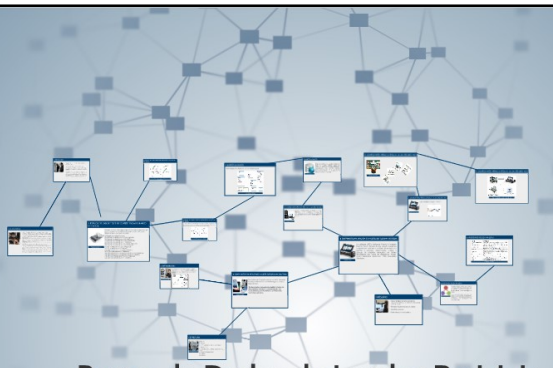
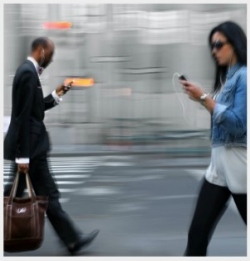


Banco de Dados de Laudos Periciais de Dispositivos Móveis

Disciplina: Segurança Computacional
Aluno: Matheus Magnusson Bolo

Prezi

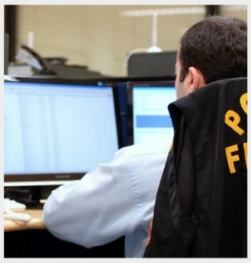
ESTRUTURA



Apresentação

Prezi

1. RESUMO

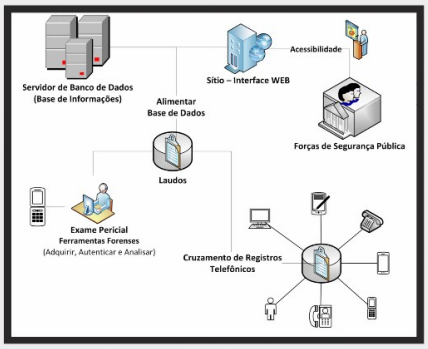


- Banco de dados de laudos periciais de dispositivos móveis a ser utilizado como padrão em todo o país;
- Estrutura relacional do banco de dados;
- Resultado esperado;
- Demonstração de modo prático.

2. INTRODUÇÃO

Luiz Rodrigo Grochocki

Problemática apresentada por [Grochocki et al. 2013] relacionada aos procedimentos periciais em dispositivos móveis, tendo como base o sistema SiCReT.



3. DISPOSITIVOS MÓVEIS E COLETA DE DADOS DIGITAIS

Dispositivos Móveis

Na Publicação Especial 800-101 do NIST (*National Institute of Standards and Technology*) os autores sugerem que:

A chave para o sucesso na análise forense de dispositivos móveis é a compreensão das características de *hardware* e *software* dos telefones celulares.

3. DISPOSITIVOS MÓVEIS E COLETA DE DADOS DIGITAIS

Cellebrite UFED

O *Cellebrite UFED* (*Universal Forensic Extraction Device*) *Touch Ultimate* é uma solução israelense composa por hardware e software proprietário que permite a extração, decodificação, análise e geração de relatórios avançados em termos tecnológicos dos dados de dispositivos móveis, sendo suportados atualmente 7.900 dispositivos diferentes.

3. DISPOSITIVOS MÓVEIS E COLETA DE DADOS DIGITAIS

Microsytemation XRY

Quando o *Cellebrite UFED* não fornece suporte ao dispositivo a ser analisado, o Instituto de Criminalista conta com o *Microstemation XRY*, que em sua versão atual, suporta 10.036 dispositivos móveis.

3. DISPOSITIVOS MÓVEIS E COLETA DE DADOS DIGITAIS

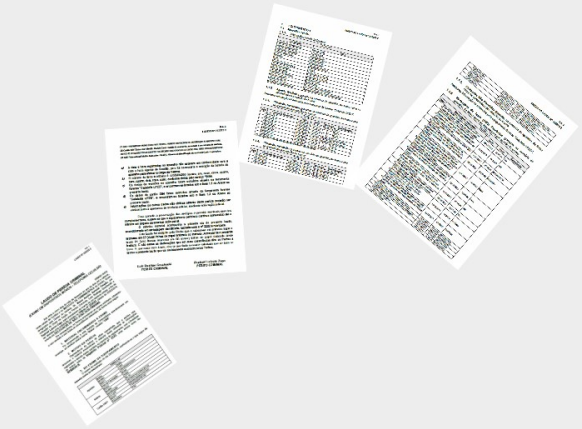
hardware/software de captura

Captura de dados em dispositivos móveis.

