100 FREE SECURITY TOOLS

For ethical hackers and forensic investigators

INSIDE CLOUD
AND SECURITY

100 FREE SECURITY TOOLS

For ethical hackers and forensic investigators

1. **Autopsy** - Open source digital forensics platform to analyze hard drives and smart phones https://www.autopsy.com
2. **EnCase** - Commercial computer forensics software for e-discovery and investigations by OpenText https://www.opentext.com/products-and-solutions/products/software/encase-platform
3. **AccessData (FTK)** - Forensic toolkit computer investigation software by AccessData https://accessdata.com/products-services/forensic-toolkit-ftk
4. **X-Ways Forensics** - Integrated computer forensics software by X-Ways Software Technology http://www.x-ways.net/forensics/
5. **Sleuth Kit** - Open source digital forensics tools for analyzing disk images and file systems https://www.sleuthkit.org
6. **Volatility** - Memory forensics framework to analyze volatile memory dumps and artifacts https://www.volatilityfoundation.org/
7. **Wireshark** - Network protocol analyzer useful for network forensics and traffic analysis https://www.wireshark.org
8. **Cellebrite UFED** - Commercial mobile forensic software to extract data from phones and tablets https://www.cellebrite.com/en/ufed-ultimate/
9. **Email Collector** - Tool to collect and analyze email data during investigations https://www.accessdata.com/products-services/e-discovery/email-examination/ftk-email-collector
10. **Forensics (DFF)** - Digital forensics framework, an open source platform for investigations https://github.com/arxsys/dff
11. **Magnet AXIOM** - Commercial digital investigations platform from Magnet Forensics https://www.magnetforensics.com/products/magnet-axiom/
12. **Oxygen Detective** - Cloud extraction tool for investigations involving cloud services https://www.oxygen-forensic.com/en/oxygen-detective
13. **OSForensics** - Specialized forensics tools for Microsoft systems from PassMark https://www.osforensics.com/
14. **NetworkMiner** - Open source network forensic analyzer useful for investigating traffic http://www.netresec.com/?page=NetworkMiner
15. **RegRipper** - Tool to parse Windows registry files and dig for useful data https://github.com/keydet89/RegRipper3.0
16. **Bulk Extractor** - Scans disk images and extract interesting bits of data https://github.com/simsong/bulk_extractor
17. **Ghiro** - Web site screenshots and analysis for forensic investigations http://www.getghiro.org/
18. **Scalpel** - File carver which recovers files based on headers and footers http://www.digitalforensicssolutions.com/Scalpel/
19. **HxD** - Hex editor useful for analyzing raw disk and memory dumps https://mh-nexus.de/en/hxd/
20. **TestDisk** - Data recovery tool, useful when file systems get corrupted https://www.cgsecurity.org/wiki/TestDisk
21. **PhotoRec** - Recovery tool specifically focused on photos and media files https://www.cgsecurity.org/wiki/PhotoRec
22. **CAINE** - Italian GNU/Linux live distribution with many forensics tools https://www.caine-live.net
23. **Axiom Cyber** - Commercial digital forensics and incident response platform https://axiomcyber.com/axiom-cyber/
24. **Belkasoft Evidence** - Commercial all-in-one forensics solution for Windows, mobile etc https://belkasoft.com/evidence
25. **Fibratus** - Tool to explore and trace Windows kernel activity and data https://www.jpcert.or.jp/english/pub/sr/ir_research.html
26. **Autopsy Browser** - GUI interface for autopsy digital forensics platform https://www.autopsy.com/browser/
27. **Kali Linux** - Penetration testing Linux distribution with many useful security tools https://www.kali.org
28. **DEFT** - Linux distribution configured specifically for computer forensics http://www.deftlinux.net
29. **Volatility Framework** - Advanced memory forensics framework with plugins and APIs https://www.volatilityfoundation.org/
30. **PyFlag** - Legacy Australian forensic and log analysis GUI platform http://www.pyflag.net

