ForensicX - Digital Forensics Report

COLLECTED_AT

"2025-05-23 22:47:17.383608"

SYSTEM_INFO

```
{
  "hostname": "AMAL",
  "platform": "Windows",
  "platform-release": "11",
  "platform-version": "10.0.26100",
  "architecture": "AMD64",
  "processor": "Intel64 Family 6 Model 140 Stepping 2, GenuineIntel",
  "ip-address": "172.20.10.7",
  "boot-time": "2025-05-23 22:05:13.474592"
}
```

RUNNING_PROCESSES

```
{'username': 'NT AUTHORITY\\SYSTEM', 'name': 'System Idle Process', 'pid': 0}
{'username': 'NT AUTHORITY\\SYSTEM', 'name': 'System', 'pid': 4}
{'username': None, 'name': '', 'pid': 140}
{'username': None, 'name': 'Registry', 'pid': 184}
{'username': None, 'name': 'smss.exe', 'pid': 736}
{'username': None, 'name': 'csrss.exe', 'pid': 872}
{'username': None, 'name': 'wininit.exe', 'pid': 1028}
{'username': None, 'name': 'csrss.exe', 'pid': 1036}
{'username': None, 'name': 'winlogon.exe', 'pid': 1128}
```

```
{'username': None, 'name': 'services.exe', 'pid': 1172}

{'username': None, 'name': 'LsaIso.exe', 'pid': 1180}

{'username': None, 'name': 'lsass.exe', 'pid': 1200}

{'username': 'AMAL\\Amal', 'name': 'esrv.exe', 'pid': 1212}

{'username': None, 'name': 'svchost.exe', 'pid': 1332}

{'username': None, 'name': 'fontdrvhost.exe', 'pid': 1368}

{'username': None, 'name': 'fontdrvhost.exe', 'pid': 1376}

{'username': 'AMAL\\Amal', 'name': 'svchost.exe', 'pid': 1388}

{'username': None, 'name': 'WUDFHost.exe', 'pid': 1456}

{'username': None, 'name': 'svchost.exe', 'pid': 1504}

{'username': None, 'name': 'svchost.exe', 'pid': 1520}
```

OPEN_PORTS

```
{'local_address': "addr(ip='127.0.0.1', port=51680)", 'remote_address': "addr(ip='127.0.0.1', port=49350)", 'status': 'TIME_WAIT', 'pid': 0}

{'local_address': "addr(ip='127.0.0.1', port=51684)", 'remote_address': "addr(ip='127.0.0.1', port=49350)", 'status': 'TIME_WAIT', 'pid': 0}

{'local_address': "addr(ip='172.20.10.7', port=138)", 'remote_address': '', 'status': 'NONE', 'pid': 4}

{'local_address': "addr(ip='::', port=49670)", 'remote_address': '', 'status': 'LISTEN', 'pid': 1172}

{'local_address': "addr(ip='::', port=49668)", 'remote_address': '', 'status': 'LISTEN', 'pid': 4728}

{'local_address': "addr(ip='0.0.0.0', port=912)", 'remote_address': '', 'status': 'LISTEN', 'pid': 6260}

{'local_address': "addr(ip='172.20.10.7', port=49408)", 'remote_address': "addr(ip='4.213.25.242', port=443)", 'status': 'ESTABLISHED', 'pid': 5872}

{'local_address': "addr(ip='127.0.0.1', port=51675)", 'remote_address': "addr(ip='127.0.0.1', port=49350)", 'status': 'TIME_WAIT', 'pid': 0}

{'local_address': "addr(ip='127.0.0.1', port=49351)", 'remote_address': '', 'status': 'LISTEN', 'pid': 1212}

{'local_address': "addr(ip='172.20.10.7', port=51653)", 'remote_address': "addr(ip='34.107.205.1', port=443)", 'status':
```

```
'TIME_WAIT', 'pid': 0}
{'local_address': "addr(ip='::', port=445)", 'remote_address': '', 'status': 'LISTEN', 'pid': 4}
{'local_address': "addr(ip='127.0.0.1', port=51676)", 'remote_address': "addr(ip='127.0.0.1', port=49350)", 'status': 'TIME_WAIT', 'pid': 0}
{'local_address': "addr(ip='::', port=21)", 'remote_address': '', 'status': 'LISTEN', 'pid': 5032}
{'local_address': "addr(ip='2401:4900:91cc:e675:64f9:7e38:2366:b356', port=51563)", 'remote_address': "addr(ip='2a03:2880:f368:120:face:b00c:0:167', port=443)", 'status': 'CLOSE_WAIT', 'pid': 4672}
{'local_address': "addr(ip='0.0.0.0', port=53281)", 'remote_address': '', 'status': 'NONE', 'pid': 14600}
{'local_address': "addr(ip='0.0.0.0', port=49667)", 'remote_address': '', 'status': 'LISTEN', 'pid': 2928}
{'local_address': "addr(ip='192.168.111.1', port=138)", 'remote_address': '', 'status': 'NONE', 'pid': 4}
{'local_address': "addr(ip='2401:4900:91cc:e675:64f9:7e38:2366:b356', port=51637)", 'remote_address': "addr(ip='2606:4700:83b2:7cbc:c276:427:5ff2:75c4', port=443)", 'status': 'TIME_WAIT', 'pid': 0}
{'local_address': "addr(ip='127.0.0.1', port=51646)", 'remote_address': "addr(ip='127.0.0.1', port=49350)", 'status': 'TIME_WAIT', 'pid': 0}
{'local_address': "addr(ip='127.0.0.1', port=51643)", 'remote_address': "addr(ip='127.0.0.1', port=49350)", 'status': 'TIME_WAIT', 'pid': 0}
```