Parâmetros
Fabricante selecionado
Modelo selecionado
Fabricante detectado
Modelo detectado
Nome do equipamento
IMEI (*International Mobile Equipment Identity*)
ICCID (*International Circuit Card ID*)
IMSI (*International Mobile Subscriber Identity*)
Endereço Bluetooth
Endereço Wi-Fi
Início da extração
Fim da extração
Data/Hora do telefone
Tipo de conexão
Versão da UFED

3. DISPOSITIVOS MÓVEIS E COLETA DE DADOS DIGITAIS

Composição do laudo



LAUDO DE PERÍCIA CRIMINAL
(EXAME EM DISPOSITIVOS MÓVEIS - TELEFONIA CELULAR)

CÓDIGO: N-812

Aos vinte e cinco dias do mês de fevereiro do ano de dois mil e catorze, nesta cidade de Curitiba e no **INSTITUTO DE CRIMINALÍSTICA** do Estado, foram designados pelo Diretor do Instituto, **Dr. Marco Aurélio Bertoldi Pimpão**, por indicação do Chefe da Seção, os Peritos Criminais, **Luiz Rodrigo Grochocki** e **Raphael Laércio Zago**, para procederem ao exame de um telefone celular, a fim de ser atendida uma solicitação contida no **Ofício nº 222/22**, datado de 25/02/2014, oriundo do **DELEGACIA DE SÃO JOSÉ DOS PINHAIS**.

Em consequência, os Peritos procederam ao exame solicitado, relatando-o com verdade e com todas as circunstâncias relevantes, da forma como segue:

1. MATERIAL ENCAMINHADO A EXAME

Foi encaminhado a este Instituto de Criminalística acondicionado em envelope, um telefone celular marca "**Nokia**", modelo "**1208**".

2. MOTIVO DA PERÍCIA

Depreende-se da leitura do ofício supracitado, que a perícia visa descrever o material encaminhado e elaborar laudo referente às informações registradas e demais dados contidos na memória do equipamento, com a finalidade de instruir autos de **Inquérito Policial nº 2222**, onde consta como réu **SENHOR B**.

3. DO EXAME DO EQUIPAMENTO

O exame foi realizado no dia 25/02/2014, verificando-se o que segue ***da maneira como se encontrava***:

TABELA Nº		
Aparelho	Marca:	Nokia
	Modelo:	1208
	IMEI[1]:	356402028331070
	País de Fabricação:	Brasil
Bateria	Marca:	Nokia
	Modelo:	BL-4C
	Identificação:	69785551441226622;22122
Cartão SIM[2]	ICC-ID[3]:	89550440000347051001
	IMSI[4]:	724044034705100
	Operadora:	TIM

Luiz Rodrigo Grochocki
PERITO CRIMINAL

(1) IMEI (International Mobile Equipment Identity): Número Internacional de Identificação do aparelho GSM.
(2) Cartão SIM (Subscriber Identity Module Card): Cartão do assinante, associado à um número de telefone.
(3) ICC-ID (Integrated Circuit Card ID): Identificador único impresso no cartão SIM, válido internacionalmente.
(4) IMSI (International Mobile Subscriber Identity): Número de identificação do assinante junto à operadora.

a) A data e hora registradas no aparelho não estavam em conformidade com a data e hora vigente de Brasília, pois foi necessária a remoção da bateria do aparelho para efetuar a carga da mesma.
b) O número da linha telefônica é: **4195404292** (quatro, um, nove, cinco, quatro, zero, quatro, dois, nove, dois), conforme obtido pelo serviço *#846#.
c) Os dados da memória do aparelho foram extraídos através da ferramenta forense "*Cellebrite UFED*", e encontram-se listados sob o **Item 1.1** do Anexo ao presente laudo.
d) Os dados do cartão SIM foram extraídos através da ferramenta forense "*Cellebrite UFED*", e encontram-se listados sob o **Item 1.2** do Anexo ao presente laudo.
e) Informações ou outros dados não obtidos através desta perícia poderão ser obtidos junto à operadora de telefonia celular, mediante solicitação judicial.

Para garantir a preservação dos vestígios e permitir eventuais quesitos complementares, sugere-se que o equipamento periciado continue apreendido até o trânsito em julgado da eventual ação penal.

