While updating some older TLS sigs in the ET Ruleset which do not make use of existing suricata buffers, I came across this a signature which detects malware using a hard-coded TLS request, specifically leveraging the first four bytes of the client random representing the GMT Unix Time.

Until this buffer is added, I am unable to fully convert the use to making use of buffers.

I see this is mentioned in [https://redmine.openinfosecfoundation.org/issues/1766](https://redmine.openinfosecfoundation.org/issues/1766) and documented in [https://redmine.openinfosecfoundation.org/projects/suricata/wiki/TLS_keyword_expansion](https://redmine.openinfosecfoundation.org/projects/suricata/wiki/TLS_keyword_expansion). However that issue is nondiscrete in it's asks.

**Related issues:**
Related to Feature #1766: TLS keyword expansion

I think this comes down to adding a 4 byte array to the state, then filling that from TLSDecodeHSHelloRandom and registering a new sticky buffer keyword to match on it.