31. Plaso (log2timeline) - Extract timestamps from various logs and aggregate timeline https://plaso.readthedocs.io/en/latest/sources/user/log2timeline.html
32. TSK (The Sleuth Kit) - File system and disk analysis tools originally focussed on NTFS https://www.sleuthkit.org/sleuthkit/
33. Redline - Host investigations and malware analysis tool by FireEye https://www.fireeye.com/services/freeware/redline.html
34. Snort - Open source intrusion detection and network monitoring system https://www.snort.org
35. Tcpdump - Capture and analyze network traffic on Unix-like systems https://www.tcpdump.org
36. Ngrep - Search within network traffic payloads like grep for text streams http://ngrep.sourceforge.net/
37. dcfldd - Disk cloning and forensics tool, version of dd with hashing https://dcfldd.sourceforge.net/
38. Wireshark - Network traffic analyzer useful for network forensics https://www.wireshark.org
39. SIFT (SANS) - Ubuntu-based distribution for forensic analysis https://digital-forensics.sans.org/community/downloads
40. Paladin - USB image mounted as virtual drive with write-protection https://sumuri.com/software/paladin/
41. CAINE Live - Self-contained bootable forensic environment https://www.caine-live.net/page5/page5.html
42. XRY (XAMN) - Commercial mobile forensic software to analyze phones https://msab.com/xry/
43. BlackLight - Powerful Windows-based forensics analysis platform https://www.blackbagtech.com/blacklight.html
44. WinHex - Hex editor, particularly helpful for low-level analyzing raw data https://www.x-ways.net/winhex/
45. Access FTK Imager - Disk and volume imaging software from AccessData https://accessdata.com/product-download
46. DC3DD - Improved version of dd for forensics, handles errors better https://github.com/Defense-Cyber-Crime-Center/DC3-DD
47. Raptor - Validation tool to verify integrity of forensic copies http://forensic.rampar.net/
48. EnCase Imager - Disk imaging tool from Guidance Software https://www.guidancesoftware.com/encase-imager
49. Guymager - Open source disk cloning and imaging tool for Linux https://guymager.sourceforge.io
50. Scalpel - File carver recovering files based on header/footer signatures http://www.digitalforensicssolutions.com/Scalpel/
51. Extundelete - Used to recover deleted files from mountable images http://extundelete.sourceforge.net/
52. Xplico - Network forensics tool that rebuilds sessions from traffic http://www.xplico.org/
53. Foremost - File carving utility to recover files using header/footer definitions http://foremost.sourceforge.net
54. Hunchback - High speed packet capture and transmission tool https://hunchback.sourceforge.net/
55. Autopsy Tools - Plugins and tools used alongside Autopsy forensics GUI https://www.autopsy.com/extend-autopsy/
56. OSForensics Imager - Hardware write block tool for connecting devices https://www.osforensics.com/tools/write-blockers.html
57. Dislocker - Decrypts Bitlocker encrypted volumes with mounted filesystem https://github.com/Aorimn/dislocker
58. Bulk Extractor - Extract forensically interesting information from disk images https://github.com/simsong/bulk_extractor
59. SANS SIFT - Ubuntu-derived distro for digital forensic analysis https://digital-forensics.sans.org/community/downloads
60. Live View - Volatile memory analysis tool for Windows systems http://liveview.sourceforge.net/
61. LRR - Tool for viewing Windows artifacts including LNK files https://github.com/EricZimmerman/LinkRunner
62. NTFS-3G - Open source cross-platform NTFS driver with write support https://www.tuxera.com/community/open-source-ntfs-3g/
63. WindowsSCOPE - Registry analysis tool for dumped SYSTEM/SAM/SECURITY hives http://www.windowsscope.com/
64. Volafax - Forensic system suited for investigations over remote areas https://github.com/jipegit/FlaxVolafox

65. Amcache Parser - Recovers data from Windows 10 Amcache.hve artifact file https://tzworks.net/prototype_page.php?proto_id=11

66. The Hive - Web interface offering querying capabilities for hive files https://thehive-project.org

67. GRR Rapid Response - Incident response framework focused on remote live forensics https://github.com/google/grr

68. Rekall - Advanced forensic memory analysis framework powered by Python http://www.rekall-forensic.com/

69. DFF - Open source digital forensics framework and platform written in Python https://github.com/arxsys/dff

70. SSDeep - Fuzzy hashing tool used for malware clustering and piecewise comparisons https://ssdeep-project.github.io/ssdeep/index.html

