



Level 0x05

SCM

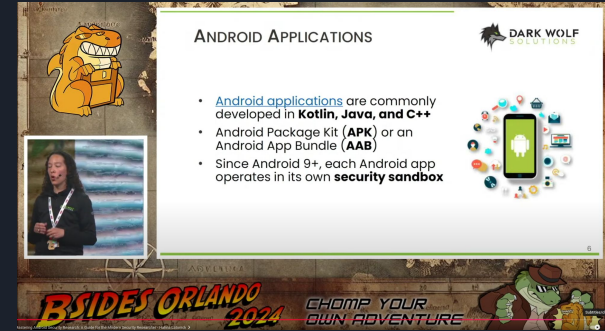


Topics

- Cyberquest
- Hacking History
- SCM
- Git demo

Events

- Videos from B-Sides Orlando
 - [Cyberwarefare in Finland](#)
 - [AI Generated Disinformation](#)
 - [Beginning Android Security Research](#)
- [Maker Faire Orlando](#)
 - Nov 9 and 10 (this weekend)
 - Central Florida Fairgrounds
 - \$15 - \$20 per person
 - 3d-printing, robotics, makers / crafters, cosplay





More Video Game Hacking

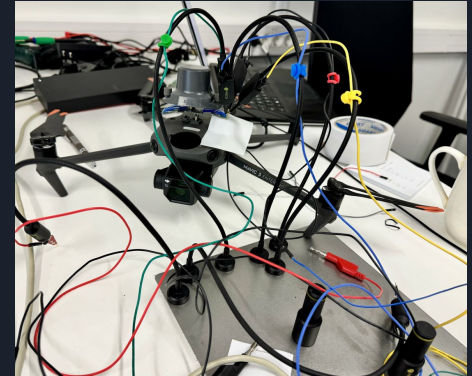
- [Reverse engineering of Dreamcast Ecco the Dolphin](#)

1. Go to the VMU Menu > New game > Enter your initials screen.
2. Enter one of these sequences, making sure not to end after 3 letters.

GYUGYU+XXX : Unlock all levels
SOCCER+XXX : Unlock bonus stage*
EXBBERX+XXX: Immortality mode*
QQRIQ+XXX : Show FPS*
XYZZYX+XXX : Show time*
POPELY+XXX : Nothing?

Joel Reymont

- Drone Hacker from Spain working in Ukraine
- [Twitter/X thread](#)
 - Drones lose signal and GPS on front-line
 - How can we get expensive surveillance drone back home?
 - Advanced GPS radio receiver





Software Configuration Management (SCM)

How we manage changes and releases of software artifacts during software development

1. Identifying Configuration Items: source code, documents
2. Version Control: keep a history of different versions
3. Build Management: compilers and building tools (make, cmake)
4. Change Management: multiple users, merging, code reviews
5. Release Management: release packages

Tapes, Floppys, Zips



- Stored our programs on tape / floppy disks
- Shared by walking to our friends house (sneakernet)
- Floppy Disks
 - 8-inch: 250 KB
 - 5 ¼ inch: 360 KB - 1.2 MB
 - 3 ½ inch: 1.44 MB
- File Containers
 - Tape Archive (tar). Unix 1979, Windows 2018
 - No compression
 - Lempel-Ziv algorithms: LZ77/LZ78 -> LZMA (7zip)
 - Many patent issues / lawsuits
 - PKWare's PK Zip. DOS 1989
 - DEFLATE: 1993 Zip2.0 and GZip





Diff

```
mwailes@Metroid:~/scratch/patch_test$ cat hw.c
#include <stdio.h>

int main(int argc, char** argv)
{
    printf("Hello World\n");
    return 0;
}
```

