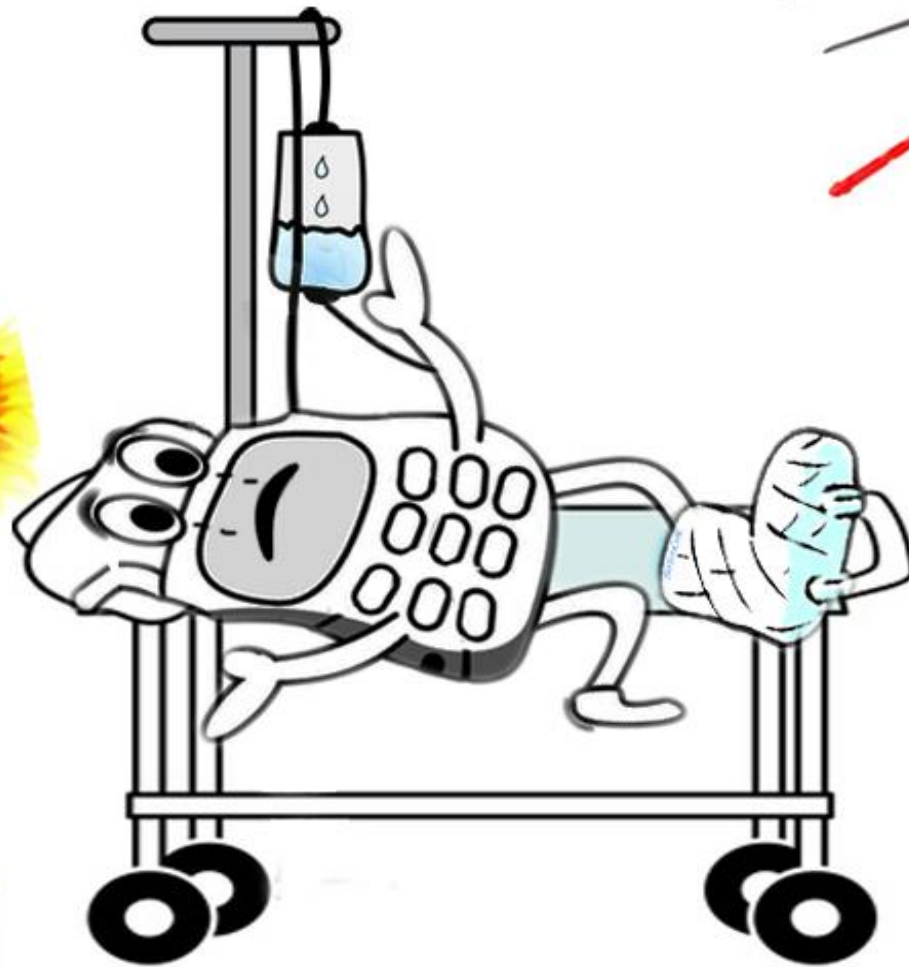


ClubHACKMag

1st Indian "HACKING" Magazine



Mobile Warfare



Issue 23 | Dec 2011
www.clubhack.com

TechGyan GSM | ToolGyan Echo Mirage|

Mom's Guide OWASP Mobile Security Project| Matriux Vibhag Forensics - Part III

LegalGyan Reasonable Security Practises under IT Act, 2008|

There was a time when mobile phones were of the size of a shoe and had no features other than calling and sms and at that time I used to play the game - Snake on my dads phone :p Now as the time has passed we have reached the age of smart phones which are capable of doing lot of stuff and world wide web of application causing serious concern where an attacker can use this platform to steal data. This issue of CHMag is dedicated Mobile/Telecom Hacking and Security.



Pankit Thakkar

The coverage of this December issue was released at ClubHack 2011, India's Pioneer International Hacking Conference held last week. Talking about ClubHack Conference, if you missed ClubHack here are the presentations available at - <http://www.slideshare.net/clubhack> and videos at <http://www.clubhack.tv/event/2011/>

We recently released CHMag's Collector's Edition Volume II. If you wish to buy the Collectors Editions (vol1 – from issue 1 to 10 & vol2- from issue 11 to 20), please write back to us: info@chmag.in. As of now its on demand printing.

Like the game - Snake, I have played lots of other games too which have reflected in the previous coverpages I have designed and yes I promise another awesome coveragepage based on a game on the theme of android security which would be the theme for an upcoming issue, for which send in your articles to info@chmag.in

ClubHACKMag

Issue 23, December 2011.

Team CHmag

Rohit Srivastwa
rohit@clubhack.com

Aarja Bhattacharyya
aarja@chmag.in

Abhijeet R Patil
abhijeet@chmag.in

Abhishek Nagar
abhishek@chmag.in

Pankit Thakkar
pankit@chmag.in

Varun V Hirve
varun@chmag.in

www.chmag.in
info@chmag.in

CONTENTS

Pg **TechGyan**
03 GSM

Pg **ToolGyan**
09 Echo Mirage

Pg **Mom'sGuide**
13 OWASP Mobile Security Project

Pg **LegalGyan**
17 Reasonable Security Practises under IT Act,2008

Pg **MatriuxVibhag**
22 Forensics - Part III



GSM

Introduction

In this article we will describe the various tools, software, hardware and techniques, that can be employed to attack the GSM. All these are described in brief and corresponding references are given so that you will be able to go and read more about the tool from the provided link.

GSM

GSM came into being during the late 1980s and was put into use in the western part of the world in the early 1990s. GSM has come a long way since then and has risen in both in terms of coverage as well as the number of subscribers. According to a survey of ITU there are about 4.1 billion people (approx 60%) who had a mobile subscription and about 90% of the people lived in an area having access to GSM [1]. India itself has around 0.865 billion mobile subscribers that is about 72% of the total population [2]. Besides communication, more and more additional services - like payment, one time passwords, tokens, sms banking etc are being deployed on top of GSM.

The GSM Problem

GSM is an old technology and it can also be regarded as one of the most successful one, but it has been over 20 years since GSM was designed, during that time several security problems have been discovered in GSM. However till recently it was not practically viable to exploit these weaknesses; partly due to the closed nature of the GSM protocol, but mostly due to all the complex signal processing involved and the high cost of the hardware needed for the same.

Here in this article we describe some currently available opensource hardware and software which can be used to play with GSM these include the Universal Software Radio Peripheral (USRP) together with the GnuRadio implementation for signal capturing and the AirProbe and OpenBTS project for handling GSM signals.

In the next section we describe the tools and tricks needed to get started playing with GSM.

Software Defined Radio (SDR)

Traditionally radios were a hardware matter, they were created to transmit and receive on specific frequencies and modulation scheme, (please note that the

word radio here is used as a generic transceiver using electro-magnetic waves for transmissions) not specifically as the device known for the reception of programmed FM broadcasts made by radio stations.

Then comes the Software Defined Radio (SDR), the main idea here is to create very versatile transceivers by emulating a lot of signal processing hardware in to the software domain. Therefore it has various advantages like costs and versatility. Imagine a universal radio with which you are able to tune in to wifi, Bluetooth, GSM, Satellite TV all with one piece of hardware and software, this is where the SDR's comes into picture, In an SDR the signal processing is implemented in software, so all that needed is a generic receiver that can receive and transmit over a range of frequencies and corresponding signal processing software viz software for processing GSM, Bluetooth, wifi etc. Still a radio can never be 100% software, some hardware is needed to capture and create radio waves.

So in a SDR all signal processing activities like (de)modulation etc. are done in software, but the actual trans-receiving is done via the hardware subsystem. This makes for a much more adaptable system, giving it the ability to receive GSM signals as well as GPS and also television broadcasts by only changing something in the software.