O referido material acompanha a primeira via do presente laudo, acondicionado em embalagem identificada, **lacrada com o nº 2222** e rubricada.

Este laudo foi redigido pelo Perito que o subscreve em primeiro lugar e impresso em 02 (duas) folhas de papel timbrado do Instituto. Acompanha o presente laudo 01 (um) **Anexo** impresso em 05 (cinco) folhas de papel timbrado deste Instituto. E são essas as declarações que em suas consciências têm os Peritos a fazer. E, por nada mais haver, deu-se por findo o exame solicitado que de tudo se lavrou o presente laudo que vai devidamente assinado pelos Peritos.

Luiz Rodrigo Grochocki
PERITO CRIMINAL

Raphael Laércio Zago
PERITO CRIMINAL

1. EQUIPAMENTO 1

1.1. Aparelho Celular:

1.1.1. Informações Gerais da Captura:

TABELA 1

Parâmetro	Valor
Fabricante selecionado:	Nokia GSM
Modelo selecionado:	1200/1208
Fabricante detectado:	(Indisponível)
Modelo detectado:	(Indisponível)
Revisão:	(Indisponível)
IMEI:	356402028331070
Código de Segurança:	12345
Início da extração:	25/02/2014 11:31:04
Fim da extração:	25/02/2014 11:31:23
Data/Hora do telefone:	(Indisponível)
Tipo de conexão:	Serial Cable
Versão da UFED:	2.2.5.0 UFED; S/N:5534651
Extração suportada para:	Agenda Telefônica, SMS, Chamadas

1.1.2. **Agenda Telefônica** gravada na memória do aparelho, da forma como se apresentava por ocasião do exame:

Nenhuma informação foi retornada pelo equipamento forense "Cellebrite UFED".

1.1.3. **Chamadas Realizadas** gravadas na memória do aparelho, da forma como se apresentava por ocasião do exame:

TABELA 2

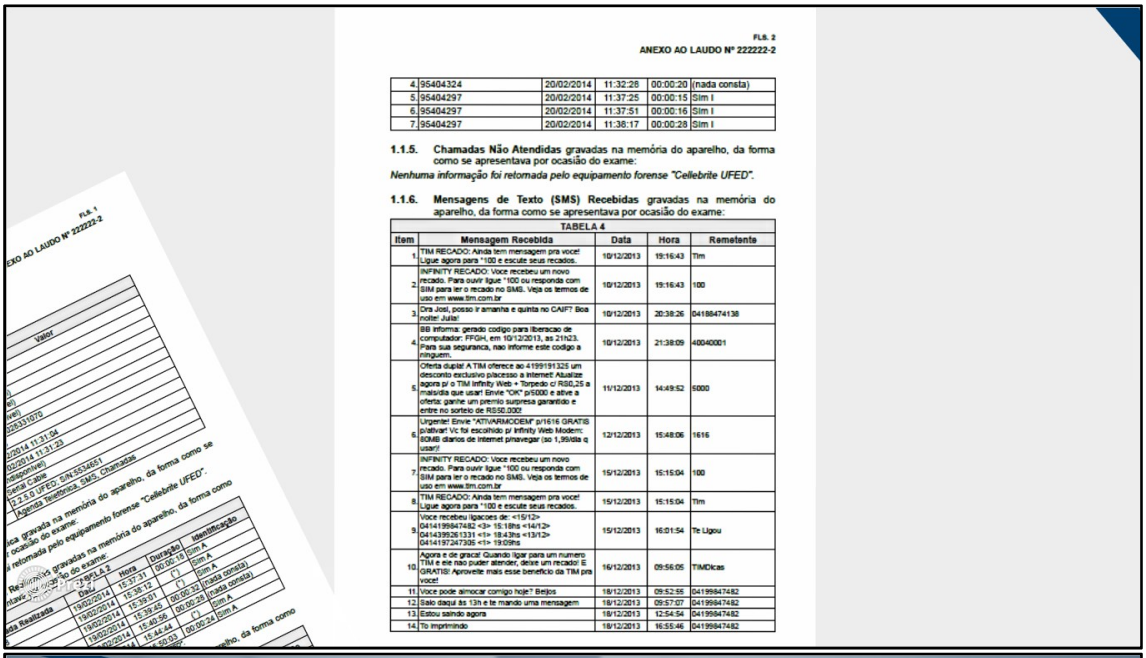
Item	Chamada Realizada	Data	Hora	Duração	Identificação
1	95404318	19/02/2014	15:37:31	00:00:18	Sim A
2	95404318	19/02/2014	15:38:12	(*)	Sim A
3	95404318	19/02/2014	15:39:01	(*)	Sim A
4	95404324	19/02/2014	15:39:45	00:00:32	(nada consta)
5	95404324	19/02/2014	15:40:56	00:00:28	(nada consta)
6	95404318	19/02/2014	15:44:44	(*)	Sim A
7	95404318	19/02/2014	15:50:03	00:00:24	Sim A

(*) Informação não retornada pelo equipamento forense "Cellebrite UFED".

