

Forensics for System Administrators II

CyberChef

Stefan Kelm
WP8-T1

Webinar, 27th of April 2022

Public

www.geant.org

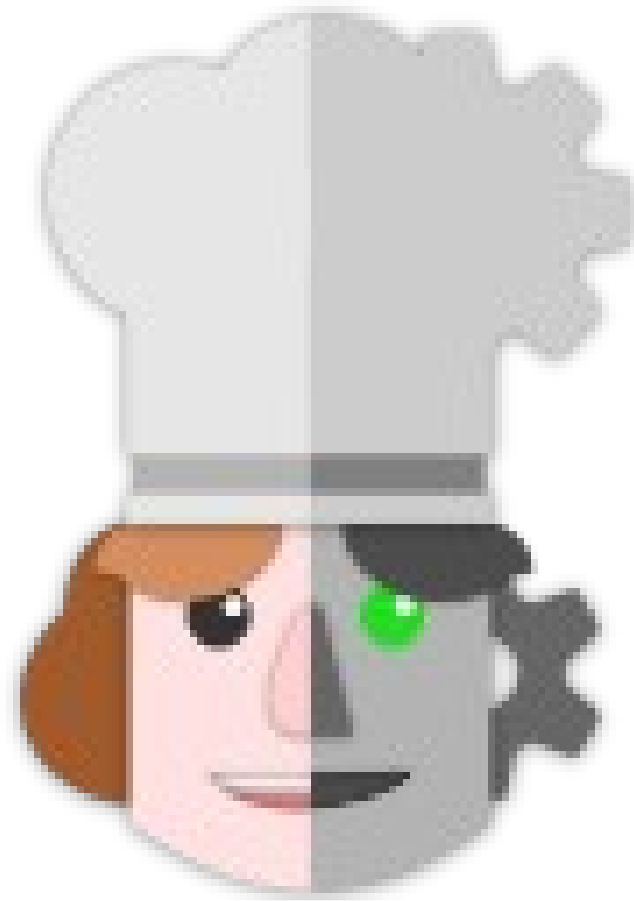
The Road Ahead: Forensics for System Administrators II



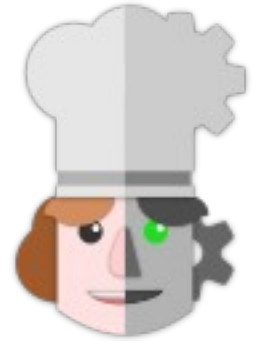
- CyberChef (demo)
- Memory Analysis Basics - First Steps
- Advanced Memory Analysis - Dealing with Malicious Code
- Persistent Storage Forensics I - Basics and First Steps
- Persistent Storage Forensics II - Advanced Approaches



“The Cyber Swiss Army Knife”