`diff` creates a little snippet of the code change between 2 versions of a file

Can email the diff to maintainer

```
mwailes@Metroid:~/scratch/patch_test$ cat hw_rev2.c
#include <stdio.h>

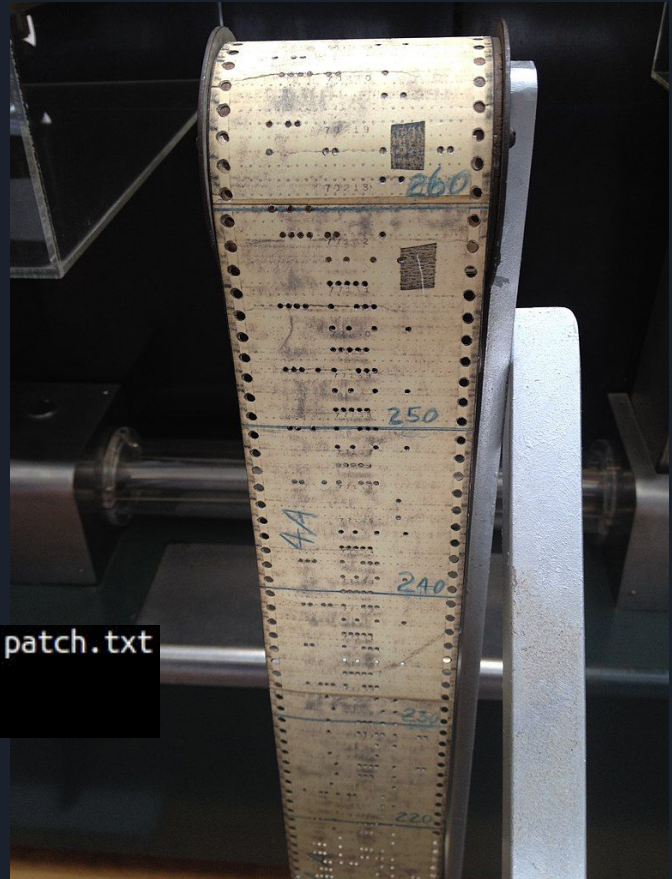
int main(int argc, char** argv)
{
    printf("Hello World\n");
    printf("Goodbye Cruel World\n");
    return 0;
}
```

```
mwailes@Metroid:~/scratch/patch_test$ diff -u hw.c hw_rev2.c
--- hw.c      2024-04-25 01:19:40.909594695 -0400
+++ hw_rev2.c 2024-04-25 01:20:15.006166220 -0400
@@ -3,6 +3,7 @@
 int main(int argc, char** argv)
 {
     printf("Hello World\n");
+    printf("Goodbye Cruel World\n");
     return 0;
 }
```


Patch

- Apply diff / patch file to update your copy of the code
- “Patch” word comes from “patching” punched holes in paper tape programs

```
mwales@Metroid:~/scratch/patch_test$ diff -u hw.c hw_rev2.c > patch.txt
mwales@Metroid:~/scratch/patch_test$ patch hw.c patch.txt
patching file hw.c
```



Graphical Diff Tools

- Kompare, meld, Beyond Compare, and Github/Gitlab have graphical diff

Photo gallery will now sort photos alphabetically

master

mwales committed on Apr 9, 2019

1 parent e7bf952 commit diaf7f6

Showing 1 changed file with 2 additions and 1 deletion.

Whitespace Ignore whitespace Split Unified

photoGallery/photo_gallery.py

```
@@ -65,6 +65,7 @@ def isImageFile(filename):
65
66 # Generate the new filename for all of the files and create thumbnails
67 filenameMap = {}
68 + filelist = sorted(filelist)
69 for singleFile in filelist:
70     if os.path.isfile(singleFile) and isImageFile(singleFile):
71         hashedName = processFile(singleFile)
72
73
@@ -83,7 +84,7 @@ def isImageFile(filename):
83 html.write('<html>\n')
84 html.write("&<body>\n\n")
85
86 - for orig in filenameMap:
87     hashname = filenameMap[orig]
88     os.rename(orig, hashname)
89     html.write('  <a href="' + hashname + '">\n')
90
91
84 html.write('<html>\n')
85 html.write("&<body>\n\n")
86
87 + for orig in sorted(filenameMap.keys()):
88     hashname = filenameMap[orig]
89     os.rename(orig, hashname)
90     html.write('  <a href="' + hashname + '">\n')
```



Centralized Version Control

- Have a central server and collect / store all those patches together!
 - Add username / password to protect the source code
 - Manage changesets over time / history of code
 - Label certain versions as releases
- Branching
 - Make long / complicated changes on branches by themselves so you don't break the build for others
- SCCS (Source Code Control System): Unix 1972
- RCS (Revision Control System): 1980 and CVS (Concurrent Versioning System): 1990
- SVN (Subversion): 2000
- IBM Rational Clearcase: Used by L3Harris for 20 years. Cost \$\$\$\$

