

# Obsah

<b>Předmluva</b>	<b>7</b>
<b>1. Úvod</b>	<b>9</b>
<b>2. Historie a vývoj oboru digitální forenzní analýza</b>	<b>11</b>
<b>2.1 Technické specializace pro forenzní analýzu</b>	<b>15</b>
2.1.1 Computer Forensics	15
2.1.2 Analýza mobilních zařízení	15
2.1.3 Data Recovery	16
2.1.4 Analýza cloudových prostředí	16
2.1.5 Analýza síťové komunikace	16
2.1.6 Analýza škodlivého kódu	16
2.1.7 Analýza operační paměti	17
2.1.8 E-Discover	17
<b>3. Profesní uplatnění digitální forenzní analýzy</b>	<b>19</b>
<b>3.1 Znalecké zkoumání</b>	<b>19</b>
<b>3.2 Internal (Insider) Threat Investigation</b>	<b>22</b>
<b>3.3 Nespokojený/Zákeřný uživatel</b>	<b>22</b>
<b>3.4 Nedbalý uživatel</b>	<b>24</b>
<b>3.5 Infiltrátor</b>	<b>26</b>
<b>3.6 Zvládání bezpečnostních incidentů</b>	<b>28</b>
<b>4. Životní cyklus zvládání bezpečnostních incidentů</b>	<b>33</b>
<b>4.1 Příprava</b>	<b>33</b>
<b>4.2 Detekce a analýza</b>	<b>34</b>
<b>4.3 Izolace, eliminace a obnova</b>	<b>34</b>
<b>4.4 Poučení z incidentu</b>	<b>35</b>
<b>5. Podmínky forenzní analýzy</b>	<b>37</b>
<b>5.1 Legalita</b>	<b>37</b>
<b>5.2 Integrita</b>	<b>37</b>
<b>5.3 Opakovatelnost/Přezkoumatelnost</b>	<b>38</b>
<b>5.4 Nepodjatost</b>	<b>38</b>
<b>6. Digital Investigation Framework</b>	<b>39</b>
<b>6.1 Zajišťování stop a dokumentace místa činu</b>	<b>39</b>
<b>6.2 Analýza zajištěných stop</b>	<b>40</b>
<b>6.3 Analýza a korelace informací</b>	<b>40</b>
<b>6.4 Formulování závěrů, reportování</b>	<b>40</b>

## 7. Digitální stopy 43

<b>7.1 Typy stop</b>	<b>43</b>
7.1.1 Originální zařízení	43
7.1.2 Best Evidence	43
7.1.3 Binární kopie	43
7.1.4 Forezní obraz disku	44
7.1.6 Custom Content Image	45
<b>7.2 Zajišťování stop</b>	<b>45</b>
<b>7.3 Priorita zajišťování stop</b>	<b>45</b>
<b>7.4 Workflow a způsoby zajišťování stop</b>	<b>46</b>
<b>7.5 Online/Live</b>	<b>47</b>
7.5.1 Operační paměť	50
7.5.2 Síťový provoz	51
7.5.3 Encrypted DISK DETECTOR (EDD)	52
7.5.4 Triage	54
7.5.5 Zajištění síťových disků	56
<b>7.6 Offline</b>	<b>57</b>
<b>7.7 Full Disk Image</b>	<b>57</b>
<b>7.8 Specializované metody zajišťování stop</b>	<b>58</b>

## 8. Datové typy 59

## 9. Analýza artefaktů operačních systémů 61

<b>9.1 Systémové registry</b>	<b>61</b>
9.1.1 Nástroje	62
9.1.2 Název počítače	65
9.1.3 Poslední přihlášený uživatel	70
9.1.4 Síťová konfigurace	71
9.1.5 Profilace WiFi sítí	72
9.1.6 Identifikace USB paměťových zařízení	74
9.1.7 Mapování USB zařízení	76
9.1.8 Spouštění aplikací	76
9.1.9 Ručně zadané cesty k souborům nebo adresářům	78
9.1.10 Remote Desktop Connection Artifacts	78
9.1.11 Background Activity Moderator (BAM)	80
9.1.12 Windows System Services	80
9.1.13 MSIX registry	81
<b>9.2 Protokoly událostí</b>	<b>84</b>
9.2.1 Přihlášení uživatelů	86
9.2.2 RDP connection	87
9.2.3 Spouštění aplikací	99
9.2.4 USB zařízení	100
9.2.5 WiFi	101
9.2.6 Internet Access	102
9.2.7 Powershell	102
9.2.8 Windows Defender	103
9.2.9 Microsoft Office	105
<b>9.3 Scheduled tasks</b>	<b>106</b>

<b>9.4 Artefakty souborových systémů</b>	<b>109</b>
9.4.1 Master File Table (MFT)	110
9.4.2 Alternate Data Stream (ADS)	112
<b>9.5 Prefetch</b>	<b>115</b>
<b>9.6 Windows Search Index DB</b>	<b>117</b>
9.6.1 File_Report	119
9.6.2 Internet_History_Report	120
9.6.3 Activity_History_Report	121
<b>9.7 Shell Items</b>	<b>122</b>
9.7.1 LNK	122
9.7.2 Recent Docs	124
9.7.3 JumpLists	125
<b>9.8 Thumbs.db and Thumbcache</b>	<b>126</b>
9.8.1 Mapování souborů	128
<b>9.9 Automatizace analýzy</b>	<b>130</b>
9.9.1 KAPE	130
9.9.2 USB Detective	133
<b>9.10 Indicator of Compromise (IOC)</b>	<b>134</b>
9.10.1 ChainSaw	136
9.10.2 Hayabusa	139
9.10.3 Thor Lite + Fenrir + Loki	140

## 10. Metadata 143

<b>10.1 Obrazové soubory</b>	<b>143</b>
10.1.1 Exchangeable Image File	144
10.1.2 ExifDataView	144
10.1.3 ExifTool	145
<b>10.2 Geolokalizace</b>	<b>148</b>
10.2.1 EXIF záznamy	148
10.2.2 Geolokace WiFi	153
10.2.3 IP adresy	155

## 11. Práce s obrazy disků 157

<b>11.1 FTK Imager</b>	<b>157</b>
11.1.1 Vytvoření obrazu disku	157
11.1.2 Otevření obrazu disku	159
11.1.3 Mount	160
11.1.4 Výpis obsahu disku – Directory Listing	160
11.1.5 Výpis kontrolních sum – Hash Listing	161
11.1.6 Custom Content Image	163
11.1.7 MAGNET Encrypted Disk Detector	164

## 12. Obnova smazaných dat 167

<b>12.1 RecycleBin</b>	<b>168</b>
<b>12.2 R-Studio</b>	<b>170</b>
<b>12.3 Data Carving</b>	<b>177</b>
<b>12.4 PhotoRec</b>	<b>177</b>
<b>12.5 BStrings</b>	<b>180</b>

<b>13. Základní kódování textu</b>	<b>183</b>
<b>13.1 Kódování Base16   Hexadecimal</b>	<b>183</b>
<b>13.2 Kódování Base64</b>	<b>184</b>
<b>14. Analýza webových prohlížečů</b>	<b>187</b>
<b>14.1 Profily</b>	<b>188</b>
<b>14.2 Nástroje</b>	<b>189</b>
<b>English Summary</b>	<b>197</b>
<b>Závěr</b>	<b>201</b>
<b>Přílohy</b>	<b>203</b>
<b>Seznam obrázků</b>	<b>205</b>
<b>Literatura</b>	<b>211</b>
<b>Rejstřík</b>	<b>223</b>