			mu proferences mu untebliet mu centributione
	page discussion edit history de	elete move watch additional statistics	my preferences my watchlist my contributions
	TOP SECRET STRAP1 COMINT	elete move watch autitional statistics	
		It is TOD SEADET STRADI COMINT, Click to report incommu	ata aantant
	The maximum classification allowed on GCVVI	ki is TOP SECRET STRAP1 COMINT. Click to report inappropri-	ale content.
		For GCWiki help contact: Support page	
	JTRIG tools and techniqu	les	
	(Redirected from JTRIG CITD - Covert Internet Technic		
navigation			
Main Page			
Help Pages			
 Wikipedia Mirror 	Overview	ITRIC Conshilition	Contacts
Ask Me About	Overview	JTRIG Capabilities	Contacts
Random page			
Recent changes			· · · · · · · · · · · · · · · · · · ·
Report a Problem			
Contacts			
GCWeb			
search	[edit] JTRIG tools		
Go Search			
taalbay			
toolbox			
What links here	Contents		
 Related changes Upload file 	1 JTRIG tools		
 Special pages 	1.1 Understanding this page		
 Printable version 	1.2 Current Priorities		
 Permanent link 	1.2.1 Engineering		
	1.2.2 Collection		
[Powered By MediaWiki	1.2.3 Effects Capability		
	1.2.4 Work Flow Management		
This page was last	1.2 E Analysia Taala		
modified on 5 July 2012, at	1000-100		
-			
	1.2.9 Snaping and Honeypots		
		ne somewhat of a Chinese menu for effects operations. Informatio	
13:05. This page has been accessed 19,579 times. All material is UK	1.2.7 Forensic Exploitation 1.2.8 Techniques 1.2.9 Shaping and Honeypots		

[edit] Understanding this page

Tools and techniques are developed by various teams within JTRIG. We like to let people know when we have something that we can think we can use, but we also don't want to oversell our capability.

For this reason, each tool indicates its current status. We may put up experimental tools or ones that are still in development so you know what we are working on, and can approach JTRIG with any new ideas. But experimental tools by their nature will be unreliable, if you raise expectations or make external commitments before speaking to us you will probably end up looking stupid.

Most of our tools are fully operational, tested and reliable. We will indicate when this is the case; however there can be reasons why our tools won't work for some operational requirements (eg if it exploits a provider specific vulnerability). There may also be legal restrictions.

So please come and speak to JTRIG operational staff early in your operational planning process.

[edit] Current Priorities

Capability Development Priorities can be fond by following the link below

🔹 CapDev Priorities (Discover) 🔒

Tool/System	Description	Status	Contacts
Cerberus Statistics Collection	Collects on-going usage information about how many users utilise JTRIG's UIA capability, what sites are the most frequently visited etc. This is in order to provide JTRIG infrastucture and ITServices management information statistics.	OPERATIONAL	JTRIG Software Developers 🖃
ITRIG RADIANT SPLENDOUR	is a 'Data Diode' connecting the CERBERUS network with GCNET	OPERATIONAL	JTRIG Software Developers 🖃
ALLIUM ARCH	JTRIG UIA via the Tor network.	OPERATIONAL	JTRIG Infrastructure Team 💷
ASTRAL PROJECTION	Remote GSM secure covert internet proxy using TOR hidden services.	OPERATIONAL	JTRIG Infrastructure Team 🖃
TWILIGHT ARROW	Remote GSM secure covert internet proxy using VPN services.	OPERATIONAL	JTRIG Infrastructure Team 🖃
SPICE ISLAND	JTRIG's new Infrastructure. FOREST WARRIOR, FRUIT BOWL, JAZZ FUSION and other JTRIG systems will form part of the SPICE ISLAND infrastructure	DEV	JTRIG Infrastructure Team 🖃
POISON ARROW	Safe Malware download capability.	DESIGN	JTRIG Infrastructure Team 🖃
FRUIT BOWL	CERBERUS UIA Replacement and new tools infrastructure – Primary Domain for Generic User/Tools Access and TOR split into 3 sub- systems.	DESIGN	JTRIG Infrastructure Team 🖃
NUT ALLERGY	JTRIG Tor web browser - Sandbox IE replacement and FRUIT BOWL sub-system	PILOT	JTRIG Infrastructure Team 🖃
BERRY TWISTER	A sub-system of FRUIT BOWL	PILOT	JTRIG Infrastructure Team 🖃
BERRY TWISTER+	A sub-system of FRUIT BOWL	PILOT	JTRIG Infrastructure Team ⊡m]
BRANDY SNAP	JTRIG UIA contingency at Scarborough.	IMPLEMENTATION	JTRIG Infrastructure Team 💷
WIND FARM	R&D offsite facility.	DESIGN	JTRIG Infrastructure Team 💷
CERBERUS	JTRIG's legacy UIA desktop, soon to be replaced with FOREST WARRIOR.	OPERATIONAL	JTRIG Infrastructure Team 🖃
BOMBAYROLL	JTRIG's legacy UIA standalone capability.	OPERATIONAL	JTRIG Infrastructure Team 🖃
JAZZ FUSION	BOMBAY ROLL Replacement which will also incorporate new collectors – Primary Domain for Dedicated Connections split into 3 sub-systems.	IMPLEMENTATION	JTRIG Infrastructure Team 🖃
COUNTRY FILE	A sub-system of JAZZ FUSION	OPERATIONAL	JTRIG Infrastructure Team 🖃
TECHNO VIKING	A sub-system of JAZZ FUSION	DESIGN	JTRIG Infrastructure Team 🖃
JAZZ FUSION+	A sub-system of JAZZ FUSION	DESIGN	JTRIG Infrastructure Team 🖃
BUMBLEBEE Dance	JTRIG Operational VM/TOR architecture	OPERATIONAL	JTRIG Infrastructure Team 🖃
AIR BAG	JTRIG Laptop capability for field operations.	OPERATIONAL	JTRIG Infrastructure Team 💷
EXPOW	GCHQ's UIA capability provided by JTRIG.	OPERATIONAL	JTRIG Infrastructure Team 🖃
AXLE GREASE	The covert banking link for CPG	OPERATIONAL	JTRIG Infrastructure Team 🔤
POD RACE	JTRIG'S MS update farm	DESIGN	JTRIG Infrastructure Team 💷
NATCHTOWER	GCNET -> CERBERUS Export Gateway Interface System	OPERATIONAL	JTRIG Software Developers 🖃
REAPER	CERBERUS -> GCNET Import Gateway Interface System	OPERATIONAL	JTRIG Software Developers 🖃
DIALd FOREST	External Internet Redial and Monitor Daemon Desktop replacement for CERBERUS	OPERATIONAL DESIGN	JTRIG Software Developers ा JTRIG Infrastructure Team ा
WARRIOR		CLOIDIN	errae mittaducture ream
DOG HANDLER	JTRIG's development network	DESIGN	JTRIG Infrastructure Team 🔤
			JTRIG Infrastructure Team 💷