Distributed Version Control

- Large projects like Linux needed a non-centralized tool (2000s)
 - Developers are all over the world, single central server would be expensive and taxed
 - Want to be able to make software changes when not connected
 - Centralized system also slower (especially large projects)
- BitKeeper (2000) became the Linux kernel CM tool
 - Had some weird license that let Linux devs use it for free
 - Controversial / flamewars
 - Drops free version used by Linux after 2 years
- Linux kernel needed a new CM tool
 - Linux Torvalds starts development of git over the course of 2 weeks
 - A few years later, it finally matures to become kernel's official CM tool
- Every computer has a full copy of the source repo
 - Slow to do initial clone
 - Really fast for EVERYTHING else





GitHub / Gitlab



- GitHub launches in 2008
 - Hosts git repo online - easily reachable by all
 - Free for open source development, \$\$ for proprietary repos (later free option too)
- Git / Github quickly become industry standard
 - L3Harris was not so quick to make the switch
- Gitlab starts in 2014
- GitHub and GitLab evolve into collaboration tools
 - Documentation: markdown, wiki
 - Discussions / bug tracking
 - Task management
 - Automation tools for testing, building, deployment
- DevOps



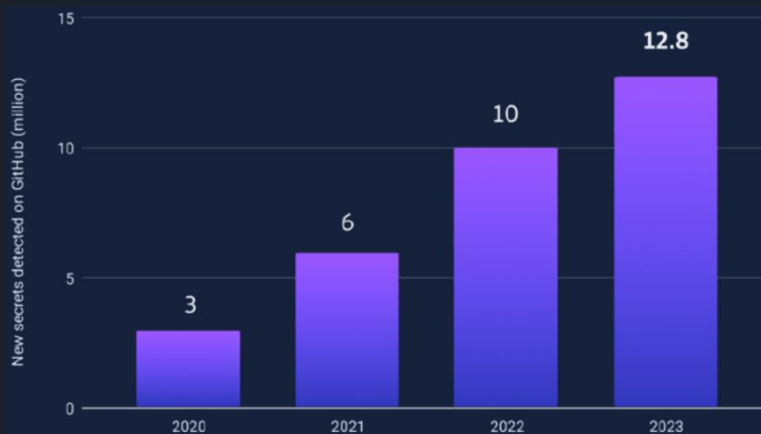
GitLab

Documentation

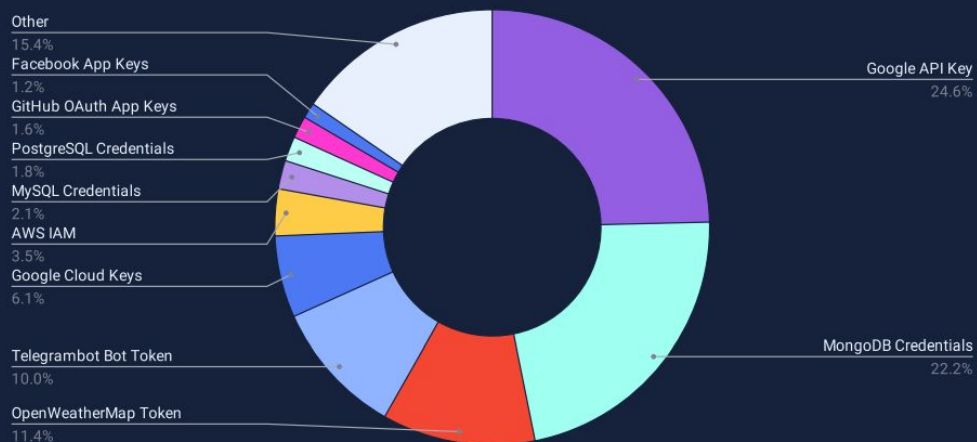
- Most git browsers have built-in markdown preview
- What is Markdown?
 - Lightweight markup language (easier than HTML)
 - Supports image embedding, tables, lists, linking, etc
 - Styling doesn't interfere much with readability
- [Markdown \(Wikipedia\)](#)
- [Github Markdown Syntax](#)
- What are we documenting?
 - What does your application do?
 - How do you build it?
 - How do you run it?
 - Future work?
 - How does it work?



