

SOMMARIO

MESSAGGIO DEL PRESIDENTE DI IISFA ITALIA.....	XIII
INTRODUZIONE	XVII

CAPITOLO PRIMO

“DI NECESSITÀ, VIRTÙ”: APPUNTI PER UNA STRATEGIA GLOBALE AL CONTRASTO DEL CYBERCRIME. L’ESPERIENZA DEL POOL REATI INFORMATICI DELLA PROCURA DI MILANO	1
1. L’IMPATTO DELLA LEGGE 48/2008 SULLE PROCURE DISTRETTUALI E LA NECESSITÀ DI RIORGANIZZARE LE METODOLOGIE DI LAVORO	1
2. IL PROBLEMA DEI CRITERI DI INDIVIDUAZIONE DELLA COMPETENZA TERRITORIALE NELLE TRUFFE INFORMATICHE ATTUATE CON UTILIZZO DI CARTE RICARICABILI (COME STRUMENTO DI PAGAMENTO A FRONTE DI UN ACQUISTO DI BENI SU PIATTAFORME DI E-COMMERCE)	7
3. IL SOMMERSO CHE AVANZA: I “SERIAL KILLER” INFORMATICI DELLA PORTA ACCANTO	11
3.1 CASI ED ESPERIENZE	13
4. LA VITTIMA, AL CENTRO	15
5. PER UNA PRIMA CLASSIFICAZIONE “ESPERIENZIALE” DELLE CATEGORIE DI REATI INFORMATICI	17
6. LE DIRETTIVE PER LA POLIZIA GIUDIZIARIA SUI PRIMI ACCERTAMENTI INVESTIGATIVI IN MATERIA DI REATI INFORMATICI E MODALITÀ DI TRASMISSIONE DELLE RELATIVE COMUNICAZIONI DI NOTIZIA DI REATO ALLA PROCURA DI MILANO	26
7. L’AGGIORNAMENTO PROFESSIONALE PER LA POLIZIA GIUDIZIARIA	30
7.1 IL PIANO DI FORMAZIONE A DISTANZA (FAD) PER IL 2012	34

8. UN SITO INTERNET INFORMATIVO PER LA CITTADINANZA E PER LA POLIZIA GIUDIZIARIA	37
9. UNA PROPOSTA DI LEGGE PER L'ASSEGNAZIONE ALLA POLIZIA GIUDIZIARIA DEI BENI INFORMATICI SEQUESTRATI/CONFISCATI NELLE INDAGINI INFORMATICHE	40
10. IN LUOGO DI UNA CONCLUSIONE	43

CAPITOLO SECONDO

LA CRESCITA DEL BISOGNO DI INVESTIRE IN ETICA E SICUREZZA	45
1. PREMESSE	45
2. SCENARI E BISOGNO DI ETICA & SICUREZZA	47
3. CHE COSA SI INTENDE PER ETICA?	53
4. ETICA, RESPONSABILITÀ SOCIALE E IMPRESA	56
5. ANALIZZARE E GESTIRE RISCHI IN AZIENDA E SOSTENIBILITÀ	62
6. BIBLIOGRAFIA	71

CAPITOLO TERZO

ETICA DEL COMPUTER ED ETICA DELL'INFORMAZIONE NELLA SOCIETÀ DELL'INFORMAZIONE IN RETE	75
1. INTRODUZIONE: L'IMPATTO DELLE TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE	75
2. L'ETICA DEL COMPUTER	78
3. L'ETICA DELL'INFORMAZIONE: LA PROSPETTIVA DI LUCIANO FLORIDI	83
3.1 CENTRALITÀ DELL'INFORMAZIONE E DECENTRAMENTO DELLA PROSPETTIVA ANTROPOCENTRICA	83
3.2 PROSPETTIVA ONTOCENTRICA INFORMATIVALE	85
3.3 IL PRINCIPIO DI EQUIVALENZA ONTOLOGICA	85
3.4 ETICA ORIENTATA AL PAZIENTE	86
3.5 L'INFOSFERA: LE LEGGI DELL'INFOSFERA	87
3.6 INFORMAZIONE E RESPONSABILITÀ	88
4. CONCLUSIONI: VINCERE IL NARCISISMO UMANO	89