1.1.4. **Chamadas Recebidas** gravadas na memória do aparelho, da forma como se apresentava por ocasião do exame:

TABELA 3

Item	Chamada Recebida	Data	Hora	Duração	Identificação
1	95404324	19/02/2014	15:43:53	00:00:36	(nada consta)
2	95404297	20/02/2014	10:16:28	00:00:10	Sim I
3	95404297	20/02/2014	10:18:38	00:00:17	Sim I



FLS. 2

ANEXO AO LAUDO Nº 222222-2

4.	95404324	20/02/2014	11:32:28	00:00:20	(nada consta)
5.	95404297	20/02/2014	11:37:25	00:00:15	Sim I
6.	95404297	20/02/2014	11:37:51	00:00:16	Sim I
7.	95404297	20/02/2014	11:38:17	00:00:28	Sim I

1.1.5. Chamadas Não Atendidas gravadas na memória do aparelho, da forma como se apresentava por ocasião do exame:

Nenhuma informação foi retornada pelo equipamento forense "Cellebrite UFED".

1.1.6. Mensagens de Texto (SMS) Recebidas gravadas na memória do aparelho, da forma como se apresentava por ocasião do exame:

TABELA 4

Item	Mensagem Recebida	Data	Hora	Remetente
1.	TIM RECADO: Ainda tem mensagem pra voce! Ligue agora para *100 e escute seus recados.	10/12/2013	19:16:43	Tim
2.	INFINITY RECADO: Voce recebeu um novo recado. Para ouvir ligue *100 ou responda com SIM para ler o recado no SMS. Veja os termos de uso em www.tim.com.br	10/12/2013	19:16:43	100
3.	Dra Josi, posso ir amanha e quinta no CAIF? Boa noite! Julia!	10/12/2013	20:38:26	84188474138
4.	BB informa: gerado codigo para liberacao de computador: FFGH, em 10/12/2013, as 21h23. Para sua seguranca, nao informe este codigo a ninguem.	10/12/2013	21:38:09	40040001
5.	Oferta dupla! A TIM oferece ao 4199191325 um desconto exclusivo p/acesso a internet! Atualize agora p/ o TIM Infinity Web + Torpedo c/ R$0,25 a mais/dia que usar! Envie "OK" p/5000 e ative a oferta: ganhe um premio surpresa garantido e entre no sorteio de R$50.000!	11/12/2013	14:49:52	5000
6.	Urgente! Envie "ATIVARMODEM" p/1616 GRATIS p/ativar! Vc foi escolhido p/ Infinity Web Modem: 80MB diarios de internet p/navegar (ao 1,95/dia q usar)!	12/12/2013	15:48:06	1616
7.	INFINITY RECADO: Voce recebeu um novo recado. Para ouvir ligue *100 ou responda com SIM para ler o recado no SMS. Veja os termos de uso em www.tim.com.br	15/12/2013	15:15:04	100
8.	TIM RECADO: Ainda tem mensagem pra voce! Ligue agora para *100 e escute seus recados.	15/12/2013	15:15:04	Tim
9.	Voce recebeu ligacoes de: <15/12> 04141998447482 <3> 15:18hs <14/12> 04143992611331 <1> 18:43hs <13/12> 04141972473135 <1> 19:09hs	15/12/2013	16:01:54	Te Ligou
10.	Agora e de graca! Quando ligar para um numero TIM e ele nao puder atender, deixe um recado! E GRATIS! Aproveite mais esse beneficio da TIM pra voce!	16/12/2013	09:56:05	TIMDicas
11.	Voce pode almocar comigo hoje? Beijos	18/12/2013	09:52:55	04199847482
12.	Saio daqui às 13h e te mando uma mensagem	18/12/2013	09:57:07	04199847482
13.	Estou saindo agora	18/12/2013	12:54:54	04199847482
14.	To imprimindo	18/12/2013	16:55:46	04199847482