Leaking Secrets



Top 10 Valid Specific Secrets Detectors in 2023



Start using GitHub

- Install git
- Create an ssh keypair on your PC
- Create an account on github
- Add your public SSH key to git account

```
user@debianTest:~$ ssh-keygen  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/user/.ssh/id_rsa):  
Created directory '/home/user/.ssh'.  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/user/.ssh/id_rsa  
Your public key has been saved in /home/user/.ssh/id_rsa.pub  
The key fingerprint is:  
SHA256:Xc0U7icZwBkIILnLrH8DvymSpexKdCtWkyayzlu8DMl user@debianTest  
The key's randomart image is:  
  
+---[RSA 3072]-----+  
|               . o=+ |  
|. + o+         |  
|. .. =o       |  
|..   .m.o     |  
||. ||. ++    |  
|...o++      |  
|..o....mm    |  
|.....oM... |  
||..o..oM+. + |  
|...o.o..oo. + |  
+---[SHA256]-----+  
  
user@debianTest:~$ cat ~/.ssh/id_rsa.pub  
ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAQgQD1F4bn48EipWrhl7CQ6y9YeiUAmyFG2V9ClFsImPaEchitUtrNsEEQuRg9QG+jxCubM/FDTftvv  
Fo/x/Mx/qXgmPqGJfKyj1=fTuhdkBrhuuuLCTIKeyypTsq1iaJ+gdAgGAPB/+e-WpLvDtBTWbyThwTSAd+lacthePhdRehatdearixBA3LFBL198voiljn  
FaAoAklawedovikSqdXCXYrgavetruho.afTeobidagapocpzoona/fvuwatht/PkwZngfyabAsFlmggcdqrfrakql-oy-JewehWT-The-Kozycjsah-SoguzlerLyZLo  
UNUMAFpghpruafScandem.FdTTHPLVLJCQCIdbfHa4zwgrtl1PMQ/rndphracadecbxOUs.vudAGUC.usPhddeltoevvne=sduvTrFrpejlLnepFCBeLLVTJJ/m9gbG  
asBC9W4VOUALSyZH2KHGXPs9oyE3NgTNBoEO3SwjmgiMbxbVVhsff77nlHNx/Poe3ChqOIkvYJD5CsTxIsEqsbTMNBnxmpih0= user@debianTes  
t
```

Public profile

Account

Appearance

Accessibility

Notifications

Access

- Billing and plans
- Emails
- Password and authentication
- Sessions
- SSH and GPG keys**
- Organizations
- Enterprises

SSH keys

This is a list of SSH keys associated with your account. Remove any keys that you do not recognize.

Authentication keys

Metroid
SHA256:
Added on Mar 21, 2021
Last used within the last 4 weeks — Read/write