Now comes the next problem this ideal scheme however is not practically viable, because in practice software are not fast enough to process a large portion of the spectrum and antennas are designed for specific frequency bands. Therefore we have more extended hardware subsystems for SDRs. Typically such a hardware subsystem consists of a wide band receiver that shifts a frequency band to a standard intermediate

frequency, which can be sampled by ADCs (Analog to Digital converter) and the resulting digital signal can be sent to a computer. Often other common equipment like amplifiers and band-pass filters are also a part of the hardware subsystem. One of the most versatile and widely used SDR systems is GNU Radio, mostly combined with a USRP as the hardware subsystem.

USRP

The Universal Software Radio Peripheral (USRP) is designed as a general purpose hardware subsystem for software defined radio. It is an open-hardware device developed by Matt Ettus and which can be ordered through his company Ettus Research [3].

A USRP consist of a motherboard which contains a Field Programmable Gate Array (FPGA), Programmable Gain Amplifier (PGA), ADC(s), DAC(s) and a communication port to connect it to the computer. Special boards called 'Daughterboards' can be plugged into the USRP motherboard to tune in the specific frequency bands needed. These daughterboards can be hooked up to appropriate antenna's for reception similarly we have daughterboards for transmission as well.



Figure 1: An USRP 1

USRP Daughterboards

A variety of daughterboards are available for specific frequencies, this can be plugged into the USRP motherboard. Currently there are about 13-15 daughterboards available, of which three are interesting in relation to GSM signals[4]:

- DBSRX, a 800 MHz to 2.4 GHz Receiver.
- RFX900, 800-1000MHz Transceiver, 200+mW output.
- RFX1800, 1.5-2.1 GHz Transceiver, 100+mW output.
- The most used GSM frequencies are GSM900 (890.2-959.8 MHz) and GSM1800 (1710.2-1879.8

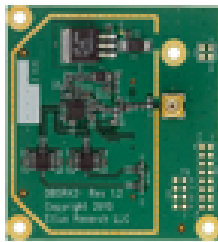


Figure 2: A DBSRX2 800 MHz to 2.35 GHz Receiver Daughterboard

MHz) in Europe, India also uses this [5], and GSM850 (824.0-894.0 MHz) and GSM1900 (1850.0-1990.0 MHz) in America and Canada. The DBSRX board covers all these frequencies, but is only a receiver board. In order to actively transmit a RFX board is needed. Keep in mind that most countries require a license to transmit on these frequencies.

Software tools that can be used for GSM analysis.

GNU Radio

GNU Radio started by Eric Blossom is a free toolkit under GPL license for implementing the software defined radios. Fundamentally GNU Radio is a library containing a variety of standard signal processing functions, these are known as blocks, typically there are hundreds of implemented blocks inside the GNU Radio implementation. These blocks are programmed to work with several different types of RF hardware but it is mostly used in combination with an USRP.

GNU Radio, fresh out-of-the-box, does not offer much in terms of GSM sniffing capabilities, although

it can be used to locate the beacon frequencies of GSM masts [18]. However GNU Radio is quite useful when used in tandem with other software packages, like AirProbe, to perform the low level functions of GSM sniffing, like reception and demodulation etc.

AirProbe

Airprobe [6] is an open-source project trying to built an air-interface analysis tool for the GSM (and possible later 3G) mobile phone standard. This project came forth out of the GSM-sniffer project [20]. The most interesting part of AirProbe is the gsm-receiver project. It is, at this moment, the best working capture tool for GSM.

Airprobe comes with two simple shell scripts that call all the necessary functions for saving the signals on a frequency to a file and for interpreting the signals in this file.

Calling

capture.sh <freq> [duration==10] [decim==112] [gain==52] with a frequency will capture the signals on that frequency to a file. The duration, decimation and gain are optional arguments with default values. A file will be created called capture_<freq>_<decim>.cfile, containing the captured IQ samples. These can then be interpreted by calling:

```
go.sh <file.cfile> [decim==112]
```

The file name has to be provided, but the decimation is again optional, though you should use the same decimation value that was used during capturing.

The go.sh script runs a python file that defines a software radio, which does all the processing needed to get the information bits out of the samples. This results in a series of hex values that represent the information as sent by the GSM network. The go.sh script uses a UNIX pipe method to have these hex-codes interpreted by gsmdecode - one of the other projects in the AirProbe repository. You could also try to convert these hex codes to a .pcap file, which can be read by the wireshark program [21].

Currently the gsm-receiver project will only decode the downlink (GSMnetwork to mobile phone).

At this moment it can handle several of the control channels in GSM (control channels will be discussed in section 4.2), and speech channels. However due to encryption (chapter 7) and frequency hopping (section 3.1.2) this will not yet work in most real world situations.

Gammu

Another good tool for capturing the GSM traces is by the uses of Gammu, which is a open source project which can manage various functions on cellular phones. In order to work with Gammu we will need a Nokia DCT3 enabled phone one such phone can be 3210. We can use Nokia phones here because, Nokia used a simple remote logging facility for debugging their DCT3 firmwares remotely but apparently forgot to remove this when going into production.

So this debugging functionality can be enabled it back using Gammu. A cable to connect the specific DCT3 phone to a computer is also needed. Once Gammu is installed on this computer [7] and the mobile phone is connected to the computer, you can run Gammu using the following commands:

```
gammu --nokiadebug nhm5_587.txt v20-25,v18-19
```

The software will then interface with the phone and create a .xml debug log of lots of packages sent to and from the mobile phone.

The .xml file that can be interpreted either by wireshark or AirProbe's gsmdecode [6].

The Gammu + Nokia phone method has a much better receive quality than the USRP + AirProbe, after all the mobile phone is specifically made to receive these signals.

OpenBTS/OpenBSC

Base Transceiver Station (BTS) is a GSM cell tower, and a Base Station Controller (BSC) is a control center for several BTSs. Both of these systems have an open-source

implementation: OpenBTS[8] and OpenBSC [9] respectively.

Both the software use different approaches to the same problem. OpenBTS, founded by David Burgess, offers a BTS implementation using the USRP and turning it into a BTS. Some of the logic normally present in a BSC is placed inside OpenBTS.

Whereas OpenBSC, developed by Harald Welte, on the other hand implements most of the BSC functions and currently includes support for two BTS types (nanoBTS and the Siemens BS-11 microBTS). It does not support an OpenBTS driven USRP.

With the help of these systems you can setup your personal GSM network, although this requires a licence in most countries, you will have to spend crores of rupees to bid for that spectrum ;)

A5/1 Cracking project

GSM communications in the countries across the world including India is encrypted using an algorithm known as A5/1. In August of 2009 a project was started to use a generic time-memory-trade-off to break A5/1, by pre-computing a large rainbow table. The pre-computation is done distributed on the Internet. Volunteers can download the table from the project's website [10], and run it on their own

computers. The probability of success with this table of decrypting the GSM communications is around fifty percent to find the encryption key for an encrypted conversation.

Sample GSM communications capture

Below figure shows a trace capture, the trace doesn't present information in a human friendly way. Therefore we use either Wireshark or gsmdecode to examine the traces.

Figure below shows what a trace examined with Wireshark looks like.

