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….

REVISION & SIGN-OFF

Change Record

Date	Author	Version	Change Reference

Document Properties

Item	Details
Document Title	OPEN-SOURCE Tools: A USG IT Handbook Companion Guide
Document Type	Guideline (Internal Use Only)
Author	Alfred Barker
Document Manager	Alfred Barker
Creation Date	10/27/2021
Last Updated	10/29/2021
Document Classification	Public

TABLE OF CONTENTS

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.

Indentify		Protect		Detect		Respond		Recover	
Technology	Open Source	Technology	Open Source	Technology	Open Source	Technology	Open Source	Technology	Open Source
Asset Management	AssetTiger ERPNext GLPI ITSM i-doit Kuwaiba Ralph ResourceSpace Snipe-IT Open-AudIT	Access Control	Apache Syncope FreeIPA Gluu Keycloak MidPoint-Security OpenAM OpenDJ OpenIAM Shibboleth Soffid WSO Identity Server	SEIM	Apache ELK Apache Metron DAD Domain Stats Freq Server OSSEC OSSIM Prelude OSS Qradar Threat Intelligence SecurityOnion ShowMeThePackets SIEMonster	Incident Response	Cyphon GRR Rapid Response PatrOwl Rastrea2r REMnux CyberCPR Shuffle SIFT Workstation The Hive	Backup	Areca BackupPC Bacula Bareos Clonezilla Duplicati Urbackup
Code Analysis Scanners	Flawfinder SonarLint SonarQube VisualCodeGrepper YASCA	Anti-Virus & Endpoint Protection	Armadito Bullguard ClamAV ClamWin Moon Secure AV	Cyber Threat Intelligence	Espial The Pyramid of Pain untappdScraper	Forensics	AmcacheParser analyzeEXT APOLLO AppCompatCacheParser Aurora IR Autopsy Awesome-Malware-Analysis bstrings chrome_parse.py decwindbx DEFT Zero DFIS docker_mount.py dpapilab ESE Analyst EvtxECmd EZ Tools EZViewer GA Cooki Cruncher GA-Parser.py Get-ZimmermanTools Hasher hotoloti iisGeoLocate ios_bfu_triage JLECmd JumpList Explorer KAPE kobackupdec LECmd mac_robber.py MacMRU Mailce MFTECmd MFTExplorer onion_peeler.py parse_mftdump.py PECmd quicklook_parser RBCmd		
Vulnerability Scanners	AppTrana Arachni GoLismero Grabber Grendel-Scan Nikto OWASP Dependency-Check Ride Sec-Helpers Vega w3af Wapiti Webcookies Wikto ZAP	API Management	3Scale API Umbrella APIMAN DreamFactory Fusio Gravitee Kong Tyk WSO2 API Manager	Cyber Threat Hunting	DeepBlueCLI DNSSpoof flare Hunting Maturity Model LaBrea.py Log Campaign Misc Powershell & VBScript PAE Update-VMs VisualSniff VulnWhisperer WhatsMy Name				
	Acheron ads-payload Asleap Autocrack BitFit Bluecrypt BTFind CoWPAtty CrackMapExec Cryptbreaker DHCPShock Diagon Digestive DynaPstalker EAP-MD5-Crack EAPMD5Pass Emergence EmuRoot evtxResourceIDGaps GCat	Awareness & Training	Gophish King Phisher Phishing Frenzy	Deception	Cowrie DCEPT DejaVu Dionaea ElasticHoney HoneyDrive Honeynet MongoDB HoneyProxy OWASP Honeypot				
		Certificate Management	Dogtag PKI EJBCA OpenCA						
		Data Loss Prevention	MyDLP OpenDLP						
		DDOS Protection	DDOS Deflate Gatekeeper Roboo						
		Encryption	AESCrypt AxCrypt BoxCryptor CipherShed Cryptomator DiskCryptor ProtonMail VeraCrypt						
		Firewall	ClearOS Endian IPFire Untangle NG Firewall OPNsense						

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 for correction or consideration.

IDENTIFY

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

	DHCPShock	https://github.com/byt3bl33d3r/DHCPShock
	Diagon	https://github.com/Project-Prismatica/Diagon
	Digestive	https://github.com/eric-conrad/digestive
	DynaPstalker	https://github.com/joswr1ght/dynapstalker
	EAP-MD5-Crack	https://github.com/MarkBaggett/MarkBaggett/blob/master/eapmd5crack.py
	EAPMD5Pass	https://github.com/joswr1ght/eapmd5pass
	Emergence	https://github.com/Project-Prismatica/Emergence
	EmuRoot	https://github.com/airbus-seclab/android_emuroot
	evtxResourceIDGaps	https://gist.github.com/joswr1ght/3d6b18b2150bd3ce1dd10d00ca2029b0
	GCat	https://github.com/byt3bl33d3r/gcat
	Gryffindor	https://github.com/Project-Prismatica/Diagon
	heimdall	https://gitlab.com/r00k/heimdall
	John the Ripper	https://www.openwall.com/john/
	Kali	https://www.kali.org/
	Kerberoasting	https://github.com/nidem/kerberoast
	KillerBee	https://github.com/riverloopsec/killerbee
	KillerZee	https://github.com/joswr1ght/killerzee
	Mailsniper for Gmail	https://github.com/0sm0s1z/MailSniper
	Metasploit	https://www.metasploit.com/
	MFSmartHack	https://github.com/joswr1ght/mfsmarthack
	MITMf	https://github.com/byt3bl33d3r/MITMf
	NM2LP	https://github.com/joswr1ght/nm2lp
	Oculus	https://github.com/Project-Prismatica/Oculus
	OffensiveDLR	https://github.com/byt3bl33d3r/OffensiveDLR
	OWASP Zap	https://www.zaproxy.org/
	Pause-Process	https://github.com/besimorhino/Pause-Process
	PCAPHistogram	https://github.com/joswr1ght/pcaphistogram
	PlistSubtractor	https://github.com/joswr1ght/plistsubtractor
	powercat	https://github.com/besimorhino/powercat
	PPTXIndex	https://github.com/joswr1ght/pptxindex
	PPTXSanity	https://github.com/joswr1ght/pptxsanity
	PPTXUrls	https://github.com/joswr1ght/pptxurls
	Prismatica	http://prismatica.io/
	Red Baron	https://github.com/byt3bl33d3r/Red-Baron
	SILENTTRINITY	https://github.com/byt3bl33d3r/SILENTTRINITY
	Slingshot	https://www.sans.org/slingshot-vmware-linux
	SprayingToolkit	https://github.com/byt3bl33d3r/SprayingToolkit
	Subterfuge	https://github.com/Subterfuge-Framework
	The C2 Matrix	https://www.thec2matrix.com/
	Tiberium	https://github.com/0sm0s1z/Tiberium
	TIBTLE2Pcap	https://github.com/joswr1ght/tibtle2pcap

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

PROTECT

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

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

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

DETECT

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

RESPOND

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

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

RECOVER

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