## Zone Identifier ADS's

With the Advent of XP SP2 when a file[1] is downloaded from the internet (i.e. by clicking on a link in explorer[2]) to an NTFS volume an Alternate Data Stream (Zone.Identifier) is created along side the downloaded file (i.e. downloadedfile.exe:zone.identifier). The content of this file is used as a security by Windows XP as security data to determine the publisher/source of the file
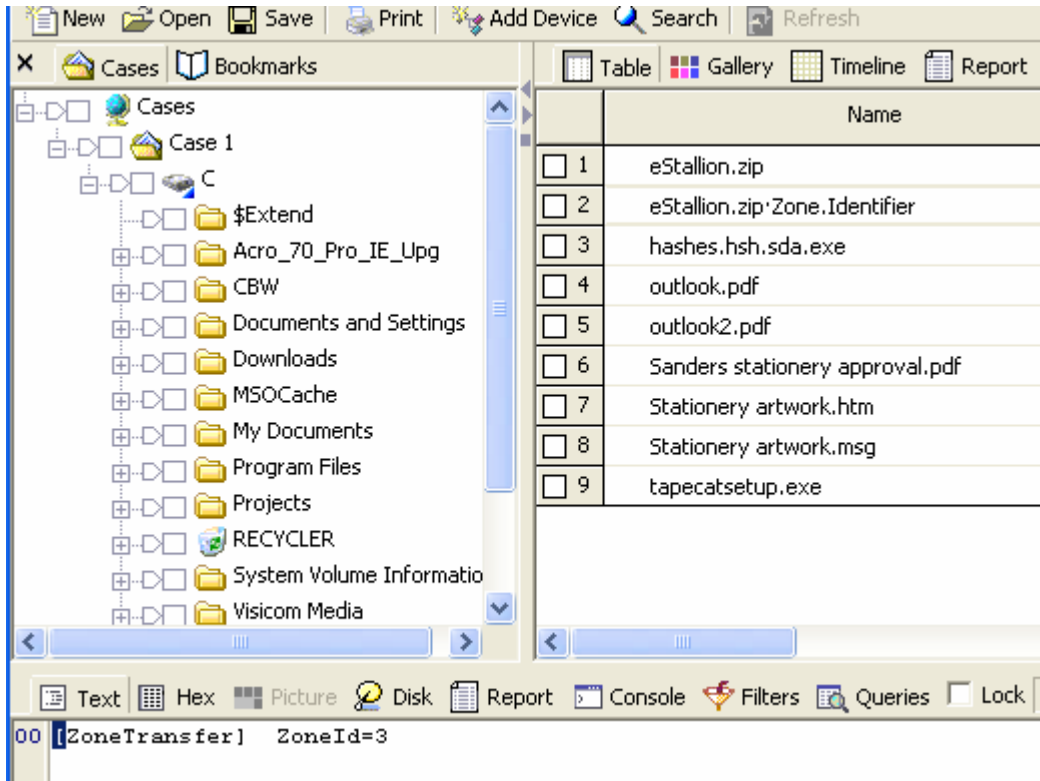


For a file downloaded from the Internet the content is typically

[ZoneTransfer]

ZoneId=3

---

[1] Checked with exe and zip files

[2] Note that a download from the internet via FTP using, say, CuteFTP or ftp via explorer will not result in an ADS being created

When you/the user chooses to execute the file a suitable waning as below is displayed



If the user chooses to Run the file but leaves the 'Always ask before opening this file' box checked the each time the file is run the dialog above will be displayed.

If the user un-checks the 'always ask…" box then the ADS will be deleted.

By looking at the properties of the file (right click – choose properties) the dialog below is displayed
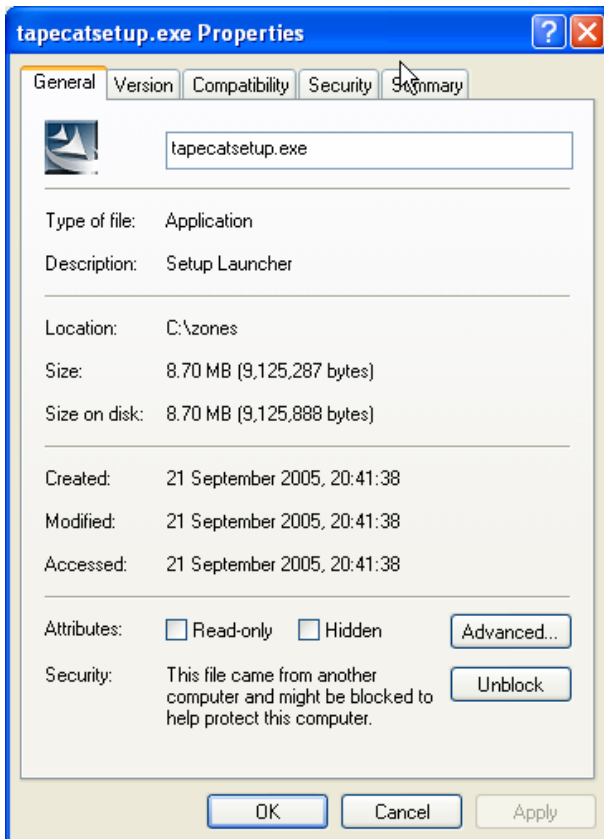