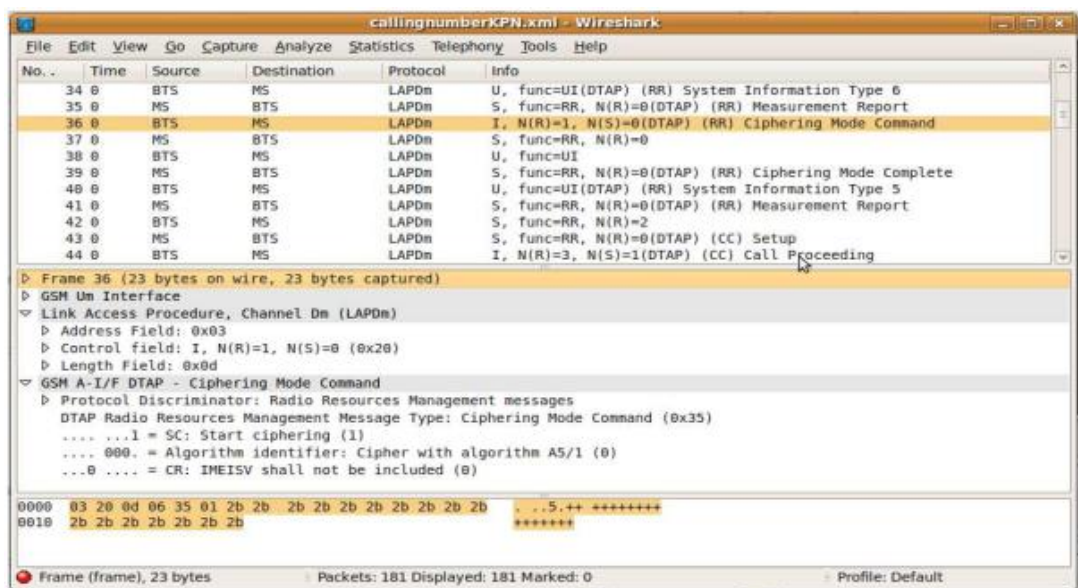


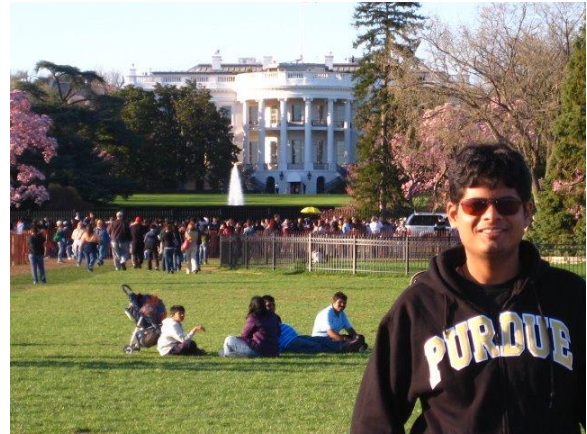
Figure 3

Wireshark is good tool for analyzing and decoding GSM traces, as it organizes all the information and conveniently shows extra information like the current frame number and frequency. The results of the interpreting with Wireshark (from version 1.2.6 on) are also better than those of Gsmdecode.

We end the article with a promise to come up with hands on tutorials on how to actually get our hands dirty trying to attack the GSM. If anyone is interested in knowing more about the current state of research on the same please feel free to email me at utsav [at] Xiarch [dot] com, questions, comments and any feedback is appreciated and will be rewarded.

References

1. Chris Tryhorn. Nice talking to you ... mobile phone use passes milestone. The Guardian, 2009. Tuesday 3 March <http://www.guardian.co.uk/technology/2009/mar/03/mobile-phones1>
2. http://en.wikipedia.org/wiki/List_of_countries_by_number_of_mobile_phones_in_use.
3. <http://www.ettus.com/company>.
4. <http://www.ettus.com/order>
5. <http://support.chinavasion.com/index.php?m=knowledgebase&a=viewarticle&kbarticleid=227#gsm-in>
6. <https://svn.berlin.ccc.de/projects/airprobe/wiki>
7. <https://svn.berlin.ccc.de/projects/airprobe/wiki/tracelog> and <http://www.gammu.org/>
8. <http://openbts.sourceforge.net/>
9. <http://bs11-abis.gnumonks.org/trac/wiki/OpenBSC>
10. <http://www.reflexor.com/trac/a51>



Utsav Mittal
utsav@Xiarch.com

Utsav, founder and Principal Consultant at Xiarch, (www.xiarch.com), earned his Masters in information security from CERIAS, Purdue University, USA. He also has a CISSP. Some of things that drive him in life are spirituality, info security and passion. He is a firm believer in God, who believes in living life to the fullest.



Echo Mirage

In the past few years, Web application security has really got some good attention. Because of this attention, we have so many proxy tools (Burp/Fiddler/Paros) readily available, are making our lives easy at each step of penetration testing.

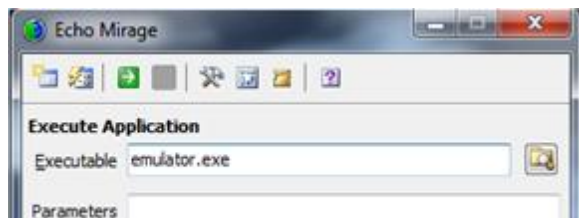
These tools are helpful when we can configure or force some applications to pass through their already configured proxy settings (IP address and port number) but what if some applications we want to test do not have that ability?? What if we have a process running in background (might be malware) and we want to see the packets that EXE is sending to the network?? Yes we can use network analyzer tool like Wireshark to capture and analyze the packets but using these tools you can only capture the packets, there is no option to tamper the packets at the runtime. If there is a requirement in which you just have to capture the packets and analyze them, Wireshark will suffice the needs, but if you really want to tamper the request and response (which we normally do using Paros/fiddler in web applications) you need to have a tool which can capture network packets and has a capability to intercept and tamper them.

To help this I would like to introduce you to a tool called Echo Mirage. This is just another excellent tool from the folks at

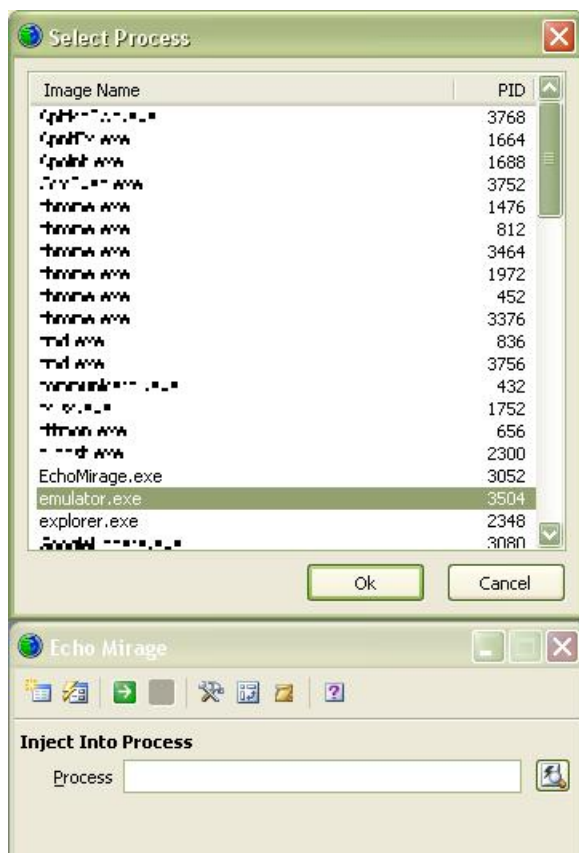
Bindshell.net, the same folks who created the famous 'BeEF'. Echo Mirage uses DLL injection and function hooking techniques to redirect network related function calls so that data transmitted and received by local applications can be observed and modified. Using these techniques this tool gives you an advantage that it will attach itself to a particular 'EXE', and only packets of that EXE are captured (in case of Wireshark we have to use filter as it captures each and every packet which goes out of the machine).