Tool	Description	Contacts	Status
AIRWOLF	YouTube profile, comment and video collection.		Beta release.
ANCESTRY	Tool for discovering the creation date of yahoo selectors.	JTRIG Software Developers ⊑ 1	Fully Operational.
BEARTRAP	Bulk retrieval of public BEBO profiles from member or group ID.	JTRIG Software Developers ≡ 1	Fully Operational.
BIRDSONG	Automated posting of Twitter updates.	JTRIG Software Developers ⊟1	Decomissioned Replaced by SYLVESTER.
BIRDSTRIKE	Twitter monitoring and profile collection. Click here for the User Guide.	JTRIG Software Developers 🖃	Fully Operational.
BUGSY	Google+ collection (circles, profiles etc.)	Tech Leads:	In early development.
DANCING BEAR	obtains the locations of WiFi access points.	[Tech Lead: Expert User:	Fully Operational.
DEVILS HANDSHAKE	ECI Data Technique.	[Tech Lead: Expert User:	Fully Operational.
DRAGON'S SNOUT	Paltalk group chat collection.	Tech Leads:	Beta release.
EXCALIBUR	acquires a Paltalk UID and/or email address from a Screen Name.	JTRIG Software Developers ⊑∎	Fully operational (against current Paltalk version)
FATYAK	Public data collection from LinkedIn.	[Tech Lead:	in development
FUSEWIRE	Provides 24/7 monitoring of Vbulliten forums for target postings/online activity. Also allows staggered postings to be made.	JTRIG Software Developers 🞫	
GLASSBACK	Technique of getting a targets IP address by pretending to be a spammer and ringing them. Target does not need to answer.	JTRIG Software Developers 🛋	Fully operational.
GODFATHER	Public data collection from Facebook.	[Tech Lead:	Fully operational.
GOODFELLA	Generic framework for public data collection from Online Social Networks.	[Tech Lead:	In Development (Supports RenRen and Xing).
HACIENDA	is a port scanning tool designed to scan an entire country or city. It uses GEOFUSION to identify IP locations. Banners and content are pulled back on certain ports. Content is put into the EARTHLING database, and all other scanned data is sent to GNE and is available through GLOBAL SURGE and Fleximart.	NAC HACIENDA Taskers ⊡	Fully operational.
ICE	is an advanced IP harvesting technique.	JTRIG Software Developers 💷	
NSPECTOR	Tool for monitoring domain information and site availability.	JTRIG Software Developers 💷	Fully Operational.
	Tool for auditing dissemination of VIKING PILLAGE data.	JTRIG Software Developers ⊡	Fully Operational.

