



# UNIVERSITY SYSTEM OF GEORGIA

## *OPEN-SOURCE TOOLS: A USG IT HANDBOOK COMPANION GUIDE*

---

*VERSION 1.0*

10/27/2021

*PUBLIC*

Abstract: This guideline is classified as “Public” and was developed for internal use. The purpose of the guideline is to complement the *USG IT Handbook* by providing a National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) centered perspective concerning the mapping of open-source tools....



## TABLE OF CONTENTS

Revision & Sign-off.....	2
Table of Contents.....	3
Introduction .....	4
Identify.....	5
Protect.....	8
Detect.....	11
Respond .....	12
Recover .....	14

# INTRODUCTION

The purpose of the guideline is to complement the *USG IT Handbook* by providing a National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) centered perspective concerning the mapping of open-source tools as illustrated in **Figure 1**.

The University System of Georgia (USG) has chosen to align with NIST standards and guidelines in the development of their cybersecurity program. This is intentional as many federal regulations map to NIST. More specifically, the U.S. Department of Education (ED) has mandated that all institutions of higher education entities (IHE) are to demonstrate Gramm-Leach-Bliley Act (GLBA) compliance through the implementation of NIST SP 800-171 Rev1. Failure to demonstrate compliance can result in IHEs losing the ability to administer federal student financial aid. Moreover, the Southern Association of Colleges and Schools Commission on Colleges (SACSCOC) has decided that GLBA compliance is to be a determining factor in accreditation. Failure to demonstrate compliance here can result in the loss of accreditation.

Technology	Identify	Technology	Protect	Technology	Detect	Technology	Respond	Technology	Recover
Asset Management	Open Source AssetTiger ERNext GPI ITSM Indot Kuwalba Rajih ResourceSpace Snipe-IT OpenAudit	Access Control	Open Source Apache Syncope FreeIPA Gluu Keycloak MidPoint-Security OpenAM OpenZi OpenIAM Shibboleth Suffid WSO (setty) Server	SEIM	Open Source Apache ELK Apache Metron DAD Domain Stats Frog Server OSSEC OSIM Prelude OSS Qradar Threat Intelligence	Incident Response	Open Source Ciphon GRR Rapid Response ParDwi ReactiveZ REMnux CyberCPR Shuffle SIFT Workstation The Hive	Backup	Open Source Areca BackupPC Bacula Bares Clonezilla Duplicati UnBackup
	Code Analysis Scanners		Anti-Virus & Endpoint Protection		Cyber Threat Intelligence		Forensics		
Vulnerability Scanners	Flawfinder SonarLint SonaRQube VisualCodeGrepper VSSA AppTrana Arachni Golismero Grabber Grendel-Scan Nikto OWASP Dependency-Check Ride Sec-Helpers Vegs w3af Wapiti Webcookies Wiko ZAP	API Management	API Management SICarie API Umbrella APIMAN DreamFactory Fusio Gravitee Kong Tik WSO2 API Manager	Cyber Threat Hunting	DeepBlueCLI DNSpooft fiare Hunting Maturity Model Labrea.py Log Campaign Misc Powershell & VBScript PAE Updates-Vbs VisualSniff VulnWhisperer WhatsMyName	Awesome-Malware-Analysis Autora IR Autopsy Awesome-Malware-Analysis b3st1ng chrome_parse.py decwindbx DEFT Zero DIPS docker_mount.py dpapilib ESE Analyst EyeCmd EZ Tools EZViewer GA-Cooler-Cruncher GA-Parser.py Get-ZimmermanTools Hidder hotoloti iisGeolocate ios_fpu_image iJCmd Jumplist Explorer KAPE kobaltusdec LECmd mac_robber.py MacOSRU Malice MFTCmd MFTExplorer onion_greeter.py parse_mftdump.py PECmd quidnoui_parser RBCmd			
	OWASP Dependency-Check Ride Sec-Helpers Vegs w3af Wapiti Webcookies Wiko ZAP	Awareness & Training	Deception	Forensics					
Vulnerability Scanners	Acheron ada-python Asleep Autocrack Blifit Bluecrypt BTFind CONPATRY CraclMapDec Cryptbreaker DHCPShoek Diggon Disruptive DynaStalker EAP-MDS-Crack EAPMD5Pass Emergence EmuRoot evbResourceIDGaps Gcat	Certificate Management	Certificate Management EJBCA OpenCA MYDLP OpenDLP	Deception	Connie DOEPT DejaVu Dionaea ElasticHoney HoneyDrive HoneyNet MongoDB HomeProxy OWASP HoneyPot	Forensics			
	OWASP Dependency-Check Ride Sec-Helpers Vegs w3af Wapiti Webcookies Wiko ZAP	Data Loss Prevention	DDoS Protection	Deception	Forensics				
Vulnerability Scanners	Acheron ada-python Asleep Autocrack Blifit Bluecrypt BTFind CONPATRY CraclMapDec Cryptbreaker DHCPShoek Diggon Disruptive DynaStalker EAP-MDS-Crack EAPMD5Pass Emergence EmuRoot evbResourceIDGaps Gcat	Encryption	Encryption AESCrypt InoCrypt BoxCryptor CipherShed Cryptomator DiskCryptor ProtonMail VeraCrypt	Deception	Connie DOEPT DejaVu Dionaea ElasticHoney HoneyDrive HoneyNet MongoDB HomeProxy OWASP HoneyPot	Forensics			
	OWASP Dependency-Check Ride Sec-Helpers Vegs w3af Wapiti Webcookies Wiko ZAP	Firewall	Firewall Untangle NG Firewall OPNsense	Deception	Forensics				

Figure 1: CSF View of Open-Source Tools

Each section in the document maps to a corresponding section within the CSF from Identify to Recover. Additionally, each section is color-coded to also correspond with the CSF. Each section has three columns of information beginning with Technology Type, followed by Tool Name, and ending on URL.