Since the theme for this edition is Mobile/Telecom Security, I would like to take an example of Android Emulator here. The problem with Android emulator is that, the proxy settings for emulator works only for the browser, it does not work with the apps installed inside the emulator. The best way is to use the base machine itself to capture the packets which emulator (the apps in emulator) is sending. This is where the tool like ECHO MIRAGE becomes very handy. To know how Echo Mirage does this all this, read through the next paragraph.

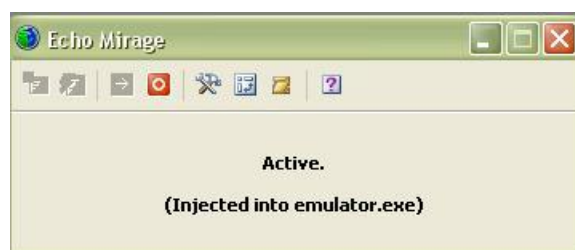
One way is to directly open an executable using echo mirage as shown in the screenshot below. You can also give the path and parameters for executing the exe using Echo Mirage. It will automatically inject the dll and start hooking the functions.



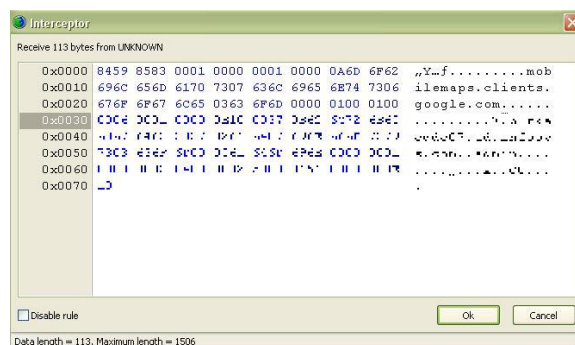
Another way is to inject into a process which is already running. Selecting this option will show you all the processes running on that system. For Echo Mirage to start its injection you just have to select any one of these processes and click on start.



If everything works fine, you will get a window show below which says “Injected into %PROCESS NAME%”.



Echo Mirage is now ready to trap and intercept all your requests which are sent through emulator.exe. The screenshot of interceptor below was taken when I tried to open Google Maps application in emulator after setting up Echo Mirage.

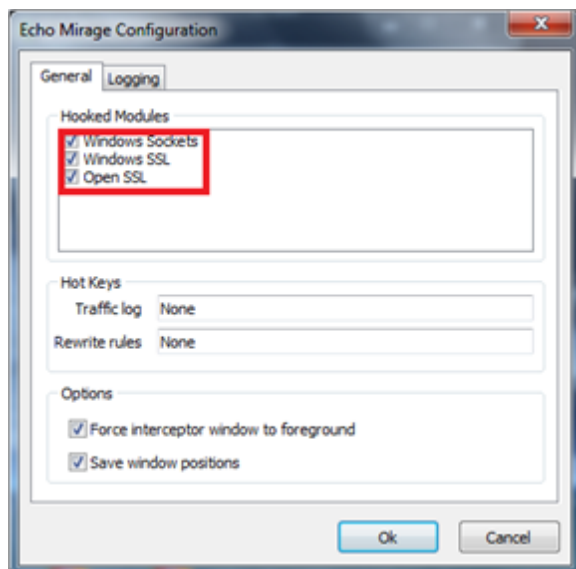


The interceptor tool intercepts the function calls in run time and unless you click on OK the request will not move forward. You can even tamper the request and response and then click on OK to move the request forward.

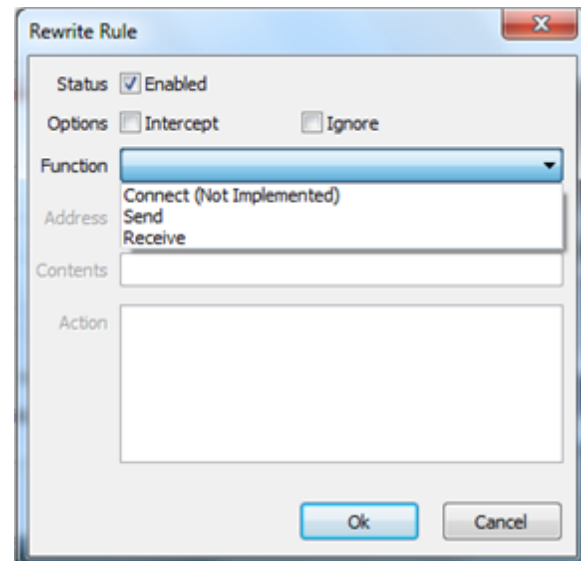
One great advantage of Echo Mirage is that it works on the calls made by process itself

and when the request is still within the application, while the other network proxy tools like burp etc intercept the requests when it has left the application.

There are many more features which makes this tool the “God of all proxies”. One of them is that in Echo Mirage, Windows encryption and OpenSSL functions are also hooked so that plain text of data being sent and received over an encrypted session is also available. This feature is not really available in any(almost) of the proxy tools.



Another one is that Traffic can be intercepted in real-time, or manipulated with regular expressions and action scripts.



This is not all, we would recommend you to run this tool and explore the features. The tool has been a life saver for us many times and for many projects we worked on.

I hope this article hits home and proves the necessity of input validations and security testing, even in thick client environments. As tools like Echo Mirage becomes more mature, this type of attack will only become more common and more dangerous. Thanks to Bindshell for developing such a wonderful tool.

About the Tool:

Name: Echo Mirage

Author: Dave Armstrong

Home Page:

<http://www.bindshell.net/tools/echomirage.html>

Latest Version: 1.2 (as on 1st DEC 2011)

**Ankur Bhargava**

ankurbhargava87@gmail.com

Ankur is Working in a MNC where his daily job includes research in Web application security, Penetration Testing. He is a Certified Ethical Hacker and has worked with Infosys Technologies where he did research on Malware Analysis, Penetration Testing, and Mobile Penetration Testing. Ankur was a speaker at CoCoN 2010, 2011 here he presented his paper on topic “Client Side Exploits Using PDF”, “Android Security”. Ankur is active member of null and OWASP Bangalore chapter.

**Ankit Goyal**

ankitgoyal06@gmail.com

Ankit is a diploma holder in “Information systems and Cyber security” from C-DAC Pune. He is a Certified Ethical Hacker and has a good knowledge in Network security, Vulnerability Assessment, Penetration Testing.



OWASP Mobile Security Project

What is the “Mobile Security Project”?

The OWASP Mobile Security Project is a centralized resource intended to give developers and security teams the resources they need to build and maintain secure mobile applications. Through the project, our goal is to classify mobile security risks and provide developmental controls to reduce their impact or likelihood of exploitation.



Top 10 Mobile Risks

The first version was released on September 23 rd, 2011 at AppSec USA by Jack Mannino, Zach Lanier and Mike Zusman. The Top 10 Risks is focused on areas of risks rather than a individual vulnerabilities, also is based on the OWASP Risk Rating Methodology.

1. Insecure Data Storage.
2. Weak Server Side Controls.
3. Insufficient Transport Layer Protection.
4. Client Side Injection.
5. Poor Authorization and Authentication
6. Improper Session Handling
7. Security Decisions via Untrusted Inputs.
8. Side Channel Data Leakage.
9. Broken Cryptography
10. Sensitive Information Disclosure.

M1 Insecure Data Storage

Sensitive data left unprotected, applies to locally stored data + cloud synced.

Impact

Confidentiality of Data Lost	Credentials Disclosed	Privacy Violations	Non-compliance
---------------------------------	--------------------------	-----------------------	----------------

M2 Weak Server Side Controls

Applies to the backend services. Not mobile specifically, but essential to get right.