71. KAPE - Target acquisition tool focused on enterprise lines of business https://www.krollartifactparser.com/

72. USB Write Blocker - Hardware ensuring write protection when imaging USB devices

73. AIL - Network and host monitoring system for identification of intrusions https://www.cert.org/incident-management/products-services/ail.cfm

74. Rifiuti2 - Analyzes Windows Recycle Bin INFO2 files and recovers filenames https://github.com/abelcheung/rifiuti2

75. VolDiff - Compares memory images and highlights differences for analysis https://github.com/aim4r/VolDiff

76. WinAudit - Scans Windows systems and reports changes from baseline http://www.winaudit.com/

77. hfind - Carves unallocated space and extracts hidden/deleted data into files https://www.mcafee.com/enterprise/en-us/downloads/free-tools/hfind.html

78. Yara - Pattern matching tool aimed at malware researchers

79. Checkm8 - Jailbreaking tool extracting data from passcode locked iOS devices https://checkm8.info/

80. Olefile - Python package for parsing OLE and Office documents https://github.com/decalage2/olefile

81. Pyew - Python tool for malware analysis static and dynamic https://github.com/joxeankoret/pyew

82. E01 Examiner - Software utility for mounting EnCase evidence file formats https://e01examiner.com/

83. USBDeview - Handy Windows tool listing all USB devices ever connected https://www.nirsoft.net/utils/usb_devices_view.html

84. Autopsy - iPhone - Autopsy module adds iOS analysis functionality https://sleuthkit.org/autopsy/plugins.php

85. DC3-MWCP - Collection of tools for forensic enterprise analysis from DC3 https://www.dc3.mil/software-catalog/

86. X-Ways Imager - Disc imaging tool to create forensic images, integrated into X-Ways Forensics http://www.x-ways.net/imager/index-m.html

87. Memoryze - Memory acquisition and analysis tool for Windows systems https://www.fireeye.com/services/freeware/memoryze.html

88. EVTExtract - Automated parsing modules for Windows event log records https://evtxtract.readthedocs.io/en/latest/

89. Speedit - Detection and analysis of spyware, keyloggers, trojans etc https://www.komodia.com/speedit-sdk

90. SniffPass - Sniffs passwords and other sensitive information from a network http://www.komodia.com/sniffpass

91. Nmap - Network scanning and host discovery tool helpful for reconnaissance https://nmap.org/

92. OSINT Framework - Gathering publicly available online data regarding targets https://osintframework.com/

93. Recon-ng - Web based open source reconnaissance framework https://github.com/lanmaster53/recon-ng

94. OSINT-SPY - Performs extensive reconnaissance using 300+ OSINT data sources https://github.com/SharadKumar97/OSINT-SPY

95. Shodan - Search engine for Internet connected devices https://www.shodan.io

96. Maltego - Link analysis and data mining for gathering information https://www.maltego.com/

97. SpiderFoot - OSINT automation tool gathering threat intelligence data https://www.spiderfoot.net/

98. Metagoofil - Extract metadata of public documents from a target website https://github.com/laramies/metagoofil

99. TheHarvester - Gather emails, names, URLs from different public sources https://github.com/laramies/theHarvester

100. Creepy - Geolocation OSINT tool to extract target location information from social media profiles https://www.geocreepy.com/

100 FREE SECURITY TOOLS

For ethical hackers and forensic investigators

Here are those same 100 resources, grouped by function.