MINIATURE HERO	Active skype capability. Provision of real time call records (SkypeOut and SkypetoSkype) and bidirectional instant messaging. Also contact lists.	JTRIG Software Developers ⊡	Fully operational, but note usage restrictions.
моитн	Tool for collection for downloading a user's files from Archive.org.	JTRIG Software Developers ⊡	Fully Operational.
MUSTANG	provides covert access to the locations of GSM cell towers.	[Tech Lead: Expert User:	Fully Operational.
PHOTON TORPEDO	A technique to actively grab the IP address of an MSN messenger user.	Tech Lead:	Operational, bu usage restrictions.
RESERVOIR	Facebook application allowing collection of various information.	JTRIG Software Developers ⊡	Fully operational, bu note operationa restrictions.
SEBACIUM	An ICTR developed system to identify P2P file sharing activity of intelligence value. Logs are accessible via DIRTY RAT.	[Tech Lead: Expert User:	
SILVER SPECTER	Allows batch Nmap scanning over TOR	JTRIG Software Developers ा	In Development
SODAWATER	A tool for regularly downloading gmail messages and forwarding them onto CERBERUS mailboxes	JTRIG Software Developers ⊑∎	Fully Operational.
SPRING BISHOP	Find private photographs of targets on Facebook.	Tech Lead:	
SYLVESTER	Framework for automated interaction / alias management on online social networks.	Tech Lead:	In Developmen
TANNER	A technical programme allowing operators to log on to a JTRIG website to grab IP addresses of Internet Cafe's.	JTRIG OSO 🖃	Replaced by HAVOK.
TRACER FIRE	An Office Document that grabs the targets Machine info, files, logs, etc and posts it back to GCHQ.	TRACER	In Developmen
VIEWER	A programme that (hopefully) provides advance tip off of the kidnappers IP address for HMG personnel.	[Tech Lead: Expert User:	Operational, bu awaiting field trial.
VIKING PILLAGE	Distributed network for the automatic collection of encrypted/compressed data from remotely hosted JTRIG projects.	PILLAGE JTRIG Software Developers ⊑	Operational
	A version of the MUSTANG and DANCING BEAR techniques that allows us to pull back Cell	[Tech Lead:	In development

[edit] Effects Capability

JTRIG develop the majority of effects capability in GCHQ. A lot of this capability is developed on demand for specific operations and then further developed to provide weaponised capability.

Don't treat this like a catalogue. If you don't see it here, it doesn't mean we can't build it. If you involve the JTRIG operational teams at the start of your operation, you have more of a chance that we will build something for you.

For each of our tools we have indicated the state of the tool. We only advertise tools here that are either ready to fire or very close to being ready (operational requirements would re-prioritise our development). Once again, involve the JTRIG operational teams early.

		-	
Tool	Description	Status	Contacts
ANGRY PIRATE	is a tool that will permanently disable a target's account on their computer.	Ready to fire (but see target restrictions).	[Tech Lead: Expe User:
ARSON SAM	is a tool to test the effect of certain types of PDU SMS messages on phones / network. It also includes PDU SMS Dumb Fuzz testing ☞.	Ready to fire (Not against live targets, this is a R&D Tool).	[Tech Lead: Expert User:]
BUMPERCAR+	is an automated system developed by JTRIG CITD to support JTRIG BUMPERCAR operations. BUMPERCAR operations are used to disrupt and deny Internet-based terror videos or other material. The technique employs the services provided by upload providers to report offensive materials.	Ready to fire.	JTRIG Software Developers ⊡
ВОМВ ВАУ	is the capability to increase website hits/rankings.	In Development.	[Tech Lead:
BADGER	mass delivery of email messaging to support an Information Operations campaign	Ready to fire.	JTRIG OSO 💷
BURLESQUE	is the capability to send spoofed SMS text messages.	Ready to fire.	JTRIG OSO 💷
CANNONBALL	is the capability to send repeated text messages to a single target.	Ready to fire.	JTRIG OSO 🖃
CLEAN SWEEP	Masquerade Facebook Wall Posts for individuals or entire countries	Ready to fire (SIGINT sources required)	[Tech Lead: Expert User:
CLUMSY BEEKEEPER	Some work in progress to investigate IRC effects.	NOT READY TO FIRE.	Tech Lead: Expert User :
CHINESE FIRECRACKER	Overt brute login attempts against online forums	Ready to fire.	FIRECRACKER
CONCRETE Donkey	is the capability to scatter an audio message to a large number of telephones, or repeatedly bomb a target number with the same message.	In development.	
DEER STALKER	Ability to aid-geolocation of Sat Phones / GSM Phones via a silent calling to the phone.	Ready to fire.	[Tech Lead: Expert User:
GATEWAY	Ability to artificially increase traffic to a website	Ready to fire.	JTRIG OSO 💷
GAMBIT	Deployable pocket-sized proxy server	In-development	JTRIG OSO 🖃
GESTATOR	amplification of a given message, normally video, on popular multimedia websites (Youtube).		[Tech Lead: ?; Expert User:
GLITTERBALL	Online Gaming Capabilities for Sensitive Operations. Currently Second Life.	In development.	
IMPERIAL BARGE	For connecting two target phone together in a call.	Tested.	[Tech Lead: Expert User:
PITBULL	Capability, under development, enabling large scale delivery of a tailored message to users of Instant Messaging services.	In development.	
POISONED DAGGER	Effects against Gigatribe. Built by ICTR, deployed by JTRIG.		Tech Lead:

PREDATORS FACE	Targeted Denial Of Service against Web Servers.		Tech Lead:
ROLLING THUNDER	Distributed denial of service using P2P. Built by ICTR, deployed by JTRIG.		Tech Lead:
SCARLET EMPEROR	Targeted denial of service against targets phones via call bombing.	Ready to fire.	JTRIG Software Developers 🖃
SCRAPHEAP Challenge	Perfect spoofing of emails from Blackberry targets.	Ready to fire, but see constraints.	
SERPENTS TONGUE	for fax message broadcasting to multiple numbers.	In redevelopment	[Tech Lead: Expert User:
SILENT MOVIE	Targeted denial of service against SSH services.	Ready to fire.	[Tech Lead:
SILVERBLADE	Reporting of extremist material on DAILYMOTION.	Ready to fire.	[Tech Lead: Expert Use
SILVERFOX	List provided to industry of live extremist material files hosted on FFUs.	Ready to fire.	[Tech Lead: Expert Use
SILVERLORD	Disruption of video-based websites hosting extremist content through concerted target discovery and content removal.	Ready to fire.	[Tech Lead: Expert Use
SKYSCRAPER	Production and dissemination of multimedia via the web in the course of information operations.	Ready to fire.	[Tech Lead: Sectio X; Expert Users: Language Team]
SLIPSTREAM	Ability to inflate page views on websites	Ready to fire.	JTRIG OSO 💷
STEALTH MOOSE	is a tool that will Disrupt target's Windows machine. Logs of how long and when the ef is active.	fect Ready to fire (but see target restrictions).	t [Tech Lead: Expert User:]
SUNBLOCK	Ability to deny functionality to send/receive email or view material online.	Tested, but operational limitations.	[Tech Lead: Sectio X; Expert User:
Swamp donkey	is a tool that will silently locate all predefined types of file and encrypt them on a targe machine.	Ready to fire (but see target restrictions).	Expert User:
TORNADO ALLEY	is a delivery method (Excel Spreadsheet) that can silently extract and run an executat on a target's machine.	Ready to fire (but see target restrictions).	Tech Lead: Expert User:
UNDERPASS	Change outcome of online polls (previously known as NUBILO)	In development.	[Tech Lead: Section X; Expert User:
VIPERS TONGUE	is a tool that will silently Denial of Service calls on a Satellite Phone or a GSM Phone.	Ready to fire (but see target restrictions).	[Tech Lead: Expert User:
WARPATH	Mass delivery of SMS messages to support an Information Operations campaign	Ready to fire.	JTRIG OSO 🖃
[edit] WOI	k Flow Management		
Tool	Description		Contacts
HOME PORTAI	A central hub for all JTRIG Cerberus tools		JTRIG Software Developers 💷
CYBER COMM	AND A centralised suite of tools, statistics and viewers for tracking current operation community.	s across the Cyber	JTRIG Software Developers ⊡
NAMEJACKER	A web service and admin console for the translation of usernames between netw gateways and other such technologies.	works. For use with	JTRIG Software Developers ⊟