**Disclaimer:** As will all open-source options, the implementation of the tool comes with risks. These tools are often provided “as-is” with no guarantee, they often come with limited support (e.g., patching), and they often require significant expertise or experience to implement. Other considerations are the implementations are almost always on-premises applications, which simply means there will need to be capital expense that will need to be considered.

As with all of our documents, they are dynamic and considered works in progress. If you discover an error or have an additional tool that the community would benefit from mapping, please submit your comment to [cybersecurity@usg.edu](mailto:cybersecurity@usg.edu) for correction or consideration.

## IDENTIFY

Technology Type	Tool Name	URL
Asset Management	AssetTiger	<a href="https://www.myassettag.com/assettiger">https://www.myassettag.com/assettiger</a>
	ERPNext	<a href="https://erpnext.com/">https://erpnext.com/</a>
	GLPI ITSM	<a href="https://glpi-project.org/">https://glpi-project.org/</a>
	I-doit	<a href="https://www.i-doit.org/">https://www.i-doit.org/</a>
	Kuwaiba	<a href="https://www.kuwaiba.org/">https://www.kuwaiba.org/</a>
	Ralph	<a href="https://ralph-ng.readthedocs.io/en/stable/">https://ralph-ng.readthedocs.io/en/stable/</a>
	ResourceSpace	<a href="https://www.resourcespace.com/">https://www.resourcespace.com/</a>
	Snipe-IT	<a href="https://snipeitapp.com/">https://snipeitapp.com/</a>
	Open-Audit	<a href="https://www.open-audit.org/">https://www.open-audit.org/</a>
Code Analysis Scanners	Flawfinder	<a href="https://dwheeler.com/flawfinder/">https://dwheeler.com/flawfinder/</a>
	SonarLint	<a href="https://www.sonarlint.org/">https://www.sonarlint.org/</a>
	SonarQube	<a href="https://www.sonarqube.org/">https://www.sonarqube.org/</a>
	VisualCodeGrepper	<a href="https://sourceforge.net/projects/visualcodegrepp/">https://sourceforge.net/projects/visualcodegrepp/</a>
	YASCA	<a href="https://sourceforge.net/projects/yasca/">https://sourceforge.net/projects/yasca/</a>
Vulnerability Scanners	AppTrana	<a href="https://www.indusface.com/web-application-scanning.php">https://www.indusface.com/web-application-scanning.php</a>
	Arachni	<a href="http://www.arachni-scanner.com/">http://www.arachni-scanner.com/</a>
	Golismo	<a href="http://www.golismo.com/">http://www.golismo.com/</a>
	Grabber	<a href="http://rgaucher.info/beta/grabber/">http://rgaucher.info/beta/grabber/</a>
	Grendel-Scan	<a href="https://sourceforge.net/projects/grendel/">https://sourceforge.net/projects/grendel/</a>
	Nikto	<a href="http://www.cirt.net/nikto2">http://www.cirt.net/nikto2</a>
	OWASP Dependency-Check	<a href="https://owasp.org/www-project-dependency-check/">https://owasp.org/www-project-dependency-check/</a>
	Ride	<a href="https://github.com/adobe/ride/blob/develop/Usage.md#the-fuzz">https://github.com/adobe/ride/blob/develop/Usage.md#the-fuzz</a>
	Sec-Helpers	<a href="https://pypi.org/project/sec-helpers/">https://pypi.org/project/sec-helpers/</a>
	Vega	<a href="https://subgraph.com/vega/">https://subgraph.com/vega/</a>
	w3af	<a href="http://www.w3af.org/">http://www.w3af.org/</a>
	Wapiti	<a href="https://wapiti.sourceforge.io/">https://wapiti.sourceforge.io/</a>
	Webcookies	<a href="https://webcookies.org/">https://webcookies.org/</a>
	Wikto	<a href="https://www.sensepost.com/research/wikto/">https://www.sensepost.com/research/wikto/</a>
ZAP	<a href="https://zapproxy.org/">https://zapproxy.org/</a>	
Penetration Testing	Acheron	<a href="https://github.com/Acheron-VAF/Acheron">https://github.com/Acheron-VAF/Acheron</a>
	ads-payload	<a href="https://github.com/ChrisAD/ads-payload">https://github.com/ChrisAD/ads-payload</a>
	Asleep	<a href="https://github.com/joswr1ght/asleep">https://github.com/joswr1ght/asleep</a>
	Autocrack	<a href="https://github.com/timbo05sec/autocrack">https://github.com/timbo05sec/autocrack</a>
	BitFit	<a href="https://github.com/joswr1ght/bitfit">https://github.com/joswr1ght/bitfit</a>
	Bluecrypt	<a href="https://www.willhackforsushi.com/?page_id=61">https://www.willhackforsushi.com/?page_id=61</a>
	BTFind	<a href="https://github.com/joswr1ght/btfind">https://github.com/joswr1ght/btfind</a>
	CoWPAtty	<a href="https://github.com/joswr1ght/cowpatty">https://github.com/joswr1ght/cowpatty</a>
	CrackMapExec	<a href="https://github.com/byt3bl33d3r/CrackMapExec">https://github.com/byt3bl33d3r/CrackMapExec</a>
	Cryptbreaker	<a href="https://www.opensecurity.io/blog/quick-password-cracks-and-audits">https://www.opensecurity.io/blog/quick-password-cracks-and-audits</a>