Impact

Confidentiality of Data Lost	Integrity of Data not Trusted	-	-
---------------------------------	----------------------------------	---	---

M3 Insufficient Transport Layer Protection

Complete lack of encryption for transmitted data. Weakly encrypted data in transit.

Impact

Man-in-the-Middle Attacks	Tampering with Data in Transit	Confidentiality of Data Lost	-
------------------------------	-----------------------------------	---------------------------------	---

M4 Client Side Injection

Complete lack of encryption for transmitted data. Weakly encrypted data in transit.

Impact

Device Compromise	Toll Fraud	Privilege Escalation	-
-------------------	------------	-------------------------	---

M5 Poor Authorization and Authentication

Can be part mobile or part architecture. Some applications rely solely on immutable, potentially compromised values (IMEI, IMSI, UUID).

Impact

Privilege Escalation	Unauthorized Access	-	-
----------------------	------------------------	---	---

M6 Improper Session Handling

Mobile applications sessions are generally much longer. They use generally HTTP Cookies, OAuth Tokens, SSO Authentication Services.

Impact

Privilege Escalation	Unauthorized Access	Circumvent Licensing and Payments	-
----------------------	------------------------	---	---

M7 Security Decisions Via Untrusted Inputs

Can be leveraged to bypass permissions and security models. Several attack vectors like Malicious Apps, Client Side Injection.

Impact

Consuming Paid Resources	Data Exfiltration	Privilege Escalation	-
--------------------------	-------------------	----------------------	---

M8 Side Channel Data Leakage

Mix of not disabling platform features and programmatic flaws. Sensitive data ends up in unintended places.

Impact

Data Retained Indefinitely	Privacy Violations	-	-
----------------------------	--------------------	---	---

M9 Broken Cryptography

Two primary categories: A) Broken implementations using strong crypto libraries, B) Custom, easily defeated crypto implementations.

Impact

Confidentiality of Data Lost	Privilege Escalation	Circumvent Licensing and Payments	-
------------------------------	----------------------	-----------------------------------	---

M10 Sensitive Information Disclosure

Applications can be reverse engineered with relative ease. Code obfuscation raises the bar, but doesn't eliminate the risk.

Impact

Credentials Disclosed	Intellectual Property Exposed	-	-
-----------------------	-------------------------------	---	---

OWASP Mobile Security Project also has the Top 10 Mobile Controls and Design Principles.

1. Identify and Protect Sensitive Data on the Mobile Device
2. Handle Password Credentials Securely on the Device
3. Ensure Sensitive Data is Protected in Transit
4. Implement User Authentication/Authorization and Session Management Correctly
5. Keep the Backend APIs (Services) and the Platform (Server) Secure
6. Perform Data Integration with Third Party Services/Applications Securely
7. Pay Specific Attention to the Collection and Storage of Consent for the Collection and Use of the User's Data
8. Implement Controls to Prevent Unauthorized Access to Paid-for Resources
9. Ensure Secure Distribution/Provisioning of Mobile Applications
10. Carefully Check any Runtime Interpretation of Code for Errors.

The roadmap of this project includes: Threat Model, Top 10 Mobile Risks, Top 10 Mobile Controls and more.

You will find all the information here:

https://www.owasp.org/index.php/OWASP_Mobile_Security_Project



Maximiliano Soler

maximilianosoler@gmail.com

Maximiliano, a fanatic of open standards, is a security Analyst working in an International Bank and participating in some Projects like Vulnerability Database, Zero Science Lab, OWASP.

T:@maxisoler

F:maximiliano.soler

PGP ID: 0x1DDEDDB1E



Reasonable Security Practices under Information Technology (Amendment) Act, 2008

Organizations are required to take “reasonable security practices and procedures” to protect personal data or information of its customers. [The ICT Ministry with the recent clarification](#) has also settled the confusion which existed regarding the application of the Rules.

This post in the FAQ format is an effort to throw light on the expression “reasonable security practices and procedures” referred in the Information Technology (Amendment) Act 2008 and the Rules thereto.

1. What is meant by ‘reasonable security practice and procedures’?

[Rule 8 \(1\) provides the definition for reasonable security practices and procedures.](#) It states as follows

“A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.”

2. What are the major standards and frameworks on information security?

There are many standards, frameworks and guidelines on information security. While some standards are very exhaustive, some are domain specific or targeted towards a particular Industry sector. Organizations can choose from a wide variety of such standards/frameworks and guidelines. A compilation of the major standards and frameworks can be found [here](#).

3. What is ISO and does India have a stake in it?

International Organization for Standardization (ISO) is the world's largest developer and publisher of International standards. It is a network of the national standards institutes of 162 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. [India is a member of ISO](#) and is represented by the Bureau of Indian Standards (BIS).

4. What is ISO 27001 standard?

ISO 27001 is the widely-recognized international standard for information security. This information security standard is not new to the country. According to the International Register of ISMS Accredited Certificates, [India has 3rd highest number of ISO 27001 certified organizations](#). The best known Information Security

Management System (ISMS) is provided in this standard. It has a total of 133 Controls spread across 11 domains.

ISO 27001 Control Domain	Objectives	Controls
Information Security Policy	1	2
Organisation of Information Security	2	11
Asset Management	2	5
Human Resources Security	3	9
Physical and environmental security	2	13
Communication and Operation Management	10	32
Access Control	7	25
Information systems acquisition, development and maintenance	6	16
Information security incident management	2	5
Business Continuity Plan	1	5
Compliance	3	10
	39	133

Figure 4

5. Why is ISO 27001 given preference over standards?

ISO 27001 is preferred due to the following reasons:

1. **Certifiable:** It is a certifiable standard. Organizations can market their certification to earn new customers. The Certification indicates that a third party accredited independent auditor has performed an assessment of the processes and controls of the organization and confirms they are operating in alignment with the comprehensive ISO 27001 certification standard

2. Exhaustive: The 11 domains with 133 controls are exhaustive enough to address the major risks to any organization.

3. Flexibility: The standard gives management a lot of flexibility in selecting and implementing the controls in the standard. There is no stringent way prescribed for implementing the controls. ISO 27002 provides guidance on implementing the controls of ISO 27001.

4. Broad Applicability: It is a general standard that can be applied to any sector. While other standards have a specific targeted audience /purpose E.g.: BS 25999- Standard for Business Continuity and Disaster Management ISO 20000-ISO standard for IT service management.

PCI DSS- Information security standard for organizations that handle cardholder information

6. Has India mandated ISO 27001 as the default security standard for the country?

Rule 8 (2) of the notification says:

The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1). It means that organization can choose and adopt standards and best practices other than ISO 27001.

However, Rule 8 (3) says that organizations using other standards "shall get its codes of best practices duly approved and notified by the Central Government for effective implementation." The authorities to be approached or the procedure to be followed in such cases is missing in the rules. This ambiguity, legal hassles and inordinate delay that can be caused are the reasons why organizations are favoring ISO 27001 standard.

The Reserve Bank of India (RBI) too has given organizations the freedom to select their own security standards/frameworks while implementing Information Security Management Systems (ISMS).

RBI in January, 2011 released the 'Working Group report on information security, electronic banking, technology risk management, and cyber frauds'

Information Security is addressed in chapter 2 of the report. In the chapter references are also found to other frameworks like COBIT and ITIL. It is also stated that "Banks may also additionally consider other reputed security frameworks and standards from well-known institutions like ISACA, DSCI, IDRBT etc.

However, a strong emphasis is laid towards implementing "ISO 27001 based Information Security Management System (ISMS) Best Practices for critical functions/processes". Thus ISO

27001 has gradually gained acceptance as the defect information security standard for the country.