3. DISPOSITIVOS MÓVEIS E COLETA DE DADOS DIGITAIS

Exame Pericial
Ferramentas Forenses
(Adquirir, Autenticar e Analisar)

Laudo de Perícia Criminal
(Arquivo XML)

Fluxo: Do Dispositivo ao Laudo Pericial Criminal

Prezi

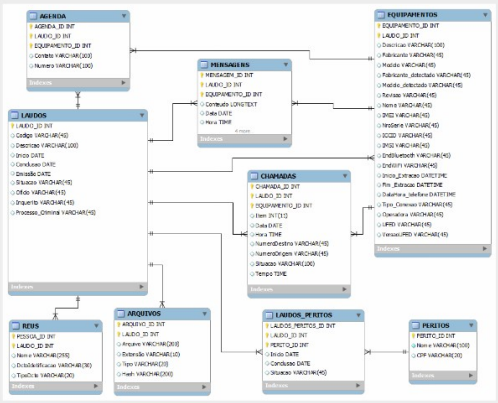
4. BANCO DE DADOS

Banco de Dados

Esta seção apresenta o projeto de banco de dados do sistema SiCReT, tendo sido adotada a Orientação a Objetos utilizando a representação UML (*Unified Modeling Language*), para uma melhor compreensão das funcionalidades e facilitação de manutenibilidade do software.

4. BANCO DE DADOS

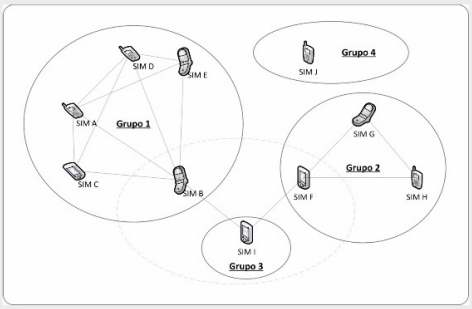
Modelo lógico de dados relativo ao BD Relacional.



Modelo Lógico de Dados

5. ESTUDO DE CASO E TESTE DE CONSISTÊNCIA DO BANCO DE DADOS

Situação simulada, considerando a extração de dados a partir de 10 (dez) cartões SIM, com tecnologia GSM, de 128KB, para a instanciação do Banco de Dados e realização de testes de consistência.



Representação Gráfica de Cruzamentos entre Dispositivos Móveis

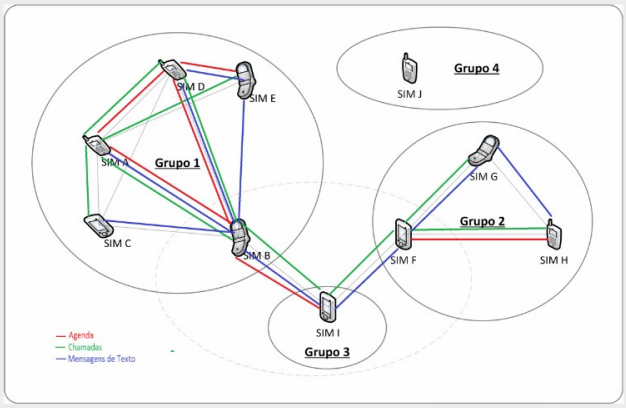
5. ESTUDO DE CASO E TESTE DE CONSISTÊNCIA DO BANCO DE DADOS

Teste de Consistência

O Estudo de Caso, utiliza alguns Tipos de Operações responsáveis por gerar os registros necessários nos dispositivos, fornecendo dados suficientes para a realização dos testes.

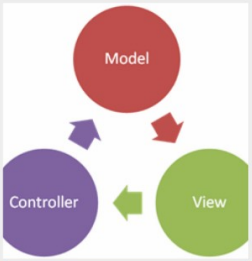
1) Registro de Contato Telefônico;
2) Chamada Realizada para Contato Registrado;
3) Chamada Realizada para um Nº Telefônico;
4) Chamada Recebida de um Contato Registrado;
5) Chamada Recebida de um Nº Telefônico;
6) Chamada Não Atendida de um Contato Registrado;
7) Chamada Não Atendida de um Nº Telefônico;
8) SMS recebido de um Contato Registrado;
9) SMS recebido de um Nº Telefônico;
10) SMS enviado para um Contato Registrado;
11) SMS enviado para um Nº Telefônico;
12) SMS armazenado nos rascunhos de um Contato Registrado;
13) SMS armazenado nos rascunhos de um Nº Telefônico;
14) SMS não enviadas de um Contato Registrado;
15) SMS não enviadas de um Nº Telefônico.