Digital Forensics Frameworks:

1. Autopsy - Open source digital forensics platform to analyze hard drives and smart phones
https://www.autopsy.com
10. Forensics (DFF) - Digital forensics framework, an open source platform for investigations
https://github.com/arxsys/dff
22. CAINE - Italian GNU/Linux live distribution with many forensics tools
https://www.caine-live.net
26. Autopsy Browser - GUI interface for autopsy digital forensics platform
https://www.autopsy.com/browser/
27. Kali Linux - Penetration testing Linux distribution with many useful security tools
https://www.kali.org
28. DEFT - Linux distribution configured specifically for computer forensics
http://www.deftlinux.net
29. Volatility Framework - Advanced memory forensics framework with plugins and APIs
https://www.volatilityfoundation.org/
39. SIFT (SANS) - Ubuntu-based distribution for forensic analysis
https://digital-forensics.sans.org/community/downloads
41. CAINE Live - Self-contained bootable forensic environment
https://www.caine-live.net/page5/page5.html
59. SANS SIFT - Ubuntu-derived distro for digital forensic analysis
https://digital-forensics.sans.org/community/downloads
68. Rekall - Advanced forensic memory analysis framework powered by Python
http://www.rekall-forensic.com/

Disk Forensics:

2. EnCase - Commercial computer forensics software for e-discovery and investigations by OpenText
https://www.opentext.com/products-and-solutions/products/software/encase-platform
3. AccessData (FTK) - Forensic toolkit computer investigation software by AccessData
https://accessdata.com/products-services/forensic-toolkit-ftk
4. X-Ways Forensics - Integrated computer forensics software by X-Ways Software Technology
http://www.x-ways.net/forensics/
5. Sleuth Kit - Open source digital forensics tools for analyzing disk images and file systems
https://www.sleuthkit.org
30. PyFlag - Legacy Australian forensic and log analysis GUI platform
http://www.pyflag.net
32. TSK (The Sleuth Kit) - File system and disk analysis tools originally focussed on NTFS
https://www.sleuthkit.org/sleuthkit/
42. XRY (XAMN) - Commercial mobile forensic software to analyze phones https://msab.com/xry/
43. BlackLight - Powerful Windows-based forensics analysis platform
https://www.blackbagtech.com/blacklight.html
44. WinHex - Hex editor, particularly helpful for low-level analyzing raw data
https://www.x-ways.net/winhex/
45. Access FTK Imager - Disk and volume imaging software from AccessData
https://accessdata.com/product-download
46. DC3DD - Improved version of dd for forensics, handles errors better
https://github.com/Defense-Cyber-Crime-Center/DC3-DD
47. Raptor - Validation tool to verify integrity of forensic copies
http://forensic.rampar.net/
48. EnCase Imager - Disk imaging tool from Guidance Software
https://www.guidancesoftware.com/encase-imager
49. Guymager - Open source disk cloning and imaging tool for Linux https://guymager.sourceforge.io

Memory Forensics:

6. Volatility - Memory forensics framework to analyze volatile memory dumps and artifacts https://www.volatilityfoundation.org/
29. Volatility Framework - Advanced memory forensics framework with plugins and APIs https://www.volatilityfoundation.org/
60. Live View - Volatile memory analysis tool for Windows systems http://liveview.sourceforge.net/
68. Rekall - Advanced forensic memory analysis framework powered by Python http://www.rekall-forensic.com/
75. VolDiff - Compares memory images and highlights differences for analysis https://github.com/aim4r/VolDiff
87. Memoryze - Memory acquisition and analysis tool for Windows systems https://www.fireeye.com/services/freeware/memoryze.html

Carving Tools:

16. Bulk Extractor - Scans disk images and extract interesting bits of data https://github.com/simsong/bulk_extractor
18. Scalpel - File carver which recovers files based on headers and footers http://www.digitalforensicssolutions.com/Scalpel/
50. Scalpel - File carver recovering files based on header/footer signatures http://www.digitalforensicssolutions.com/Scalpel/
51. Extundelete - Used to recover deleted files from mountable images http://extundelete.sourceforge.net/
52. Xplico - Network forensics tool that rebuilds sessions from traffic http://www.xplico.org/
53. Foremost - File carving utility to recover files using header/footer definitions http://foremost.sourceforge.net
55. Autopsy Tools - Plugins and tools used alongside Autopsy forensics GUI https://www.autopsy.com/extend-autopsy/
57. Dislocker - Decrypts Bitlocker encrypted volumes with mounted filesystem https://github.com/Aorimn/dislocker
58. Bulk Extractor - Extract forensically interesting information from disk images https://github.com/simsong/bulk_extractor
77. hfind - Carves unallocated space and extracts hidden/deleted data into files https://www.mcafee.com/enterprise/en-us/downloads/free-tools/hfind.html