A similar position exists in Japan, where ISO 27001 has tacitly become the National Information Security Standard.

Due to this Japan today has the highest number of ISO 27001 certified organizations.

7. By implementing ISO 27001 are we 100 % secure?

Organizations cannot claim to be 100% secure by implementing ISO 27001. No standard or framework can guarantee 100% security. Security is not about compliance to a particular standard/framework. A good post on the topic can be found [here](#).

8. By implementing ISO 27001 can the organizations free themselves from the legal liabilities?

Compliance to ISO 27001 by itself will not absolve the organization from liabilities.

Rule 8 (1) states that:

“In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security

programme and information security policies.”

Therefore organizations will have to prove that they had carried out their due diligence activities.

For Example: Under Rule 8 (4) of the notification

The audit of reasonable security practices and procedures is to be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertakes significant up gradation of its process and computer resource.

9. What is the liability that can arise for being negligent in implementing and maintaining reasonable security practice and procedures?

Section 43A of Information Technology Act, 2008 speaks about the compensation to be paid for being negligent in implementing and maintaining reasonable information security practices and procedures. The section provides for damages to be paid by way of compensation to the person so affected.

It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances. Compensation claims upto Rs 5 crore are now handled by Adjudicating Officers while claims above Rs 5 crore are handled by the relevant courts.

10. Does India have its own Standard/framework?

India is keen on having a stringent framework for information security. However, a one size fits all approach cannot be taken. The country needs a framework which is flexible enough to meet the requirements of different sectors of the economy.

The Data Security Council of India has released a framework for [data security and privacy](#). These frameworks are currently under pilot implementation in some organizations in the country. It is hoped DSCI will release detailed toolkits for its implementation.

The Reserve Bank of India (RBI) has also released several guidelines relating to security in banks. Some of these guidelines can be applied to other sectors as well. The [Working Group report on information security, electronic banking, technology risk management, and cyber frauds](#) and [the checklist to facilitate conduct of computer audit](#) are the major ones among them.



S. Jacob

jacob.cybersecurity@gmail.com

S. Jacob is a lawyer and a cyber security enthusiast. He deals with technology laws focusing on cyber/information security regulations. He has experience advising clients on IT Governance, Risk Management, Security and Privacy Compliance. He also possesses a host of information security certifications. He blogs at www.eSuraksha.net



Forensics - Part III

Hi readers, in the previous forensics issues we have seen how to use Vinetto to analyse thumbs.db files from a machine or from an image. As a continuation to the early analysis tools, we have another in this issue.

In Forensics investigation web history is the major part to gather the evidences. Web traces can be found in index.dat files and other cookies.

Using Pasco we can find evidences in index.dat files which store IE and Chrome browsed cache, whereas Firefox has its own cache files.

PASCO

Pasco is a Latin word which means to Browse. It is used to analyze the index.dat files to get the Internet history from an IE installed machine. It is used to reconstruct the data from an index.dat file. Pasco gives the output in CSV format and it can be extracted to a spreadsheet. We can get some information as Record type, URL, Modified time, Access time, File name, Directory, HTTP headers from the index.dat file.

index.dat :

It is a repository of information such as web URLs, search queries and recently opened files. Its purpose is to enable quick access to data used by Internet Explorer. The index.dat file is user-specific and is open as long as a user is logged on in Windows. Separate index.dat files exist for the Internet Explorer history, cache, and cookies. These files are created for each and every user. A cookie is a small file containing data that the web server places on a user's computer so it may request back at a later date.

Some of the areas where you can find index.dat files is C:\documents and settings\user directory

How it is helpful for forensic analysis:

- To know the user internet activity
- To know user motto for accessing the internet

How to Use

Command to find index.dat in a HDD:

```
find /media/Drive -name index.dat
```

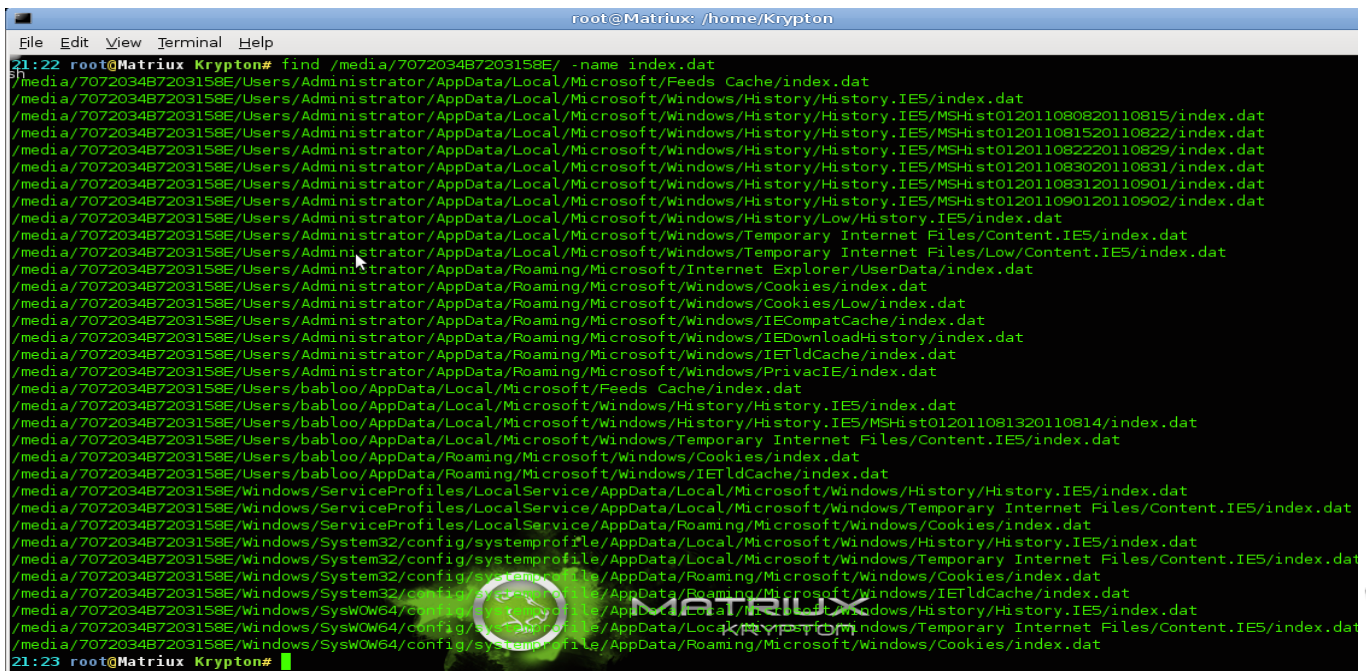
(See Figure 1)

Implementation

```
$ pasco Options "path of the index.dat file"
> path of excel file | any options to sort the data
```