metadata. Developers 3 JEED Team. The challenge is to scale up to over 1,200 users whilst remaining agile, efficent and responsive to customer needs. Tech. Lead JILES is a JTRIG bespoke web browser. Expert User INDELEMAN is a distributed real-time event aggregation, tip-off and tasking platform utilised by JTRIG as a middleware levelopers 3 TRIG Software Developers 3 OUTWARD is a collection of DNS lookup, WHOIS Lookup and other network tools. TRIG Software Developers 3 OUTWARD is a collection of DNS lookup, WHOIS Lookup and other network tools. TRIG Software Developers 3 OUTWARD is a collection of DNS lookup, WHOIS Lookup and other network tools. TRIG Software Developers 3 Standard is a data index and repository that provides analysts with the ability to query data collected from the Developers 3 TRIG Software Developers 3 Standing is a data index and repository that provides analysts with the ability to query data collected from the Developers 3 TRIG Software Developers 3 Standing is a categorisation database accessed via web service. TRIG Software Developers 3 TRIG Software Developers 3 foot Description Contacts TRIG Software Developers 3 TRIG Software Developers 3 foot Description Contacts TRIG Software Developers 3 <	Tool	Description	Contacts
ELATE between tagets. Developers I is a suite of tools for monitoring taget use of the UK auction site eBay (tww ebay co.uk). These tools ar JTRIG Software Developers I Developers I PRIMATE is a JTRIG tool that aims to provides the capability to identify trends in seized computer media data an ITRIG Software Developers I TRIG Software Developers I PRIMATE is a JTRIG tool that aims to provides the capability to identify trends in seized computer media data an ITRIG Software Developers I TRIG Software Developers I DEDI Team. The challenge is to scale up to over 1,200 users whilst remaining agile, efficent and response to controomer needs. Trech Lead DILES is a USE of tool which queries a set of online resources. This allows analysts to quickly check the ITRIG Software Developers I TRIG Software Developers I DOUTWARD is a collection of DNS lookup, WHOIS Lookup and other network tools. TRIG Software Developers I DEVELOPT is a data index and repository that provides analysts with the ability to query data collected from the etc. TRIG Software Developers I DEVELOPT is a data adde and repository that provides analysts with the ability to query data collected from the etc. TRIG Software Developers I Developers I is a database of C2C identifiers obtained from a variety of unique sources, and a TRIG Software Developers I TRIG Software Developers I Out Description Contacts Trech Lead Expert Users Out INCY is a	BABYLON		
ELANE hosted on an internet server, and results are retreived by encrypted email. Developers III is a JTRIG fool that aims to provides the capability to identify trends in seized computer media data and an anternet data. JTRIG Software JTRIG will abortly be rolling out a JEDI pod to every desk of every member of an intelligence Production Texn. The challenge is to scale up to over 1,200 users whilst remaining agile, efficent and responsive to customer needs. Trech Lead Trech Lead JTRIG Software Developers III is a distributed real-time event aggregation, tip off and tasking platform utilised by JTRIG so a middleware layer. JTRIG Software Developers III OUTWARD is a collection of DNS lookup, WHOIS Lookup and other network tools. JTRIG Software Developers IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	CRYOSTAT		
Primurite metadata. Developers JTRIG will shortly be rolling out a JEDI pod to every desk of every member of an intelligence Production customer needs. The childence is to scale up to over 1,200 users whilst remaining aglie, efficent and responsive to customer needs. The childence is to scale up to over 1,200 users whilst remaining aglie, efficent and responsive to customer needs. The childence is to scale up to over 1,200 users whilst remaining aglie, efficent and responsive to customer needs. The childence is to scale up to over 1,200 users whilst remaining aglie, efficent and responsive to customer needs. The childence is the scale up to over 1,200 users whilst remaining aglie, efficent and responsive to customer needs. The childence is the scale up to over 1,200 users whilst remaining aglie, efficent and responsive to customer needs. The childence is the scale up to over 1,200 users while the	ELATE		
JEED! Team. The challinge is to scale up to over 1,200 users whilst remaining agile, efficent and responsive to customer needs. Tech Lead JILES is a JTRIO bespoke web browser. Tech Lead ISED is a distributed real-time event aggregation, tip-off and tasking platform utilised by JTRIO as a middleware Developers 3 OUTWARD is a collection of DNS lookup, WHOIS Lookup and other network tools. JTRIO Software Developers 3 OUTWARD is a collection of DNS lookup, WHOIS Lookup and other network tools. JTRIO Software Developers 3 TANGLEFOOT is a duit processe stormed data into globaccidor internation. JTRIO Software Developers 3 StAMMER is a data index and repository that provides analysts with the ability to query data collected from the etc. JTRIO Software Developers 3 Is a data index and repository that provides analysts with the ability to query data collected from the etc. JTRIO Software Developers 3 Is a data index and repository that provides analysts with the ability to query data collected from the etc. JTRIO Software Developers 3 Is a data index and repository that provides analysts with the ability to query data collected from the set or unare name. JTRIO Software Developers 3 Is a data base of C2C identifiers for Intelligence Community assets acting online. JTRIO Software Developers 3 Is a database of C2C identifiers obinthed from a variety of unique sources, and a	PRIMATE		
JILES Is a JIRIG bespice web provider. Expert User: MIDDLEMAN is a distributed real-time event aggregation, tip-off and tasking platform utilised by JIRIG as a middleware IJIRIG Software Developers II JIRIG Software Developers II OUTWARD is a collection of DNS lookup, WHOIS Lookup and other network tools. JIRIG Software Developers II TANCLEFOOT is a bulk search tool which quaries a set of online resources. This allows analysts to quickly check the JIRIG Software Developers II JIRIG Software Developers II Centromation is a data index and repository that provides analysts with the ability to query data collected from the internet from various JIRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts JIRIG Software Developers II Centro Description Contacts Developers II STANDER is a categorisation database accessed via web service. JIRIG Software Developers II Developers II Contout is a database of C2C identifiers to fintelligence Community assets acting online, JIRIG Software Developers II Software Developers II QUINCY is an enterprise level suite of tools for the exploitation of selzed media. ITECh Lead Expert User: Cedit Description Contacts ITECh Lead Expert User: ITECh Lead Expert User: Guint (FOT-Ensic Exploitation ITEL Software Deve	JEDI	Team. The challenge is to scale up to over 1,200 users whilst remaining agile, efficent and responsive	<u>. </u>