DHCPShock	<a href="https://github.com/byt3bl33d3r/DHCPShock">https://github.com/byt3bl33d3r/DHCPShock</a>
Diagon	<a href="https://github.com/Project-Prismatica/Diagon">https://github.com/Project-Prismatica/Diagon</a>
Digestive	<a href="https://github.com/eric-conrad/digestive">https://github.com/eric-conrad/digestive</a>
DynaPstalker	<a href="https://github.com/joswr1ght/dynapstalker">https://github.com/joswr1ght/dynapstalker</a>
EAP-MD5-Crack	<a href="https://github.com/MarkBaggett/MarkBaggett/blob/master/eapmd5crack.py">https://github.com/MarkBaggett/MarkBaggett/blob/master/eapmd5crack.py</a>
EAPMD5Pass	<a href="https://github.com/joswr1ght/eapmd5pass">https://github.com/joswr1ght/eapmd5pass</a>
Emergence	<a href="https://github.com/Project-Prismatica/Emergence">https://github.com/Project-Prismatica/Emergence</a>
EmuRoot	<a href="https://github.com/airbus-seclab/android_emuroot">https://github.com/airbus-seclab/android_emuroot</a>
evtxResourceIDGaps	<a href="https://gist.github.com/joswr1ght/3d6b18b2150bd3ce1dd10d00ca2029b0">https://gist.github.com/joswr1ght/3d6b18b2150bd3ce1dd10d00ca2029b0</a>
GCat	<a href="https://github.com/byt3bl33d3r/gcat">https://github.com/byt3bl33d3r/gcat</a>
Gryffindor	<a href="https://github.com/Project-Prismatica/Diagon">https://github.com/Project-Prismatica/Diagon</a>
heimdall	<a href="https://gitlab.com/r00k/heimdall">https://gitlab.com/r00k/heimdall</a>
John the Ripper	<a href="https://www.openwall.com/john/">https://www.openwall.com/john/</a>
Kali	<a href="https://www.kali.org/">https://www.kali.org/</a>
Kerberoasting	<a href="https://github.com/nidem/kerberoast">https://github.com/nidem/kerberoast</a>
KillerBee	<a href="https://github.com/riverloopsec/killerbee">https://github.com/riverloopsec/killerbee</a>
KillerZee	<a href="https://github.com/joswr1ght/killerzee">https://github.com/joswr1ght/killerzee</a>
Mailsniper for Gmail	<a href="https://github.com/Osm0s1z/MailSniper">https://github.com/Osm0s1z/MailSniper</a>
Metasploit	<a href="https://www.metasploit.com/">https://www.metasploit.com/</a>
MFSmartHack	<a href="https://github.com/joswr1ght/mfsmarthack">https://github.com/joswr1ght/mfsmarthack</a>
MITMf	<a href="https://github.com/byt3bl33d3r/MITMf">https://github.com/byt3bl33d3r/MITMf</a>
NM2LP	<a href="https://github.com/joswr1ght/nm2lp">https://github.com/joswr1ght/nm2lp</a>
Oculus	<a href="https://github.com/Project-Prismatica/Oculus">https://github.com/Project-Prismatica/Oculus</a>
OffensiveDLR	<a href="https://github.com/byt3bl33d3r/OffensiveDLR">https://github.com/byt3bl33d3r/OffensiveDLR</a>
OWASP Zap	<a href="https://www.zaproxy.org/">https://www.zaproxy.org/</a>
Pause-Process	<a href="https://github.com/besimorhino/Pause-Process">https://github.com/besimorhino/Pause-Process</a>
PCAPHistogram	<a href="https://github.com/joswr1ght/pcaphistogram">https://github.com/joswr1ght/pcaphistogram</a>
PlistSubtractor	<a href="https://github.com/joswr1ght/plistsubtractor">https://github.com/joswr1ght/plistsubtractor</a>
powercat	<a href="https://github.com/besimorhino/powercat">https://github.com/besimorhino/powercat</a>
PPTXIndex	<a href="https://github.com/joswr1ght/pptxindex">https://github.com/joswr1ght/pptxindex</a>
PPTXSanity	<a href="https://github.com/joswr1ght/pptxsanity">https://github.com/joswr1ght/pptxsanity</a>
PPTXUrls	<a href="https://github.com/joswr1ght/pptxurls">https://github.com/joswr1ght/pptxurls</a>
Prismatica	<a href="http://prismatica.io/">http://prismatica.io/</a>
Red Baron	<a href="https://github.com/byt3bl33d3r/Red-Baron">https://github.com/byt3bl33d3r/Red-Baron</a>
SILENTRINITY	<a href="https://github.com/byt3bl33d3r/SILENTRINITY">https://github.com/byt3bl33d3r/SILENTRINITY</a>
Slingshot	<a href="https://www.sans.org/slingshot-vmware-linux">https://www.sans.org/slingshot-vmware-linux</a>
SprayingToolkit	<a href="https://github.com/byt3bl33d3r/SprayingToolkit">https://github.com/byt3bl33d3r/SprayingToolkit</a>
Subterfuge	<a href="https://github.com/Subterfuge-Framework">https://github.com/Subterfuge-Framework</a>
The C2 Matrix	<a href="https://www.thec2matrix.com/">https://www.thec2matrix.com/</a>
Tiberium	<a href="https://github.com/Osm0s1z/Tiberium">https://github.com/Osm0s1z/Tiberium</a>
TIBTLE2Pcap	<a href="https://github.com/joswr1ght/tibtlet2pcap">https://github.com/joswr1ght/tibtlet2pcap</a>