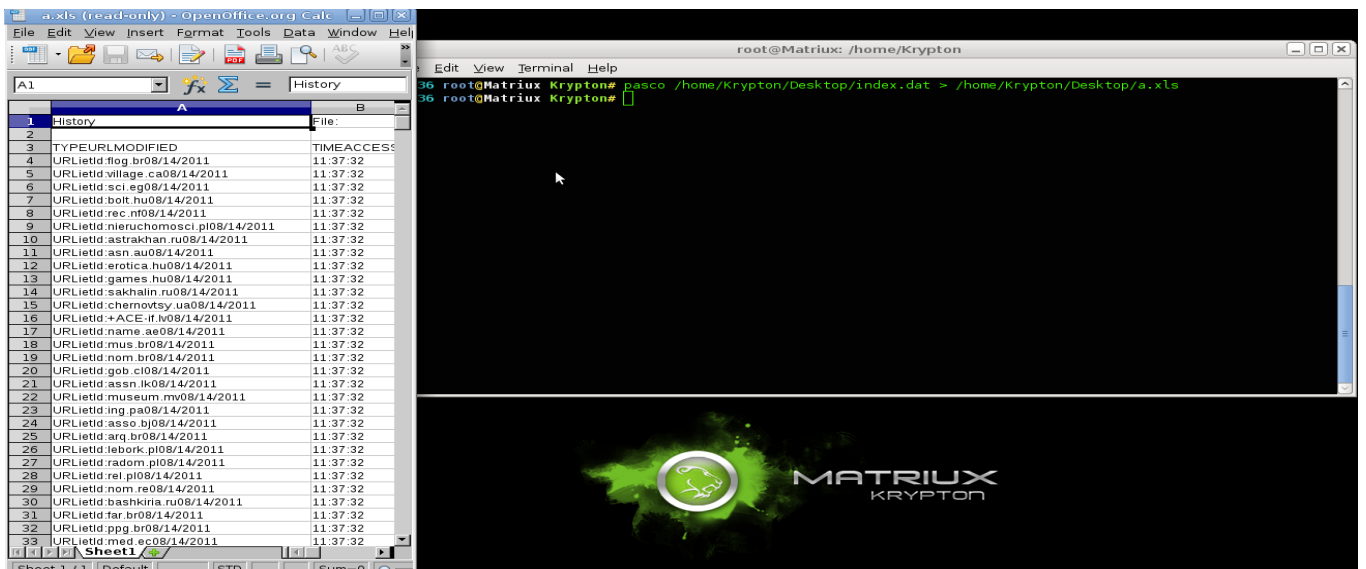
Example:

```
$ pasco
/home/Krypton/Desktop/index.dat
> /home/Krypton/Desktop/a.xls |
sort -M
```



```
root@Matriux: /home/Krypton
File Edit View Terminal Help
21:22 root@Matriux Krypton# find /media/7072034B7203158E/ -name index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Local/Microsoft/Feeds/Cache/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Local/Microsoft/Windows/History/History.IE5/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012011080820110815/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012011081520110822/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012011082220110829/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012011083020110831/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012011083120110901/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012011090120110902/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Local/Microsoft/Windows/History/Low/History.IE5/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Roaming/Microsoft/Internet Explorer/UserData/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Roaming/Microsoft/Windows/Cookies/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Roaming/Microsoft/Windows/Cookies/Low/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Roaming/Microsoft/Windows/IECompatCache/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Roaming/Microsoft/Windows/IEDownloadHistory/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Roaming/Microsoft/Windows/IETldCache/index.dat
/media/7072034B7203158E/Users/Administrator/AppData/Roaming/Microsoft/Windows/PrivacyIE/index.dat
/media/7072034B7203158E/Users/babloo/AppData/Local/Microsoft/Feeds/Cache/index.dat
/media/7072034B7203158E/Users/babloo/AppData/Local/Microsoft/Windows/History/History.IE5/index.dat
/media/7072034B7203158E/Users/babloo/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012011081320110814/index.dat
/media/7072034B7203158E/Users/babloo/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/index.dat
/media/7072034B7203158E/Users/babloo/AppData/Roaming/Microsoft/Windows/Cookies/index.dat
/media/7072034B7203158E/Users/babloo/AppData/Roaming/Microsoft/Windows/IETldCache/index.dat
/media/7072034B7203158E/windows/ServiceProfiles/LocalService/AppData/Local/Microsoft/Windows/History/History.IE5/index.dat
/media/7072034B7203158E/windows/ServiceProfiles/LocalService/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/index.dat
/media/7072034B7203158E/windows/ServiceProfiles/LocalService/AppData/Roaming/Microsoft/Windows/Cookies/index.dat
/media/7072034B7203158E/windows/System32/config/systemprofile/AppData/Local/Microsoft/Windows/History/History.IE5/index.dat
/media/7072034B7203158E/windows/System32/config/systemprofile/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/index.dat
/media/7072034B7203158E/windows/System32/config/systemprofile/AppData/Roaming/Microsoft/Windows/Cookies/index.dat
/media/7072034B7203158E/windows/System32/config/systemprofile/AppData/Roaming/Microsoft/Windows/IETldCache/index.dat
/media/7072034B7203158E/windows/SysOW64/config/systemprofile/AppData/Local/Microsoft/Windows/History/History.IE5/index.dat
/media/7072034B7203158E/windows/SysOW64/config/systemprofile/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/index.dat
/media/7072034B7203158E/windows/SysOW64/config/systemprofile/AppData/Roaming/Microsoft/Windows/Cookies/index.dat
21:23 root@Matriux Krypton#
```

Figure 1



History	File
1	History
2	TYPEURLMODIFIED
3	TIMEACCESS
4	URLLetId:flog.br08/14/2011
5	URLLetId:village.ca08/14/2011
6	URLLetId:sci.eg08/14/2011
7	URLLetId:bolt.hu08/14/2011
8	URLLetId:rec.m08/14/2011
9	URLLetId:nieruchomosci.pl08/14/2011
10	URLLetId:astrakhan.ru08/14/2011
11	URLLetId:asn.au08/14/2011
12	URLLetId:erotica.hu08/14/2011
13	URLLetId:games.hu08/14/2011
14	URLLetId:arq.br08/14/2011
15	URLLetId:chernovtsy.ua08/14/2011
16	URLLetId:+ACE-if.m08/14/2011
17	URLLetId:name.ae08/14/2011
18	URLLetId:mus.br08/14/2011
19	URLLetId:nom.br08/14/2011
20	URLLetId:gob.cl08/14/2011
21	URLLetId:assn.lk08/14/2011
22	URLLetId:museum.mv08/14/2011
23	URLLetId:ing.pa08/14/2011
24	URLLetId:asso.bj08/14/2011
25	URLLetId:arq.br08/14/2011
26	URLLetId:leborc.pl08/14/2011
27	URLLetId:radom.pl08/14/2011
28	URLLetId:rel.pl08/14/2011
29	URLLetId:nom.re08/14/2011
30	URLLetId:bashkiria.ru08/14/2011
31	URLLetId:far.br08/14/2011
32	URLLetId:ppg.br08/14/2011
33	URLLetId:med.ec08/14/2011

```
root@Matriux: /home/Krypton
Edit View Terminal Help
36 root@Matriux Krypton# pasco /home/Krypton/Desktop/index.dat > /home/Krypton/Desktop/a.xls
36 root@Matriux Krypton#
```

Figure 2

The output is written to a excel file which is stored on Desktop, which is sorted according to the month.

Options for using

- -t Field Delimiters
- -d Undelete Activity Records

Pasco is the best handy tool for Internet history analysis.

Another way of retrieving data from browser stored files.

How we can use sqlite in forensics?

Using this sqlite will be a fetch while we go through sqlite databases in Mozilla firefox/chrome profile folders , using this we can analyse the user browser activities.

You can find the paths of the profile folders in below mentioned locations.

Mozilla Firefox –
....\AppData\Roaming\Mozilla\Firefox\Profiles*.default\

Chrome –
...\AppData\Local\Google\

This tool can be identified in Mantra browser Arsenal > framework > mantra

What is SQLite?

SQLite is an embedded SQL database engine.SQLite reads and writes directly to ordinary disk files. A complete SQL database with multiple tables, indices, triggers, and views, is contained in a single disk file. The database file format is cross-platform – you can freely copy a database between 32-bit and 64-bit systems.SQLite a popular database engine choice on memory constrained gadgets such as smart phones,

PDAs, and MP3 players. Its primary usage can be:-

- Simple to administer
- Simple to operate
- Simple to embed in a larger program
- Simple to maintain and customize

How to Use SQLite ?