MIDULENAN layer. Developers I OUTWARD is a collection of DNS lookup, WHOIS Lookup and other network tools. JTRIG Software Developers I TANCLEFOOT is a bulk search tool which queries a set of online resources. This allows analysts to quickly check the online presence of a target. JTRIG Software Developers I CHIT-ADIUTO (Vote: is a tool that processes kinnet data into geolocation information JTRIG Software Developers I SLAMMER is a data index and repository that provides analysts with the ability to query data collected from the intermet from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts JTRIG Software Developers I Eedit Databases TRIG Software Developers I Iteration various JTRIG Software Developers I Eedit Database of C2C identifiers for Intelligence Community assets acting online, either under alias of real name. JTRIG Software Developers I Is a database of C2C identifiers for Intelligence Community assets acting online, suite of tools for exploring this data. JTRIG Software Developers I Intermet from various for exploring this data. Trech Lead Expert Users: QUINCY is a neterprise level suite of tools for the exploitation of seized media. Trech Lead Expert Users: Eedit Description Contacts Trech Lead Expert Users: Expert User; <td>JILES</td> <td>is a JTRIG bespoke web browser.</td> <td>[Tech Lead: Expert User:]</td>	JILES	is a JTRIG bespoke web browser.	[Tech Lead: Expert User:]
OUTWARD is a collection of DNS lookup, WHOIS Lookup and other network tools. Developers I TANGLEFOOT is a bulk search tool which queries a set of online resources. This allows analysts to quickly check the online presence of a target. JTRIG Software Developers I SURFAMINE is a data index and repository that provides analysts with the ability to query data collected from the intermet from various JTRIG software Developers I JTRIG Software Developers I SLAMMER is a data index and repository that provides analysts with the ability to query data collected from the intermet from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts etc. JTRIG Software Developers I [edit] Databases JTRIG Software Developers I Developers I is a database of C2C identifiers for Intelligence Community assets acting online, JTRIG Software Developers I Itrice Software Developers I is a database of C2C identifiers obtained from a variety of unique sources, and a JTRIG Software Developers I Itrice Software Developers I QUINCY is a enterprise level suite of tools for the exploitation of seized media. Itrice Lead Expert Users: [edit] Forensic Exploitation Itrice Software Developers I Itrice Lead Expert Users: [edit] Forensic Exploitation Itrice Software Developers I Itrice Lead Expert Users: [edit] <td>MIDDLEMAN</td> <td></td> <td></td>	MIDDLEMAN		
TANCLEFOIL online presence of a target. Developers I SCHEZANING (50011) La tool that processes kannet data into geolocation information JTRIG Software Developers I SLAMMER is a data index and repository that provides analysts with the ability to query data collected from the Internet from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts etc. JTRIG Software Developers I [edit] Databases Contacts [edit] Description Contacts BYSTANDER is a categorisation database accessed via web service. JTRIG Software Developers I conbult is a database of C2C identifiers for Intelligence Community assets acting online, either under alias or in real name. JTRIG Software Developers I NEWPIN is a database of C2C identifiers obtained from a variety of unique sources, and a suite of tools for exploring this data. ITRIG Software Developers I [edit] Forensic Exploitation [fech Lead] Expert Users: [redit] Forensic Exploitation [fech Lead] Expert Users: sFL The Signit Forensics Laboratory was developed within NSA. It has been adapted by JTRIG as its email extraction and first pass analysis of seized media solution. [rech Lead] Expert User: SFL is a tool to extract data from field forensics' reports created by Celldek, Cellebrite, XRY, upload	OUTWARD	is a collection of DNS lookup, WHOIS Lookup and other network tools.	
ALCOLIS E a tool that processes kismet data into geolocation information JTRIG Software Developers I SLAMMER is a data index and repository that provides analysts with the ability to query data collected from the Internet from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts etc. JTRIG Software Developers I [edit] Databases Contacts [FSTANDER] is a categorisation database accessed via web service. JTRIG Software Developers I [is a database of C2C identifiers for Intelligence Community assets acting online, its a database of C2C identifiers obtained from a variety of unique sources, and a suite of tools for exploring this data. JTRIG Software Developers I [edit] Forensic Exploitation [fech Lead] Expert Users: [edit] Forensic Exploitation [fech Lead] [fech Lead] [edit] Forensic Exploitation [fech Lead] [fech Lead] [edit] Forensic Exploitation [fech Lead] [fech Lead] [s a tool to extract wiFi connection history (MAC and timing) when supplied with a copy of the gistry structure or run on the box. [fech Lead] [fech Lead] [s a tool to extract mobile phone data from a copy of the phone's memory (usually supplied as an image file extracted through FTK. [fech Lead] [fech Lead] [s a tool to extract mobile phone data from a copy of the phone	TANGLEFOOT		
SLAMMER is a data index and repository that provides analysts with the ability to query data collected from the intermet from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts JTRIG Software Developers I Itement from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts Developers II Itement from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts Developers II Itement from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts Developers II Itement from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts Developers II Itement from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts JTRIG Software Developers II Itement from various JTRIG sources, and a so the component of the sources, and a JTRIG Software Developers II JTRIG Software Developers II Itement from various JTRIG sources are a suite of tools for the exploitation of seized media. ITRIG Software Developers II QUINCY is an enterprise level suite of tools for the exploitation of seized media. ITRIG Software Developers II Itement from various JTRIG sources, such as EARTHLING, HACIENDA Expert Users: ITRIG Software Developers II Itement from treal name. Item character Software Developers II Item character Software Developers II QUINCY is a nenterprise level suite		is a tool that processes kismet data into geolocation information	
Tool Description Contacts BYSTANDER is a categorisation database accessed via web service. JTRIG Software Developers I is a database of C2C identifiers for intelligence Community assets acting online, either under alias or in real name. JTRIG Software Developers I NEWPIN is a database of C2C identifiers obtained from a variety of unique sources, and a suite of tools for exploring this data. JTRIG Software Developers I QUINCY is an enterprise level suite of tools for the exploitation of seized media. ITech Lead: Expert Users: I [edit] Forensic Exploitation Contacts Itel is an enterprise level suite of tools for the exploitation of seized media. Ifech Lead: Expert Users: I [edit] Forensic Exploitation Ifech Lead: I Itel is an enterprise level suite of tools for the exploitation of seized media. Ifech Lead: I [edit] Forensic Exploitation Ifech Lead: I Itel is a cold to extract WiFi connection history (MAC and timing) when supplied with a copy of the registry structure or run on the box. Ifech Lead: I SFL The Sigint Forensics Laboratory was developed within NSA. It has been adapted by JTRIG as its email extraction and first-pass analysis of seized media solution. Ifech Lead: I Snoopy is a tool to extract data from field forensics' reports created by Celldek, Cellebrite, XRY, uploa to Newpin		etc.	