	VoIP Hopper Voltaire W3af Wapiti Wfuzz wiki-dictionary-creator WitnessMe	<a href="https://github.com/iknowjason/voiphopper">https://github.com/iknowjason/voiphopper</a> <a href="https://voltaire.publickey.io/">https://voltaire.publickey.io/</a> <a href="http://w3af.org/">http://w3af.org/</a> <a href="https://wapiti.sourceforge.io/">https://wapiti.sourceforge.io/</a> <a href="https://tools.kali.org/web-applications/wfuzz">https://tools.kali.org/web-applications/wfuzz</a> <a href="https://github.com/ChrisAD/wiki-dictionary-creator">https://github.com/ChrisAD/wiki-dictionary-creator</a> <a href="https://github.com/byt3bl33d3r/WitnessMe">https://github.com/byt3bl33d3r/WitnessMe</a>
Risk Assessment	Eramba Grabber Nikto2 OpenVAS SimpleRisk Vega	<a href="https://www.eramba.org/">https://www.eramba.org/</a> <a href="https://tools.kali.org/web-applications/grabber">https://tools.kali.org/web-applications/grabber</a> <a href="https://cirt.net/Nikto2">https://cirt.net/Nikto2</a> <a href="https://www.openvas.org/">https://www.openvas.org/</a> <a href="https://www.simplerisk.com/">https://www.simplerisk.com/</a> <a href="https://subgraph.com/vega/">https://subgraph.com/vega/</a>

## PROTECT

Technology Type	Tool Name	URL
Access Control	Apache Syncope	<a href="https://syncope.apache.org/">https://syncope.apache.org/</a>
	FreeIPA	<a href="https://www.freeipa.org/page/FreeIPAv2:Access_Control">https://www.freeipa.org/page/FreeIPAv2:Access_Control</a>
	Gluu	<a href="https://www.gluu.org/">https://www.gluu.org/</a>
	Keycloak	<a href="https://www.keycloak.org/">https://www.keycloak.org/</a>
	MidPoint-Security	<a href="https://www.midpoint-security.com/">https://www.midpoint-security.com/</a>
	OpenAM	<a href="https://github.com/OpenIdentityPlatform/OpenAM">https://github.com/OpenIdentityPlatform/OpenAM</a>
	OpenDJ	<a href="https://github.com/OpenIdentityPlatform/OpenDJ">https://github.com/OpenIdentityPlatform/OpenDJ</a>
	OpenIAM	<a href="https://www.openiam.com/products/access-manager/">https://www.openiam.com/products/access-manager/</a>
	Shibboleth	<a href="https://www.shibboleth.net/">https://www.shibboleth.net/</a>
	Soffid	<a href="https://www.soffid.com/soffid/">https://www.soffid.com/soffid/</a>
WSO Identity Server	<a href="https://wso2.com/identity-and-access-management/">https://wso2.com/identity-and-access-management/</a>	
Anti-Virus & Endpoint Protection	Armadito	<a href="https://www.armadito.com/">https://www.armadito.com/</a>
	Bullguard	<a href="https://www.bullguard.com/products/bullguard-antivirus.aspx">https://www.bullguard.com/products/bullguard-antivirus.aspx</a>
	ClamAV	<a href="https://www.clamav.net/">https://www.clamav.net/</a>
	ClamWin	<a href="http://www.clamwin.com/">http://www.clamwin.com/</a>
	Moon Secure AV	<a href="https://sourceforge.net/projects/moonav/">https://sourceforge.net/projects/moonav/</a>
API Management	3Scale	<a href="https://www.3scale.net/">https://www.3scale.net/</a>
	API Umbrella	<a href="https://apiumbrella.io/">https://apiumbrella.io/</a>
	APIMAN	<a href="https://www.apiman.io/latest/">https://www.apiman.io/latest/</a>
	DreamFactory	<a href="https://www.dreamfactory.com/">https://www.dreamfactory.com/</a>
	Fusio	<a href="https://www.fusio-project.org/">https://www.fusio-project.org/</a>
	Gravitee	<a href="https://www.gravitee.io/">https://www.gravitee.io/</a>
	Kong	<a href="https://konghq.com/">https://konghq.com/</a>
	Tyk	<a href="https://tyk.io/">https://tyk.io/</a>
	WSO2 API Manager	<a href="https://wso2.com/api-management/">https://wso2.com/api-management/</a>
Awareness & Training	Gophish	<a href="https://getgophish.com/">https://getgophish.com/</a>
	King Phisher	<a href="https://github.com/rsmusllp/king-phisher">https://github.com/rsmusllp/king-phisher</a>
	Phishing Frenzy	<a href="https://www.phishingfrenzy.com/">https://www.phishingfrenzy.com/</a>
Certificate Management	Dogtag PKI	<a href="https://www.dogtagpki.org/wiki/PKI_Main_Page">https://www.dogtagpki.org/wiki/PKI_Main_Page</a>
	EJBCA	<a href="https://www.ejbca.org/">https://www.ejbca.org/</a>
	OpenCA	<a href="https://www.openca.org/">https://www.openca.org/</a>
Data Loss Prevention	MyDLP	<a href="https://mydlp.com/">https://mydlp.com/</a>
	OpenDLP	<a href="https://github.com/ezarko/opendlp">https://github.com/ezarko/opendlp</a>
DDOS Protection	DDOS Deflate	<a href="https://github.com/jgmdev/ddos-deflate">https://github.com/jgmdev/ddos-deflate</a>
	Gatekeeper	<a href="https://github.com/AltraMayor/gatekeeper">https://github.com/AltraMayor/gatekeeper</a>
	Roboo	<a href="https://github.com/yuri-gushin/Roboo">https://github.com/yuri-gushin/Roboo</a>
Encryption	AESCrypt	<a href="https://www.aescrypt.com/">https://www.aescrypt.com/</a>
	AxCrypt	<a href="https://axcrypt.net/">https://axcrypt.net/</a>