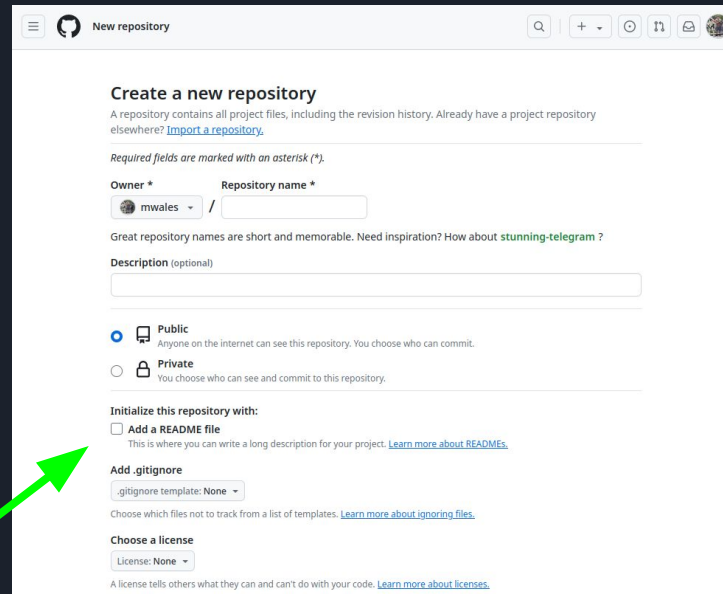
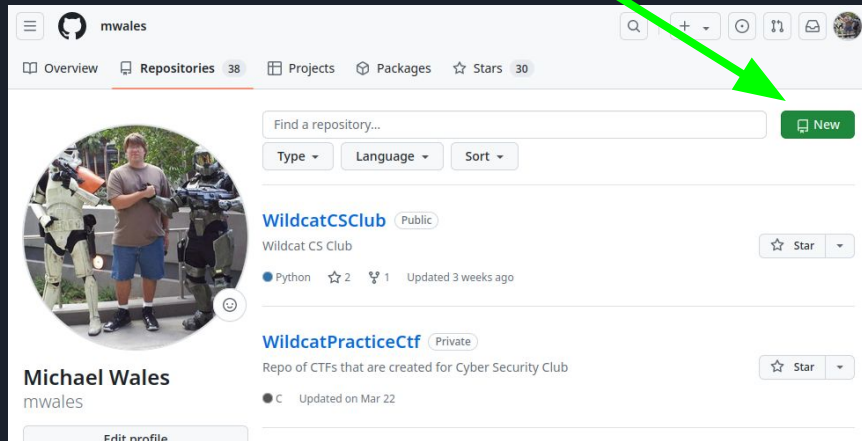
Delete

Lunar SSH Key
SHA256:
Added on Aug 2, 2022
Last used within the last 3 months — Read/write

Delete

ctf_droplet

Create a repo on github.com



Grab the URL for the repository

The screenshot shows the GitHub interface for the repository 'mwales / WildcatCSClub'. The 'Code' dropdown menu is open, displaying options for cloning the repository. The SSH URL is highlighted by a green arrow. The repository name 'WildcatCSClub' is also highlighted by a green arrow.

Repository: mwales / WildcatCSClub

Buttons: Unpin, Code (3), Fork (1), Star (2)

Clone options:

- Local
- Codespaces
- Clone
- HTTPS
- SSH
- GitHub CLI

SSH URL: `git@github.com:mwales/WildcatCSClub.git`

Additional options: Download ZIP

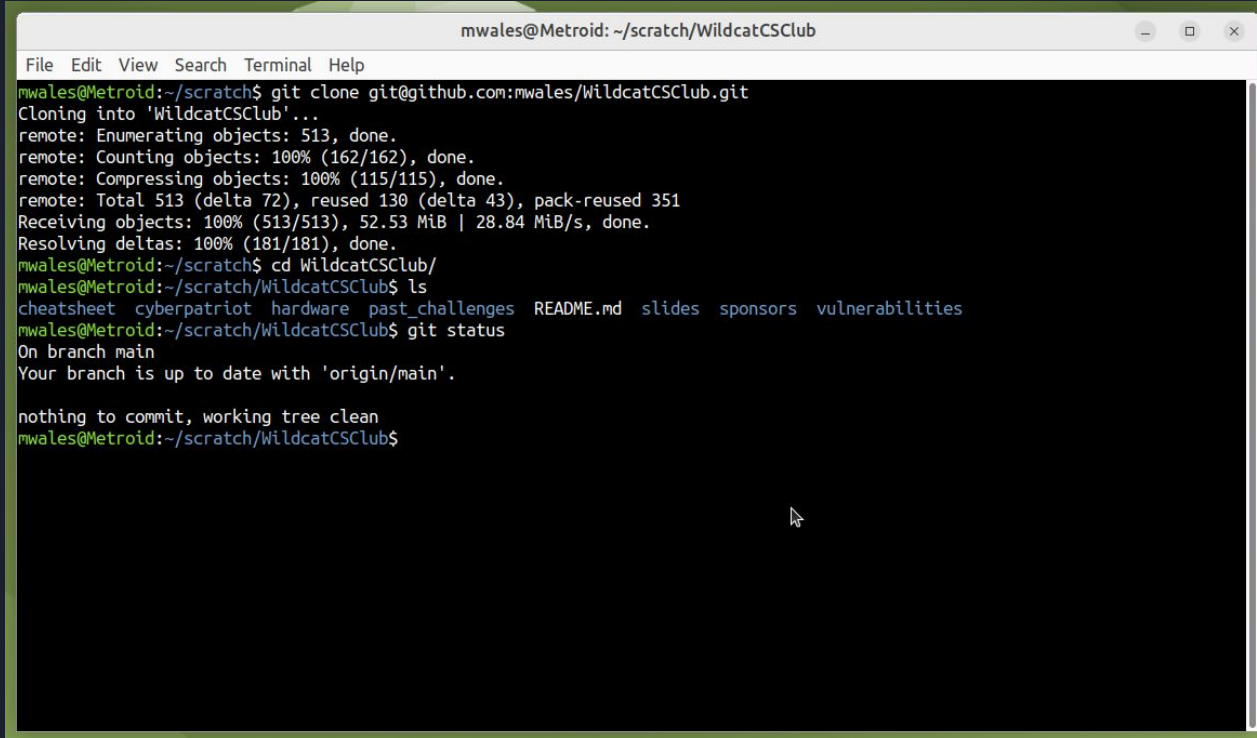
Repository description: WildcatCSClub

Repository content: cheatsheet, cyberpatriot, hardware/secret_vault, past_challenges, slides, sponsors, vulnerabilities, README.md

Repository statistics: 3 watching, 1 fork

Repository languages: Python 63.4%, C 21.1%, Shell 15.5%

Clone the repo



```
mwwales@Metroid: ~/scratch/WildcatCSClub
File Edit View Search Terminal Help
mwwales@Metroid:~/scratch$ git clone git@github.com:mwwales/WildcatCSClub.git
Cloning into 'WildcatCSClub'...
remote: Enumerating objects: 513, done.
remote: Counting objects: 100% (162/162), done.
remote: Compressing objects: 100% (115/115), done.
remote: Total 513 (delta 72), reused 130 (delta 43), pack-reused 351
Receiving objects: 100% (513/513), 52.53 MiB | 28.84 MiB/s, done.
Resolving deltas: 100% (181/181), done.
mwwales@Metroid:~/scratch$ cd WildcatCSClub/
mwwales@Metroid:~/scratch/WildcatCSClub$ ls
cheatsheet  cyberpatriot  hardware  past_challenges  README.md  slides  sponsors  vulnerabilities
mwwales@Metroid:~/scratch/WildcatCSClub$ git status
On branch main
Your branch is up to date with 'origin/main'.

nothing to commit, working tree clean
mwwales@Metroid:~/scratch/WildcatCSClub$
```

Update your code

```
mwailes@Metroid: ~/scratch/WildcatCSClub
File Edit View Search Terminal Help
mwailes@Metroid:~/scratch/WildcatCSClub$ ls
cheatsheet cyberpatriot hardware past_challenges README.md slides sponsors vulnerabilities
mwailes@Metroid:~/scratch/WildcatCSClub$ git status
On branch main
Your branch is up to date with 'origin/main'.

Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        modified:   README.md

no changes added to commit (use "git add" and/or "git commit -a")
mwailes@Metroid:~/scratch/WildcatCSClub$ git diff
diff --git a/README.md b/README.md
index b6bf753..e5a51e1 100644
--- a/README.md
+++ b/README.md
@@ -14,6 +14,8 @@ of the 50 or so challenges the we worked on over the year.
 * [2023 Code Quest Pictures](https://lockheedmartin.smugmug.com/Code-Quest/Code-Quest-2023/FL-Orlando/)
 * [Lockheed Martin Cyber Quest Information](https://www.lockheedmartin.com/en-us/who-we-are/communities/cyber-quest.html)
 * [2023 Cyber Quest Pictures](https://lockheedmartin.smugmug.com/CYBERQUEST/CYBERQUEST-2023/Orlando-FL/)
+* [2024 Code Quest Pictures](https://lockheedmartin.smugmug.com/Code-Quest/2024-Code-Quest/FL-Orlando)
+* [2024 Cyber Quest Pictures](https://lockheedmartin.smugmug.com/CYBERQUEST/Cyber-Quest-2024/FL-Orlando)

## Other possible in-person competition option for 2023-2024

mwailes@Metroid:~/scratch/WildcatCSClub$
```