Note the security warning.

If the user clicks on the unblock button the ADS is deleted.

**What does this mean forensically?**

My research has been very limited but it seems that the zone referred to in the above is the security zones referenced in the Internet Options as below.
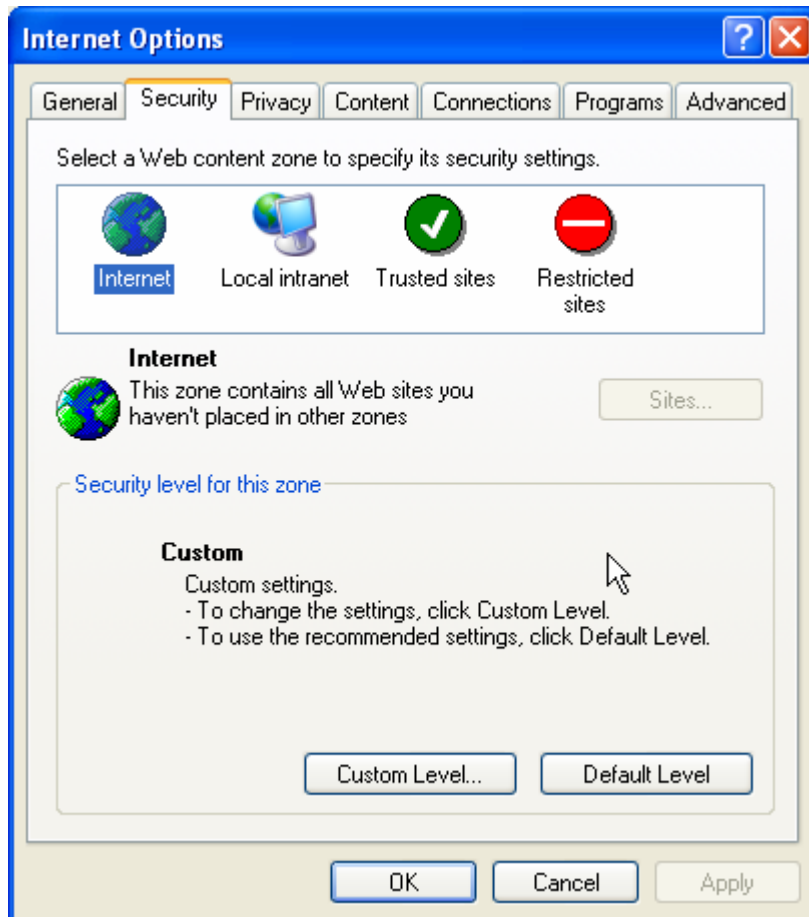


A link on MSDN enumerates the values that different zones can have. In general you should not see most of these and I expect that values in the Zone.Identifier are likely to be limited to values URLZONE_INTRANET and URLZONE_INTERNET (see below) and possibly URLZONE_UNTRUSTED. This of course still gives us useful intelligence as to where a file was obtained from

The values in the following table are either explicitly assigned, i.e.
URLZONE_USER_MIN = 1000 or are incrementing numbers i.e.
URLZONE_INTRANET      = 1
URLZONE_TRUSTED       = 2
URLZONE_INTERNET      = 3
URLZONE_UNTRUSTED   = 4

```
typedef enum tagURLZONE {

    URLZONE_PREDEFINED_MIN = 0,

    URLZONE_LOCAL_MACHINE = 0,

    URLZONE_INTRANET,

    URLZONE_TRUSTED,

    URLZONE_INTERNET,

    URLZONE_UNTRUSTED,

    URLZONE_PREDEFINED_MAX = 999,

    URLZONE_USER_MIN = 1000,

    URLZONE_USER_MAX = 10000
} URLZONE;
```

Experiment has shown that if you place a web site into the trusted zone then an ADS is not created when a file is downloaded.