	<p>BoxCryptor  Ciphershed  Cryptomator  DiskCryptor  ProtonMail  VeraCrypt</p>	<p><a href="https://www.boxcryptor.com/en/">https://www.boxcryptor.com/en/</a>  <a href="https://www.ciphershed.org/">https://www.ciphershed.org/</a>  <a href="https://cryptomator.org/">https://cryptomator.org/</a>  <a href="https://sourceforge.net/projects/diskcryptor/">https://sourceforge.net/projects/diskcryptor/</a>  <a href="https://protonmail.com/">https://protonmail.com/</a>  <a href="https://www.veracrypt.fr/code/VeraCrypt/">https://www.veracrypt.fr/code/VeraCrypt/</a></p>
Firewall	<p>ClearOS  Endian  IPFire  Untangle NG Firewall  OPNsense  pfSense  Shorewall  Smoothwall  VyOS</p>	<p><a href="https://www.clearos.com/marketplace/network/Firewall">https://www.clearos.com/marketplace/network/Firewall</a>  <a href="https://www.endian.com/">https://www.endian.com/</a>  <a href="https://www.ipfire.org/">https://www.ipfire.org/</a>  <a href="https://www.untangle.com/untangle-ng-firewall/">https://www.untangle.com/untangle-ng-firewall/</a>  <a href="https://opnsense.org/">https://opnsense.org/</a>  <a href="https://www.pfsense.org/">https://www.pfsense.org/</a>  <a href="https://shorewall.org/">https://shorewall.org/</a>  <a href="https://www.smoothwall.com/">https://www.smoothwall.com/</a>  <a href="https://docs.vyos.io/en/latest/firewall.html">https://docs.vyos.io/en/latest/firewall.html</a></p>
IDS/IPS	<p>OpenWIPS  OSSEC  Snort  Suricata  Zeek (BRO)</p>	<p><a href="https://openwips-ng.org/">https://openwips-ng.org/</a>  <a href="https://www.ossec.net/">https://www.ossec.net/</a>  <a href="https://www.snort.org/">https://www.snort.org/</a>  <a href="https://suricata-ids.org/">https://suricata-ids.org/</a>  <a href="https://zeek.org/">https://zeek.org/</a></p>
Secrets Management	<p>Confidant  Conjur  HashiCorp Vault  Kbsecret  Keywhiz</p>	<p><a href="https://lyft.github.io/confidant/">https://lyft.github.io/confidant/</a>  <a href="https://www.conjur.org/">https://www.conjur.org/</a>  <a href="https://www.hashicorp.com/products/vault">https://www.hashicorp.com/products/vault</a>  <a href="https://kbsecret.github.io/#/intro/">https://kbsecret.github.io/#/intro/</a>  <a href="https://square.github.io/keywhiz/">https://square.github.io/keywhiz/</a></p>
Mail Protection	<p>MailCleaner  MailScanner  OrangeAssassin  Proxmox  ScrolloutF1</p>	<p><a href="https://www.mailcleaner.net/">https://www.mailcleaner.net/</a>  <a href="https://www.mailscanner.info/">https://www.mailscanner.info/</a>  <a href="https://github.com/SpamExperts/OrangeAssassin">https://github.com/SpamExperts/OrangeAssassin</a>  <a href="https://www.proxmox.com/en/proxmox-mail-gateway">https://www.proxmox.com/en/proxmox-mail-gateway</a>  <a href="http://www.scrolloutf1.com/">http://www.scrolloutf1.com/</a></p>
MFA	<p>FreeOTP  LinOTP  MultiOTP  PrivacyIDEA</p>	<p><a href="https://freeotp.github.io/">https://freeotp.github.io/</a>  <a href="https://www.linotp.org/">https://www.linotp.org/</a>  <a href="https://github.com/multiOTP/multiotp/wiki">https://github.com/multiOTP/multiotp/wiki</a>  <a href="https://www.privacyidea.org/">https://www.privacyidea.org/</a></p>
Network Access Control	<p>FreeNAC  openNAC  PacketFence</p>	<p><a href="https://github.com/Boran/freenac">https://github.com/Boran/freenac</a>  <a href="http://opennac.org/opennac/en.html">http://opennac.org/opennac/en.html</a>  <a href="https://packetfence.org/">https://packetfence.org/</a></p>
Sandbox	<p>Cuckoo Sandbox  Sandboxie</p>	<p><a href="https://cuckoosandbox.org/">https://cuckoosandbox.org/</a>  <a href="https://www.sandboxie.com/">https://www.sandboxie.com/</a></p>
VPN	<p>Algo  Freelan</p>	<p><a href="https://github.com/trailofbits/algo">https://github.com/trailofbits/algo</a>  <a href="https://www.freelan.org/">https://www.freelan.org/</a></p>