add, commit, push

```
mwwales@Metroid: ~/scratch/WildcatCSClub
File Edit View Search Terminal Help
* [Lockheed Martin Cyber Quest Information](https://www.lockheedmartin.com/en-us/who-we-are/communities/cyber-quest.html)
* [2023 Cyber Quest Pictures](https://lockheedmartin.smugmug.com/CYBERQUEST/CYBERQUEST-2023/Orlando-FL/)
+* [2024 Code Quest Pictures](https://lockheedmartin.smugmug.com/Code-Quest/2024-Code-Quest/FL-Orlando)
+* [2024 Cyber Quest Pictures](https://lockheedmartin.smugmug.com/CYBERQUEST/Cyber-Quest-2024/FL-Orlando)

## Other possible in-person competition option for 2023-2024


mwwales@Metroid:~/scratch/WildcatCSClub$ git add README.md
mwwales@Metroid:~/scratch/WildcatCSClub$ git status
On branch main
Your branch is up to date with 'origin/main'.

Changes to be committed:
  (use "git restore --staged <file>..." to unstage)
        modified:   README.md

mwwales@Metroid:~/scratch/WildcatCSClub$ git commit -m "Added 2024 contest picture link"
[main 10e39fe] Added 2024 contest picture link
1 file changed, 2 insertions(+)
mwwales@Metroid:~/scratch/WildcatCSClub$ git push
Enumerating objects: 5, done.
Counting objects: 100% (5/5), done.
Delta compression using up to 16 threads
Compressing objects: 100% (3/3), done.
Writing objects: 100% (3/3), 377 bytes | 377.00 KiB/s, done.
Total 3 (delta 2), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (2/2), completed with 2 local objects.
To github.com:mwwales/WildcatCSClub.git
   5b5e36e..10e39fe  main -> main
mwwales@Metroid:~/scratch/WildcatCSClub$
```

Git history


Commits

 main

🔍 All users | 📅 All time


Commits on Apr 26, 2024

Added 2024 contest picture link

 mwales committed 2 minutes ago


Commits on Apr 5, 2024

New slides


 mwales committed 3 weeks ago

Commits on Apr 4, 2024


Still can't splel

 mwales committed 3 weeks ago


Fixed typo in writeup link

 mwales committed 3 weeks ago

Renamed directory for password checker writeup


 mwales committed 3 weeks ago

Password Checker partial writeup

 mwales committed 3 weeks ago

Commits on Apr 3, 2024

Fixing broken links in writeups and what not

 mwales committed 3 weeks ago

Adding some partial writeups as the year winds down

mwales@Metroid: ~/scratch/WildcatCSClub

File Edit View Search Terminal Help

commit 10e39fe716329cb1334314e01911ae40e03b49d1 (HEAD -> main, origin/main, origin/HEAD)
Author: Michael Wales <mwales3@gmail.com>
Date: Fri Apr 26 02:55:54 2024 -0400

Added 2024 contest picture link

commit 5b5e36eb26794aa0dce18c2aca60686050d9c816
Author: Michael Wales <mwales3@gmail.com>
Date: Fri Apr 5 03:22:12 2024 -0400

New slides

commit d0629dc8bd44b83efb6cc3472fc866f85b80fa8b
Author: Michael Wales <mwales3@gmail.com>
Date: Thu Apr 4 02:57:56 2024 -0400

Still can't splel

commit f4b9448045a69c2a51aede676999078944103d27
Author: Michael Wales <mwales3@gmail.com>
Date: Thu Apr 4 02:56:48 2024 -0400

Fixed typo in writeup link

commit d177dbb59d07f0a7693f3e11c38f4a029ff363e7
Author: Michael Wales <mwales3@gmail.com>
Date: Thu Apr 4 02:54:59 2024 -0400

Renamed directory for password checker writeup



Links

- <https://www.britannica.com/topic/ARPANET/A-packet-of-data>
- https://ethw.org/History_of_Lossless_Data_Compression_Algorithms
- <https://www.bleepingcomputer.com/news/security/over-12-million-auth-secrets-and-keys-leaked-on-github-in-2023/>
-