CAPITOLO QUARTO

LA TIMELINE: ASPETTI TECNICI E RILEVANZA PROCESSUALE	93
1. PREMESSA	93

2. LA TIMELINE	95
3. IL PROBLEMA DELL' "ORA ESATTA"	98
4. METODOLOGIA	102
4.1 ANALISI DEI Timestamp PRESENTI NEI FILE SYSTEM	103
4.2 ANALISI DEI Timestamp CONTENUTI ALL'INTERNO DEI FILE	103
4.3 RISCONTRO CON ALTRI RIFERIMENTI TEMPORALI RILEVABILI	104
4.4 CONTESTUALIZZAZIONE DEI Timestamp	105
5. CASE STUDY: CREAZIONE ED ANALISI DELLA TIMELINE	106
5.1 I PROBLEMI DELL' ANALISI TRADIZIONALE	106
5.2 ANTI-FORENSICS	107
5.3 ESTENSIONE DELLE TIMELINE	108
5.4 IMPOSTAZIONE DEL CASE STUDY	109
5.5 I TOOL PER LA GENERAZIONE DI TIMELINE	110
5.6 I TOOL PER LA GENERAZIONE DI SUPERTIMELINE	111
5.7 LOG2TIMELINE E LE SUPERTIMELINE	112
5.8 AMBIENTE DI LAVORO	115
5.9 "MONTAGGIO" DELL'IMMAGINE FORENSE	115
5.10 ESTRAZIONE DELLA TABELLA MFT	121
5.11 GENERAZIONE DELLA SUPERTIMELINE	123
5.12 ANALISI DEI RISULTATI	131
5.13 STRUMENTI PER RAFFINARE L' ANALISI	138
5.14 NOTE PRATICHE SULLA SINCRONIZZAZIONE TEMPORALE	140
6. VALORE PROBATORIO	144
7. CONCLUSIONI	147
8. BIBLIOGRAFIA	147
CAPITOLO QUINTO	
LIVE FORENSICS	151
1. INTRODUZIONE	151
2. COSA DICE LA LEGGE	153
2.1 CASI E FORME DELLA PERQUISIZIONE	153
3. ATTIVITÀ PRELIMINARI	156
4. PERQUISIZIONE LOCALE	159
4.1 VALIDAZIONE E PREPARAZIONE DELLA STRUMENTAZIONE	162
4.1.1 LA SCELTA DEGLI STRUMENTI: OPEN SOURCE VS CLOSED SOURCE	164
4.2 MAPPATURA DELLA RETE	165

4.3 VOLATILE DATA COLLECTION	167
4.3.1 ORARIO DI SISTEMA	168
4.3.2 MEMORIA RAM	169
4.3.3 AREA APPUNTI	173
4.3.4 INFORMAZIONI DI SISTEMA	174
4.3.5 UTENTI COLLEGATI	177
4.3.6 FILE APERTI	179
4.3.7 CONNESSIONI DI RETE	180
4.3.8 PROCESSI, SERVIZI E DRIVER	182
4.3.9 MAPPATURE DEI DRIVE E CARTELLE CONDIVISE	186
4.3.10 RILEVAMENTO DI SISTEMI DI CIFRATURA	191
4.4 LIVE ANALYSIS (NON-VOLATILE INFORMATION)	193
4.4.1. REGISTRO DI WINDOWS	194
4.4.2. CRONOLOGIA DEGLI EVENTI DI SISTEMA	194
4.4.3. INTERNET HISTORY E CACHE	195
4.5 FLAGRANZA DI REATO	198
4.6 SHUTDOWN E REPERTAMENTO FISICO	199

CAPITOLO SESTO

LA RETE E LE INFORMAZIONI:

RACCOLTA E USO ILLECITO DEI DATI	201
1. RETE ED INFORMAZIONI	201
1.1 PANORAMICA SULLE FONTI APERTE	202
2. LE INFORMAZIONI	204
2.1 METODI E SISTEMI DI RACCOLTA	204
2.2 LA VALUTAZIONE	206
3. USO ILLECITO DELLA RACCOLTA DI INFORMAZIONI	207
3.1 INTRODUZIONE	207
3.2 UN CASO DI PHISHING	208
3.3 IL TERRORISMO ISLAMICO E LA RETE	210
4. LA RACCOLTA DI INFORMAZIONI DAL WEB AD USO PREVENTIVO ED INVESTIGATIVO	213
4.1 IL CASO ECHELON	213
4.2 UNA NUOVA FRONTIERA: L'INVESTIGATIVE WEB PROFILING	216
4.3 NOME IN CODICE REYNARD	218
5. CONCLUSIONI	219
6. BIBLIOGRAFIA ESSENZIALE	220

