Forensic Tools

100 Useful Forensic Tools

1. Autospy
2. EnCase
3. AccessData(FTK)
4. X-Ways Forensics
5. Sleuth Kit
6. Volatility
7. Wireshark
8. Cellebrite UFED
9. Email Collector
10. Forensics(DFF)
11. Magnet AXIOM
12. Oxygen Detective
13. OSForensics
14. NetworkMiner
15. RegRipper
16. Bulk Extractor
17. Ghiro
18. Scalpel
19. HxD
20. TestDisk
21. PhotoRec
22. CAINE
23. Axiom Cyber
24. Belkasoft Evidence
25. Fibratus
26. Autopsy Browser
27. Kali Linux
28. DEFT
29. Volatility Framework
30. PyFlag
31. Plaso (log2timeline)
32. TSK (The Sleuth Kit)
33. Redline
34. Snort
35. Tcpdump
36. Ngrep
37. dcfldd
38. Wireshark
39. SIFT (SANS)
40. Paladin
41. CAINE Live
42. XRY (XAMN)
43. BlackLight
44. WinHex
45. Access FTK Imager
46. DC3DD
47. Raptor
48. EnCase Imager
49. Guymager
50. Scalpel
51. Extundelete
52. Xplico
53. Foremost
54. Hunchback
55. Autopsy Tools
56. OSForensics Imager
57. Dislocker
58. Bulk Extractor
59. SANS SIFT
60. Live View
61. LRR
62. NTFS-3G
63. WindowsSCOPE
64. Volafox
65. Amcache Parser
66. The Hive
67. GRR Rapid Response

©Cyber Threat Intelligence

68. Rekall
69. DFF
70. SSDeep
71. KAPE
72. USB Write Blocker
73. AIL
74. Rifiuti2
75. VolDiff
76. WinAudit
77. hfind
78. Yara
79. Checkm8
80. Olefile
81. Pyew
82. E01 Examiner
83. USBDeview
84. Autopsy - iPhone
85. DC3-MWCP
86. X-Ways Imager
87. Memoryze
88. EVTXtract
89. Speedit
90. SniffPass
91. Nmap
92. OSINT Framework
93. Recon-ng
94. OSINT-SPY
95. Shodan
96. Maltego
97. SpiderFoot
98. Metagoofil
99. TheHarvester
100. Creepy

From:
https://wiki.fortier-family.com/ - **Warnaud's Wiki**

Permanent link:
https://wiki.fortier-family.com/cybersecurity/tools/forensic

Last update: **2026/09/20 14:33**