recovery solution made by the creators of IDA Pro. PhotoRescue will undelete, unerase and recover pictures and files lost on corrupted, erased or damaged compact flash (CF) cards, SD Cards, Memory Sticks, SmartMedia and XD cards.

ReviveIt Revive It (RevIt) is an experimental carving tool, initially developed for the DFRWS 2006 carving challenge. It uses 'file structure based carving'. Note that RevIt currently is a work in progress.

Magic Rescue is a file carving tool that uses "magic bytes" in a file contents to recover data.

X-Ways Forensic provides a robust list of file types as well as the ability to specific custom file headers/trailers. File types are available for carving, identification and filtering.

Belkasoft Evidence Center Belkasoft Forensic Carver and Belkasoft Evidence Center support data carving for Instant Messenger and Browser artifacts. These tools support carving of physical or logical Windows drives as well as popular forensic image formats like Encase Evidence Files, DD or SMART.

9) Memory Imaging

9.1) Windows Software

[WindowsSCOPE] Pro, Law Enforcement, available at http://www.windowsscope.com

Can capture, analyze, graph in depth physical and virtual memory codes and structures. Proprietary and standard formats (windd), snapshot repository, snapshot comparison. All Windows OSs (Xp, Vista, 7), 32 and 64 bit supported

Phantom Probe USB based fetch

PCIe card and ExpressCard for hardware-assisted DRAM acquisition launched in 2011

WindowsSCOPE Live available at http://www.windowsscope.com and Android market Allows live memory analysis of Windows computers from Android phones and tablets. Launched in 2011

MANDIANT Memoryze

Can capture and analyze memory. Supports reading dumps (raw/dd format) from other tools. http://www.mandiant.com/software/memoryze.htm

MoonsolsDumpIt

This utility is used to generate a physical memory dump of Windows machines. It works with both x86 (32-bits) and x64 (64-bits) machines.

The raw memory dump is generated in the current directory, only a confirmation question is prompted before starting.

Perfect to deploy the executable on USB keys, for quick incident responses needs.

http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7

HBGary

Fastdump and Fastdump Pro

Fastdump (free with registration) Can acquire physical memory on Windows 2000 through Windows XP 32 bit but not Windows 2003 or Vista.

Fastdump Pro Can acquire physical memory on Windows 2000 through Windows 2008, all service packs. Additionally, Fastdump Pro supports:

- 32 bit and 64 bit architectures
- Acquisitions of greater than 4GB
- Fast acquisitions through the use of larger page sizes (1024KB) but also supports a strict mode that enforces 4KB page sizes.
- Process probing which allows for a more complete memory image of a process of interest.
- Acquisition of the system page file during physical memory acquisition. This allows for a more complete memory analysis.

FTK Imager can acquire live memory and paging file on 32bit and 64bit systems.

9.2) Linux/Unix

/dev/mem

On Unix systems, the program dd can be used to capture the contents of physical memory using a device file (e.g. /dev/mem and /dev/kmem). In recent Linux kernels, /dev/kmem is no longer available. In even more recent kernels, /dev/mem has additional restrictions. And in the most recent, /dev/mem is no longer available by default, either. Throughout the 2.6 kernel series the trend has been to reduce direct access to memory via pseudo-device files. See, for example, the message accompanying this patch: http://lwn.net/Articles/267427/.

/dev/crash

On Red Hat systems (and derived distros such as CentOS), the crash driver can be loaded to create a pseudo-device for memory access ("modprobe crash"). This module can also be compiled for any system with minor effort, see http://gleeda.blogspot.com/2009/08/devcrash-driver.html. Note that acquisition from the resulting /dev/crash driver needs significant testing as reading the wrong segments of memory such as PCI or BIOS mapped memory can easily lead to hung systems.

Second Look

This commercial memory analysis product has the ability to acquire memory from Linux systems, either locally or from a remote target via DMA or over the network. It comes with pre-compiled Physical Memory Access Driver (PMAD) modules for hundreds of kernels from the most commonly used Linux distributions.

fmem (Linux)

fmem is kernel module, that creates device /dev/fmem, similar to /dev/mem but without limitations. This device (physical RAM) can be copied using dd or other tool. Works on 2.6 Linux kernels. Under GNU GPL.

Linux Tool Caveats: Most of the above tools all create raw devices equivalent to /dev/mem which is not safe to image. Care must be taken to avoid addresses that are not RAM backed. On linux /proc/iomem exposes the correct address ranges to image, marked with "System RAM".

9.3) Virtual Machine Environments

Qemu allows you to dump the memory of a running image using pmemsave.

e.g. pmemsave 0 0x20000000 /tmp/dumpfile

Xen allows you to live dump the memory of a guest domain using the dump-core command.