5. ESTUDO DE CASO E TESTE DE CONSISTÊNCIA DO BANCO DE DADOS



Representação Gráfica de Cruzamentos entre Dispositivos Móveis: Agenda, Chamadas e Mensagens de Texto.

6. PROTÓTIPO DO SISTEMA SiCReT



MVC (Model-View-Control)

O sistema SiCReT utiliza como padrão o modelo MVC (Model-View-Control), garantindo a separação da interface, do controle de fluxo e das regras do projeto.

Sendo possível realizar alterações em cada uma das camadas isoladamente, diminuindo o retrabalho proveniente da necessidade de atualização em aplicações Web.

6. PROTÓTIPO DO SISTEMA SiCReT

NOME	DESCRIÇÃO
Eclipse Platform - Indigo 3.7.1	Criação do projeto, programação Java, serviços servidor Tomcat. Disponível em: http://www.eclipse.org/
PRIMEFACES 3.0	Framework de componentes ricos. Disponível em: http://www.primefaces.org/
Hibernate 3.5.6	Persistência dos informações no Banco de Dados. Disponível em: https://www.hibernate.org/
Spring 3.0.5	Framework de Inversão de Controle e Injeção de Dependência. Disponível em: http://www.springsource.org/
MySQL 5.5.25	Sistema Gerenciador de Banco de Dados. Disponível em: http://www.mysql.com/
Apache Tomcat 7.0.21	Contêiner de aplicações web. Disponível em: http://tomcat.apache.org/
MySQL Workbench 5.2.34 CE	Interface gráfica para administrar e trabalhar com o banco de dados MySQL. Disponível em: http://www.mysql.com/
JSSE	Java Secure Sockets Extension
JAAS	Java Authentication an Autorization Service

Ferramentas e Tecnologias

7. CONCLUSÃO

- Proposta de um BD de laudos periciais em dispositivos móveis;
- Simulação para descrever um estudo de caso;
- Integração de um sistema computacional de maior proporção, com aplicação de técnicas de mineração de dados;
- Integração entre os diversos Institutos de Criminalística do Brasil, auxiliando o entendimento sobre as forças que governam o fluxo criminoso e disponibilização de ferramentas de apoio aos Serviços de Inteligência e Policiamento Preditivo.

8. REFERÊNCIAS

- Garms, J.; Somerfield, D.. “Professional Java Security”. Wrox Press Ltd, 2001.
- Grochocki, L. R.; Vrubel, A.; Zago, R. L.; Decarli, A.; Freitas, C. O. A.. SiCReT - Sistema de Cruzamento de registros Telefônicos. In: XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), 2013, Manaus: Sociedade Brasileira de Computação, 2013. v. 1. p. 527-536.
- Hemrajani, A. “Desenvolvimento Ágil em JAVA com SPRING HIBERNATE E ECLIPSE”. Pearson Education, 2007.
- Jansen, W.; Ayers, R. “Computer Security - guidelines on cell phone forensics”. National Institute of Standards and Technology – NIST, Special Publication 800- 101, May 2007, 104 p. Disponível em <http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf> Acesso em maio 2014.
- McLaughlin, B. “Java and XML”. Mike Loukides, 2000.
- MOREIRA NETO, O. “Entendendo e Dominando o Java para Internet”. Digerati Books, 2009. 320p.
- OAKS, S. “Segurança de dados em Java”. Editora Ciência Moderna, 1999.
- REIS, A. B. “Metodologia científica em perícia criminal”. Campinas, SP: Millenium, 2011.
- ROSA, M. V. F. “Perícia Judicial - Teoria e Prática”. Sérgio Antônio Fabris Editor, 1999.
- Ultra, R. G.; Tech, M. “Data Mining Techniques to Analyze Crime Data”. International Journal For Technological Research In Engineering, Volume 1, Issue 9, May-2014, p. 882-884.
- Watson, A. “Visual Modelling: past, present and future”. Disponível em <http://www.uml.org/Visual_Modeling.pdf> Acesso em maio de 2014.
- WEISER, M. “Some Computer Science Issues in Ubiquitous Computing”. Communications of the ACM, v. 265, n. 3, 1993, p. 137 - 143.