	OpenVPN Outline VPN Pritunl SoftEther Streisand StrongSwan WireGuard	<a href="https://openvpn.net/">https://openvpn.net/</a> <a href="https://getoutline.org/en/home">https://getoutline.org/en/home</a> <a href="https://pritunl.com/">https://pritunl.com/</a> <a href="https://www.softether.org/">https://www.softether.org/</a> <a href="https://github.com/StreisandEffect/streisand">https://github.com/StreisandEffect/streisand</a> <a href="https://www.strongswan.org/">https://www.strongswan.org/</a> <a href="https://www.wireguard.com/">https://www.wireguard.com/</a>
WAF	IronBee ModSecurity NAXSI Raptor Shadow Daemon Vulture WebKnight	<a href="https://sourceforge.net/projects/ironbee/">https://sourceforge.net/projects/ironbee/</a> <a href="https://modsecurity.org/">https://modsecurity.org/</a> <a href="https://github.com/nbs-system/naxsi">https://github.com/nbs-system/naxsi</a> <a href="https://securityonline.info/raptor-waf-web-application-firewall/">https://securityonline.info/raptor-waf-web-application-firewall/</a> <a href="https://shadowd.zecure.org/overview/introduction/">https://shadowd.zecure.org/overview/introduction/</a> <a href="https://www.vultureproject.org/">https://www.vultureproject.org/</a> <a href="https://www.aqtronix.com/?PageID=99">https://www.aqtronix.com/?PageID=99</a>
Web/URL Filtering	E2Guardian GoGuardian MitmProxy ufdbGuard	<a href="http://e2guardian.org/cms/index.php">http://e2guardian.org/cms/index.php</a> <a href="https://www.goguardian.com/">https://www.goguardian.com/</a> <a href="https://mitmproxy.org/">https://mitmproxy.org/</a> <a href="https://www.urlfilterdb.com/products/ufdbguard.html">https://www.urlfilterdb.com/products/ufdbguard.html</a>

## DETECT

Technology Type	Tool Name	URL
SEIM	Apache ELK	<a href="https://www.elastic.co/what-is/elk-stack">https://www.elastic.co/what-is/elk-stack</a>
	Apache Metron	<a href="https://metron.apache.org/">https://metron.apache.org/</a>
	DAD	<a href="https://github.com/dhoelzer/DAD">https://github.com/dhoelzer/DAD</a>
	Domain Stats	<a href="http://github.com/markbaggett/domainstats">http://github.com/markbaggett/domainstats</a>
	Freq Server	<a href="http://github.com/markbaggett/freq">http://github.com/markbaggett/freq</a>
	OSSEC	<a href="https://www.ossec.net/">https://www.ossec.net/</a>
	OSSIM	<a href="https://sourceforge.net/projects/os-sim/">https://sourceforge.net/projects/os-sim/</a>
	Prelude OSS	<a href="https://www.prelude-siem.org/">https://www.prelude-siem.org/</a>
	Qradar Threat Intelligence	<a href="https://github.com/SecurityNik/QRadar---Threat-Intelligence-On-The-Cheap">https://github.com/SecurityNik/QRadar---Threat-Intelligence-On-The-Cheap</a>
	SecurityOnion	<a href="https://securityonion.net/">https://securityonion.net/</a>
	ShowMeThePackets	<a href="https://github.com/dhoelzer/ShowMeThePackets">https://github.com/dhoelzer/ShowMeThePackets</a>
SIEMonster	<a href="https://siemonster.com/">https://siemonster.com/</a>	
Cyber Threat Intelligence	Espial	<a href="https://www.spydersec.com/Espial">https://www.spydersec.com/Espial</a>
	The Pyramid of Pain	<a href="https://bit.ly/PyramidOfPain">https://bit.ly/PyramidOfPain</a>
	untappdScraper	<a href="https://github.com/WebBreacher/untappdScraper">https://github.com/WebBreacher/untappdScraper</a>
Cyber Threat Hunting	DeepBlueCLI	<a href="https://github.com/sans-blue-team/DeepBlueCLI">https://github.com/sans-blue-team/DeepBlueCLI</a> <a href="https://drive.google.com/file/d/0B0qDfJ30s2I9bXVwX3VXNzBOMzA/edit">https://drive.google.com/file/d/0B0qDfJ30s2I9bXVwX3VXNzBOMzA/edit</a>
	DNSSpooF	
	flare	<a href="https://github.com/HASecuritySolutions/flare">https://github.com/HASecuritySolutions/flare</a>
	Hunting Maturity Model	<a href="https://bit.ly/HuntingMaturityModel">https://bit.ly/HuntingMaturityModel</a>
	LaBrea.py	<a href="https://github.com/dhoelzer/ShowMeThePackets/blob/master/Scapy/LaBrea.py">https://github.com/dhoelzer/ShowMeThePackets/blob/master/Scapy/LaBrea.py</a>
	Log Campaign	<a href="https://github.com/HASecuritySolutions/LogCampaign">https://github.com/HASecuritySolutions/LogCampaign</a>
	Misc Powershell & VBScript	<a href="https://github.com/EnclaveConsulting">https://github.com/EnclaveConsulting</a>
	PAE	<a href="https://github.com/dhoelzer/ShowMeThePackets/tree/master/PAE">https://github.com/dhoelzer/ShowMeThePackets/tree/master/PAE</a>
	Update-VMs	<a href="https://github.com/HASecuritySolutions/Update-VMs">https://github.com/HASecuritySolutions/Update-VMs</a>
	VisualSniff	<a href="https://github.com/dhoelzer/VisualSniff">https://github.com/dhoelzer/VisualSniff</a>
	VulnWhisperer	<a href="https://github.com/HASecuritySolutions/VulnWhisperer">https://github.com/HASecuritySolutions/VulnWhisperer</a>
WhatsMy Name	<a href="https://github.com/WebBreacher/WhatsMyName">https://github.com/WebBreacher/WhatsMyName</a>	
Deception	Cowrie	<a href="https://github.com/cowrie/cowrie">https://github.com/cowrie/cowrie</a>
	DCEPT	<a href="https://github.com/secureworks/dcept">https://github.com/secureworks/dcept</a>
	DejaVu	<a href="https://github.com/bhdresh/Dejavu">https://github.com/bhdresh/Dejavu</a>
	Dionaea	<a href="https://github.com/DinoTools/dionaea">https://github.com/DinoTools/dionaea</a>
	ElasticHoney	<a href="https://github.com/jordan-wright/elastic_honey">https://github.com/jordan-wright/elastic_honey</a>
	HoneyDrive	<a href="https://sourceforge.net/projects/honeydrive/">https://sourceforge.net/projects/honeydrive/</a>
	Honeynet	<a href="https://www.honeynet.org/">https://www.honeynet.org/</a>
	MongoDB HoneyProxy	<a href="https://github.com/Plazmaz/MongoDB-HoneyProxy">https://github.com/Plazmaz/MongoDB-HoneyProxy</a>
	OWASP HoneyPot	<a href="https://owasp.org/www-project-honeypot/">https://owasp.org/www-project-honeypot/</a>