CAPITOLO SETTIMO	
POSTA ELETTRONICA E REATI INFORMATICI	223
1. CRIMINI E POSTA ELETTRONICA	223
1.1 POSTA ELETTRONICA IN CHIARO	224
1.2 ESAME PARTICOLAREGGIATO DELLE DIVERSE TIPOLOGIE DI UNA EMAIL	228
1.3 PRINCIPALI PROTOCOLLI DI POSTA	228
2. POSTA ELETTRONICA ED INVESTIGAZIONI	231
2.1 ACQUISIZIONE DELLE EMAIL	231
2.2 FORENSICS E BEST PRACTICE	233
2.2.1 CARVING DEI FILE DI POSTA ELETTRONICA	234
2.2.2 PRESENTAZIONE DEI RISULTATI E VALORE PROBATORIO	235
2.2.3 ESEMPIO DI UN CASO CLASSICO	236
3. LA EMAIL COME MEZZO DI PROVA NEL PROCESSO PENALE	237
3.1. LA DISCIPLINA DELL' ASSUNZIONE DEI MEZZI DI PROVA SCIENTIFICI	240
3.2 VALUTAZIONE DEI MEZZI DI PROVA DIGITALI (EMAIL)	243
3.3 LA SCALA DEI VALORI PROBATORI DELLA EMAIL	247
4. PREVISIONE NORMATIVA DEI REATI COMMESSI A MEZZO EMAIL	249
CAPITOLO OTTAVO	
IMAGE/VIDEO FORENSICS: CASI DI STUDIO	261
1. INTRODUZIONE	261
2. CONTRAFFAZIONE E ALIBI INFORMATICO	262
2.1 CONTRAFFAZIONE	262
2.2 ALIBI INFORMATICO	265
2.2.1 ANALISI DEL FORMATO MINIDV	266
2.2.2 ANALISI DEI METADATI	268
2.2.3 EVIDENZE SUL FORMATO ANALOGICO	269
2.2.4 ANALISI DEL SUPPORTO	271
2.2.5 CONSIDERAZIONI FINALI	271
3. VERIFICA DELLA COMPATIBILITÀ DELLE CARATTERISTICHE ANTROPOMETRICHE DI UN INDAGATO A PARTIRE DA INFORMAZIONI ESTRATTE DA FRAME VIDEO	271
3.1 MIGLIORAMENTO DEI FILMATI	274
3.2 COMPARAZIONE DELLE FIGURE (SHAPES) DI DUE SOGGETTI	278

3.3 MISURAZIONE DELL'ALTEZZA	284
4. ANALISI E MISURE DI VELOCITÀ DI VEICOLI/PERSONE IN MOVIMENTO	287
5. CONCLUSIONI	291
6. BIBLIOGRAFIA	291
CAPITOLO NONO	
IPAD FORENSICS	293
1. IL TABLET IPAD	293
1.1 IPAD	295
1.2 IPAD 2	299
2. IL SISTEMA OPERATIVO IOS	302
3. FILE SYSTEM HFS+	304
4. PARTIZIONI IOS	308
5. PRINCIPALI APPLICAZIONI	308
6. DATABASE SQLITE E FILE PLIST	310
6.1 DATABASE SQLITE	310
6.2 PROPERTY LIST	310
7. ISOLAMENTO DEL DISPOSITIVO IPAD	311
7.1 JAMMER	312
7.2 GABBIA DI FARADAY	313
7.3 ISOLARE L'IPAD	315
8. ACQUISIZIONE DEL DISPOSITIVO IPAD	315
8.1 ACQUISIZIONE LOGICA	316
8.2 ACQUISIZIONE LOGICA DI DISPOSITIVI BLOCCATI	316
8.3 ACQUISIZIONE LOGICA UTILIZZANDO ITUNES	318
8.4 ACQUISIZIONE LOGICA UTILIZZANDO HARDWARE O SOFTWARE DEDICATI	320
8.5 ACQUISIZIONE FISICA	320
8.6 ACQUISIZIONE FISICA UTILIZZANDO HARDWARE O SOFTWARE DEDICATI	322
9. ANALISI DEL DISPOSITIVO IPAD	332
9.1 CARVING DI FILE IMMAGINE	338
10. BIBLIOGRAFIA	345
CAPITOLO DECIMO	
INTRODUZIONE ALLA BLACKBERRY FORENSICS	347
1. INTRODUZIONE	347
2. CARATTERISTICHE TECNOLOGICHE	348
3. FUNZIONALITÀ ED ARCHITETTURA	350