FILE_HASHES

```
{
  "C:\\WINDOWS/System32/drivers/etc/hosts": {
    "MD5": "3688374325b992def12793500307566d",
    "SHA1": "4bed0823746a2a8577ab08ac8711b79770e48274",
    "SHA256": "2d6bdfb341be3a6234b24742377f93aa7c7cfb0d9fd64efa9282c87852e57085"
  },
  "C:\\WINDOWS/System32/cmd.exe": {
    "MD5": "e86a8609fea011c240950f5369d12714",
    "SHA1": "7b2fd51a940ab72605853e43b6857f3b93ee86b0",
    "SHA256": "83c991bf32bbc3546eb62f45f9b3fd35abbf5bbb7e57ef8ea298822bfd4788ab"
  }
}
```

USB_DEVICE_HISTORY

BROWSER_HISTORY

Found Chrome History file at: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History

RAM_SNAPSHOT

```
{'pid': 0, 'name': 'System Idle Process', 'memory_MB': 0.01}

{'pid': 4, 'name': 'System', 'memory_MB': 3.54}

{'pid': 140, 'name': '', 'memory_MB': 38.46}

{'pid': 184, 'name': 'Registry', 'memory_MB': 25.43}

{'pid': 736, 'name': 'smss.exe', 'memory_MB': 0.0}

{'pid': 872, 'name': 'csrss.exe', 'memory_MB': 1.31}

{'pid': 1028, 'name': 'wininit.exe', 'memory_MB': 0.02}

{'pid': 1036, 'name': 'csrss.exe', 'memory_MB': 2.11}

{'pid': 1128, 'name': 'winlogon.exe', 'memory_MB': 1.23}

{'pid': 1172, 'name': 'services.exe', 'memory_MB': 6.72}

{'pid': 1180, 'name': 'LsaIso.exe', 'memory_MB': 0.02}

{'pid': 1200, 'name': 'lsass.exe', 'memory_MB': 14.09}

{'pid': 1212, 'name': 'esrv.exe', 'memory_MB': 19.46}

{'pid': 1332, 'name': 'svchost.exe', 'memory_MB': 19.33}

{'pid': 1368, 'name': 'fontdrvhost.exe', 'memory_MB': 2.71}

{'pid': 1376, 'name': 'fontdrvhost.exe', 'memory_MB': 0.15}

{'pid': 1388, 'name': 'svchost.exe', 'memory_MB': 2.27}

{'pid': 1456, 'name': 'WUDFHost.exe', 'memory_MB': 7.47}
```

```
{'pid': 1504, 'name': 'svchost.exe', 'memory_MB': 12.27}

{'pid': 1520, 'name': 'svchost.exe', 'memory_MB': 8.82}
```

SCREENSHOT_FILE

```
"ForensicX_Report\\screenshot.png"
```