BYSTANDER is a categorisation database accessed via web service. JTRIG Software Developers II CONDUIT is a database of C2C identifiers for Intelligence Community assets acting online, either under alias or in real name. JTRIG Software Developers II NEWPIN is a database of C2C identifiers obtained from a variety of unique sources, and a suite of tools for exploring this data. JTRIG Software Developers II QUINCY is an enterprise level suite of tools for the exploitation of seized media. Tech Lead: Expert Users: [edit] Forensic Exploitation If contacts Ited if the contact in the box. If contacts BEARSCRAPE Can extract WiFi connection history (MAC and timing) when supplied with a copy of the registry structure or run on the box. If contacts SFL The Signit Forensics Laboratory was developed within NSA. It has been adapted by JTRIG is a tool to extract mobile phone data from a copy of the phone's memory (us-ully supplied as an image file extracted through FTK. If ech Lead: If ech Lead			
CONDUT is a database of C2C identifiers for Intelligence Community assets acting online, iter under alias or in real name. JTRIG Software Developers I NEWPIN is a database of C2C identifiers obtained from a variety of unique sources, and a suite of tools for exploring this data. JTRIG Software Developers I QUINCY is an enterprise level suite of tools for the exploitation of seized media. If Ech Lead: Expert Users: Exploitation [edit] Forensic Exploitation Contacts Tool Description Contacts BEARSCRAPE Can extract WiFi connection history (MAC and timing) when supplied with a copy of the registry structure or run on the box. If ech Lead: Expert User: Exploitation SFL The Sigint Forensics Laboratory was developed within NSA. It has been adapted by JTRIG as its email extract dhrough FTK. If ech Lead: Expert User: Expert User: Expert User: Is a tool to extract data from field forensics' reports created by Celldek, Cellebrite, XRY, upload to Newpin. If ech Lead: If ec		•	
NEWPIN is a database of C2C identifiers obtained from a variety of unique sources, and a suite of tools for exploring this data. JTRIG Software Developers II QUINCY is an enterprise level suite of tools for the exploitation of seized media. ITech Lead: Expert Users: II [edit] Forensic Exploitation Contacts Tool Description Contacts BEARSCRAPE can extract WiFi connection history (MAC and timing) when supplied with a copy of the registry structure or run on the box. ITech Lead: IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	CONDUIT ^{is}	s a database of C2C identifiers for Intelligence Community assets acting online, JTRIG Software Develo	
QUINCY is an enterprise level suite of tools for the exploitation of seized media. [Tech Lead: Expert Users:] [edit] Forensic Exploitation Contacts Tool Description [Tech Lead:] BEARSCRAPE can extract WiFi connection history (MAC and timing) when supplied with a copy of the registry structure or run on the box. [Tech Lead:] SFL The Sigint Forensics Laboratory was developed within NSA. It has been adapted by JTRIG as its email extraction and first-pass analysis of seized media solution. [Tech Lead:] Snoopy is a tool to extract mobile phone data from a copy of the phone's memory (usually supplied as an image file extracted through FTK. [Tech Lead:] is a tool to extract data from field forensics' reports created by Celldek, Cellebrite, XRY, upload to Newpin. [Tech Lead:] wobileHoover Snoopy and USIM detective. These reports are transposed into a Newpin XML format to upload to Newpin. [Tech Lead:] Nevis is a tool developed by NTAC to search disk images for signs of possible Encryption [Tech Lead:]	NEWPIN ^{is}	s a database of C2C identifiers obtained from a variety of unique sources, and a JTRIG Software Develo	opers 🖃
Image: Perform and the second seco			Expert Users:
Tool Description Contacts BEARSCRAPE can extract WiFi connection history (MAC and timing) when supplied with a copy of the registry structure or run on the box. Tech Lead: Sepert User: User: Second as its email extraction and first-pass analysis of seized media solution. Tech Lead: Sepert User: Second as an image file extracted through FTK. Snoopy is a tool to extract data from field forensics' reports created by Celldek, Cellebrite, XRY, Snoopy and USIM detective. These reports are transposed into a Newpin. Tech Lead: Tech Lead: Tech Lead: Second as Newpin XML format to upload to Newpin. Nevis is a tool developed by NTAC to search disk images for signs of possible Encryption Tech Lead: Tech Lead: Second as Newpin XML format to upload to Newpin.	QUINCY is	s an enterprise level suite of tools for the exploitation of seized media.	
BEARSCRAPE can extract WiFi connection history (MAC and timing) when supplied with a copy of the User:] [Tech Lead:] SFL The Sight Forensics Laboratory was developed within NSA. It has been adapted by JTRIG as its email extraction and first-pass analysis of seized media solution. [Tech Lead:] Snoopy is a tool to extract mobile phone data from a copy of the phone's memory (usually supplied as an image file extracted through FTK. [Tech Lead:] NobileHoove is a tool to extract data from field forensics' reports created by Celldek, Cellebrite, XRY, upload to Newpin. [Tech Lead:] Nevis is a tool developed by NTAC to search disk images for signs of possible Encryption [Tech Lead:]	[edit] For	ensic Exploitation	
BEARSCRAPE registry structure or run on the box. User:] SFL The Sigint Forensics Laboratory was developed within NSA. It has been adapted by JTRIG as its email extraction and first-pass analysis of seized media solution. [Tech Lead:] Snoopy is a tool to extract mobile phone data from a copy of the phone's memory (usually supplied as an image file extracted through FTK. [Tech Lead:] MobileHoover is a tool to extract data from field forensics' reports created by Celldek, Cellebrite, XRY, Snoopy and USIM detective. These reports are transposed into a Newpin XML format to upload to Newpin. [Tech Lead:] Nevis is a tool developed by NTAC to search disk images for signs of possible Encryption [Tech Lead:]	Tool	Description Contacts	5
SFL The Signt Forensics Laboratory was developed within NSA. It has been adapted by JTRIG as its email extraction and first-pass analysis of seized media solution. Expert User: Snoopy is a tool to extract mobile phone data from a copy of the phone's memory (usually supplied as an image file extracted through FTK. Tech Lead: MobileHoover Snoopy and USIM detective. These reports are transposed into a Newpin XML format to upload to Newpin. Tech Lead: Nevis is a tool developed by NTAC to search disk images for signs of possible Encryption Tech Lead:	BEARSCRAPE		ad: Expert
Shoopy as an image file extracted through FTK. [Tech Lead] MobileHoover is a tool to extract data from field forensics' reports created by Celldek, Cellebrite, XRY, shoopy and USIM detective. These reports are transposed into a Newpin XML format to upload to Newpin. [Tech Lead] Nevis is a tool developed by NTAC to search disk images for signs of possible Encryption [Tech Lead]	SFL	The Sigint Forensics Laboratory was developed within NSA. It has been adapted by JTRIG	
MobileHoover Snoopy and USIM detective. These reports are transposed into a Newpin XML format to upload to Newpin. Itech Lead: Nevis is a tool developed by NTAC to search disk images for signs of possible Encryption Itech Lead:		as its email extraction and first-pass analysis of seized media solution.	
Nevis		is a tool to extract mobile phone data from a copy of the phone's memory (usually supplied	ad:
	Snoopy	is a tool to extract mobile phone data from a copy of the phone's memory (usually supplied as an image file extracted through FTK. is a tool to extract data from field forensics' reports created by Celldek, Cellebrite, XRY, Snoopy and USIM detective. These reports are transposed into a Newpin XML format to	