## RESPOND

Technology Type	Tool Name	URL
Incident Response	Cyphon	<a href="https://www.cyphon.io/">https://www.cyphon.io/</a>
	GRR Rapid Response	<a href="https://grr-doc.readthedocs.io/en/latest/">https://grr-doc.readthedocs.io/en/latest/</a>
	PatrOwl	<a href="https://www.patrowl.io/home">https://www.patrowl.io/home</a>
	Rastrea2r	<a href="https://github.com/rastrea2r/rastrea2r">https://github.com/rastrea2r/rastrea2r</a>
	REMnux	<a href="https://remnux.org/">https://remnux.org/</a>
	CyberCPR	<a href="https://www.cybercpr.com/">https://www.cybercpr.com/</a>
	Shuffle	<a href="https://shuffler.io/">https://shuffler.io/</a>
	SIFT Workstation	<a href="https://digital-forensics.sans.org/community/downloads">https://digital-forensics.sans.org/community/downloads</a>
	The Hive	<a href="https://thehive-project.org/">https://thehive-project.org/</a>
Forensics	AmcacheParser	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/AmcacheParser.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/AmcacheParser.zip</a>
	analyzeEXT	<a href="file:///C:/Users/kmarshall/Documents/Curriculum%20Overall/Free/github.com/halpomeranz">file:///C:/Users/kmarshall/Documents/Curriculum Overall/Free/github.com/halpomeranz</a>
	APOLLO	<a href="https://github.com/mac4n6/APOLLO">https://github.com/mac4n6/APOLLO</a>
	AppCompatCacheParser	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/AppCompatCacheParser.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/AppCompatCacheParser.zip</a>
	Aurora IR	<a href="https://www.cyberfox.blog/aurora-incident-response/">https://www.cyberfox.blog/aurora-incident-response/</a>
	Autopsy	<a href="https://www.autopsy.com/">https://www.autopsy.com/</a>
	Awesome-Malware-Analysis	<a href="https://www.openhub.net/p/awesome-malware-analysis">https://www.openhub.net/p/awesome-malware-analysis</a>
	bstrings	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/bstrings.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/bstrings.zip</a>
	chrome_parse.py	<a href="https://github.com/mdegrazia/Chrome-Parse">https://github.com/mdegrazia/Chrome-Parse</a>
	decwindbx	<a href="https://github.com/dfirfpi/decwindbx">https://github.com/dfirfpi/decwindbx</a>
	DEFT Zero	<a href="https://distrowatch.com/table.php?distribution=deft">https://distrowatch.com/table.php?distribution=deft</a>
	DFIS	<a href="https://github.com/halpomeranz/dfis">https://github.com/halpomeranz/dfis</a>
	docker_mount.py	<a href="https://github.com/att/docker-forensics/blob/master/docker-mount.py">https://github.com/att/docker-forensics/blob/master/docker-mount.py</a>
	dpapilab	<a href="https://github.com/dfirfpi/dpapilab">https://github.com/dfirfpi/dpapilab</a>
	ESE Analyst	<a href="http://github.com/markbaggett/ese-analyst">http://github.com/markbaggett/ese-analyst</a>
	EvtxECmd	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/EvtxExplorer.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/EvtxExplorer.zip</a>
	EZ Tools	<a href="https://digital-forensics.sans.org/community/downloads/digital-forensics-tools">https://digital-forensics.sans.org/community/downloads/digital-forensics-tools</a>
	EZViewer	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/EZViewer.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/EZViewer.zip</a>
	GA Cooki Cruncher	<a href="https://github.com/mdegrazia/Google-Analytic-Cookie-Cruncher">https://github.com/mdegrazia/Google-Analytic-Cookie-Cruncher</a>
	GA-Parser.py	<a href="https://github.com/mdegrazia/Google-Analytic-Parser">https://github.com/mdegrazia/Google-Analytic-Parser</a>
	Get-ZimmermanTools	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/Get-ZimmermanTools.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/Get-ZimmermanTools.zip</a>
	Hasher	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/hasher.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/hasher.zip</a>
	hotoloti	<a href="https://github.com/RealityNet/hotoloti">https://github.com/RealityNet/hotoloti</a>
	iisGeoLocate	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/iisGeolocate.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/iisGeolocate.zip</a>
	ios_bfu_triage	<a href="https://github.com/RealityNet/ios_bfu_triage">https://github.com/RealityNet/ios_bfu_triage</a>
	JLECmd	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/JLECmd.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/JLECmd.zip</a>
	JumpList Explorer	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/JumpListExplorer.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/JumpListExplorer.zip</a> <a href="https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape">https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape</a>
KAPE	<a href="https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape">https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape</a>	
kobackupdec	<a href="https://github.com/RealityNet/kobackupdec">https://github.com/RealityNet/kobackupdec</a>	

