# Forensics Tool and Its utilization

### Volatile Memory Forensics

1. RAM Capturers
2. Tools:
3. Volatality Download  Docs
4. Dumpit Download Docs
5. RamDump Download  Docs
6. Magnet Ram capture Download Docs
7. FTK Imager Download Docs
8. Belkasoft Live RAM Capturer Download Docs
9. Volafox  Download   for MacOS
10. WindowsScope Download

### Imaging & Analysis of Logical and Physical Drives

11. Imaging of HDD, Pen drives and write blocker
12. Tools:
13. The Sleuth Kit Autopsy Download Docs
14. Helix Download
15. Mac-Robber Download Docs
16. Access Data FTK Imager Download Docs
17. ProDiscover Forensic Download Docs
18. EnCase Tool Download Docs
19. Magnet forensics tool Download Docs
20. X-Ways Forensics Download Doc
21. Shadow explorer Download Docs
22. USB Write Blocker Download Docs
23. Guymager Download Docs

### Retrieving & Reviewing Logs

24. System & Registry Analysis
25. Tools:
26. USB Deview Download Docs
27. USB Historian Download Docs
28. Process Explorer Download Docs
29. PE Viewer Download Docs
30. Process monitor Download Docs
31. Log Parser Download Docs
32. LastActivityView Download Docs
33. Dependency walker Download Doc
34. Reg Ripper Download Docs
35. Registry Recon Download Docs
36. System Recon Tools Download
37. Registry Explorer Download Docs
38. RegShot Download
39. Resource Hacker Download Docs

### Extracting Information

40. Finding metadata, recovering data stream and analysis of files
41. Tools:
42. E-Discovery Download Docs
43. Exif Data Viewer Download Docs
44. Ghiro Download Docs
45. Photorec Download Docs
46. Agent Ransack Download
47. NFI Defraser Download
48. Forensic User Info Download
49. Jeffrey’s Metadata viewer web
50. Mosses Forensics Tool Web
51. Forensically Web
52. Fotoforensics Web
53. Tineye Reverse Image Search Web

### Data Recovery

54. Tools :
55. Foremost Download Docs
56. Recuva Download Docs
57. Mini tool power data recovery Download Docs
58. Passware Download
59. EaseUS Download
60. EDB Viewer Download
61. Disk Drill Download
62. ISOBuster Download

### Multimedia Forensics

63. Steganography, hiding and finding secret messages
64. Tools :
65. Camouflage (Imager Steganography) Download Docs
66. Ssuite Picsel (Imager Steganography) Download Docs
67. Hide n Send (Imager Steganography) Download Docs
68. OpenStego Download
69. crypture Download
70. Steghide Download
71. Xiao Steganography (Imager Steganography) Download Docs
72. Quickstego (Imager Steganography) Download Docs
73. wbStego (Document Steganography) Download Docs
74. Our secret (Video Steganography) Download Docs
75. Quick crypto (Folder Steganography) Download Docs
76. invisible secret Download
77. Deep Sound Download
78. Sonic visualizer Download
79. Openpuff Download
80. Netcross Download

81. StegDetect
82. Spammimic Web (Mail Steganography)

### Mobile Device Forensics

83. Collecting evidence from mobile phones
84. Tools:
85. Oxygen forensics Download Docs
86. XRY Mobile Forensics Download Docs
87. Magnet Mobile Forensics Download Docs
88. Google Maps Investigator Download
89. Paraben Download1 Download2 Docs
90. Mobiledit Download Docs

### Network Evidence & Forensics Investigation

91. Live Network Analysis of Devices
92. Wireless Capture Traffic & Analysis
93. Tools:
94. NMAP Download Docs
95. Wireshark Download Docs
96. Xplico Download Docs
97. Cacti Network Forensics Tool Download Doc
98. Observium Download Docs
99. Angry IP Scanner Download Docs
100. NetworkMiner packet analyzer Download Docs
101. Forensic Investigator in Splunk Download Docs
102. NIDS Network forensics Download Docs
103. Other Tool Web

### Browser forensics

104. Extracting information from browser, Email,
105. Tools:
106. Internet Evidence Finder Download Docs
107. Bulk extractor Download Docs
108. Browser History Download Docs
109. Dumpzilla Download Doc
110. Mail Examiner Download
111. Email tracker Download

### Signature, Hashing, encryption

112. Tools:
113. Hex Editor Download Docs
114. Win Hex Download Docs
115. Hash Check Download Docs

116. Igorware Download Docs
117. Garry kesler database of file signatures Web
118. Hash File database Web
119. TrueCrypt Download
120. Encrypted Disk Detector Download
121. HashMyFiles Download
122. Malware database Web

**Database Forensics**

123. Forensics Toolkit for Database Download
124. http://dbgroup.cdm.depaul.edu/DF-Toolkit.html

**TCToolkit** (The Coroner's Toolkit)

125. NirSoft launcher Download Resource Doc,
126. Coffee (Computer Online Forensic Evidence Extractor is a tool kit) Download Docs
127. Windows Sysinternal Tool Suite Download Docs
128. PlainSight Download Docs
129. Crowdstrike Download Docs
130. FAW (Forensics Acquisition of Websites) Download Docs
131. Toolsley Dowload Docs
132. CodeSuite Download Docs (IP authenticity)

**Anti-Computer Forensics**

133. CCleaner Download
134. Evidence Eliminator Download
135. DECAF Download
136. Privacy Eraser Download
137. Batch Purifier Download
138. Dban Download
139. Blancco Download

**Bootable Forensics Tools and OS**

140. Santoku OS Download
141. SANS Investigative Forensic Toolkit (SIFT) Download
142. DEFT OS Download
143. Parrot OS Download
144. Paladin Forensics suite Download
145. CAINE (Computer Aided INvestigative Environment ) + Win UFO (Windows Ultimate Forensics Outflow) Download Docs
146. SOF-ELK Download

**Incident response**

147. FireEye RedLine Download
148. Eric Zimmerman Tools Download Docs
149. Cyber Triage Download Docs
150. Alien Vault Download
151. Hive Project Download
152. Cyphon Download
153. IBM Qrader Doc
154. Splunk Doc