Network Monitoring:

7. Wireshark - Network protocol analyzer useful for network forensics and traffic analysis https://www.wireshark.org
14. NetworkMiner - Open source network forensic analyzer useful for investigating traffic http://www.netresec.com/?page=NetworkMiner
34. Snort - Open source intrusion detection and network monitoring system https://www.snort.org
35. Tcpdump - Capture and analyze network traffic on Unix-like systems https://www.tcpdump.org
36. Ngrep - Search within network traffic payloads like grep for text streams http://ngrep.sourceforge.net/
38. Wireshark - Network traffic analyzer useful for network forensics https://www.wireshark.org
54. Hunchback - High speed packet capture and transmission tool https://hunchback.sourceforge.net/
73. AIL - Network and host monitoring system for identification of intrusions https://www.cert.org/incident-management/products-services/ail.cfm

Windows Artifact Analysis:

15. RegRipper - Tool to parse Windows registry files and dig for useful data
https://github.com/keydet89/RegRipper3.0
25. Fibratus - Tool to explore and trace Windows kernel activity and data
https://www.jpcert.or.jp/english/pub/sr/ir_research.html
61. LRR - Tool for viewing Windows artifacts including LNK files
https://github.com/EricZimmerman/LinkRunner
62. NTFS-3G - Open source cross-platform NTFS driver with write support
https://www.tuxera.com/community/open-source-ntfs-3g/
63. WindowsSCOPE - Registry analysis tool for dumped SYSTEM/SAM/SECURITY hives
http://www.windowsscope.com/
65. Amcache Parser - Recovers data from Windows 10 Amcache.hve artifact file
https://tzworks.net/prototype_page.php?proto_id=11
66. The Hive - Web interface offering querying capabilities for hive files https://thehive-project.org
74. Rifiuti2 - Analyzes Windows Recycle Bin INFO2 files and recovers filenames
https://github.com/abelcheung/rifiuti2
76. WinAudit - Scans Windows systems and reports changes from baseline http://www.winaudit.com/
83. USBDeview - Handy Windows tool listing all USB devices ever connected
https://www.nirsoft.net/utils/usb_devices_view.html
85. DC3-MWCP - Collection of tools for forensic enterprise analysis from DC3 https://www.dc3.mil/software-catalog/
88. EVTExtract - Automated parsing modules for Windows event log records
https://evtxtract.readthedocs.io/en/latest/

Hex Editors:

19. HxD - Hex editor useful for analyzing raw disk and memory dumps https://mh-nexus.de/en/hxd/
44. WinHex - Hex editor, particularly helpful for low-level analyzing raw data https://www.x-ways.net/winhex/

Data Extraction Tools:

8. Cellebrite UFED - Commercial mobile forensic software to extract data from phones and tablets
https://www.cellebrite.com/en/ufed-ultimate/
9. Email Collector - Tool to collect and analyze email data during investigations
https://www.accessdata.com/products-services/e-discovery/email-examination/ftk-email-collector
11. Magnet AXIOM - Commercial digital investigations platform from Magnet Forensics
https://www.magnetforensics.com/products/magnet-axiom/
12. Oxygen Detective - Cloud extraction tool for investigations involving cloud services https://www.oxygen-forensic.com/en/oxygen-detective
13. OSForensics - Specialized forensics tools for Microsoft systems from PassMark
https://www.osforensics.com/
23. Axiom Cyber - Commercial digital forensics and incident response platform
https://axiomcyber.com/axiom-cyber/
24. Belkasoft Evidence - Commercial all-in-one forensics solution for Windows, mobile etc
https://belkasoft.com/evidence
31. Plaso (log2timeline) - Extract timestamps from various logs and aggregate timeline
https://plaso.readthedocs.io/en/latest/sources/user/log2timeline.html
33. Redline - Host investigations and malware analysis tool by FireEye
https://www.fireeye.com/services/freeware/redline.html
37. dcfldd - Disk cloning and forensics tool, version of dd with hashing https://dcfldd.sourceforge.net/