	LECmd	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/LECmd.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/LECmd.zip</a>
	mac_robber.py	<a href="https://github.com/att/docker-forensics/blob/master/mac-robber.py">https://github.com/att/docker-forensics/blob/master/mac-robber.py</a>
	MacMRU	<a href="https://github.com/mac4n6/macMRU-Parser">https://github.com/mac4n6/macMRU-Parser</a>
	Malice	<a href="https://github.com/maliceio/malice">https://github.com/maliceio/malice</a>
	MFTECmd	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/MFTECmd.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/MFTECmd.zip</a>
	MFTEExplorer	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/MFTEExplorer.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/MFTEExplorer.zip</a>
	onion_peeler.py	<a href="https://github.com/mdegrazia/OnionPeeler">https://github.com/mdegrazia/OnionPeeler</a>
	parse_mftdump.py	<a href="https://github.com/mdegrazia/mft-parse">https://github.com/mdegrazia/mft-parse</a>
	PECmd	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/PECmd.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/PECmd.zip</a>
	quicklook_parser	<a href="https://github.com/mdegrazia/OSX-QuickLook-Parser">https://github.com/mdegrazia/OSX-QuickLook-Parser</a>
	RBCmd	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/RBCmd.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/RBCmd.zip</a>
	RecentFileCacheParser	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/RecentFileCacheParser.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/RecentFileCacheParser.zip</a>
	RECmd	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/RegistryExplorer_RECmd.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/RegistryExplorer_RECmd.zip</a>
	Registry Explorer	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/RegistryExplorer_RECmd.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/RegistryExplorer_RECmd.zip</a>
	safari_parser.py	<a href="https://github.com/mdegrazia/Safari-Internet-History-Parser">https://github.com/mdegrazia/Safari-Internet-History-Parser</a>
	SDB Explorer	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/SDBExplorer.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/SDBExplorer.zip</a>
	ShellBags Explorer	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/ShellBagsExplorer.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/ShellBagsExplorer.zip</a>
	sigs.py	<a href="https://github.com/clausing/scripts/blob/master/sigs.py">https://github.com/clausing/scripts/blob/master/sigs.py</a>
	SOF-ELK	<a href="https://github.com/philhagen/sof-elk">https://github.com/philhagen/sof-elk</a>
	sqlparse.py	<a href="https://github.com/mdegrazia/SQLite-Deleted-Records-Parser">https://github.com/mdegrazia/SQLite-Deleted-Records-Parser</a>
	SRUM-DUMP	<a href="http://github.com/markbaggett/srum-dump">http://github.com/markbaggett/srum-dump</a>
	thunderbird_parser.py	<a href="https://github.com/mdegrazia/Thunderbird-Email-Parser">https://github.com/mdegrazia/Thunderbird-Email-Parser</a>
	TimeApp	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/TimeApp.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/TimeApp.zip</a>
	Timeline Explorer	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/TimelineExplorer.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/TimelineExplorer.zip</a>
	tln_parse.py	<a href="https://github.com/clausing/scripts/blob/master/tln_parse.py">https://github.com/clausing/scripts/blob/master/tln_parse.py</a>
	unssz	<a href="https://gist.github.com/dfirfpi/2602b726af1b944efa723d34b624ad88">https://gist.github.com/dfirfpi/2602b726af1b944efa723d34b624ad88</a>
	VSCMount	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/VSCMount.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/VSCMount.zip</a>
	w10pfdecomp	<a href="https://gist.github.com/dfirfpi/113ff71274a97b489dfd">https://gist.github.com/dfirfpi/113ff71274a97b489dfd</a>
	Werejugo	<a href="http://github.com/markbaggett/werejugo">http://github.com/markbaggett/werejugo</a>
	WxTCmd	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/WxTCmd.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/WxTCmd.zip</a>
	XWFIM	<a href="https://f001.backblazeb2.com/file/EricZimmermanTools/XWFIM.zip">https://f001.backblazeb2.com/file/EricZimmermanTools/XWFIM.zip</a>

# RECOVER

Technology Type	Tool Name	URL
Backup	Areca	<a href="https://www.areca.com.tw/">https://www.areca.com.tw/</a>
	BackupPC	<a href="https://backuppc.github.io/backuppc/">https://backuppc.github.io/backuppc/</a>
	Bacula	<a href="https://www.bacula.org/">https://www.bacula.org/</a>
	Bareos	<a href="https://www.bareos.org/en/">https://www.bareos.org/en/</a>
	Clonezilla	<a href="https://clonezilla.org/">https://clonezilla.org/</a>
	Duplicati	<a href="https://www.duplicati.com/">https://www.duplicati.com/</a>
	Urbackup	<a href="https://www.urbackup.org/">https://www.urbackup.org/</a>