1.Welcome\_to\_the\_2020\_de1ctf

挂上梯子加入tgchannel，加入后根据提示得到flag

2. Misc杂烩/Misc Chowder

流量分析。使用wireshark导出所有包含的文件，知乎使用foremost批量提取可以得到7张图片，其中一张png是谷歌网盘的url截图，下载后使用binwalk不断分离（套娃）。

最后找到一个zip，最后爆破得到密码

3. mc\_champion

根据提示玩游戏，最后身上东西全卖掉换弓箭，打完会拿到加密信息

Encoded Message:

F5GUGMRQ

GIYC2RCF

IJKUOLKW

JFCVOORN

FEFFC4RR

KBDVG62G

GNYGQZJT

L5EGMTSU

GNPTA4ZN

KRBF6RTZ

OZYHE7T5

使用base32解密

/MC2020-DEBUG-VIEW:-)

Qr1PGS{F3phe3\_HfNT3\_0s-TB\_Fyvpr~}

再使用rot13解密

De1CTF{S3cur3\_UsAG3\_0f-GO\_Slice~}

4. Easy Protocol

hint为.cab文件，改后缀后拿到提示

