CERT Tapioca 1.0 and Expired CA Certificates

Problem:

After installing the mitmproxy CA certificate in a client system, you get an error in the client application stating that the website certificate is invalid. Depending on the browser used, the errors may include:

- NET::ERR_CERT_DATE_INVALID
- The certificate is not trusted because the issuer certificate has expired.
- This certificate has expired or is not yet valid

Cause:

When CERT Tapioca restarts the mitmproxy capture via `mitm.sh`, the `.mitmproxy` directory is copied from a static copy provided by Tapioca. This CA certificate expired on July 10, 2016 for CERT Tapioca 1.0.

Solution:

Delete the `~/.mitmproxy` directory:

```
rm -rf ~/.mitmproxy
```

Modify the `~/.mitm.sh` script to not copy over the `~/.mitmproxy` contents:

~/mitm.sh

```
#!/bin/bash

#cp -a ~/.mitmproxy_CA/* ~/.mitmproxy
sudo ~/iptables_mitmproxy.sh
mitmproxy -T -w ~/logs/flows.log
```

This can be done by commenting out the first line that begins with `cp`, or by removing it.