4. MECCANISMI DI SICUREZZA ADOTTATI	352
5. ASPETTI GENERALI DELL'ATTIVITÀ FORENSE	355
6. LA DATA RETENTION DI RIM	355
7. ATTIVITÀ SUL SERVER BES	357
8. INFORMAZIONI GENERATE DAL BLACKBERRY DESKTOP MANAGER	360
9. GESTIONE DEL TERMINALE	361
10. ACQUISIZIONE LOGICA DELLE INFORMAZIONI IN MEMORIA	362
11. IL FORMATO DEI FILE DI BACKUP	365
12. UTILIZZO DEI SIMULATORI	370
13. ANALISI DELLE INFORMAZIONI ACQUISITE DAL TERMINALE	371
14. LE PROBLEMATICHE DELL'ACQUISIZIONE FISICA	375
15. CONCLUSIONI	376
16. BIBLIOGRAFIA	376

CAPITOLO UNDICESIMO

WINDOWS REGISTRY FORENSICS:**INTRODUZIONE ALLE RISORSE MOST RECENTLY USED****ANALISI DELLE SHELLBAGS**

	379
1. INTRODUZIONE	379
1.1 NOMENCLATURA	380
2. LISTE MRU	380
2.1 RICERCHE	381
2.2 LAST VISITED	381
2.3 OPENSAVE	382
2.4 RUN	382
2.5 USER ASSIST	382
2.6 SHELLBAGS	384
2.6.1 CONTENUTO DI SHELLNORAM	385
2.6.2 CONTENUTO DI BAGMRU	386
2.6.3 CONTENUTO DI BAGS	388
2.6.4 IL VALORE MRULISTEX	388
2.6.5 LEGGERE LE SHELLBAGS	389
2.6.6 QUALI DATI SI POSSONO OTTENERE	391
2.6.7 INTERAZIONI CON L'UTENTE	392
2.6.8 IL VALORE ITEMPOS	393
3. TOOLS	395
3.1 TZWORKS – SBAG.EXE -	

WWW.TZWORKS.NET/PROTOTYPE_PAGE.PHP?PROTO_ID=14	395
3.2 X-WAYS FORENSICS 16 - WWW.WINHEX.COM	396
3.3 WRA – 1.5.2 -	
HTTP://MYSITE.VERIZON.NET/HARTSEC/FILES/WRA.ZIP	397
3.4 REGRIPPER -	
HTTP://REGRIPPER.NET/REGRIPPER/REGRIPPER030911.ZIP	398
3.5 SHELLBAGSVIEW - HTTP://WWW.NIRSOFT.NET	399
4. CASE STUDY	400
5. CONCLUSIONI	401
6. RIFERIMENTI BIBLIOGRAFICI E RISORSE INTERNET	402
6.1 TOOLS	402
CAPITOLO DODICESIMO	
MOBILE FORENSICS: CASE STUDY SU ANDROID	403
1. PREMESSA	403
2. I DATI UTILI PER UNA INDAGINE FORENSE:	
PARTE GENERALE	403
3. SEQUESTRO ED ISOLAMENTO DEL DISPOSITIVO: CENNI	405
4. ACQUISIZIONE LOGICA FORENSE CON OXYGEN	
FORENSIC SUITE	408
5. CONCLUSIONI	416
CAPITOLO TREDICESIMO	
DAL REATO DI RICICLAGGIO	
AL REATO DI CYBERLAUNDERING	419
1. INTRODUZIONE	419
2. COME SI CERCA DI “OCCULTARE” L’EFFETTIVA	
ORIGINE E IL PERCORSO DEL DENARO?	421
3. IL RICICLAGGIO ARRIVA SUL WEB	422
4. COME SOGGETTI DEL TUTTO IGNARI POSSONO	
DIVENTARE COMPLICI ED AUTORI DI REATI	422
5. CYBERLAUNDERING: IL RICICLAGGIO DEL	
FUTURO ORMAI PRESENTE	425
PROFILO AUTORI	429