You can list the available machines to find the host machine you care about using xm list and see the configuration.

Dumping is a matter of sudo xm dump-core -L /tmp/dump-core-6 6

10) Disk Imaging

10.1) Hardware imagers

Data Compass

A hardware and software complex tool produced by SalvationDATA that can imaging data from bad sectors,unstable heads and other patient drives,for more information,you can login in the website:http://www.salvationdata.com

DeepSpar Disk Imager

Handles Data Recovery Imaging issues, drive instability, and bad sectors. http://www.deepspar.com/products-ds-disk-imager.html - Data Sheet and Whitepaper available for download from product web page.

Data copy king

Handles hard drive and flash drive Imaging issues, drive instability,bad sectors and even scratched drives. http://www.disk-imager.com/index.htm - Data Sheet and reviews available from product web page.

ICS Solo3

Supports USB, Firewire and SCSI drives. http://www.icsforensic.com/

Logicube Talon

Supports USB

PSIClone

Built-in PATA, SATA, USB and write blocker. http://www.thepsiclone.com/

Enhanced Error Handling and Logging

Voom HardCopy III

Allows destination drive to be formatted in NTFS.

10.2) Unix-based imagers

guymager

guymager supports all relevant forensic formats (dd, ewf, aff). It is very user friendly and faster than known commercial imagers running under Windwos. As it is based on libewf, it supports all the different subformats found in libewf.

http://guymager.sourceforge.net/

ewfacquire

Part of the libewf library package, ewfacquire can create evidence files in the EnCase and FTK Imager E0* (EWF-E01) and SMART s0* (EWF-S01) formats. ewfacquire calculates an MD5 hash while the data is being acquired. Ewfacquire provides support for byte swapping of media bytes. This is useful for dealing with big endian media on and little endian architectures and vice versa. It also has intelligent error recovery.

https://sourceforge.net/projects/libewf/

aimage

Part of the AFF system, aimage can create files is raw, AFF, AFD, or AFM formats. AFF and AFD formats can be compressed or uncompressed. aimage can optionally compress and calculate MD5 or SHA-1 hash residues while the data is being copied. It has intelligent error recovery, similar to what is in ddrescue.

AIR

AIR (Automated Image and Restore) is a GUI front-end to dd/dcfldd designed for easily creating forensic bit images.

http://air-imager.sourceforge.net/

dcfldd

A version of dd created by the Digital Computer Forensics Laboratory. dcfldd is an enhanced version of GNU dd with features useful for forensics and security, such as calculating MD5 or

SHA-1 hashes on the fly and faster disk wiping.

dd

A program that converts and copies files, is one of the oldest Unix programs. I can copy data from any Unix "file" (including a raw partition) to any other Unix "file" (including a disk file or a raw partition). This is one of the oldest of the imaging tools, and produces raw image files. Extended into dcfldd.

EnCase LinEn

Linux-based version of EnCase's forensic imaging tool.

dd_rescue

http://www.garloff.de/kurt/linux/ddrescue/

A tool similar to dd, but unlike dd it will continue reading the next sector, if it stumbles over bad sectors it cannot read.

iLook IXimager

The primary imaging tool for iLook. It is Linux based and produces compressed authenticatable image files that may only be read in the iLook analysis tool.

MacQuisition Boot CD

Provides software to safely image Macintosh drives.

OSFClone

http://www.osforensics.com/tools/create-disk-images.html

Self booting open source version of Tiny Core Linux using dc3dd with RAW and AFF support.

rdd

http://sourceforge.net/projects/rdd

Rdd is robust with respect to read errors and incorporates several other functions: MD5 and SHA-1 hashing, block hashing, entropy computation, checksumming, network transfer, and output splitting.

sdd

Another dd-like tool. It is supposed to be faster in certain situations.

Windows-based imagers

AccessData

Their ultimate tool lets you "READ, ACQUIRE, DECRYPT, ANALYZE and REPORT (R.A.D.A.R.)."

ASR

A tool for imaging and analyzing disks.

DIBS

Can image and convert many file formats. Also builds mobile toolkit.

EnCase

Can image with out dongle plugged in. Only images to E0* file.

FTK Imager by AccessData

Can image and convert many image formats. Including E0* (EWF-E01), s0* (EWF-S01) and dd. Also a free tool.

Ghost

FTK can read forensic, uncompressed Ghost images.

iLook

The IRS's set of forensic tools and utilities. iLook V8 can image in Windows.

Paraben

A complete set of tools for Windows (and handheld) products.

ProDiscovery

Images and searches FAT12, FAT16, FAT32 and all NTFS files.

X-Ways Forensics

Has some limited imaging capabilities. The output is raw format.

X-Ways Replica

Performs hard disk cloning and imaging. The output is raw format.