Data Extraction Tools (continued):

40. Paladin - USB image mounted as virtual drive with write-protection https://sumuri.com/software/paladin/

56. OSForensics Imager - Hardware write block tool for connecting devices https://www.osforensics.com/tools/write-blockers.html

64. Volafax - Forensic system suited for investigations over remote areas https://github.com/jipegit/FlaxVolafox

67. GRR Rapid Response - Incident response framework focused on remote live forensics https://github.com/google/grr

69. DFF - Open source digital forensics framework and platform written in Python https://github.com/arxsys/dff

70. SSDeep - Fuzzy hashing tool used for malware clustering and piecewise comparisons https://ssdeep-project.github.io/ssdeep/index.html

71. KAPE - Target acquisition tool focused on enterprise lines of business https://www.krollartifactparser.com/

79. Checkm8 - Jailbreaking tool extracting data from passcode locked iOS devices https://checkm8.info/

80. Olefile - Python package for parsing OLE and Office documents https://github.com/decalage2/olefile

84. Autopsy - iPhone - Autopsy module adds iOS analysis functionality https://sleuthkit.org/autopsy/plugins.php

Data Recovery Tools:

20. TestDisk - Data recovery tool, useful when file systems get corrupted https://www.cgsecurity.org/wiki/TestDisk

21. PhotoRec - Recovery tool specifically focused on photos and media files https://www.cgsecurity.org/wiki/PhotoRec

Specialized Tools:

17. Ghiro - Web site screenshots and analysis for forensic investigations http://www.getghiro.org/

81. Pyew - Python tool for malware analysis static and dynamic https://github.com/joxeankoret/pyew

82. E01 Examiner - Software utility for mounting EnCase evidence file formats https://e01examiner.com/

86. X-Ways Imager - Disc imaging tool to create forensic images, integrated into X-Ways Forensics http://www.x-ways.net/imager/index-m.html

89. Speedit - Detection and analysis of spyware, keyloggers, trojans etc https://www.komodia.com/speedit-sdk

90. SniffPass - Sniffs passwords and other sensitive information from a network http://www.komodia.com/sniffpass

OSINT Tools:

91. Nmap - Network scanning and host discovery tool helpful for reconnaissance https://nmap.org/

92. OSINT Framework - Gathering publicly available online data regarding targets https://osintframework.com/

93. Recon-ng - Web based open source reconnaissance framework https://github.com/lanmaster53/recon-ng

94. OSINT-SPY - Performs extensive reconnaissance using 300+ OSINT data sources https://github.com/SharadKumar97/OSINT-SPY

95. Shodan - Search engine for Internet connected devices https://www.shodan.io

96. Maltego - Link analysis and data mining for gathering information https://www.maltego.com/

97. SpiderFoot - OSINT automation tool gathering threat intelligence data https://www.spiderfoot.net/

98. Metagoofil - Extract metadata of public documents from a target website https://github.com/laramies/metagoofil

OSINT Tools (continued):

91. Nmap - Network scanning and host discovery tool helpful for reconnaissance https://nmap.org/
92. OSINT Framework - Gathering publicly available online data regarding targets https://osintframework.com/
93. Recon-ng - Web based open source reconnaissance framework https://github.com/lanmaster53/recon-ng
94. OSINT-SPY - Performs extensive reconnaissance using 300+ OSINT data sources https://github.com/SharadKumar97/OSINT-SPY
95. Shodan - Search engine for Internet connected devices https://www.shodan.io
96. Maltego - Link analysis and data mining for gathering information https://www.maltego.com/
97. SpiderFoot - OSINT automation tool gathering threat intelligence data https://www.spiderfoot.net/
98. Metagoofil - Extract metadata of public documents from a target website https://github.com/laramies/metagoofil
99. TheHarvester - Gather emails, names, URLs from different public sources https://github.com/laramies/theHarvester
100. Creepy - Geolocation OSINT tool to extract target location information from social media profiles https://www.geocreepy.com/

FOLLOW ME ON:
(click icon below)

YouTube

in

INSIDE CLOUD
AND SECURITY