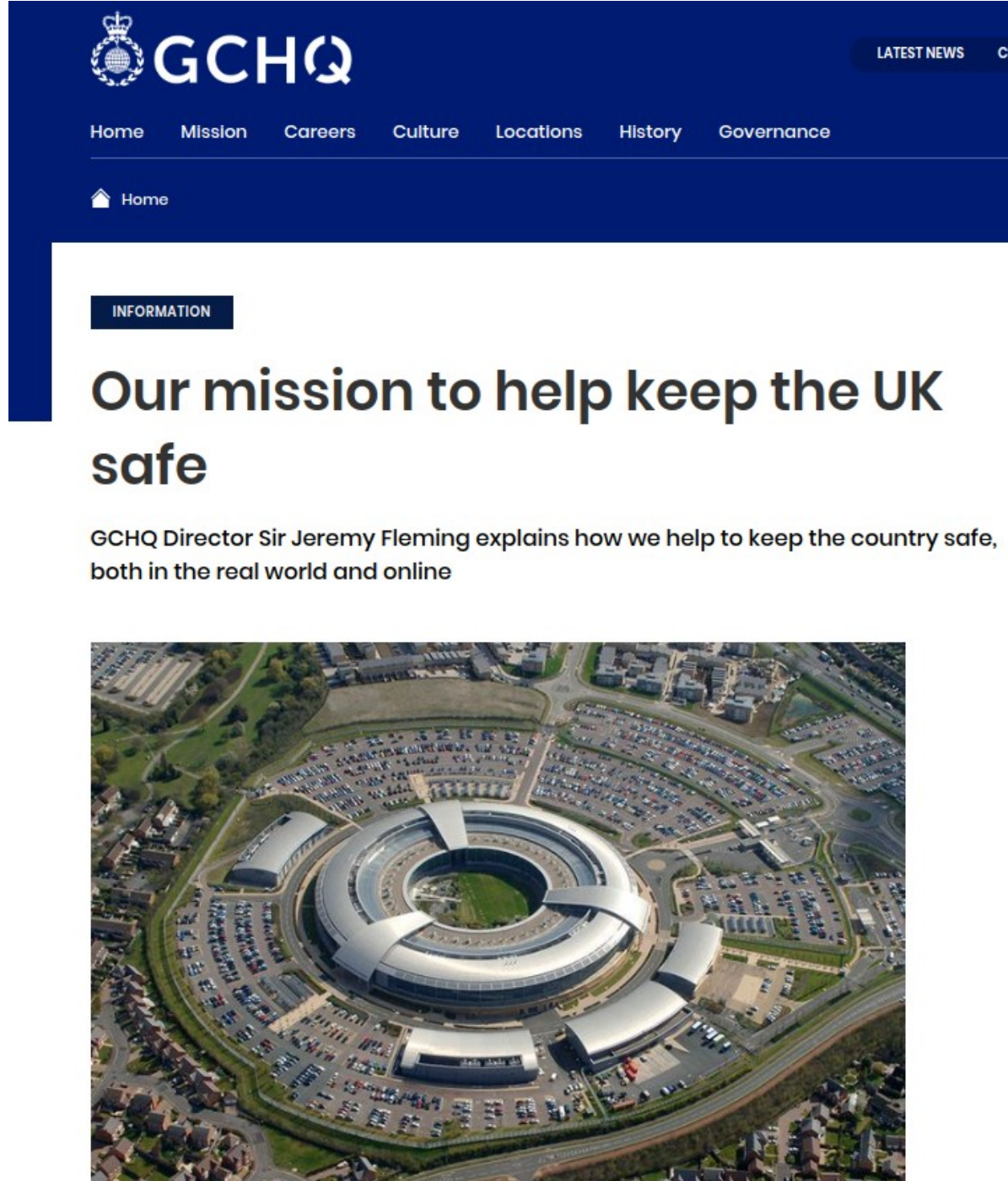


In their (GCHQ's) own words



"CyberChef is a simple, intuitive web app for carrying out all manner of "cyber" operations within a web browser. These operations include simple encoding like XOR and Base64, more complex encryption like AES, DES and Blowfish, creating binary and hexdumps, compression and decompression of data, calculating hashes and checksums, IPv6 and X.509 parsing, changing character encodings, and much more."

GCH who?



GCHQ

LATEST NEWS CUR


Home Mission Careers Culture Locations History Governance

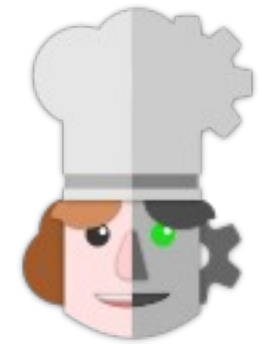
Home

INFORMATION

Our mission to help keep the UK safe

GCHQ Director Sir Jeremy Fleming explains how we help to keep the country safe, both in the real world and online





Why CyberChef?

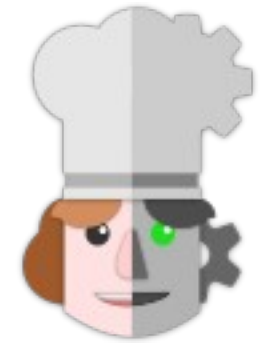
- Value of CyberChef
 - Lots and lots (yes, hundreds!) of operations within a single application
 - Powerful operation search engine built-in
 - Combine *operations* into *recipes* – hence the name “CyberChef”
 - All you need is a browser – nothing to install
 - No Internet connection necessary – completely client-side
 - GCHQ never sees what you’re doing
 - It’s on github – completely OpenSource and free!
 - under active development
 - Everything you do **can** be bookmarked, saved, shared with colleagues, posted to blogs, Twitter, etc.
 - ... which is especially useful when your workflow consists of recurring tasks

Demo time!

Fancy scanning that QR code we just generated ...? ;-)

Recipe			Input
Generate QR Code ⏏ ⏸			<code>https://www.google.de</code>
Image Format PNG	Module size (px) 5	Margin (num modules) 2	Output 
Error correction Medium			
			

Wrapping up



Notes and recommendations

- There often is more than one way to achieve a goal
- Regular Expressions to the rescue! ;-)
- Save (and share!) your recipes
- Turn off “Auto Bake” when using large recipes/large inputs
- Use the “Comment” operation for taking notes
- Check out Matt’s huge list of CyberChef recipes on github
- Caveat
 - I could only show you a fraction of CyberChef’s functionality, so ...
 - ... please go through the (huge) list of operations to see which ones are most useful to **your** daily workflow(s)

Thank you

Any questions?

Next Webinar: *Memory Analysis Basics - First Steps*

May 4th, 2022

www.geant.org



References

- <https://github.com/gchq/CyberChef>
- <https://gchq.github.io/CyberChef> (Live Demo, running on GCHQ's github account, as well as download location for the ZIP archive)
- <https://github.com/mattnotmax/cyberchef-recipes>
- <https://www.dfn-cert.de/en/Trainings.html> (all our previous trainings, including slides and recordings)