SQLite can be added as a add-on for Firefox, after installing the addon You can observe it in tools>SQLite Manager

Even we can use a package of SQLite browser , can download the package from <http://sourceforge.net/projects/sqlitebrowser/> It is similar as the SQLite Manager to use , but we need the dependent dll's which is present in the folder to work.SQLite can be used to create ,add , retrieve and delete the entries in the database table.

Using SQLite

Open database files in sqlite using open option.Database of chrome can be only accessible when the browser is closed, if we are using SQLite manager for analysis we can see the database files listed in the top drop down list shown in fig.we can change the default path to our custom directories if any. Selecting the table in the left frame we can access the entries, we can add duplicates,delete and edit the entries with the options.

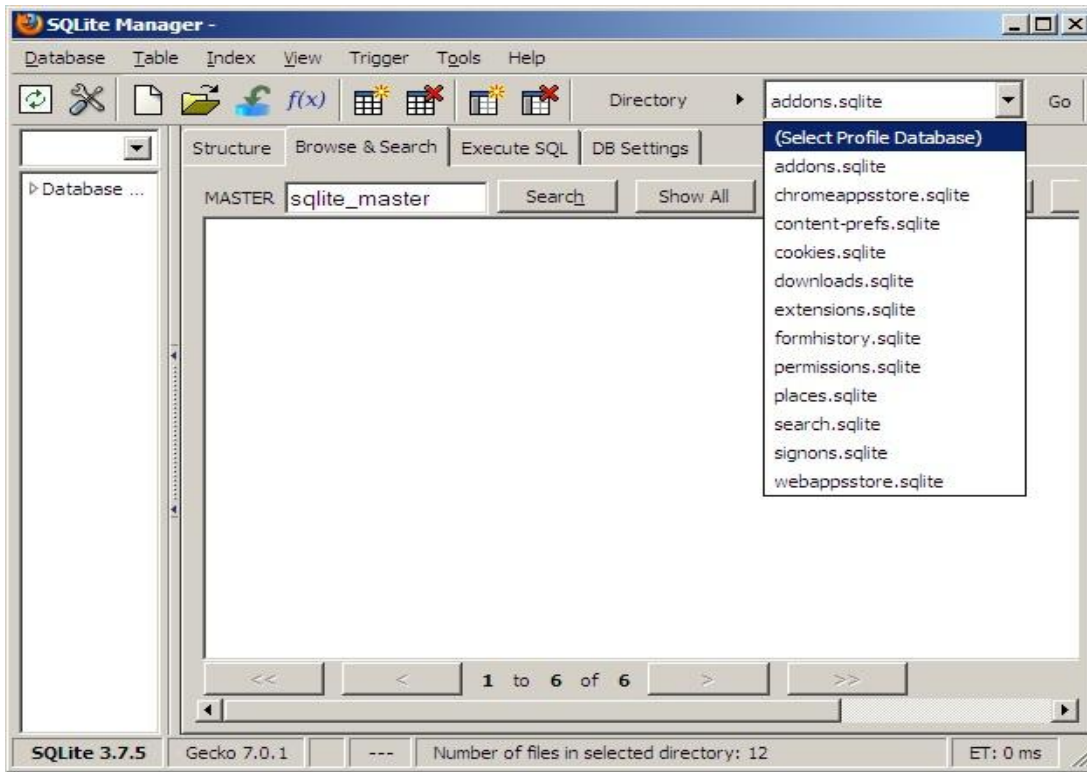


Figure 3

Using Execute SQL tab we can execute custom sql commands to create , edit , or delete the tables. we can add user defined functions by using the User-Defined Functions tab which is by default hidden, visible on clicking f(x) button.

Database can be import / export as CSV,xml and sql files from Import tab and File menu. Some important files from which we can gather information includes: -

Firefox	Chrome	Description
cookies.sqlite	cookies	Cookies
Formhistory.sqlite	Web Data	Details filled in a form
Places.sqlite	history, Top sites, Web Data	Browser activities such as bookmark, visits and keyword search
Signons.sqlite	logindata	Uname password stored in the browser cache
key3.db	logindata	stored passwords

Figure 4

Sqlite is the other good option to analyse the database files for browsers.

For any further details/queries mail @report@matruix.com

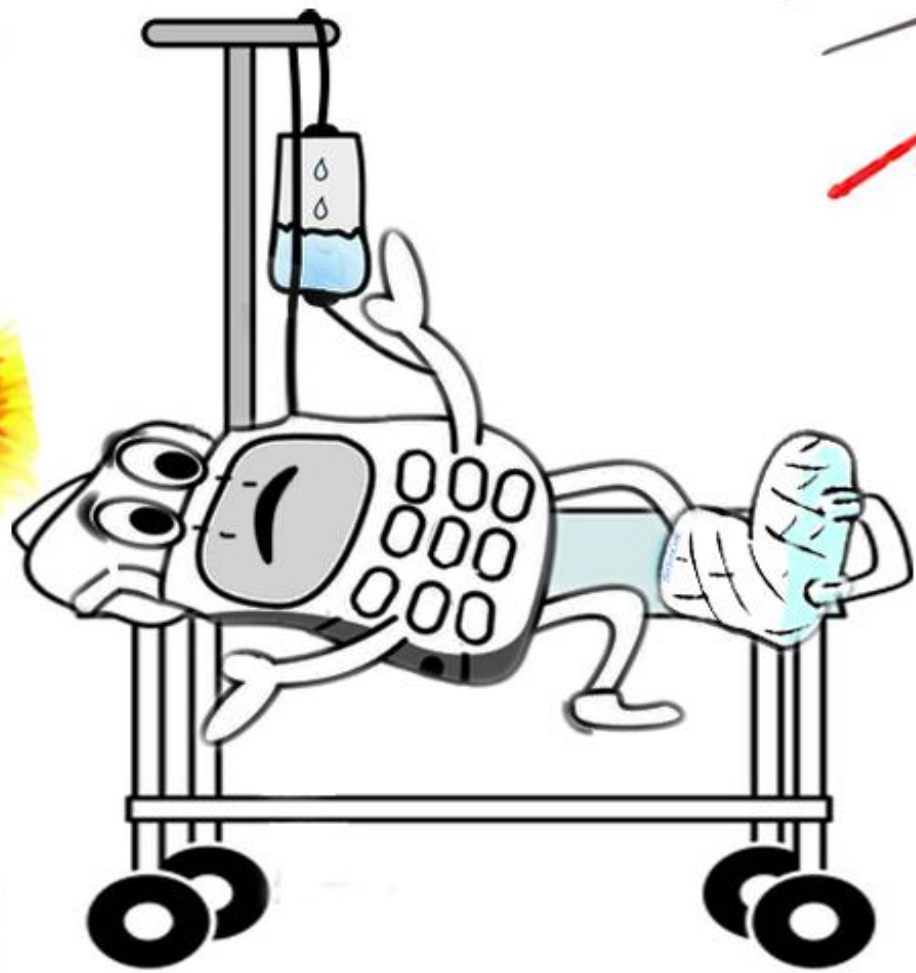
Follow us at @matriuxtig3r on twitter and <http://facebook.com/matriuxtig3r>



Pardhasaradhi.Ch

pardhu19872007@gmail.com

Pardhasaradhi is working as a Systems QA engineer. He is an active member of ClubHack, HackIT, null and working with Matriux Forensics team . He is also one of the moderators for null Hyderabad chapter. His interests include Forensics, Auditing, Penetration Testing and Designing.



Mobile Warfare