

## User Documentation for FEX Utility

**FEX** (Forensic Exploration Tool) is a command-line utility designed for digital forensic investigations. It provides a range of features to help investigators analyze system states, processes, services, and more. Below is a detailed outline of the available commands and their functions.

---

### Table of Contents

1. General Usage
  2. Commands Overview
  3. Command Details
    - [1. drives](#)
    - [2. hash](#)
    - [3. ipinfo](#)
    - [4. memdump](#)
    - [5. netstat](#)
    - [6. now](#)
    - [7. procdump](#)
    - [8. prockill](#)
    - [9. procllist](#)
    - [10. servlist](#)
    - [11. timecheck](#)
    - [12. usbinf](#)
    - [13. users](#)
- 

### General Usage

Run the FEX utility from the command line with the desired command and parameters (if required).

#### Syntax:

```
FEX <command> [parameters]
```

#### Example:

```
FEX procllist
```

Use `FEX help` to display the full list of available commands or `FEX help <command>` for details about a specific command.

---

### Commands Overview

Command	Description
drives	Lists all connected drives and their capacities.
hash	Generates file hashes for integrity checks.
ipinfo	Lists all IP address information.
memdump	Dumps memory for all processes to a file.
netstat	Displays active network connections.
now	Displays the current date and time.
procdump	Dumps memory for a specific process.
prockill	Terminates a process by name or ID.
proclist	Lists all running processes and their IDs.
servlist	Lists all services with statuses and types.
timecheck	Compares system time to an internet time server.
usbinfo	Lists all connected USB devices.
users	Displays system user accounts and logon info.

---

## Command Details

### 1. drives

**Description:** Lists all connected drives along with their type, total size, and free space.

**Usage:**

```
FEX drives
```

**Example Output:**

Drive	Type	Total Size	Free Space
-----			
C:\	Fixed	500 GB	200 GB
D:\	CD-ROM	Not Ready	Not Ready
E:\	Removable	32 GB	10 GB

---

### 2. hash

**Description:** Generates cryptographic hashes for a file.

**Usage:**

```
FEX hash <file_path>
```

**Example:**

```
FEX hash C:\example.txt
```

---

### 3. ipinfo

**Description:** Lists all IP address information for network interfaces on the system.

**Usage:**

```
FEX ipinfo
```

---

### 4. memdump

**Description:** Creates memory dumps for all running processes and saves them to the specified directory.

**Usage:**

```
FEX memdump <output_directory>
```

**Example:**

```
FEX memdump C:\Dumps
```

---

### 5. netstat

**Description:** Displays active network connections, including local and remote IP addresses, ports, and states.

**Usage:**

```
FEX netstat
```

**Example Output:**

Proto	Local Address	Foreign Address	State
TCP	192.168.1.100:443	203.0.113.5:5023	ESTABLISHED
UDP	0.0.0.0:68	*:*	LISTENING

---

### 6. now

**Description:** Displays the current system date and time in ISO 8601 format.

**Usage:**

```
FEX now
```

**Example Output:**

```
2024-11-27T22:45:21.1234567Z
```

---

## 7. procdump

**Description:** Creates a memory dump for a specific process.

**Usage:**

```
FEX procdump <process_name_or_id> <output_directory>
```

**Example:**

```
FEX procdump notepad C:\Dumps
```

---

## 8. prockill

**Description:** Terminates a process by name or ID.

**Usage:**

```
FEX prockill <process_name_or_id>
```

**Examples:**

- Kill by process name:

```
FEX prockill notepad
```

- Kill by process ID:

```
yaml
```

```
FEX prockill 1234
```

---

## 9. proclist

**Description:** Lists all running processes with their names and process IDs.

**Usage:**

```
FEX proclist
```

**Example Output:**

Process Name	Process ID
notepad	1234
explorer	5678
chrome	9102

---

## 10. servlist

**Description:** Lists all services, including their statuses (e.g., Running, Stopped) and startup types (e.g., Automatic, Manual).

**Usage:**

```
FEX servlist
```

---

## 11. timecheck

**Description:** Checks the system time against an internet time server and reports discrepancies.

**Usage:**

```
FEX timecheck [time_server_url]
```

- **Without URL:** Uses a default internet time server.
- **With URL:** Compares time to the specified time server.

**Example:**

```
FEX timecheck http://worldtimeapi.org/api/timezone/Etc/UTC
```

---

## 12. usbinfo

**Description:** Lists all connected USB devices, including their names, manufacturers, and statuses.

**Usage:**

```
FEX usbinfo
```

**Example Output:**

Device Name	Manufacturer	Status
SanDisk USB Flash Drive	SanDisk	OK
Logitech Webcam	Logitech	OK
Generic USB Hub	Microsoft	OK
USB Composite Device	Unknown	OK

---

## 13. users

**Description:** Lists all system users along with logon details and statuses.

**Usage:**

```
FEX users
```

---

## Additional Information

- **Help:** Use `FEX help` to display the list of available commands.
- **Errors:** If an unknown command is entered, the utility will display `Unknown command!`

## User Documentation for FEX Utility

**Copyright © 2024 Experts in Software Engineering, LLC. All Rights Reserved.**

This document and the FEX Utility software are proprietary to Experts in Software Engineering, LLC. Unauthorized reproduction, distribution, or modification of this document or associated software, in whole or in part, is strictly prohibited.

FEX Utility is provided as-is for investigative purposes. Experts in Software Engineering, LLC makes no warranties regarding the accuracy, reliability, or suitability of the software for any specific purpose. Use at your own risk.

For inquiries or support, please contact:

- **Company:** Experts in Software Engineering, LLC
- **Website:** [www.ExpertsInSoftware.com](http://www.ExpertsInSoftware.com)