Tool	Description		Contacts
CHANGELIN	G Ability to spoof any email address and send email under that identity		JTRIG OSO 🖃
наvок	Real-time website cloning technique allowing on-the-fly alterations		JTRIG OSO 🖃
MIRAGE			JTRIG OSO 🖃
SHADOWCA	T End-toEnd encrypted access to a VPS over SSH using the TOR network		JTRIG OSO 🖃
SPACE Rocket	is a programme covering insertion of media into target networks. CRINKLE CUT is a tool develo CISA to enable JTRIG track images as part of SPACE ROCKET.	oped by ICTR-	Tech Lead: Experi User:
RANA	is a system developed by ICTR-CISA providing CAPTCHA-solving via a web service on CERBE intended for use by BUMPERCAR+ and possibly in future by SHORTFALL but anyone is welc		Tech Lead: Expert U
LUMP	A system that finds the avatar name from a SecondLife AgentID		JTRIG Software Developers ≡
GURKHAS SWORD	Beaconed Microsoft Office Documents to elicite a targets IP address.		JTRIG Software Developers 🛋
[edit] Sh	haping and Honeypots		
[edit] Sh Tool	haping and Honeypots Description	Contacts	
		Contacts JTRIG OSC) =1
Tool	Description		
Tool DEADPOOL HUSK	Description URL shortening service Secure one-to-one web based dead-drop messaging platform	JTRIG OSC) 🖃
Tool DEADPOOL HUSK LONGSHOT	Description URL shortening service Secure one-to-one web based dead-drop messaging platform File-upload and sharing website	JTRIG OSC JTRIG OSC JTRIG OSC) 🖃
Tool DEADPOOL HUSK LONGSHOT MOLTEN-MA	Description URL shortening service Secure one-to-one web based dead-drop messaging platform File-upload and sharing website AGMA CGI HTTP Proxy with ability to log all traffic and perform HTTPS Man in the Middle.	JTRIG OSC JTRIG OSC JTRIG OSC) 🖬) 🖬 ware Developers
Tool DEADPOOL	Description URL shortening service Secure one-to-one web based dead-drop messaging platform File-upload and sharing website AGMA CGI HTTP Proxy with ability to log all traffic and perform HTTPS Man in the Middle.	JTRIG OSC JTRIG OSC JTRIG OSC JTRIG Soft) ==) == ware Developers =) ==
Tool DEADPOOL HUSK LONGSHOT MOLTEN-MA NIGHTCRAW	Description URL shortening service Secure one-to-one web based dead-drop messaging platform File-upload and sharing website AGMA CGI HTTP Proxy with ability to log all traffic and perform HTTPS Man in the Middle. VLER Public online group against dodgy websites Image hosting and sharing website	JTRIG OSC JTRIG OSC JTRIG OSC JTRIG Soft JTRIG OSC) ==) == ware Developers =) ==
Tool DEADPOOL HUSK LONGSHOT MOLTEN-MA NIGHTCRAW PISTRIX	Description URL shortening service Secure one-to-one web based dead-drop messaging platform File-upload and sharing website AGMA CGI HTTP Proxy with ability to log all traffic and perform HTTPS Man in the Middle. VLER Public online group against dodgy websites Image hosting and sharing website	JTRIG OSC JTRIG OSC JTRIG OSC JTRIG Soft JTRIG OSC) ==) == ware Developers =) ==

Category: JTRIG

Crown Copyright] © 2008 or is held under licence from third parties. This information is exempt under the Freedom of Information Act and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on

About GCWiki Privacy policy Disclaimers

TOP SECRET STRAP1 COMINT The maximum classification allowed on GCWiki is TOP SECRET STRAP1 COMINT. Click to report inappropriate content.